DynamicTrust: The Trust Development in Peer-to-Peer Environments

Yan Wang
Department of Computing
Macquarie University
Sydney, NSW 2109
Australia
yanwang@ics.mq.edu.au

Vijay Varadharajan
Department of Computing
Macquarie University
Sydney, NSW 2109
Australia
vijay@ics.mq.edu.au

Abstract

In peer-to-peer (P2P) environments, trust is a very important issue when transactions/interactions occur between peers. In general, the trust evaluation on transactions/interactions relies on the recommendations from other peers, which may be inaccurate. This paper presents DynamicTrust*, a P2P trust evaluation system. It is based on our peer trust evaluation model, which measures the credibility of peers' recommendations, and thus filters noise in responses and obtains more accurate and objective trust values.*

1 Introduction

In peer-to-peer (P2P) environments, the trust evaluation on a peer relies on the recommendations of other peers, which may be unknown either. This may result in inaccurate trust evaluations.

In [1], the authors proposed $XRep$: a reputation-based approach for evaluating the reputation of peers through distributed polling algorithm before downloading any information. EigenTrust [2] collects the *local trust values* of all peers to calculate the *global trust value* of a given peer. In [3], the authors proposed a voting reputation system that collects responses from other peers on a given peer. The final reputation value is calculated combining the values returned by responding peers and the requesting peer's experience with the target peer. This is more reasonable than the model in [1]. However, this work and the work in [2] don't explicitly distinguish transaction reputation and recommendation reputation. This may cause severe bias for reputation evaluation as a peer with good transaction reputation may have a bad recommendation reputation especially when recommending competitors.

A lying peer's evaluation is incorrect most of the time, which may be a positive exaggeration or a negative exaggeration. Therefore, the process to identify a liar requires a series of interactions that occur in different rounds or periods. [4] presented a method to measure the recommendation trust. But the method of evaluating aggregated trust values can be further improved.

In this paper, we present *DynamicTrust*, a peer trust evaluation system, which is based on our peer trust evaluation models. In our approach, posterior to some interactions with a target peer which is unknown before, the end-peer gives trust evaluations over the target peer. Meanwhile, other peers' evaluations can be collected to measure their recommendation trust (credibility) so as to filter noise in recommendations and obtain more objective aggregated trust values. A method for estimating initial credibility is also studied. Additionally, a set of experiments has been conducted to study the properties of the proposed models.

2 Trust Evaluation

In the following context, we study the trust evaluation method with the following assumptions: 1) there are more honest peers than lying peers, and 2) the requesting peer is honest.

2.1 Aggregated Rating

If P_r has a number of interactions with target peer P_x during period $[t_{start}, t_{end}]$, it can collect the trust values of P_x given by other peers so as to aggregate these values with its own experience.

Let $\tilde{T}_{i\to x}^{(k)}$ denote the trust value on T_x given by P_i in round k at time t_k, the *aggregated trust value* by P_r can be calculated as follows:

$$\tilde{T}_{r\to x}^{(k)} = w_r^{(k)} \cdot T_{r\to x}^{(k)} + (1 - w_r^{(k)}) \cdot \bar{T}_x^{(k)} \qquad (1)$$

where

- $\bar{T}_x^{(k)} = \frac{1}{m}\sum_{i=1}^{m} T_{i\to x}^{(k)}$, m is the number of responding peers;

- $w_r^{(k)}$ is the weight to P_r's experience in round k at t_k and $w_r^{(k-1)} < w_r^{(k)}$ $(t_{k-1} < t_k)$.

Formula (2) controls the changes of w_r by using two parameters: α $(0.5 < \alpha < 1)$ and β $(\beta \in \{1,\ 2,\ 3, \ldots\})$.

$$w_r^{(k)} = 1 - \alpha^{k^{\frac{1}{\beta}}},\ 0.5 < \alpha < 1\ and\ \beta \in \{1,\ 2,\ 3, \ldots\} \quad (2)$$

Typically, $w_r^{(1)}$, the weight of $T_{r\to x}^{(1)}$, is less than 0.5 (e.g. 0.3) as it weights the first interaction between P_r and P_x during $[t_{start}, t_{end}]$. So the mean of trust values from other peers should be weighted more (e.g. 0.7). k corresponds to the kth *round* in period t_k. Given the same α and β, the larger k is, the larger $w_r^{(k)}$ is. This means that with more and more interactions, trust values of P_x given by P_r should be weighted more. Other peers' evaluations become less and less important. Given the same α, the increment of $w_r^{(k)}$ is subject to β. The larger β is, the more slowly the $w_r^{(k)}$ increases.

2.2 Evaluation and Noise

With more and more interactions with peer P_x, on one hand, P_r obtains more and more *direct* interaction trust evaluations over P_x and aggregate them with other peers' trust evaluations and thus obtain the new objective evaluations from P_r's perspective. On the other hand, based on the aggregated trust values, it is possible for P_r to identify a peer with noise whose evaluations are deviated from the "main stream" peers. Thus the credibility of a responding peer can be estimated based on the recommendation deviations in a series of rounds. In the following context, we use '*credibility*' to represent the measurement of recommendation trust.

In our model, we classify four kinds of evaluations as follows: 1) *honest evaluation* 2) *positive exaggeration* 3) *negative exaggeration*, and 4) *random exaggeration*. In our model, we don't explicitly identify 'malicious peers' when measuring credibilities. Any evaluation deviation is identified as the noise.

Definition 1: Assume $T_{i\to x}^{(k)}$ represents the trust value given by P_i in round k at t_k over P_x and $\tilde{T}_x^{(k)}$ represents the aggregated trust value. *P_i's evaluation deviation in round k* is

$$d_{i\to x}^{(k)} = |T_{i\to x}^{(k)} - \tilde{T}_x^{(k)}| \quad (3)$$

2.3 Credibility Evaluation

The credibility value (in $[0,\ 1]$) is in inverse proportion to the deviation (in $[0,\ 1]$). Meanwhile, the new credibility results from the deviation of the current round and the peer's previous credibilities (history).

Definition 2: Given the credibility $c_i^{(k-1)}$ for peer P_i in last round $(k-1)$, the deviation $d_i^{(k)}$ in the current round k, *the new credibility* $c_i^{(k)}$ can be calculated as follows:

$$c_i^{(k)} = c_i^{(k-1)} + \theta_i^{(k)} \cdot (1 - {d_i^{(k)}}^{\frac{1}{s}} - c_i^{(k-1)}) \quad (4)$$

where $\theta_i^{(k)}$ is an *impact factor*

$$\theta_i^{(k)} = \frac{e^{|1 - {d_i^{(k)}}^{\frac{1}{s}} - c_i^{(k-1)}|} - 1}{e + 1} \quad (5)$$

$s = 1, 2, 3, \ldots$ is a *strictness factor* which is used to control the curve. The higher s is, the stricter the evaluation is.

3 Further Discussion

3.1 Initial Credibility Assignment

In the above method, an initial credibility value $c_i^{(0)}$ should be given so that new credibility values (i.e. $c_i^{(1)},\ c_i^{(2)},\ \ldots$) can be calculated in the subsequent rounds. However, in the beginning, P_r may not know the credibility of each responding peer P_i especially when P_r is a new peer. In this case, P_r can assign a value to each peer's credibility, say, $c^{(0)} = 0.5$. This value may not reflect the true credibility.

Alternatively, if P_r knows the interaction trust status of several (e.g. 3) peers (referred to as *testing peers*), it can enquiry other peers their evaluations over unknown peer P_x and testing peers. With the replies on the testing peers, the initial credibility of a responding peer can be calculated. This is more accurate than simply assigning an initial value as 0.5.

3.2 Aggregated Trust Value

With c_i, more accurate trust values can be obtained.

Definition 3: Suppose peer P_r has collected the trust evaluations over peer P_x from a set of intermediate peers $IP = \{P_1,\ P_2,\ \ldots,\ P_m\}$ in round k. $c_i^{(k-1)}$ is the credibility of peer P_i obtained in round $k-1$. Then the trust value of peer P_x in round k is:

$$\bar{T}_x^{(k)} = \frac{1}{m}\sum_{i=1}^{m} c_i^{(k-1)} \cdot T_{i\to x}^{(k)} \quad (6)$$

Herein the definition of $\bar{T}_x^{(k)}$ in formula (1) has been rectified by considering the credibility of each responding peer.

Thus according to formulas (1) and (6), more accurate *aggregated trust values* $\tilde{T}_{r\to x}^{(k)}$ can be obtained:

$$\tilde{T}_{r\to x}^{(k)} = w_r^{(k)} \cdot T_{r\to x}^{(k)} + \frac{1 - w_r^{(k)}}{m} \cdot \sum_{i=1}^{m} (c_i^{(k-1)} \cdot T_{i\to x}^{(k)}) \quad (7)$$

According to the above method, after a series of interactions and recommendations, the credibility of each responding peer can be calculated. At a certain round, the requesting peer can apply a threshold to filter responding peers with low credibility. Hereby these peers are blacklisted.

Definition 4: Suppose peer P_r has collected the trust evaluations over peer P_x from a set of intermediate peers $IP^{'} = \{P_1,\ P_2,\ \ldots,\ P_{m'}\}$ in round k. $c_i^{(k-1)}$ is the credibility of peer P_i obtained in round $(k-1)$. λ is the credibility threshold. Then the *trust value of peer P_x in round k* is:

$$\tilde{T}_{r\to x}^{(k)} = w_r^{(k)} \cdot T_{r\to x}^{(k)} + \frac{1 - w_r^{(k)}}{m^{'}} \cdot \sum_{i=1}^{m^{'}} (c_i^{(k-1)} \cdot T_{i\to x}^{(k)}) \quad (8)$$

where

$$P_i \in IP^{'} = \{P_j | c_j^{(k-1)} \geq \lambda\},\ m^{'} = |IP^{'}|, \text{ and}$$

$$\text{blacklist } BL = \{P_j | c_j^{(k-1)} < \lambda\}$$

However, formula (8) can be further improved.

Definition 5: With a set of trustworthy responding peers in $IP^{'} = \{P_1,\ P_2,\ \ldots,\ P_{m'}\}$, their recommended trust values $\{T_{i\to x}^{(k)}\}$ and credibility values $\{c_i^{(k-1)}\}$, the *aggregated trust value of peer P_x in round k* is:

$$\tilde{T}_{r\to x}^{(k)} = w_r^{(k)} \cdot T_{r\to x}^{(k)} + \frac{1 - w_r^{(k)}}{m^{'}} \cdot \sum_{i=1}^{m^{'}} (w_i^{(k-1)} \cdot T_{i\to x}^{(k)}) \quad (9)$$

where

$$w_i^{(k-1)} = \frac{c_i^{(k-1)}}{\sum_{i=1}^{m^{'}} c_i^{(k-1)}} \quad (10)$$

Here, we rectify formula (8) by replacing $c_i^{(k-1)}$ with $w_i^{(k-1)}$. As $c_i^{(k-1)} \leq 1$ (e.g. 0.8, 0.9), $\frac{1}{m^{'}} \cdot \sum_{i=1}^{m^{'}} (c_i^{(k-1)} \cdot T_{i\to x}^{(k)})$ leads to a lower trust value. However $\frac{1}{m^{'}} \cdot \sum_{i=1}^{m^{'}} (w_i^{(k-1)} \cdot T_{i\to x}^{(k)})$ can rectify the deviation. The performance differences are compared in our experiments illustrated in sections 4.1 and 4.2.

4 Experiments

4.1 Experiment 1

In this experiment, we study the trust evaluation over peer P_x, whose true trust value tt is 0.65, by collecting the evaluations from a set of peers where 50% peers give negatively exaggerating evaluations.

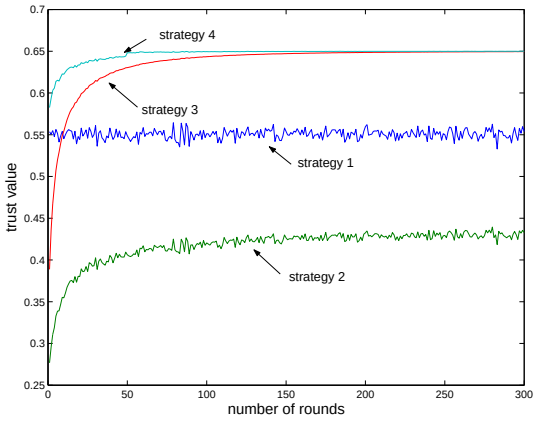

Figure 1. Experiment 1 50% Negatively Exaggerating Peers ($s = 2,\ tt = 0.65$)

In this experiment, we set $s = 2$, $\alpha = 0.7$, $\beta = 2$. The reason that we consider only class 1 (honest) and class 3 (negative exaggeration) peers is that this is an extremely malicious environment. If both classes 2, 3 and 4 peers are considered, their deviations may counteract each other.
We compare four evaluation strategies in this experiment.

Strategy 1 : The final trust value obtained in each round is the mean of all evaluations.

Strategy 2 : This strategy aims to rectify strategy 1. The credibility of each responding peer is taken into account in the trust evaluation even if the peer's credibility is very low (see formula (6)).

Strategy 3 : This strategy applies the weight w_r of the responding peer P_r via formula (7).

Strategy 4 : This strategy improves strategy 3 by ignoring low credibility peers. The threshold is set to be $\lambda = 0.6$ from the $50th$ rounds onwards. Meanwhile, $c_i^{(k-1)}$ is replaced by $w_i^{(k-1)}$ (formula (9)).

In this experiment, there are 3 classes among negatively exaggerating peers. Their mean deviations are 0.1, 0.2 and 0.3 respectively. In contrast, the deviation of a honest peer is approximately 0.07. In Figure 1, it is easy to see that strategies 1 and 2 lead to low trust values where strategy 2 is even less accurate than strategy 1 as each peer's credibility is less than 1.0 resulting in $c_i * T_i < T_i$. In strategy 3, the trust values become more and more accurate as the requesting peer's experience becomes more important. In strategy 4, the trust values can be improved earlier as c_i is replaced by w_i and low credibility peers are ignored.

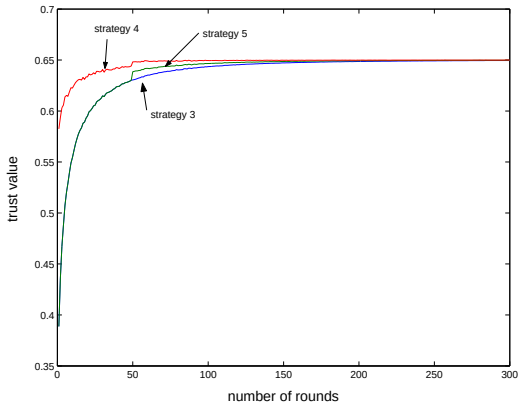

Figure 2. Experiment 2 50% Negatively Exaggerating Peers ($s = 2,\ tt = 0.65$)

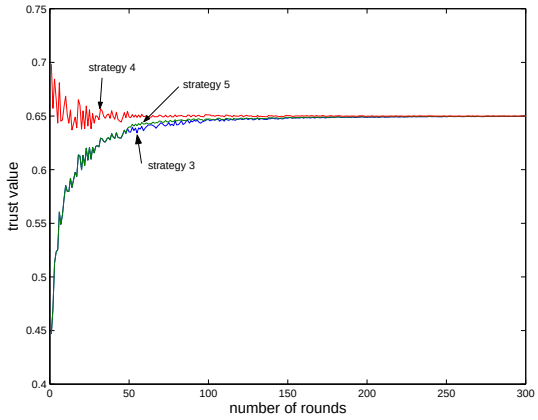

Figure 3. Experiment 2 50% Positively Exaggerating Peers ($s = 2,\ tt = 0.65$)

4.2 Experiment 2

In this experiment we compare strategy 4 with strategy 5, which was the best strategy proposed in our previous work in [4].

Strategy 5 : This strategy improves strategy 3 by ignoring low credibility peers, where the threshold is set to be $\lambda = 0.6$ from the $50th$ rounds onwards. Like strategy 3, this strategy also applies the weight w_r of the responding peer P_r via formula (7).

The results with 50% negatively exaggerating peer, and 50% randomly exaggerating peers are plotted in Figures 2 and 3. It is easy to see in all cases, strategy 5 slightly improves strategy 3. But it is inferior to strategy 4 when $k < 100$.

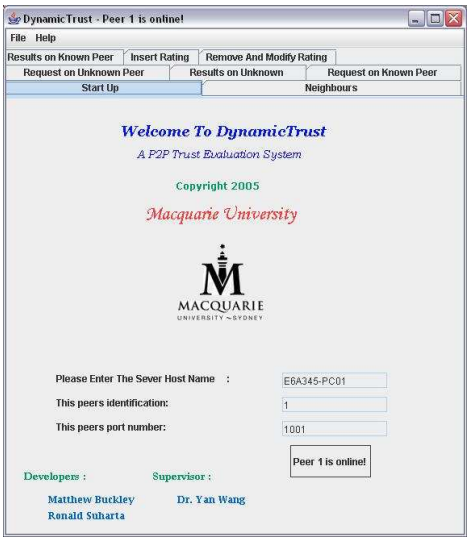

Figure 4. DynamicTrust UI

5 Conclusions

We have implemented *DynamicTrust* - a prototype system based on Java and XML incorporating the proposed models. Our approach takes into account the credibility of responding peers, which is measured via a series of transactions and recommendations. Moreover, the final trust value results from both the requesting peer's evaluation and other peer's evaluations while the former one becomes more and more important. The result is more objective than the direct transaction trust values which may be intuitive.

References

[1] E. Damiani, S. D. C. di Vimercati, S. Paraboschi, P. Samarati, and F. Violante. A reputation based approach for choosing reliable resources in peertopeer networks. In *Proceedings of ACM CCS'02*, pages 207–216, Washington DC, USA, November 2002.

[2] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. In *Proceedings of the 12th International WWW Conference*, Budapest, Hungary, May 2003.

[3] S. Marti and H. Garcia-Molina. Limited reputation sharing in p2p systems. In *Proceedings of ACM EC'04*, pages 91–101, New York, USA, May 2004.

[4] Y. Wang and V. Varadharajan. $Trust^2$: Developing trust in peer-to-peer environments. In *Proceedings of 2005 IEEE International Conference on Services Computing (SCC 2005)*, pages 24–31, Orlando, Florida, USA, July 12-15 2005.