Trust^2: Developing Trust 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, a peer needs to interact with unknown peers for the services provided. This requires the trust evaluation prior to and posterior to interactions. This paper presents $Trust^2$: a novel and dynamic peer trust evaluation model, which aims to measure the credibility of peers' recommendations, and thus to filter noise in responses and obtain more accurate and objective trust values. In our model, prior to any interaction, the trust value results from the evaluations given by other peers. Posterior to interactions, the trust values results from both other peers' evaluations and the requesting peer's experience. In the aggregation of trust evaluations, the weight to the requesting peer becomes higher and higher. Meanwhile, during this process, the credibility of each responding peer's recommendation can be measured round by round. This leads to the filtering of low credibility peers and the improvement of trust evaluations.

1 Introduction

In most peer-to-peer (P2P) systems, before interacting with an unknown peer, it is natural to doubt its trustworthiness. There is a need to determine the level of trust that can be placed on the peer before conducting the transaction.

Traditionally in the security area, the common mechanism that has been used to identify the interacting entity is based on identity based certificates. A registered peer should apply a certificate from a Certificate Authority (CA) that can be used for authenticating the peer to other peers. The authentication has been used to form the basis of "trust" in deciding whether to carry out a transaction or not. However it is clear such an approach is very limited as certificates may not necessarily convey much about the level of trust one peer is willing to place on another. An alternative technique is to take into account of the previous history of interactions of the peer (e.g. [8]). By collecting feedbacks from other peers about their comments on the previous interactions, the end-peer may analyze and thereafter determine the trust value of the peer being investigated.

In this paper, we present $Trust^2$: a novel peer trust evaluation model. In our method, prior to any interactions, the trust value of an unknown peer can be determined by investigating its interaction history with other peers. Following this, if the evaluation result is good enough, the requesting peer can interact with the unknown peer, which becomes familiar hereafter. With more and more interactions, it is possible to give more accurate trust evaluation to the peer, which results from the quality of the service of the peer. Meanwhile, other peers' evaluations can be collected to measure their credibilities so as to filter noise in evaluations and obtain more accurate trust values. We also propose a method, which weights more to the requesting peer's evaluations after a number of rounds, wherein the initial weight is quite low but the temporal dimension is added. A set of experiments has been conducted to study the properties of the proposed models.

This paper is organized as follows. In section 2, we review some existing works. Section 3 presents our approach for peer trust evaluation. Some experiment results are illustrated in section 4. In section 5, we conclude our work.

2 Related Work

In [2], the authors proposed $XRep$: a reputation-based approach for evaluating the reputation of peers through distributed polling algorithm before downloading any information. The approach adopts a binary rating system and it is based on the Gnutella [1] query broadcasting method using TTL limit.

EigenTrust [3] collects the *local trust values* of all peers to calculate the *global trust value* of a given peer. This is not realistic in real applications. Additionally, EigenTrust [3]

Proceedings of the 2005 IEEE International Conference on Services Computing (SCC'05)
0-7695-2408-7/05 $20.00 © 2005 IEEE

adopts a binary rating function, interpreted as one (positive or satisfactory), or zero or negative one (unsatisfactory or complaint).

In [4], the authors propose 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 given peer. This seems more reasonable than the model in [2]. However, this work and the work in [3] 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.

[5] proposes several trust metrics for the trust evaluation in a decentralized environments (e.g. P2P) where a trust value is a probabilistic value in the interval of $[0,\ 1]$. Prior to the interaction with an unknown peer x, the end peer collects other peers' trust evaluations over X. A method has been proposed for trust modification after a series of interactions with x that a good value results from the cumulation of constant good behaviors leading to a series of constant good trust values. In [6] the time dimension is taken into account in the trust evaluation wherein fresh interactions are weighted more than old ones.

In [12], the authors extend their previous work in [10] and [11] proposing the method of exponential averaging taking into account a series of interactions of the requesting peer itself. It is similar to the work in [6]. However the weight to an older interaction is not greater than a fresher one. Meanwhile all weights should be normalized. These are not strictly followed in [12]. [11] presents a method for detecting possible lying peers that is based on the requesting peer's experience. We argue that each peer's individual trust evaluation over a given peer is fully dependant on the experience, the quality of service and the honesty of the evaluating peer. The evaluations may vary from time to time and from peer to peer. However, a lying peer's evaluation is incorrect most of the time, which may be positive exaggeration or negative exaggeration. Therefore, the process to identify a liar requires a series of interactions that occur in different rounds or periods.

In the literature, most earlier works adopt binary rating models, such as [8], [9] and [2]. These models consider the P2P network for information sharing only. As mentioned in [12], binary ratings work pretty well for file sharing systems where a file is either the definitive correct version or is wrong, but cannot accurately model richer services such as web services and e-commerce, where a boolean may not adequately represent a peer's experience of the quality of service (QoS) with other peers, e.g., the quality of products the peer sends and the expected delivery time [12]. Therefore most recent works [11, 5, 12, 6] adopt the numeral rating system where the trust values are in an interval (e.g. $[0,\ 1]$).

In this paper we propose a dynamic and iterative process for peer trust evaluation and amendment. Here we take into account the credibility of each responding peer, which is derived from the deviations of its recommendations, and is amended through a series of interactions by the requesting peer. This hence provides more precision to the trust evaluation, which results from the evaluations from both the requesting peer and the responding peers.

3 Trust Evaluation

In the following context, we study the trust evaluation method with the following assumptions:

1. most peers are honest, and
2. the requesting peer is honest.

3.1 Local Rating

For a peer P_A, if it has interactions with a peer P_B, it can give a local trust evaluation $T^{(k)}_{A\to B}$ for the interaction occurred in round k at time t_k. The value is calculated considering the quality of the service provided by P_B. The quality of the service comes from several aspect represented by a set of attributes relevant to service quality: $\{x_1, x_2, \ldots, x_n\}$.

If R_i is the rating of attribute x_i, a crisp evaluation value can be obtained by calculating the overall direct trust value $T_{A\to B}$ of the value x as:

$$T_{A\to B} = \sum w_{x_i} * R_i \tag{1}$$

where the relative importance assigned to each attribute is modelled as a weight w_{x_i}, $\sum w_{x_i} = 1$. All weights are given by an end-peer (consumer). In addition, fuzzy logic can be adopted for local ratings [7].

3.2 Aggregated Rating

If a peer P_r has no interaction history with peer P_x, P_r can enquire other peers about the latest trust status of P_x. Suppose the trust values from a set of intermediate peers $IP = \{P_1,\ P_2,\ \ldots,\ P_m\}$ are

$$T_{1\to x}, T_{2\to x},\ \ldots,\ T_{m\to x}$$

The mean trust value can be simply calculated as

$$\bar{T_x} = \sum_{i=1}^{m} T_{i\to x}$$

If P_r has a number of interactions with P_x during period $[t_{start}, t_{end}]$=$\{t_1, t_2, \ldots, t_l\}$ where $t_k < t_{k+1}$ $(1 \leq k < l)$, it can evaluate P_x's trust value as follows:

$$T_{r \to x} = \sum_{k=1}^{l} w^{(k)} \cdot T_{r \to x}^{(k)} \quad (2)$$

where

- $0 \leq w^{(k)} < w^{(k+1)} < 1, 1 \leq k \leq l-1$;
- $\sum_{k=1}^{l} w^{(k)} = 1$.

Equation (2) weights more to recent interactions. This is a time-based evaluation method where fresher interactions are more important than old ones. But it takes into account P_r's experience only.

Alternatively, the requesting peer P_r can enquire the trust values of P_x given by other peers so as to aggregate these values with its own experiences.

Definition 1: For the interaction in round k at time t_k, the *aggregated trust value* by P_r can be calculated as follows:

$$\tilde{T}_{r \to x}^{(k)} = w_r^{(k)} \cdot T_{r \to x}^{(k)} + (1 - w_r^{(k)}) \cdot \bar{T}_x^{(k)} \quad (3)$$

where

- $\bar{T}_x^{(k)} = \sum_{i=1}^{m} T_{i \to x}^{(k)}$
- $w_r^{(k)}$ is the weight to P_r's experience in round k at t_k and $w_r^{(k-1)} < w_r^{(k)}$ $(t_{k-1} < t_k)$.

Equation (3) takes into account both P_r's experience and other peers' experience with P_x leading to more objective trust evaluation. Moreover, with more and more interactions with P_x, P_r is more 'confident' with its own experiences. This is reflected by w_r, which may be very low in the beginning (e.g. 0.1 or 0.3) but it becomes higher and higher in later rounds.

Here the aggregated trust value is not the kind of global trust value as in [3] which is costly and not realistic to obtain in P2P environments. $\tilde{T}$ is partially subjective to P_r's evaluation. So it is still a local value but is more trustworthy than $\bar{T}$ form P_r's perspective.

To control the changes of w_r, we propose a function using two parameters: α and β.

Definition 2: Given parameters α $(0.5 < \alpha < 1)$ and β $(\beta \in \{1, 2, 3, \ldots\})$, *the weight to P_r's evaluation in round k* can be calculated as follows:

$$w_r^{(k)} = 1 - \alpha^{k^{\frac{1}{\beta}}},\ 0 < \alpha < 0.5 \, and \, \beta \in \{1, 2, 3, \ldots\} \quad (4)$$

In equation (4), α is the initial weight for $\bar{T}_x^{(1)}$ (see equation (3)) while the weight $w_r^{(1)}$ (where $k = 1$) is $1 - \alpha$. Typically, $w_r^{(1)}$, the weight of $T_{r \to x}^{(1)}$ is less than 0.5 (e.g. 0.1 or 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. 0.9 or 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.

The above features are depicted in Figure 6 in section 4.1.

In addition, the valuation of β is dependant on applications. If 20 means high quantity of interactions, $\beta = 1$ is suitable. If 500 means high quantity of interactions, $\beta = 2$ or $\beta = 3$ is more suitable.

3.3 Evaluation and Noise

In the initial round evaluation ($k = 0$), typically the requesting peer P_r can send requests to his friend peers to collect their evaluations against unknown peer P_x. These friend peers are those peers with whom P_r has good interaction history. However, the limitation is that it is highly dependant on P_r's friend peers, i.e. the number of friend peers, their interaction history with P_x. Furthermore, this method takes the interaction trust as the recommendation trust (credibility). Namely, recommendations from peers with trustworthy quality of services are trustworthy. Nevertheless, in the real world, interaction trust and recommendation trust are different. A good peer providing good quality of service may denigrate other peers especially when those peers provide the same kinds of services. Meanwhile, if P_r is a new peer, it can hardly have any fiend peers to enquire with.

Alternatively, P_r can send requests to its neighbors and to other peers via its neighbors collecting their trust evaluations over P_x. Inevitably this method leads to noise in the trust evaluation as the credibility of each responding peer is not known.

As we introduced in section 3.2, with more and more interactions with peer x, which is unknown to P_r in the beginning, and the evaluations from responding peers, the requesting peer is more and more confident of its evaluation over P_r. However, the equation (3) in section 3.2 doesn't take into account the credibility of responding peers' recommendations or filter any possible noise in the replied recommendations.

With more and more interactions with peer x, on one hand, P_r obtains more and more interaction trust values over x, which are *direct* interaction trust evaluations. By aggregating its direct evaluations with other peer' evaluations (*indirect evaluations*), the new aggregated evaluation becomes more and more objective from P_r's perspective. On

the other hand, based on the objective aggregated trust values, it is possible for P_r to identify a peer with noise whose evaluations are deviated from the "main stream" peers or to identify a peer whose evaluations are close to the "main stream" peers. Thus the credibility of a responding peer can be estimated based on a series of interactions by P_r and the evaluations of other peers in different rounds. These credibilities are useful as well when P_r wants to know the trust values of other unknown peers. Meanwhile, with updated credibilities, the trust evaluation over P_x becomes more accurate and objective. In the following context, we use '*credibility*' to represent the measurement of recommendation trust.

Here we classify four kinds of evaluations as follows:

1. **honest evaluations** the evaluating peer is honest and its evaluation reflects the quality of service;
2. **positive exaggeration** the peer's evaluation is always better than the true value by a certain extent;
3. **negative exaggeration** the peer's evaluation is always worse than the true value by a certain extent;
4. **random exaggeration** the peer's evaluation is positive exaggeration or negative exaggeration randomly. The mean of all evaluations may be close to the true value, but any individual value in a certain round may have significant deviation.

In Figure 1-4 depict the above four classes where the true trust value $tt = 0.7$.

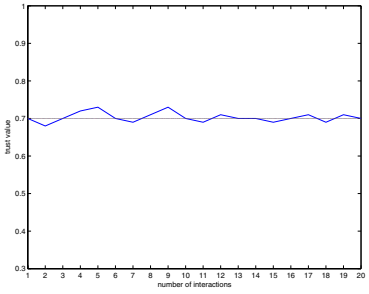

Figure 1. Class 1 Trust Evaluation ($tt = 0.7$)

The above classification is different from the one in [11] which replaces the 4th class with a 'compensation' class where the given value is always the compensation of the true value. That is not realistic in applications and it actually belongs to the above class 4.

In this paper, we don't explicitly identify 'malicious peers'. Any evaluation deviation is identified as noise. The aim of our model is to find objective trust values that should be more accurate with less noise.

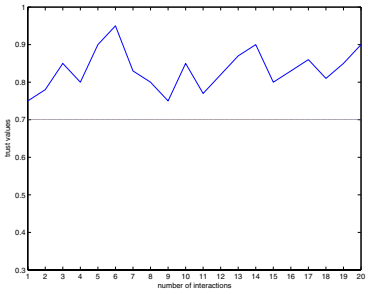

Figure 2. Class 2 Trust Evaluation ($tt = 0.7$)

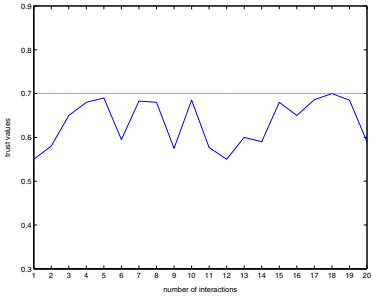

Figure 3. Class 3 Trust Evaluation ($tt = 0.7$)

Definition 3: Assume $T_{i\to x}^{(k)}$ represents the trust value given by P_i in round k at t_k over P_x and $\bar{T}_x^{(k)}$ represents the mean trust value. *P_i's evaluation deviation in round k* is

$$d_{r\to x}^{(k)} = T_{r\to x}^{(k)} - \bar{T}_x^{(k)} \tag{5}$$

3.4 Credibility Evaluation

The deviation of a responding peer can be used to measure its credibility. If its evaluation is far away from the "main stream" peers, its credibility will be low though it may not a malicious peer or a liar. Otherwise, it should obtain a high credibility. The deviations in different rounds can be used to derive the new credibilities of a responding peer.

The relationship of deviation and credibility is as follows:

1. A low deviation (in $[0,\ 1]$) leads to high credibility (in $[0,\ 1]$);
2. A high deviation (in $[0,\ 1]$) leads to a low credibility (in $[0,\ 1]$).

Meanwhile, the new credibility results from the deviation of the current round and the peer's previous credibilities (history). Some principles are as follows:

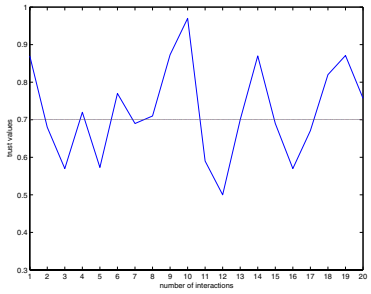

Figure 4. Class 4 Trust Evaluation ($tt = 0.7$)

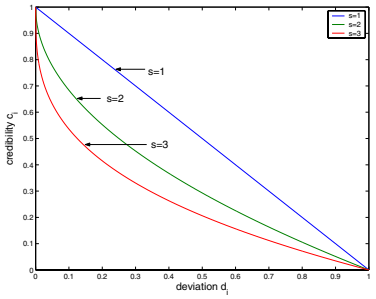

Figure 5. the relationship between d_i and c_i

Principle 1: Incremental number of ratings taken into account in an evaluation reduces the level of modification applied over the credibility evaluation until a certain level of confidence is achieved. Then the modification applied becomes constant.

Principle 2: A larger change of the existing credibility value and the newly given credibility value should cause more changes in the credibility evaluation. In contrast, a smaller change will have a less effect.

In our method, if it is the first time to get trust evaluation reply from a responding peer P_i, an initial value is assigned for its credibility (e.g. $c_i^{(0)}$=0.5).

Definition 4: In the kth round, if the true trust value of a peer is tt and the trust value given by peer P_i is $T_{i\to x}^{(k)}$, the *deviation* is

$$d_i^{(k)} = |T_{i\to x}^{(k)} - tt| \tag{6}$$

Here it can be simply assumed that the credibility is *approximately*

$$c_i^{(k)} = 1 - d_i^{(k)\,\frac{1}{s}} \tag{7}$$

where s is a *strictness factor* which is used to control the curve. Figure 5 depicts the relationship between d_i and c_i. For example, if $d_i = 0.25$, then $c_i = 0.75,\ 0.5,\ 0.37$ when $s = 1,\ 2,\ 3$ respectively. The higher s is, the stricter the evaluation is. However, as we discussed in principles 1 and 2, equation (7) cannot reflect any credibility history.

In the following, we define a new equation for credibility evaluation, which takes into account credibility history but uses several arguments only.

Definition 5: 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:

$$c_i^{(k)} = c_i^{(k-1)} + \theta_i^{(k)} \cdot (1 - d_i^{(k)\,\frac{1}{s}} - c_i^{(k-1)}) \tag{8}$$

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

$$\theta_i^{(k)} = \frac{e^{|1-d_i^{(k)\,\frac{1}{s}} - c_i^{(k-1)}|} - 1}{e+1} \tag{9}$$

In equation (8), the new credibility $c_i^{(k)}$ results from the previous credibility $c_i^{(k-1)}$ and the current deviation $d_i^{(k)}$. The change may be an increment or a decrement, which results from $\theta_i^{(k)}$ and $(1 - d_i^{(k)\,\frac{1}{s}} - c_i^{(k-1)})$ where $\theta_i^{(k)} \geq 0$. That means if $1 - d_i^{(k)} > c_i^{(k-1)}$, it is an increment. Otherwise it is a decrement. However, the quantity of the change is also controlled by $\theta_i^{(k)}$, which has the following properties.

Property 1: If $1 - d_i^{(k)\,\frac{1}{s}} = c_i^{(k-1)}$, then $\theta_i^{(k)} = \theta_{min} = 0$;

This property means that if $1 - d_i^{(k)\,\frac{1}{s}} = c_i^{(k-1)}$, there is no change with $c_i^{(k-1)}$ and $c_i^{(k)}$.

Property 2: If $1 - d_i^{(k)\,\frac{1}{s}} \neq c_i^{(k-1)}$, then $\theta_i^{(k)} > 0$;

This property means that if $1 - d_i^{(k)\,\frac{1}{s}}$ and $c_i^{(k-1)}$ are different, there will be an increment or a decrement for the credibility modification.

Property 3: The larger $|1 - d_i^{(k)} - c_i^{(k-1)}|$ is, the larger $\theta_i^{(k)}$ is;

Property 4: When $|1 - d_i - c_i^{(k-1)}| = 1$, $\theta_{max} = 0.462$.

Properties 3 and 4 outline the relationship between $|1 - d_i^{(k)\,\frac{1}{s}} - c_i^{(k-1)}|$ and $\theta_i^{(k)}$. More details can be found in our experiments presented in section 4.2.

Initial Credibility Assignment In the above method, an initial credibility value $c_i^{(0)}$ should be given so that new credibility values (i.e. $c_i^{(1)}$, $c_i^{(2)}$, ...) can be calculated in the subsequent rounds. However, in the beginning, peer P_r

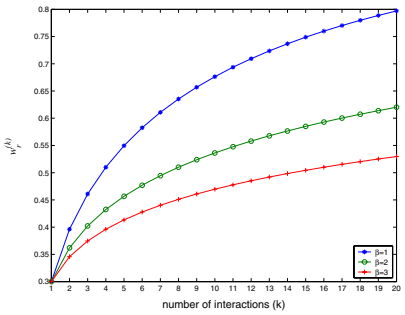

Figure 6. Experiment 1 ($\alpha = 0.7$)

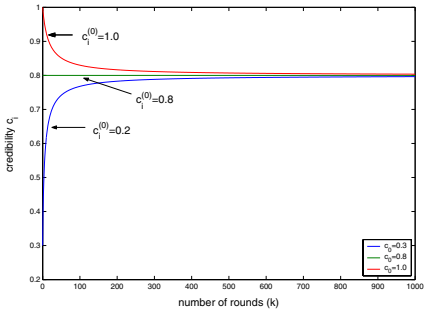

Figure 7. Experiment 2 ($d_i = 0.2,\ s = 1$)

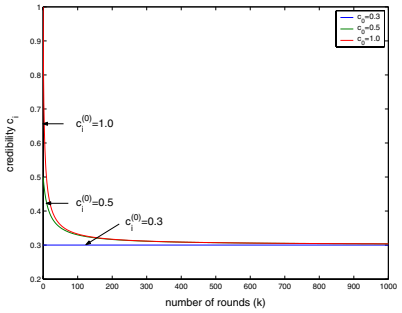

Figure 8. Experiment 2 ($d_i = 0.7,\ s = 1$)

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. But the credibility value can be modified in different rounds which will be closer to the true value.

Definition 6: 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:

$$\bar{T}_x^{(k)} = \sum_{i=1}^{m} c_i^{(k-1)} \cdot T_{i \to x}^{(k)} \tag{10}$$

Herein the definition of $\bar{T}_x^{(k)}$ in definition 1 has been rectified with the credibility of each responding peer to be taken into account. Additionally, in a certain round, if the credibility of a responding peer is no more than a threshold μ, it will be deleted in the list.

Thus according to equations (10) and (3), more accurate *aggregated trust values* can be obtained.

$$\tilde{T}_{r \to x}^{(k)} = w_r^{(k)} \cdot T_{r \to x}^{(k)} + (1 - w_r^{(k)}) \cdot \sum_{i=1}^{m} c_i^{(k-1)} \cdot T_{i \to x}^{(k)} \tag{11}$$

4 Experiments

In this section, we present the experimental results illustrating the properties of equations and methods.

4.1 Experiment 1

In this experiment, we study the variations of $w_r^{(k)}$ (see equation (4)) where $\alpha = 0.2$ and β is set to be 1, 2 and 3 respectively. The result is plotted in Figure 6. In Figure 6 $\alpha = 0.7$ and $k \in \{1, 2, \ldots, 20\}$. It illustrates that a larger β leads to a slower changing of $w_r^{(k)}$.

4.2 Experiment 2

In this experiment, we aim to study the properties of equations (8) and (9). The strictness factor s is set to be 1 in Figure 7 and 8, and 2 in Figure 9 and 10.

In Figure 7, the deviation d_i is set as 0.2 while the initial credibility $c_i^{(0)}$ is set to 0.2, 0.8 and 1.0 respectively. From the result we can observe that when $c_i^{(0)} = 0.8$, then c_i is constant and $c_i = 0.8 = 1 - 0.2 = 1 - d_i$. If $c_i^{(0)}$ is set to be a low value 0.2, c_i can be increased round by round. The value reaches approximately $1 - d_i$. So is the case where $c_i^{(0)} = 1$ and c_i is decreased approaching $1 - d_i$. From this experiment, it is easy to see that

$$lim_{k \to \infty} c_i^{(k)} = 1 - d_i^{\frac{1}{s}} \tag{12}$$

In Figure 8, the deviation is set to be $d_i = 0.7$ while the initial credibility $c_i^{(0)}$ is set to be 0.3, 0.5 and 1.0 respectively.

It is easy to see that an accurate $c_i^{(0)}$ (e.g. 0.3) leads to subsequent accurate credibilities though an inaccurate $c_i^{(0)}$ can be rectified by increments or decrements. But in any case equation (12) holds.

Figure 9 and 10 plot two cases where $s = 2$ and one of three initial credibility values in each case is set to be $1 - d_i^{\frac{1}{2}}$.

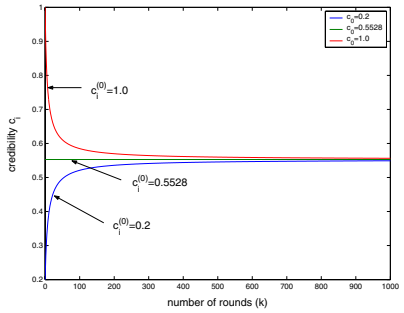

Figure 9. Experiment 2 ($d_i = 0.2,\ s = 2$)

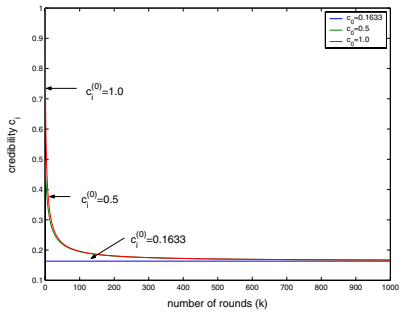

Figure 10. Experiment 2 ($d_i = 0.7,\ s = 2$)

The curve change trends are exactly the same as Figure 7 and 8 as $1 = 0.7^{\frac{1}{2}} = 0.5528$ and $1 - 0.7^{\frac{1}{2}} = 0.1633$. So equation (12) holds.

4.3 Experiment 3

In this experiment, we study the trust evaluation over peer P_x, whose true trust value tt is assumed to be 0.8, by collecting the evaluations from a set of peers where 30% or 50% peers give negatively exaggerating evaluations.

In this experiment, we set the strictness factor $s = 2$. The reason to consider class 1 (honest) and 3 (negative exaggeration) peers only is that this is an extremely malicious environment. If both class 2, 3 and 4 peers are considered, their deviations may counteract each other.

We compare four evaluation strategies in this experiments. They are improved one by one.

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

Strategy 2 : This strategy improves 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.

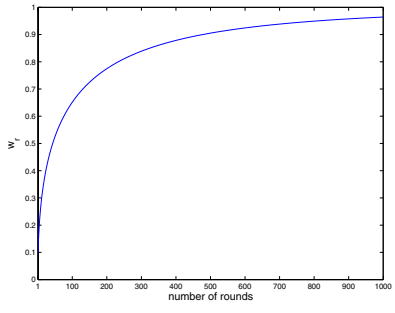

Figure 11. w_r in Experiment 3 ($\alpha = 0.9,\ \beta = 2$)

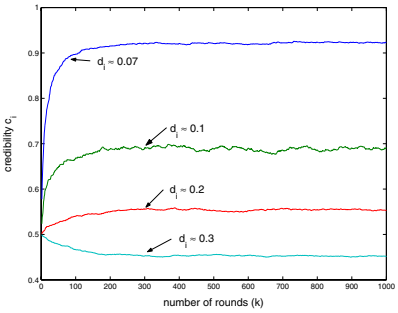

Figure 12. c_i in Experiment 3 ($s = 2,\ c_i^{(0)} = 0.5$)

Strategy 3 : This strategy applies the weight w_r of the responding peer P_r via equation (11). In the experiment, we set $\alpha = 0.9$, $\beta = 2$ (see Figure 11).

Strategy 4 This strategy improves strategy 3 by ignoring low credibility peers, where the threshold is set to be $\mu = 0.6$ from the $50th$ rounds onwards.

In this experiment, there are 3 classes among negatively exaggerating peers. Their mean deviations are 0.1, 0.2 and 0.3 respectively (see Figure 12). In contrast, the deviation of a honest peer is approximately 0.07. In Figure 13, it is easy to see that strategy 1 and 2 lead to low trust values. In strategy 3, the trust values become more and more accurate but the trust values in strategy 4 can be improved earlier and better when some low credibility peers are ignored.

Figure 14 depicts the results from another experiment where 50% peers are negatively exaggerating. In this case, strategy 1 and 2 obtain lower values than those in Figure 13. But in strategy 3 and 4 trust values can be improved very quickly as well.

5 Conclusions

In this paper, we present $Trust^2$: a novel model for trust evaluation in P2P environments. This model takes into ac-

Proceedings of the 2005 IEEE International Conference on Services Computing (SCC'05)
0-7695-2408-7/05 $20.00 © 2005 IEEE

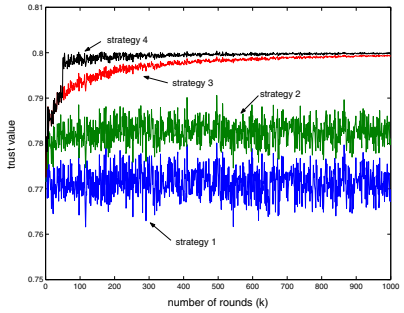

Figure 13. Experiment 3 ($s = 2,\ tt = 0.8$**,** $\alpha = 0.9,\ \beta = 2$**)**

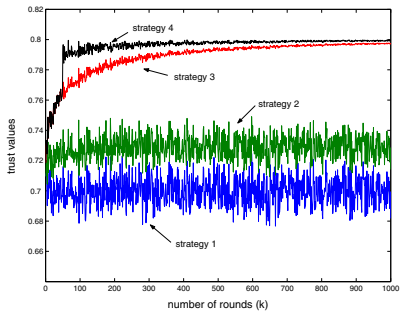

Figure 14. Experiment 3 ($s = 2,\ tt = 0.8$**,** $\alpha = 0.9,\ \beta = 2$**)**

count the credibility of responding peers that is valuable to identify inaccurate recommendations and thus improve the precision of trust evaluations. Meanwhile, a method for credibility evaluation has been proposed that is based on recommendation history. 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. This is realistic in real applications and helps obtain more objective trust values.

References

[1] *GNutella*. http://www.GNutella.com/.

[2] 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 Conference on Computer and Communication Security (CCS'02)*, pages 207–216, Washington DC, USA, November 2002.

[3] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. In *Proceedings of the Twelfth International World Wide Web Conference*, Budapest, Hungary, May 2003.

[4] S. Marti and H. Garcia-Molina. Limited reputation sharing in p2p systems. In *Proceedings of ACM Conference on Electronic Commerce (EC'04)*, New York, USA, May 2004.

[5] Y. Wang and V. Varadharajan. Interaction trust evaluation in decentralized environment. In K. Bauknecht, M. Bichler, and B. Pröll, editors, *Proceedings of 5th International Conference on Electronic Commerce and Web Technologies (EC-Web04)*, volume LNCS 3182, pages 144–153, Zaragoza, Spain, August-September 2004.

[6] Y. Wang and V. Varadharajan. A time-based peer trust evaluation in p2p e-commerce environments. In *Proceedings of 5th International Conference on Web Information Systems Engineering (WISE'04)*, volume LNCS 3306, pages 730–735, Brisbane, Australia, November 22-24 2004.

[7] Y. Wang and V. Varadharajan. Two-phase peer evaluation in p2p e-commerce environments. In *Proceedings of the 2005 IEEE International Conference on e-Technology, e-Commerce and e-Serivce (EEE-05)*, pages 654–657, Hong Kong, China, March 29-April 1, 2005.

[8] L. Xiong and L. Liu. PeerTrust: A trust mechanism for an open peer-to-peer information system. Technical Report GIT-CC-02-29, Georgia Institute of Technology, 2002.

[9] L. Xiong and L. Liu. PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Trans. Knowl. Data Eng.*, 16(7):843–857, 2004.

[10] B. Yu and M. P. Singh. An evidential model of distributed reputation management. In *Proceedings of First International Joint Conference on Autonomous Agents and Multiagent Systems*, pages 294–301, 2002.

[11] B. Yu and M. P. Singh. Detecting deception in reputation management. In *Proceedings of Second International Joint Conference on Autonomous Agents and Multiagent Systems*, pages 73–80, 2003.

[12] B. Yu, M. P. Singh, and K. Sycara. Developing trust in large-scale peer-to-peer systems. In *Proceedings of 2004 IEEE First Symposium on Multi-Agent Security and Survivability*, pages 1–10, August 2004.