

DynamicTrust: Three-Dimensional Dynamic Computing Model of Trust in Peer-to-Peer Networks

Fengming Liu

School of Management and
Economics,
Shandong Normal University
No.88 Wenhua Road(E.), Jinnan
Shandong Province, P.R. China
86+531+86180509
liufm69@163.com

Wenyin Zhang

Information School,
Linyi Normal University
Linyi, Shandong, P.R.China
86+539-2060257
zwyxrx@163.com

Yongsheng Ding

College of Information Sciences
and Technology,
Donghua University
No. 2999, Renmin Road (N.)
Songjiang, Shanghai P.R. China
86+21+67792323
ysding@dhu.edu.cn

Xiyu Liu

School of Management and
Economics,
Shandong Normal University
No.88 Wenhua Road(E.), Jinnan
Shandong Province, P.R. China
86+531+86180509
sdxyliu@163.com

Mingchun Zheng

School of Management and
Economics,
Shandong Normal University
No.88 Wenhua Road(E.), Jinnan
Shandong Province, P.R. China
86+531+86180509
zhmc163@163.com

Yu Liu

Department of commerce,
Jinan Technology College
No.48 Maanshan Road(E.), Jinnan
Shandong Province, P.R. China
86+531+86301137
Mrliu73@126.com

ABSTRACT

With the application of peer-to-peer network, how to promote cooperation between peers has gotten more and more important. Most of traditional security technologies can not be applied in P2P network very well to promote the cooperation because of the special characteristics of P2P network such as openness and anonymity, etc. Trust has been proven to be essential to enforcing cooperative behavior in peer-to-peer networks. Trust relationship depends on trustee's trustworthiness. So, in this paper, we present a three-dimensional computing model of dynamic trust to try to find a way to address the problem. Firstly, we give a three-dimensional computing model of trust and make a dynamics analysis to trust of peer. Next, considered the new peer without trustworthiness can not do anything almost, we propose an algorithm of initial trustworthiness based on the new peer's abilities. To compute the direct trustworthiness and the recommended trustworthiness, we colligate the time as a dynamic factor. Finally, based on the trustworthiness computed by trust fusion algorithm, we present a mechanism of making trust decision to promote cooperation. The simulation results have showed that our model can enhance the cooperation between peers and avoid the malicious peers from destroying behaviors.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
GEC'09, June 12-14, 2009, Shanghai, China.
Copyright 2009 ACM 978-1-60558-326-6/09/06...\$5.00.

Categories and Subject Descriptors

C.2.0 [Computer-Communication Networks]: General—
Security and protection

General Terms

Security, Design, Algorithms.

Keywords

Peer-to-Peer Networks; Trust Management System

1. INTRODUCTION

Peer-to-Peer network becomes a new prevalent architecture which offers ideal and immense environments for resources sharing and distributed computing in the Internet. It is a distributed system with no centralized control. Each peer in the system has similar functionalities and plays the same role of a server or a client. And, participating peers can sign in and out at will. This "open" structure has many advantages [1]: adaptation, self-organization, load-balancing, fault-tolerance, availability through massive replication and the ability to pool together and harness large amounts of resources. As more and more users have powerful processors, large storage spaces and fast network connections, more peers seek to coordinate these resources for common goals. In the P2P system, each peer is owned and operated by an independent peer, and the peers collectively form a self-organizing, self-maintaining network with no central authority [2]. As a result, P2P system performance is highly dependent on the amount of voluntary resource contribution from the individual peers. There is no central authority because of their unique decentralized nature to dictate the rules for peer interaction and that interaction often occur among previously unknown peers, so peers might maliciously behave and harm others in the system [3].

For example, within a file sharing application, a malicious peer could provide infected files to compromise the integrity of those who download and open these files [4]. Therefore, one of the fundamental challenges for open and decentralized P2P systems is the ability to manage risks involved in interacting and collaborating with previously unknown and potentially malicious peers.

Trust is a fundamental factor in human relationships enabling collaboration and cooperation to take place. In human-human interaction, a great deal of information, such as gestures, facial expressions, relationship to other people and objects in the vicinity, and shared histories are all used as cues to assist in understanding the explicit communication. These shared cues, or context, help to facilitate grounding between participants in an interaction. Trust is a good way of motivating cooperative actions, which has been recently suggested as an effective security mechanism for open environments such as P2P networks and mobile Ad Hoc networks, and considerable research has been done on modeling and managing trust to improve security [5-8] and to promote node cooperation [9-12].

As shown by existing works, such as [13-15], reputation-based trust management systems can successfully mitigate this risk by computing the trustworthiness of a certain peer from that peer's behavior history. That is, they demand a high number of interactions before a change of behavior is reflected in the computed trust value. However, the trust computation metrics employed by the existing systems do not provide adequate reaction to quick changes in peers' behavior [16]. Moreover, malicious peers could even oscillate between periods of building and "milking" the reputation [15, 17].

Peers in large interactions are concerned with the results of the particular interactions in which they participate. They are also interested in their own reputation. Usually, dyadic relations are embedded in a network of relations with overlapping sets of peers. These overlaps create dependencies between the relations. A prime example is provided by P2P networks that allow for reputation effects: A peer has to take into account not only the partner's responses to his behaviors, but also how his behavior affects his reputation with other peers that are relevant to him. In recent years, many empirical and theoretical studies [18-26] have addressed the effects of reputation on the behavior of peers in cooperation problems called trustworthiness evaluation. However, in these works, there are some problems. First, the trustworthiness of the new peer that just joins the network has no evidences to be computed. This problem makes the good peer to share resources into dilemma. Secondly, most parts of those works make use of the records of interaction between peers to compute trustworthiness of peer. The problem is those model did not make different old records from new records. Time should be considered into the evaluation of peer's trustworthiness. Thirdly, the recommended trustworthiness relies on the recommendations information of peer's neighbors. No model considers the recommendation path, and even its length. More, the context of peer should be taken into account in the computation of trustworthiness. Finally, there is no incentive mechanism included in trust model.

So, in this paper, we present a three-dimensional computing model of dynamic trust to try to find a way to address the problem. Firstly, we give a three-dimensional computing model of

trust and make a dynamics analysis to trust of peer. Next, considered the new peer without trustworthiness can not do anything almost, we propose an algorithm of initial trustworthiness based on the new peer's abilities. To compute the direct trustworthiness and the recommended trustworthiness, we colligate the time as a dynamic factor. Finally, based on the trustworthiness computed by trust fusion algorithm, we present a mechanism of making trust decision to promote cooperation. The simulation results have showed that our model can enhance the cooperation between peers and avoid the malicious peers from destroying behaviors.

The remainder of this paper is organized as follows. Section 2 gives a description of related works. In Section 3, detailed description of dynamic computing model of trust is presented. Section 4 present our simulation results and discuss some possible problems to our scheme and how we can cope with them. Finally, in Section 5 summarizes the main findings.

2. THREE-DIMENSIONAL COMPUTATION MODEL OF DYNAMIC TRUST

By considering scenarios where direct information about the trustee, we study context-sensitive trust establishment. We claim that even in such situations there are better options for trustors to choose from than to trust/distrust blindly. For example, the trustor can evaluate the trustworthiness of another peer somehow related to the trustee. In many real situations humans act like this. Context-sensitive computing is as an ability to detect and react to environment variables of each peer [27].

2.1 Three-Dimensional Computation Model

Trust is a very complex social and psychological phenomenon that involves many aspects and dimensions, such as in the social network, the person's appearance charm impact on the confidence, his/her ability determine whether competent to finish some works, interaction record contacts with credibility, and so on. In P2P networks, we refer to similar mechanism, and generally believed that the factors impact trustworthiness of peers is their ability attribute, past interaction records and evaluation given by other peers [28]. That is, they are the ability attribute of node (the initial trustworthiness), the direct trustworthiness and recommended trustworthiness. Although the trust of a peer is a dynamic process of adjustment, but it always changes in the three-dimensional space with these three factors (as shown in Figure 1).

The first dimension is the ability attribute of peers. The initial value of trust gotten bases on the peer's abilities like the amount of resources owned, network bandwidth, computing power and other attributes affect the cooperation between the peers. Just as we look for some files we want, we will visit the sites correspondingly own a large number files.

The second dimension is direct trust. The number of interaction in the past period of time, in particular, the number of successful interaction directly impact on the trustworthiness of peer. Also, we can ignore those old record happened in the past long time, and mainly focus on inspecting the most recent interactive records. Meanwhile, the interactive environment has some impact on the evaluation of direct trustworthiness.

The third dimension is recommended trustworthiness. It was computed by integrating the recommendation of other peers. When a peer consult the recommendation from other peers to another peer, we firstly make sure of the recommendations whether come from the right peers in order to avoid malicious recommendation, conspiracy, and so on. Secondly, when we adopt the recommendation, we will consider the trustworthiness of the recommended peers and the length of the recommended path.

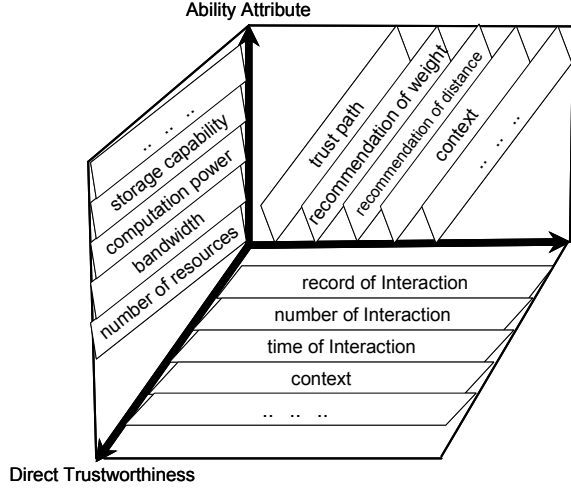


Fig. 1 Three-Dimensional Trust Computation Model

2.2 Computation Algorithms of Trustworthiness

The dynamic nature of trust decides by the natural attribute of peers in the trust relationships [29]. The dynamic trust of peer also can be quantifiable and be computed. So, we present a dynamic three-dimension model of trust called DynamicTrust as shown in Fig. 1. The dynamic change causes by the three dimensions: the peer's ability attribute, direct trustworthiness, and recommended trustworthiness. Firstly, we base on the correlative ability of peer to provide service to compute the initial trustworthiness. Secondly, taking into account the timing of interaction record of the interactive peers in the computation of direct trustworthiness, we set different weight to denote different time interaction records. That is, those new records will be set higher weight than those old records. Finally, we fully consider the dynamic characteristic of trust path and peer itself recommended, and the creditability of the peer who provided recommendation.

Definition 1 The Initial Trustworthiness (IniTrust) is a kind of trustworthiness of the peer just joins network system based on his/her ability attribute.

Definition 2 The Direct Trustworthiness (DirTrust) is a kind of trustworthiness of those peers who had the interactive experience based on the interactive record to be computed.

Definition 3 The Recommended Trustworthiness (RecTrust) is a kind of trustworthiness based on the information recommended by the trusted third party to be computed when a peer lacked of interactive information with another peer.

We define the peer in network as $E(A, R, T)$. Where,

A denote the set of peer's ability attribute, R is the set of interactive record, and $T = \{IniTrust, DirTrust, RecTrust\}$ is set of trustworthiness. The set of peer's ability attribute is the context of peer itself. So, we set those peers who provide the same kind services have the same set of ability attribute based on that these peers provide different service have different context.

2.2.1 Capability-Based Initial Trustworthiness

The new peer who just joins the network has no interactive information for those other peers. So we propose an algorithm for the new peer to compute its trustworthiness called initial Trustworthiness based on itself ability attribute. Then, those other peers can rely on the initial trustworthiness to make a decision whether the new peer is trust. With the initial trustworthiness, the new peer could get some operations granted and should be encouraged to cooperate with other peers. Moreover, it can reduce the network risk because of blind trust to new peer.

In the network, there exist some peers such as A, B, C, D, and E who provide the same kind service as shown in Fig. 2. The initial trustworthiness of each peer is zero before the evaluation.

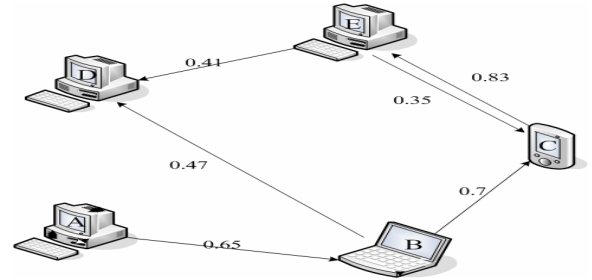


Fig.2 the Trust Web

Table 1 the Table of Quantitative to Ability Attribute of Peer

Ability Attribute							
	a_1	Value	a_2	Value	\dots	a_n	Value
Attribute	Level 1	m_1	Level 1	m_2	\dots	Level 1	m_n
Level	Level 2	m_1-1	Level 2	m_2-1	\dots	Level 2	m_n-1
	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
	Level	m_1	Level	m_2	\dots	Level	m_n
		1		1	\dots		1

Assumed the attribute of peer is $A(a_1, a_2, \dots, a_n)$, where a_i denotes the i th attribute of peer. The attribute denotes the service ability of peer. So, we classify and quantify the attribute a_i as $1, 2, \dots, m_i$. Where, the highest level is 1 and the lowest level is m_i . The value of m_i is possibly different to each attribute of peer. Every level will be set an

integer x_{ij} , ($j = 1, \dots, m_i$). That is, if the service ability of peer is low, x_{ij} will be small and x_{ij} will be big if the ability is high. For example, in the file sharing system, if a peer has a small number files, it denotes this has limit service ability. The value of x_{ij} is from m_i to 1 as shown in table 1.

Then, we can get the next formula,

$$x_{ij} = m_i - j + 1 \quad (15)$$

Where, the level j is the i th service ability attribute a_i .

Because the different attribute will has the effecting power to its trustworthiness when peer provide service for other peers, we set the attribute a_i has the weight w_i ($0 < w_i < 1$). And, the context of peer has some effecting to the evaluation for each peer, we set the effecting of context is $\gamma(\varepsilon_1)$, where $\gamma(\varepsilon_1) \in [0, 1]$. We can get the formula of the initial trustworthiness denoted as T_{init} ,

$$T_{init} = \gamma(\varepsilon_1) * \frac{\sum_{i=1}^n w_i * x_{ij}}{n * m} \quad (j = 1, \dots, m_i) \quad (16)$$

Based on the initial trustworthiness, the new peer can be identified the service capabilities, thus supporting the decision-making. Thereby it avoids a new peer joining the network to be distrusted because of no record of interaction, for example that is unfair for a peer in particular with provision of resources. With the initial level of trust, the new peer could be compared and then the initial trust relation could be established, the initial interaction could be happened, thus enhance better network peers as soon as possible accumulate their network reputation and enhance their own trustworthiness.

2.2.2 Direct Trustworthiness

There are two peers had interactions like A and B as shown in Fig. 2. Their interactive record set is $R_{A \rightarrow B}(P, F)$. Where, P is the set of successful interaction and F is the set of failed interaction. $P = (p, (\alpha_i, t_i))$, where, p is the number of successful interaction, α_i is the satisfied degree of the i th interaction of A with B, and t_i is the time when the i th successful interaction happened. $F = (f, (\beta_j, t_j))$, where, f is the number of failed interaction, β_j is the unsatisfied degree of the j th interaction of A with B, and t_j is the time when the j th failed interaction happened. For the interactive record, there exist a problem is time. That is, in our model, the new interactive records have more effecting power than those old records for trustworthiness of computation. So, we set a different weight to each record based on the time. Then we get weight of the i th successful interaction record as the next formula.

$$\Delta pt_i = \frac{1}{t_{sys} - t_i} \quad (i = 1, \dots, p) \quad (17)$$

And the weight of the j th failed interaction record can be gotten from the next formula.

$$\Delta ft_j = \frac{1}{t_{sys} - t_j} \quad (j = 1, \dots, f) \quad (18)$$

Where, t_{sys} is the current time of system. That is, the value of weight is larger, the interactive record is newer. At the same time, its effecting power to the computation of trustworthiness is bigger. So, the dynamic characteristic of the trust is fully represented. The value of α_i and β_j will get from the next table 2.

Table 2. the vale of α_i and β_j

Degree of satisfied α_i	Degree of unsatisfied β_j
Totally satisfied $\alpha_i = 1$	Unsatisfied $-0.5 < \beta_j < 0$
Much satisfied $0.5 \leq \alpha_i < 1$	Much unsatisfied $-1 < \beta_j \leq -0.5$
Satisfied $0 \leq \alpha_i < 0.5$	Totally unsatisfied $\beta_j = -1$

$T_{A \rightarrow B}$ denotes the direct trustworthiness of A with B. Then, the computation formula is shown as follows.

$$T_{A \rightarrow B} = \gamma(\varepsilon_2) * \frac{(\sum_{i=1}^p \Delta pt_i * \alpha_i + \sum_{j=1}^f \Delta ft_j * \beta_j)}{p + f} \quad (19)$$

Where, $\gamma(\varepsilon_2)$ denote the effecting degree of context.

Based on the direct interaction between two peers recorded, we can calculate the direct trustworthiness by formula 19. With the trustworthiness, it can help the peer to make the trust authentication and establish the trust relationship, and then form trust web. Because trust is asymmetry, that is, A trust B does mean B trust A. So, we model this trust web using directed graph as shown in Fig. 2. The direction of arrow denotes the direction of trust. For example if A points to B, it represents A trust B.

2.2.3 Recommended Trustworthiness

For some peers in the network, there have no enough interactive information to make the evaluation of the direct trustworthiness. And then, the peer needs help from its trusted peers to provide some recommendations for the peer to be evaluated. With those recommendations, the trustworthiness can be computed. For example, in the Fig. 2(the value labeled on the directed line is the direct trustworthiness), there lack of directly interaction or enough information of peer A and D. But peer D has directly interaction with B and E. So, if D put interactive request to A, A can request some recommendations on D from B and E. In order to avoid the malicious recommendation, we only take these recommendations from peers in the trust paths, such as $A \rightarrow B$ and $A \rightarrow B \rightarrow C \rightarrow E$.

Assumed peer X want to make the evaluation for Y, X has no enough information of Y. So, X send some helps of recommendation through trust path. There is a trust path $X \cdots \rightarrow V \rightarrow U \rightarrow W \cdots \rightarrow Z$, and its length is $m (\leq d)$.

Where, d is the maximum length of the trust path and the direction of arrow denote the direction of trust. U is the $i (\leq m)$ th peer providing recommendation in the path. V is the $i-1$ th peer and W is the $i+1$ th peer. And, some peers except X in the trust path that means not all of those peers except X in the trust path have enough directly interactive information with Y as shown Fig. 3.

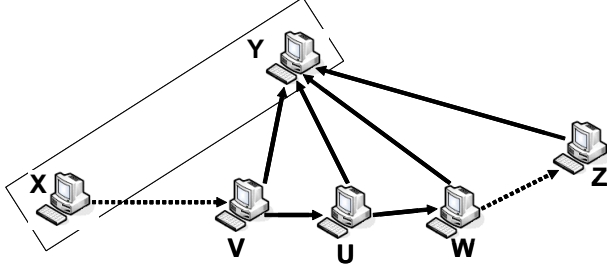


Fig. 3 the trust path of providing recommendation

We define the recommended information from each peer in the trust path as $R_{E(i)J}(T_{E(i) \rightarrow J}, T_{E(i) \rightarrow E(i+1)})$. Where, $R_{E(i)J}$ is the recommended information for peer J from the i th peer $E(i)$ in the trust path, $T_{E(i) \rightarrow J}$ denotes the direct trustworthiness of $E(i)$ with peer J , and $T_{E(i) \rightarrow E(i+1)}$ is the direct trustworthiness of $E(i)$ with $E(i+1)$. $T_{E(i) \rightarrow J}$ is zero that denotes this peer have no direct interactive information with peer J . Considered the effect of the length of the trust path, we set a variable of distance effect. That is, the recommendations of peers from near distance have more important than those far off in the trust path. The formula of the distance effect variable is $S = \frac{1}{i^2}$. Then, we can get the formula of recommended trustworthiness $T_{X \cdots \rightarrow Y}$,

$$T_{X \cdots \rightarrow Y} = \gamma(\varepsilon_3) * \sum_{d=1}^S \frac{\sum_{i=1}^d (T_{E(i) \rightarrow Y} * T_{E(i-1) \rightarrow E(i)})}{d} = \gamma(\varepsilon_3) * \frac{\sum_{i=1}^d (T_{E(i) \rightarrow Y} * T_{E(i-1) \rightarrow E(i)})}{d} \quad (20)$$

Where, $\gamma(\varepsilon_3)$ denote the effecting degree of context.

If the number of trust path is k , we can sum those recommended trustworthiness from each trust path and make an average. Then, the computation formula of the recommended trustworthiness is modified as the next,

$$\bar{T}_{X \cdots \rightarrow Y} = \frac{1}{k} \sum_{j=1}^k T_{X \cdots \rightarrow Y} \quad (21)$$

2.2.4 Fusion Algorithm of Trustworthiness in DynamicTrust Model

The fusion formula of the trustworthiness is,

$$T = \gamma(\varepsilon_1, \varepsilon_2, \varepsilon_3) * (\phi * T_{init} + \varphi * T_{A \rightarrow B} + \delta * \frac{1}{k} * \sum_{j=1}^k T_{X \cdots \rightarrow Y}) \quad (22)$$

Where, ϕ, φ, δ respectively denotes the ratio of the initial trustworthiness, the direct trustworthiness, and the recommended trustworthiness in the peer's trustworthiness, and there is $\phi + \varphi + \delta = 1$.

So, based on the trustworthiness of peer, we can set the threshold of trustworthiness for accessing control. It can limit the network behavior of peers, stop the malicious peers from destroying network security, and advance the efficiency of network services.

2.3 Decision-Making Mechanism of Trust

According to the trustworthiness of peer, we design the next mechanism of trust.

1) Strategy of trustworthiness threshold.

In the network services, we pre-settle different level of service corresponding to different trustworthiness threshold. That is, just only the peer's trustworthiness is greater than the threshold, it could consume the service. So, when a peer wants to choose a peer to interact, it can random choose a peer who its trustworthiness is greater than the threshold of the level. The load of the peers have the highest trustworthiness can be lightened a certain extent based on this strategy.

If $T_{request} \geq T_{threshold}$ then *Aggree* else *Disagree* end.

Where, $T_{request}$ is trustworthiness of the peer requests to consume service, and $T_{threshold}$ is the threshold of trustworthiness.

2) Strategy of close trustworthiness.

Based on the character of preference of the scale-free network model in small world phenomenon, those peers are partial to connect the existing peers who have high trustworthiness. But, it is easily to overload these peers and make congestion happened. So, we promote the control strategy as shown:

If $T_{request} \in [T_1, T_2]$ and $T_{provide} \in [T_1, T_2]$ then *Aggree* else *Disagree* end.

Where, $T_{request}$ is trustworthiness of the peer requests to consume service, $T_{provide}$ is trustworthiness of the peer provides service, and $[T_1, T_2], (T_1 < T_2)$ is the range of trustworthiness.

That is, when a peer look for peers who can provide some service it need, it should look for those peers whose trustworthiness is close to it. Peers base on this strategy to provide service and consume service.

This strategy is propitious to the balance of network load and reasonable to distribute the resources, because it group peers with different level of trustworthiness and peers can only interact with peers in the same group.

3) Strategy of the highest trustworthiness.

Based on this strategy, the peer providing service chooses the peer whose trustworthiness is the highest in those peers who want consume the same service. So, the peer who has higher trustworthiness always would get the service it wants. In this way, it can incent peers share its resources to get high trustworthiness, and prevent the malicious peers from destroying network.

If $T_{request}$ is the highest then Agree else Disagree end.

Where, $T_{request}$ is trustworthiness of the peer requests to consume service.

3. SIMULATIONS

Our research group preliminarily has designed a platform of biological network agent-oriented according to the key concepts and principles of ecological system [30-32]. The platform made full use of the characters of agent such as autonomy, mobility, and collaboration, etc. And, on the platform, the complexity of distributed applications embodied by a kind of natural interaction of computing components. The network services and applications were achieved by the large number of agents through interaction among them or environment on the platform. An agent is a biological entity implemented as a JAVA object. So, it is easy to construct the giant, open, complex, and wide-area distributed computing environment. Then, the biological network platform is a novel computing environment, and it has some fascinating characteristics like self-organized, survivable, self-evolved, expandable, and self-adaptive.

EigenTrust model describes an algorithm to decrease the number of downloads of inauthentic files in a peer-to-peer file-sharing network that assigns each peer a unique global trust value, based on the peer's history of uploads. It presents a distributed and secure method to compute global trust values, based on Power iteration. By having peers use these global trust values to choose the peers from whom they download, the network effectively identifies malicious peers and isolates them from the network [33].

PeerTrust model of PeerTrust is a reputation-based trust supporting framework, which includes a coherent adaptive trust model for quantifying and comparing the trustworthiness of peers based on a transaction-based feedback system and a decentralized implementation of such a model over a structured P2P network. This model has two main features. First, it introduces three basic trust parameters and two adaptive factors in computing trustworthiness of peers, namely, feedback a peer receives from other peers, the total number of transactions a peer performs, the credibility of the feedback sources, transaction context factor, and the community context factor. Second, it defines a general trust metric to combine these parameters. Other contributions include strategies used for implementing the trust model in a decentralized P2P environment, evaluation mechanisms to validate the effectiveness and cost of PeerTrust model [15].

On the biological network platform, we implement three models: EigenTrust, PeerTrust, and DynamicTrust (proposed in this paper). In this experiment, a biological agent represents a peer in the P2P services environment. And, there are 1000 agents on the platform. The services are files provided or downloaded.

3.1 Impact of Initial Trustworthiness

In this paper, the initial trustworthiness of peer based on itself ability attribute was first proposed. So, we design a set of experiment of comparing the impact of the initial trustworthiness to the trust evolution of peer. We set 500 peers have the value of initial trustworthiness is zero, 300 peers is 0.2, and 200 peers is 0.4. Each peer has a number of files. The interactive behaviors are providing and consuming. We compute the trustworthiness of peers by the interaction records based on the algorithm of DynamicTrust model. The data we got from the experiment shown as the Fig. 4. Because of the different initial trustworthiness, the trustworthiness of peers has shown big difference. The lower initial trustworthiness the peers had, its trustworthiness increased is the slower. So, the more power of ability the peers have, they will get more initial trustworthiness, their effect and contribution will get to exert to the other peers.

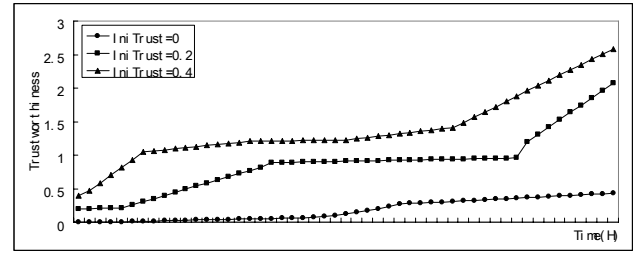


Fig 4 Impact of the initial trustworthiness

3.2 Successful Interaction between Peers

In the second experiment, we compare the impact of trustworthiness to the successful ratio of interaction to three trust models. The experimental results are shown in the Fig. 5. We set the time of interaction as the context to denote the dynamic of trust. When the trustworthiness of peer is comparatively low, the ratio of successful interaction is low. With the interactions obviously increased, the ratio of successful interaction is promoted. In our trust model, the trustworthiness can be fleetly increased because of the initial trustworthiness. So, the ratio of successful interaction is fleetly increased. However, in this experiment, we do not consider the existing of malicious peers in the network.

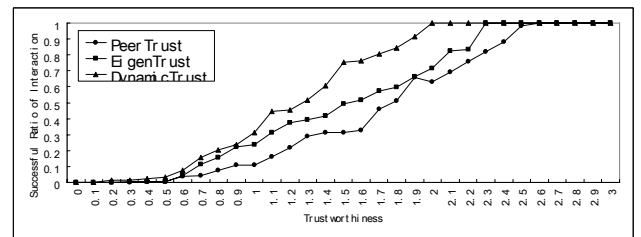


Fig. 5 Impact of trustworthiness to the successful ratio of interaction

3.3 Detection of Malicious Peer

In the third experiment, we make the detection of malicious peers. First, there are 100 peers we set as malicious peers. Their malicious behaviors are free-riding and providing fault files. We experiment it 9 times and three of each model. And then we average the data we get from experiment. The results are shown in the Fig. 6. Our model has no obvious merit comparing to the other model. However, our model can detect malicious peers and prevent the malicious behaviors in a certain extent. And then, it can take incentive effect to the good peers.

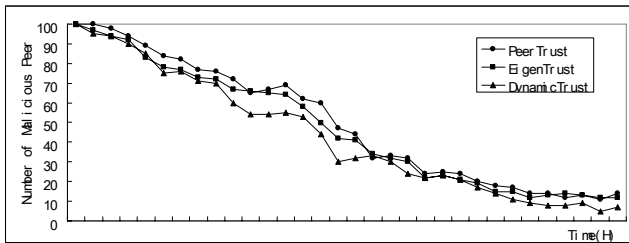


Fig. 6 the detection of malicious peers

4. CONCLUSIONS

In this paper, we firstly proposed a context-sensitive fitness law to judge the abilities of peers. Next, we took the dynamics analysis of peer's trust in three-dimensional evolutionary space. And then, giving full consideration to the personality characteristics of peers and the dynamic characteristics of trust, we presented a dynamic computing model of trust based on the ability attribute of peers, the interactive records, and the recommended information in a reasonable, practical, comparability, workable principles in the distributed services environment. So, we divided the peer's trustworthiness into initial trustworthiness, direct trustworthiness, and recommended trustworthiness, and respectively designed the computation algorithms. Based on the peer's trustworthiness, interactive services could furthest be achieved between peers. Also, the malicious behaviors could be controlled because of the trustworthiness threshold of services. So, the honest peers can be incentive and the network stability can be promoted, and the extent of network security can be improved. Subsections

5. ACKNOWLEDGMENTS

This work was supported in part by the Natural Science Foundation of China (No. 90718011), Key Project of the National Nature Science Foundation of China (No. 60534020), Program for New Century Excellent Talents in University from Ministry of Education of China (No. NCET-04-415), the Cultivation Fund of the Key Scientific and Technical Innovation Project from Ministry of Education of China (No. 706024) and International Science Cooperation Foundation of Shanghai (No. 061307041), the Natural Science Foundation of China (No. 60873058), the Natural Science Foundation of Shandong Province (No. Z2007G03), and the Science and Technology Project of Shandong Education Bureau, and the Project of the Social Science Planning of Shandong Province (No. 08JDC128).

6. REFERENCES

- [1] Daswani, N., Garcia-Molina, H., and Yang, B. 2002. Open Problems in Data-Sharing Peer-to-Peer Systems. In

Proceedings of the 9th international Conference on Database theory (January 08-10, 2003). D. Calvanese, M. Lenzerini, and R. Motwani, Eds. Lecture Notes in Computer Science, vol. 2572. Springer-Verlag, London, 1-15.

- [2] Feldman, M. and Chuang, J. 2005. Overcoming free-riding behavior in peer-to-peer systems. *SIGecom Exch.* 5, 4 (Jul. 2005), 41-50. DOI=<http://doi.acm.org/10.1145/1120717.1120723>
- [3] Claudiu Duma, Nahid Shahmehri, and Germano Caronni, 2005. Dynamic Trust Metrics for Peer-to-Peer Systems. In *Proceeding of the 16th International Workshop on Database and Expert Systems Applications* (August 22-26, 2005), IEEE Computer Society.
- [4] Chien E. 2003. Malicious Threats of Peer-to-Peer Networking. Technical Report. Symantec Security Response.
- [5] Abdul-Rahman, A. and Hailes, S. 2000. Supporting Trust in Virtual Communities. In *Proceedings of the 33rd Hawaii International Conference on System Sciences*-Volume 6 - Volume 6 (January 04-07, 2000). HICSS. IEEE Computer Society, Washington, DC, 6007.
- [6] Dewan P. and Dasgupta P. 2005. Securing P2P Networks Using Peer Reputations: Is There a Silver Bullet? In *Proceedings of IEEE Consumer Communications and Networking Conference* (January 03-06, 2005). Las Vegas, US, 30-36.
- [7] Liu Z., Joy A.W., and Thompson R.A. 2004. A Dynamic Trust Model for Mobile Ad Hoc Networks. In *Proceedings of the 10th IEEE international Workshop on Future Trends of Distributed Computing Systems* (May 26 - 28, 2004). FTDCS. IEEE Computer Society, Washington, DC, 80-85.
- [8] Pirzada, A. A. and McDonald, C. 2004. Establishing trust in pure ad-hoc networks. In *Proceedings of the 27th Australasian Conference on Computer Science - Volume 26* (Dunedin, New Zealand). Estivill-Castro, Ed. ACM International Conference Proceeding Series, vol. 56. Australian Computer Society, Darlinghurst, Australia, 47-54.
- [9] Buchegger S. and Boudec J.L. 2002. Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks. In *Proceedings of Tenth Euromicro PDP (Parallel, Distributed and Network-based Processing)* (January 2002). Gran Canaria, 403-410.
- [10] He Q., Wu O.D., and Khosla P. 2004. SORI: A Secure and Objective Reputation-Based Incentive Scheme for Ad-Hoc Networks. In *Proceedings of IEEE Wireless Communications and Networking Conference Volume 2* (March 21-25, 2004). Atlanta, GA, 825-830.
- [11] Michiardi, P. and Molva, R. 2002. Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Proceedings of the IFIP Tc6/Tc11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security* (September 26 - 27, 2002). B. Jerman-Blazic and T. Klobucar, Eds. IFIP Conference Proceedings, vol. 228. Kluwer B.V., Deventer, The Netherlands, 107-121.
- [12] Papaioannou, T. G. and Stamoulis, G. D. 2004. Effective use of reputation in peer-to-peer environments. In *Proceedings of the 2004 IEEE international Symposium on Cluster*

- Computing and the Grid (April 19 - 22, 2004). CCGRID. IEEE Computer Society, Washington, DC, 259-268.
- [13] Damiani, E., di Vimercati, D., Paraboschi, S., Samarati, P., and Violante, F. 2002. 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 (Washington, DC, USA, November 18 - 22, 2002). V. Atluri, Ed. CCS '02. ACM, New York, NY, 207-216. DOI= <http://doi.acm.org/10.1145/586110.586138>
- [14] Kamvar S.D., Schlosser M.T., and Garcia-Molina H. 2003. Eigenrep: Reputation Management in P2P Networks. In Proceeding of International WWW Conference (May, 2003), IEEE Computer Society, Budapest, Hungary, 640-651.
- [15] Xiong L. and Liu L. 2004. PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities. IEEE Trans. on Knowl. and Data Eng. 16, 7 (Jul. 2004), 843-857. DOI= <http://dx.doi.org/10.1109/TKDE.2004.1318566>
- [16] Cvrcek D. 2004. Dynamics of Reputation. In Proceeding of 9th Nordic Workshop on Secure IT-Systems (November 2004), Helsinki, FI, 1-14.
- [17] Manchala, D. W. 2000. E-Commerce Trust Metrics and Models. IEEE Internet Computing 4, 2 (Mar. 2000), 36-44. DOI= <http://dx.doi.org/10.1109/4236.832944>
- [18] Mui, L., Mohtashemi, M., and Halberstadt, A. 2002. A Computational Model of Trust and Reputation for E-businesses. In Proceedings of the 35th Annual Hawaii international Conference on System Sciences (Hicss'02)- Volume 7 - Volume 7 (January 07 - 10, 2002). HICSS. IEEE Computer Society, Washington, DC, 188.
- [19] Resnick, P., Kuwabara, K., Zeckhauser, R., and Friedman, E. 2000. Reputation systems. Commun. ACM 43, 12 (Dec. 2000), 45-48. DOI= <http://doi.acm.org/10.1145/355112.355122>
- [20] Jøsang A. and Ismail R. 2002. The Beta Reputation System. In Proceedings of the 15th Bled Electronic Commerce Conference (June 2002). Slove- nia.
- [21] Wang, Y. and Vassileva, J. 2003. Bayesian Network-Based Trust Model. In Proceedings of the 2003 IEEE/WIC international Conference on Web intelligence (October 13 - 17, 2003). Web Intelligence. IEEE Computer Society, Washington, DC, 372.
- [22] Yu, B. and Singh, M. P. 2002. An evidential model of distributed reputation management. In Proceedings of the First international Joint Conference on Autonomous Agents and Multiagent Systems: Part 1 (Bologna, Italy, July 15 - 19, 2002). AAMAS '02. ACM, New York, NY, 294-301. DOI= <http://doi.acm.org/10.1145/544741.544809>
- [23] Manchala, D. W. 2000. E-Commerce Trust Metrics and Models. IEEE Internet Computing 4, 2 (Mar. 2000), 36-44. DOI= <http://dx.doi.org/10.1109/4236.832944>
- [24] Sabater, J. and Sierra, C. 2002. Reputation and social network analysis in multi-agent systems. In Proceedings of the First international Joint Conference on Autonomous Agents and Multiagent Systems: Part 1 (Bologna, Italy, July 15 - 19, 2002). AAMAS '02. ACM, New York, NY, 475-482. DOI= <http://doi.acm.org/10.1145/544741.544854>
- [25] Kaur D. and Dominic Wilson, 2004. Trust Evaluation within a Type-2 Fuzzy Logic Framework. In Proceedings of the International Joint Conference on Neural Networks IJCNN and IEEE International Conference on Fuzzy Systems (July 25-29, 2004). IEEE-FUZZ 2004, Budapest, Hungary, 203-208.
- [26] Giorgos Zacharia and Pattie Maes, 2000. Trust Management through Reputation Mechanisms. Applied Artificial Intelligence, 14, 9 (October 2000), 881-907.
- [27] Blaze M., Feigenbaum J., and Lacy J. 1996. Decentralized Trust Management. In Proceeding of the 17th IEEE Symposium on Security and Privacy, 164-173.
- [28] Terzis S., Wagealla W., English C., McGettrick A., and Nixon P. 2004. The SECURE Collaboration Model: SECURE Deliverables D2.1, D.2.2 and D2.3. <http://secure.dsg.cs.tcd.ie>.
- [29] Marsh S. 1994. Formalising Trust as a Computational Concept. Doctoral Thesis. Department of Mathematics and Computer Science, University of Stirling.
- [30] Kinatader M. and Pearson S. 2003. A Privacy-Enhanced Peer-to-Peer Reputation System. In Proceedings of the 4th International Conference on Electronic Commerce and Web Technologies, LNCS 2378, Springer.
- [31] Ren L.-H. and Ding Y.-S. 2002. A New Network Simulation Platform Based on Ecological Network Computation. Journal of System Simulation, 14, 11(2002), 1497-1499, 1503.
- [32] Ding Y.-S. and Ren L.-H. 2003. Design of a Bio-network Architecture Based on Immune Emergent Computation. Control and Decision, 18, 2 (2003), 185-189.
- [33] Kamvar, S. D., Schlosser, M. T., and Garcia-Molina, H. 2003. The Eigentrust algorithm for reputation management in P2P networks. In Proceedings of the 12th international Conference on World Wide Web (Budapest, Hungary, May 20 - 24, 2003). WWW '03. ACM, New York, NY, 640-651. DOI= <http://doi.acm.org/10.1145/775152.775242>