TELKOMNIKA, Vol.11, No.11, November 2013, pp. 6534~6539
e-ISSN: 2087-278X

Autonomy Domain Trust Model in Manufacturing Grid based on User Trust Agent

Junyu Xiao*, Zhangwei Yang, Feng Jiang
Department of Education and Technology, Pingxiang University, Pingxiang 337000, Jiangxi, China
*Corresponding author, e-mail: 26945824@qq.com

Abstract

Trust security is one of the hotspot in manufacturing grid. The paper proposes a trust model to suit for manufacturing grid, based on domain trust model. It manages trust value of grid user from the introducing of user trust agent in autonomy domain. Furthermore, it considers the impact of time decay and the punishment of malicious transactions. The model is effective in reducing the malicious transaction of grid user to improve security of manufacturing grid through analysis and experiment simulation.

Keywords: *autonomy domain, trust agent, manufacturing grid, trust model*

1. Introduction

The Grid technology is strongly recommended network infrastructure. Grid computing system is integrating distributed calculation, storage and knowledge etc together into a virtual super computer. By this way, resources-sharing is improved greatly. Grids tend to be more loosely coupled, heterogeneous, geographically dispersed and flexible. So Grid system is much more complicated than traditional Internet environment. In order to make the Grid computing more securely, more attracting and more conveniently communicate between grid entities, the security between entities seems extraordinarily important.

Trust is an important aspect of grid security. It is an important method of guarantee security of grid. In the gird calculation environment, good trust relationship should be set up between nodes. The current high-performance calculating systems are based on trust policy to open to users. Grid nodes can be adjusted and updated trust relationship through historical direct or indirect contacting experience. It maximizes the security in the grid.

With the advancement in networking and multimedia technologies enables the distribution and sharing of multimedia content widely. In the meantime, piracy becomes increasingly rampant as the customers can easily duplicate and redistribute the received multimedia content to a large audience. Insuring the copyrighted multimedia content is appropriately used has become increasingly critical.

Although encryption can provide multimedia content with the desired security during transmission, once a piece of digital content is decrypted, the dishonest customer can redistribute it arbitrarily [2, 3].

2. Based on Domain Trust Model

According to different structure and different location of grid entities (including grid service provider and grid users), grid can be divided into lots of independent autonomy domain. Each autonomy domain includes lots of grid entities. There are independent administrative strategies and security strategies between autonomy domains.

There are trust relationship and trust choice between gird entities. The grid environment is dynamic and uncertain. The trust relationship should be known when interactions occur between entities. Reference 4 mentioned designing ideas based on reputation-based trust model. It divide grid into several management domains. The trust relationship between nodes is divided into trust within domains and trust between domains. Different strategies are taken to deal with these different trust relationships. The complexity of calculating trust value within domain depends on the numbers of nodes. Instead the complexity of calculating trust value

Received April 12, 2013; Revised June 19, 2013; Accepted July 20, 2013

between domains depends on the numbers of domains. In this model, the number of the entities is the only parameter of complexity of calculating trust value. The advantage is the complexity of calculation is low. But there are also some disadvantages such as: no consideration of context. Normally context environment is a determinant of trust. There are no setup method of initial trust and trust value updating. No consideration of the effect of time attenuation affecting trust value which reduce the exactness of trust. No consideration of punishment of malicious nodes which reduce the trust security.

There are weakness of low exactness of trustworthiness and low grid security based in traditional domain trust model. Experts proposed several improved models. Reference 5 mentioned trust model which based on Dempster-Shafer (D-S) proof theory trust model. According to relevant rules, evaluate the trustworthiness into three categories(trustworthy, not trustworthy and unsure) . In reference 6 the trustworthiness based on fuzzy set was discussed. It categorizes trustworthiness into different degree and set up trust set function. In reference 7 the trustworthiness based on joint probability distributions was discussed. In reference 8 the trustworthiness based on action was discussed. Use trust and reputation as measurement. Use trust attenuation function to reflect the change of trust according to time. Aforementioned trust models make improvement based on traditional trust model from aspects of context, time attenuation etc. The grid security is improved significantly.

3. Trust Study on Manufacturing Grid

Manufacturing Grid is a special kind of grid. It use sound grid environment to set up manufacturing coordinating model. Manufacturing grid has characteristics of common grid such as sharing, open and coordination. But at the same time there are potential safety hazard such as malicious entity cheating. The trust conception is introduced in Grid. A reliable third party is set up which calculate the value of trustworthiness. By this way, the Qos of Grid is improved. In the manufacturing Grid, there is no reliable third party. It is difficult to set up trustworthiness between entities.

Manufacturing grid is widely distributed and complicated. The reasonable division of autonomy domain will affect the setup of trust. In reference 9 it discussed manufacturing grid resources service Trust-Qos evaluation model. It divides resources into 9 autonomy domains. It also divides the trust evaluation into within domain and between domains. In reference 10, it discussed the manufacturing resources reputation model in manufacturing grid environment. It divides the enterprise's reputation into resource reputation and service reputation. For the resource reputation is the initial configuration trust evaluation value. After cooperation, the trust value was updated according to experience. These two models are directly evaluating the trust value. There is no consideration of trust recommendation. But in manufacturing grid it is a most important part. Besides, both models don't consider the time attenuation and punishment to malicious action. The malicious action in manufacturing grid will affect more seriously than other grid environment such as resource grid or calculation grid. A failed transaction may affect the survival of the manufacturer.

4. Manufacturing Grid User Trust Agent

In the manufacturing grid environment, there are many entities, these entities are dynamic. To grid entities, autonomy domains are comparably stable. So he trust model based on autonomy domain is suitable.

4.1. GSP Directly Manage User Trust

In autonomy domain, the participants in the grid exchange are grid users and grid service providers. Only if trust relationship is set up can they exchange reliably. There are many GSP and grid users in one autonomy domain. In the user trust list of GSP, there are many user credit records in different GSP. Like Figure 1.

Use GSP to directly manage the relationship with grid users. It requires GSP high efficiency of handling. When grid users request service, GSP will handle according to below procedures.

Step 1: User A request service from GSP. In order to safeguard the reliability of service, User A need GSP with high standard Qos. I.e. meet certain trustworthiness.

Step 2: GSP will seek trust value of the grid user in the user trust list file. If it is under the trust line, the exchange will be refused. The grid user need request service to other GSP till get permit. Then the GSP will provide resources and service to UserA.

Step 3: When UserA get service and finish exchange. It will submit result to GSP and request GSP to update the credit profile.

Step 4: When GSP receive request, it will update user trust list. Then the transaction is finished.

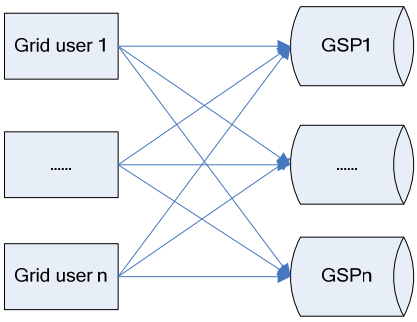

Figure 1. GSP Directly Manage User Trust

In the manufacturing grid, the method of using GSP to directly manage user trust has such advantages as simple calculation and high performance efficiency. But there are still some disadvantages in the practical use as below: 1)in the manufacturing grid, the number of grid users is huge. One GSP need handle lots of request from grid users at the same time. So The trust management efficiency is low. 2) GSP has weakness of dynamics and uncertainty which make the exchange between grid users low reliability. 3) Malicious users will register as new users anytime and send service request to GSP. It will waste much resource of GSP. So GSP can not recognize malicious users easily. 4)The exchange result is got from independent user, the accuracy of the trust evaluation is not so high.

4.2. Introduction of User Trust Agent

In order to solve aforementioned problems, this paper introduces autonomy domain user trust Agent UTA. As the trustworthy third party, UTA manage the Credit of autonomy domain grid users. Both GSP and grid users will check the behavior of UTA and get reference trust value. The UTA model is like below graphic.

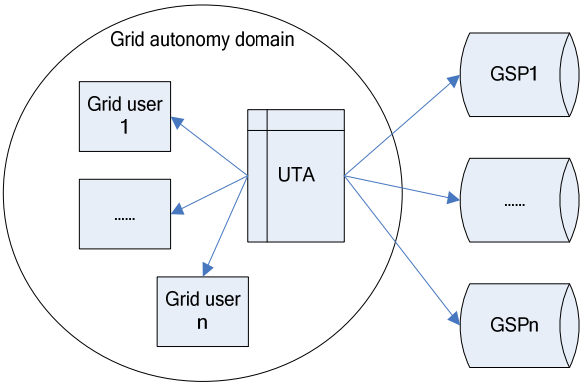

Figure 2. UTA Trust Model

When grid user request service, the UTA model will handle according to below procedure:

Step 1: UserA send request to UTA to get GSP list which meet trust conditions.

Step 2: According to the historical exchange records between Grid users and GSP, UTA evaluate the trustworthiness of these GSP. Upon the request from UserA, UTA will response qualified GSP list to UserA.

Step 3: UserA will choose one familiar GSP and request resources and then response the result to UTA.

Step 4: When UTA receive the response result, it will extract the user's trust profile in the autonomy domain and will issue trust certificate to User A.

Step 5: UserA will request service with submitting the certificate to appointed GSP. GSP will decide whether provide service or not according to the trustworthy level in the certificate.

Step 6: If GSP accept to provide service, then UserA and GSP begin to exchange. After the transaction, both parties will response the result to UTA. UTA will update the trust records of both then the transaction is over. If GSP doesn't accept to provide service, UserA need choose GSP again then revert to Step5.

After introducing autonomy domain UTA to manufacturing grid trust model, UTA become reliable third party to both grid users and GSP. The transactions are carried out based on the trust records provided by UTA. From the perspective of Grid user, the trust model is like below procedure in Figure 3.

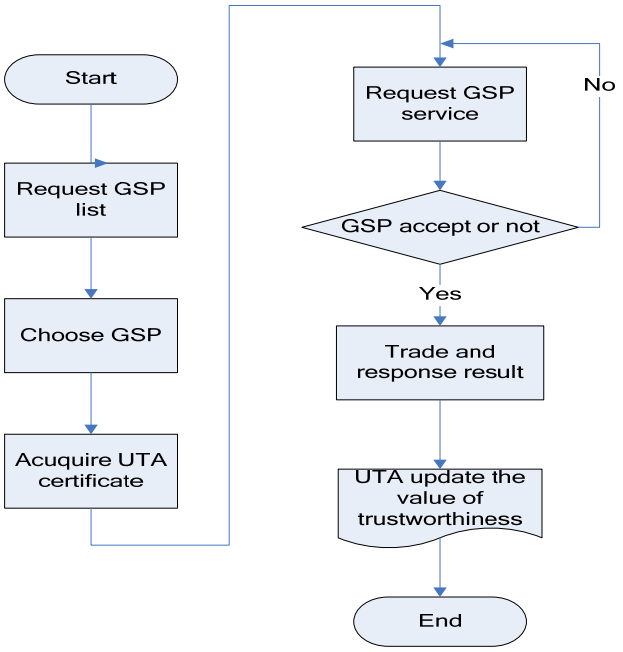

Figure 3. Trust Model Procedures

Compared to the trust model of GSP directly managing users, UTA has such advantages as higher management efficiency, higher reliability and higher safety. GSP only need face UTA instead of huge numbers of users. By this way the trust evaluation and management efficiency are improved. At the same time, grid users only need face the stable UTA instead of dynamic GSP. UTA has high authorities in autonomy domain. It can manage grid users effectively and avoid of cheating. UTA can get transaction records of all grid users and GSP in the domain. By this way, the trust evaluation result will be more accurate.

4.3. Punishment on Malicious Trade

In manufacturing grid, the harm of malicious trade is much higher than normal grid. It will lead to critical crisis of the enterprise. So in the manufacturing grid model, the punishment to malicious trade must be introduced. Every transaction of grid user must be carried out through the certificate issued by UTA. By this way, UTA can accurately tell whether the user exchange maliciously.

For example of User A, Ns represent the successful trade numbers in UTA kept records, Nf represent failed numbers. So the value of trustworthiness T is calculated as:

$$T = \frac{\mathrm{Ns}}{\mathrm{Ns} + \lambda \mathrm{N_f}} (\lambda \geq 1) \quad (1)$$

λ is punishment factor. When the number of malicious trade is bigger, the value of λ will be bigger. It will reduce the value of trustworthiness of UserA. Finally it will be excluded by UTA. In order to safeguard the safety of manufacturing grid, λ will be progressively increased base on exponent 10. For example, if the UserA made one malicious trade, λ is 10, if made two malicious trading, λ is 10×10, three times 10×10×10 …. If UserA make more malicious trade, the trust value will be nearly 0. So it can avoid malicious attack to manufacturing grid.

At the same time, considering the factor of time attenuation affecting trustworthiness. The nearer the transaction is, the more trustworthy it is. in order to show the recent trade affect trustworthy more, when UTA get transaction records, it can set one parameter Sum. Extract recent transactions to calculate the value of trustworthiness T. Normally when Sum is smaller, it can embody clearer about time attenuation. But when malicious trade appears, using sum can not accurately calculate the value of trustworthiness. In order to easily recognize malicious users, non-fixed value should be taken to determine Sum. For the recent malicious users, if the value of sum is smaller, the effect of punishing malicious trade is clearer. F represents times of malicious trade. Below table records the updating trustworthiness profile.

Table 1. UserA Trustworthiness Profile

F	Sum	λ	Ns	N_f	T
1	1000	10	999	1	0.9901
2	500	100	498	2	0.7135
3	200	1000	197	3	0.0616
4	100	10000	96	4	0.0024

When Grid user and GSP finish transaction and response the result to UTA, UTA will update the history transaction records taking sum transactions to calculate the value of trustworthiness and update the trust profile to the user. Next time when the user request service it will be recorded in the trust certificate. If one user made several malicious transactions, the value of trustworthiness is nearly o, so it will be kicked off the manufacturing grid.

4.4. Simulation Experiment and Result Analysis

In order to verify the effectiveness of the introduction of UTA, a simulation experiment is carried out in a model calculating grid environment. The experiment contains two parts part A is Grid User request service directly from GSP. Part B is Grid User request service from UTA. After request service, the total transactions are 100 times with 5 malicious trade. Figure 4 shows the value of trustworthiness under two parts.

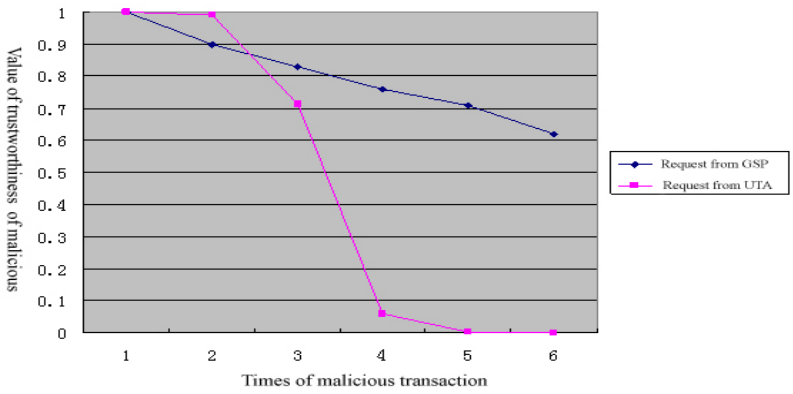

Figure 4. Value of Trustworthiness Change

The experiment shows with the increase of malicious trade, the value of trustworthiness under the model of GSP direct management is decreased slightly. It will make the malicious users keep malicious exchange with GSP. In the manufacturing grid it is not allowed. However in the UTA model, if two malicious transactions appears, the value of trustworthiness of malicious user will be decreased significantly nearly to 0. It avoid the further malicious transactions and safeguard the whole security of manufacturing grid.

Furthermore, the model of GSP direct manage user's trust can not Resist the white washing attack between new users and malicious users through transforming identity. Based on the model of this article, malicious users's continuous or random White Washing attack will be reduce the penalty factor credit quickly after the success of previous attacks by GSP. When the malicious user's trust close to 0, GSP no longer trust the proxy that an attacker can not be sustained, and curb malicious attacks effectively.

5. Conclusion

Manufacturing grid requires strict security of grid. Autonomy domain trust model calculates and evaluates the value of trustworthiness of entities which is the basis of resources sharing and coordination. With the introduction of UTA in autonomy domain grid user trust management and the consideration of time attenuation and punishment to malicious trade, the value of trustworthiness of users is more accurately calculated. The security problem in manufacturing grid is effectively solved.

References

[1] Foster I, Kesselman C, Tuecke S. The anatomy of the grid: Enabling scalable virtual organizations. *International Journal of Supercomputer Applications*. 2001; 15(3): 1-10.
[2] Zhangwei Yang. Shaobin Huang. *Research on trust model in autonomous domain of campus grid*. Proceedings of 2011 International Conference on Computer Science and Service System. 2011; 1670-1673.
[3] Rahman A, Hailes S. *Supporting Trust in Virtual Communities.* Proceedings of the 33rd Hawaii International Conference on System Sciences. 2000; 6007-6016.
[4] A Josang, SJ Knapskog. *A metric for trusted systems.* Proceedings of the 21st National Information Systems Security Conference. 1998; 16-29.
[5] Azzedin F, Muthucumaru Maheswaran. *Towards Trust-Aware Resource Management in Grid Computing Systems.* Proceedings of the 2nd IEEE/ACM International Symposium on Cluster Computing and the Grid. 2002; I-6.
[6] Li xiaoyong, Gui Xiaolin. Quantified trust model based on multi-dimension decision in reliable network. *IT Journal*. 2009; 32(3): 405-416.
[7] A Josang, S Hird, E Faccer. *Simulating the Effect of Reputation Systems on e-Markets.* Proceedings of the First International Conference on Trust Management. 2003; 179-194.
[8] Hu yefa, Tao fei, Zhou zude. Manufacturing grid resources service Trust-QoS evaluation and application. *Chinese Journal of Mechanical Engineering*. 2007; 43(12): 131-136.
[9] Wang Xiaolin, Zhang Yun, Qing Zhaobo. Study on the decision-making method of manufacturing partner selection under virtual enterprise environmen. *China Mechanical Engineering*. 2007; 18(10): 1197-1200.
[10] Foster I, Kesselman C, Nick J, Tuecke S. Grid services for distributed system integration. *IEEE Computer*. 2002; 35(6): 37-46.
[11] Ma li, Zheng weimin. Synthesize trust degree evaluating model for an information grid environment. *Journal of Tsinghua University (Sci &Tech).* 2009; 49(4): 599−603.