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 $[t_{\text{start}}, t_{\text{end}}]$, it can collect the trust values of $P_x$ given by other peers so as to aggregate these values with its own experience.

Let $T_{x,k}$ denote the trust value on $P_x$ given by $P_i$ in round $k$ at time $t_k$, the aggregated trust value by $P_r$ can be calculated as follows:

$$T^{(k)}_{x,z} = w^{(k)}_r \cdot T^{(k)}_{x,z} + (1 - w^{(k)}_r) \cdot T^{(k)}_x$$  \hspace{1cm} (1)

where
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:

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

$$\theta_i^{(k)} = \frac{e^{[\theta_i^{(1)} - c_i^{(k-1)}] - 1}}{e + 1}$$

where $\theta_i^{(1)}$ is an impact factor

$s = 1, 2, 3, \ldots$ 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, $P_i$ may not know the credibility of each responding peer $P_j$ especially when $P_i$ is a new peer. In this case, $P_i$ can assign a value to each peer’s credibility, say, $c_i^{(0)} = 0.5$. This value may not reflect the true credibility.

Alternatively, if $P_i$ knows the interaction trust status of several (e.g. 3) peers (referred to as testing peers), it can enquire other peers’ 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 of 0.5.

3.2 Aggregated Trust Value

With $c_i$, more accurate trust values can be obtained.

**Definition 3:** Suppose peer $P_i$ 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:

$$T_i^{(k)} = \frac{1}{m} \sum_{i=1}^{m} c_i^{(k-1)} \cdot t_{i-x}^{(k)}$$

Herein the definition of $t_{i-x}^{(k)}$ 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 $T_{1,r}^{(k)}$ can be obtained:

$$T_{1,r}^{(k)} = w_{r}^{(k)} T_{1,r}^{(k-1)} + 1 - w_{r}^{(k)} \sum_{i=1}^{m} c_{i}^{(k-1)} \cdot T_{1,r}^{(k-1)}$$ (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 $P_{r}$ from a set of intermediate peers $IP' = \{P_{1}, P_{2}, \ldots, P_{m'}\}$ in round $k$. $c_{j}^{(k-1)}$ is the credibility of peer $P_{j}$ obtained in round $(k - 1)$. $\lambda$ is the credibility threshold. Then the trust value of peer $P_{r}$ in round $k$ is:

$$T_{r}^{(k)} = w_{r}^{(k)} T_{r}^{(k-1)} + 1 - w_{r}^{(k)} \sum_{i=1}^{m'} c_{i}^{(k-1)} \cdot T_{i,r}^{(k-1)}$$ (8)

where

$$P_{i} \in IP' = \{P_{j} | c_{j}^{(k-1)} \geq \lambda\}, m' = |IP'|, \text{ and}$$

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 $\{T_{i,r}^{(k-1)}\}$ and credibility values $\{c_{i}^{(k-1)}\}$, the aggregated trust value of peer $P_{r}$ in round $k$ is:

$$T_{r}^{(k)} = w_{r}^{(k)} T_{r}^{(k-1)} + 1 - w_{r}^{(k)} \sum_{i=1}^{m'} w_{i}^{(k-1)} c_{i}^{(k-1)} \cdot T_{i,r}^{(k)}$$ (9)

where

$$w_{i}^{(k-1)} = \frac{c_{i}^{(k-1)}}{\sum_{i=1}^{m'} c_{i}^{(k-1)}}$$ (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), $\frac{1}{m'} \sum_{i=1}^{m'} c_{i}^{(k-1)}$. $T_{r}^{(k-1)}$ leads to a lower trust value. However, $\frac{1}{m'} \sum_{i=1}^{m'} w_{i}^{(k-1)} c_{i}^{(k-1)} \cdot T_{i,r}^{(k)}$ 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 $P_{r}$, whose true trust value $tt$ is 0.65, by collecting the evaluations from a set of peers where 50% peers give negatively exaggerating evaluations.
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 $w_{P}$ of the responding peer $P_{i}$ 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 $k < 100$.

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