ENHANCEMENTS TO REPUTATION BASED TRUST MODELS FOR IMPROVED RELIABILITY IN GRID COMPUTING

SRIVARAMANGAI.P, RENGARAMANUJAM SRINIVASAN
Senior Lecturer, Retd.Prof /CSE Dept
Botho College, BSA University, Chennai
BOTSWANA, INDIA
sri_padma_2000@yahoo.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.

The main purpose of security mechanisms in any distributed environment such as the Grid 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, 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; traditional security mechanisms are unable to protect against this type of security threat.

Trust and reputation systems, on the other hand, can very well provide protection against such threats. Reputation models can be modeled in such a way they it could provide reliability for both users and providers. Reputation systems provide a way for building trust through social control, by utilizing community based feedbacks about past experiences of peers to help making recommendations and judgments on the quality and reliability of the transactions. Reputation and trust systems are soft security mechanisms which can assure behavior conformity.

In this paper two new reputation based trust models are proposed. The first, model, Model 1, uses a new factor called compatibility, which is based on Spearman's rank correlation. The feed backs of the recommenders which are incompatible with those of the initiator are eliminated by using the compatibility factor.

Model 2 is an improvement over the Model 1. In this model, new factors are included for measuring the direct trust. In order to effectively evaluate the trustworthiness of different entities and to address various malicious behaviors, this comprehensive trust model based on reputation, is proposed. Two important factors – context and size, are incorporated in evaluating the trustworthiness of entities.

Key-Words: - Grid computing, Reputation, Trust, Reliability

1. Introduction

1.1 Overview

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.

1.1.1 Reputation and Trust

Marsh [1994] was one of the first to define the trust concept from a computational point of view. He takes the definition of [Deutch 1962] which states that trusting behaviour occurs when an individual perceives an ambiguous path, the result of which could be good or bad, and the occurrence of the result is dependent on the actions of another person, the bad result being more harmful than the good result being beneficial. When we say that we trust someone or someone is trust worthy, we assume that the probability that he/she will perform an action that is beneficial to us is high. On the other hand when we say that someone is untrustworthy, we imply that the beneficial probability is very low and the detrimental probability is high.

Reputation is what is generally said or believed about a person or thing's character [Arenas, 2006]. Therefore, reputation is a measure of trustworthiness, in the sense of reliability. Reputation can be the source of building trust. Abdul Rahman et al [2000] define reputation as an expectation about an entity's behavior based upon it's past behavior. The rest of the sections are organized as follows:

Section 1 of this paper describes the Grid environment and has brought out the importance of the trust mechanism in the successful operation of the Grid. The scope of the research work is defined and the contributions are listed. Section 2 provides an overview of the related work. Section 3 introduces a new factor called compatibility, which is evaluated using Spearman's rank correlation coefficient. It is shown that Model 1 using the compatibility factor eliminates the biased and otherwise incompatible feedbacks and leads to reliable transactions in the Grid..Section 4 presents Model 2 and enhancement of Model 1 with the incorporation of parameters context and job size in the evaluation of direct trust. Section 5 gives the experimental results and Section 6 concludes the thesis by summing up the findings and suggesting the scope for future work.

2. Related work

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. 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 feedbacks from transactions, the number of transactions, the credibility of feedbacks and the criticality of the transaction.

Bayesian models directly model the statistical interaction between the consumers and the providers. Wang and Vassileva [2003] use a naive Bayesian network which is generally used for representing and analyzing models involving uncertainty, to represent the trust of a user with a provider, the concept of trust being defined in terms of both the capability of the provider in providing services, and the reliability of the user in providing the recommendations about other users. The advantage of Bayesian systems is that they provide a sound theoretical basis for computing reputation scores, whereas the main disadvantage is that it might be too complex and difficult to interpret.

Kamvar et al [2003] considered that each peer stores its trust values locally for the rest of the peers. They did not enforce a method for obtaining these trust values, but they suggest that the trust values could be obtained by evaluating each previous transaction between peers, thus being a form of direct trust. Each peer normalizes these trust values obtaining values in the interval (0, 1), 1 being assigned to the most trusted peer. In order to obtain a global view of the network, as in [Bin and Singh 2002], each peer can ask referrals from its neighbours regarding a third peer. The received trust values can be aggregated using the local trust values, which are the credibility factors of the neighbour.

Azzedin and Muthucumaru [2002] proposed a behavior based trust model. They suggest that the Trust Level is based upon past experience and a specific context. Boolin and Jizhou [2006] 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.

Stakhanova [2004] 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. [2005] 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.

In their approach, the initiator host calculates the reputation value of the target host based on its previous experiences and gathered feedbacks from other hosts. The recommenders who give feed backs can be from the same administrative control (neighbor) or from different trusted domain (friends) or from a completely strange domain (stranger). Direct trust is retrieved from the trust table and indirect trust is calculated by considering the feedbacks from all other hosts and the feed backs are multiplied by corresponding credibility factors. Total trust comprises of direct trust and indirect trust in which higher weightage is given for direct trust. If the total trust is greater than the minimum prescribed threshold value the model accepts the resource.

In order to allocate weightage to feed backs given by different recommenders they have defined a factor called credibility. The factor takes values between zero and one; they are based on three parameters, similarity, activity and popularity. The credibility factor is given by the expression 1 where a, b and c are fractions with a>b>c and a+b+c=1.

$$\text{Credibility} = a * \text{similarity} + b * \text{activity} + c * \text{popularity} \quad (1)$$

3. Model 1: - Trust model to eliminate unreliable feedbacks

In the previous section we described the Tajeddine model and explained the credibility factor. The credibility factor takes in to account how much reliance we can place on the individual feed backs obtained from third parties. The credibility factor is a function of similarity, activity and popularity factors, and we had given expressions for the same.

Let us now focus our attention on the similarity factor given in expression 2.

$$sim(x,y) = 1 - \sqrt{\frac{\sum_{i=1}^{n}\sum(u_i - v_i)^2}{25\,n}} \qquad (2)$$

Here x is the initiator and y is the recommender. u_i and v_i are reputation values assigned by x & y to a common third entity i.

Let us consider a few examples to illustrate the significance of the similarity factor.

Let A be the initiator. He would like to have feedback about some prospective supplier P. Let B be the recommender, B recommends P with a reputation score of 4 out of the maximum possible score 5. The question is, whether A can consider this value. The existing model calculates the similarity factor to assess the similarity between A's and B's evaluations. This is achieved by comparing the evaluation of A and B about some common set of providers. Let C, D, E, F, G, H, I, J, K and L be the common set of providers with whom A and B have interacted. Table 1 gives one possible set of scores.

In Example 1 (Table 1) both the initiator and the recommender give the same referral values for all the entities. The existing model calculates similarity by using the expression (2).

Similarity = 1-0 = 1.

We define compatibility as

$$Compatablity = 1 - \frac{6\sum_{i=1}^{n}\sum dr_i^2}{n(n^2-1)} \qquad (3)$$

Where dr_i is the difference in the rankings for i^{th} value. Compatibility factor as defined by us is the spearman's ranking coefficient between two sets of evaluations.

Table 1 Example1

Providers	C	D	E	F	G	H	I	J	K	L
Score given by A (Initiator) u_i	4.4	4.2	4.0	3.8	3.6	2.9	2.7	2.5	2.3	2.1
Score given by B (Recommender) v_i	4.4	4.2	4.0	3.8	3.6	2.9	2.7	2.5	2.3	2.1
Rank given by A Initiator	1	2	3	4	5	6	7	8	9	10
Rank given by B recommender	1	2	3	4	5	6	7	8	9	10

Compatibility = 1 –0 = 1. Since both the entities give the same referrals, the similarity and the compatibility factors become unity. Let us consider a few more examples to compare similarity and compatibility. The individual sets of scores are given by Tables 2 to 6 and the cumulative results are given in Table 7.

Table 2 Example 2

Providers	C	D	E	F	G	H	I	J	K	L
Score given by A (Initiator) u_i	4.4	4.2	4.0	3.8	3.6	2.9	2.7	2.5	2.3	2.1
Score given by B (Recommender) v_i	3.4	3.2	3.0	2.8	2.6	1.9	1.7	1.5	1.3	1.1
Rank given by A Initiator	1	2	3	4	5	6	7	8	9	10
Rank given by B recommender	1	2	3	4	5	6	7	8	9	10

In the Example 2 (Table 2), we find that the difference |d| between the two sets of evaluations is 1 in each case.

$$sim(x,y) = 1 - \sqrt{\frac{1}{25}} = 1 - \frac{1}{5} = 0.8$$

Compatibility = 1 since the rankings are the same.

Both the expressions work well in this case. In Example 3 (Table 3) the difference |d| between the two sets of evaluations is 1 in each case. But the initiator gives a score of one more than the score given by the recommender for first five entities, and one less for the next five entities. In this case, the similarity factor is 0.8 and the compatibility factor is -0.212. Here, the compatibility factor is a better indication.

Table 3 Example 3

Providers	C	D	E	F	G	H	I	J	K	L
Score given by A (Initiator) u_i	4.4	4.2	4.0	3.8	3.6	2.9	2.7	2.5	2.3	2.1
Score given by B (Recommender) v_i	3.4	3.2	3.0	2.8	2.6	3.9	3.7	3.5	3.3	3.1
Rank given by A Initiator	1	2	3	4	5	6	7	8	9	10
Rank given by B recommender	4	6	8	9	10	1	2	3	5	7

Table 4 Example 4

Providers	C	D	E	F	G	H	I	J	K	L
Score given by A (Initiator) u_i	4	4	4	4	4	4	4	4	4	4
Score given by B (Recommender) v_i	1	1	1	1	1	1	1	1	1	1
Rank given by A Initiator	5.5	5.5	5.5	5.5	5.5	5.5	5.5	5.5	5.5	5.5
Rank given by B recommender	5.5	5.5	5.5	5.5	5.5	5.5	5.5	5.5	5.5	5.5

In Example 5 (Table 5) A's scores are in the reverse order of B's scores. The similarity factor is 0.26 whereas the compatibility factor is -1 which shows a completely negative correlation. The similarity factor fails to indicate the correct result, whereas the compatibility factor provides a better indication.

Table 6 Cumulative results

Example Number	Difference between scores given by A and B	Similarity	Compatibility
1	d = 0	1	1
2	d = 1	0.8	1
3	d=1 for first 5 sets and d=-1 for second 5 sets.	0.8	-0.212
4	d=0 A give all equal higher values B gives all equal lower values	0.4	1
5	d is varying .Values are exact reverse of each other	0.26	-1

A perusal of Table 6 reveals the following information. The Similarity factor fails in examples 3 and 5. The compatibility factor fails in example 4 where both A and B have given uniform scores to all parties, with a difference, that A has given a uniformly high score of 4 while B has given a uniformly low score of 1. Apparently A would like to continue with all these entities while B will take none of them. Otherwise, we find that the compatibility factor is successful in capturing correctly the nature of evaluations.

Therefore, we recommend the use of the compatibility factor, which is successful with the elimination of biased feed backs. However in order to eliminate cases corresponding to Example 4, we make the following rule.

Calculate the compatibility factor using the expression 2.

IF the compatibility factor > 0 and

$u_i=u_j$(for all i and j) and

$v_i=v_j$ (for all i and j) and

$u_i-v_i >= 0.5$ then

the compatibility factor = the similarity factor

ENDIF.

The proposed model adopts two more factors (3) and (4) given by PATROL Model [2007], by slightly modifying them. Activity is defined as the ratio of the number of interactions of the recommender entity to the total number of interactions by all the recommenders. In this expression the denominator factor is the total count of interactions of the entities with the positive compatibility factor. The interactions by all the entities are not included in this expression. Similarly the specificity is the ratio of the number of interactions of the recommender entity as a provider to the total number of interactions of all the providers with the positive compatibility factor.

$$activity = \frac{number\ of\ interactions\ of\ the\ recommender\ entity\ as\ a\ user}{Total\ number\ of\ interactions\ by\ all\ recommenders\ as\ users} \quad (4)$$

$$Specificity = \frac{number\ of\ interactions\ of\ the\ recommender\ entity\ as\ a\ provider}{Total\ number\ of\ interactions\ by\ all\ recommenders\ as\ providers} \quad (5)$$

Credibility factor is calculated by using expression 1.

In this model, compatibility is given a higher weightage than the other two.Total trust is given by the expression 6.

$$Trust = \frac{\alpha[DT]+\beta[IT]}{\alpha+\beta} \quad (6)$$

DT represents direct trust and IT represents indirect trust. Indirect trust is given by the expression7.

IT=IT1+IT2
(7)

Where

$$IT1 = \frac{\sum_{i=1}^{n} \delta_{1i}\ rep\ \frac{y}{z_i}}{\sum_{i=1}^{n} \delta_{1i}} \quad (8)$$

$$IT2 = \frac{\sum_{i=1}^{n} \delta_{2i}\ rep\ \frac{y}{t_i}}{\sum_{i=1}^{n} \delta_{2i}} \quad (9)$$

where δ_1 and δ_2 are credibility factors.

$\sum_{i=1}^{n} \delta_{1i}\ rep\ \frac{y}{z_i}$ represents weighted sum of repuations of y as represented by neighbours.

$\sum_{i=1}^{n} \delta_{2i}\ rep\ \frac{y}{t_i}$ represents weighted sum of repuations

4. MODEL 2 – A COMPREHENSIVE TRUST MODEL

In order to effectively evaluate the trustworthiness of different entities and to address various malicious behaviors, we have designed and developed a comprehensive trust model based on reputation. Two important trust factors are identified in evaluating the trustworthiness of entities. They are, context and size.

In the previous model proposed by us, two types of trust have been taken, in to consideration, namely, direct trust and indirect trust. Indirect trust is measured from the reputation score of other entities. In the first model, the initiator eliminates the feed backs of entities whose evaluation procedure is not correlated to that of his own. This model and other existing models take the direct trust score from the table. There is no categorization of the type of jobs. The proposed model, Model 2 measures direct trust based upon different parameters such as context and size. A factor called complexity is defined to take care of the above two parameters.

Model 2 categorizes the jobs. The model assumes that the feedback values given by the user for one kind of job provided by an entity, are different from another kind of job by the same entity. So the model uses three types of trusts, namely, DT1, DT2 and indirect trust. DT1 represents the trust of the user on the provider as a result of the same kind of transactions, and DT2 for different types of transactions. Indirect trust is calculated by the same expression as that of the previous models. Further, this model considers the fact that the reputation values are not always constant. When there is no transaction between two entities for a long period of time then the value of reputation is brought down. Thus this model adopts a function called the decay function, which decreases the value of reputation when there is no transaction, over a given interval. After the elapse of a specific period with out any transaction this decrement is done.

4.1 Computation of Trust:

In this model three types of jobs are considered. The jobs can be the transfer of files, printing or computing. Further, the size of the jobs can fall under three categories- small, medium and large. The system assigns the complexity factor based upon context and size (Table 7). Nine different combinations of contexts and sizes of jobs are considered and a complexity factor is assigned for each of the combinations. Thus there are nine types of transactions; from Table 7, it follows that the complexity factor is highest (=1) for large computational jobs, and the smallest (=0.25) for simple file transfer jobs.

Let us consider a scenario where A is the user and wants to use the resource, say the printer of the provider P. Let the job size be medium. Thus, from Table 7, the transaction type is 5. Before submitting the job to P, the user A has to be satisfied about the trust worthiness of P. The system refers to all the previous transactions between the user A and the provider P. (Table 8). If there are any transactions of the same type-s, context and size being the same as per the current requirement, then the average of the reputation values of all these transactions is taken as DT1.Thus $DT1_{x,y,s}$ the direct trust of the user x on y based on the same type of transactions as the present requirement, is given by expression 10.

$$DT1_{x,y,s} = \frac{\forall i \text{ type } s \; \Sigma_{i=1} r_i}{f_s} \quad (10)$$

where f_s refers to the frequency of the same type of transactions and r_i corresponds to the reputation value based on the i_{th} transaction.

Perusing Table 8, we find that there are two transactions of the type 5 ($No:2 ,9) corresponding to C2,M combination. Thus DT1 is evaluated as $DT1_{x,y,s} = \frac{3.98+2.85}{2} = 3.41$

Table 7 Complexity Table

job type	Context	Size	Complexity Factor
1	C1	S	0.25
2	C1	M	0.4
3	C1	L	0.5
4	C2	S	0.4
5	C2	M	0.5
6	C2	L	0.6
7	C3	S	0.6
8	C3	M	0.8
9	C3	L	1

C1: File transfer, C2: Printing, C3: Computing

Table 8 Transactions between A and P

S.NO	Context	Size	Reputation	Job type
1	C2	L	2.9	6
2	C2	M	3.98	5
3	C1	S	2.36	1
4	C1	M	2.85	2
5	C1	L	2.91	3
6	C2	L	2.25	6
7	C2	S	3.53	4
8	C3	S	2.01	7
9	C2	M	2.85	5
10	C1	M	3.05	2
11	C3	M	1.81	8
12	C1	S	3.05	1

The direct trust between x and y based on differing type of transactions $DT2_{x,y,d}$ is given by expression 11.

$$DT2_{x,y,d} = \frac{\sum_{k=1}^{n} \sum_{i=1}^{m} c_i r_i / f_i}{n} \qquad (11)$$

where n is the number of differing transaction types. If A and P have transacted all the types of transactions, n will be (9-1=) 8. However, if P is not the provider for computational jobs, then n will be (6-1=) 5.

From the data presented in Table 8,

$$DT2_{x,y,d} = \frac{1.545+0.675+1.140+1.45+2.118+1.705+1.44}{7}$$

=9.574/7 =1.368

Total direct trust is given by the expression 12.

$$DT_{x,y,c} = \gamma\left[DT1_{x,y,s}\right] + \theta\left[DT2_{x,y,d}\right] \qquad (12)$$

Weightage for DT1 is assumed to be 0.8 and for DT2 is 0.2.Hence

DT = (0.8*3.41+0.2*1.368) = 2.728+ 0.2736 = 3.002.

This direct trust is substituted for $DT_{x,y,c}$ in expression 12 and indirect trust is computed by the same method given by expressions 7 to 9. Direct trust is given more weightage. Total trust is calculated to be 2.8 and hence the resource is accepted by the user.

Let us consider another example. A requests the provider P for executing a job of small size. $DT1_{x,y,s}$ is calculated by using expression 10 as follows. Since there is only one transaction with the same context and size that value is taken for the DT1.

$$DT1_{x,y,s} = 2.01$$

$DT2_{x,y,d}$ is calculated by using expression 11.

$$DT2_{x,y,d} = \frac{1.545+0.675+1.140+1.45+2.118+1.705+1.44}{7}$$

= (10.073) / 7 = 1.439.

DT = (0.8*2.01 +0.2*1.439) = 1.608+0.288=1.896

Hence, in this case the direct trust is low. The total trust here is 1.8 and hence the resource is not accepted by the user. In the above two examples we have considered the same user and the provider. In the first example, the resource is accepted. But in the second example the same user rejects the provider in a different context.

Total trust is measured by using the set of expressions 13 & 14.

The trust of an object x about an object y at context c is given by

$$trust_{xy,c} = \frac{\alpha[DT_{xy,c}] + \beta[IT_{xy}]}{\alpha + \beta} \quad (13)$$

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

$DT_{xy,c}$ represents direct trust, IT_{xy} represents indirect trust .

$$IT_{xy} = IT1_{xy} + IT2_{xy} \quad (14)$$

Other models, including our previous models, do not have any categorization of jobs. The provider may be better in providing one kind of job than the other kind. For example, a provider who may be the best in a printing job may exhibit unsatisfactory behavior in executing computing jobs. Case 1 and Case 2 bring out this important aspect. The user accepts the resource from a provider for one kind of job , rejects the resource from the same provider for a different kind of job. The **PATROL** model and our previous models store only a single reputation value. Hence, his net reputation value will be more or less than the threshold value. As a result the provider may be rejected by the same user for the same printing job the next time, even though he is good in printing. So we feel that the categorization of jobs is necessary for any comprehensive model.

4.2 Decaying Function

As time passes, entity reputation with respect to other entities typically changes to an unknown state, if little or no interaction occurs between them. When an entity Z receives a request (from entity *X*) for reputation information about entity *Y*, it modifies its reputation information relative to *Y* by using a decaying factor and then sends the result to the requesting entity.

$$rep\ y_{\Box,t} = rep\ y_{\Box,t_0} * \gamma \quad (15)$$

where γ depends on time . If t is the current time and t_0 is the time at which the last transaction took place, then the calculation of γ is as follows.

$\gamma = 1$ if $t - t_0 < 1$ month

$\gamma = 0.75$ if $1 < t - t_0 < 2$

$\gamma = 0.5$ if $2 < t - t_0 < 3$

$\gamma = 0$ if $t - t_0 > 3$.

4.3 Updating the reputation

The reputation value in the data base is updated after each transaction is successfully completed. The updation is done by using the following rules.

IF a new reputation value > The existing reputation value

Update the existing value by (new reputation*0.3+old reputation * 0.7)

ELSE IF (old reputation>new reputation) and (old reputation – new reputation)>1 then go by the new reputation. ENDIF

ELSE Update the reputation by (new reputation*0.7+old reputation * 0.3) ENDIF.

5. Experiments and results.

Several simulation studies have been conducted to establish the superiority of the proposed model. The first study has been conducted by taking two models one the existing model **PATROL** [Tajeddine et al 2007], and the other the Model 2 which is the present proposal, an improvement over model 1. This model also includes parameters for measuring direct trust . In this model 20 users and 20 providers are taken in to account. A transaction table is also maintained to keep track of all the transactions. Out of 150 cases, there is perfect agreement in 134 cases, and disagreement in 16 cases. Table 9 gives the cumulative result and Table 10 describes the disagreement cases. For the simulation study users 1-5 and providers 1-5 are malicious.

Table 9 Cumulative Result for study 1

Simulation	**YY**	**NN**	**YN**	**NY**	**TOTAL**
1.	**56**	**78**	**12**	**4**	**150**
Percentage	**37**	**52**	**8**	**3**	**100**

Models compared: Patrol model & Model 2

taken in order

As shown by Table 10 there are 16 disagreement cases. In the first 12 cases either the provider or the user is assumed to be malicious. So the proposed model rightly denies the transaction. Since the model applies the two way test criterion that is, it checks both the malicious user and the provider, it denies the transaction. In the last four cases, both the users and providers are reputed; so, the transactions are granted by our model. The PATROL model wrongly denied the transactions because it took the malicious nodes' feed backs in to account .The through put for the **PATROL** model is 45 % and for the proposed model it is 40%, and the reliability is further increased than our previous model by including the job type.

Table 10 Disagreement cases for study 1

S.NO	User	Provider	PATROL Model	Model 2
1	15	3	YES	NO
2	19	1	YES	NO
3	11	2	YES	NO
4	15	2	YES	NO
5	10	5	YES	NO
6	8	3	YES	NO
7	16	4	YES	NO
8	16	5	YES	NO
9	10	3	YES	NO
10	5	11	YES	NO
11	18	4	YES	NO
12	10	3	YES	NO
13	14	15	NO	YES
14	14	14	NO	YES
15	20	17	NO	YES
16	18	20	NO	YES

Agreement between the existing model and the proposed model is found to be 89 % and disagreement is 11 % and we have analyzed each of the disagreement cases.

The second simulation study has been conducted by considering Model 1 our previous model in the last chapter, and the proposed Model 2. Simulation has been conducted three times each with 100 runs. The results are tabulated in Tables 11 and 12.

Table 11 A comparisons of Model 1 and Model 2

Simulation	YY	NN	YN	NY	TOTAL
1.	31	60	4	5	100
2	20	68	4	8	100
3	21	72	3	4	100
Total	72	200	11	17	300
Cumulative Percentage	25	66	3.6	5.4	100

Table 11 gives a comparison of Models 1 and 2. There is (25+61) 91% agreement and 9% disagreement. The disagreement is due to the additional factors for measuring direct trust. For Model 1, the through put is 28.6 % (25+3.6), while the throughput for the second model is increased to 30.4 % (25+5.4). The reliability is increased in this model by including different contexts of interactions, and at the same time the through put is also increased. Table 12 presents all the disagreement cases. Transactions 1 to 11 were rejected by our previous model, Model 1, where as they have been granted by the proposed model. Transactions 12 to 28 are granted by Model 1, and denied by Model2 . In all these examples both the user and the provider are reputed.

Table 12 Disagreement cases for simulation

S.NO	User	Provider	Model 1	Model 2
1	13	6	No	yes
2	11	8	No	yes
3	6	8	No	yes
4	11	14	No	yes
5	17	10	No	yes
6	7	12	No	yes
7	17	7	No	yes
8	12	15	No	yes
9	12	10	No	yes
10	8	6	No	yes
11	9	7	No	yes
12	12	19	Yes	no
13	6	20	Yes	no
14	19	14	Yes	no
15	6	8	Yes	no
16	7	9	Yes	no
17	18	15	Yes	no
18	13	11	Yes	no
19	11	12	Yes	no
20	7	20	Yes	no
21	17	7	Yes	no
22	13	20	Yes	no
23	9	6	Yes	no
24	7	18	Yes	no
25	15	12	Yes	no
26	10	20	Yes	no
27	9	18	Yes	no
28	3	12	Yes	no

Let us illustrate this with an example. Consider a situation in which the user is 17 and the provider 7 (Table 16, transactions 7 & 21). Both entities are reputed. Model 1 denies the transaction 7 where as Model 2 accepts it. Model 2 stores three reputation values, such as reputation value 1 for computing, 3 for printing and 3.2 for file sharing. There is no categorization of jobs in Model 1. Hence, only one reputation value is stored by Model 1 for all types of jobs. The reputation value stored in Model 1 is 2.3. The job type for model 2 is printing. The overall trust for the printing job by Model 2 is found to be greater than the threshold value, and hence the model grants the transaction. The total trust in Model 1 is less than the threshold value, since the direct trust is 2.3.Hence the transaction is denied.

Now, another request comes from the same initiator (transaction 21).But this time the job type is computing. In Model 2, the reputation value for computing is 1. The total trust is found to be less than the minimum threshold, and hence the job is not executed. In the first model due to the previous transactions the reputation value has gone up. So, this time the transaction is accepted. The categorization of jobs facilitates the right sanction of transactions. An entity which is good in providing one kind of service may not be good in executing another type of job. In this illustration, transaction 7 is denied and 21 is accepted by Model 1. Transaction 7 is a printing job and 21 is computing. The computing job is more complex than the printing job. Hence, the decision of Model 2 is more accurate than that of Model 1.

The next simulation is done by varying the parameters. First, the context is kept constant and the simulation is by varying the size. Then the size is kept constant and the context is varied. Finally, both the parameters are varied .Figure 1 shows the through put when the context is kept constant as C1, that is, file sharing, and the size is varied from small, medium and large. When the context is C1 the total through put is 22% out of which size small is 5%, medium is 10% and large is 7%.

In the first simulation the through put is 22%, 26% in the second and 25 % in the third. The through put depends on the past transactions. The results clearly show that there are more number of reputed transactions of the type C2, since the total trust is calculated from DT1 ,DT2 and indirect trust . DT1 and DT2 depend on the number of previous transactions and their corresponding reputation values. Next, the experiments are repeated, by keeping the size constant and varying the context. First the size is kept as small; then it is repeated, for size medium and large.

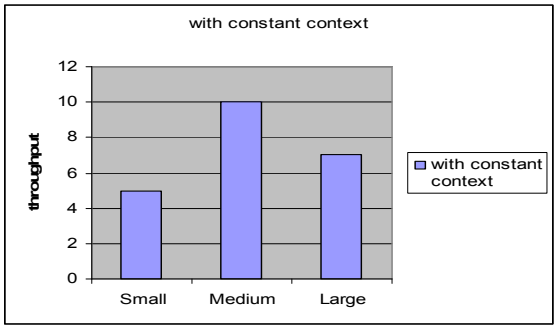

Figure 1 Simulation with varying sizes and Context

constant: C1

When the size is small, the through put is found to be 27%; when the size is medium the through put is 28%, and when the size is large the through put is 29%. Here, the throughput depends on the number of transactions of the particular job type.

6. Conclusions and future enhancements.

Security is one of the important aspects of Grid computing. There are several security issues among which trust relationship is the most prevailing issue. Hence, developing a trust model which addresses this issue is the main objective of the paper.

It has been shown that the model by Tajeddine et al does not assure complete reliability. The model took into account all the feedbacks, irrespective of the variations in the evaluation procedures; this results in large differences in the feedback values. The similarity factor defined by them fails to take care of the above factor. In this thesis, the proposed model evaluates a new factor called ‘compatibility’, which is based on Spearman’s ranking coefficient between sets of feedback values of the recommenders and the initiator. By considering the recommendations from only the recommenders whose feedbacks yield a

positive correlation with those of the initiator, it has been shown that such a method improves the behavior conformity in grid transactions.

The model is further enhanced by including additional parameters such as context, (to take care of the nature of the job) and the job size. Thus, an efficient reputation model has been proposed to improve the grid reliability. All the models proposed have been validated by appropriate simulation studies.

The Models can be further enhanced for efficient resource selection in Grid Computing. We have considered only the trust factor for the selection of the resource; cost factors like communication cost, computing cost etc can be included, so that the final selection by the user is cost effective.

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. 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.
8. 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.
9. 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.
10. 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
11. 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.
12. 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.
13. 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.
14. 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.