A Comprehensive Trust Model for Improved Reliability in Grid

Srivaramangai P
MCA Department ,BS Abdur Rahman University
Chennai , Tamilnadu, India

Renagaramanujam Srinivasan
Retd . prof. CSE Department, BS Abdur Rahman University
Chennai , Tamilnadu, India

ABSTRACT

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 in the internet. Reputation based systems can be used in grid to improve the reliability of transactions. Reliability is the probability that a process will successfully perform it's prescribed task without 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. This paper aims at providing a robust and reliable model by eliminating the feed backs of the entities which are not having any compatibility with it's own evaluation procedure, This model further applies two way test criteria for initiator and provider and also includes new expression for measuring direct trust.

I. 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 some one or some one 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 behaviour based on information about or observations of its past behaviour. 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.

II. 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).

In our previous publication [13] the trust system is made more robust by eliminating the unreliable feedbacks by using rank correlation method. The model is further improved in our last publication [14] by adding two way test criteria.

III. PROPOSED MODEL

The proposed model is further enhancement of the second one. In the last two models proposed by us, 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.

Computation of Trust:

Suppose a scenario goes like this. A is the user and wants to use the resource of provider P. The user wants to execute a job of size medium. The system assigns complexity for the above job by referring the predefined assigned complexities. Nine different combinations of context and size of jobs are taken and complexity is assigned for each combination . After assigning complexity the feed backs of the same kind of jobs between the same user and provider is taken and direct trust is calculated by the below formulae.

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

$$\text{Trust}_{I,l,c} = \frac{\alpha\,[\,DT_{I,l,c}\,] + \beta\,[\,IT_{I,l,c}\,]}{\alpha + \beta} \qquad (3.1)$$

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

$$DT_{I,l,c} = \frac{\theta\ [DT1_{I,l,c]} + ¥\,[\,DT2_{j,l,c}\,]}{\theta + ¥} \qquad (3.2)$$

Where $\theta > ¥$ and $\theta + ¥ = 1$

$$DT1_{I,l,c} = \frac{\sum_{i=1}^{n} r_i}{\sum_{i=1}^{n} f_i} \qquad (3.3)$$

$$DT2_{I,l,c} = \frac{\sum_{i=1}^{n} c_i\, r_i}{\sum_{i=1}^{n} f_i} \qquad (3.4)$$

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.

$$IT=indirecttrust1+indirecttrust2 \qquad (3.5)$$

$$\text{indirecttrust1} = \frac{\sum_{i=1}^{n} \delta 1_{i}\,\text{rep } y/z_i}{\Sigma\ \delta 1_{i}} \qquad (3.6)$$

$$\text{indirect trust 2} = \frac{\sum_{i=1}^{m} \delta 2\ i\ \text{rep } y/t_i}{\Sigma\,\delta 2_{i}} \qquad (3.7)$$

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

Credibility = a*compatibility + b*activity + c*specificity

where a>b>c and a+b+c=1 .

$$\text{Compatibility} = 1 – 6\,\Sigma\, d_{R\,i}2/\ n\ (n2\ - 1) \qquad (3.8)$$

Where $d_{R\ I}$ gives the difference in ranks.

$$\text{activity} = \frac{\text{No of interactions of entity as user}}{\text{Total number interactions by all entities}} \qquad (3.9)$$

$$\text{Specificity} = \frac{\text{No of interactions of entity as a provider}}{\text{Total number of interactions}} \qquad (3.10)$$

IV. 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.

Table 4.1 Cumulative Result

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

Table 4.2 Disagreement cases

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

Out of 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.

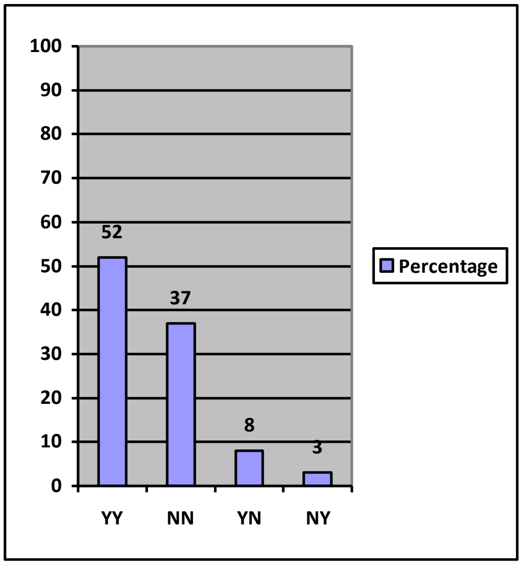

Figure 4.1 Allocation by two models

V. CONCLUSION

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.

ACKNOWLEDGMENT

The authors would like to express their thanks to Dr. P. Kanniappan, Vice chancellor, Dr.V.M.Periasamy , Registrar, Dr.K.M.Mehata the Dean and Dr.P.Sheik abdul Khader , HOD/Dept of Computer Applications of B.S.Abdur Rahman University for the environment provided.

REFERENCES

1. Gheorghe Cosmin Silaghi, Alvaro E. Arenas, 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. 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.
3. Bearly, T. and Kumar, V. (2004) ‘Expanding trust beyond reputation in peer-to-peer systems’, Proceedings

of the 15th International Workshop on Database and Expert Systems Applications (DEXA '04), 30 August–3 September, Zaragoza, Spain, pp.966–970.

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

5. 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 ,

6. Zachari G. and Maes P.(2000) , 'Trust management through reputation mechanisms', Applied Artificial Intelligence, Vol 14 , No 9, pp 881-907.

7. Chrysanthos Dellarocas. , (2005) ,'Reputation mechanism design in online trading environments with pure moral hazard' , Info. Sys. Research, Vol 16, No 2, pp 209–230,

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. 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.

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

11. Farag 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. 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.

13. **Srivaramangai P.,** Srinivasan R., (2009) ,'Reputation Based Trust Model With Elimination Of Unreliable Feed backs ' in International Journal of Information technology and Knowledge Management , Vol 2, NO 2, pp.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 , Vol 7 , No 5 , pp.33-39.