International Journal of Information Technology and Knowledge Management
July-December 2009, Volume 2, No. 2, pp. 455-459

REPUTATION BASED TRUST MODEL WITH ELIMINATION OF UNRELIABLE FEEDBACKS

P. Srivaramangai[*] & Dr. R. Srinivasan[**]

Grid computing system is the one where individual entities share their resources with others in their own domain as well as with other domain. The resources should be shared with out loosing individual's confidentiality and control over their resources. To achieve this and ensure grid security various models have been proposed and one of them is the trust model. Reputation based trust models are coming up to address the problems in behavior conformity. The reputation values in these models are evaluated in a democratic manner based upon the feedback from other entities. This paper investigates such reputation based trust models in the presence of malicious entities which give deliberately wrong feedbacks. We propose an enhancement by which the malicious feed backs are eliminated by rank correlation method. Thus the work enhances the behavioral conformity in the presence of malicious entities.

1. Introduction

Grid computing is a system, which provides distributed services that integrates wide variety of resources with different quality of services. Security plays a very important role in grid systems. Security challenges in grid can be classified in to three categories, integration challenge, interoperability challenge, and trust relationship challenge [1].

In general security mechanisms in any environment must give protection against malicious behavior of participating members. Authorization and authentication restrict access to the resources [1]. But in the grid application the one who uses the resource also needs reliable and secure services. Reputation based trust models address this problem. The main issues characterizing the reputation systems are the trust metric (how to model and compute the trust) and the management of reputation data how to securely and efficiently retrieve the data required for the trust computation.

The existing models include all the feedbacks irrespective of their evaluation procedures. There must be a model which considers only reliable feedbacks so that behavior conformity is ensured. This paper proposes a model, which makes the evaluated trust values more robust by eliminating the unreliable feedbacks.

2. Related Work

Li xiong and liu present [5] a reputation-based framework. They claim that feed back values only are not enough for the calculation of trust and reputation. Y. Wang and J. Vassileva [6] propose a reputation model based on Bayesian network. According to their model the peers needs are different in different situations. Selcuk et al. suggests in [7] a reputation based trust management system in which the reliability is calculated based on previous transactions. Ayman Tajeddine *et al.* in [8] propose a very 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. F. Azzedin, M. Maheswaran [9] discuss about managing trust in grid by proposing a behavior trust management model. Trust levels are graded from a to f. Both direct and indirect trust are considered.

Gui Xiaolin, Xie Bing [10] propose a trust model based on behavior tracks. Attenuation function is corporated for decaying factor. Baolin Ma *et al.* in [11] present a reputation based trusted model. Their model considers both direct feed back and feed back from other entities Direct trust is given with more weightage than the indirect score. Beulah kurian, Gregor von laszewki [12] provide a way for efficient resource selection. Their approach is similar to Azzedin approach [9] except for a new parameter "context".

3. Proposed Model

The proposed work is an enhancement of the existing model [8] that uses both direct trust and indirect trust. Direct trust is calculated from the transactions which are done directly by the initiator and is given higher weightage. Indirect trust is measured by getting feed backs from entities in the same domain and also from other domains. In the basic model the credibility of the recommenders feedback is estimated by considering different parameters such as similarity, activity and specificity.

[*] MCA Dept., BSA University, Chennai, Tamilnadu, India.
E-mail: sri_padma_2000@yahoo.com
[**] CSE Dept., BSA University, Chennai, Tamilnadu, India.
E-mail: drrsrs@yahoo.com

The existing model took all the feedbacks into consideration while calculating the trust values. In the proposed model we assume that there can be a few malicious entities that can give a wrong feedbacks about other entities. Even if single entity is giving a wrong feedback, it is sufficient to alter the decision from one state (grant) to another (not grant). In the real world we expect a set of malicious entities trying to disrupt the smooth functioning of the grid system by false reporting by giving false feedbacks. They can do so because the feedbacks that such entity gives are based on an entity's own evaluation.

The case for the modification of the existing method can be put forth as follows: Suppose A is the initiator and he wants to get feedbacks about a potential entity P. B and C have already transacted business with P. A would like to use the feedbacks of B and C about P, so as to determine whether to shortlist P as a candidate provider or drop him from listing.

The existing method simply uses the scores given by B and C and evaluates the trustworthiness of the provider as a function of above feedbacks. We go on to ask the questions – are the feedbacks given by entities are reliable? Unbiased? Trustworthy?

We can answer the above question if A, B, and C have given feedbacks about some common entities say E1, E2, E3, E4 and E5. A compares his feedbacks about these common entities with those given by B and C. If there is a positive correlation then A takes the feedback back into account; and if the correlation is <=0 A ignores the corresponding feedbacks. For example if A's evaluations regarding entities E1, E2, E3, E4 and E5 are 4.8, 4, 3.6, 2.4 & 2 and the evaluations of B and C respectively are 4.2, 3.9, 3.5, 2.5, 2.1 and 2.9, 2.7, 3, 3.5, 4.2 then A will not consider the feedback of C.

Thus A the initiator entity can evaluate the trustworthiness of provider I, based on views of colleagues, whose evaluation schemes are similar to his. The correlation can be obtained by any of the standard methods available such as Pearson Product Moment Correlation, Spearman rank Order Correlation (rho) or the Kendall rank order Correlation (tau) and we have chosen Spearman's Rank Coefficient. Thus even if an entity tries to play havoc by giving false or unreliable feedback values they can be identified and eliminated from consideration.

In this paper, we focus only on eliminating unreliable feedback values from adversely affecting trust calculations. Quarantining such false feedback providers, if such actions are found to the deliberate is an issue that is to be considered separately and it is beyond the scope of this paper.

Ranking:

Since the feedbacks are collected from different domains, there is a chance of getting biased inputs. The feedbacks are sorted and rank is assigned. Rank correlation is calculated. If the result is positive then that entities feedback will be taken. Otherwise feedback values will not be considered. Only the feedbacks of entities with positive correlation are considered for calculating reputation.

$$\text{Similarity} = 1\text{–}6\ \Sigma\ d_i 2\ /\ n\ (n2\text{–}1)$$

$$\text{activity} = \frac{\text{number interactions by recommenders}}{\text{Total number interactions by all recommenders}}$$

$$\text{Specificity} = \frac{\text{Number of interactions with initiator}}{\text{Total number of interactions with all other hosts}}$$

Credibility = a * similarity + b * activity + c * specificity where $a > b > c$ and $a + b + c = 1$

3.1 Computation of Reputation:

Consider the scenario where entity x wants to interact with entity y to complete some task. X wants to measure the trustworthiness of y. The direct trust is calculated based upon the behavior of target entity on direct transactions. Then it inquires reputation of y from the entities in the same domain and from other domain. The reputation will be calculated from the formula given below.

$$\text{Rep } y/x_k = u\text{*direct trust} + v\ *\ \text{indirect 1} + w\ *\ \text{indirect 2}$$

Where $u + v + w = 1$ and $u > v > w$.

$$\text{indirect 1} = \Sigma\ \alpha_i \text{ rep } y/xi$$

$$\frac{i \neq k}{\Sigma \alpha_i}$$

$$i \neq k$$

$$\text{indirect 2} = \Sigma\ \beta_j \text{ rep } y/xi$$

$$\frac{j \neq k}{\Sigma \beta_i}$$

$$j \neq k$$

α, β are credibility factors...

Host Y is new to the system:

In the case where Host Y is a new host that has just joined the system and which, consequently, has not yet interacted with any other hosts, X interacts with Y according to a predefined first impression value that X uses which may be a minimum value. Y will be assigned with unharmful resources for the initial period.

If the reputation is greater then the minimum threshold value the job will be assigned to y. Otherwise it will be rejected. After the transaction is over the reputation table will be updated by taking the new value. The decaying factor is considered for modifying the reputation of each entity with time.

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

rep *y*/*z* = final value + (final value – initial value) * γ

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

γ = 1 if $t–t_0 < 1$ month
γ = 0.75 if $1< t–t_0 < 2$
γ = 0.5 if $2< t–t_0 < 3$
γ = 0 if $t–t_0 > 3$

4. EXPERIMENTS AND RESULTS

The reputation Table of the entities are given below.

Table 1
Reputation Table

	A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*
A	——	4.31	3.23	4.73	4.41	3.47	4.32	4.25	4.21	4.79	2.72	4.19	4.21	2.65	4.11
B	4.67	———	3.11	4.21	4.37	3.36	4.22	4.22	4.19	4.87	2.43	4.87	4.9	3.21	4.05
C	1.87	1.32	———	1.49	1.92	3.82	0.78	1.09	1.01	1.66	3.76	1.36	1.54	3.82	2.01
D	4.42	4.55	2.87	———	4.21	2.56	4.01	4.56	3.99	4.32	3.05	4.45	4.12	2.14	4.03
E	3.51	3.21	1.92	2.75	———	1.91	3.44	3.11	3.57	3.35	1.49	2.66	3.33	1.34	3.21
F	1.25	1.19	3.78	1.23	1.81	——-	1.12	1.43	1.04	1.9	4.01	1.38	1.09	4.73	1.25
G	3.11	2.89	1.86	2.94	3.65	1.78	——-	3.32	3.45	2.61	1.76	3.99	2.1	1.33	3.2
H	2.88	3.7	1.65	3.2	3.87	1.54	3.65	———	3.22	3.81	1.14	3.19	3.89	1.89	3.98
I	3.34	3.19	1.45	3.48	3.79	1.14	3.24	3.09	——-	3.02	1.64	3.72	2.58	1.65	3.58
J	4.28	4.17	2.86	4.07	4.01	2.11	4.21	4.17	4.97	——-	3.34	4.52	4.37	2.98	4.67
K	1.32	1.09	4.32	1.34	1.73	4.91	1.08	1.19	1.09	1.55	——-	1.83	1.99	3.67	1.14
L	4.41	4.69	2.52	4.17	4.09	2.34	3.99	3.98	4.56	4.44	2.12	——	4.53	3.09	4.55
M	4.11	4.45	2.13	4.61	3.38	2.66	4.09	4.15	4.35	4.84	3.23	4.39	——	2.45	4.22
N	1.52	1.45	4.67	1.45	1.57	2.67	1.43	1.47	1.86	1.84	4.81	1.19	2.16	——	1.01
O	3.11	3.45	1.23	3.54	2.99	1.34	2.99	3.23	3.19	2.96	1.99	3.03	3.72	1.45	——-

Two sets of experiments are performed to evaluate the feedbacks. The models are simulated by taking SQL server as backend and java as front end. The parameters considered are tabulated below.

Table 2
Experimental Parameters

Parameters	*Description*
N	The no of domains
P	No of entities
K	The reputation values

The experiment is to evaluate the reliability of the models and show how the biased feedbacks can affect the system. In the simulation the existing model is compared with the proposed model, which eliminates biased feedbacks.

The total no of entities is set to 15 and the simulation is run 10 times. For the first experiment the unreliable feedbacks are also taken for allocating the resources. Due to those feedbacks the resources are allocated to wrong entity and some times the resource is being denied for right entity. In the second experiment the biased feedbacks are not considered and the results are more accurate.

Out of ten trials two of them are observed to be contradictory.

First Set :

Initiator: B

Provider: I

No of trials 10

No of nodes 15

The feed backs of the nodes which are having negative correlation are not taken for calculating trust. In the existing model the initiator rejects the resource. In the new model the resource is accepted. Since both the entities that is the initiator and the provider are taken as good the acceptance of the resource is more accurate.

Second Set:

Initiator: N

Provider: A

Table 3
Spearman's Rank Correlation Coefficient between *B* & Others.

	B	*A*	*C*	*D*	*E*	*F*	*G*	*H*	*J*	*K*	*L*	*M*	*N*	*O*
B	—-	4.67	3.23	4.73	4.41	3.47	4.32	4.25	4.79	2.72	4.19	4.21	2.65	4.11
A	4.31	—-	3.11	4.21	4.37	3.36	4.22	4.22	4.87	2.43	4.87	4.9	3.21	4.05
C	1.32	1.87	—-	1.49	1.92	3.82	0.78	1.09	1.66	3.76	1.36	1.54	3.82	2.01
D	4.55	4.42	2.87	—-	4.21	2.56	4.01	4.56	4.32	3.05	4.45	4.12	2.14	4.03
E	3.21	3.51	1.92	2.75	—-	1.91	3.44	3.11	3.35	1.49	2.66	3.33	1.34	3.21
F	1.19	1.25	3.78	1.23	1.81	—-	1.12	1.43	1.9	4.01	1.38	1.09	4.73	1.25
G	2.69	3.11	1.86	2.94	3.65	1.78	—-	3.32	2.61	1.76	3.98	2.1	1.33	3.2
H	3.7	2.88	1.65	3.2	3.87	1.54	3.65	—-	3.81	1.14	3.19	3.89	1.89	2.98
J	4.17	4.28	2.86	4.07	4.01	2.11	4.21	4.17	—-	3.34	4.52	4.37	2.98	4.67
K	1.09	1.32	4.32	1.34	1.73	4.91	1.08	1.19	1.55	—-	1.83	1.99	3.67	1.14
L	4.69	4.41	2.52	4.17	4.09	2.34	3.99	3.98	4.44	2.12	—-	4.53	3.09	4.55
M	4.45	4.11	2.13	4.61	3.39	2.66	4.09	4.15	4.84	3.23	4.39	—-	2.45	4.22
N	1.45	1.52	4.67	1.45	1.57	4.67	1.43	1.47	1.84	4.81	1.19	2.16	—-	1.01
O	3.45	3.71	1.23	3.54	2.99	1.34	2.99	3.23	2.96	1.99	3.03	3.72	1.45	——
	RC	**0.85**	**-0.67**	**0.45**	**0.20**	**-0.32**	**0.08**	**0.08**	**0.07**	**0.29**	**-0.52**	**-1.01**	**0.005**	**-0.6**

N is assumed to be malicious. It gives false feed back. In the existing model the resource is accepted and in the new model the resource is rejected. In the existing model all values are taken and the result is acceptance of the resource. That is the existing model is providing resource for wrong entity. In the new model the resource is denied after giving due consideration to the reliable feed backs which is the more accurate allocation. The values are as shown in the following Table.

Table 4
Spearman's Rank Correlation Coefficient between *N* & Others

	N	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*O*
B	3.21	——-	3.11	4.21	4.37	3.36	4.22	4.22	4.19	4.87	2.43	4.87	4.9	4.05
C	3.82	1.32	——-	1.49	1.92	3.82	0.78	1.09	1.01	1.66	3.76	1.36	1.54	2.01
D	2.14	4.55	2.87	——	4.21	2.56	4.01	4.56	3.99	4.32	3.05	4.45	4.12	4.03
E	1.34	3.21	1.92	2.75	——	1.91	3.44	3.11	3.57	3.35	1.49	2.66	3.33	3.21
F	4.73	1.19	3.78	1.23	1.81	——-	1.12	1.43	1.04	1.9	4.01	1.38	1.09	1.25
G	1.33	2.89	1.86	2.94	3.65	1.78	——-	3.32	3.45	2.61	1.76	3.99	2.1	3.2
H	1.89	3.7	1.65	3.2	3.87	1.54	3.65	——-	3.22	3.81	1.14	3.19	3.89	3.98
I	1.65	3.19	1.45	3.48	3.79	1.14	3.24	3.09	——-	3.02	1.64	3.72	2.58	3.58
J	2.98	4.17	2.86	4.07	4.01	2.11	4.21	4.17	4.97	——-	3.34	4.52	4.37	4.67
K	3.67	1.09	4.32	1.34	1.73	4.91	1.08	1.19	1.09	1.55	——-	1.83	1.99	1.14
L	3.09	4.69	2.52	4.17	4.09	2.34	3.99	3.98	4.56	4.44	2.12	——	4.53	4.55
M	2.45	4.45	2.13	4.61	3.38	2.66	4.09	4.15	4.35	4.84	3.23	4.39	——-	4.22
O	1.45	3.45	1.23	3.54	2.99	1.34	2.99	3.23	3.19	2.96	1.99	3.03	3.72	——
RC		**0.005**	**-.005**	**-.033**	**-0.15**	**.35**	**-0.46**	**-0.51**	**-0.47**	**-0.2**	**0.6**	**-0.4**	**-0.03**	**-0.23**

Most of the malicious nodes have correlated reputation values with *N*, which is also malicious. So finally the resource is rejected in the new model. Since all the values are taken in the first model it is wrongly concluded. The over all result of all executions are given below,

Table 5
Result

Execution	*Initiator*	*Provider*	*TS1*	*New model*	*TS2*	*Existing model*
1	D	N	1.509	NO	1.766	NO
2	C	E	2.068	NO	2.303	NO
3	H	G	3.293	YES	3.064	YES
4	I	M	4.336	YES	4.124	YES
5	N	A	2.863	NO	3.271	YES
6	C	I	1.662	NO	2.023	NO
7	B	I	3.16	YES	2.686	NO
8	J	M	4.516	YES	4.365	YES
9	M	F	0.979	NO	1.476	NO
10	H	N	1.538	NO	1.768	NO

The graphs below depict the allocation for existing model & proposed model

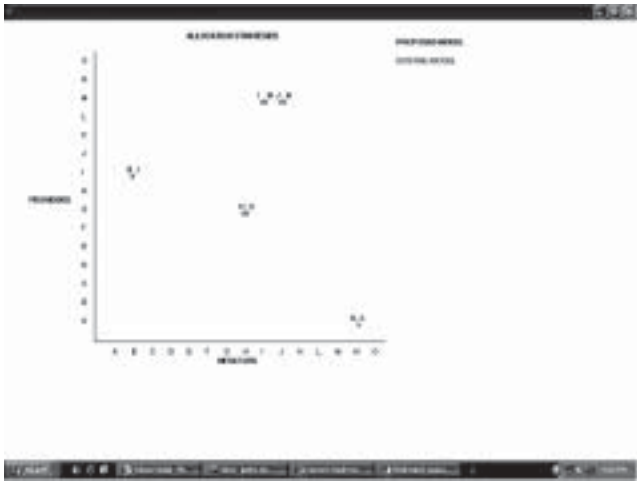

Figure 1: Results for Existing Model & Proposed Model

CONCLUSION

In this paper the reputation based trusted model is enhanced by eliminating the biased inputs. It improves the security for the entities which is going to use the resources in the grid environment.

REFERENCE

[1] A. Arenas "State of Art Survey on Trust and Security in Grid Computing System (2006).

[2] Gheorghe Cosmin Silaghi, Alvaro E. Arenas, Luis Moura Silva," Reputation-Based Trust Management Systems and their Applicability to Grids "*CoreGRID Technical Report Number* TR-0064 (2007).

[3] Marcim Adamski, Alvaro Arenas, Angelos Bilas "Trust and Security in Grids: A State of the Art" CoreGRID White Paper Number WHP-0001 (2008).

[4] A. Abdul-Rahman and S. Hailes. "Supporting Trust in Virtual Communities". In *HICSS'00: Proceedings of the 33rd Hawaii International Conference on System Sciences*, **6** (2000) 6007, Washington, DC, USA. IEEE Computer Society.

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

[6] Y. Wang and J. Vassileva, "Trust and Reputation Model in Peer-to-Peer Networks," Proceedings of the Third International Conference on Peer-to-Peer Computing (P2P'03), (2003).

[7] A. Selcuk, E. Uzun, and M. Pariente, "A Reputation-Based Trust Management System for P2P Networks," IEEE International Symposium on *Cluster Computing* and the Grid (2004).

[8] Ayman Tajeddine Ayman Kayssi Ali Chehab Hassan Artail "A Comprehensive Reputation-Based Trust Model for Distributed Systems " *IEEE* (2005).

[9] F. Azzedin, M. Maheswaran "Evolving and Managing Trust in Grid Computing System" *IEEE CCECE*, (2002).

[10] Gui Xiaolin, Xie Bing "Study on Behavior Based Trust Model in Grid Security System "Proceedings of the 2004 IEEE International Conference on *Services Computing* (SCC'04).

[11] Baolin Ma, Jizhou Sun, Ce Yu "Reputation-Based Trust Model in Grid Security System,'' **3**(8) (2006) (Serial No. 21) *Journal of Communication and Computer*, ISSN1548-7709, USA.

[12] Beulah Kurian, Gregor Von Laszewki "Reputation Based Grid Resource Selection.

[13] Vectors *http://java.sun.com/j2se/1.4.2/docs/api/java/util/Vector.html.*