Building reliability model in Grid Computng

Vivekananth. P
Botho College
Gaborone
Botswana
vivek.jubilant@gmail.com

ABSTRACT: *In the recent period, Grid computing has emerged as the incremental level of distributed computing. It integrates the users and resources which are scattered in various domains. The Grid and its related technologies will be used only if the users and the providers mutually trust each other. The system must be as reliable and robust as of their own. The reliability can be defined as the probability of any process to complete it's task successfully as the way it was expected. In grid the reliability of any transaction can be improved by considering trust and reputation. Trust depends on one's own individual experiences and referrals from other entities. This paper proposes a model which improves reliability in grid by considering reputation and trust.*

Keywords: Trust, Reputation, Reliabilty, Grid security

Received: 11 September 2010, Revised 12 October 2010, Accepted 16 October 2010

1. Introduction

A Grid integrates and coordinates resources and users within different domains. Grid computing is interconnected computer systems where the machines share the resources which are highly heterogeneous. To achieve reliable transactions mutual trust must be established between the initiator and the provider. Trust is measured by using reputation and reputation is the collective opinion of others.

Trust can be defined as strong belief in an entity to act dependably, securely and reliably in a specific context. When we say that we trust someone or someone is trust worthy [1], 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 some one is un trust worthy we imply that the beneficial probability is very low and detrimental probability is high.

According to Abdul-Rahman and Hailes [2], a reputation is the expectation about an entity's behavior based on information about or observations of its past behavior. Reputation is what is generally said or believed about a person or thing's character [3]. Therefore, reputation is a measure of trustworthiness, in the sense of reliability. Reputation can be the source of building trust. 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.

The main purpose of security mechanisms in any distributed environment such as 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 will typically protect resources from malicious users, by

restricting access to only authorized users. However, in many situations one has 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.

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 that 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 recommendation and judgment on quality and reliability of the transactions..Reputation and Trust systems are soft security mechanisms which can assure behavior conformity. The reliability of any transaction obviously increases when feed backs of past experience of same type of jobs are considered and given with more weightage. The rest of the sections are organized as follows. Section 2 analyzes the similar previous work. Section 3 discusses about the proposed model. Section 4 gives details of experiments and analysis of results and section 5 concludes.

2. Related work

The simplest form of computing reputation scores is proposed by Resnick and Zeckhauser [4] who simply measure the reputation by finding the *sum of* the number of positive ratings and negative ratings separately, and keep the total score as the positive score minus the negative score . The advantage is that it is very simple model where anyone can understand the principle behind the reputation score, while the disadvantage is that it is primitive and therefore gives a poor picture on participants' reputation score.

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 rater trustworthiness/reputation, the age of the rating, the distance between rating and current score, etc. Xiong and Liu in their paper [5] use an adjusted weighted average of amount of satisfaction that a user gets for each transaction. The parameters of the model include the feedback from transactions, the number of transactions, the credibility of feedbacks, the criticality of the transaction.

Zacharia and Maes [6] review some systems in 2000 that address reputation management in e-commerce sites. Regarding on-line trading environments, Dellarocas [7] analyzes reputation mechanisms from a game-theoretical point of view. He allows opportunistic players to take part of the game and his analysis is fully based on mathematics developments.

Probabilistic / Bayesian models directly model the statistical interaction between the consumers and the providers. Wang and Vassileva [8] 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 recommendations about other users.

Baolin Ma,Jizhou Sun [9] talk about trust model based on reputation. In this model both direct and indirect trust are calculated by using reputation. Direct trust is calculated and the value of direct trust is used to find the value of indirect trust. Gregor von laszewki [10] provide a way for efficient resource selection by considering Eigen trust algorithm. Their approach is similar to Azzedin approach [11] except for a new parameter context. Ayman Tajeddine et al. [12] propose an impressive reputation based trust model. In this approach the initiator host calculates reputation value of target host based on its previous experiences and gathered feedbacks from other hosts. The recommenders can be from the same administrative control (neighbor) or from different trusted domain (friends) or from a completely strange domain (stranger).

Srivaramangai [13] talk about the trust system is made more robust by eliminating the unreliable feedbacks by using rank correlation method. The model is further improved in Srivaramangai [14] by adding two way test criteria.

3. Proposed Model

The proposed model is further enhancement. In the last two models proposed, two types of trust have been taken, 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 evolution procedure are not correlated to that of its' own. The second model is further enhanced by adding two way test criteria. In that model the transaction is allowed only when the user trust score as evaluated by the provider is greater than the pre defined threshold value and the provider trust score is greater than

the threshold of the user. These two models and other existing models take the direct trust score from the table. There is no categorization of type of jobs. This model measures direct trust based upon different parameters such as context, size and complexity. It categorizes the jobs. The model assumes that the feedback value given by the user for one kind of job provided by one entity is different from another kind of job by the same entity. So the model uses three types of trust namely DT1, DT2 and indirect trust. DT1 represents trust of user on the provider as a result of same kind of transactions and DT2 for different type of transactions. Indirect trust is calculated by same expression as that of previous models. This model adheres to the fact that the reputation values are not always constant. When there is no transaction between two entities for a longer period of time than the value of reputation should be brought down. So this model adopts a function called decay function which will decrease the value of reputation when there is no transaction for a given interval. After each transaction is over the updation is done.

3.1 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 1). 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 1, 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 3.1) , 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 3.2). 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 1.

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

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

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

Table 3.1 Complexity Table

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

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

Table 3.2 Transactions between A and P

The trust of an object l about an object I at context c is given by

$$\text{trust}_{x,y,c} = \frac{\alpha\,[DT_{x,y,c}] + \beta[IT_{x,y,c}]}{\alpha + \beta} \tag{2}$$

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

$DT_{x,y,c}$ represents direct trust, $IT_{x,y,c}$ represents indirect trust

$$IT_{x,y} = IT1_{x,y} + IT2_{x,y} \tag{3}$$

$$IT1_{x,y} = \frac{\sum_{i=1}^{n} \delta_{1i}\, rep\, \frac{y}{z_i}}{\sum_{i=1}^{n} \delta_{1i}} \tag{4}$$

$$IT2_{x,y} = \frac{\sum_{i=1}^{n} \delta_{2i}\, rep\, \frac{y}{t_i}}{\sum_{i=1}^{n} \delta_{2i}} \tag{4}$$

$\delta 1, \delta 2$ are credibility factors

z_i represents i^{th} entity in the neighbor domain and t_i represents i^{th} entity in the friend domain.

Indirect trust is calculated by considering the recommendations from reliable entities. The factors such as credibility, compatibility, activity and specificity are considered for measuring indirect trust. The elimination of feed backs is done by using the compatibility factor.

$$\textit{crediblity} = a * \textit{compatablity} + b * \textit{activity} + c * \textit{specificity}$$

$$\textit{Where } a + b + c = 1 \textit{ and } a > b > c. \tag{5}$$

$$\textit{compatablity} = 1 - \frac{6\sum_{i=1}^{n} \sum d\eta_i^2}{n\,(n^2 - 1)} \tag{6}$$

$$activity = \frac{number\ of\ interactions\ by\ an\ entity\ as\ a\ user}{total\ number\ of\ interactions\ by\ all\ entities} \quad (7)$$

$$specificity = \frac{number\ of\ interactions\ by\ an\ entity\ as\ a\ provider}{total\ number\ of\ interactions\ by\ all\ entities} \quad (8)$$

$\sum_{i=1}^{n} \delta_{1t}\, rep\frac{y}{z_i}$ represents weighted sum of reputations of y as represented by neigbours.

$\sum_{i=1}^{n} \delta_{2t}\, rep\frac{y}{t_i}$ represents weighted sum of reputations of y as represented by friends.

$$DT_{x,y,c} = \gamma[DT1_{x,y,c}] + \theta[DT2_{x,y,c}] \quad (9)$$

Where γ and θ are suitable weighing factors and $\gamma > \theta$ and $\gamma + \theta = 1$.

$DT1_{x,y,c}$ Direct trust of x on y which is obtained from the transactions of same type.

$DT2_{x,y,c}$ Direct trust of x on y which is obtained from the transactions of different type.

$$DT1_{x,y,c} = \frac{\sum_{i=1}^{n} r_i}{n} \quad (10)$$

r_i represents Reputation value of entity y by x on i^{th} transaction and n represents the Total number of transactions .

$$DT2_{x,y,c} = \frac{\sum_{i=1}^{n} c_i r_i}{\sum_{i=1}^{n} f_i} \quad (11)$$

c_i represents suitable credibility and r_i the reputation value of entity y by x on i^{th} transaction and f_i represents the frequency.

4. Experiments and Results

Simulation study has been conducted for the existing model and the proposed model.

Model 1 : Existing model as proposed by [12].

Model 2 : Present model eliminates biased feed backs by using compatibility factor and applies two way test criteria to decide the transaction . This model also includes parameters for measuring direct trust . In this model 20 users and 20 providers are taken. Out of 150 cases, there is perfect agreement for 134 cases, disagreement for 16 cases. Table 4.1 gives cumulative result and Table 4.2 describes the disagreement cases. The model assumes user 1-5 and provider 1-5 are malicious.

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

Table 4.1 Cumulative Result 1

As depicted by Table 4.2 there are 16 disagreement cases. In the first 12 cases either the provider or the user is assumed malicious nodes. So the proposed model rightly denies the transaction. Since the model applies two way test criteria that is it checks for both malicious user and provider it denies the transactions. The last four cases both the users and providers are reputed so the transactions is granted by our model. The through put is also fair enough that is 52 % and the reliability is further increased than our previous model by including the job type. Figure 4.1 shows the allocation by the two models.

On the whole it was found that 91% agreement was there out of three simulations between two models. The remaining 9%

disagreement due to the addition of new factors such as context and complexity. Here also the user 1 to user 5 and provider 1 to provider 5 are assumed malicious nodes. The proposed model further improves reliability by preventing malicious nodes to participate in the transactions.

S.NO	User	Provider	Model1	Model2
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

Table 4.2 Disagreement Cases 1

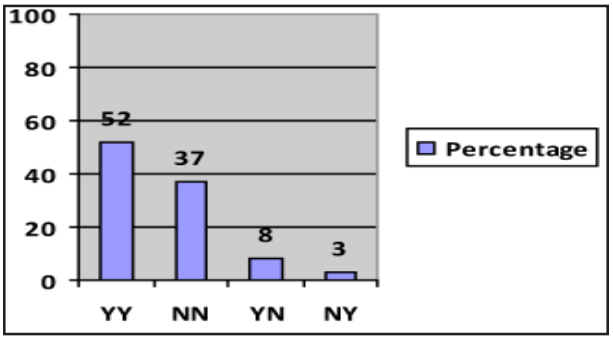

Figure 4.1 Allocation by two models

Second simulation study was conducted by taking the previous model proposed by us [14] and the proposed model was found to be more accurate because of the additional parameters. This time simulation was run three times each with 100 runs. The results were given in table 4.3 and 4.4.

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

Table 4.3 Cumulative Results 2

S.NO	User	Provider	Model1	Model2
1	13	3	**yes**	**no**
2	11	1		
3	6	4		
4	11	2		
5	17	5		
6	6	3		
7	17	5		
8	12	5		
9	16	4		
10	8	1		
11	9	5		
12	5	2	**no**	**yes**
13	6	20		
14	19	14		
15	6	8		
16	3	1		
17	18	15		
18	3	1		
19	3	2		
20	7	20		
21	17	7		
22	13	20		
23	9	6		
24	7	18		
25	15	12		
26	10	20		
27	9	18		
28	3	12		

Table 4.4 Disagreement Cases 2

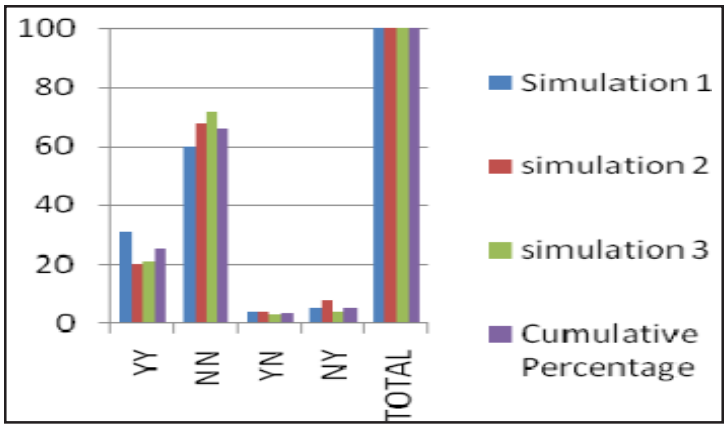

Figure 4.2 Cumulative result

Table 4.4 depicts all the disagreement cases. Transactions 1 to 11 are granted by our previous model where as rejected in the proposed model. In all these transactions the providers are assumed to be malicious. So our proposed model rightly corrects

the error occurred in the previous model. Transactions 12 to 28 are granted by new model where as rejected by the previous model. In all these transactions either both the providers and users are malicious or good. That is the reason the transactions are approved by the new system. Thus the new system eliminates the small percentage of erroneous decision from the previous model. The system is made more reliable. Figure 4.2 shows the allocation by the two models.

5. Conclusions

This paper present has presented a new comprehensive trust model in the sense it takes cognizance of both provider and user sensibilities. The model includes new expression for measuring direct trust by categorizing the type of jobs. Further by eliminating biased feedbacks from both user and provider groups the resultant transactions become more reliable and secure. Simulation study describes the superiority of the proposed comprehensive trust model over the existing models.

References

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

[2] Abdul-Rahman, A., 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, p 6007-6016.

[3] Bearly,T., Kumar, V. (2004). Expanding trust beyond reputation in peer-to-peer systems, *In:*Proceedings of the 15th International Workshop on Database and Expert Systems Applications (DEXA '04), 30 August–3 September, Zaragoza, Spain, p.966–970.

[4] Resnick, P., Zeckhauser, R. (2002). Trust among strangers in internet transactions, Empirical analysis of eBay's reputation system. 11, p. 127–157.

[5] Xiong, L., Liu, L.(2004). PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities, *IEEE Transactions on Knowledge and Data Engineering*, 16 (7) 843-857.

[6] Zachari, G., Maes, P.(2000). Trust management through reputation mechanisms, *Applied Artificial Intelligence*, 14 (9) 881-907.

[7] Dellarocas,Chrysanthos (2005). Reputation mechanism design in online trading environments with pure moral hazard, *Info. Sys. Research*, 16 (2) 209–230.

[8] Wang,Y., Vassileva, J., (2003). Trust and reputation model in peer-to-peer networks, *In*: Proceedings of the Third International Conference on Peer-to-Peer Computing, Linköping, Sweden, p.150–157.

[9]Ma, Boolin ., Sun, Jizhou(2006). Reputation-based Trust Model in Grid Security System, *Journal of Communication and Computer* 3 (8) 41-46.

[10] Beulah kurian, Gregor von laszewki . (2003). Reputation based grid resource selection' in the proceedings of the workshop on adoptive resource selection, p 28-36.

[11] Farag Azzedin and Muthucumaru Maheswaran.(2002). Evolving and Managing Trust in Grid Computing Systems, *In:* Proceedings of the Canadian Conference on Electrical & Computer Engineering, V 3, p.1424-1429 .

[12] Tajeddine, A., Kayssi, A., Cheab, A., Artail, H. (2005). A comprehensive reputation-based trust model for distributed systems, *In*:The IEEE Workshop on the Value of Security through Collaboration (SECOVAL), September 5–9, Athens, Greece, l (3–4) 416–447.

[13] Srivaramangai P., Srinivasan R. (2009). Reputation Based Trust Model With Elimination Of Unreliable Feed backs, *International Journal of Information Technology and Knowledge Management*, 2 (2) 455-459.

[14] Srivaramangai, P., Srinivasan, R. (2010). Reputation based Two Way Trust Model for Reliable Transactions In Grid Computing in International journal of Computer Science Issues , 17 (5) 33-39.

[15] Vivekananth, P. (2010). An Overview of Trust models and proposal of new model based on Resource Selection in Grid Computing, *International Journal of Engineering and Technology*, 2 (4) 387-389.

[16] Vivekananth,P.(2010). Trusted Resource allocation in Grid Computing by using Reputation, I*nternational Journal of Computer Science & Communication* 1 (2) 23-25.