Interaction Trust Evaluation in Decentralized Environments

Yan Wang and Vijay Varadharajan

Department of Computing
Macquarie University
Sydney, NSW 2109
Australia
{yanwang, vijay}@ics.mq.edu.au

Abstract. In decentralized environments, such as P2P, as lack of central management, the trust issue is prominently important for interactions between unfamiliar peers. This paper first presents a probabilistic approach for evaluating the interaction trust of unfamiliar peers according to their interaction history. In addition, after an interaction, peers can evaluate each other and modify the trust status. Based on it, this paper presents an approach for trust value modification after interactions.

1 Introduction

Recent years, P2P and Grid technologies have widely obtained attentions in both research and industry communities. Some successful systems emerged, such as GNutella [1], Kazaa [2], SETI@home [3] and Globus [4]. These systems enable the share of resources in a loosely-coupled network consisting of a large number of peers. Each peer contributes its information and even CPU resource to the network. Tasks, such as exchanging a set of large volume or large partition information, or completing a complex and partitioned task, could be achieved through the interaction and collaboration of all involved peers.

As lack of the central management in most P2P systems, the dynamic status of each peer as well as the network causes trust evaluation a very important issue. Before interacting with an unfamiliar (strange) peer, it is rational to doubt its trustworthiness. Therefore, to enable the trust evaluation prior to interacting with a set of unfamiliar peers makes the transaction securer. In particular, when P2P network is used for e-commerce applications, the trust evaluation prominently becomes a more important issue.

To evaluate the trustworthiness of a peer, some methods can be adopted. Generally there are two categories for these methods. One is based on the mechanism of security certificate authentication. A registered peer should apply a certificate from a Certificate Authority (CA) that can be used for identifying the peer to other peers. This is useful to authenticate a new peer which may newly join the community or it has no interaction history with other peers. And thus the initial trust can be established if the authentication process is successful.

The other category is to investigate a peer with which the end-peer has no interaction history but others do [5]. By collecting the 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 propose a novel model that evaluates the trust values of peers. In our method, the trustworthiness of a certain peer can be determined by investigating the interaction history of other peers if the end-peer has no previous interaction with it. Meanwhile a method is also proposed for modifying the trust value of a peer after the interaction with it is completed.

2 Related Work

There are numerous notions of trust and different kinds of trust that satisfy different properties that can be established differently [5].

In terms of computer security, trust is considered as a fundamental concept. An entity is trustworthy if there is sufficient credible evidence leading to believe that the system will meet a set of given requirements. Trust is a measure of trustworthiness, relying on the evidence provided [6]. For instance, in traditional client/server systems, a client should pass the authentication verification by the server before obtaining any privilege for accessing the data from the server. Far from that, a more complex mechanism is proposed in [7] as the process of trust negotiation, where the two parties need to open the respective authentication policy to each other and exchange their required certificates (i.e. credentials in [7]). The outcome of credential exchange depends on if each party accepts the autointoxication policy of the other side and if they have sufficient evidence and credentials to meet the requirement of the other party. These work is generally based on existing standards such as X.509 [8] or PGP [9] and provides various extensions. They are valuable for initial trust establishment for two strangers.

But these methods only take into account the authentication and authority of a peer that may ask certain level access privilege or intend to involve a specific interaction. The outcome after authentication is simply '*Yes*' or '*No*' where '*Yes*' means the authentication is successful and '*No*' means unsuccessful. No previous interaction histories are evaluated. In terms of calculation, this is a non-calculative trust [10].

On the other hand, trust can be defined in terms of trust belief and trust behavior [11]. Trust belief between two parties is the extent to which a party believes that the other party is trustworthy in a certain situation. Trustworthy means one is willing and able to act in the other party's interests. Trust behavior between two parties is the extent to which a party depends on the other in a given situation with a feeling of relative security, even though negative consequences are possible. If a trust belief means "party A believes that party B is trustworthy", then it will lead to a trust behavior as "A trusts B" [5].

[5] proposed a PeerTrust model considering the trust belief between two peers in a P2P environment. In this model, each peer will give an evaluation as Satisfaction (S) or Complaint (C) to another peer after their interaction. Any peer

can collect these information about a given unfamiliar peer so as to evaluate the peer in terms of the degree of satisfaction it receives in providing services to other peers in the past. Anyway, we would like to argue that it is a bit simple for more exact trust evaluation if a peer assigns just satisfaction or complaint after it receives the service of the other peer. Moreover, how to evaluate the trust value of a peer if the end-peer has at least one interaction already is not mentioned in the literature.

3 Trust Evaluation

In this section, we will propose our model that evaluates the trust values of peers by investigating other peers. In our method, the trustworthiness of a certain peer can be determined by investigating the interaction history of other peers if the end-peer has no previous interaction with it. After the investigation, the probability of a given threshold of trust value for a peer can be calculated. With these collected results, a set of peers can be chosen that satisfy the requirement of the end-peer. After that, the end-peer can choose some of them to collaborate for completing specific tasks. Meanwhile a method is also proposed for modifying the trust value of a peer after the interaction with it is completed. In the following context, for the sake of simplicity, we assume that feedbacks are collected from a large number of honest peers after the process of filtering malicious complaining peer. A method for identifying malicious complaining peers can be found in [12].

3.1 Trust Metrics

In P2P environments, a peer can be client and server anytime providing shared resources and services to the open community. The trust of a given peer is the existing cumulative degree of satisfaction from other peers based on the services and their quality it ever provided to these peers.

1. For an individual peer, its degree of satisfaction with another peer which is a service provider in an interaction can be a real number among a predefined scope (e.g. a real number among [0,1]), not just simply 1 or 0. The value may result from the service quality, the recognition by the end-peer.
   For example, end-peer A broadcasts a set of tasks to a set of remote peers. After the results are returned, A could compare the quality of services performed by different peers. If a peer frequently misbehaved, it will constantly get low evaluation by most other peers. The final trust value is the cumulative sum of feedbacks from a large number peers for a relative long period.
2. Regarding a certain peer, suppose the initial trust value is a very low value (e.g., $0.1 \in [0, 1]$), constant good behaviors should be able to upgrade its trust value. Anyway, constant good behaviors in a short period (with only a few interactions) should promote less than that in a relatively longer period (with many interactions). Meanwhile, a positive high value should affect less to a peer with high trust value. For example, suppose the trust value is a

real number among [0,1], if peer A has got its cumulative trust value of 0.9, a new higher value 0.95 can only give a minor positive affect (e.g., +0.001) to A's trust value. The positive increment of A's trust value should result from constant good behaviors. Likewise, in such a case, a new lower value also brings minor negative affect to a high value peer since the high value is established through long-term interactions with good behaviors.

3.2 Trust Evaluation Method

Now suppose an end-peer A hopes to have a transaction with a peer X, with whom A has no previous interaction history. To evaluate the trust status of X, A will have to investigate the trust value through other peers which have transaction histories with X.

Now we assume that each peer gives a trust value (a real value) between 0 and 1 over the other after a transaction. That is if peer Y just has a transaction with peer Z, the trust value given by Y over Z is denoted as $T_{Y\to Z} \in [0,1]$. "1" means the highest satisfaction degree while "0" means the lowest one. After having collected a set of feedbacks from other peers, A could analyze the data and make the estimation on the trust status of peer X based on Gauss Distribution in Probability Theory [13].

Suppose peer A has sent requests to a set of intermediate peers $\{M_1, M_2, \ldots, M_k\}$ from which A will collect feedbacks

$$\{T_{M_1\to X}, T_{M_2\to X}, \ldots, T_{M_k\to X}\}$$

The *mean trust value* $\bar{T}$ can be calculated as

$$\bar{T} = \frac{1}{k}\sum_{i=1}^{k} T_{M_i\to X} \tag{1}$$

Accordingly, the *sample variance* is

$$S^2 = \frac{1}{k-1}\sum_{i=1}^{k}(T_{M_i\to X} - \bar{T})^2 \tag{2}$$

Let $\mu = \bar{T}$, $\sigma^2 = S^2$. Since $T \sim N(\mu, \sigma^2)$, for any random variable T and a given value v, according to the theory of Gauss Distribution [13], we have the distribution function as follows

$$F(v) = P(T \le v) = \frac{1}{\sqrt{2\pi}\sigma}\int_{-\infty}^{\frac{v-\mu}{\sigma}} e^{-\frac{x^2}{2}}dx \tag{3}$$

Likewise, we have

$$P(T > v) = \frac{1}{\sqrt{2\pi}\sigma}\int_{\frac{v-\mu}{\sigma}}^{\infty} e^{-\frac{x^2}{2}}dx \tag{4}$$

Definition 1: After having collected $\{T_{M_1 \to X}, T_{M_2 \to X}, \ldots, T_{M_n \to X}\}$ from a set of intermediate peers $\{M_1, M_2, \ldots, M_n\}$ and calculated $\bar{T}$ and S^2, $P(v_1 < T \leq v_2)$, *the probability of X's trust value in a given scope* $(v_1, v_2]$ $(v_1 < v_2,\ v_1,\ v_2 \in [0, 1])$, is

$$P_\alpha^X(v_1, v_2) = P(v_1 < T \leq v_2) = \frac{1}{\sqrt{2\pi}\sigma} \int_{\frac{v_1-\mu}{\sigma}}^{\frac{v_2-\mu}{\sigma}} e^{-\frac{x^2}{2}} dx \tag{5}$$

Definition 2: From definition 1, end peer A could calculate *the probability that peer X's trust value is better than a given value* $v \in [0, 1]$.

$$P_\beta^X(v) = P(T > v | T \in (0, 1]) = \frac{P(v < T \leq 1)}{P(0 < T \leq 1)} = \frac{\int_{\frac{v-\mu}{\sigma}}^{\frac{1-\mu}{\sigma}} e^{-\frac{x^2}{2}} dx}{\int_{-\frac{\mu}{\sigma}}^{\frac{1-\mu}{\sigma}} e^{-\frac{x^2}{2}} dx} \tag{6}$$

If there are a number of potential peers $\{X_1, X_2, \ldots, X_n\}$ that peer A can complete transactions with, the request sent by A will ask other peers to reply their feedbacks about the trust value over there peers. Given a trust value threshold φ, the final best peer B can be chosen as

$$\exists B \in \{X_1, X_2, \ldots, X_n\}, \quad P_a^B(\varphi) = \max_{1 \leq i \leq n} \{P_a^{X_i}(\varphi)\} \tag{7}$$

3.3 Trust Modification after Interactions

In this section, we will discuss the method for trust modification after interactions.

In addition to the trust metrics in section 3.1, some principles on trust value computation are as follows:

1. Incremental number of ratings taken into account in an evaluation reduces the level of modification applied over the trust rating until a certain level of confidence is archived. Then the modification applied becomes constant.
2. A larger difference of the existing trust value and the newly given trust value should certainly cause more changes in the trust evaluation. In contrast, a smaller difference will have less affect.

A Possible Solution Here we suppose that after an interaction, a satisfaction degree $s_i \in [0,\ 1]$ at time t_i can be given. With s_i, the corresponding trust value is

$$T_i = s_i^m \tag{8}$$

where m is an integer and $m \geq 1$

We call m a *strictness factor*. For example, suppose a satisfaction degree is $s_i = 0.9$, then $T_i = 0.9$ if $m = 1$ or $T_i = 0.81$ if $m = 2$. The larger m is, the lower T_i is. The larger m is, the stricter it is.

But equation (8) cannot reflect the relationship between current trust value T_i and previous trust value T_{i-1}.

If T_{i-1} is the trust value at time t_{i-1}, s_i is the satisfaction degree obtained at time t_i, then the trust value at time t_i is

$$T_i = T_{i-1} + \theta_i \cdot (s_i - T_{i-1}^{\frac{1}{m}})^m \tag{9}$$

where m=1, 2, 3, ...; θ_i is the *impact factor* determining the impact of recent change on the trust value.

Here, we define θ_i as

$$\theta_i = \frac{e^{1-T_{i-1}} - 1}{e + 1} \tag{10}$$

Analyzing the above equations, we can observe that

1. If $T_{i-1} = 1$ then $\theta_i = 0$. So $T_i = T_{i-1}$. Namely if $\lim_{i\to\infty} T_{i-1} = 1$, then $\lim_{i\to\infty} \theta_i = 0$ and $\lim_{i\to\infty} T_i = T_{i-1}$
   From this property, we can know that if the trust value of a peer is very high (e.g. 1) after many interactions, the new trust value will have minor affect (refer to principle (2) in section 3.1).
2. If $T_{i-1} = 0$, then according to equation (10),

$$\theta_i = \frac{e-1}{e+1} \approx 0.46 = \theta_{max}$$

   Hence from equation (9), we have

$$T_i = \frac{e-1}{e+1} \cdot s_i^m$$

   From this property we could know that for a new peer with no interaction history, its initial value is 0. In its first interaction, if the satisfaction degree is 1, the new trust value will be about 0.46, extremely better than the previous value 0. But it is still far from 1. This is because of principle (2) of trust metrics in section 3.1. The cumulative trust value should result from constant interactions with positive feedback. If the peer continues obtaining positive high values, its trust value can move further toward 1.

Anyway, the problem with equations (10) and (9) exists when a peer X has gained very high trust value (e.g. 1) after sufficient $i-1$ interactions with another peer Y. If in the ith interaction, Y was cheated or something serious occurred. How to assign a new trust value?

Now consider a typical case:

Suppose $T_{i-1} = 1$ and $v_i = 0$. According to equation (10), $\theta_i = 0$. So the trust value of peer X will not be affected. Therefore, equation (10) only considers the case of positive increment. The case of negative increment should also be taken into account.

A Corrected Solution Now let's discuss the correctness of the above solution.

Definition 3: If T_{i-1} is the trust value at time t_{i-1}, s_i is the satisfaction degree obtained at time t_i, *then the trust value at time* t_i is

$$T_i = T_{i-1} + \theta_i \cdot (s_i^m - T_{i-1}) \tag{11}$$

where m=1, 2, 3, ...; θ_i is the impact factor determining the impact of recent change on the trust value.

Definition 4: Now, we define the *impact factor* as

$$\theta_i = \frac{e^{|s_i^m - T_{i-1}|} - 1}{e + 1} \tag{12}$$

The properties of equation (11) and (12) are discussed as follows.

Property 1: If $\lim_{i\to\infty} |s_i^m - T_{i-1}| = 1$, then $\lim_{i\to\infty} \theta_i = \theta_{max}$.

From equation (12), it is easy to have

$$\text{if } \lim_{i\to\infty} |s_i^m - T_{i-1}| = 1, \text{ then } \lim_{i\to\infty} \theta_i = \frac{e-1}{e+1} = \theta_{max}$$

From this property, we could observe that in the two cases discussed in section 3.3, $|s_i^m - T_{i-1}| = 1$. So no matter what the peer gets, a positive or a negative feedback, the weight will be the maximum. If peer X was assigned a new satisfaction degree as 0 while its previous trust value is 1, according to equation (12) and (11), its new trust value will become 0.54, which is in an intermediate level (relatively low level).

Meanwhile, for a new peer with no interaction history, its initial value is 0. In its first interaction, if the satisfaction degree is 1, the new trust value will be about 0.46, extremely better than the previous value 0. But it is still far from 1. This is because of principle (2) of trust metrics in section 3.1. The cumulative trust value should result from constant interactions with positive feedback. If the peer continues obtaining positive high values, its trust value can move further toward 1.

Property 2: If $\lim_{i\to\infty} |s_i^m - T_{i-1}| = 0$, then $\lim_{i\to\infty} \theta_i = 0$.

In this property, when $\lim_{i\to\infty} T_{i-1} = 1$, if s_i is very close to T_{i-1}, namely $\lim_{i\to\infty} s_i = 1$, then $\lim_{i\to\infty} |s_i^m - T_{i-1}| = 0$ and hence $\lim_{i\to\infty} \theta_i = 0$. This means that if a peer's trust value is very high, a new high value of satisfaction degree will not affect the trust value too much.

Property 3: For any $s_i \in [0, 1]$ and $T_i \in [0, 1]$, $\theta_i \in [0, 0.46]$. According to definition 4, the more the difference of T_{i-1} and s_i^m is, the larger θ_i is. This is consistent to principle (2) in section 3.3.

Principle (1) in section 3.3 will be examined in our experiments.

4 Simulation

4.1 Experiment 1

This experiment compares the impact of different values of strictness factor m on the trust evaluation (see equation (11) and (12)). We set m to 1, 2, and 3 respectively. With static $s_i = 0.9$, the trust value variations are illustrated in Fig. 1. We can observe that with the same T_0 and s_i, the higher the m is, the lower the T_i is.

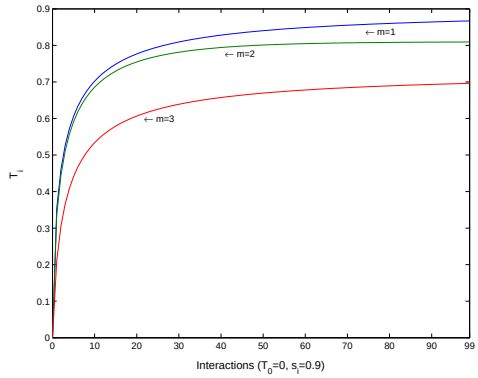

Fig. 1. T_i variations in experiment 1

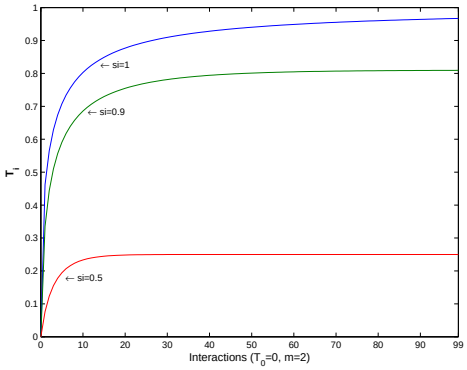

Fig. 2. T_i variations in experiment 2

4.2 Experiment 2

In this experiment, we set $m = 2$ and set static s_i in different values aiming at observing the variation of trust value (see Fig. 2). Meanwhile the wight variations are illustrated in Fig. 3. The performances in Fig. 2 are consistent to principle (2) in section 3.1 and principle (1) in section 3.3.

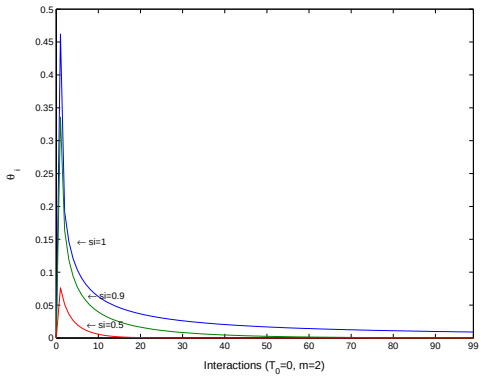

Fig. 3. θ_i variations in experiment 2

In this experiment, the initial trust value is set as 0. We can observe that when having sufficient interactions with stable s_i, the final trust value is approximately s_i^m, namely $\lim_{i \to \infty} T_i = s_i^m$.

From Fig. 3, we can observe that with static s_i, θ_i becomes less and less soon. The performance is consistent to principle (2) in section 3.1.

5 Conclusions

In this paper, we have discussed the approach for evaluating the interaction trust in P2P environment. We also proposed an approach for trust modification after interactions. They are valuable for peers to collect other peers' interaction history to the trust evaluation or identify each other's service satisfactory degree for trust modification. The property analysis and simulation have examined that the trust metrics and principles are basically followed.

Moreover, we envisage that trust and security are two prominent dimensions in P2P environments where lacks central management. We will continue working on the security and trust framework incorporating the interaction trust evaluation approach. Meanwhile, the interaction trust evaluation can be combined with certificate and security based trust evaluation/establishment before any interaction occurs between two unfamiliar peers. Furthermore the method to eliminate the negative effect of malicious peers which evaluate very low values to other peers will be explored in our future work.

References

1. *GNutella*. http://www.GNutella.com/.
2. *Kazaa*. http://www.Kazaa.com/.
3. *SETI @home*. http://www.SETI@home.com/.
4. *Globus*. http://www.Globus.com/.
5. L. Xiong and L. Liu, "PeerTrust: A trust mechanism for an open peer-to-peer information system," Tech. Rep. GIT-CC-02-29, Georgia Institute of Technology, 2002.
6. M. Bishop, *Computer Security: Art and Science*. Addition-Wesley Press, 2003.
7. T. Yu, M. Winslett, and K. E. Seamons, "Interoperable strategies in automated trust negotiation," in *Proceedings of ACM Conference on Computer and Communications Security 2001*, pp. 146–155, 2001.
8. International Telecommunication Union, *Rec.* X.*509-Information Technology-Open Systems Interconnection-The Directory: Authentication Framework*, August 1997.
9. P. Zimmerman, PGP *User's Guide, MIT Press*. 1994.
10. B. Nooteboom, *Trust: Foundations, Functions, Failure and Figures*. Edward Elgar Publishing Inc., 2002.
11. D. H. Knight and N. L. Chervany, "The meaning of trust," Tech. Rep. WP9604, Universoty of Minnesota, Management Information Systems Research Center, 1996.
12. K. Aberer and Z. Despotovic, "Managing trust in a peer-2-peer information system," in *Proceedings of CIKM 2001*, pp. 310–317.
13. G. Grimmett, *Probability: An Introduction*. Oxford University Press, 1986.