http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 10 (4): 759-768, 2011
ISSN 1812-5638 / DOI: 10.3923/itj.2011.759.768

Research on Trust Cloud-based Subjective Trust Management Model under Open Network Environment

[1]Yu Dingguo, [2]Chen Nan and [1]Tan Chengxiang
[1]Department of Computer, Tongji University, Shanghai 201804, China
[2]School of Qianjiang, Hangzhou Normal University, Hangzhou 310012, China

Abstract: The key to the study of subjective trust management is how to obtain and evaluate trust knowledge. Based on cloud model, this study proposes a trust cloud-based subjective trust assessment and management model, provides the design of trust cloud and the policy of the obtainment and computing of trust information and supply a method of trust decision based on trust cloud model. Trust cloud model can efficiently unify the fuzziness, randomness and uncertainty of the subjective trust.

Key words: Trust management, trust assessment, subjective trust, cloud model, trust cloud, trust decision

INTRODUCTION

With the development and popularity of the Internet, large number of emerging network application services appear, such as electronic commerce, P2P file sharing, etc. Under these emerging application environments, features like the strangeness of users, huge number of resources, heterogeneous operating environment and dynamics and autonomy of active targets turn up. There are certain risks exist in the interaction between networks entities, fraud often occurs (Wang and Li, 2003). How to solve the trust and security problems under open network environment has become a major challenge.

Traditional access control technology which based on the authentication and authorization of the resource requestor cannot meet the requirements of trust management under open network environment. Some trust management systems like policymaker (Blaze *et al.*, 1998), remains some drawbacks such as singleness of protected object, asymmetry of trust information, too much emphasis on certificates and access control policy and ignore the impact of reputation on trust, etc.

Trust is a universal and important concept in human society and trust mechanism will also be an important complement to the network security mechanisms. There is great similarity between recommendations based trust model and interpersonal social networks, a node's trust judgment to the trading objects on the basis of its transaction history and the recommendation of friend nodes. This trust management mechanism has been extensively studied, this study will further discuss and study it.

Currently the study on the trust relationships between entities under open network environment mainly focuses on two aspects: objective trust and subjective trust. Objective trust, an evidence-based relationship, can be accurately described, reasoned and verified. Its presentation is the trust management systems: PolicyMaker (Blaze *et al.*, 1998) and KeyNote (Blaze *et al.*, 1999), which proposed by Blaze *et al.* (1998). Subjective trust, essentially based on reputation, has the feature of fuzziness, randomness and uncertainty. It cannot be accurately described and verified. The research of subjective trust mainly refers to social trust network model.

Subjective trust model can be divided into local trust model and global trust model. In local trust model, a node first consult the recommended level of a certain node from its neighbor nodes, then integrate the history of transactions between itself and this node and finally determines trust value. The purpose of the introduction of the global trust model is to weaken the effect of malicious nodes' collaborative cheating. In this model, a node has a unique global trust value and it integrates all the trust valuation of the whole network, so a malicious node cannot obtain a high trust value just by false valuation given by its several acquainted partners (Wang and Vassileva, 2003).

Currently, the measure and formal modeling of subjective trust mainly focus on probability theory, fuzzy set theory and artificial intelligence theory. Based on the expect for entity to complete the task, literatures (Beth *et al.*, 1994; Josang and Knapskog, 1998; Josang, 1999; Wang and Vassileva, 2003) calculate the probability for entity to complete the task according to positive and

Corresponding Author: Yu Dingguo, Department of Computer, Tongji University, Shanghai 201804, China

negative experience and measure the entity's trust value by this probability. The drawback is that they make the ambiguity and uncertainty equal to random; Literatures (Song *et al*., 2005; Zhang and Yang, 2005; Chen and Ye, 2008) refers to the trust mechanism between interpersonal social relationship and calculate the node's local trust value by knowledge of fuzzy logic reasoning on the basis of fuzzy reasoning theory, finally aggregate global reputation. When the node's global reputation is calculated by fuzzy logic inference rules, the rate of detecting malicious nodes is always high. The trust model proposed by literatures (Yu and Singh, 2002; Junmao *et al*., 2005; Tian *et al*., 2008) denote the valuation of a node to a trading node as an evidence of the support to it and make use of D-S evidence combination rules to combine all the evidences from the recommenders as a node's trust value.

Using probability to quantify the random or using fuzzy mathematics-related tools to determine the fuzzy value is the method to study the uncertainty of subjective trust from different aspects, but all fail to comprehensively assess the trust information. Besides, the result of studying trust relationship all comes down to accurate numeric by using axiomatic methods in probability theory or fuzzy mathematics-related tools, resulting in the lack of ambiguity of trust information, so study in this way will have serious limitations.

We designed and implemented one trust cloud-based subjective trust management system for our project Trust Management under Open Network Environment in Shanghai, China, from 2009 to 2010. In this study, we will introduce our model-the subjective trust management model based on trust cloud.

CLOUD MODEL

Concept of cloud

Def. 1: Cloud (Deyi *et al*., 1995). Let U be a domian represented by accurate numeric. Ã is a certain corresponding qualitative concept in U. Quantitative value x∈U is a random realization of qualitative concept. For any one of the elements x in domain U, there exists a random number $y = \mu_{\tilde{A}}(x) \in [0, 1]$ with stable tendency, i.e., μ: U→[0, 1], ∀x ∈ U, x→μ(x). $\mu_{\tilde{A}}(x)$ is called the certainty degree of x to Ã. The distribution of x in domain U is called cloud and each (x, y) is called cloud droplet.

Cloud is donated by three numerical characteristics: Ex (Expectation), En (Entropy) and He (Hyper entropy). C(Ex, En, He) is called eigenvector of cloud and the numerical characteristics of cloud are shown in Fig. 1. Ex is the most suitable representation of this qualitative concept point-Ã in the domain and is the most typical sample point of this quantity concept; En represents the size range accepted by qualitative concept, ie ambiguity and is also the measure of uncertainty of qualitative concept. En is decided by both randomness and fuzziness of concept; He is the measure of uncertainty of the entropy and can be understood as the entropy of En.

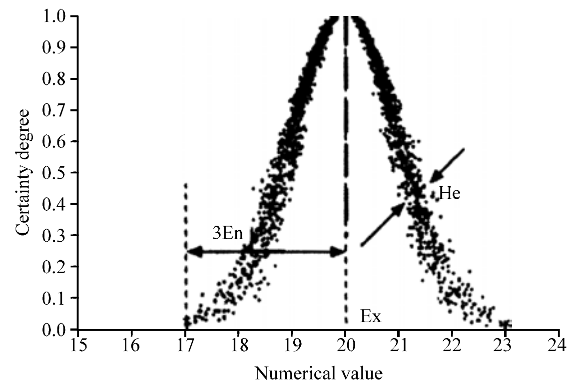

Fig. 1: Numeric characteristics of cloud

One-dimensional normal cloud

Def. 2: One-dimensional normal cloud (Li and Liu, 2004; Wang *et al*., 2008). Let U be a domian represented by accurate numeric. C is a certain corresponding qualitative concept in U. Quantitative value x∈U is a random realization of qualitative concept. If x meets: $x \sim N(Ex, En'^2)$ in which $En' \sim N(En, He^2)$ and the certainty degree of x to C meets the formula:

$$\mu = e^{-\frac{(x-Ex)^2}{2(En')^2}}$$

then, the distribution of x in domain U is called one-dimensional normal cloud.

In one-dimensional normal cloud, the contribution of cloud droplets to the concept is different and the whole contribution of all the elements in domian U to concept C is 1. Since,

$$\frac{1}{\sqrt{2\pi}En}\int_{Ex-3En}^{Ex+3En} \mu_{\tilde{A}}(x)dx = 99.74\%$$

so, the main contribution in domain U to qualitative concept C falls into the range [Ex-3En, Ex+ 3En], the contribution of the cloud droplet elements which falls outside the range to the qualitative concept can be neglected. This is the normal cloud's 3En rules (Huang and Wang, 2008).

Cloud generator

Cloud generation algorithm is called cloud generator (Deyi *et al*., 1995). There are mainly two kinds of generators: forward and backward cloud generator. Forward cloud generator generates the required number of cloud droplets under the circumstance that the cloud eigenvector C(Ex, En, He) is known. Backward cloud generator calculates the cloud eigenvector C(Ex, En, He) according to certain number of data. Algorithms 1 and 2 are forward and backward cloud generator algorithm of one-dimensional normal cloud, respectively (Deyi *et al*., 1995; Lu and Wu, 2009; Liu *et al*., 2004).

Algorithm 1: Forward cloud generator algorithm of one-dimensional normal cloud

Input: Cloud eigenvector C(Ex, En, He) and the number of cloud droplet N
Output: N cloud droplets
Algorithm steps:

1 Generate a normal random number En' whose expectation is En and standard deviation is He;
2 Generate a normal random number x whose expectation is Ex and absolute value of standard deviation is En';
3 Calculate:

$$y = e^{-\frac{(x-Ex)^2}{2(En')^2}}$$

4 Make (x,y) a cloud droplet;
5 Repeat step 1-4 until N cloud droplets are generated

Algorithm 2: Backward cloud generator algorithm of one-dimensional normal cloud

Input: N cloud droplets: x_i
Output: Cloud eigenvector C(Ex, En, He)
Algorithm steps:

1 Calculate sample mean of the set of data according to x_i:

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$$

Sample variance:

$$S^2 = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x})^2$$

Standard deviation:

$$std = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2}$$

2 $Ex = \bar{x}$
3 En = std
4 $He = \sqrt{s^2 - En^2}$
5 Output C(Ex, En, He)

TRUST CLOUD MODEL

Concept of trust cloud

Trust cloud is a special cloud model, which describes the trust relationship between entities in the form of cloud.

Def. 3: Trust valuation space (Wang *et al*., 2008): Trust valuation space TD is an ordered collection of values in quantitative domain range [0,n], noted as <0,n> and the collection is made up of continuous or discrete monotone values. Each value of the ordered collection represents the trust degree of the subject to the object. n is a positive integer, 0 and n is respectively the lower and upper limit of the trust degree of TD. And the closer the subjective trust degree is to 0, the lower the objective trust degree is; the closer the subjective trust degree is to n, the higher the objective trust degree is.

Def. 4: Trust space (Wang *et al*., 2008): Trust space TS is an ordered concept collection which can qualitatively express subjective trust and it uses qualitative concept to express subjective trust degree. One or several trust levels can be preset for TS, which can be neglected also.

Def. 5: Trust cloud: Trust cloud describes subjective trust concept by one-dimensional normal cloud model. Trust space TD is the quantitative domain U of the cloud and trust space TS is a qualitative trust concept collection. $x \in TD$ is a quantitative trust valuation of qualitative concept $e \in TS$. Among them, the certainty degree of x to e, $y = \mu(x) \in [0, 1]$, is a random number with stable tendency, i.e., $\mu: TD \to [0, 1], \forall x \in TD, x \to \mu(x)$, among them the distribution of x in domain U is called trust cloud and each (x,y) is called a cloud droplet.

Trust cloud can be expressed as: TC(Ex, En, He), among them Ex is trust expectation, reflecting the basic trust degree; En is trust entropy, reflecting the uncertainty of trust relationship; He is trust hyper entropy, reflecting the uncertainty of trust entropy.

The merger of trust cloud

The merger of trust cloud means merge several trust clouds with the same character into a new trust cloud. That can be understood as merging several property trust clouds of entities into an integrated trust cloud, or as merging valuation trust clouds of entities in several time points into an integrated trust cloud.

Def. 6: Let TC (Ex, En, He) is a trust cloud and k is a positive constant. Trust cloud TC (kEx, kEn, He) is called the product of trust cloud TC and k and noted as k×TC. (Huang and Wang, 2008).

Def. 7: (Lu and Wu, 2008). Let trust cloud TC_1 (Ex_1,En_1,He_1) and TC_2 (Ex_2,En_2,He_2), the trust cloud TC(Ex,En,He) = TC ((Ex_1,Ex_2), (En_1,En_2), (He_1,He_2)) represents the merger of TC_1 and TC_2, noted as $TC_1 \oplus TC_2$. Among them:

$$Ex = (Ex_1, Ex_2) = \frac{1}{2}(Ex_1 + Ex_2) \quad (1)$$

$$En = (En_1, En_2) = \frac{1}{2}\sqrt{En_1^2 + En_2^2} \quad (2)$$

$$He = (He_1, He_2) = \frac{1}{2}(He_1 + He_2) \quad (3)$$

When we merge several property trust clouds of entities into an integrated trust cloud, because of the difference of the attributes' weights in trust valuation, in the course of merger we need to take weight factor of each attribute trust cloud into consideration and the weight factor is notes as:

$$\omega = \{\omega_i \mid \omega_i > 0, \sum_{i=1}^{m} \omega_i = 1\}$$

According to Def. 6 and 7, the weighted merging formula of m attribute trust clouds is:

$$TC(Ex,En,He) = (\omega_1 \times TC_1) \oplus (\omega_2 \times TC_2) \oplus \cdots \oplus (\omega_m \times TC_m)$$

among them:

$$Ex = (\omega_1 \times Ex_1, \omega_2 \times Ex_2, \cdots, \omega_m \times Ex_m) = \frac{1}{m}\sum_{i=1}^{m} \omega_i Ex_i \quad (4)$$

$$En = (\omega_1 \times En_1, \omega_2 \times En_2, \cdots, \omega_m \times En_m) = \frac{1}{m}\sqrt{\sum_{i=1}^{m} (\omega_i En_i)^2} \quad (5)$$

$$He = (He_1, He_2, \cdots, He_m) = \frac{1}{m}\sum_{i=1}^{m} He_i \quad (6)$$

Transfer of trust cloud

The transfer of trust information is to transfer the trust information provided by recommendation entities to trust evaluator; the value is decided by the recommendation trust of the evaluator to the recommendation entity and the direct trust of the recommendation entity to the evaluator.

Def. 8: (Lu and Wu , 2008). TC_{AB} (Ex_{AB}, En_{AB}, He_{AB}) and TC_{BC} (Ex_{BC}, En_{BC}, He_{BC}), respectively represents the trust cloud of Entity A to Entity B and the trust cloud of Entity B to Entity C, then the trust cloud of Entity A to Entity C is TC_{AC}, noted as TC_{AC} (Ex_{AC}, En_{AC}, He_{AC}) = $TC_{AB} \otimes TC_{BC}$. Among them:

$$Ex_{AC} = Ex_{AB} \times Ex_{BC} \quad (7)$$

$$En_{AC} = Min(\sqrt{En_{AB}^2 + En_{BC}^2}, 1) \quad (8)$$

$$He_{AC} = Min(\sqrt{He_{AB}^2 + He_{BC}^2}, 1) \quad (9)$$

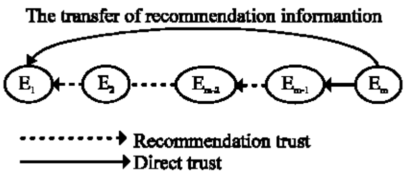

Fig. 2: Course of trust information transfer

If the trust information recommended by a recommendation entity also comes from another recommendation entity, such trust information will form a recommendation path through recommendation relationship and the end of the path is the recommendation entity with direct experience of those to be evaluated. As Fig. 2 shows, there are m entities $E_1, E_2, ..., E_m$ in the trust transfer network, among them $TC_i = (Ex_i, En_i, He_i)$ represents the trust cloud of entity E_i to entity E_{i+1} and $TC_{1,m}(Ex_{1,m}, En_{1,m}, He_{1,m})$ = $TC_1 \otimes TC_2 \otimes ... \otimes TC_m$, represents the trust expression to entity E_m obtained by entity E_m by the transfer chain of trust information.

We can see from Def. 8 that $TC_{1,m}(Ex_{1,m}, En_{1,m}, He_{1,m})$ = $TC_1 \otimes TC_2 \otimes ... \otimes TC_m$ which is described in Fig. 2. Among them:

$$Ex_{1,m} = \prod_{i=1}^{m} Ex_i \quad (10)$$

$$En_{AC} = Min(\sqrt{\sum_{i=1}^{m} En_i^{\,2}}, 1) \quad (11)$$

$$He_{AC} = Min(\sqrt{\sum_{i=1}^{m} He_i^{\,2}}, 1) \quad (12)$$

Comparison of trust cloud

In the security system based on subjective trust valuation and management, the policy to determine whether a node is safe is always based on preset trust threshold. If the trust value of a node calculated by trust valuation model is higher than this threshold, then the node is considered as safe and entities can choose to trade with it.

In subjective trust valuation model based on trust cloud model, trust cloud model is represented by three characteristic numeric Ex, En and He. So, the preset threshold is also the trust cloud represented by three characteristic parameters and such trust cloud is called benchmark cloud which can be expressed as TCS(Exs,Ens,Hes). The trust cloud of potential collaborators obtained by trust valuation is called comparison cloud which can be expressed as TCC(Exc,Enc,Hec).

Algorithm 3: The comparison algorithm of trust cloud

Input: Benchmark cloud TCS(Exs,Ens,Hes) and comparison cloud TCC(Exc,Enc,Hec)
Output: Comparison result(trust/mistrust)
Algorithm Steps:

```
1 if (Enc/Hec<5) return mistrust;
  // the discreteness degree of comparison
  //cloud is high
2 if (Exc≥Exs)
  2.1 if (Enc≤Ens) return trust;
  //the trust base of comparison cloud is high while
  // the uncertainty is low
  2.2 else
    2.2.1 if (Exc-3Enc≥Exs-3Ens) return trust;
    //the uncertainty of comparison cloud is high
    //while the overall trust value is higher than that of benchmark cloud
    2.2.2 else
      The result is determined by similarity measurement algorithm of
      trust cloud;
3 else //(Exc<Exs);
  3.1 if (Enc≥Ens)return mistrust;
    // the trust base of comparison cloud is low
    //while the uncertainty is high;
  3.2 else //(Exc<Exs)&&(Enc<Ens);
    3.2.1 if(Exc-3Enc≥Exs-3Ens)
      The result is determined by similarity measurement algorithm of
      trust cloud;
    3.2.2 else return mistrust;
      //the overall trust value of comparison
      //cloud is lower than that of benchmark cloud:
```

The comparison policies of trust cloud involves the similarity concept of trust cloud and if you want to know the related similarity definition and measurement algorithm, please refer to Literatures (Lu and Wu, 2009; Zhang *et al*., 2004). In the following page we will provide the comparison algorithm of trust cloud by integrated Literature (Lu and Wu, 2009; Zhang *et al*., 2004).

From Algorithm 3 and Fig. 3, we can analyze the form of comparison cloud and benchmark cloud by category (Lu and Wu, 2009):

- In the situation when the expectation of comparison cloud is higher than that of benchmark cloud while the entropy is lower than that of benchmark cloud is the ideal form. Such form must meet the trust requirement
- In the situation when the expectation of comparison cloud is lower than that of benchmark cloud while the entropy is higher than that of benchmark cloud, both parameter standards are lower than those of standard cloud. So such situation obviously doesn't meet the requirement.
- When the expectation of comparison cloud is higher than that of benchmark cloud and the entropy is also

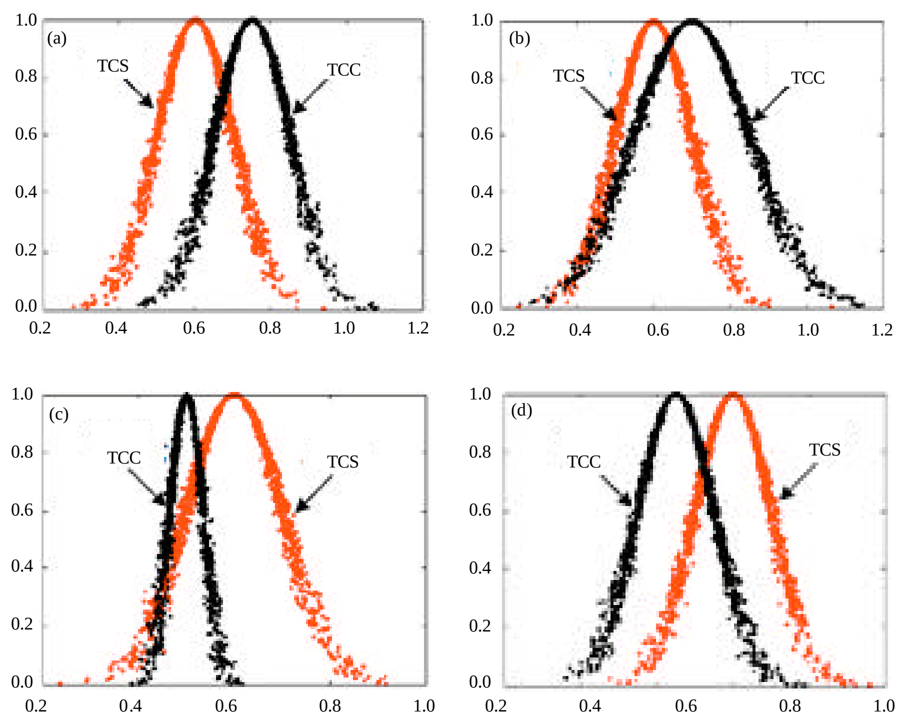

Fig. 3: Comparison cloud and benchmark cloud. (a) Exc≥Exs && Exc-3Enc≥Exs-3Ens, (b) Exc≥Exs && Exc-3Enc≤Exs-3Ens, (c) Exc<Exs && Exc-3Enc≥Exs-3Ens and (d) Exc<Exs && Exc-3Enc≤Exs-3Ens

higher than that of benchmark cloud, the distribution range of comparison cloud needs to be determined. If the Ex-3En value of comparison cloud is higher than the relative value of benchmark cloud, which means the overall trust value of comparison cloud is higher than that of benchmark cloud and the form of comparison cloud is shown as the location on the right side of benchmark cloud. Such situation can be considered as in accordance with trust requirement, as shown in Fig. 3a; it is a comparatively complicated situation when the Ex-3En value of comparison cloud is lower than the relative value of benchmark cloud, the result can be determined by similarity measurement algorithm of trust cloud, as shown in Fig. 3b

- The situation when the expectation of comparison cloud is lower than that of benchmark cloud and the entropy is also lower than that of benchmark cloud should be considered by category too. If the Ex-3En value of comparison cloud is higher than the relative value of benchmark cloud, the result needs to be further determined by similarity measurement algorithm of trust cloud, as shown in Fig. 3c; if the Ex-3En value of comparison cloud is lower than the relative value of benchmark cloud, that means the overall trust value of comparison cloud is lower than that of benchmark cloud and the form of comparison cloud is shown as the location on the left side of benchmark cloud. Such situation can be considered as not in accordance with trust requirement, as shown in Fig. 3d

TRUST CLOUD-BASED SUBJECTIVE TRUST VALUATION AND MANAGEMENT POLICY

Design of trust cloud

The subjective trust valuation between entities in open network depends on the judgment to the history trading behavior of each other and the satisfaction degree of the judgment result determines the trust degree of an entity.

In this study, we use numeric collection [0, 0.25, 0.5, 0.75, 1] as the trust space TD and use discrete data scale to describe the trust degree. Collection [Very Dissatisfied, Dissatisfied, No Comment, Satisfied, Very Satisfied] represents trust space TS and the trust degree is divided into 5 levels. The correspondence between trust space and trust degree space is shown as Table 1.

Def. 9: Trust vector: Trust vector is the corresponding N-dimensional vector space to trust level N of trust space and the vector corresponding to trust level is also the history accumulation description of the judgment result of the trading behaviour to the target entity.

Table 1: Description and scale of trust degree

Trust Level	Trust description	Scale
1	Very satisfied	1.00
2	Satisfied	0.75
3	No comment	0.50
4	Dissatisfied	0.25
5	Very dissatisfied	0.00

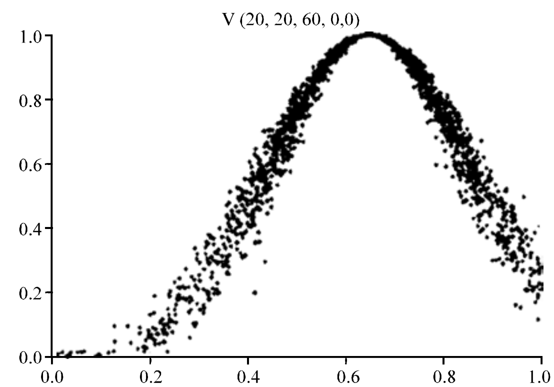

Fig. 4: The trust cloud expressed by trust vector

We have designed five trust level mentioned above and the corresponding trust vector is a 5-dimensional vector space. If there are totally 100 trading behaviors between entity A and entity B and the valuations of B from A are respectively very satisfied for 20 times, satisfied for 20 times and no comment for the rest times, then the trust vector of A to B can be expressed as $V_{AB} = (20, 20, 60, 0, 0)$.

After inputting trust vector into the backward cloud generator, we can get three characteristic parameters of the trust cloud and then the complete cloud figure can be described by the forward cloud generator. Figure 4 shows cloud description of the trust relationship expressed by trust vector $V_{AB} = (20, 20, 60, 0, 0)$.

Obtain of trust information

In the trust cloud-based subjective trust valuation model described in this study, trust information is made up of direct experience and local recommendation information, i.e., integrated trust cloud is made up of direct trust cloud and recommendation trust cloud, as shown in the following formula:

$$TC = \rho \cdot TC_{dir} \oplus (1-\rho) \cdot TC_{rec} \quad (0 \le \rho \le 1) \tag{13}$$

TC is an integrated trust cloud; TC_{dir} is the direct trust cloud generated by direct experience; TC_{rec} is the recommendation trust cloud generated by recommendation information; Parameter ρ is the proportion of direct information and recommendation information. If ρ = 1, then the integrated trust cloud is completely made up of direct trust cloud while none recommendation information is taken into consideration.

Calculation of direct information

Def. 10: Time window: Time window also, called time frame, is a time interval (the size of time window is equal to the interval length), which is used to represents the feedback to the trading behavior in this time interval. The window moves with the time, i.e. the end time of last window is the start time of the next window. The length of time window can be determined according to specific scenarios. If the interaction among entities is comparatively frequent, the length of window can be short; on the contrary, we can set the time window by a comparatively long period time. Besides, the number of window can also be determined according to specific scenarios.

To be brief, positive integer is used in this study to mark time window. The larger the number is, the closer the times is to now.

To each time window, there is a trust vector representing valuation result of the trading entity's behavior in this time window. If V^k_{AB} = (20, 30, 40, 8, 2) is the trust vector of A to B in time window W^k, then the corresponding trust cloud to the time window generated by cloud generator is TC^k_{AB}.

Besides, in order to calculate the trust degree of entities more accurately, we must differentiate the effect of different window trading results on the calculation of trust degree. In this model, we allocate different weight to different time windows according to the distance from now. The closer the time window is to now, the weight endowed is higher; the further the time window is to now, the weight endowed is lower. In addition, a kind of attenuation function is introduced and by making use of the restriction effect of such attenuation function, we achieve the goal that the allocation of the weight is more stable and reasonable.

Def. 11: Attenuation function f: When we calculate the trust degree, compared with the trading in time window k, the discount rate of the trading in time window n is called attenuation function, expressed as:

$$f(k) = \rho^{n-k},\quad 0 < \rho < 1,\quad 0 \le k \le n$$

By using the defined attenuation function f, each time window will have a corresponding attenuation factor (function value). For example, the corresponding attenuation factor to time window W^k is ρ^{n-k}. So, if the assistance attenuation factor occurred in current window is 1, then the attenuation amplitude is considered as 0; if the first time assistance attenuation factor is ρ^{n-1} compared with now, then the attenuation amplitude is the largest.

From the above analysis we can see, direct trust cloud is integrated by the corresponding trust clouds to each time window according to certain weight, i.e.,

$$TC_{dir} = f(1)\bullet TC^1_{dir} \oplus f(2)\bullet TC^2_{dir} \oplus \cdots \oplus f(k)\bullet TC^k_{dir} \oplus \cdots \oplus f(n)\bullet TC^n_{dir} \quad (14)$$

This time window-based trust calculation has the following advantages:

- It can indicate the time dimension of trust and enhance the dynamic adaptability
- On the other hand it can efficiently decrease the effect of large amount of dishonest feedback provided by collaborative fraud malicious nodes in a very short time on the accuracy of trust valuation

Calculation of recommendation cloud

In this study, we simulate the property of social trust network and use local recommendation policy. If we need to know the conduct of a stranger, we will first inquire about him from our friends. According to the trading history, the entity will send a trust information recommendation request to part of its most trusting entities. If current entity is A, now A need to get the trust valuation to Entity C from its most trusting friends, i.e., their recommendation information. There are N entities who have the history of trading with A at all and Entity A will respectively save the trust vectors of trading result valuation to them (including each time window), then we can directly generate their corresponding direct trust clouds TC_{A1}, TC_{A2},...,TC_{AN} and accept the most trusting previous $M(M \le N)$ trust clouds (M clouds with the largest Ex value) according to Ex parameter value of trust cloud. Suppose their Ex value are Ex_1,Ex_2,...,Ex_M, respectively and A send its recommendation request to them, then their feedback recommendation information can be expressed by trust cloud as TC_{1C},...,TC_{iC},...,TC_{MC} $(1 \le i \le M)$, respectively, in which we suppose each entity has done feedback. In addition, in order to relate recommendation information to direct experience, we will calculate recommendation cloud through the transmission form of trust cloud, so the trust cloud of the recommendation information of Entity C obtained by Entity A can be calculated by the following formula:

$$TC_{rec} = TC_{A1} \otimes TC_{1C} \oplus \cdots \oplus TC_{Ai} \otimes TC_{iC} \oplus \cdots \oplus TC_{AM} \otimes TC_{MC} \quad (15)$$

Changing rate of trust degree

The foundation and development of subjective trust relationship is a long-term and changing course, in which the essential characteristic of trust relationship is the object's trust degree is changing with the time and meanwhile the object's trust degree is also an important factor which should be considered in the course of trust decision. For example, in the two adjacent time windows, the change of different object's trust degree is not the same. Some objects' trust degree will be raised, but raising speed is also not the same; some objects' trust degree will fall down, but the falling speed is also not the same. The concept of changing rate of trust degree will be introduced in the following.

Def. 12: Changing rate of trust degree: The changing rate of trust degree means the changing rate of Ex value of objects' trust degree in adjacent windows and it can be calculated by the following formula:

$$Ex_{rate} = \frac{\Delta Ex}{\Delta t} = \frac{Ex_{i+1} - Ex_i}{t_{i+1} - t_i} \tag{16}$$

Ex_{i+1} and Ex_i, respectively represents the expectations of the subjective trust clouds of the objects' trust degree in adjacent two windows and t_{i+1} and t_i are the lower limits of these two time windows. Ex_{rate} represents the changing status of object's trust degree, and the trust degree has no change when $Ex_{rate} = 0$; the trust degree decreases when $Ex_{rate}<0$ and the more the absolute value of Ex_{rate} is, the more the trust degree decreases; the trust degree increases when $Ex_{rate}<0$ and the more the Absolute value of Ex_{rate} is, the more the trust degree increases.

Trust decision

In the trust cloud-based subjective trust valuation and management policy, trust decision will be divided into 3 cases:

- Judge whether the trust degree of the object meets the requirement needed

According to specific applications, we preset the corresponding benchmark cloud TCS(Exs,Ens,Hes), then compare the integrated trust cloud TCC(Exc,Enc,Hec) and benchmark cloud of the obtained object to be evaluated by the comparison algorithm of trust cloud, thus we can judge the whether the trust degree of the object meets the application requirements or not.

- Choose the best collaboration object from numbers of candidate objects

According to specific applications, we respectively calculate the integrated cloud of each object, then choose the object with relatively large expectation value Ex as the collaboration object; if the expectation values of two (or more) candidate objects do not have huge difference (the absolute value of the difference is lower than the threshold value), then we choose the object with relatively low trust entropy En as the collaboration object.

- Judge the trust changing trend of the object

We calculate the trust changing rate of the object to be evaluating and then judge the trust changing trend by trust changing rate.

EXPERIMENT AND RESULT ANALYSIS

The experiment proposed in this study take the method of simulation with real data to verify the trust decision method put forward in this study. According to the trust degree valuation data of the real object in a certain C2C shopping website, we collect the trust degree valuation data of 5 objects which provide similar products and the accumulative number of the subjective trust degree valuation of each object is above 800.

We use 5 levels to describe the subjective trust valuation of the website. The level can be expressed by the number of star. One-star means the lowest level and five-star means the highest level. The valuation result is added up in the experiment without the consideration of the effect of time on trust. So, time window and attenuation function are not needed is the experiment and the transfer and merger of trust will not be calculated.

Table 2 list the trust valuation data, the average of trust valuation data and the trust cloud eigenvalue calculated by trust cloud model of 5 objects (expressed as ABCDE).

From Table 2, the average of trust valuation data of object A is lower than that of others. The average of trust valuation data of B,C,D and E are the same. This situation brings difficulty to the subjective trust decision, but only by generating the numerical eigenvalue of subjective trust cloud, we can overcome this drawback intuitively, simply and efficiently.

We see from the numerical eigenvalue of subjective trust cloud of these 5 objects listed in Table 1, the Ex

Table 2: Objects' trust valuation and trust cloud eigenvalue

Trust objects	★	★★	★★★	★★★★	★★★★★	Average trust value	Ex	En	He
A	74	77	88	155	590	4.1	4.427	0.453	1.146
B	45	29	46	123	732	4.5	4.797	0.178	0.816
C	34	30	45	154	703	4.5	4.815	0.089	0.588
D	21	45	65	103	685	4.5	4.808	0.099	0.618
E	18	32	61	187	664	4.5	4.809	0.098	0.619

The number of star express the level of subjective trust valuation. One-star means the lowest level and five-star means the highest level value of the objects can coincide with the average trust value well, i.e., the Ex value of objects with relatively low, the average trust value is relatively low and vice versa. The Ex value of object A is obviously lower than that of others, so the satisfiability of A can be considered lower than that of others. The Ex values of B, C, D and E are very close, so it's almost impossible to further determine the object's trust value only by Ex value. However, both En and He value of object C are lower than those of object B, D and E. So, the stability of satisfiability of C can be considered higher than that of B, D and E.

CONCLUSION

Subjective trust valuation-based trust relationship is of great uncertainty, so the key to subjective trust valuation and management research is how to evaluate and obtain trust information. In this study we introduce cloud model and refer to social trust network properties, then propose the trust cloud-based subjective trust management model. By using the numerical features such as expectation, entropy and hyper entropy, we judge the subjective trust information with randomness and fuzziness; then we divide trust into direct trust and recommendation trust and characterize the effect and the degree of effect of time on subjective trust through time window and attenuation function. Cloud model overcome the drawback that Fuzzy Math strictly expresses the concept of fuzziness through accurate and unique membership function and comparatively efficiently solve the tough problem of the fuzziness and uncertainty of trust expression.

ACKNOWLEDGMENT

This study is supported by the National High Technology Research and Development Program of China (863 Program), No. 2006AA01Z438.

REFERENCES

Beth T., M. Borcherding and B. Klein, 1994. Valuation of trust in open networks. Proceedings of the 3rd European Symposium on Research in Security, (ESORICS'94), Springer-Verlag, Brighton, pp: 3-18.

Blaze, M., J. Feigenbaum and M. Strauss, 1998. Compliance checking in the policy maker trust management system. Proc. Int. Conf. Financ. Cryptography, 1465: 254-274.

Blaze, M., J. Feigenbaum and A.D. Keromytis, 1999. KeyNote: Trust management for public key infrastructures. Proceedings of the 6th Security Protocols International Workshop, (SPI'99), Springer, London, pp: 59-63.

Chen, H.W. and Z.W. Ye, 2008. Research of P2P trust based on fuzzy decision-making. Proceedings of the 12th International Conference on Computer Supported Cooperative Work in Design, April 16-18, Xi'an, China, pp: 793-796.

Deyi, L., M. Haijun and S. Xuemei, 1995. Membership cloud and membership cloud generators. Comput. Res. Dev., 32: 16-21.

Huang, H. and R. Wang, 2008. Subjective trust assessment model based on membership cloud theory. J. Commun., 29: 13-19.

Josang, A. and S.J. Knapskog, 1998. A Metric for Trusted Systems. Global IT Security. Austrian Computer Society, Wien, pp: 541-549.

Josang, A., 1999. Trust-based decision making for electronic transactions. Proceedings of the 4th Nordic Workshop on Secure Computer Systems, Nov. 1-2, Stockholm University, Sweden, pp: 5-20.

Junmao, Z., Y. Shoubao and F. Jianping, 2005. A grid and P2P trust model based on recommendation evidence reasoning. J. Comput. Res. Dev., 42: 797-803.

Li, D.Y. and C.Y. Liu, 2004. Study on the universality of the normal cloud model. Eng. Sci., 6: 28-34.

Liu, C., M. Feng, X. Dai and D. Li, 2004. A new algorithm of backwark cloud. J. Syst. Simulat., 16: 2417-2421.

Lu, F. and H. Wu, 2008. Research of trust valuation based on cloud model. Eng. Sci., 10: 84-90.

Lu, F. and H. Wu, 2009. Research of trust valuation and decision-making based on cloud model in grid environment. J. Syst. Simulat., 21: 421-426.

Song, S., K. Hwang, R. Zhou and Y.K. Kwok, 2005. Trusted P2P transactions with fuzzy reputation aggregation. IEEE Internet Comput., 9: 24-34.

Tian, C.Q., S.H. Zou, W.D. Wang and S.D. Cheng, 2008. A new trust model based on recommendation evidence for P2P networks. Chinese J. Comput., 31: 270-281.

Wang, C. and B. Li, 2003. Peer-to-peer overlay networks: A survey. Technical Report, Department of Computer Science, Hong Kong University of Science and Technology.

Wang, S., L. Zhang, S. Wang, N. Ma and S. Wang, 2008. Evaluation approach of subjective trust based on cloud model. Int. Conf. Comput. Sci. Software Eng., 3: 1062-1068.

Wang, Y. and J. Vassileva, 2003. Trust and reputation model in peer-to-peer networks. Proceedings of the 3rd International Conference on Peer-to-Peer Computing, Sept. 1-3, IEEE Computer Society, Washington, DC., pp: 150-159.

Yu, B. and M.P. Singh, 2002. An evidential model of distributed reputation management. Proceedings of the 1st International Joint Conference on Autonomous Agents and Multiagent Systems, July 15-19, ACM, New York, pp: 294-301.

Zhang, S.Q. and Y.T. Yang, 2005. A fuzzy set-based trust and reputation model for P2P networks. J. Harbin Eng. Univ., 26: 764-766.

Zhang, Y. and D. Zhao and D. Li, 2004. The similar cloud and the measurement method. Inform. Control, 33: 129-132.