Int. J. Communications, Network and System Sciences, **2009, 6, 546-554**
doi:10.4236/ijcns.2009.26060 Published Online September 2009 (http://www.SciRP.org/journal/ijcns/).

A Trust Model Based on the Multinomial Subjective Logic for P2P Network

Junfeng TIAN[1], Chao Li[1], Xuemin HE[2], Rui TIAN[1]
[1]*College of Mathematics & Computer Science, Hebei University, Baoding, China*
[2]*Department of Modern Science & Technology, Agricultural University of Hebei, Baoding, China*
Email: *jftian@hbu.cn*
Received March 9, 2009; *revised May* 17, 2009; *accepted July* 7, 2009

ABSTRACT

In order to deal with the problems in P2P systems such as unreliability of the Service, security risk and attacks caused by malicious peers, a novel trust model MSL-TM based on the Multinomial Subjective Logic is proposed. The model uses multinomial ratings and Dirichlet distribution to compute the expectation of the subjective opinion and accordingly draws the peer's reputation value and risk value, and finally gets the trust value. The decay of time, rating credibility and the risk value are introduced to reflect the recent behaviors of the peers and make the system more sensitive to malicious acts. Finally, the effectiveness and feasibility of the model is illustrated by the simulation experiment designed with peer-sim.

Keywords: Trust, Multinomial Subjective Logic, Reputation, Risk, Dirichlet Distribution

1. Introduction

P2P technology is a new distributed network model which doesn't rely on the server. This model has been applied widely in areas such as peer-to-peer compute, information sharing, distributed search and so on. It realized the sharing of the network information and resources by the direct exchange between peers in the systems. In this network, all the peers are equal, and truly achieve equality communications between the networks [1]. However, with the extensive and in-depth applications of the existing P2P system, its defects are exposed gradually. The performance of P2P systems cannot achieve the best condition theoretically [2]. The main reasons are the unreliability of the service, security risk and attacks caused by malicious peers [3]. These problems impose serious constraints on the cooperative relations between the users in the P2P system. In addition, co-operation between users in P2P systems is limited, and the most fundamental reason is lack of trust between users and effective cooperation mechanisms. So it cannot motivate users to participate in the system cooperation more actively. The anonymity, high degree of openness as well as the peer type, purpose and other factors led to peers' different action [4]. The loss of trust between users leads to a severe damage to the performance of P2P network and hampers the further development of P2P network.

Therefore, in order to strengthen the cooperation among peers and improve the overall availability of P2P services, it is a great significance to constructing a reliable trust management model for effectively resources selection and inspiring co-operation.

2. Related Works

Nowadays the research of P2P trust is mainly focused on building reliable trust management model. Trust Management (TM) is first proposed by Blaze M. in 1996 [5], and then it became a research focus of network security.

The PeerTrust [6,7] model proposed by L. Xiong combines both local and global reputation with confidence coefficient, and considers several factors influencing credibility quantification, the model can cope with virtual ratings well. However, the PeerTrust model does not offer measurements for factors of trust and methods for defining confidence coefficient. The P2P-oriented and reputation-based trust management model proposed in reference [8] introduces risk factor, and proposes to quantize risk with information entropy. This model is superior to some existing trust models in terms of both security and other aspects.

Jøsang makes research on trust management based on Subjective Logic [9], and proposes Evidence Space and Opinion Space that are used to describe and measure trust relationship. Also, he offers a series of Subjective

Logic Operators [10] which are used for trust value deducing and integrating computing. In this binominal Subjective Logic [11], Bata distribution [12] that is used for describing binominal posterior probability is used as basis, and probability density is defined by positive and negative events, then the probability trust value of every event created among peers is computed. Later, Jøsang proposed multinomial Subjective Logic [13,14] which is based on Dirichlet multinomial probability distribution [15] and allows for ratings of different levels, this can be used for computing reputation, it provides more flexible platform for designing reputation systems. However, neither the influence of the time decay on trust value nor the trust integration of different weights is considered in the Subjective Logic model. It cannot protect the attacked target from excessive derogation or exaggerating brought by malicious peers. Besides, it does not consider reflecting the indeterminacy and risk brought by defective interaction in terms of trust computing, and could not monitor probable attack and potential threaten from defective peers.

To deal with the problems mentioned above, we propose a new P2P trust model based on multinomial Subjective Logic-MSL-TM (Multinomial Subjective Logic Based Trust Model). It adopts multinomial ratings, and uses Dirichlet distribution function to compute expected value of subjective opinion, with, which we can get the reputation value and risk value of peers, and get trust value of peers finally.

The main innovations of the paper are:

1) By making use of self interaction experience and interaction experience of other entity in the system, entity evaluates the trust value of entities that would interact with it, and introduces time decay and rating credibility into trust evaluation to make the trust value of peers reflect their recent action and eliminate excessive derogation or exaggerating brought by normal peers, then potential dangers can be prevented effectively, such as cooperative cheating and derogation.

2) Considering potential attack from variant types of defective peers, this paper not only computes reputation value when computing trust value of peers, but also analyzes its historical action, and introduces potential indeterminacy risk value as appendix of reputation value.

3) We can adjust the value of reputation and risk appropriately to make the trust value of peers more sensible to defective action, and achieve the goal of detecting defective action.

A detail description of our proposed trust model is presented in Section 3, and the method for computing trust value is provided as well. In Section 4, we perform the simulation experiments, and the experiment results and analysis are reported. The last section ends the paper by presenting some concluding remarks.

3. MSL-TM trust model

In this paper, we propose a trust model MSL-TM that is facing to P2P file-sharing primarily. The model can also be used to P2P data management, P2P collaborative computing, and e-business applications systems.

3.1. Related definition

Definition 1, trust.

The reliability, credibility, and capacity to provide services of an entity reflected in the interaction.

Definition 2, **ratings.**

One peer gives another peer a quantitative value in accordance with their action when they interact with each other.

Definition 3, local trust.

The local trust peer X to Y, is based on the interaction history of peer x and y, and the historical ratings of the interaction of x, then get the expectations of future behavior (trust level) of x to y.

Definition 4, global trust.

The global trust of peer Y is a credibility of y derived from the ratings of y's neighbor on y.

Definition 5, reputation.

It can get the individual expectations of future behavior through observation or ratings information of a history of individual acts. Reputation is composed of local trust and global trust. Calculation methods see Subsection 3.5.

Definition 6, risk.

Risk is a concept of economics. In economics, risk refers to the uncertainty of loss; it is a negative deviation from the consequences of uncertainty to the expected target.

In this paper, it reflects the unreliability of the peer recently, which is the uncertainty of the interaction results and the probability of adverse consequences. The value of the risk Ri is composed of Local expectations of negative ratings $\vec{E}_L$, global expectations of negative ratings $\vec{E}_A$ and Risk components of the uncertainty in opinion u_X. Calculation methods are introduced in Subsection 3.6.

Definition 7, trust value.

The quantized value of trust for one entity to another, it's related to the reliability, integrity and performance of the peer. We use T to denote the trust value x to y. Re and Ri denote the reputation value and risk value of peer y respectively, α, β is their weight. Then the trust

value of peer y is:

$$T = \alpha \mathrm{Re} - \beta \mathrm{Ri} \quad (1)$$

Where $0 \le \alpha, \beta \le 1$.The value of α, β are determined by the degree of optimism of x to y.

The more optimistic to the y's behavior and interaction results, the bigger the value of α / β is, so that it can weaken the influence of risk on the trust value. Oppositely, The more pessimistic to y's behavior and interaction results, the smaller of the value of α / β is, so that the trust value is more sensitive to the risk value. In order to calculate more precisely, in this paper, we set, $\beta = N_{R(x3)} / N_{Total}$, $N_{R(x3)}$ is the number of rating $R(x_3)$, N_{Total} is the number of total ratings.

3.2. Multinomial Ratings

In binomial subjective logic, ratings are considered to be either true or false. This makes the ratings too one-sided and rigid. Now we introduce multinomial ratings.

$$\vec{R} = (R(x_i) \mid i = 1...k)$$

In this paper, we take trinomial ratings for example, mainly for P2P file-sharing applications. According to the degree that the consumer satisfies with the service quality, the ratings for the provider's service are divided into three levels, then after consumers completing download, they can make the corresponding ratings. The three levels are:

$$\vec{R} = (R(x_i) \mid i = 1...3)$$

$R(x_1)$=B(bad)：The document is false or malicious or non-responsive.

$R(x_2)$=C(common)：The document is true but the quality is not good or download has delayed.

$R(x_3)$=G(good)：The document is true and the quality is good, the speed of download is fast.

The ratings are divided by many parameters according to the real situation., this paper we refer to a ternary group (authenticity, download speed, quality). In practical applications, the test parameters can be increased.

Authenticity: If the document downloaded is the one the user requested, it's a true document, otherwise it's a false document.

Download speed: is the time how long the user has waited. We define a parameter K=file size/transfer speed, the value of K is given according to the actual situation. k1, k2 is two middle values, when K<k1, the download speed is too slow or non-response; when K∈[k1，k2], the speed is not very good; When K>k2, the speed is fast.

3.3. Visualizing Opinion in the Space

Let $X=\{x_i|i=1,\ldots,k\}$ be a frame, then the composite function $\omega_X=(\vec{b}, u, \vec{a})$ [13] is an opinion over X., where

Table 1. The classification of the quality.

Quality	Data document	Video or audio document
Good	No data loss	Smooth screen, good sound quality
Common	Have a small amount of data loss and bit error	Screen not smooth, sound is not clear
Poor quality or malicious files	A serious data loss, or download the file with virus	Screen can not be displayed, poor sound quality or the file download with virus

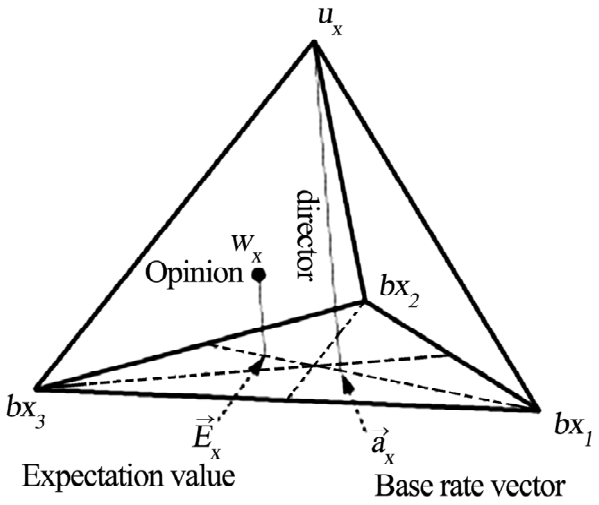

Figure 1. Opinion pyramid with example trinomial opinion.

$\vec{b}$ is a vector of belief masses over the propositions of X, u is the uncertainty mass, and $\vec{a}$ is a vector of base rate values over the propositions of X. These components satisfy:

$$\vec{b} \in [0, 1]^k, \quad \vec{b}(\varphi) = 0, \sum_{x \in X} \vec{b}(x) \le 1;$$

$$u + \sum_{x \in X} \vec{b}(x) = 1;$$

$$\vec{a}(\varphi) = 0, \sum_{x \in X} \vec{a}(x) = 1$$

The probability expectation value of the opinion is:

$$E_X = \vec{b}(x_i) + \vec{a}(x_i) u_X,$$

where .

$$E_X(\varphi) = 0, \sum_{x \in X} E_X(x) = 1$$

Trinomial opinions can be visualized as points inside a triangular pyramid as shown in Figure 1. The top vertex U_X represents uncertainty, the three vertex of the bottom

b_{x1}, b_{x2}, and b_{x3} represent three Belief vectors. The projector starting from the opinion point is parallel to the line that joins the uncertainty vertex and the base rate point on the bottom. The point at which the projector meets the bottom determines the expectation value of the opinion, i.e. it coincides with the point corresponding to expectation value E_X.

We are interested in knowing the probability distribution over the disjoint elements of a frame. In case of a binary frame, it is determined by the Beta distribution. In the general multinomial case it is determined by the Dirichlet distribution, which describes the probability distribution over a k-component random variable P(x_i), i=1…k,

$$p(x_i) \geq 0, \sum_{i=1}^{k} p(x_i) = 1,$$

then the multinomial Dirichlet density function over X can be expressed as:

$$f(\vec{p} \mid \vec{\alpha}) = \frac{\Gamma(\sum_{i=1}^{k}(\alpha(x_i)))}{\prod_{i=1}^{k}\Gamma(\alpha(x_i))} \prod_{i=1}^{k} p(x_i)^{(\alpha(x_i)-1)} \quad \textbf{(2)}$$

because $\alpha(x_i) = r(x_i) +$, then:

$$f(\vec{p} \mid \vec{r}, \vec{a}) = \frac{\Gamma(\sum_{i=1}^{k}(r(x_i) + Ca(x_i)))}{\prod_{i=1}^{k}\Gamma(r(x_i) + Ca(x_i))} \prod_{i=1}^{k} p(x_i)^{(r(x_i)+Ca(x_i)-1)} \quad \textbf{(3)}$$

where $r(x_i) \geq 0$, $a(x_i) \geq 0, \sum_{x \in X} \vec{a}(x) = 1$, $C \geq 2$.

C is a priori constant, $\vec{r}$ is observation evidence, in this paper, we use it for ratings, $\vec{a}$ is base rate.

Dirichlet distributions translate observation evidence directly into probability density functions. The representation of evidence, together with the base rate, can be used to denote opinions:

$$\begin{cases} b_X(x_i) = \dfrac{r(x_i)}{C + \sum_{j=1}^{k} r(x_i)} \\ u_X = \dfrac{C}{C + \sum_{j=1}^{k} r(x_i)} \end{cases}, i = 1, ..., k \quad \textbf{(4)}$$

The probability expectation values is expressed as:

$$E(p(x_i) \mid \vec{r}, \vec{a}) = \frac{r(x_i) + Ca(x_i)}{C + \sum_{j=1}^{k} r(x_i)}, i = 1, ..., k \quad \textbf{(5)}$$

3.4. Dynamic Base Rate

Agents will come and go during the lifetime of a market, and it is important to be able to assign new members a reasonable base rate reputation. In the simplest case, this can be the same as the initial default reputation that was given to all agents during bootstrap. However, it is possible to track the average reputation score of the whole community and this can be used to define the base rate for new agents, either directly or with a certain additional bias. Not only new agents, but also existing agents with a standing track record can get the dynamic base rate. After all, a dynamic community base rate reflects the whole community, and should therefore be applied to all the members of that community.

The global rating after the combination of the opinions is $\vec{R}_F$ (the computing method is given in Subsection 3.5.2), and $\vec{E}_F$ is the global expectation vector (the computing method is given in Subsection 3.5.2). This vector then needs to be normalized to a base rate vector, the base rate at time t +1 is then simply expressed as the global expectation vector at time t: $\vec{a}_F = \vec{E}_{F_r}$.

3.5. Calculation of the Reputation Value Re

The reputation value Re is composed of local trust L and global trust A, and can be calculated as follows:

$$\mathrm{Re} = \gamma L + (1-\gamma)A, 0 \leq k \leq 1 \quad \textbf{(6)}$$

where γ is the weight of the local trust, (1-γ) is the weight of the global trust.

3.5.1. Calculation of the Local Trust L

The local trust is based on the history ratings to calculate the trust level of one peer to another. It is similar to human society; an individual builds up his (her) trust to another through local contacts. The local trust is not only relevant to the history ratings, in order to reflect the objectivity and accuracy of the calculation; we introduce the following two factors:

1) Time decay: Agents will change their behavior over time; the research based on economic theory shows that: when computing the current reputation, reducing the weight of the history ratings can make the reputation converge at a steady state. The longer the time is, the smaller of the impact on the reputation by the ratings. The shorter the time interval from now, the better the effect of the ratings, so it is necessary to give the recent ratings a higher weight [16,17].

We denote the ratings in level x_i as Ry(x_i), equal to give y a rating of level x_i, the value is 1.Ti is the time decay factor, $\mathrm{Ti}=e^{-(t-t_{Ry}(x_i))}$, where t is Current time, $t_{Ry}(xi)$ is the time when $R_y(X_i)$ is given.

The cumulative ratings to y with time decay is $R_{y,t}(X_i)$,

Including n times ratings. Then $R_{y,t}$ can be expressed as:

$$R_{y,t}(x_i)=\sum_{k=1}^{n} e^{-(t-t_{R_y^k(x_i)})}\times R_y^k(x_i), i=1,2,3 \quad \textbf{(7)}$$

where $R_y^k(x_i)$ is the k[th] ratings of y, t is the current time, $t_{R_y^k(x_i)}$ is the time when the k[th] ratings is given.

2) Rating credibility D_R

Definition 8, Neighbor peer: Let i and j be two peers of the p2p network respectively, if peer i has interact with peer j, and then j is the neighbor peer of i. In this paper we call the peers who give other peers ratings rater, and the peers which have been given ratings ratee.

Definition 9, rating credibility: Reflects the degree of credibility of the ratings is given, whose value can be used as a weight of ratings given by a peer.

It can prevent the derogation by malicious peers through using the rating credibility. It is very subjective that one peer gives ratings to another, so the malicious ratings of a neighbor peer can bring a bad effect to the reputation of the rated peer. Therefore the accuracy is affected by the credibility of the ratings of the neighbor peer.

The rating credibility should not be given subjectively, in this paper, the rating credibility is defined as D_R, The rater's trust value T and the global expectation $E_A(x_i)$ of ratings level i are defined as a measure factor:

$$D_R=kT+(1-k)E_A(x_i), i=1,2,3 \quad \textbf{(8)}$$

where k is the weight of the rating credibility (1-k) is the weight of the expectation value.

To some extent, the rater's trust value T determines the rating credibility of the rating $R_y(X_i)$; In addition, if the expectation value of this kind of ratings is small, the rating of this peer is unreliable. It can eliminate excessive derogation or exaggerating brought by malicious peers through introducing the rating credibility.

$$R_{y,t,D_R}(x_i)=D_R\cdot R_{y,t}(x_i), i=1,2,3 \quad \textbf{(9)}$$

We can obtain local expectations of different rating levels as follows by putting the Formula (9) into the Formula (5):

$$E_L(x_i)=\frac{R_{y,t,D_R}(x_i)+Ca_F(x_i)}{C+\sum_{j=1}^{k} R_{y,t,D_R}(x_j)}, i=1,2,3 \quad \textbf{(10)}$$

where i=1…k, and k=3 in this paper.

By giving expectations of different rating levels a weight value, the peer's local trust value can be calculated as follows:

$$L=\sum_{i=1}^{k}\varepsilon(x_i)E_L(x_i), i=1,2,3 \quad \textbf{(11)}$$

3.5.2. Calculation of the Global Trust L

Peer y's global trust is related to the following factors:

1) The number of y's neighbor peers. The more of the number of neighbor peers, the smaller of the uncertainties relatively, then y's global trust is more accurate; On the contrary, if the number of neighbors peers has nothing to do with the global trust, a small number of malicious peers are easy to uplift each other's reputation through collusiveness.

2) The rating credibility of y's Neighbor peers. The higher of neighbor peer's credibility rating, the more credible of the ratings given by them; on the contrary, if neighbor peer's credibility rating is low the ratings cannot be trusted.

3) The ratings of y's neighbor peers. If neighbor peers give a good rating, the global trust will be enhanced; otherwise, the risk level of the peers will be enhanced.

In many situations there will be multiple sources of evidence, and fusion can be used to combine evidence from different sources. A distinction can be made between two cases.

The two peers observe the process during disjoint time periods. In this case the observations are independent, and it is natural to simply add the observations from the two peers, and the resulting fusion is called cumulative fusion.

Let the two observers' respective opinions be expressed as

$\omega_X^A=(\vec{b}_X^A,u_X^A,\vec{a}_X^A)$ and $\omega_X^B=(\vec{b}_X^B,u_X^B,\vec{a}_X^B)$

over the same frame $X=\{x_i\mid i=1,...,k\}$. Let $\omega_X^{A\Diamond B}$ be the opinion such that:

When $u_X^A\neq 0 \ \vee \ u_X^B\neq 0$:

$$\begin{cases} b_{x_i}^{A\Diamond B}=\dfrac{b_{x_i}^A u_X^B+b_{x_i}^B u_X^A}{u_X^A+u_X^B-u_X^A u_X^B} \\ u_X^{A\Diamond B}=\dfrac{u_X^A u_X^B}{u_X^A+u_X^B-u_X^A u_X^B} \end{cases} \quad \textbf{(12)}$$

When $u_X^A=0 \ \wedge \ u_X^B=0$:

$$\begin{cases} b_{x_i}^{A\Diamond B}=\gamma b_{x_i}^A+(1-\gamma)b_{x_i}^B \\ u_X^{A\Diamond B}=0 \end{cases},$$

where

$$\gamma=\lim_{\substack{u_X^A\to 0\\ u_X^B\to 0}}\frac{u_X^B}{u_X^A+u_X^B} \quad \textbf{(13)}$$

Then $\omega_X^{A\Diamond B}$ is called the cumulatively fused opinion of ω_X^A and ω_X^B, representing the combination of independent opinions of A and B. By using the symbol '$\oplus$' to designate this belief operator, we define:

$$\omega_X^{A\Diamond B}\equiv\omega_X^A\oplus\omega_X^B \quad \textbf{(14)}$$

The two peers observe the process during the same time period. In this case the observations are dependent, and it is natural to take the average of the observations

by the two peers, and the resulting fusion is called averaging fusion.

Let the two observers' respective opinions be expressed as $\omega_X^A = (\vec{b}_X^A, u_X^A, \vec{a}_X^A)$ and $\omega_X^B = (\vec{b}_X^B, u_X^B, \vec{a}_X^B)$ over the same frame $X = \{x_i \mid i = 1,...,k\}$. Let $\omega_X^{A\Diamond B}$ be the opinion such that:

When $u_X^A \neq 0 \ \vee \ u_X^B \neq 0$:

$$\begin{cases} b_{x_i}^{A\Diamond B} = \dfrac{b_{x_i}^A u_X^B + b_{x_i}^B u_X^A}{u_X^A + u_X^B} \\ u_X^{A\Diamond B} = \dfrac{2u_X^A u_X^B}{u_X^A + u_X^B} \end{cases} \quad (15)$$

when $u_X^A = 0 \ \wedge \ u_X^A = 0$:

$$\begin{cases} b_{x_i}^{A\Diamond B} = \gamma b_{x_i}^A + (1-\gamma) b_{x_i}^B \\ u_X^{A\Diamond B} = 0 \end{cases},$$

where

$$\gamma = \lim_{\substack{u_X^A \to 0 \\ u_X^B \to 0}} \frac{u_X^B}{u_X^A + u_X^B} \quad (16)$$

Then $\omega_X^{A\Diamond B}$ is called the cumulatively fused opinion of ω_X^A and ω_X^B, representing the combination of independent opinions of A and B. By using the symbol '$\underline{\oplus}$' to designate this belief operator, we define:

$$\omega_X^{A\Diamond B} \equiv \omega_X^A \underline{\oplus} \omega_X^B \quad (17)$$

The global ratings $\vec{R}_F$ can be computed by combining the two fusion operator above, and then the global expectation is:

$$E_A(x_i) = \frac{R_F(x_i) + Ca_F(x_i)}{C + \sum_{j=1}^k R_F(x_j)}, i = 1,2,3 \quad (18)$$

The global trust can be calculated as follows:

$$A = \sum_{i=1}^k \varepsilon(x_i) E_A(x_i), i = 1,2,3 \quad (19)$$

3.6. Calculation of the Risk Value Ri

There are problems simply considering the reputation value, it lacks sensitivity to perceive the disorder behavior of the peers, and unable to identify malicious peers. In this paper risk reflects the recent level of the peers' reliability. The value of the risk Ri is composed of Local expectations of negative ratings $\vec{E}_L$, global expectations of negative ratings $\vec{E}_A$ and Risk components of the uncertainty in opinion u_X. Then the risk can be expressed as:

$$Ri = \lambda E_L(x_1) + (1-\lambda) E_A(x_1) + (1 - a_F(x_1)) u_X \quad (20)$$

where λ is the weight of the local expectation, (1-λ) is the weight of global expectation, $(1 - a_F(x_1))$ is the level of contribution of the uncertainty in the opinion to the risk. $\vec{a}_F$ is the base rate.

u_X can be gotten from the Formula (4):

$$u_X = \frac{C}{C + \sum_{j=1}^k R_{y,t,D_R}(x_j)}$$

When the negative ratings are multinomial, for example $R(x_1), R(x_2) \ldots R(x_3)$ are all negative ratings, we should introduce a parameter ρ for the weight of different level, $P_R(x_1) > P_R(x_2) > \ldots P_R(x_n)$, then:

$$Ri = \sum_{i=1}^n \rho_{R(x_i)} (\gamma E_L(x_i) + (1-\gamma) E_A(x_i) + (1 - a_F(x_i)) u_X) \quad (21)$$

The introduction of risk has two functions. On one hand, it is more accurately to reflect the trust value combining with the reputation. When there are more good interactions, the risk value will be small, and then the effect of the risk value on the trust value will be smaller. On the contrary, when there are more bad interactions, the risk value will be larger, and the trust value will be decreased. So considering the risk can be considered as an punishment to the malicious peers. On the other hand, because the risk comes from the interactive history of failure, risk value is determined by the degree of these failures, the larger the degree of loss is, the greater the risk is. The risk values can be used as a prediction of its future behavior. So, it can be used as an effective means to identify malicious peers.

4. Simulation and Analysis

4.1. Experimental Environments

Simulating Peer-to-Peer (P2P) overlay networks is a common problem for researchers and developers. Several solutions exist to solve this problem. The PeerSim P2P simulator proposed by BISON [18] is one of the most known among researchers. All the simulations in this paper are based on PeerSim [19]. The philosophy of PeerSim is to use a modular approach, as the preferred way of coding with it is to re-use existing modules. These modules can be of different kinds, for example there are modules which can construct and initialize the underlying network, modules which can handle the different protocols, modules to control and modify the network and so on. PeerSim offers a lot of these modules in its sources, which ease greatly the coding of new applications. PeerSim 1.0 supports two simulation models: the cycle-based model and a more traditional event-based

model. Simulations in this paper use the former model. The main interfaces on which the PeerSim is based are listed as follows:

1) Peer: The P2P network is composed of peers. A peer is a container of protocols. The peer interface provides access to the protocols it holds and a fixed ID of the peer.

2) Protocol: It defines the behaviors of peers in the network.

3) Control: Classes implementing this interface can be scheduled for execution at certain points during the simulation. These classes typically observe or modify the simulation.

4) Linkable: Typically implemented by protocols, this interface provides a service to other protocols to access a set of neighbor peers. The instances of the same linkable protocol class over the peers define an overlay network.

A more detail introduction of PeerSim is shown in reference [19]. As a reference, we simulate the EigenRep [20] model simultaneously.

Assume there is a file sharing system, users need to download some files from it, and then authenticity of the file is the unique criterion for judging whether the interaction is successful or not. Here, we assume the file-sharing network is ideal, which is any user can find any files (It may be inauthentic) they want and all peers that are claimed as owner of them. Users take simple action, they choose the trust worthiest one among all the peers that are claimed as owners of needed files, and then the users interact with it (download).

Given a simulation network with 1000 peers, assume there are 10000 files. We allocate the files to 1000 peers randomly. Among these peers, the malicious ones take percentage from 0.1 to 0.5. Assume we can location all the files of the system in our simulation, and each file is owned by at least one good peer, every peer must accomplish 100 times of interaction in the whole simulation. In every interaction, objects choose one file randomly from the files that they have never owned and downloaded. Successful interaction makes the users own these files, and failed interaction would not increase user's files. In the whole simulation, every peer chooses one file that it does not own to download. If users own the files finally, then the download succeeds, otherwise, it fails. The ratio of successful times to failed times is called successful probability of interaction.

We design the several types of peers as following:

1) Good peers. Both the service they offered and their evaluation to other peers are all authentic.

2) Malicious peers.

a) General malicious peers. This type of peers offers virtual service only, and they offer authentic files at a probability of 40% for every service request.

b) Collusive malicious peers. This type of peers decry good peers while exaggerating their cahoots, they offer virtual upload service.

c) Strategy malicious peers. This type of peers adopt certain strategy when uploading, they may offer authentic files at different probability according to different cases. In details, they offer authentic files at a low probability when trust value is high, while offer authentic files at a high probability when trust value is low. In this way, they maintain their trust value at a credible threshold that the system defined, in case of being detected.

The initial trust values are defined as 0.5; parameters of the model are defined in Table 2.

4.2. Simulation results and analysis

4.2.1. The Trust Value Variation of the Four Types of Peers as the Interaction Times Increases

Figure 2 illustrates the trust value trend of the four types of peers as the increasing of interaction times. As shown in the figure, the trust value of good peers increases gradually, while that of general malicious peers decrease rapidly. The trust value of strategy malicious peers undulate to some extent, that is because these peers are cunning, it is hard to identify them, and however, their trust value trend is decrease on the whole. We can see that the model illustrates the trust value of peers' changes with interaction times, what is just as expected.

4.2.2. Influence of Percentage of General Malicious Peers on Successful Interaction Ratio

Figure 3 shows the variation of successful interaction probability of MSL-TM as variation of the ratio of malicious peers takes under the mode of no-reputation system and EigenRep as well as two parameters. Assume good peers offer authentic files at a probability of 0.97% in the

Table 2. Simulation parameters and their values.

Parameter	α	β	γ	k	λ	C
Value	0.7 or 1	0.3 or 0	0.7	0.6	0.7	2

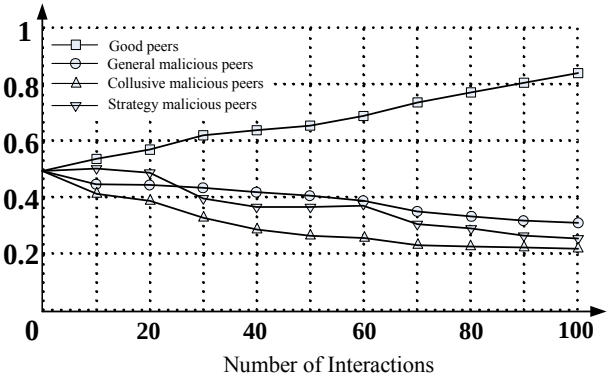

Figure 2. Variation of the four types of peers as the time of interaction increases.

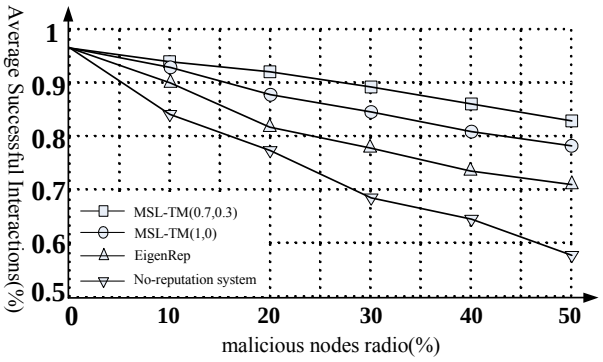

Figure 3. Influence of percentage of general malicious peers to successful interaction ratio.

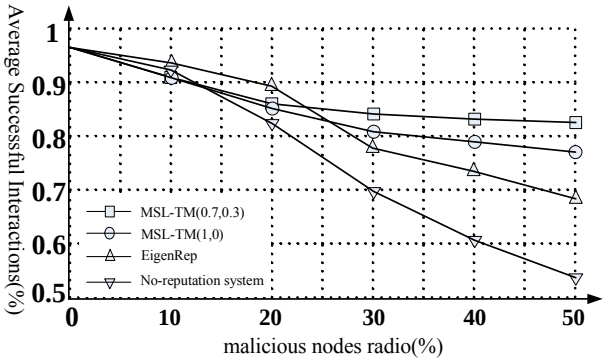

Figure 4. Influence of percentage of collusive malicious peers to successful interaction ratio.

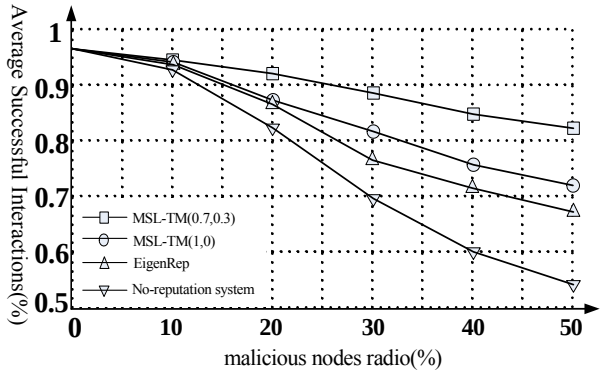

Figure 5. Influence of percentage of strategy malicious peers to successful interaction ratio.

simulation, while general malicious peers do at a probability of 40% in order to hide their malicious action. As the figure illustrates, interaction probability is 97% when there is not malicious peers. However, the no-reputation system, without any precaution and defense, it's the successful interaction probability of decrease rapidly as malicious peers increase. EigenRep is short of punish strategy for the malicious peers that offer authentic service at certain probability, so the successful interaction probability decreases obviously; MSL-TM (0.7,0.3)shows strong superiority as introduces risk factor(β =0.3). The reason of it is that this model quantifies risk with expectation and indeterminacy, and then we are surer about actions of peers.

4.2.3. Influence of Percentage of Collusive Malicious Peers on Successful Interaction Ratio

Collusive malicious peers decry all good peers that have interacted with it and exaggerate their cahoots, they try to destroy the validity of network by decreasing the trust value of authentic peers and increasing that of their cahoots. This is a serious cooperative cheat actually. From the result and comparation as illustrated in Figure 4, we can see the influence of decry and magnify on successful interaction probability is not obvious, the reason is that no-reputation system and EigenRep is lack of punishment strategy. However, as virtual services that malicious peers offered increase, the interaction probability of system decrease obviously. Our model introduces rating credibility and risk factor, though the successful identification ratio of collusive may decrease in the beginning, it becomes stable as restrain to malicious peers. This model can reach a successful rate of 80% under the condition that fifty percent of peers are collusive malicious peers, it can depress influence of decry and magnify effectively.

4.2.4. Influence of Percentage of Strategy Malicious Peers on Successful Interaction Ratio

Strategy malicious peers are cunning, they have a latent period. Assume this kind of peers provide true files at a probability of 30% when trust value is above 0.6, otherwise, at a probability of 0.6, we call the peers with trust value below 0.5 as incredible peers. As shown in Figure 5, strategy malicious peers hide it by providing true files in the beginning, so there is very little difference from the successful interaction ratio of these mechanisms. As the number of interaction increases, malicious action of some peers begins expose. But as EigenRep does not take any action, it cannot identify their dynamic action. Besides, it has not any punishment mechanism to cheating, so successful interaction ratio decreases largely as the percentage of malicious peers increases. The successful probability of MSL-TM (0.7, 0.3) which considers risk decrease less than that of MSL-TM (1,0) which takes reputation into account only. This told us the importance of computing risk value, and it is accurate to quantify risk with expectation and indeterminacy. The experiment result proves that MSL-TM is robust to risk in condition that percentage of malicious peers variant.

5. Conclusions

In this paper, we take multinomial subjective logic as

basis, adopt multinomial ratings, and compute expected value of opinions with Dirichlet distribution function, with which we can get the reputation value and risk value of peers, and get trust level of peers finally. We quantify risk with expectation and indeterminacy to hold actions of peers more accurate, which improves successful interaction probability. The experiment results show that MSL-TM is robust to resist risks in condition that percentage of malicious peers' changes, this is prior to existed models in many indexes. We will further improve subjective logic in our future research, such as doing research of dynamic of prior const C to make it more reality, and decreasing complexity of our model, so that it can serve for P2P much better.

6. Acknowledgements

This work is supported by the National Natural Science Foundation of China under Grant No. 60873203, the Natural Science Foundation of Hebei Province under Grant No. F2008000646, and the Guidance Program of the Department of Science and Technology in Hebei Province under Grant No. 072135192.

7. References

[1] Ramaswamy and L. L1, "Freeriding: A new challenge to peer-to-peer file sharing systems," in 36th Annual Hawaii International Conference on System Sciences (HICSS236), 2003.

[2] C. Lin and X. H. Peng, "Research on trustworthy networks," Chinese Journal of Computers, Vol. 28, No. 5, pp. 751–758, May 2005.

[3] D. S. Peng, C. Lin, and W. D. Liu, "A distributed trust mechanism directly evaluating reputation of nodes," Journal of Software, Vol. 19, No. 4, pp. 946–955, April 2008.

[4] X. Y. Li and X. L. Gui, "Research on dynamic trust model for large scale distributed environment," Journal of Software, Vol. 18, No. 6, pp. 1510–1521, June 2007.

[5] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," in J. Dale, G Dinolt, editors, Proceedings of the 17th Symposium on Security and Privacy, Oakland, IEEE Computer Society Press, CA, pp. 64–173, 1996.

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

[7] L. Xiong and L. Liu, "A reputation-based trust model for peer-to-peer ecommerce communities," Proceedings of IEEE International Conference on Electronic Commerce, New York, pp. 228–229, 2003.

[8] C. Q. Tian, S. H. Zou, W. D. Wang, and S. D. Cheng, "Trust model based on reputation for peer-to-peer networks," Journal on Communications, Vol. 29, No. 4, pp. 63–70, 2008.

[9] A. Jøsang, "A logic for uncertain probabilities," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, Vol. 9, No. 3, pp. 279–311, June 2001.

[10] A. Jøsang, "The consensus operator for combining beliefs," Artificial Intelligence Journal, Vol. 142, No. 12, pp. 157–170, October 2002.

[11] A. Jøsang, "Probabilistic logic under uncertainty," in the Proceedings of Computing: The Australian Theory Symposium (CATS2007), CRPIT, Vol. 65, Ballarat, Australia, January 2007.

[12] A. Jøsang and R. Ismail, "The beta reputation system," in Proceedings of the 15th Bled Electronic Commerce Conference, Bled, Slovenia, June 2002.

[13] A. Jøsang, "Conditional reasoning with subjective logic," Journal of Multiple-Valued Logic and Soft Computing, Vol. 14, No. 2–3, pp. 155–185, 2008.

[14] A. Jøsang, "Cumulative and averaging unfusion of beliefs," in the Proceedings of the International Conference on Information Processing and Management of Uncertainty (IPMU2008), Malaga, June 2008.

[15] A. Jøsang and H. J. Dirichlet, "Reputation systems," In the Proceedings of the International Conference on Availability, Reliability and Security (ARES), Vienna, Austria, April 2007.

[16] B. A. Huberman and F. Wu, "The dynamics of reputations," Journal of Statistical Mechanics: Theory and Experiment, Vol. 4, pp. 1−17, 2004.

[17] W. Yuan, J. S. Li, and P. L. Hong, "Distributed peer-to-peer trust model and computer simulation," Journal of System Simulation, Vol. 18, No. 4, pp. 938−942, 2006.

[18] BISON, http://www.cs.unibo.it/bison/.

[19] PeerSim, http://peersim.sourceforge.net/.

[20] S. D. Kamvar and M. T. Schlosser, "EigenRep: Reputation management in P2P networks," in S. Lawrence, editor, Proceedings of the 12th International World Wide Web Conference, ACM Press, Budapest, pp. 123–134, May 2003.

