A Model for Providing List of Reliable Providers for Grid Computing

Srivaramangai.P
Senior Lecturer
Botho College
Gaborone
Botswana

Rengaramanujam Srinivasan
Retd. Professor
BSA University
Chennai, India

ABSTRACT
Grid computing is an interconnected computer system, where machines share resources that are highly heterogeneous. 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. The main objective of the paper is to develop a reliable and robust two way trust model for the Grid system. Thus the goals of this proposed trust model are as follows. The Model should eliminate the incompatible and biased feed backs of the recommenders. It should provide a two way trust mechanism so that the view points of both consumers and providers are taken care of. It should also tune the direct trust calculation to finer granularity by considering parameters such as context, job size and job complexity. Finally, it should provide a ranked list of providers, so that the initiator can choose the most trusted provider based on the availability. This proposed Model encompasses all the above said features and it provides the most trusted reliable provider.

General Terms
Grid Computing

Keywords
Trust, Reputation, reliability .

1. INTRODUCTION
The goal of Grid Computing is to create the illusion of a simple yet large and powerful self managing virtual computer out of a large collection of connected heterogeneous systems sharing various combinations of resources. The resources in a Grid are shared in a flexible, coordinated and secured manner. Most of the Grid applications involve very large data bases with highly secure data. The security challenges faced in a Grid environment can be grouped in to three categories.

- Integration with existing systems and technologies.
- Interoperability with different hosting environments.
- Trust relationship among interacting hosting environments.

Security requires the three fundamental services: authentication, authorization, and encryption. A Grid resource must be authenticated before any checks can be done as to whether or not any requested access or operation is allowed within the Grid. Once the Grid resources have been authenticated within the Grid, the Grid user can be granted certain rights to access a Grid resource. But within the Grid application the one who uses the resource also needs reliable and secure services. The reliability of any transaction is the probability of successful running or completion of a given task. So there is a need for a trust system which ensures a level of robustness against malicious nodes. Trust must be established from both the sides.

When some one is trust worthy, it is assumed that the probability that he/she will perform an action which is highly beneficial. On the other hand when some one is untrustworthy, then the beneficial probability will be very low and the detrimental probability will be high. The strongest expression of this view has been given by [1] who argues that the notion of trust should be avoided when modeling economic interactions, because it adds nothing new, and that well known notions such as reliability, utility and risk are adequate and sufficient for that purpose. According to Williamson, the only type of trust that can be meaningful for describing interactions is personal trust. He argues that personal trust applies to emotional and personal interactions such as love relationships where mutual performance is not always monitored and where failures are forgiven rather than sanctioned.

Trust can be thought of as a firm belief in an entity to act dependably, securely and reliably in a specific context [2]. Trust depends upon the entities of time and context. For example, an entity A wants to use the resources of B, if the resource is a file then the required trust level will be lower. But if A wants to execute his code in B's machine then the required trust level will be higher. The code may even attempt to corrupt the whole system.

The difference between trust and reputation can be illustrated by the following statements:

(1) "I trust you because of your good reputation."

(2) "I trust you despite your bad reputation."

The first sentence says that the first party believes the second one since the second one has a very good reputation. The good reputation may be obtained from one's own experience or from an other's feed backs. The second sentence says that the first one believes the second in spite of the bad recommendations from others .This may be due to the strong belief or trust the first one has in the second. Personal experience typically carries more weight than second hand trust referrals or reputation, but in the absence of personal experience, trust often has to be based on referrals from others.

Reputation can be considered as a collective measure of trustworthiness (in the sense of reliability) based on the referrals or feed backs from members in the same community. An individual's subjective trust can be derived from a combination of received referrals and personal experience.

2. LITERATURE SURVEY

Gilbert et al. [3] had developed a trust model based on reputation systems and feedback mechanisms. The paper distinguishes three types of reputation systems, namely positive, negative and hybrid systems. They stress the advantage of using hybrid systems to maintain data integrity. Dewan [4] stresses the need to introduce external motivation for peers to cooperate and be trustworthy and recommends the use of 'digital reputations', which represent the online transaction history of a host.

Boolin and Jizhou [5] discussed a trust model based on reputation. In this model both direct and indirect trusts are calculated by using reputation. Direct trust is calculated, and the value of the direct trust of others is used to find the value of indirect trust. A reputation management algorithm for P2P networks, called the EigenTrust, is introduced in [6]. Every peer *i* rates other peers based on the quality of the service they provide. Therefore, every peer *j* with whom *i* had business with, will be rated with a grade S_{ij}. To globalize this algorithm the individual grading scheme is normalized. Hence, for each peer *j*, the normalized local trust value c_{ij} is defined as

$$c_{ij} = \frac{\max(Sij,0)}{\sum_j \max(Sij,0)}$$

(1)The normalized local trust values throughout the P2P domain are aggregated, by means of a transitive trust mechanism. Peer *i* asks its acquaintances for their opinions about other peers and weighs the opinion by the trust it places in his friends (Expression 2).

$$t_{ij} = = \sum_k C_{ik} C_{kj}$$

(2) where t_{ij} represents the trust that peer *i* puts in peer *j* based on the opinion of his friends *{k}*. The coefficients are assembled into a matrix. The process of obtaining the trust values of friends is repeated to obtain the transitive closure of the matrix.

(i.e., T = (CT)2 Ci would mean that peer i is asking for the opinion of his friends' friends, and T = (CT)3 Ci for the opinions of their friends). Therefore, after n iterations, where n is the rank of the matrix, the transitive trust is obtained.

Stakhanova [7] proposed a decentralized reputation based trust model for selecting the best peer. A local table is maintained for each entity to store the transaction records of all the other entities. Each entity table stores the id of all the other entities in the network, their reputation values, the number of bad transactions that occurred and the total number of transactions performed. A concrete formula is presented for calculating the Trust value of the entities willing to provide the resource. Stakhanova actually calculates the mistrust value, and if the value is above a given threshold value, reject the resource.

Tajeddine et al. [8] proposed an impressive reputation based trust model. This model was extended, and they developed a comprehensive model called PATROL in [2007] . Their works are based on the TRUMMAR model which was developed by Derbas et al [2004] for mobile agents.

Tajeddine et al. in **PATROL** [9] further enhanced their previous model by adding another parameter called cooperation. The cooperation value reflects the willingness of a host to cooperate and give services to other hosts. This value depends on the number of times a host responded to an interaction with respect to the total number of interactions that it was asked for in the last Time interval. This model also considers two threshold values for trust. If the total trust is greater than the higher trust level 1, then the transaction is allowed, and if it is less than the minimum trust level then the transaction is not allowed. If the trust level is between these two levels then decision is taken based on probability.

Mármol [10] presents some of the most important and critical security threats that could be applied in a trust and reputation scheme. He also describes and analyzes each of those threats and propose some recommendations to face them when developing a new trust and reputation mechanism.

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

In order to facilitate users to select the best provider, a trust model based on reputation has been designed and developed. In the two models already proposed in our previous work [11] the total trust is measured by summing up the two trusts, direct and indirect. In Model 3 again our previous work [11], different factors were introduced, such as the context and size for calculating the direct trust. In this Model, Model 3 is further enhanced and a ranked list of providers providing a particular resource is presented. The user can choose the best provider. In

case the best provider is busy and is engaged in some other activity, the next best provider from the list can be chosen. Hence, the proposed enhancement 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 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.

This Model is an enhancement of Model 3 which includes the two way test criterion and also considers the parameters of context and size. In Models 1, 2 and 3, for any initiator's request, only one provider is randomly selected. Models 1 and 2 calculate trust, by combining direct trust, which is obtained out of direct experiences, and indirect trust which is calculated by using the referrals from the recommenders. The feedbacks of the recommenders which do not have a positive correlation with that

of the initiator are not considered. In Model 3 direct trust is not directly obtained from the table and is evaluated based on parameters.

The problem with Model 3 is that for an initiator's request, if the provider also agrees then the transaction will take place. However, among the multitude of providers, the chosen one may or may not be the best from the trustworthiness point of view, even though his trust level may be above the minimum threshold. The proposed Model checks all the possible providers and displays a ranked list of providers on the basis of trustworthiness. Such an effort to make a global selection of all possible providers may take a long time; therefore, as soon as an entity gets at least four providers with a trust value above the threshold, which is set at a level higher than the minimum trustworthiness, the search stops and the results are displayed.

4. EXPERIMENTS AND SIMULATION RESULTS

The simulation is done by considering the three models.

- The Stakhanova Model.
- The PATROL Model
- The proposed model- The proposed 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 a printing job. Out of these fifteen entities E, F, J, N are assumed to do only file sharing. C, I, K, O do the 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, the size parameter has not been considered. Also, in this simulation, it is assumed that all the entities are not well reputed for all the services they provide. An entity may be having a good reputation for one kind of service, but not for another kind of service. Here B is well reputed for computing and File sharing. 'A' is well reputed for file sharing and not for printing. Entity G has a good reputation for printing. Out of fifteen entities, F is least reputed and O is malicious.

It is to be noted that the Stakhanova and PATROL Models do not provide the categorization of jobs. Therefore, the first simulation study has been done without providing the categorization of jobs for these two models. This simply means, that the two models assume, that if a provider is good say, in computing and he provides a printing service, he will be good, in that also. On that basis, there will be a single trust value for each provider, irrespective of the nature of the job. Thus, the first simulation study has been done, without categorization for these two models, and with categorization for the proposed Model .

In the first simulation, F is the initiator. F requests for printing. All the providers who provide this service and whose trust value is greater than the threshold are considered. In the Stakhanova model the total mistrust is calculated by using the expression

$$\mathbf{MTTV(L)} = \mathbf{DW} * (\mathbf{B}, \mathbf{dir}) + \mathbf{IDW} * (\mathbf{B}, \mathbf{indir}).$$

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

Trust = $(\alpha[DT] + \beta[IT])/(\alpha + \beta)$ (4)

$$DT1_{x,y,s} = \frac{\forall i \in types \sum_{i=1} r_i}{f_s} \quad (5)$$

$$trust_{x,y,c} = \frac{\alpha\lfloor DT_{x,y,c}\rfloor + \beta\lfloor IT_{x,y}\rfloor}{\alpha+\beta} \quad (6)$$

Where α and β are the weighing factors in expression 4 and DT is the direct trust and IT is the indirect trust. The values are sorted. In proposed Model the direct trust is calculated by using the expression 5, and the total trust is calculated by the expression 6. The values are sorted and ranks are assigned. Table .1 shows the results of this simulation study.

Table 1: Comparison of the Stakhanova and Patrol Models and This Model

(With out inclusion of parameters) & this Model: Context: Printing

Intiator	Providers	Stakhanova Model trust	rank	Patrol Model trust	rank	Proposed Model trust	rank
F	O	0.433	4	Not granted		Not granted	
F	C	0.319	3	3.077	1	2.601	3
F	A	0.17	1	Not granted		Not granted	
F	K	0.22	2	2.801	2	3.603	1
F	G	0.795	5	Not granted		2.585	4
F	B	1.078	6	2.577	4	Not granted	
F	I	1.233	7	Not granted		Not granted	
F	D	1.785	8	2.654	3	2.623	2

From a perusal of Table 1, it follows that the top 3 printing providers are

A, K and C by the Stakhanova model, C, K and D by the Patrol model and K, D and C by the proposed The proposed Model. The Stakhanova model ranks all the providers. But the Patrol Model and The proposed Model do not consider all the providers. They choose the providers whose trust value satisfies the minimum threshold value. It is seen that the malicious provider O has been given the fourth rank by the Stakhanova model, while, the other two models rightly deny the transaction.

The fourth provider chosen by the Patrol Model is B. But B has a good reputation only in computing. B does not satisfy the minimum value in The proposed Model, and hence, the transaction is not granted. Instead, G, which is good in the printing job is put in the fourth position. In this simulation, the provider O is malicious. The Patrol Model, as it considers all the feed backs, wrongly grants the transaction between F and B. But the proposed Model eliminates the biased feed backs; it also considers the two way test criteria and rightly denies the transaction. In order to provide a robust comparison, it was decided to provide the benefit of categorization for the Stakhanova and Patrol models, and the rest of the studies have been done on that basis. Here, in this simulation, the number of malicious nodes is assumed to be one which is only 6.6 %. So the variations between the Patrol model and The proposed Model are minimal.

The categorization of jobs is incorporated in the Stakhanova and Patrol Models and the same experiments are repeated for all the three models. Table 2 shows the improved results. In row 1 of Table 1 the Stakhanova Model assigns rank 4 for entity O, which is assumed to be malicious, and Row 1 of Table 2 shows how the rank assigned by the same model is brought down to 6, after incorporating the categorization of jobs for the same model. However, unlike in the other two models O continues to be ranked.

Table 2: Ranking list of providers for the context printing

Intiator	Providers	Stakhanova Model trust	rank	Patrol Model trust	rank	Proposed Model trust	rank
F	O	0.921	6	Not granted		Not granted	
F	C	0.323	4	2.953	2	2.567	3
F	A	0.081	1	2.51	4	Not granted	
F	K	0.249	3	3.563	1	3.652	1
F	G	0.20	2	Not granted		2.585	4
F	B	1.111	7	Not granted		Not granted	
F	I	1.195	8	Not granted		Not granted	
F	D	0.840	5	2.541	3	2.613	2

Again the best provider is 'A' by the Stakhanova model, while K is found to be the best for printing by the other two models. The PATROL model relegates A to the fourth place, while The proposed Model does not grant the transaction. Entity A is well reputed for file sharing and not for printing. As the Patrol Model considers all the feed backs, including that of O, it wrongly places the entity A in the fourth position. Since, Stakhanova model does not have any expression for the credibility factor, it wrongly places entity A in the first place.

In the second set-up G is the initiator. G requests for file sharing. So all the providers who provide this service and satisfy the fit criteria are considered. Table 3 shows the results of this simulation.

Table 3: Ranking list of providers for the context File sharing

Intiator	Providers	Stakhanova Model Trust	Rank	Patrol Model Trust value	Rank	Proposed Model Trust	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	Not granted		Not granted	
G	F	0.364	6	Not granted		Not granted	

G is the initiator. There are eight providers for this kind of job. These providers are ranked, based on the mistrust value in the Stakhanova model. The least mistrust value will be ranked first. This time all the providers are good. There is no malicious provider for file sharing. So there is not much variation between the Patrol Model and The proposed Model. From Table 3 it follows that the best of three providers in order for file sharing are - L, A and tB by the Stakhanova model; A, J, B by the PATROL model and A, B, J by the proposed Model.

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.

Table 4: Ranking list of providers for the context, 'computing'

Initiator	Providers	Stakhanova Model Trust	Rank	Patrol Model trust	rank	Proposed Model trust	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

From Table 4, it can be found that the best provider for the computing job is B, by the PATROL model and The proposed Model. Here also, all the providers of computing are assumed to be good. There are no malicious providers. So there is not much variation between both the models. Figures 1, 2 and 3 present these allocations graphically.

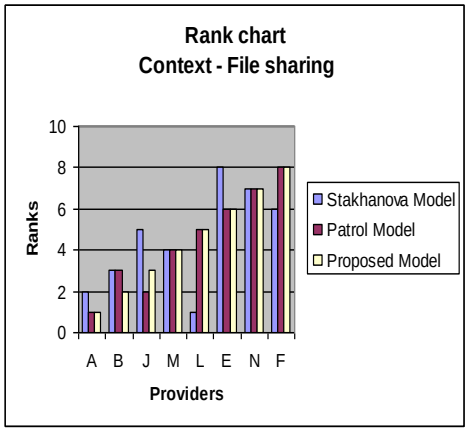

Figure .1 Ranks for resources as provided by the three models – the Stakhanova Model, the Patrol Model and The proposed Model.Context: File sharing

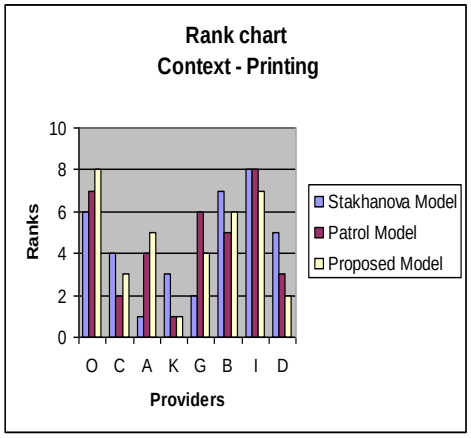

Figure 2 Ranks for resources as provided by the three models – the Stakhanova Model, the Patrol Model and The proposed Model. Context: Printing

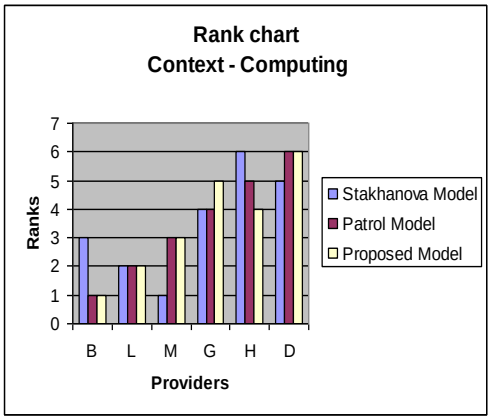

Figure 6.3 Ranks for resources as provided by the three models – the Stakhanova Model, the Patrol Model and The proposed Model. Context: Computing.

The Stakhanova model and the PATROL model do not provide for the categorization of the trust values based on the job type. The categorization of jobs had been included with these two models solely to provide a robust comparison. It is seen that even with this benefit, the Stakhanova model remains in the third place; the Patrol model rises to a close second place. How ever, the lead margin for The proposed Model is higher, if malicious nodes are present. Thus The proposed Model has been shown to be the best and complete model.

5. CONCLUSION

This paper has described a Model , which is a super set of Models 1, 2 and 3of our previous work. Thus, this Model incorporates all the features of Model 1, Model 2 and Model 3. In addition to that, this Model provides a pool of providers whose reputation is higher than a stipulated value, so that its throughput is higher than that of all the other models. The experimental results bring out the improvements of this Model in comparison with the our previous models.

5. REFERENCES

[1] Williamson O.E. [1993], "Calculativeness, Trust and Economic Organization",. Journal of Law and Economics, Vol 36,No 1, pp: 453-486.

[2] Gheorghe Cosmin Silaghi, Alvaro E. Arenas, Luis Moura Silva, (2007), 'Reputation-based trust management systems and their applicability to grids', Core GRID Technical Report Number TR-0064 URL: http://www.coregrid.net.

[3] Gilbert, A., Abraham, A. and Paprzycki, M. (2004) "A system for ensuring data integrity in grid environments", Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC '04), Vol. 1,LasVegas,USA, pp.435–439.

[4] Dewan, P. (2004) 'Peer-to-peer reputations', Proceedings of the 18th International Parallel and Distributed Processing Symposium (IPDPS'04), April 26–30, Santa Fe, NM, USA, pp.1783–1785.

[5] 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.

[6] 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.

[7] Stakhanova N., Ferrero S., Wong J. and Cai Y., [2004], "A reputation-based trust management in peer-to-peer network systems," in the ... International Workshop on. Database and Expert Systems Applications, pp. 776-781.

[8] 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.

[9] 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.

[10] **Félix Gómez Mármol, Gregorio Martínez Pérez, [**2009]," Computers & Security", Vol. 28, Nos. 7, pp.545-546.

[11] Srivaramangai P., Srinivasan R., (2011), 'Enhancements to Reputation Based Trust Models for Improved Reliability in Grid Computing', in WSEAS transactions on computers, Vol 10 , No 53 , pp 1-4

6. AUTHOR'S PROFILE

Srivaramangai.P is a Phd Research Scholar in Department of Computer Science and Engineering at Mother Teresa University, Kodaikanal, India. She is currently a involved in developing a Reputation based trust model for grid. She is senior faculty in Botho College, Gaborone, Botswana. She graduated her Bachelor of Science in the discipline of Mathematics at Madras University, India then she graduated her Master of Computer Applications in Reputed Bharathidasan University Tirchurapalli. She has a vast experience in lecturing and tutoring the modules like Object Oriented Analysis and Design, Programming in C, Computer Networks, Management Information System, Enterprise Resource Planning, Software Engineering Methodologies,Network Security and Distributed Computing both for UG and PG Engineering students. She has experiences in teaching in different countries like India, Ethiopia, Bhutan, Botswana.Her total teaching experience is around 30 years which includes 13 years of experience as senior lecturer in BSA

University ,Chennai, India. Her publications include 4 National Conference Proceedings, 4 International Journal publications (including WSEAS Transaction in Computers) and also was a speaker in AITEC-Mozambique International conference held in Maputo, Mozambique .