ISSN 1512-1232

# TRUST MODEL TO PRESENT A POOL OF PROVIDERS FOR RESOURCE SELECTION IN GRID COMPUTING

Vivek Ananth P
Lecturer-Botho college, Gaborone, Botswana, vivek.jubilant@gmail.com

***Abstract***

*A Grid integrates, coordinates resources and users from different domains. Grid computing is an interconnected computer system, where machines share resources that are highly heterogeneous. Grid computing and its related technologies will only be adopted by users, if they are confident that their data and privacy are secured, and the system is as scalable, robust and reliable as of their own, in their places. Trust and reputation systems have been recognized as playing an important role in decision making on the internet. Reputation based systems can be used in a Grid to improve the reliability of transactions. Reliability is the probability that a process will successfully perform its prescribed task without any failure at a given point of time. Hence, ensuring reliable transactions plays a vital role in grid computing. To achieve reliable transactions, mutual trust must be established between the initiator and the provider. Trust is measured by using reputation, where reputation is the collective opinion of others. If there are 'n' number of providers of a particular type of job, then all the providers are taken in to account. The total trust is calculated for all the providers and a ranked list of the providers is made available. If the provider with the highest rank is not available, then the next provider in the rank list may be approached. Thus, the user can choose the best available provider.*

## 1 INTRODUCTION

Grid computing is an enhanced form of distributed computing. The main purpose of security mechanisms in any distributed environment is to provide protection against malicious parties. There is a whole range of security challenges that are yet to be met by traditional approaches. Traditional security mechanisms such as authentication and authorization will typically protect resources from malicious users, by restricting access to only authorized users. However, in many situations users have to protect themselves from those who offer resources so that the problem in fact is reversed. Information providers can deliberately mislead by providing false information, and traditional security mechanisms are unable to protect against this type of security threat. Since Grid computing facilitates the sharing of computational resources, it badly needs a system which takes care of such security threats. Trust and reputation systems on the other hand can very well provide protection against such threats. The difference between these two approaches to security was first described by Rasmussen & Jansson [1996] who used the term hard security for traditional mechanisms like authentication and access control, and soft security for what they called behavior control mechanisms .Trust and reputation systems are examples of soft security mechanisms. The Trust model based on Reputation can very well address this problem. More over the Reputation based model can assure behavior conformity. Behavior conformity can be measured by using behavioral trust which can be defined as fulfilling the expectation of others.

Reputation models can be modeled in such a way that they could provide reliability for both users and providers. Reputation systems provide a way for building trust through social control by utilizing community based feedback about past experiences of peers to help making recommendations and judgments on the quality and reliability of the transactions. These kinds of models are vital for a Grid computing system where the trust relationship is one of the important issues.

ISSN 1512-1232

## 2 LITERATURE SURVEY

A number of disciplines have looked at various issues related to trust, including the incremental values assigned by people in transactions with a trusted party and how trust affects people's beliefs and decision making. Considerable work has been done on trust in computer science, most of them being focused in the area of security. Formal logical models [Burrows 1990 , Frendrup 2002] have been used in the context of cryptography and authentication. Recently, due to the emergence of e-commerce, there has been a great progress in developing computational models of trust. Ba, Whinston, and Zhang [2002], provided a game theoretic approach of trust and conclude that in the presence of an authenticating third party, the most utilitarian course of action for a user is to behave honestly. A number of models have been proposed, and among those models, the eBay system is the most widely known reputation model. [Kollock 1999, Resnick 2000, Resnick 2002, Snyder 2000].

The simplest form of computing reputation scores is proposed by Resnick and Zeckhauser [2002], who simply measure the reputation by finding the sum of the number of positive ratings and negative ratings separately, and evaluate the total score as the positive minus the negative score. The advantage is that, it is a very simple model where anyone can understand the principle behind the reputation score, while the disadvantage is that it is primitive, and therefore does not give the correct picture of the participants' reputation.

Advanced models in this category compute a weighted average of all the ratings, where the rating weight can be determined by factors such as the raters' trustworthiness, reputation, the age of the rating, the distance between the rating and current score, etc. Xiong and Liu [2004] used an adjusted weighted average of the amount of satisfaction that a user gets for each transaction. The parameters of the model are the feedback from transactions, the number of transactions, the credibility of feedbacks and the criticality of the transaction.

Trust and reputation systems have been recognized as playing an important role in decision making in the Internet world [Grandison , Sloman 2000] and [Jøsang, Ismail 2007]. Customers and sellers must trust themselves and the services they are offered and offer. Regarding the grid systems, the fundamental idea is that of resource sharing [Foster et al 2001].

Internet sites mainly use summation-based reputation systems. These systems are based on counting all votes or grades an entity receives. The votes can be counted simply on behalf of the user or they can be averaged or weighted. As summation-based reputation systems are mainly used in e-commerce marketplaces, they are mostly centralized. Their big advantage is the simplicity of the reputation scheme. This makes the reputation value to be easily understood by the participants and allows a direct conversion between reputation assessment and trust. The most widely known reputation system of this kind is the eBay. Other systems are the Amazon, Epinios, BizRate etc. [http:// www.Amazon.com, http://www.epinios.com, http:// www.bigrate.com, Silaghi, 2007].

## 3 TWO WAY TRUST MODEL TO SELECT PROVIDER'S POOL

In order to facilitate users to select the best provider, I have designed and developed a trust model based on reputation. Hence, this model provides comprehensive choices for the user.

The initiator places a request for a resource randomly. The users can request for the resource printer, computing or file sharing. The providers are categorized into three groups. One group of providers does file sharing; the second group of providers handles printing and the third group deals with a computing job. There can be several overlaps in these groups. Many providers can do more than one job.

The new Model which includes the two way test criterion, and considers the factors of context and size.

The New Model checks all the possible providers and displays a ranked list of providers on the basis of trustworthiness. Such an effort to make a selection of all possible providers may take a long time, therefore an entity as soon as gets at least four providers with a trust value above the

ISSN 1512-1232

threshold, which is set higher than the minimum trustworthiness,; then the search stops and the results are displayed.

## 4 EXPERIMENTS AND RESULTS

The simulation is done by considering the three models:

- The Stakhanova Model.
- The PATROL Model
- My new enhanced model

For the simulation study fifteen entities A,B,C,D,E,F,G,H,I,J,K,L,M,N,O are considered. F is the initiator and it requests for printing job. Out of these fifteen entities E, F, J, N are assumed to do only file sharing. C,I,K,O do printing job, and H provides computing alone. Among these entities B provides all the three kind of jobs. A provides both file sharing and printing. L and M provide both file sharing and computing. G and D provide both printing and computing. This categorization is incorporated in this model. In order to simplify the presentation size parameter has not been considered.

It is to be noted that Stakhanova and PATROL Model do not provide categorization of jobs. Therefore we have done the first simulation study with out providing categorization of jobs for these two models. This simply means that the two models assume, if a provider is good say, in computing and if he provides printing service, then in that also he will be good. On that basis, there will be a single trust value for each provider, irrespective of the nature of the job. Thus we have done our first simulation study, with out categorization for these two models and with categorization for New Model.

In the first set-up F is the initiator. F requests for printing. All the providers who provide this service is considered. In the first model that is Stakhanova model the total mistrust is calculated by using the expression

$$\mathbf{M}\mathrm{TTV}(\mathrm{L}) = \mathrm{DW} * (\mathrm{B}, \mathrm{dir}) + \mathrm{IDW} * (\mathrm{B}, \mathrm{indir}) \tag{1}$$

The values are sorted in the ascending order of mistrust and the ranks are assigned. Similarly in the PATROL model the trust value is calculated by using

$$\mathrm{Trust} = \frac{\alpha[\mathrm{DT}] + \beta[\mathrm{IT}]}{\alpha + \beta} \tag{2}$$

And the values are sorted. In the enhanced model the direct trust is calculated by using the expression

$$DT1_{x,y,s} = \frac{\forall i \in type\ s\ \sum_{i=1} r_i}{f_s} \tag{3}$$

and the total trust is by the expression

$$trust_{x,y,c=} \frac{\alpha\left[DT_{x,y,c}\right] + \beta\left[IT_{x,y}\right]}{\alpha + \beta} \tag{4}$$

where $\alpha > \beta$ and $\alpha + \beta = 1$.

The values are sorted and the ranks are assigned.

| initiators | Providers | Stakhanova Model | | Patrol Model | | New Model | |
|---|---|---|---|---|---|---|---|
| | | Trust value | Rank | Trust value | Rank | Trust value | Rank |
| F | O | 0.921 | 6 | 1.976 | 7 | 1.513 | 8 |
| F | C | 0.323 | 4 | 2.974 | 2 | 2.598 | 3 |
| F | A | 0.081 | 1 | 2.381 | 4 | 2.139 | 5 |
| F | K | 0.249 | 3 | 3.571 | 1 | 3.661 | 1 |
| F | G | 0.20 | 2 | 2.188 | 6 | 2.185 | 4 |
| F | B | 1.111 | 7 | 2.318 | 5 | 2.002 | 6 |

ISSN 1512-1232

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| F | I | 1.195 | 8 | 1.849 | 8 | 1.842 | 7 |
| F | D | 0.840 | 5 | 2.54 | 3 | 2.632 | 2 |

**Table 1.** comparison of Stakhanova Model, Patrol Model (With out inclusion of parameters) & new Model: Context: Printing

Table 1 shows the results of this simulation. From a perusal of Table 1 it follows that the top 3 printing providers are A , K ,C by Stakhanova model , C , K and D for Patrol model and K , D and C by the proposed Model 4. In order to provide a robust comparison, we decided to provide the benefit of categorization for Stakhanova model and Patrol models and rest of our studies have been done on that basis.

| Intiator | Providers | Stakhanova Model | | Patrol Model | | New Model | |
|---|---|---|---|---|---|---|---|
| | | Trust value | Rank | Trust value | Rank | Trust value | Rank |
| F | O | 0.433 | 4 | 0.897 | 8 | 1.513 | 8 |
| F | C | 0.319 | 3 | 2.977 | 1 | 2.598 | 3 |
| F | A | 0.17 | 1 | 1.016 | 7 | 2.139 | 5 |
| F | K | 0.22 | 2 | 2.799 | 2 | 3.661 | 1 |
| F | G | 0.795 | 5 | 1.188 | 5 | 2.185 | 4 |
| F | B | 1.078 | 6 | 1.677 | 4 | 2.002 | 6 |
| F | I | 1.233 | 7 | 1.126 | 6 | 1.842 | 7 |
| F | D | 1.785 | 8 | 2.454 | 3 | 2.632 | 2 |

**Table 2**. Ranking list of providers for the context printing

The categorization of jobs are incorporated in Stakhanova Model and Patrol Model and the same experiments are repeated for all the three models. Table 2 shows the improved results. Row 1 of Table 2 shows the ranks as assigned by the three models. Stakhanova Model assign 6 for entity O, Patrol Model assign rank 7 and Model 4 gives rank as 8.

Again the best provider is A by Stakhanova model, while K is found to be the best for printing in Table 2.

| Intiator | Providers | Stakhanova model | | Patrol Model | | New Model | |
|---|---|---|---|---|---|---|---|
| | | Trust value | Rank | Trust value | Rank | Trust value | Rank |
| A | B | 0.129 | 3 | 4.178 | 1 | 4.268 | 1 |
| A | L | 0.091 | 2 | 4.072 | 2 | 4.155 | 2 |
| A | M | 0.071 | 1 | 3.872 | 3 | 4.022 | 3 |
| A | G | 0.302 | 4 | 2.944 | 4 | 2.996 | 5 |
| A | H | 1.44 | 6 | 2.936 | 5 | 3.054 | 4 |
| A | D | 0.840 | 5 | 2.54 | 6 | 2.632 | 6 |

**Table 3.** Ranking list of providers for the context File sharing

In the second set-up G is the initiator. G requests for file sharing. So all the providers who provide this service is considered. In the first model that is Stakhanova model the total mistrust is calculated by using the expression (1). The values are sorted in the ascending order of mistrust and the ranks are assigned. Similarly in the PATROL model the trust value is calculated by using the expression (2), and the values are sorted. In the enhanced model the direct trust is calculated by using the expression (3) and the total trust is by the expression (4) The values are sorted and the ranks are assigned. Table 3 shows the results of this simulation. The next simulation is for the context computing. The initiator is A and the providers for the computing jobs are B,L,M,G,H,D. Their trust values and rankings are given in Table 4.

ISSN 1512-1232

| Intiator | Providers | Stakhanova Model- | | Patrol Model | | New Model | |
|---|---|---|---|---|---|---|---|
| | | Trust value | Rank | Trust value | Rank | Trust value | Rank |
| G | A | 0.081 | 2 | 4.056 | 1 | 4.378 | 1 |
| G | B | 0.107 | 3 | 4.014 | 3 | 4.314 | 2 |
| G | J | 0.21 | 5 | 4.047 | 2 | 4.286 | 3 |
| G | M | 0.127 | 4 | 3.909 | 4 | 4.177 | 4 |
| G | L | 0.071 | 1 | 3.899 | 5 | 4.134 | 5 |
| G | E | 0.834 | 8 | 3.174 | 6 | 3.285 | 6 |
| G | N | 0.411 | 7 | 1.722 | 7 | 1.503 | 7 |
| G | F | 0.364 | 6 | 1.444 | 8 | 1.285 | 8 |

**Table 4.** Ranking list of providers for the context computing

Table 4 shows the results of simulation. G is the initiator. There are eight providers for this kind of job. These providers are ranked based on the mistrust value in Stakhanova model. The least mistrust value will be ranked first. In the PATROL model the trust values are sorted and the corresponding ranks are assigned which are given is column 6 of Table 3. Column 8 of Table 3 shows the ranks of the providers as assigned by the proposed model. Since the proposed model is the enhanced model which includes different factors context and size and also the model has the categorization of jobs the results are more accurate.

If the top ranked provider is unavailable the proposed model facilitates the user to select the next available provider.From the Table 3 it follows that best of three providers in the order of file sharing are-L, A and B by Stakhanova model; A , J , B by PATROL model and A , B , J by our Model There is a strong correlation between PATROL model and our Model .

From Table 4 we find that the best provider for the computing job is B by the PATROL model and New Model . Figures 1, 2 and 3 present these allocations graphically

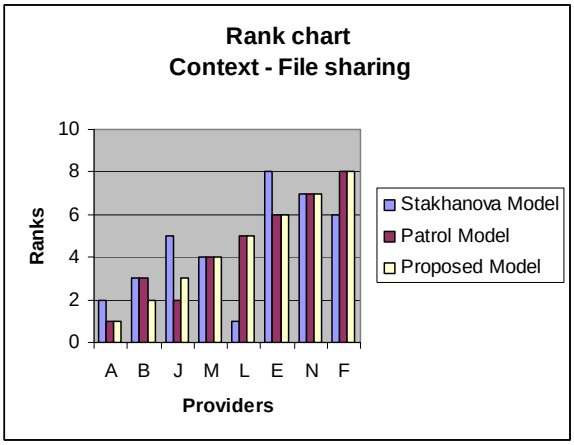


**Figure 1**. Rank chart for resources context: File sharing:

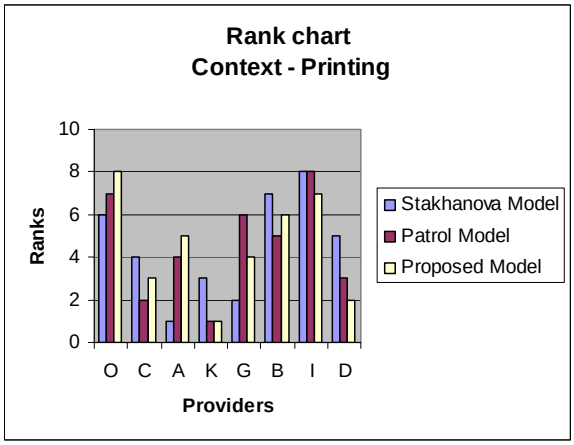


**Figure 2**. Rank chart for resource: context:Printing

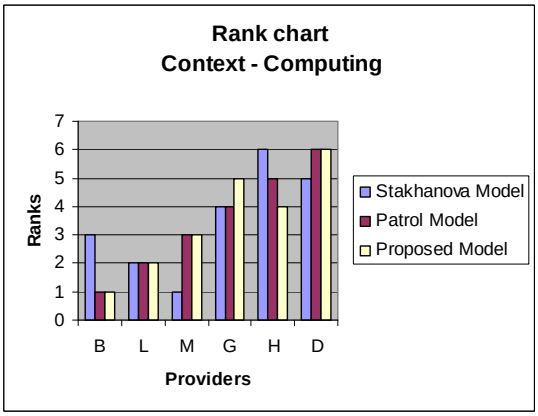


**Figure 3**. Rank chart of providers: context: Computing

ISSN 1512-1232

The Stakhanova model and the PATROL model do not provide the categorization of the trust values. However, based on the job, category has been adopted in order to provide a robust comparison for the three models'. After incorporating the categorization of jobs the results are comparatively improved and the proposed model is found to be effective and complete.

## CONCLUSION

This model gives the prospective list of providers based on the trust value. The experimental results prove the improvement of this model when compared with the previous models.

## REFERENCES


1. Abdul-Rahman A. and Hailes S., (2000) , 'Supporting trust in virtual communities', In *HICSS '00:* Proceedings of the33rd Hawaii International Conference on System Sciences-Volume 6, Washington, DC, USA,IEEE Computer Society, pp 6007-6016.
2. Marsh S.(1994) Formalising Trust as a Computational Concept, Ph.D. Thesis, University of Stirling.
3. Deutch.M (1962), "Cooperation and trust: Some theoretical notes",. In the proceedings *Nebraska Symposium on Motivation*, Nebraska University Press, pp:275–319.
4. Resnick P, Kuwabara K, Zeckhauser R, and Friedman V. (2000), "Reputation systems". *Communications of ACM*, Vol 43,No 12, pp : 45–48 .
5. Resnick P, and Zeckhauser R . (2002), 'Trust among strangers in internet transactions', Empirical analysis of eBay's reputation system. Vol. 11, pp. 127–157.
6. Kollock, Peter. (1998) "Design Principles for Online Communities." , PC Update , vol 15, No 5, pp : 58-60.
7. Kollock, Peter. (1998) "Design Principles for Online Communities." , PC Update , vol 15, No 5, pp : 58-60.
8. Xiong L., and Liu L. , (2004) 'PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities' , IEEE Transactions on Knowledge and Data Engineering, Vol. 16, No. 7, pp 843-857.
9. Wang, Y. and Vassileva, J. (2003) 'Trust and reputation model in peer-to-peer networks', Proceedings of the Third International Conference on Peer-to-Peer Computing, Linköping, Sweden, pp.150–157.
10. Kamvar S.D, Schlosser M.T. and Garcia-Molina.H., (2003) 'The eigentrust algorithm for reputation management in p2p networks. 'In *WWW '03:* Proceedings of the 12th international conference on World Wide Web, New York, NY, USA ,pp 640–651.
11. Azzedin and Muthucumaru Maheswaran.(2002)' Evolving and Managing Trust in Grid Computing Systems.' Proceedings of the Canadian Conference on Electrical & Computer Engineering, Vol 3, pp.1424-1429
12. Boolin Ma, Jizhou Sun.(2006) , 'Reputation-based Trust Model in Grid Security System.', Journal of Communication and Computer', Vol 3, No 8 , pp . 41-46.
13. Stakhanova N., Ferrero S., Wong J. and Cai Y., [2004], "A reputation-based trust management in peer-to-peer network systems, International Workshop on. Database and Expert Systems Applications, pp. 776-781.
14. Tajeddine, A., Kayssi, A., Cheab, A. and Artail, H. (2005) 'A comprehensive reputation-based trust model for distributed systems', The IEEE Workshop on the Value of Security through Collaboration (SECOVAL), September 5–9, Athens, Greece, Vol. 1, Nos. 3–4, pp.416–447.
15. Tajeddine A, Ayman Kayssi, Ali Chehab, and Hassan Artail, [2007]," PATROL: a comprehensive reputation-based trust model", Int. J. Internet Technology and Secured Transactions, Vol. 1, Nos. 1/2, pp 108-131.


**Article received: 2011-05-09**