Int. J. Communications, Network and System Sciences, 2009, 3, 169-247
doi:10.4236/ijcns.2009.23025 Published Online June 2009 (http://www.SciRP.org/journal/ijcns/).

A Novel Approach to Improve the Security of P2P File-Sharing Systems

Cuihua ZUO, Ruixuan LI[+], Zhengding LU
College of Computer Science and Technology,
Huazhong University of Science and Technology, Wuhan, China
E-mail: *zuocuihua@smail.hust.edu.cn, {rxli,zdlu}@hust.edu.cn*
Received February 15, 2009; *revised April* 6, 2009; *accepted April* 16, 2009

ABSTRACT

The recent and unprecedented surge of public interest in peer-to-peer (P2P) file-sharing systems has led to a variety of interesting research questions. How to minimize threats in such an open community is an important research topic. Trust models have been widely used in estimating the trustworthiness of peers in P2P file-sharing systems where peers can transact with each other without prior experience. However, current P2P trust models almost take no consideration for the nature of trust, fuzzy, complex and dynamic, which results in low efficiency in resisting the attacks of malicious nodes. In this paper, a new trust model named NatureTrust that can alleviate the shortage brought by the nature of trust is proposed. In order to cope with the fuzzy characteristic of trust, linguistic terms are used to express trust. Additionally, fuzzy inference rules are employed to evaluate trust of each transaction so as to handle the complex characteristic of trust. Furthermore, risk factor is deployed into NatureTrust to represent and reason with the dynamic characteristic of trust. Both risk and trust factors are considered in evaluating the trustworthiness of each peer. Experimental results show that the trust model analyzed here thus stands against malicious act effectively.

Keywords: Peer-to-Peer (P2P), File-Sharing, Security, Risk, Trust Model, Fuzzy Inference

1. Introduction

In peer-to-peer (P2P) file-sharing systems, all peers are both users and providers of resources and can access each other directly without intermediary agents. Typically, peers are autonomous, anonymous and self-interested, which means individuals seek to maximize their own goal achievement rather than act in a benevolent manner. Consequently, security becomes an open problem in these large and distributed systems since peers can break their commitments or provide sub-standard or even malicious services. Though trust models, like EigenTrust [1] and PeerTrust [2,3], can be used to help P2P systems deal with the security problem, they do not consider the nature of trust: fuzzy, complex and dynamic characteristics [4]. Hence, they can not achieve a preferable effect.

The three types of natural characteristics of trust are as follows. 1) Fuzzy characteristic: the fuzzy nature of trust means it is imprecise and sometimes ambiguous when we express trust or try to explain a trust level. 2) Complex characteristic: the complex nature of trust arises from the fact that there are multiplicity of ways in determining the trust and a variety of views about trust. 3) Dynamic characteristic: the dynamic nature of trust refers to trust not being constant or stable but always changing as time passes. However, Current research seldom considers these three characteristics of trust in peer-to-peer file-sharing systems.

The ultimate goal of our research is to solve the security problem effectively in distributed P2P file-sharing systems, which is incurred by the nature of trust: fuzzy, complex and dynamic. Towards the end, NatureTrust, a new trust model is proposed, which introduces linguistic terms instead of numerical values to express trust and imports fuzzy inference rules to infer trust value of each transaction. The risk factor is also taken into account when evaluating the trustworthiness of each peer.

The rest of this paper is organized as follows. The introduction of related work about trust models is provided in Section 2. Section 3 presents a new trust model which

[+]Corresponding author. E-mail: rxli@hust.edu.cn.

considers risk factor and trust factor separately in order to alleviate the security issues aroused by malicious peers in P2P networks. This section explains how to express trust, how to apply fuzzy inference rules into trust evaluation, and how to compute risk value. In addition, this section also describes the implementation strategies of this new trust model. Then Section 4 evaluates the performance of the proposed trust model with simulation experiments, followed by the conclusion and future work in Section 5.

2. Related Work

In Peer-to-Peer networks, peers cooperate to perform a critical function in a decentralized manner. Among the heterogeneous peers, some might be honest and provide high-quality service, some might be buggy and unable to provide high-quality service, some might be even malicious by providing bad services or harming the consumers. In the current P2P file-sharing systems, there are mainly three types of malicious peers: simple malicious peer, traitor and hypocritical peer.

In order to cope with such malicious behavior, some reputation-based P2P trust models have been proposed. As is well known, centralized reputation systems has been widely applied in e-commerce [5,6], such as eBay [7]. Some researches [8,9,10] suggested reputation based systems as an effective way for protect the P2P network from possible abuses by malicious peers. Reputation systems can help peers establish trust among them based on their past behaviors and feedbacks. Let us see several prominent decentralized reputation systems in the P2P domain. [11,12] proposes a reputation-based approach for P2P file sharing systems (called P2PRep). P2PRep runs in a fully anonymous P2P environment, where peers are identified using self-assigned opaque identifiers. [13] presents a similar approach, called XRep, which extends P2Prep by considering the reputations of both peers and resources. P2PRep and XRep do not consider the credibility of voters. Hence, malicious peers can give bad votes to an honest peer or give good votes to a dishonest peer, which results in a significant decline in the performance of restraining malicious behavior.

EigenTrust is also a reputation-based approach for P2P file sharing systems. In EigenTrust, each peer is assigned a unique global reputation value. However, it is not clear if their approach is feasible for large-scale P2P systems, in which some local reputation values are unreachable for the requesting peers. [14] suggests an approach to trust management for semantic web which is similar to EigenTrust, but ratings are personalized for each user based on his personal experience. Both approaches simply assume that peers are honest and therefore cannot defend some attacks like deceptions and rumors. PeerTrust develops a P2P trust model, so that peers can quantify and compare the trustworthiness of other peers and perform trusted interactions based on their past interaction histories without trusted third parties.

PET [15] proposes a personalized trust model to help the construction of a good cooperation, especially in the context of economic-based solutions for the P2P resource sharing. It designs a risk evaluation to handle the dramatic spoiling of peers. However, only denoting the opinion of the short-term behavior, the risk evaluation does not react on the dynamic nature of trust totally. Unlike the above, the risk evaluation in our trust model represents the fluctuating of peers' trust in the past behavior. In [16,17], ECMBTM is proposed which use cloud-model [18] to model trustworthiness and uncertainty of trust relationships between peers. But the trust aggregation is so complex that it's hard to apply it to practice.

Our work is inspired by these previous works for reputation-based P2P trust models and benefits from the nature of trust. But there are some differences between our effort and the above reputation systems. Firstly, in this paper, we focus on both risk and trust two aspects in evaluating the trustworthiness of peers. In addition, we use linguistic terms to express trust and employ fuzzy inference rules to evaluate trust of each transaction. More importantly, neither of the above reputation systems addresses the strategic behavior by malicious peers.

3. Trust Model

Trust is an accumulative value for the past behavior and reflects the overall evaluation on the valued peer. However, it is not sensitive enough to perceive the suddenly spoiling peer because it needs time to decrease the accumulative score. Meanwhile, it is also hard to perceive traitors who may behave properly for a period of time in order to build up a strongly positive trust, and then begin defecting. What's worse, it is harder to perceive the malicious peers with strategically altering their behavior. Therefore, trust is not enough in evaluating the actions of peers due to its dynamic characteristic.

When a peer involves in a transaction, it is entering into an uncertain interaction, which has an associated risk of failure or reduced performance. For security, the trust model need take risk factor into account. Hence, the main focus of this paper is the design of NatureTrust that is a unique characteristic with the combination of trust and risk factors for evaluating the trustworthiness of peers in P2P file-sharing systems. Here, we use a two-tuples with trust and risk values Tr: (T, R) to express the trustworthiness of peers. Additionally, each peer stores the values of trust and risk of its acquaintances using a XML document. Peers can change their XML documents to achieve some recommendation information.

3.1. Evaluation of an Interaction

Trust is fuzzy and complex when we express it. In P2P file-sharing systems, it is hard to give an accurately nu-

merical value after an interaction, and peers can have different views or policies in evaluating trust, which throws the trust evaluation system into disorder. For instance, one generous peer gives a trust value 0.9 to a certain service, while another one just gives 0.5 to it. Meanwhile, the situation occurs a lot if peers give precise trust values just in accordance with their own standards. In this situation, some malicious peers are easy to give unreasonable evaluations purposely, which may exaggerate the credibility of their conspirators or slander that of the benevolent peers. Besides, the trust evaluation can derive from different measurement criteria, such as "quality", "speed" and so on. This means a trusting agent is hard to explicitly articulate and specify a trust value that he or she has in another trusted agent after a transaction. Therefore, how to evaluate trust value for each transaction becomes an important problem.

In this section, we deal with different measurement criteria of evaluating trust by introducing linguistic terms and fuzzy inference rules. Concretely, we first define the set of measurement criteria for evaluating trust and give different grades for each measurement criterion according to user's satisfaction degree. Furthermore, we classify trust into different grades and establish a series of inference rules from the grades of measurement criteria to the grade of trust, and then use these rules to infer trust grade of each transaction. Finally, we define a map function *h* that maps from each trust grade to a corresponding trust value for each transaction.

Definition 1: Supposing that the set of linguistic terms about the trust grades is $X=\{x_1,x_2,\ldots,x_N\}$, and the set of trust value is $Y=\{y_1,y_2,\ldots,y_N\}$, $Y\subset [0,1]$, where N is the number of the trust grades. The function h(x) maps each element $x_i\in X$ into a value $y_i\in Y$, $h: X\to Y$. So y_i is the corresponding trust value of the trust grade x_i.

For example, we define N=6, X={distrust, a little trust, ordinary trust, a lot of trust, extraordinary trust, absolute trust}, Y={0,0.2,0.4,0.6,0.8,1}. The map function h can be defined as below:

$$h(x)=\begin{cases}1 & (x=\text{"absolute trust"})\\ 0.8 & (x=\text{"extraordinary trust"})\\ 0.6 & (x=\text{"a lot of trust"})\\ 0.4 & (x=\text{"ordinary trust"})\\ 0.2 & (x=\text{"a little trust"})\\ 0 & (x=\text{"distrust"})\end{cases} \quad \textbf{(1)}$$

In this paper, we assume C={C1,C2,…,Cm} as the set of m different measurement criteria, and for each measurement criterion Ci, there is a corresponding set to describe its grade, such as Ci: $\{c_1,c_2,\ldots,c_k\}$. For example, aiming at the service of file download, users can evaluate trust according to two criteria-file quality and download speed, so the set C can be defined as {file quality, download speed}. The set Q={bad quality, normal quality, good quality} can be regarded as the grade of the criterion "file quality" and the set S={slow speed, normal speed, fast speed} that of the criterion "download speed".

Since fuzzy inference is good at handling imprecise inputs, such as assessments of quality or speed, and allows inference rules to be specified by imprecise linguistic terms, such as "good quality" or "slow speed", we use fuzzy inference rules to combine the appraising information from different aspects of trust. The basic form of fuzzy inference rules is as follows:

If C1 is c_1 **and** C2 is c_2 … **and** Cm is c_m
then T is x.

Also using the above example, we might have rules such as the following.

If "file quality" is "good quality" **and** "download speed" is "fast speed"
then trust appraisement is "absolute trust".
If "file quality" is "good quality" **and** "download speed" is "normal speed"
then trust appraisement is "extraordinary trust".

Thus, after a transaction between peer i and peer j, peer i will give the appraisement like this: "good quality" and "normal speed". Through the above rules, we can infer that trust appraisement is "extraordinary trust". Similarly, according to the map function h(x) in the above, the trust value of peer j in view of peer i based on this direct interaction with peer j is 0.8.

3.2. Trust Computation

In this section, we present a general trust metric that combines the direct and indirect factors into a coherent scheme to compute the overall trust value.

Definition 2: we define $t_{ij}^{(n)}$ as the trustworthy of peer j in view of peer i in the n-th direct transaction. The value of $t_{ij}^{(n)}$ can be gained according to the inference method described in Subsection 3.1.

Definition 3: We define t_{ij} as the reliability of peer j in view of peer i based on its direct interactions with peer j.

$$t_{ij}=\frac{\sum_{n=1}^{M} t_{ij}^{(n)} * (1-\mu)^{M-n}}{\sum_{n=1}^{M}(1-\mu)^{M-n}} \quad \textbf{(2)}$$

where μ ($0<\mu<1$) is a time declining constant, and it determines the weights given to the most recent past observations. The bigger μ is, the faster the past observation is forgotten. M is the total number of direct interactions between i and j.

Definition 4: we define r_{ij} as the total recommendation from other peers who has even transacted with peer j.

$$r_{ij}=\lambda*\frac{\sum_{1}^{m} t_{il} * t_{lj}}{\sum_{1}^{m} t_{il}}+(1-\lambda)*\frac{\sum_{1}^{g} t_{zj}}{g} \quad \textbf{(3)}$$

The first part in the above formula is the recommendation from trustworthy references which have transactions with peer i, and the second part is the recommendation from unknown references. m and g are the number of trustworthy references and the number of unknown references respectively. l and z denote the peers of trustworthy references and unknown references respectively. λ is the weight to indicate how the peer i values the importance of the recommendation from trustworthy references and from unknown references. Certainly, comparing to unknown references, the peers who have even transacted with i is more trustworthy. So λ is bigger than 0.5 normally.

Definition 5: we define T_{ij} as the reliability of peer j in view of peer i based on its direct interactions and other peers' recommendation.

$$T_{ij} = w * t_{ij} + (1-w) * r_{ij} \quad \textbf{(4)}$$

From the definitions above, T_{ij} is decided by two factors. One is the reliability of peer j in view of peer i based on its direct interactions with peer j. The other is the total recommendation of peer j from other peers. As we known, peers always trust in themselves than others' recommendation, so w is bigger than 0.5.

3.3. Risk Computation

Peer's behavior can change dynamically, which implies that we need rely on not only the trust factor to evaluate the trustworthiness of peers, but also the risk factor. In NatureTrust, we use entropy of information theory to quantify the risk of each transaction between two peers. In information theory, entropy expresses the uncertainty degree of information. The smaller the entropy is, the lower the uncertainty degree is.

In this paper, the calculation of risk is based on the trust values from the direct interactions in the past which is reliable and self-determined, for risk is used to describe the fluctuation of peers' actions.

Definition 6: We define R_{ij} as the risk value of peer j in view of peer i. The formula of calculating risk value is as follows.

$$R_{ij} = \begin{cases} \dfrac{1}{\log N} * H_{ij} & (M \geq N) \\ R_0 & (M < N) \end{cases} \quad \textbf{(5)}$$

$$H_{ij} = -\sum_{k=1}^{N} p_{ij}^{k} * \log(p_{ij}^{k}) \quad \textbf{(6)}$$

In the above formulae, N is the total number of the classification of trust grades, and H_{ij} is the value of entropy relying on p_{ij}^{1}, p_{ij}^{2}, …, p_{ij}^{N}, which express the probability of N different trust grades appearing in M times direct interactions between peer i and j respectively. R_0 is the initialization value of risk. From the Equation (6), we can educe $0 \leq H_{ij} \leq \log N$, thus $0 \leq R_{ij} \leq 1$.

For example, we also suppose that the trust degree is classified into 6 grades, such as {distrust, a little trust, ordinary trust, a lot of trust, extraordinary trust, absolute trust}, and the corresponding set of trust values is {0, 0.2, 0.4, 0.6, 0.8, 1}. Assuming peer i and j have 10 times transactions in the past and the trust values are {0.6, 0.8, 0.6, 0.4, 0.6, 0.8, 0.8, 0.4, 1, 0.6}, then the probability p_{ij}^{1}, p_{ij}^{2}, …, p_{ij}^{6} are 0, 0, 0.2, 0.4, 0.3, 0.1, respectively. Hence, the values of entropy and risk can be computed according to the above formulae: H_{ij}=−(0.2*log0.2 + 0.4*log0.4 + 0.3*log0.3 + 0.1*log0.1)=0.556, $R_{ij} = H_{ij}$/ log6=0.715.

3.4. Managing Data

Figure 1 gives a sketch of evaluation mechanism for NatureTrust. There is no central database. The data that are needed to compute the trust value and risk value for peers are stored across the network in a distributed manner. Each peer has a data manager that is responsible for trust evaluation and risk evaluation.

The data manager of each peer performs two main functions. On the one hand, it submits recommendation information for other peers. On the other hand, it is responsible for evaluation the peer's trustworthiness. This task is performed in trust and risk two aspects. In risk aspect, the peer only relies on its own direct trust values to computer the risk value. These direct trust values derive from measurement criteria of trust, trust grades, inference rules and mapping function, which described in Subsection 3.1. In trust aspect, the peer needs to collect trust data from other peers in the network, and then combines direct trust to compute the total trust value. Hence, each peer need store the information of trust grades, measurement criteria of trust, inference rules, trust values of direct transactions and mapping function.

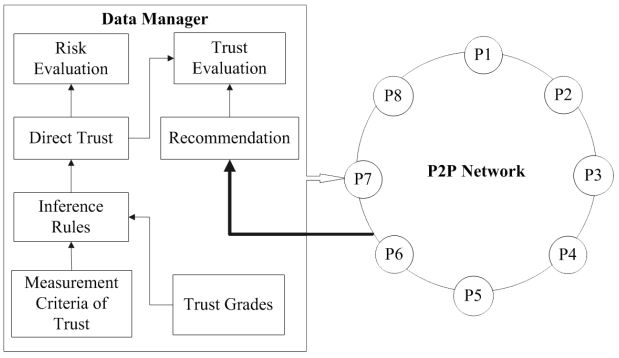

Figure 1. NatureTrust architecture.

3.5. Peer Selection Scheme

A key objective of peer selection scheme is to select one peer or a subset of peers that is or are most qualified to provide service in terms of the trustworthiness. The trust and risk values can help peers to form a trust action on other peers and compare the trustworthiness of a set of peers. A higher trust value T_{pq} and a lower risk value R_{pq} indicate that peer q is more trustworthy in view of peer p in terms of the collection evaluation from other peers and its direct transactions with peer q.

There are two usages of the trust and risk values in P2P file-sharing systems. First, a peer p can rely on a pair of trust and risk values with another peer q to determine whether to perform the next transaction with peer q. Assuming T_{pq} and R_{pq} are the trust value and the risk value of peer q in view of peer p, respectively. A simple rule for peer p to form a trust action on peer q can be $T_{pq} \geqslant T_{threshold}(p)$ and $R_{pq} \leqslant R_{threshold}(p)$, where $T_{threshold}(p)$ and $R_{threshold}(p)$ are the trust threshold value and the risk threshold value for peer p to trust other peers, respectively. The factors that determine these two threshold values include the extent to which peer p is willing to trust others, the importance of the sharing files in peer p. For example, a good file may own both higher trust threshold value and lower risk threshold value. More complex decision rules can be applied, but are not our focus in this paper.

The second usage is to compare the trustworthiness of a list of peers. For example, a peer who issues a file download request can first choose a set of potential peers from the peers who respond to this request according to its two threshold values. Then, it can compare the trustworthiness of the potential peers based on their trust and risk values and select the optimal peer to download the file. By doing this, it can reduce the risk of downloading inauthentic or corrupted files from untrustworthy peers. However, how do we compare the trustworthiness of two potential peers – one with higher trust value, but the other with lower risk value? Hence, we need strike a good balance between trust and risk. For example, if we give the same weight to them, the peer who with the bigger value of (T - R) will be regarded more credible, where T denotes trust value and R means risk value.

From the above analysis, we can see that the peer that has the biggest trust value will not be the optimal choice to provide service all the time. When a peer is suddenly spoiling or intermittently spiteful, although the peer may have a strongly positive trust by a large number of good transactions in the past, its risk is also increase obviously because of the fluctuation of its actions. Hence, the security of systems can be improved effectively by introducing risk factor.

4. Performance Evaluation

We perform a series of experiments to evaluate the NatureTrust approach and show its effectiveness and robustness against different malicious behaviors of peers.

4.1. Simulation Setup

We use the simulator PeerSim [19] for evaluating the performance of NatureTrust. In our simulation, we use BRITE [20,21] to generate P2P network with 100 peers, and the average number of links of each node is 2. We distribute 100 files to these 100 peers and each peer has about 10 different files. In other words, each file has about 10 replicas. We split peers into two types, namely, good peers and malicious peers. The percentage of malicious peers is denoted by k. The behavior pattern for good peers is to always cooperate in transactions, while malicious peers' behavior pattern depends on their types. In this paper, we mainly discuss three types of malicious peers: simple malicious peer who may deceive other peers at random, traitor who may behave properly and attain a high trust for a period of time, but begin defecting suddenly, hypocritical peer who may strategically alter its behavior in a way that benefits itself such as starting to behave maliciously with a certain probability after it builds up a strongly positive trust.

In our simulation, we classify trust grade into 6 types which has been introduced in Subsection 3.1, and the trust criteria are "file quality", "download speed" and "respond time". All peers use the same inference rules which will not be listed here in detail. Besides, in peer selection scheme, we give the same weight to trust and risk.

For each experiment in the following, the experiment environment is initialized by performing 1000 transactions among peers randomly. Then, each peer initializes its trust and risk threshold values according to its own situation. For example, the peer with high trust value can set high trust threshold value for its sharing files, while the peer with low trust value can set low trust threshold value for its sharing files. Finally, every peer, in turn, issues a request for some file to the community until the number of transactions achieves 6000. Important to note that if a peer who initiates a request for some file can not locate an appropriate peer to do transaction, the peer will give up this request and the next request from another peer will be initiated.

For comparison purpose, we also simulate XRep, PeerTrust and PET trust models. In distributed environment, an important issue is increasing the ratio of successful transaction, so we attend to compare our model with XRep, PeerTrust and PET against three types of malicious attacks. All experiment results are averaged over three runs of the experiments. Table 1 summarizes

the main parameters related to the community setting and the computation of trust and risk values. The default values are also listed.

Definition 7: Let TSR denotes transaction successful ratio which is the ratio of the number of successful transactions over the number of total transactions. Nt represents the number of total transactions and Ns denotes the number of successful transactions.

$$TSR = \frac{Ns}{Nt} \quad (7)$$

We use this metric to estimate the effectiveness of trust models against the behavior of malicious peers. The greater TSR is, the more effective the model is.

4.2. Effectiveness against Malicious Peers

In the first set of experiments, we study the transaction success rate with regard to the number of transactions under the attack of simple malicious peers. As to our data set used in experiments, we test different rate (r=0.25,0.5,0.75) of a malicious peer acting maliciously and the result is shown in Figure 2. From the figure we can see, in addition to XRep, the other three approaches have the similar transaction success rate. This is because, even if the computed trustworthiness of peers do not reflect accurately the uncertainty of the peers being cooperative, but they indeed differentiate good peers from simple malicious peers in most cases by the ranking of trust value. XRep is less efficient than other approaches, for it does not consider the credibility of voters. Furthermore, we also observe that the bigger the rate r is, the faster the malicious peers are exposed. Accordingly, the growth of success rate is quicker.

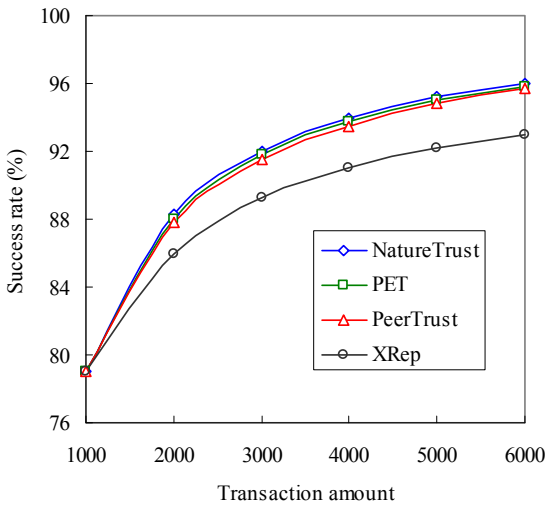

Figure 2. Compare success rate under the attack of simple malicious peers.

The second experiment (Figure 3) shows the variation of the transaction success rate with the increase of transaction amount under the attack of traitors. In this experiment, we presume the malicious peers start deceiving behavior once their trust value is bigger than T_θ=0.8. In this figure, we see an obvious superiority of the transaction success rate in PET and our approach with risk factor. This confirms that supporting risk is an important feature in a P2P community as peers can able to avoid the attack of suddenly spoiling peers. Moreover, another observation is that the success rate firstly decreases, and then increases as the increase of transaction amount. The reason is as follows. At the beginning, malicious peers almost act kindly in order to improve their trust value. Once their trust value is big enough, they can start deception. Hence, the success rate firstly decreases. However, as the malicious peers behaving maliciously, they expose themselves gradually, so the success rate increases subsequently.

In the third experiment (Figure 4), we discuss the variation of the transaction success rate as the number of transaction increasing from 1000 to 6000 under the attack of hypocritical peers. In this experiment, we presume the hypocritical peers strategically alter its behav-

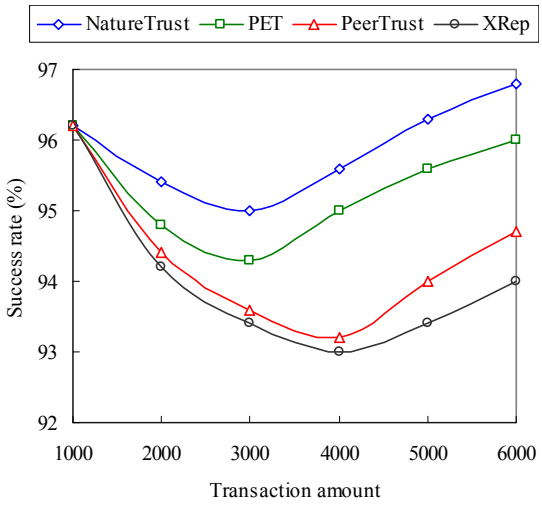

Figure 3. Compare success rate under the attack of traitors.

Table 1. Simulation parameters.

Parameter name	Parameter description	Default value
P	The number of peers in the community	100
k	The percentage of malicious peers	30%
F	The number of files	100
S	The number of replicas for each file	10
N	The number of trust grades	6
R_0	The initial value of risk	0.4
w	The weight factor	0.7
μ	Time declining constant	0.2
λ	The weight factor	0.8

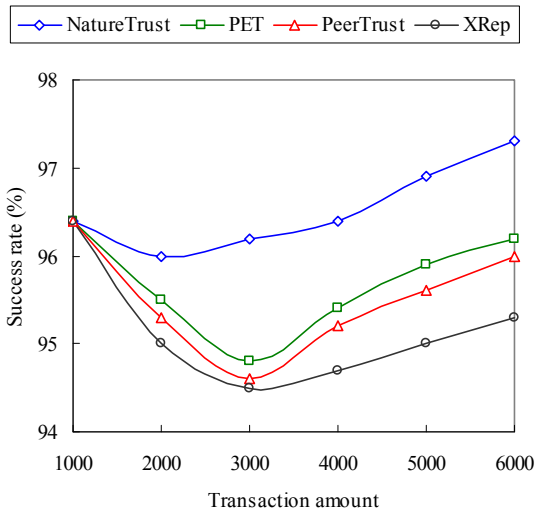

Figure 4. Compare success rate under the attack of hypocritical peers.

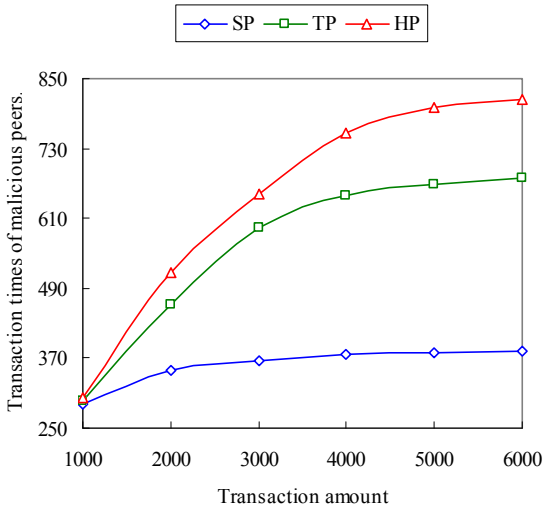

Figure 5. The benefit of isolating malicious peers.

ior in the way that they start to behave maliciously with a certain probability Pr=0.3 after it builds up a strongly positive trust value T_α=0.85. It is clear that the gain of the transaction success rate in NatureTrust is more obvious than that of the other three approaches, which illuminates that the evaluation of peers' trustworthiness in NatureTrust is more effective than others against the attack of hypocritical peers.

In Figure 5, we show the variation of the transaction times of malicious peers as the gain of transaction amount under the attack of three types of malicious peers using our trust model, where SP denotes simple malicious peers with r=0.5, TP denotes traitors with T_θ=0.8 and HP means hypocritical peers with T_α=0.85 and Pr=0.3. We can see that the growth of transaction times of malicious peers nearly stops when the total transaction amount is bigger than 5000 under the attack of three types of malicious peers. This means that three types of malicious peers are isolated quickly in our approach. Therefore, our trust model is beneficial to restraining the malicious behavior of peers.

5. Conclusions

In this paper, we analyze the nature of trust. We apply linguistic terms to express trust and employ fuzzy inference rules to evaluate trust. The fuzzy inference adopted in this paper restrains the unfair appraisements to some extent, for peers can obtain trust values according to the same inference rules. Thus, the security of the system is improved. Furthermore, risk factor is deployed to reason with the dynamic characteristic of trust. The application of the risk scheme aims to solve the security problems, such as traitor and hypocritical behavior, for the risk value increases as soon as the peer defects. Though its trust value can't decrease obviously, we can also detect the malicious act relying on risk value. In the end, the experiments show that the proposed trust model is more efficient than XRep, PET and PeerTrust.

As for our future work, we will continue to perfect the NatureTrust. We will consider other cheating or vicious behaviors in P2P file-sharing systems, and further research other methods to detect such behaviors.

6. Acknowledgements

This work is supported by the National Natural Science Foundation of China (60403027, 60773191, 60873225), the National High Technology Research and Development Program of China (863 Program) (2007AA01 Z403).

7. References

[1] 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 World Wide Web Conference, pp. 640–651, 2003.

[2] L. Xiong and L. Liu, "A reputation-based trust model for peer-to-peer e-commerce communities," in Proceedings of the IEEE International Conference on E-Commerce, 2003.

[3] L. Xiong and L. Liu, "PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities," in Proceedings of IEEE Transactions on Knowledge and Data Engineering, Vol. 16, No. 7, pp. 843–857, 2004.

[4] E. J. Chang, F. K. Hussain, and T. S. Dillon, "Fuzzy nature of trust and dynamic trust modeling in service oriented environments," in Proceedings of the 2nd ACM

Workshop on Secure Web Services (SWS'05), Fairfax, Virginia, USA, 2005.

[5] D. W. Manchala, "E-commerce trust metrics and models," IEEE Internet Computing, Vol. 4, No. 2, 2000.

[6] L. Xiong and L. Liu, "A reputation-based trust model for peer-to-peer e-commerce communities," in Proceedings of the IEEE Conference on E-Commerce, June 2003.

[7] P. Resnick and R. Zeckhauser, "Trust among strangers in Internet transactions: Empirical analysis of eBay's Reputation system," in Proceedings of NBER Workshop on Empirical Studies of Electronic Commerce, 2000.

[8] F. Cornelli, E. Damiani, S. D. C. di Vimercati, S. Paraboschi, and P. Samarati, "Choosing reputable servents in a P2P network," in Proceedings of the 11th World Wide Web Conference, 2002.

[9] E. Damiani, S. Vimercati, S. Paraboschi, P. Samarati, and F. Violante, "A Reputation-based approach for choosing reliable resources in peer-to-peer networks," in Proceeding of CCS, 2002.

[10] S. Kamvar, M. Schlosser, and H. Garcia-Molina, "EigenTrust: Reputation management in P2P networks," in Proceedings of the 12th WWW Conference, 2003.

[11] F. Cornelli, E. Damiani, S. D. C. di Vimercati, S. Paraboschi, and P. Samarati, "Choosing reputable servents in a P2P network," in Proceedings of the 11th International World Wide Web Conference, pp. 376−386, 2002.

[12] E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, and P. Samarati, "Managing and sharing servents' reputations in P2P systems," in proceedings of IEEE Transactions on Knowledge and Data Engineering, pp. 840−854, 2003.

[13] E. Damiani, S. D. C. di Vimercati, S. Paraboschi, P. Samarati, and F. Violante, "A reputation-based approach for choosing reliable resources in Peer-to-Peer networks," in Proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 207−216, 2002.

[14] M. Richardson, R. Agrawal, and P. Domingos, "Trust management for the semantic web," in Proceedings of the 2nd International Semantic Web Conference, pp. 351−368, 2003.

[15] Z. Q. Liang and W. S. Shi, "PET: A personalized trust model with reputation and risk evaluation for P2P resource sharing," in Proceedings of the 38th Hawaii International Conference on System Sciences, 2005.

[16] G. W. Zhang, J. H. Kang, and R. He, "Towards a trust model with uncertainty for e-commerce systems," in proceedings of the IEEE International Conference on e-Business Engineering, 2005.

[17] R. He, J. W. Niu, and K. Hu, "A novel approach to evaluate trustworthiness and uncertainty of trust relationships in Peer-to-Peer computing," in proceedings of the 5th International Conference on Computer and Information Technology (CIT'05), 2005.

[18] D. Y. Li, "The cloud control method and balancing patterns of triple link inverted pendulum systems," Chinese Engineering Science, Vol. 1, No. 2, pp. 41−46, 1999.

[19] PeerSim: A peer-to-peer simulator. http://peersim. source forge.net/.

[20] BRITE, http://www.cs.bu.edu/brite/, 2007.

[21] A. Medina, A. Lakhina, I. Matta, et al., "BRITE: Universal topology generation from a user's perspective," Technical Report BUCS-TR-2001-003, Boston University, April 2001.

