Trust and Reputation Algorithms for Unstructured P2P Networks

Shanshan Chen
College of Overseas Education, College of Computer
Nanjing University of Posts and Telecommunications
Nanjing, China
e-mail: chenss@njupt.edu.cn

Yunchang Zhang, Geng Yang
College of Computer
Nanjing University of Posts and Telecommunications
Nanjing, China

Abstract—**Reputation-based trust management is an effective method to improve network security in P2P networks. In this paper, we present a trust evaluation model based on parameter-estimation algorithms to enhance the accuracy of trust evaluation in unstructured P2P networks. Trust evaluation includes direct and second-hand trust information. It estimates and updates the trust value and uncertainty of each peer by computing mean value and variance for the collected information. We also take an incentive and punishment mechanism to stimulate peers collaboration. Simulations are performed to show the effectiveness of our model. Our model can restrain more malicious behaviors than EigenTrust.**

Keywords-unstructured P2P networks; trust; reputation estimation

I. INTRODUCTION

The availability of ubiquitous communications through the Internet is driving the migration of commerce and business from direct interactions between people to electronically mediated interactions. PEER-TO-PEER (P2P) online communities can be seen as truly distributed computing applications in which peers share information or their computations, distribute tasks or execute transactions. Numerous applications based on P2P networks have gained significant acceptance [1-3], such as Napster, Gnutella, KaZaA, BitTorrent, SETI@home, JXTA, etc. Those P2P systems interconnect computers, clusters, storage systems to make possible the sharing of existing resources, including CPU time, storage, network bandwidth, equipment, data, and software applications. However, P2P communities are often established dynamically with peers that are unrelated and unknown to each other.

In P2P networks, Peers join and leave the systems freely and dynamically [4, 5], making P2P networks very vulnerable to abuses by selfish and malicious peers [6]. Therefore, establishing trust among anonymous peers plays a vital role in upholding the quality of service and enforcing security in P2P applications. Reputation management is essential for peers to access the trustworthiness of others and to selectively interact with more reputable ones [7]. Without reputation management, peers are lack of incentive to contribute their resources or to participate in computing. A reputation-based system detects, aggregates, and updates trust information about participants' past behaviors for helping peers to make decisions. It also encourages trustworthy behaviors, and distinguishes the trusted from the untrusted.

Most reputation systems like eBay require a central server to store and distribute the reputation information. They are simple and successful reputation systems. However, centralization scheme may cause the problems of single-point failure and high overload of the center server. Instead, most existing P2P reputation systems calculate the reputation scores by aggregating peer feedbacks in a fully distributed manner [8-10]. Building an efficient, scalable and secure P2P reputation system is still a challenging task.

Due to the issue above, in this paper, we propose a parameter-estimation trust model named P-Trust. In Section 2 the components of our model and the process of establishing trust are described in detail. In Section 3, we evaluate our model under the P2P file-sharing settings. Finally, Section 4 concludes the paper and future work.

II. TRUST MODEL: P-TRUST

We propose a novel reputation-based probabilistic model based on parameter-estimation in unstructured P2P networks. Each peer continuously evaluates other peers by its local trust information and second-hand information. Meanwhile, trust increase and degradation are also brought about by incentive and punishment mechanism.

A. P-TRUST's Architecture

As is shown in Fig. 1, we propose a high level architecture similar to the TrustGuard framework [10]. Each peer has a Trustguard and a reputation manager. The direction of the arrow represents the flow of the information.

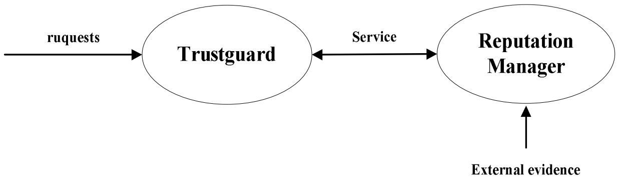


Figure 1. P-Trust's Architecture

This paper is supported by the National Natural Science Foundation of China (Contract No. 60873231); and Innovation Project for Postgraduate Cultivation of Jiangsu Province, China (Contract No. CX07B_109Z).

978-1-4244-5273-6/09/$26.00 ©2009 IEEE

The Trustguard module is responsible for monitoring the behaviors of other peers and determines whether the peer response to requests from others or not. Here, we can set a threshold to filter the requests (service and recommendation request) from untrustworthy peers. The threshold can be changed dynamically with the reputation system. Compared with the reputation systems without Trustguard, P-Trust can guard the requests from some unknown or malicious peers referring to local trust only.

All peers maintain local trust values of peers whom they have transacted with in the reputation manager. When a peer wants to get a kind of resource, it also needs to calculate service providers' reputation by second-hand information available. After having transacted with another peer, it updates another peer's trust value locally on the basis of the feedback. Additionally, we take measures to encourage true second-hand recommendation and punish dishonest information provider. We will describe the reputation system in detail in the following subsection.

B. Direct Observation

In this section, we describe our policy for computing direct trust on historical transactions. We compute direct trust values by Normal distribution $N(\mu, \sigma)$, where the μ indicates expected trust value of the service provider, and σ provides the degree of uncertainty to the trust value. Let R denote actual trust value of the target peer. Consequently, an ideal distribution of the trust value will be $N(\mu=R, \sigma\to0)$, if μ equals 0.7, statistically, it can be explained that the peer will provide honest service with a probability of 70%. Then using μ and σ, the model can characterize peer's direct trust in the eyes of one peer quite clearly.

We suppose that X is a set of discrete random variable, it follows Normal Distribution $N(\mu, \sigma)$. $\{X_1, X_2, X_3, ...X_n\}$ is a sample from X, where $X_i(i=1...n)$ denotes the evaluation of the i'th transaction. We use Moment Estimation to estimate expectation and variance of the Normal Distribution as follows:

$$\hat{\mu} = \bar{X} = \frac{1}{n}\sum_{i=1}^{n} X_i \qquad \hat{\sigma}^2 = \frac{1}{n}\sum_{i=1}^{n}(X_i - \bar{X})^2 \qquad (1)$$

We can see that $\hat{u}$ is the average of each trust value, and the formulas above don't pay attention to fading of trust values. So we add a weight $w(t)$ to each evaluation, direct trust value is calculated by the formula.

$$\hat{\mu} = \bar{X} = \frac{1}{n}\sum_{i=1}^{n} X_i * w(t) \qquad \hat{\sigma}^2 = \frac{1}{n}\sum_{i=1}^{n}(X_i * w(t) - \bar{X})^2 \qquad (2)$$

Here, each direct evaluation decays exponentially as:

$$w(t) = \rho^t, (0 < \rho < 1, t = 0...n) \qquad (3)$$

where ρ is a constant to show the degree of trust fading. Obviously, the weight $w(t)$ varies with time. There are two methods for trust fading. One method is that trust value fades by transaction times, and the other is that trust value decays over time. So t in (3) can be regarded as transaction times or a period of time. We find that the latter method is more reasonable than the former. For an instance, peer A has twice transactions with B, and only transacts with C once, each evaluation of A to B and C is described as Table I.

TABLE I. EVALUATION ON EACH TRANSACTION

Peer	The 1th period	The 2th period
B	0.8	0.8
C	0.8	N/A

Given ρ=0.9, we adopt the times decay in this situation, in peer A's eyes B's trust value is $\hat{u}$=0.76, and C's trust value is $\hat{u}$=0.8. C doesn't make any transactions in a certain period time with A but gets higher trust value than B.

C. Reputation Aggregation

Reputation management and trust evaluation not only can rely on every peer's own experience but also information aggregation recommended by others. In this way, we can collect more subjective trust values. If a querying peer Q tries to estimate the reputation of another peer C, and gets two items of feedback from A (denoted as f_A) and B (denoted as f_B) with A~$N(\mu_A, \sigma_A)$ and B~$N(\mu_B, \sigma_B)$ respectively. The estimation on the reputation of peer C(μ_C, σ_C) can be generated from the following equations.

$$\mu_C = \frac{\sigma_B}{\sigma_A + \sigma_B} * f_A + \frac{\sigma_A}{\sigma_A + \sigma_B} * f_B \qquad \frac{1}{\sigma_C^2} = \frac{1}{\sigma_A^2} + \frac{1}{\sigma_B^2} \qquad (4)$$

However, the simple strategy incurs some potential risks for abuse. Some peers can indirectly improve their reputation by debasing other peers. Generally, a peer should give more weight to the direct observation made by itself than the evidence obtained from other peers. Furthermore, the evidence from different peers should be weighed in proportion with their respective trust values. An approach [7, 11] is proposed, which is based on the concept of belief discounting. So our new expression for the reputation aggregation is defined as:

$$\mu_C = \frac{\sigma_B}{\sigma_A + \sigma_B} * f_A * \mu_A + \frac{\sigma_A}{\sigma_A + \sigma_B} * f_B * \mu_B \qquad (5)$$

We can see that some peers with higher trust values can be of greater influence than others with inferior trustworthiness. However, some peers with high trust values do not provide true information. For example, some malicious peers may achieve high trust values by disguising themselves to provide some good services, and giving untruthful recommendations to other peers. Therefore, similarity weight measure is discussed to cope with the problem.

Let $S(A)$ denote the set of peers that have interacted with peer A. The set of peers that interacted with peer A and B is denoted by $CS(A,B)=S(A)\cap S(B)$. To measure the evaluation similarity of peer A and B, peer A can calculate the evaluation similarity between A and B over the common set $CS(A,B)$. We consider the trust values scored by A and B over $CS(A,B)$ as two vectors. PeerTrust propose (6) to characterize the similarity $Sim(A,B)$, where f_{AK} denotes the trust value of peer A to K.

$$Sim(A,B)=1-\sqrt{\frac{\sum_{K\in CS(A,B)}(f_{AK}-f_{BK})^2}{|CS(A,B)|}} \tag{6}$$

There exists a cosine-based similarity algorithm to argue the trustworthiness of feedback information [12], as (7).

$$Sim(i,j)=\frac{\sum_{k\in CS(i,j)} f_{ik}*f_{jk}}{\sqrt{\sum_{k\in CS(i,j)} f_{ik}^2}*\sqrt{\sum_{k\in CS(i,j)} f_{jk}^2}} \tag{7}$$

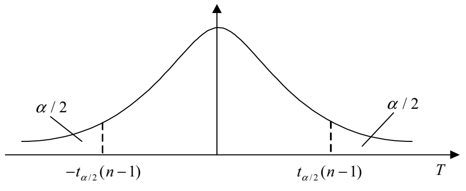
We adopt (7) to implement our approach, and the reputation of peer C is estimated finally as the formula.

$$\mu_C=\frac{\sigma_B}{\sigma_A+\sigma_B}*f_A*Sim(A,Q)+\frac{\sigma_A}{\sigma_A+\sigma_B}*f_B*Sim(B,Q) \tag{8}$$

D. Incentive and Punishment Mechanism

In order to restrain false feedbacks from other peers and urge peers to provide good quality of service and give real feedbacks, we also develop an incentive and punishment mechanism to update trust values. We regard the target peer's actual trust value as a benchmark. We can assume that there will be very few of peers give too higher or lower evaluations, that is, most of the evaluation values will be near the benchmark.

We use a probabilistic technique of interval estimation for T-Distribution to judge whether recommendation information is trustworthy or not. Let 1-α represent the confidence interval, $\bar{X}$ and S denote the expectation and variance from the samples. For the uncertainty of σ^2, we use S^2 as the unbiased estimation of σ^2 and conclude the result as follows:



$$\frac{\bar{X}-\mu}{S/\sqrt{n}}\sim t(n-1)$$

Figure 2. Distribution of feedbacks

We can get the interval estimation of μ with the confident interval 1-α in Fig. 2. Thus, the recommenders can be divided into two classifications, their trust values would be updated according to (9).

A: $f_{jk}\in\left(\bar{X}-\frac{S}{\sqrt{n}}t_{\alpha/2}(n-1),\bar{X}+\frac{S}{\sqrt{n}}t_{\alpha/2}(n-1)\right)$

B: except A.

$$\mu_j^{new}=\begin{cases}\mu_j+\eta*(1-\mu_j), & f_{jk}\in A\\ \mu_j-\theta*\mu_j, & f_{jk}\in B\end{cases} \tag{9}$$

Where η, θ can be adjusted dynamically according to the system. But it must make sure that $0<\eta<\theta<1$, because trust value should be hard to accumulate and easy to lose, so a misbehavior may cause a great decline of trust value. You can see from (9), if $f_{jk}\in A$, trust value of peer j will increase, but otherwise drop. In a reputation system, peers observe the behavior of other peers and update trust values by rewarding good behaviors and punishing spurious behaviors.

III. SIMULATION

We perform a set of simulations to evaluate the effectiveness and robustness of P-Trust and EigenTrust in the P2P file-sharing settings.

Peers are classified into three categories as shown in Table II. Good peers provide real files and true feedbacks. Ordinary peers offer files and feedbacks randomly. Malicious peers always supply spiteful files and feedbacks.

TABLE II. PEER CATEGORIES

Peer Type	File Quality	Feedback Accuracy
Good peer	Good	True
Ordinary peer	Random	Random
Malicious peer	Bad	False

There are 1000 peers and 10000 distinct files in our experiments. 100 random distinct files are assigned to each peer. We carry out 1000 times experiments with 5 downloads at a time. Table III shows some other parameters and default values.

TABLE III. SIMULATION PARAMETERS

Parameter	Description	Default
α	Size of unconfident interval	0.05
θ	Increase factor of trust value	0.02
η	Decrease factor of trust value	0.01

First of all, the percentages of good peer, ordinary peer and malicious peer are 30%, 60% and 10% respectively. We compare the ratio of file successful downloads under different conditions: (1) Scheme with NoTrust. There is no trust management countermeasure in P2P file-sharing. Each peer randomly selects a peer who has the demanded file by the file search algorithm. (2) Scheme with EigenTrust. In the case, each peer downloads files according to EigenTrust model. (3) Scheme with P-Trust. The number of experiment times was increased from 100 to 1000. We measure the ratio of the number of successful downloads to the total amount of downloads, as shown in Fig. 3.

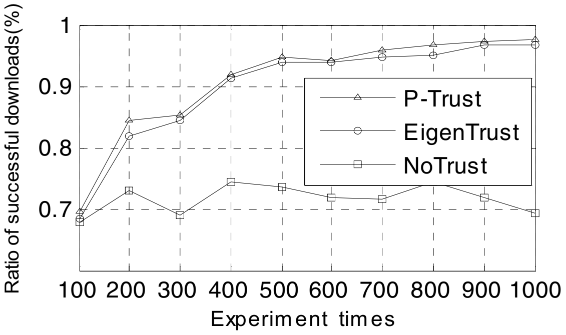


Figure 3. Ratio of successful downloads in three schemes

Nevertheless, the curve of P-Trust always stays at the top of the graph, which is a little higher than the curve of EigenTrust. After about 400 experiments, the ratio of successful downloads become higher than 90% and keep stable. On the other hand, the curve of NoTrust always stays at the bottom and remains horizontal approximately during the process of experiments.

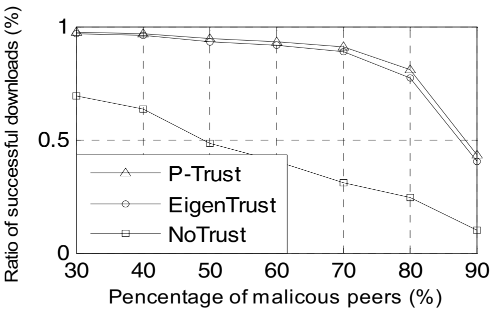


Figure 4. Ratio of successful downloads change with percentage of malicious peers

In this scenario, Peers are just divided into good peers or malicious peers. The percentage of malicious peers is varied in increments of 10% from 30% to 90%. We observe outcome of the ratio of successful downloads after 1000 downloads, as shown in Fig. 4. As the rate of malice becomes larger, the ratio of successful downloads about the three schemes all fall. The curve of P-Trust is always on top, and the curve of NoTrust descends quickly owing to the percentage of malicious peers on the increase. When the malicious percentage reaches 80%, our model of the ratio of successful downloads still holds 75%, and exceeds the ratios of EigenTrust and NoTrust. As a result, P-Trust is a more effective model to restrain malicious behaviors than EigenTrust.

IV. Conclusion

Our primary goal in the paper is providing a parameter-estimation approach to predict the trustworthiness of the peers in unstructured P2P networks. The method is to estimate others' future behaviors based on personal experiences and second-hand information. Moreover, incentive and punishment mechanism is taken to update trust values. We find that our model performs better than EigenTrust in the same simulation settings from many aspects, such as high successful downloads and low overhead.

Acknowledgment

This paper is supported by the National Natural Science Foundation of China (Contract No. 60873231), and Innovation Project for Postgraduate Cultivation of Jiangsu Province, China (Contract No. CX07B_109Z).

References

[1] D. Qiu, and R. Srikant, "Modeling and Performance Analysis of BitTorrent-Like Peer-to-Peer Networks," Proc. ACM Sigcomm,2004.

[2] W. W. Terpstra, J. Kangasharju, C. Leng, A. P. Buchmann, "BubbleStorm: Resilient, Probabilistic, and Exhaustive Peer-to-Peer Search," Proc. ACM Sigcomm, 2007.

[3] Y. Liu, Li Xiao, and Lionel M Ni, "Building a Scalable Bipartite P2P Overlay Network," IEEE Trans. Parallel and Distributed Systems,vol. 18, pp. 1296-1306, 2007.

[4] Y. Kulbak and D. Bickson, "The eMule Protocol Specification," Hebrew University Technical Report, TR-2005-03, Jan. 2005.

[5] J. A. Pouwelse, P. Garbacki, D. H. Epema, and H. J. Sips,"The BitTorrent P2P File-sharing System: Measurements and Analysis," 4th Int'll Workshop on Peer-to-Peer Systems (IPTPS'05), 2005.

[6] D. Hughes, G. Coulson, and J. Walkerdine, "Free Riding on Gnutella Revisited: The Bell Tolls?" IEEE Distributed Systems Online, vol. 6, June 2005.

[7] L. Xiong and L. Liu, "PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities," IEEE Trans. Knowledge and Data Eng., vol.16, no. 7, pp. 843-857, 2004.

[8] K. Aberer and Z. Despotovic, "Managing Trust in a Peer-2-Peer Information System," Proc. 10th Int'l Conf. Information and Knowledge Management, 2001.

[9] S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The Eigentrust Algorithm for Reputation Management in P2P Networks," Proc.ACM World Wide Web Conf. (WWW '03), May 2003.

[10] M. Srivatsa, L. Xiong, and L. Liu, "Trustguard: Countering Vulnerabilities in Reputation Management for Decentralized Overlay Networks," Proc. 14th Int'l World Wide Web Conf., pp. 422-431, 2005.

[11] Chang-yong Niu, Jian Wang, and Ruimin Shen, "A Trust-Enhanced Topology Adaptation Protocol for Unstructured P2P Overlays," Third International Conference on Semantics, Knowledge and Grid. Shan Xi, 2007, pp. 200-205.

[12] Jing-Tao LI, Yi-Nan JING, Xiao-Chun XIAO, Xue-Ping WANG, and Gen-Du ZHANG, "A Trust Model Based on Similarity-Weighted Recommendation for P2P Environments," http://www.jos.org.cn/1000-9825/18/157.htm, Jan. 2007 [Journal of Software, China, 2007, 18(1), pp.157−167.]