A New Sensitive and Robust Grid Reputation System Based on Rating of Recommenders

Yongrui Cui†, Mingchu Li†, Yizhi Ren†‡, Kouichi Sakurai‡

†Information Security and Grid Technology Laboratories
School of Software, Dalian University of Technology Dalian, 116621, P.R.China
cyr811127@gmail.com

‡Dept. of Computer Science and Communication Engineering, Kyushu University Hakozaki, Fukuoka
812-81, Japan
sakurai@csce.kyushu-u.ac.jp

Abstract This paper proposes a sensitive and robust reputation system for grid environments. A punishment factor is introduced to express the subjective opinion of evaluators and destroy the reputation of bad performers rapidly, which improves the sensitivity of the reputation system. By evaluating the reputation of recommenders, our solution filters out dishonest recommendations during the process of trust evaluation, thus making the reputation system more robust against vicious attacks such as fake transaction attacks and badmouthing attacks by dishonest recommenders. Moreover, the introduction of inter-organizational trust enables the proposed reputation system to be more suitable for grid environments that span multiple autonomous organizations.

1 Introduction

1.1 Background and Motivation

During the past several decades, various reputation systems are proposed and applied in distributed environments such as E-commerce platforms, P2P systems and Grid environment. Most of them are designed to protect the interests of consumers by evaluating reputation and performance of resource providers. However, transaction and cooperation are both bilateral relationships. Service consumers can also do harm to service providers by refusing to pay full price or leaving dishonest feedback ratings. Therefore, it is also necessary to monitor and punish the malicious service consumers. Therefore, besides the behaviors of service providers, a reputation system should also trace and evaluate service consumers' behaviors both to weed out misbehavior and to encourage voluntary feedback provision. A possible way is to build reputations for consumers according to the honesty of their past trading behaviors and recommendations, making the whole grid population more cooperative. On the other hand, a grid reputation system should also have essential features such as ***Accuracy and Sensitivity***.

1.2 Related Works

Though lots of reputation systems are proposed for online business and P2P environments, the research on grid reputation system is still in its infancy stage [1]. GridEigenTrust [2] is a famous grid reputation system which extends the EigenTrust [3] model to allow its usage in grid environment. However, this model becomes vulnerable to malicious feedback ratings from dishonest raters. Many reputation systems are proposed to overcome this problem, Florian Kerschbaum *et al* [4] propose the PathTrust model, which tolerates and counteracts the misbehavior of raters effectively by calculating reputation values within a directed graph consists of grid nodes and their direct trust relationships. Some papers [5][6] develop different filtering method to filter out unfairly and dishonest recommendations. In [7], EntityTrust model is proposed to combat malicious feedbacks based on the estimation of an entity's feedback credibility using the combination of multi-targets and special target evaluation algorithm.

1.3 Challenge Issues

Some key challenge issues about reputation system in grid environment are needed to be solved as follows: (1) How to describe the subjective opinion of the evaluators to express the trust relationships more accurately; (2) How to depict the change trend of the trust relationship to make the trust evaluation more sensitively; (3) How to resist attacks from dishonest recommenders to make the reputation system more robust.

1.4 Our Contribution

To address the issues above, we propose a new grid reputation system. The contributions of our work are mainly as follows: First, we propose an evaluating mechanism for reputation of service consumers to protect the interests of service providers and restrain dishonest feedback ratings from malicious consumers. Moreover, the evaluation of consumers' reputation provides an incentive mechanism to encourage consumers to give feedbacks in a more active way. Secondly, an adaptive model based on the global experience of consumers and the rational reference of previous trust value is proposed to express the reputation fluctuation more sensitively. Thirdly, we enhance the robustness against collusion attacks especially fake transaction and badmouthing attacks by pruning the trust overlay graph based on the reputation of recommenders. Finally, the inter-organizational trust is combined with direct and recommended trust, making our reputation system more suitable for grid environments.

1.5 Comparing Our New Results to Related Works

Differing from the abovementioned studies, we propose the concept "recommender reputation", and combine evaluation of consumers' reputation with global property of trust overlay networks to weed out misbehaviors of consumers and therefore protect the interests of providers and make the reputation system more robust.

2 Reputation evaluation

Let $SP\_set_{sc,sn} = \left\{ sp_{sc,i,sn} \mid 1 \le i \le n_{sc} \right\}$ denote the set of providers of service *sn* which interacts with service consumer *sc*, where n_{sc} is the total number of $sp_{sc,i,sn}$. The following subsections will describe the reputation evaluation algorithm in detail.

2.1 Direct trust evaluation

Direct trust is the accumulated experience between entities through direct interactions. It is one of the most intuitive expressions about the trust relations between entities and the most important foundation of personalized reputation evaluation. Mathematically, the current feedback appears as follows:

$$pfb_{sc,sp,sn}^{q} \in [0,1] \qquad (1)$$

where *sc* is the service consumer which consume the service *sn* provided by *sp*, and *q* is the set of contexts for evaluating the performance of service.

To maintain orderly cooperation, let $DT_{sc,sp,sn}$ denote the direct trust between consumer *sc* and provider *sp* when consuming service *sn* to express the subjective perception of evaluator. We denote $\overline{DT_{sc,sn}} = \sum_{i=1}^{n_{sc}} DT_{sc,i,sn} \Big/ n_{sc}$ as the mean value of direct trusts between *sc* and the providers of service *sn*, then an punishment factor $imf_{i,j,sn}$ is denoted as:

$$imf_{sc,sp,sn} = \frac{\sum_{DT_{sc,i.sn} \le \overline{DT_{sc,sn}}} DT_{sc,i,sn}}{\sum_{i=1}^{n_{sc}} DT_{sc,i,sn}} \qquad (2)$$

Then the feedback can be amended as follows:

$$fb_{sc,sp,sn}^{q} = \begin{cases} imf_{sc,sp,sn} \cdot pfb_{sc,sp,sn}^{q} & \text{if} \quad pfb_{sc,sp,sn}^{q} < \overline{DT_{sc,sn}} \\ pfb_{sc,sp,sn}^{q} & \text{if} \quad pfb_{sc,sp,sn}^{q} \ge \overline{DT_{sc,sn}} \end{cases} \qquad (3)$$

The introduction of $imf_{sc,sp,sn}$ makes the bad performers receive lower feedbacks when their performance is worse than most of their competitors.

We update the direct trust value using a heuristic update rule based on idea of Avila-Rosas *et al* [19] as follows:

$$DT_t = DT_{t-1} + \alpha\left(DT_{t-1}, fb_t\right) \cdot \left(fb_t - DT_{t-1} \right) \qquad (4)$$

Note that we simplify the expression of *DT* to make the formula more readable. Function α is a discounting factor which indicates how fast the trust value changes and how this affects the memory of the system. It depends on the similarity between the expectation value formed by accumulated experiences and the last feedbacks. The value of $\alpha\left(DT_0, fb_1\right)$ is initialized to 0.5 to imply that the evaluator will give the first feedback carefully and will learn to give accurate feedback through accumulated experience. The similarity is described by a similarity function $\beta\left(DT_{t-1}, fb_t\right) \in (0,1)$ which is denoted as:

$$\beta\left(DT_{t-1}, fb_t\right) = 1 - e^{-10 \cdot SR} \qquad (5)$$

where *SR* is a similarity rate related with the similarity between current feedback and past experience:

$$SR = \left| \frac{\left(fb_t - DT_{t-1} \right) + \left(fb_t - fb_{t-1} \right)}{2} \right| \qquad (6)$$

Then, the function α is updated as:

$$\alpha\left(DT_{t-1}, fb_t\right) = \frac{\alpha\left(DT_{t-2}, fb_{t-1}\right) + \beta\left(DT_{t-1}, fb_t\right)}{\lambda}, t \geq 2 \qquad (7)$$

where λ is the slope factor for adjusting the change rate of α, which is denoted as follows:

$$\begin{cases} \lambda = 2 & \text{if } \mathrm{DT}_{t-1} \geq fb_t \\ \lambda = \lambda_m, \ \lambda_m \geq 2 & \text{if } \mathrm{DT}_{t-1} < fb_t \end{cases} \qquad (8)$$

We can see obviously that $DT_0 = fb_0$, and the direct trust relation between two participants can be built through the algorithm above.

2.2 Recommended trust evaluation

We regard direct trust between two participants as the recommended trust provided by one participant to another. The recommendation will be performed automatically. We build a directed weighted graph G_{DT} consisting of all nodes (as vertices) and direct trust relations between them (as edges), and define the weight of the path <*i*,*k*,*j*> from *i* to *j* via *k* as $W(i,k,j,sn) = DT(i,k,sn) \cdot DT(k,j,sn)$. Since $DT(i,j,sn) < 1$ (and therefore the weight of each path is degressive), the heaviest weighted path $w_{\max}(i,j,sn)$ can be calculated using a derivative *Dijkstra* algorithm which amends the calculation rule by calculating the product of all edges within the path. We build a new graph G_{RT} ($G_{RT} = G_{DT} - DT\left(sc, sp, sn\right)$) which is the sub-graph of G_{DT}. Then we regard $w_{max}\left(sc, sp, sn\right)$ on G_{RT} as the best recommendation from global participants, namely $RT\left(sc, sp, sn\right) = w_{max}\left(sc, sp, sn\right)$.

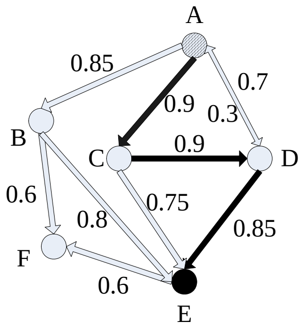

Fig. 1 Recommendation graph

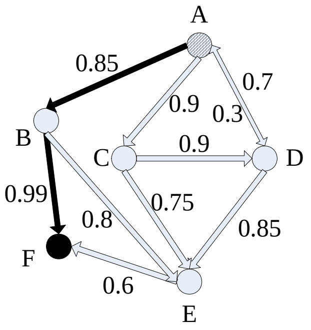

Fig. 2 Recommendation graph with flatter attackers

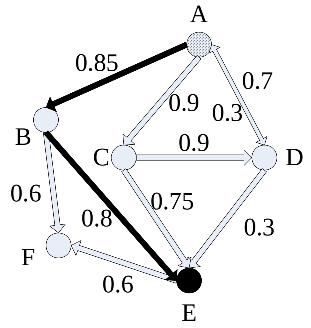

Fig. 3 Recommendation graph with badmouthing attackers

Note that we select the best recommendation automatically based on the product of direct trust values, the accuracy of the recommendation depends on the accuracy of the direct trust evaluation among recommenders on the recommendation train. A good performer does not necessarily be a good recommender. Malicious recommenders can distort the recommendation by building fake direct trust relations. For example, assume that node *B* and *F* in Figure 1 are complicit flatter attackers, they increase the direct trust value from 0.8 to 0.99 by leaving high feedback ratings repeatedly, as a result which is shown in Figure 2, the best recommended trust from *A* to *F* can be calculated as

$$RT\left(A,F,sn\right)=W\left(A,B,F,sn\right)=0.8415.$$

Obviously, for consumer *A*, provider *F* becomes more attractive than *E*. On the other hand, as shown in Figure 3, assume that node *D* slanders E and decreases the direct trust value from 0.9 to 0.3 by leaving low feedback ratings repeatedly, the best recommended trust from *A* to *E* can be calculated as

$$RT\left(A,E,sn\right)=W\left(A,B,E,sn\right)=0.68.$$

Although another path was found to calculate the best recommendation, the value of the best recommendation decreased because of the breakage of the original honest recommendation chain.

In our trust model, we solve these problems by evaluating the recommendation behavior of recommenders. In particular, recommenders (consumers) are ranked in the form of reputation value according to accuracy of their recommendations. We call this reputation as “recommender reputation” which is expressed by a real number between 0 and 1. In order to encourage recommenders to provide accurate recommendation, we calculate recommender reputation based on the comparison of the current feedback from the recommender and the reputation of service provider being evaluated. The reputation of a recommender will be evaluated whenever his recommendation is referenced by a service consumer to evaluate the reputation of a service provider.

Let $R_{sc,sp,sn,t}$ be the reputation value of service provider *sp* when providing service *sn* to consumer *sc* at time *t*. Let $RoR_{re,t}$ denote the recommender reputation of *re* at time *t* and $sfr_{re,t}$ denote the similarity between feedback left by *re* for a provider *sp* and the reputation of *sp* at time *t*. Then

$$sfr_{re,t}=SimF\left(DT_{re,sp,sn,t},R_{sc,sp,sn,t}\right),$$

where *SimF* is a similarity function which is denoted as:

$$SimF\left(m,n\right)=1-e^{-6\bullet\left|{}^{m-n}\!/_{m+n}\right|}\qquad(9)$$

Similar to the direct trust model in section 3.1, we denote that

$$RoR_{re,t}=RoR_{re,t-1}+\alpha_r\left(RoR_{re,t-1},sfr_{re,t}\right)\bullet\left(sfr_{re,t}-RoR_{re,t-1}\right)\qquad(10)$$

where function α_r is a discounting factor which indicates how fast the reputation value changes after a recommender gave the recommendation and how this affects the memory of the system, which is updated as:

$$\alpha_r\left(RoR_{re,t-1},sfr_{re,t}\right)=\frac{\alpha_r\left(RoR_{re,t-2},sfr_{re,t-1}\right)+\beta_r\left(RoR_{re,t-1},sfr_{re,t}\right)}{2}\qquad(11)$$

where

$$\beta_r\left(RoR_{re,t-1},sfr_{re,t}\right)=1-e^{-10\bullet\left|sfr_{re,t}-\frac{RoR_{re,t-1}+sfr_{re,t}}{2}\right|}\qquad(12)$$

The value of $\alpha_r\left(RoR_{re,0},sfr_{re,1}\right)$ is initialized to 0.5.

In our reputation system, the dishonest recommendations will be filtered out by the low reputation value of its recommender. To realize this aim, first we define the weight of each vertex *v* as RoR_v and the weight of path <*i*,*k*,*j*> is revised as the product of the weight of vertices and edges within the path, which is denoted as

$$W'(i,k,j,sn)=DT(i,k,sn)\cdot RoR_k\cdot DT(k,j,sn)\qquad.$$

Then we prune G_{RT} by cutting edges starting from the dishonest recommender whose recommender reputation is lower than a threshold. The prune will be processed repeatedly until there is no dishonest recommender within the recommendation path. For example, let the threshold be 0.8, since recommender *B* in Figure 2 provides dishonest recommendations and its recommender reputation value is lower than threshold, edge $\overrightarrow{BE}$ and $\overrightarrow{BF}$ will be cut. The pruning result is shown in Figure 4. The recommended trust value from *A* to *F* becomes 0.4049, reflecting the real performance of *F*. On the other hand, since recommender *D* in Figure 3 slanders participant *E* and its recommender reputation value is lower than threshold, edge $\overrightarrow{DE}$ will be cut as shown in Figure 5. Then the recommended trust value from *A* to *E* becomes 0.68. Note that the pruning algorithm does not recover the original recommended trust value. However, we argue that it at least prevents *D* from providing bad recommendations. Moreover, reputation evaluation itself is an incentive mechanism, and the low reputation will discourage the dishonest behaviors of *D*.

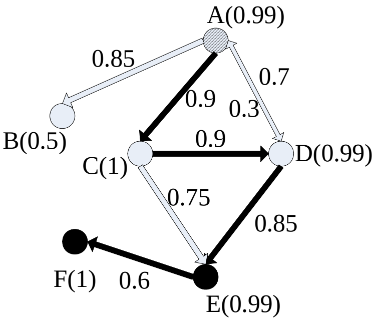

Fig. 4 Pruning of recommendation graph with flatter attackers

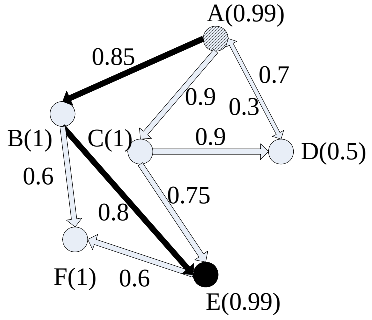

Fig. 5 Pruning of Recommendation graph with badmouthing attackers

2.3 Inter-organizational trust evaluation

Let $IT(O_i, O_j, sn)$ be the initial trust evaluation of O_i in O_j about service sn if they had initial interactions before. Let $LT(O_i, O_j, sn)$ be the current trust evaluation, then the trust relations between O_i and O_j can be represented as a linear combination of $IT(O_i, O_j, sn)$ and $LT(O_i, O_j, sn)$. We evaluate $LT(O_i, O_j, sn)$ by returning the average of feedbacks left by the nodes within O_i for O_j. Let $E_T(O_i, O_j, sn)$ be the collection of nodes in O_i which have interacted with nodes in possession of service sn in O_j and $E_R(O_i, O_j, m, sn)$ be the collection of nodes in O_j which have interacted with node m in O_i. Then

$$LT(O_i,O_j,sn) = \frac{\sum_{et\in E_T} DT(et, E_R(O_i,O_j,et,sn),sn)}{|E_T|\cdot|E_R|} \tag{13}$$

Then, the trust evaluation O_i leaves for O_j can be calculated as:

$$ODT(O_i,O_j,sn) = \frac{(\alpha_o \cdot IT(O_i,O_j,sn) + \beta_o \cdot LT(O_i,O_j,sn))}{\alpha_o+\beta_o} \tag{14}$$

where α_o and β_o are constant weights and $0 \le \alpha_o, \beta_o < 1$.

2.4 Reputation evaluation

The reputation evaluation performed by node *sc* for *sp* is calculated as follows:

$$\begin{aligned} &R(sc,sp,sn) = \beta \cdot RT(sc,sp,sn)) \\ &+ODT(O_{sc},O_{sp},sn)\cdot(\alpha\cdot DT(sc,sp,sn) \end{aligned} \tag{15}$$

where $\alpha \ge 0$, $\beta \ge 0$, and $\alpha+\beta=1$. The value of α and β depends on the specific application environment of the reputation system, but under normal circumstances should meet $\alpha > \beta$.

3 Simulation

3.1 Simulation Setup

In our simulations, we use 1000 participants to simulate a service grid environment, where each participant plays two different roles: service provider and service consumer. The participants are divided into 10 groups to simulate the autonomous organizations where 30 services are distributed uniformly and each participant provides 3 services, i.e. there are 100 providers for each service in the simulated grid. In each round, a service consumer is uniformly chosen among all participants and a requested service is uniformly chosen among all services. Service providers are selected probabilistically according to their reputation values, which enables a newcomer has the opportunity to be selected. After each transaction, the consumer will give feedback for the service provider.

The default coefficients are specified as: $\alpha_0 = 0.2$; $\beta_0 = 0.8$; $\alpha = 0.7$; $\beta = 0.3$; $\lambda_m = 4$. Moreover, we assume that there have been some initial feedbacks to simulate a well-functioning grid environment.

3.2 Resistance against badmouthing attacks

Badmouthing attacks are simulated to see whether the dishonest recommendation can be restrained so as to prevent the attackers from earning more profit than honest providers. We assume that all of the participants provide 99% good services. The proportion of attackers is increased from 10% to 50%, and each attacker gives 10 negative feedbacks (0.1) for another random-chosen attacker per real transaction, i.e. the attackers slander each other to destroy reputations. Figure 6 shows the comparison of average profit obtained by cheaters and honest participants applying EigenTrust, PathTrust and our proposed algorithm respectively. It is not difficult to see that the profit of the attackers did not decreased obviously under slander when our model and PathTrust are applied, however, EigenTrust can not prevent badmouthing attacks efficiently.

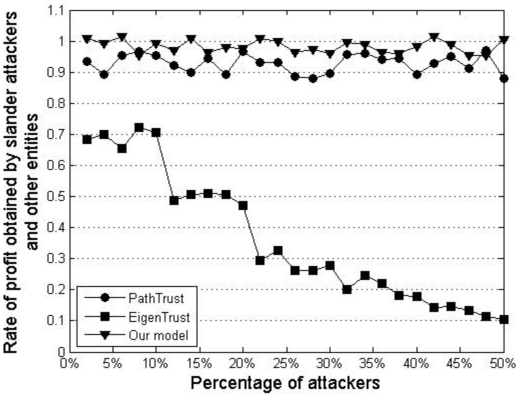

Fig. 6 Resistance to badmouthing attacks

4 Conclusions

We propose a novel grid reputation system which enables accurate, sensitive and robust reputation evaluation in grid environments through the introduction of an impact factor and the reputation evaluation of recommenders.

Acknowledgement

The first author of this research is supported by Nature Science Foundation of China under grant No.: 60673046, 90715037, University Doctor Subject Fund of Education ministry of China under grant No.: 200801410028, National 973 Plan of China under grant No.: 2007CB714205 and Natural Science Foundation Project of Chongqing, CSTC under grant No.: 2007BA2024

References

[1] G.C. Silaghi, A.E. Arenas, L.M. Silva. Reputation-based trust management systems and their applicability to grids, Technical report, TR-0064, Institutes on Knowledge and Data Management & System Architecture, CoreGRID - Network of Excellence, 2007. http://www.coregrid.net/mambo/images/stories/TechnicalReports/tr-0064.pdf.

[2] G.V. Laszewski, B.K. Alunkal, I. Veljkovic. Towards reputable grids, Scalable Computing: Practice and Experience, 6 (3) (2005) 95-106.

[3] S.D. Kamvar, M.T. Schlosser, H. Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks, in: Proceedings of the 12th International Conference on World Wide Web, Budapest, HUNGARY, 2003, pp. 640-651.

[4] F. Kerschbaum, J. Haller, Y. Karabulut, P. Robinson. Pathtrust: A trust-based reputation service for virtual organization formation, in: Proceedings of 4th International Conference on Trust Management, Pisa, Tuscany, Italy, 2006, pp. 193-205.

[5] C. Dellarocas. Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior. In: proceedings of 2nd ACM Conference on electronic commerce, Minneapolis, MN, October 17-20, 2000.

[6] A. Whitby, A. Josang, J. Indulska. Filtering out unfair ratings in Bayesian reputation systems. The Icfain Journal of Management Research, 4 (2) (2005) 48-64.

[7] Y.D. Mei, X.S. Dong, Z.H. Tian, S.Y. Guan, H. Chen. EntityTrust: Feedback credibility-based global reputation mechanism in cooperative computing system. In: proceedings of 12th International Conference on Computer Supported Cooperative Work in Design (CSCWD 2008), 2008, pp. 797-802.