A Reliable Fuzzy Theory based Reputation System in Grid

Liao Hongmei
School of Computer Science and Technology China University of Mining and Technology, Xuzhou, China
Email: lhm@cumt.edu.cn
Wang Qianping and Li Guoxin
School of Information and Electric Engineering, China University of Mining and Technology, Xuzhou, China
Email:qpwang@cumt.edu.cn

***Abstract*—Trust is a fundamental concern in Grid environment. Behavior trust that varies with time is indispensable in the trust system. Because of the fuzzy nature of behavior trust, it is more appropriate to adopt fuzzy logic to express and compute trusts and reputations than adopt probabilities approach. A new reliable fuzzy theory based reputation system in Grid environment is proposed. By variable weighted fuzzy comprehensive evaluation, Direct Trust can be gotten and the affection of the ill factor have low value can be highlighted by give it a larger weight and then Grid entities can avoid choosing service providers with some defective. By derivation and combination of trust, Reputation can be obtained. Expert's experience is used to set and simplify fuzzy rules. A distributed hash table based Dual Two-Layer Chord Protocol is proposed to store and retrieve reputations. Simulation results show that entities in Grid can use resources or deploy services more securely in the support of the reliable fuzzy theory based reputation system.**

***Index Terms*—trust model, Grid, fuzzy comprehensive evaluation, reputation system, distributed hash table**

I. Introduction

Security has been the focus of grid systems recently. Trust model plays an important role in security field. It is often classified into two categories: identity trust and behavior trust. Identity trust is static. Once the identity is authenticated, the behaviors of the entities will not be monitored any more even though they might do something harmful, whereas behavior trust is dynamic trustworthiness. Behavior trust is based on transactions between entities in the past time. If the entity do something wrong or harmful, its behavior trust value will then be dropped down, other entities may decide to give up choosing it as a service provider based on its behavior trust value.

Many trust models based on entity behaviors have been proposed. In the trust model proposed by Alfarez Abdul-Rahman and Stephen Hailers, trust is divided into Direct Trust and Recommend Trust [1]. Audun Jφsang, Andrew Whitby [2] [3] proposed a beta reputation system, which is based on beta probability density functions with which feedback and derive reputation ratings are combined. Lik Mui, Mojdeh Mohtashemi [4] proposed a rating system based on a Bayesian probabilistic framework which also used the beta distribution. But trust is a subjective and inaccurate value which is decided by the Grid entity, it is difficult to describe with accurate probability distribution. It is also difficult to ensure the independency of events in beta reputation system and Bayesian probabilistic framework.

Few behavior trust models based on fuzzy logic in Grid are proposed [5] [6] [7]. But the fixed weighted fuzzy comprehensive evaluation in [5] is not suited; Shanshan Song and Kai Hwang suggest enhancing the trust index of a resource site by upgrading its intrusion defense capabilities and checking the success rate of jobs running on the platforms, but the computing of directed trust is not mentioned in [7].

In this paper, a new reliable fuzzy theory based reputation system in Grid is proposed. Direct Trust is gotten by variable weighted fuzzy comprehensive evaluation and expert experience is used to set and simplify fuzzy rules while used in computing of reputation. By variable weight based fuzzy comprehensive evaluation, the affection of the ill factor have low value can be highlighted by give it a larger weight and Grid entities can avoid choosing service providers with some defective.

A reputation system gathers, distributes, and aggregates feedback about participant's behaviors and it can help people make decisions about who to trust. Most literatures stored reputation information in the node itself or in some central nodes. However, storing in the node itself is not secure enough and Storing in central nodes is easy to cause bottleneck. To address this problem, we proposed a Distributed Hash Table(DHT) based Dual Two-Layer Chord Protocol (DTLCP) as reputation storage and retrieval infrastructures with which the reputation system can provide efficient storage and queries that operate in O(logN) +O(M)overlay hop(N is the number of domains in Grid and N the number of nodes in a domain, M<<N) and can answer queries even if the system is continuously changing. Initialization of reputation and updating of reputation are all discussed in this paper.

Corresponding author: Liao Hongmei .

doi:10.4304/jcp.5.5.782-790

II. TRUST AND REPUTATION

In this paper, we will adopt the definition of trust in papers [8] [9].

Trust is usually divided into direct and indirect trust. If an entity *P* did not transact with entity *Q* in the past, it has no direct trust value about *Q*. An entity without direct trust or having no enough confidence on its direct trust on another entity should use indirect trust. Recommend trust and reputation are both indirect trust.

A Definition of direct trust and reputation

The definition of direct trust and reputation are as follows:

Trust is the firm belief in the competence of an entity to act as expected such that this firm belief is not a fixed value associated with the entity but rather it is subject to the entity's behavior and applies only within a specific context at a given time.

The direct trust level on an entity is built on past experiences and is given for a specific context and a given time frame. For example, entity *P* might trust entity *Q* to use its storage resources but not to execute programs using these resources. The trust level is specified for a given time frame because the trust level today between two entities is not necessarily the same trust level a year ago.

The definition of reputation: The reputation of an entity is an expectation of its behavior based on other entities' observations or the collective information about the entity's past behavior within a specific context at a given time.

Seeking the reputation of a specific entity relies on information from a set of other entities referred to as recommenders set. A recommender is an entity that gives recommendation using its direct trust table that includes trust values for entities with which the recommender had prior direct transactions.

Usually a node *P* need to integrate direct trust stored itself and indirect trust such as reputation to determine whether or not trust entity *Q* and transact with it. The final trust value is computed as follows:

$\alpha *$directly trust $\oplus$ $\beta *$ indirect trust(reputation)

α and β respectively expressed the weights of these two trust relationship in trust system. When the interactions between entities *P* and *Q* frequently, directly trust should get a larger weight. Set $\alpha > \beta$, that is, trustworthiness of node *Q* is based more on direct relationship with ***Q*,** rather than the reputation of ***Q*.** While when the entities *P* and *Q* have little or no contact with each other a long time, set $\alpha < \beta$.

B. Trust Relationships Within domain and Trust Relationships between domains

A Grid computing system is a geographically distributed environment with autonomous domains that share resources amongst themselves. One primary goal of such a Grid environment is to encourage domain-to-domain interactions and increase the confidence of domains to use or share resources: (a) without losing control over their own resources; and (b) ensuring confidentiality for others. To achieve this, the trust relationship can be divided into in-domains trust and cross-domain trust. Cross-domain trustworthiness makes such geographically distributed systems become more attractive and reliable for day-to-day use. Monitoring and managing the behavior of the entity and building a trust level based on that behavior is needed.

In-Domain trust relationship is the trust relationship between nodes in the same Grid domain, usually decided by both domain strategy and behavior trust. It is more stable and easy to confirmed; strategies such as identity trust can be used simultaneously. In-domain trust relationship is often centralized management, our paper focuses on the more complex and common cross-domain trust relationships. Notation trust and reputation represent the cross-domain trust and cross-domain reputation seperately in the rest of this paper.

Cross-domain trust is defined as trust relationship of Grid nodes in different Grid domains in this paper. Some authors get the final trust value of node *P* on *Q* in different domains by combining the weight of node *Q* in domain D_Q that *Q* is exist and domain trust of D_Q. Domain trust is determined by transaction history of all nodes in this domain.

However, the weight of node within domain can not reflect its performance outside. And if there is a malicious node in domain, according to the penalty strategy, the domain trust will be greatly reduced, so that nodes with high credibility in this domain will lose many trading opportunities.

In this paper, if entity *P* and entity *Q* are cross-domain nodes, the final trust value of *P* on *Q* will depend on their mutual direct trust and reputation of node *Q* also.

III. RELIABLE FUZZY COMPREHENSIVE EVALUATION OF TRUST

Because trust is determined by multiple factors such as an entity's capabilities, honesty and reliability, and so on, we will first give a reliable comprehensive evaluation of direct trust.

With fuzzy theory, trust can partially belong to a set and this is represented by the set membership.

Let $X = \{x_0, x_1, \cdots\cdots, x_n\}$ be the problem domain that trust manage will be researched in. x_i ($i=1, 2,..., n$) denote the entity in the Grid. The definition of fuzzy set is:

A fuzzy set is any set that allows its members to have different grades of membership (membership function) in the interval [0, 1].

Definition: Let *X* be the domain, and let *x* be the element of the set *X*, $\forall x \in X$ there is the mapping:

$$X \to [0,1],\ x \mapsto \mu_A(x) \in [0,1]$$

The fuzzy set *A* in *X* is expressed as a set of ordered pair $A = \{(x \mid \mu_A(x))\},\ \forall x \in X$.

$\mu_A(x)$ is the membership function of fuzzy set *A*, which describes the membership of the element *x* of the base set *X* in the fuzzy set *A*. The grade of membership $\mu_A(x_0)$ of a membership function $\mu_A(x)$ describes for the special element $x=x_0$, to which grade it belongs to the fuzzy set A. This value is in the unit interval [0, 1].

In Grid, the grade of trust can be described by membership degree of different fuzzy sets in X which denote different trust levels. M different fuzzy sets T_i $(i=1, 2,..., M)$, which are in the set of all fuzzy sets in X can be used to denote M different trust levels. For example, when $M=6$, six fuzzy sets T_i $(i=1, 2,...,6)$ can be used to denote six different trust levels in Grid. The trust level of T_i $(i=1,2,...,6)$ is defined as follows:

T_1 denotes the "entire trust" fuzzy set;
T_2 denotes the "very trust" fuzzy set;
T_3 denotes the "trust" fuzzy set;
T_4denotes the "distrust" fuzzy set;
T_5 denotes the "very distrust" fuzzy set;
T_6 denotes the "entire distrust" fuzzy set.

The membership function of x to fuzzy set T_j can be denoted as $T_j(x)$. To a concrete x_i, the membership degree is $T_j(x_i)$, which can be marked as T_{ij}. Trust vector of x_i is :

$V=\{v_0,v_1,...,v_6\}$,v_j $(j=1,2,...,6)$, v_j denotes the membership degree of x_i to T_j. But x_i can simultaneously belong to another fuzzy set T_k, such that $T_k(x_i)$ characterizes the grade of membership of x_i to T_k.

A. Ordered Weighted Averaging Operations

The discussion above does not take the context of trust and different factors into account in trust computing. In real Grid environment, Trust and Reputation both depend on some context. For example, entity P trusts entity Q as multimedia provider, but it does not trust Q as a storage provider. So in the context of requesting a multimedia service, Q is trustworthy. But in the context of providing storage service, Q is untrustworthy.

Even in the same context, the trust is not determined by only one factor. It is often evaluated from several aspects (factors). For each aspect, it develops a kind of trust. The overall trust depends on the combination of the trusts in each aspect. Every factor play role in deciding whether the entity is trustworthy to interact with in this context.

For example, as for the total trust evaluation in some context, there are four important factors (attributes). Suppose the following is the evaluation factors (attributes) aggregation:

$$E=\{ E_1,E_2,E_3,E_4\}$$

E_1,E_2,E_3,E_4 represent service time, contract abidance, stipulate violating and job success rate separately. There may be several subgroup factors in each factor. In this paper, for simplification, we will not discuss the subgroup factors.

Suppose the Trust fuzzy evaluation aggregation is:

$$T=(T_1,T_2,T_3,T_4,T_5,T_6)$$

The relationship R denotes the mapping of E to T. That is, the element r_{ij} in R is the membership degree of e_i to T_j.

Matrix $R=(r_{ij})_{4\times 6}$ is the fuzzy comprehensive judgment Matrix of entity trust in some context.

The final trust value will be combined closely with the value assignment of each evaluation factor in E. The nature of weight is shown in the quantity of different factors on objects at different levels, i.e. the different influence from all aspects on the Trust. Let $w=(w_1,w_2,...,w_n)$ be a "weighting vector" such that w_i is in [0, 1] for all i and $\sum_{1}^{n} w_i = 1$.

Suppose w_i is the weight of the factor e_i. So, the trust vector $V=\{v_1,v_2,v_3,v_4,v_5,v_6\}$can be gotten by the following fuzzy mapping:

$$\{v_1,v_2,v_3,v_4,v_5,v_6\}=(w_1,w_2, w_3,w_4) \circ (r_{ij})_{4\times 6} \text{ And}$$

$$v_i=w_1*r_{1j}+ w_2*r_{2j}+ w_3*r_{3j}+ w_4*r_{4j} \quad (j=1,2,\ldots,6)$$

This aggregation operation is often called "ordered weighted averaging operations".

B. Varialble Weight based Fuzzy Comprehensive Evaluation of Trust

In ordered weighted averaging operations, weighting vector $w=(w_1,w_2,...,w_n)$ is fixed. That is, once the weight of each factor is set, it will not be changed whatever the actual situation is.

But if the value of some attribute of an entity such as contract abidance is too small, even if the other attributes are all good, the entity is not trusty. In ordered weighted averaging operations, the high value of the other attributes will counteract the low value of the bad attribute contract abidance. If we increase the weight of contract abidance, when the entity abide contract well, other attributes can not be manifested.

By increasing the weight of the attribute when its value is low, we can give prominence to deficiency. That is variable weight based fuzzy comprehensive evaluation of trust which can be described as follows:

1) Suppose the value of evaluation factors (attributes) $E=\{E_1,E_2,E_3,E_4\}$ is denoted as $u_1,u_2,...,u_n$. $u_i \in [0, u_m]$, $i=1,2,...,n$. u_i is the trust value of factor Ei .When attribute E_i is in the best situation , $u_i = u_m$. When attribute E_i is in the worst situation , $u_i = 0$.

2) The weight of factor E_i is denoted as w_i, it is function of $(u_1,u_2,u_3,...,u_n)$. That is, $w_i=w_i(u_1,u_2,...,u_n)$, $(i=1,2,...,n)$. The weight of factor Ei , depends on the separate values of all factors. $w_i \in [0,1]$ and $\sum_{1}^{n} w_i = 1$.

Especially, $w_{mi}=w_i(u_m, u_m, ..., u_m)$, $i=1,2,...,n$ and $w_{mi} \in (0,1)$, $\sum_{i=1}^{m} w_{mi} = 1$. w_{mi} is called base weight , and it can be gotten by hierarchical analytic approach.

$w_{0i}=w_i(u_m ,..., u_m , 0 , u_m ,..., u_m)$, $i=1, 2, ... , n$, $w_{0i} \in (0,1)$. w_{0i} denotes the weight of factor E_i when E_i has its min value and the other factors have their max values. w_{0i} can be set by the specialist as the max value of weight of factor E_i. So the influence of factor E_i can be amplified.

3) In order to find appropriate variable weight $w(u_1,...,u_i,...,u_n)$, $i=1,2,...,n$, which is nonincreasing function of u_i and $\sum_{i=1}^{n} w_i u_i$ which is nondecreasing function of u_i, we introduce function $\lambda_i(u)(i=1,2,...,n)$, which matches the following criteria：

- $\lambda_i(u)$is defined in $[0,u_m]$，it is not negative and bounded；

- u_i is a nonincreasing differentiable function in $[0,u_m]$; $\lambda_i'(u) \le 0, (u \in [0, u_m])$;
- let $\lambda_i(0)= \lambda_{0i}$, $\lambda_i(u_m)= \lambda_{mi}$. λ_{0i} denotes the maximum of $\lambda_i(u)$ and λ_{mi} denotes the minimum value of $\lambda_i(u)$.

To a given set of single-factor assessment of $(u_1,...,u_i,...,u_n)$, a function $\lambda_i(u_i)(i=1,2,...,n)$ can be obtained by the means in literature[10], let

$$w_i(u_1,u_2...,u_n) = \frac{\lambda_i(u_i)}{\sum_{j=1}^{n}\lambda_j(u_j)} \quad (i=1,2,..,n) \tag{1}$$

It have been proved that $w_i(u_1,u_2,...,u_n),i=1,2,...,n,$ in (1) can be the variable weight [10].

C. Application of Variable Weight based Fuzzy Comprehensive Evaluation in Trust Model

Suppose in the trust model node *P* needs to give a comprehensive evaluation of another node *Q* which have had trade with it in the context of storage services.

The trust value in storage services of node *Q* is determined by four factors (attributes) ,that is ,the set of evaluation factors is {compliance with the contract, the completion time of service, quality of service, whether or not a malicious act}, their basis weights have been known, which are (0.3,0.2,0.3,0.2), the max weights of these four factors $(w_{01},w_{02},w_{03},w_{04})$ are determined by some experts, which are (0.7,0.5,0.6,0.7).Let

$$\lambda_{mi}=w_{mi}(i=1,2,...,n) \tag{2}$$

$(\lambda_{m1}, \lambda_{m2}, \lambda_{m3}, \lambda_{m4})$= (0.3, 0.2, 0.3, 0.2). By definition of w_{0i} and w_{mi}, as well as (1)and (2) ,we can get formula (3):

$$w_{0i} = \frac{\lambda_{0i}}{\lambda_{0i} + \sum_{j \ne i} w_{mj}}, i = 1,2,... n \tag{3}$$

$$\lambda_{0i} = \frac{w_{0i}\sum_{j \ne i} w_{mj}}{1 - w_{0i}}, i = 1,2,..., n \tag{4}$$

By calculation, we can obtain that $(\lambda_{01}, \lambda_{02}, \lambda_{03}, \lambda_{04})$ = (1.63, 0.8, 1.05, 1.87). .

For given $u_1,u_2,...,u_n$, Fixed i ,let u_i changed to be u, and $u>=u_i$ .Denote

$$\lambda_0 = \sum_{j \ne i}\lambda_j(u_j), v_0 = \frac{1}{\lambda_0}\sum_{j \ne i}\lambda_j(u_j)u_j \tag{5}$$

$$w_i(u) = w_i(u_1,..., u_{i-1}, u, u_{i+1},..., u_n) \tag{6}$$

It can be testified that:

1) $w(u_1,...,u_i,...,u_n)$ is a nonincreasing function of u_i unconditionally;
2) Suppose $w_i(u_1,u_2,...,u_n)$ have been obtained by (1) ,the necessary and sufficient conditions of that $\sum_{j=1}^{n} w_j u_j$ is a nondecreasing function of u_i are:

$$\lambda'_i(u) \ge -\frac{1}{\lambda_0(u - v_0)}\lambda_i(u)(\lambda_0 + \lambda_i(u)) \tag{7}$$

There are usually three solution to compute the λ_i which meets (7) [10], In this paper ,we choose the following formula [10].

To a fixed i, there is:

$$\lambda_{*i} = \sum_{j \ne i} w_{mj} \le \lambda_0 \le \sum_{j \ne i}\lambda_{0j} = \lambda^*_{\bullet i} \tag{8}$$

By expression (8), the values of $\lambda_{*i}, \lambda^*_{\bullet i}$ ($i=1,2,...,n$)can be calculated for each identified i.

By expression (7), fix i, let

$$\begin{cases} \dfrac{d\lambda_i(u)}{du} = -\dfrac{u_m^{k_i-1}}{\lambda^*_{\bullet i}u^{k_i}}\lambda_i(u)(\lambda^*_{\bullet i} + \lambda_i(u)) \\ \lambda_i(0) = \lambda_{0i}, \lambda_i(u_m) = w_{mi} \end{cases} \tag{9}$$

It can be proved that $\lambda_i(u)$ derived from (9) and $w_i(u_1,u_2,...,u_n)$ determined by (1) need to meet that $\sum_{j=1}^{n} w_j u_j$ is a nondecreasing function of u_i [10]. The solution of (9) can be gotten as follows:

$$\lambda_i(u) = \frac{\lambda^*_{\bullet i}\lambda_{0i}}{\lambda^* \exp(\frac{1}{1-k_i}(\frac{u}{u_m})^{1-k_i})}, i = 1,2,..., n \tag{10}$$

In (10),

$$\lambda^* = \sum_{i=1}^{n}\lambda_{0i} = 5.35$$, and

$$k_i = 1 - \frac{1}{\ln\frac{\lambda_{0i}(\lambda^*_{\bullet i} + w_{mi})}{\lambda^* w_{mi}}}$$.

Solution $w_i(u_1,u_2,...,u_n)$ $(i=1,2,...,n)$ can derived from (1)an (10).

According to the formulas (3) , (8) and (10), λ_{0i}, λ_{*i} , $\lambda^*_{\bullet i}$ and k_i , for specific i ,can be calculated as shown in Tab. Ⅰ.

TABLE I.
VARIABLES IN VARIALBLE WEIGHT BASED FUZZY COMPREHENSIVE EVALUATION OF TRUST

	E_1	E_2	E_3	E_4
w_{mi}	0.3	0.2	0.3	0.2
λ_{0i}	1.63	0.8	1.05	1.87
$\lambda^*_{\bullet i}$	3.72	4.55	4.3	3.48
λ_{*i}	0.7	0.8	0.7	0.8
k_i	0.289	0.211	0.09233	0.4627

Suppose there are two sets of trust evaluation of factors$\{E_1,E_2,E_3,E_4\}$ whose define area is [0, 10] . The values of these two sets of trust evaluation are respectively [6,8,7,9] and [7,9,8,4].

To get the fuzzy comprehensive trust evaluations of these two groups, we should first change the trust evaluation on [0,10] into membership degrees in six fuzzy sets. The collection of trust evaluation reviews is described in section Ⅱ. Relation *R* represents the map from *E* to *T*. Element r_{ij} in *R* represents the membership degree of e_i to fuzzy set T_j.

$R=(r_{ij})_{4*6}$ denotes the fuzzy comprehensive evaluation matrix in some context. If these six fuzzy sets T_1,T_2,T_3,T_4,T_5,T_6 all adopt trapezoidal membership functions, and parameters [a, b, c, d] are set separately as [-1.8, -0.2, 0.2, 1.8], [0.2, 1.8, 2.2, 3.8], [2.2,3.8, 4.2, 5.8], [4.2, 5.8, 6.2, 7.8], [6.2, 7.8, 8.2, 9.8], [8.2, 9.8, 10.2, 11.8], then the first set of trust evaluation [6,8,7,9] can be fuzzyfied and changed into a fuzzy comprehensive evaluation matrix as shown in Fig. 1:

$$\begin{array}{c|cccccc} & T_1 & T_2 & T_3 & T_4 & T_5 & T_6 \\ E_1 & r_{11} & r_{12} & r_{13} & r_{14} & r_{15} & r_{16} \\ E_2 & r_{21} & r_{22} & r_{23} & r_{24} & r_{25} & r_{26} \\ E_3 & r_{31} & r_{32} & r_{33} & r_{34} & r_{35} & r_{36} \\ E_4 & r_{41} & r_{42} & r_{43} & r_{44} & r_{45} & r_{46} \end{array} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0.5 & 0.5 & 0 \\ 0 & 0 & 0 & 0 & 0.5 & 0.5 \end{bmatrix}$$

Figure 1. Fuzzy Comprehensive Evaluation Matrix of Trust with Evaluation Vector is [6, 8, 7, 9].

The second set of trust evaluation [7, 9, 8, 4] is changed into a fuzzy comprehensive evaluation matrix as shown in Fig. 2:

$$\begin{array}{c|cccccc} & T_1 & T_2 & T_3 & T_4 & T_5 & T_6 \\ E_1 & r_{11} & r_{12} & r_{13} & r_{14} & r_{15} & r_{16} \\ E_2 & r_{21} & r_{22} & r_{23} & r_{24} & r_{25} & r_{26} \\ E_3 & r_{31} & r_{32} & r_{33} & r_{34} & r_{35} & r_{36} \\ E_4 & r_{41} & r_{42} & r_{43} & r_{44} & r_{45} & r_{46} \end{array} = \begin{bmatrix} 0 & 0 & 0 & 0.5 & 0.5 & 0 \\ 0 & 0 & 0 & 0 & 0.5 & 0.5 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

Figure 2. Fuzzy Comprehensive Evaluation Matrix of Trust with Evaluation Vector is [7,9,8,4].

Adopt fix weighted fuzzy comprehensive evaluation; let $w=(w_1,w_2,...,w_n)$ represents the fixed weight vector of factor vector $(E1,E2,E3,E4)$.$w_i \in [0, 1]$ stands for the weight of factor e_i, $\sum_1^n w_i = 1$. By the following fuzzy mapping:

$\{v_1,v_2,v_3,v_4,v_5,v_6\}=(w_1,w_2, w_3,w_4) \circ (r_{ij})_{4\times 6}$ And $v_i=w_1*r_{1j}+ w_2*r_{2j}+ w_3*r_{3j}+ w_4*r_{4j}$ (j=1,2,…,6), comprehensive trust vector $V=\{v_1,v_2,v_3,v_4,v_5,v_6\}$ can be gotten.

The comprehensive value of the two sets of trust evaluation can be separately computed:

V_1= [0 0 0 0.45 0.45 0.1];

V_2= [0 0 0.2 0.15 0.55 0.1].

Defuzzification is the reverse process of fuzzification. Trust and Reputation we have gotten above is a "fuzzy" result, that is, the result is described in terms of membership in fuzzy sets. Defuzzification would transform this result into a single number indicating the trust level of an entity. This may be necessary if we wish to output a real number to the user. An average of maxima method or a centroid method can be used to do this work.

It is usually assumed that an entity P will only engage in a transaction with entity Q if the level of trust exceeds some personal threshold (the level of acceptable trustworthiness), which depends on the transaction context.

Defuzzification is the reverse process of fuzzification. Trust and Reputation we have gotten above is a "fuzzy" result, that is, the result is described in terms of membership in fuzzy sets. Defuzzification would transform this result into a single number indicating the trust level of an entity. This may be necessary if we wish to output a real number to the user. An average of maxima method or a centroid method can be used to do this work.

With centroid-based defuzzification, we can get the outcomes V_1=7.2424 ; V_2=7.0424.

It can be seen that the value of factors E_4 is outstandingly low, that means the entity is defective in factors E_4. To get the decider's adequate attention, we should increase its weight to highlight the disadvantages. Variable weight based fuzzy comprehensive evaluation is applied in trust model.

According to variable weight based fuzzy comprehensive evaluation algorithm, we can get the weights of factors and comprehensive trust values on these two sets of evaluations [6, 8, 7, 9] and [7, 9, 8, 4].

Parameters of the first set of evaluations , $\{\lambda_1(u),\lambda_2(u),\lambda_3(u),\lambda_4(u)\}$, can be computed with formula （10）:

$\{\lambda_1(u),\lambda_2(u),\lambda_3(u),\lambda_4(u)\}$= {0.4262, 0.2351, 0.3803, 0.2095}.

Parameters of the second set of evaluations are:

$\{\lambda_1(u),\lambda_2(u),\lambda_3(u),\lambda_4(u)\}$= {0.3805, 0.2119, 0.3432, 0.3900}

Variable weights of every factor on evaluations [6, 8, 7, 9] and [7, 9, 8, 4] are as Tab. Ⅱ:

TABLE II.
VALUES OF VARIABLE WEIGHTS WHEN EVALUATIONS ARE GIVEN

Evaluation	Weight	E_1	E_2	E_3	E_4
[6,8,7,9]	w_i	0.3407	0.1879	0.3040	0.1675
[7,9,8,4]	w_i	0.2870	0.1599	0.2589	0.2942

With variable weight based fuzzy comprehensive evaluation algorithm, the comprehensive trust vectors of valuations[6,8,7,9] and [7,9,8,4] can be gotten:

V_1=[0 0 0 0.4927 0.4236 0.0838];

V_2=[0 0 0.2942 0.1435 0.4824 0.0799];

Defuzzify these two trust vectors by centroid method, we can get the following results:

V_1=7.1347,V_2=6.6500.

Compare this results computed by variable weight based fuzzy comprehensive evaluation and the results computed by fixed weighted fuzzy comprehensive evaluation, we can find that former is always smaller than the latter except that every single factor in the assessment factors have taken the maximum.

The affection of the ill factor have low value can be highlighted by give it a larger weight in variable weight based fuzzy comprehensive evaluation. The comprehensive trust value will then be decreased even if its other factors have high evaluations. By variable weight based fuzzy comprehensive evaluation, the Grid entities can avoid choosing service providers with some defective.

IV. RELIABLE AND LOAD BALANCING REPUTATION SYSTEM

If entity P has direct interacting with entity Q in the past time, it has its own direct trust value on Q. Reputation is an entity's belief in another entity's capabilities, honesty and reliability based on recommendations received from other entities within a specific context at a given time[11] [12]. Reputation is global. Any node in Grid can request and get the same value of another node's reputations. The reputations are distributed stored in the Grid, and can be gotten repeatedly. Reputation system can avoid repeating computing in recommand trust system and can reduce network traffic.

A. Representation of Reputation

Reputation of an entity is an expectation of its behavior based on other entities' observations or the collective information about the entity's past behavior within a specific context at a given time.

The latest updating time and the times of trades of the node will affect the reliability and validity of reputation information. Let n denotes the times of trades of node Q ; V denotes the synthetic reputation vector. Reputation of node Q in context c at time t can be described as follows:

$$Q\text{'s } Reputation_c \quad value\ V \quad Time\ t \quad count\ n \cdot$$

B. Initialization of Reputation

Because in dynamic grid, nodes and domains can join at any time, proper initialization of reputation is needed.

Identity authentication system can help determine the initial reputation values. In cross-domain trust system, to make new nodes have opportunities to participate in the transactions with nodes in different domains, we set the initial reputation of a new node as T_3 (denotes the "trust" fuzzy set), set the times of trades as 0. Trust level $T3$ will give the node opportunities to participate in the transactions, and can avoid high risk from unfamiliar new nodes. The Parameter n which denotes the times of trades of node Q will give the information that the reliability of the reputation values of Q.

C. Reliable and load balancing storing and accessing mechanisms of reputation system

In Most literatures, reputations were stored in the node itself or in the domain central node. However, storing in the node itself is not secure enough and Storing in domain central nodes is easy to cause bottleneck.

In this paper, we proposed a Dual Two-Layer Chord Protocol (DTLCP) as reputation storage and retrieval infrastructures. Chord is a distributed lookup protocol proposed by Ion Stoica, etc[14][15]. It is a protocol based on Distributed Hash Tables. By using consistent hash function, a node's identifier is chosen by hashing the node's IP address, while a reputation identifier key is produced by hashing the reputation information. And we use globally participating function that maps reputation keys to node identifiers to insert the information into the network. Reputation key k is assigned to the first node whose identifier is equal to or follows (the identifier of) k in the identifier space. A Chord node needs only a small amount of "routing" information about other nodes. Because this information is distributed, a node resolves the hash function by communicating with other nodes. Each node uses finger tables[15] to maintain information about other nodes as guide to forward reputation queries.

Chord treated all nodes as the same. If there are more nodes leave or join the Grid, the cost of updating figure tables will increased. However, Participating nodes in Grid are not equivalent. Some super peers, such as domain central nodes or some LAN gateways are more powerful and stable than the other ordinary nodes. The routing information updating cost of network composed of super peers will be much smaller than the entire Grid. And Chord is not reliable for its storing reputation information only in one location.

In the Dual two-layer Chord Protocol, we divided the Grid into two layers. The first layer is composed of super peers and the second layer is composed of nodes in one Grid domain.

1) In the first layer, each super node has finger entries at power of two intervals around the identifier circle, each super node can forward a query at least halfway along the remaining distance between the node and the target identifier. Because a node's finger table generally does not contain enough information to directly determine the successor of an arbitrary key k, a successor list is stored in each super node. Fig. 3 shows the Chord ring of the first layer and Finger Table and Successor List of super node *S8*.

By hashing the reputation R, reputation key of R is obtained; and with chord protocol in[18],we can find the first location *S1* of this reputation. Combine this reputation key and identifier of *S1* as identifier *R2*. By hashing *R2*, with the same method, we can find the second location of Reputation *S2*.

2) As the number of nodes in one domain M is much smaller than the number N in the first layer, in the domains managed by *S1 and S2*, each node has only a successor list, as shown in Fig. 4. Apply consistent hash function in the second layer and find a node to store the reputation information separately; Fig. 4 shows the path taken by a query from node *N6* for reputation key 25 in the second layer of Grid.

3) When node P has a transaction with node Q, it will require the reputation of Q first. In the support of DTLCP, two nodes with Q's reputations will return reputations of Q. If the two values are equal, the reputations are thought trustable. When the transaction is end, update the values in these two locations.

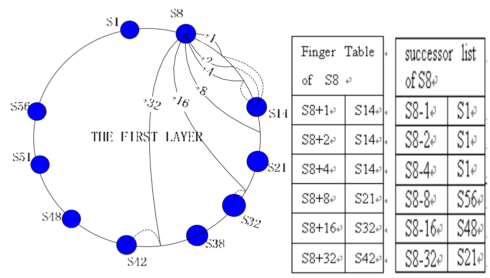


Figure 3. Chord ring of the first layer and Finger Table and successor list of super node S8.

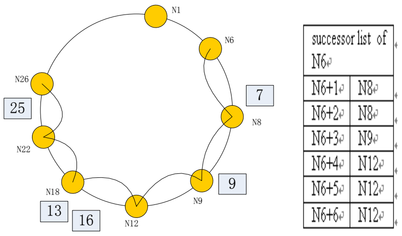


Figure 4. The path taken by a query from node *N6* for reputation key 25 in the second layer of Grid

In an N-Domain Grid network, each super node maintains information about only *O(logN)* other super nodes, and a lookup requires *O(logN)* messages. In the support of DTLCP, the reputation system can provide efficient storage and queries that operate in *O(logN) +O(M)*overlay hop. *M* is much smaller than *N* in Grid. Chord-based DTLCP can adapt efficiently as nodes join and leave the system, and can answer queries even if the system is continuously changing.

D. *Updating of Reputation*

Regular updating will cause local network congestion. In this paper, we update the reputation by encryption channel immediately after transaction. The Old reputation values have decayed with time. However, the immediate new direct trust value need no time decay. The updating of reputation is described as follows:

$$Q\text{'s Reputation}_{c_1}\ \ value\, V_1\ \ Time\ \mathrm{t}_1\ \ count\ \mathrm{n}$$

$$\wedge\, P\ \ rectrusts_{c_2}\ Q\ value\ \ V_2\ \ Time\ \mathrm{t}_2$$

$$\wedge\, c_1 \approx c_2$$

$$\Rightarrow Q\text{'s}\ \ \mathrm{Re}\,putation\ c_{c_1 \circ c_2}\ \ value\,((\gamma(t_1 - t_Q, c_1) * V_1) \oplus w * V_2)/(w + *\gamma(t_1 - t_Q, c_1))$$

$$\mathrm{Time}\ \mathrm{t}_2\ \ \mathrm{count}\ (\mathrm{n}+1)$$

w is weight of the new direct trust value of node *P* on node *Q*. *w* is proportional to the recommend honest reputation of *P* which can be obtained from DTLCP system, and is inversely proportional to the times of transactions of *Q*.

Parameter *count* denotes the times of transactions that node *Q* has participated. It is updated after every transaction and reflects the reliability of the reputation value. For example, a node *A* has transacted 1000 times is more reliable than a node *B* which only transacted 10 times even if their reputation value is the same.

Expression $\gamma(t_1 - t_Q, c_1)$ is the time decay function which will affect the weight of old reputation in the updating algorithm.

V. Application Scenarios of Reputation System

In a Grid, there are a large number of service providers. Trust and reputation system is needed to help choose more secure and reliable service provides.

Due to the dynamic, open and competitive environment, the application of reputation system in Grid is based on Agent and Virtual Organizations(VO)[13]. The application scenarios can be described as follows:

1) The establishment of virtual organizations: The Agent which wants to get some service initiated service request first; and then resource discovery component localized *n* service providers. A temporary virtual organizations is established, the requesting Agent will be the organization managers of the virtual organization and manager various operations in VO.

2) The manager Agent send bid invitations and service requirements to these *n* service providers. Service providers may be more than one. They can provide a set of services or share a big service task together.

3) At the same time, manager Agent inquires the reputation values of these *n* service providers by DTLCP.

4) Based on the retrieved reputations of these service providers from DTLCP and other feedback information from these service providers, the Agent will decide whether or not to use the services they provided.

5) During the operation of a VO, the reputations of service providers, such as reputations on implementation of the contract or the quality of services provided are monitored by a Monitor Agent. If there is breach of contract or a drop in the quality of service, the MA will report it to the reputation system, and their reputation will be decreased. A member with too low reputation value will be triggered to exit. In order to ensure the availability of virtual organization, re-formation of VO is needed when necessary.

6) The Services ended and the virtual organizations are revocated.

As can be seen from the above description, the Grid transaction in the support of reputation system is more reliable and more suitable for dynamic, open and complex Grid environment.

VI. Simulation Experiment and Results Analysis of Fuzzy Inference Based Reputation Update

As described in section III, six fuzzy subsets are set to express "reputation" linguistic variables. Suppose weight of the new direct trust *w* is computed as 0.2, and 12 fuzzy reasoning rules are set as shown in Fig. 5. The new updated reputation value is obtained by the aggregation operation of these 12 fuzzy reasoning rules with *fuzzy bounded sum* operator ⊕. Every fuzzy rule has a weight in the aggregation.

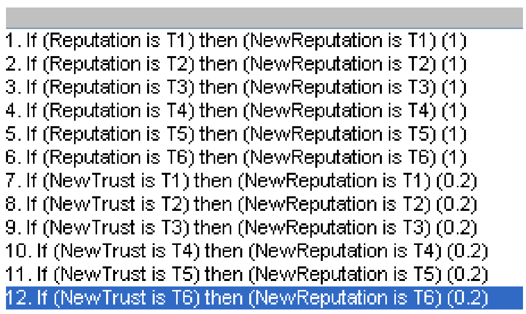

1. If (Reputation is T1) then (NewReputation is T1) (1)
2. If (Reputation is T2) then (NewReputation is T2) (1)
3. If (Reputation is T3) then (NewReputation is T3) (1)
4. If (Reputation is T4) then (NewReputation is T4) (1)
5. If (Reputation is T5) then (NewReputation is T5) (1)
6. If (Reputation is T6) then (NewReputation is T6) (1)
7. If (NewTrust is T1) then (NewReputation is T1) (0.2)
8. If (NewTrust is T2) then (NewReputation is T2) (0.2)
9. If (NewTrust is T3) then (NewReputation is T3) (0.2)
10. If (NewTrust is T4) then (NewReputation is T4) (0.2)
11. If (NewTrust is T5) then (NewReputation is T5) (0.2)
12. If (NewTrust is T6) then (NewReputation is T6) (0.2)

Figure 5. Fuzzy Rules of Reputation Updating.

With the original reputation value R_{old} is 0.518, and the new direct trust T_{new} is 0.723, under the support of these fuzzy reasoning rules, we can calculate the new value of the reputation R_{new} =0.559. The rules viewer of all reputation updating fuzzy rules is shown in Fig. 6.

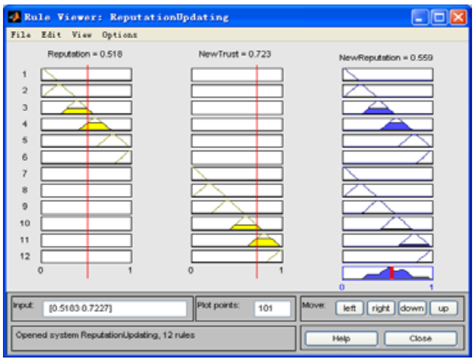


Figure 6. Rules viewer of all reputation updating fuzzy rules.

The input and output surface viewer of reputation composing when the weight of new direct trust *w* is 0.2 is shown in Fig. 7.

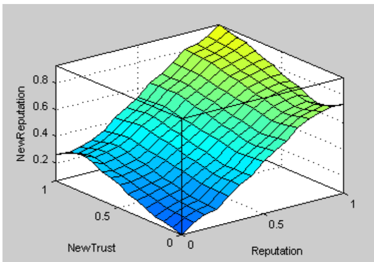


Figure 7. Input and Output Surface Viewer When the Weight of New direct Trust is 0.2.

If the reliability of old reputation of *Q* is not high, that is, the times of transactions of *Q* is small, the last reputation is updated a long time ago or the reputation in recommend context of node *P* transacted with *Q* is relatively high, the weight of new direct trust of *P* on *Q, w,* will be higher. Suppose the weight *w* is computed as 0.6, the input and output surface viewer of reputation composing based on fuzzy reasoning rules is shown in Fig. 8.

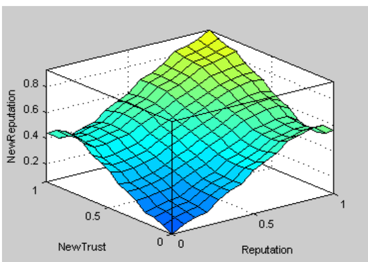


Figure 8. Input and Output Surface Viewer When the Weight of New direct trust is 0.6.

From Fig. 7 and Fig. 8 we can see, when the weight of new direct trust is higher, the new reputation increased with new direct trust faster. That is, if the times of transactions of *Q* is small, the last reputation is updated a long time ago or if the recommend reputation of node *P* is relatively high, the impact of new direct trust on new reputation is higher.

VII. CONCLUSIONS

Trust and Reputation system plays an important role in Grid security field. In this paper, fuzzy theory is used to express and compute trust. The direct trust matrix can be gotten by variable weight based fuzzy comprehensive evaluation. By increasing the weight of the attribute when its value is low, such as the evaluation of factor contract abidance is too small, we can give prominence to deficiency, and then the Grid entities can avoid choosing service providers with some defective.

Reputations are obtained by fuzzy deriving and fuzzy combination. Initialization of reputation and updating of reputation are all discussed in this paper. A DHT based Dual Two-Layer Chord Protocol(DTLCP)is proposed as reputation storage and retrieval infrastructures with which the reputation system can provide efficient storage and queries that operate in *O(logN)* +*O(M)*overlay hop(*N* is the number of domains in Grid and *M* the number of nodes in a domain, *M*<<*N*). DTLCP can adapt efficiently as nodes join and leave the system, and can answer queries even if the system is continuously changing.

In the support of this reliable fuzzy theory based reputation system, trusts and reputations in Grid can be expressed and computed appropriately and simulation experiment and results analysis demonstrate that entities in Grid can interact with other entities more securely.

In this paper, the fuzzy reasoning rules is established and simplified based on experts experience. In the future further study, we will focus on the automatically generation of fuzzy rules base, with fuzzy neural networks and genetic algorithms.

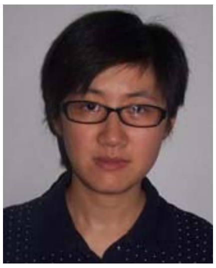
ACKNOWLEDGMENT

The authors wish to thank the anonymous reviewers for their valuable comments and suggestions. This work was supported by the Natural Science Foundation of Jiangsu Province of China under Grant NO.BK2006039.

REFERENCES

[1] Alfarez Abdul-Rahman, Stephen Hailes, "Supporting Trust in Virtual Communities," *33rd Hawaii International Conference on System Sciences(hicss 00)*-Volume 6, 2000 IEEE Press, Dec. 2007, pp. 6007.
[2] Audun Jφsang, "The Beta Reputation System", *15th Bled Electronic Commerce Conference; e-Reality: Constructing the e-Economy; Bled, Slovenia*, June2002.
[3] Andrew whitby, Andun Jφsang; "Filtering Out Unfair Ratings in Bayesian Reputation Systems"; *Icfain Journal of Management Research*. Feb.2005, Vol.IV.No.2 pp.48-64.
[4] Lik Mui, Mojdeh Mohtashemi; "Ratings in Distributed Systems: A Bayesian Approach". *Workshop on Information Technologies and Systems* (WITS'2001).
[5] Tang W, Chen Z, "Research of subjective trust management model based on the fuzzy set theory," *Journal of software*, 2003, 14(8):1401-1408.
[6] Tang W, Hu JB, Chen Z; "Research on a Fuzzy Logic-Based Subjective Trust Management Model," *Journal of Computer Research and Development* 42(10), 2005, pp. 1654~1659.
[7] Shanshan Song, Kai Hwang, and Mikin Macwan, "Fuzzy Trust Integration for Security Enforcement in Grid Computing, " *NPC 2004, LNCS 3222*, pp. 9-21.

[8] Farag Azzedin and Muthucumaru Maheswaran, "Evolving and Managing Trust in Grid Computing Systems," *Proceedings of the 2002 IEEE Canadian Conference on Electrical Computer Engineering*, vol.3, pp. 1424- 1429.
[9] Yao Wang, Julita Vassileva, "Trust and Reputation Model in Peer-to-Peer Networks", *Proceedings of the Third International Conference on Peer-to-Peer Computing* (P2P'03), 2003 IEEE. Sep. 2003, pp.150 – 157.
[10] Peng Zuzeng and Sun Wenyu, *Fuzzy Mathematics and its application*, Wuhan University Press, Sep. 2007.
[11] B. K. Alunkal, "Grid Eigen Trust – A Framework for Computing Reputation in Grids," *Master Thesis submitted to Computer Science Department, Illinois Institute of Technology*, Chicago, 2003.
[12] F. Azzedin and M. Maheswaran, "Trust Brokering System and its Application to Resource Management in Public-Resource Grids," *18th International Parallel and Distributed Processing Symposium* (IPDPS'04).Santa Fe: IEEE Computer Society, 2004, pp.22-32.
[13] Jianhua Shao, W Alex Gray, Nick J Fiddian Vikas; "Supporting Formation and Operation of Virtual Organizations in a Grid Environment," *The UK OST e-Science second All Hands Meeting 2004* (AHM'04), Nottingham, UK ,Sep. 2004.
[14] I. Stoica, R. Morris, D.R. Karger, M.F. Kaashoek, H.Balakrishnan, "Chord: a scalable peer-to-peer lookup service for Internet applications", *Proceedings of the 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications* (SIGCOMM 2001), ACM Press, 2001, pp. 149–160.
[15] Yuh-Jzer Joung, Jiaw-Chang Wang; "Chord2: A two-layer Chord for reducing maintenance overhead via heterogeneity"; *Computer Networks* 51 (2007) 712–731.



Liao Hongmei was born in Anhui, China on 1977/11/27. She received her B.S. degree in Computer Science and technology from Northeast Normal University(China) in 2000, and her M.S. degree in Computer Science and Technology from China University of Mining and Technology in 2007. Currently, she is a Ph.D. student in School of Computer Science and Technology, China University of Mining and Technology.

She is now a Lecturer in Computer Science and Technology , China University of Mining and Technology. Her research interest is on data fusion, trust model, reputation system, routing protocols in Grid and wireless sensor networks.

Wang Qianping was born in Anhui, China in 1964. He received his Ph.D. degree from Institute of Computing Technology of the Chinese Academy of Sciences in 1997.

In 2000–2002, he visited the Department of Computer Science, Hong Kong University of Science and Technology and researched in "Digital Factory". Now, he is a Professor of the Department of Computer Science and Technology in China University of Mining and Technology. His current research interests include network security and routing protocols in P2P Networks, mobile and pervasive computing and analysis of algorithms for deployment.

Li Guoxin was born in Hebei, China in 1978/10/22. He received his B.S in 2001 from School of Information and Electric Engineering, China University of Mining and Technology.

He is now a Lecturer in Computer Science and Technology , China University of Mining and Technology. He is currently working toward a Ph.D. degree at China University of Mining and Technology. His current research involves security of networks and trust system in P2P and Grid.