VOMES: A VIRTUAL ORGANIZATION MEMBERSHIP EVALUATION SYSTEM

Junwei Cao [*]
Zhen Wang
Research Institute of Information Technology
Tsinghua National Laboratory for Information Science and Technology
Tsinghua University, Beijing 100084, P. R. China
[*]Corresponding email: jcao@tsinghua.edu.cn

Abstract

A grid supports geographically distributed sharing of CPUs, storage and network resources among multiple organizations, which can be considered as a special type of Virtual Organizations (VO) consisting of resources and users. A CyberInfrastructure (CI) environment supports formation and management of multiple such VOs to meet various computing demands for researchers and scientists in different areas. A VO can be founded for a certain scientific collaboration so that a trust domain can be established to aggregate and manage appropriate resources and users. How to found a trustable VO and aggregate reliable resources and users for the cross-domain collaboration in a CI becomes an important issue. In this work, we provide detailed comparison of trust management in three different types of virtual communities: e-commerce, peer-to-peer (P2P) and grid environments. A VO Membership Evaluation System (VOMES) is proposed to address this new challenge brought by the CI environment. VOMES includes a layered reputation system and a committee based decision-making method to verify a new applicant to a VO and maintain corresponding VO trust levels. Simulation results show that our reputation system is accurate, robust and stable. The committee based fuzzy decision-making method can also be used to identify malicious members from reliable ones. VOMES can automatically help members in a CI environment establish and maintain VOs with high trust levels.

Key Words: Cyberinfrastructure, Virtual Organizations, Grid Computing, Trust Management, Reputation Calculation

1. Introduction

Modern scientific research has great and various requirements for experimental instruments, computational ability and collaboration across organizations and subjects [1]. In order to support larger scale resource sharing, some grids no longer just focus on specific scientific applications but are expanded to handle multiple scientific research projects and meet various computing demands from researchers, such as Open Science Grid (OSG) [2], Enabling Grids for E-science (EGEE) [3], Tera Grid [4] and so on. As these multifunctional grids are general platforms to provide computing support for various scientific applications, they are termed as CyberInfrastructure (CI) [1][5][6][7]. For one scientific project, a specific Virtual Organization (VO) [8][9] is proposed, established and managed in the CI. A VO is a set of Users and Resource Providers (RPs) with agreements on usage purposes and sharing policies. As one of the most widely used grids, OSG supports more than twenty VOs for different scientific projects, ranging from biology to astrophysics, which are managed by different organizations, institutes or laboratories [2].

In a CI environment, one of the most important issues is how to establish a VO with appropriate Users and RPs. In traditional grids, all Users and RPs have been verified with each other in real world and enable their agreement on how to share resources on the network through certificates assigned by the same Certificate Authority (CA), which means they all belong to a same trust domain [10][11]. But in order to meet various requirements from scientific projects on computing resources, in a CI environment members (Users or RPs) usually belong to different trust domains and have complex memberships with each other. One VO is established for one trust domain and one scientific application. Since CI members come from various fields and its number much more than that of grids, it is impossible for CI members to verify each other and establish trust relationship in real world.

Existing VO management tools, such as VOMS [12] and GUMS [13], all focus on membership information services, without any automatic trust evaluation mechanism. To verify a new applicant, VOMS sends this application and self-description to a certain representative. The representative verifies the new applicant personally from several aspects, including past membership records and resource usage plans with following limitations [14].

- The procedure of verifying an applicant deeply relies on representative's individual experience and knowledge. As the member number in a CI environment (e.g. OSG) is always very large, it is impossible for representatives to get familiar with all the applicants
- Since the judgment is given by an individual, the result could involve subjective factors. In this case, a tool is required to provide objective evaluation information to minimize subjective influence.
- More representatives always mean more dissension but leads to a more accurate decision. Representatives with current tools can only consult manually with each other by Emails, which is not efficient to meet the CI requirement.
- The registration based on Emails and manual operations takes at least several days to complete one registering procedure and requires that representatives and VO administrators keep on line.

To address issue mentioned above, we propose VOMES based on a layered reputation system and committee based fuzzy decision-making method. A reputation system is provided to track members' historical activities and use a reputation value to characterize their behaviors. The reputation system is in charge of recording all interactions in a CI environment. It calculates two kinds of reputation for a member, global reputation and local reputation. Global reputation calculation is based on the records of all interactions the given member involves, presenting general judgment to it. Local reputation is calculated using interactions only between two specific members, which represent the judgment of one member on another. These two reputation values can describe a member behavior pattern comprehensively and accurately in different aspects. A VO administrator can designate a committee of several representatives to verify the new applicant to the VO according to the reputation system and representatives' individual experiences. Every representative hands up their own judgment about the applicant according to the global and local reputation values to the committee. The committee makes a decision after comprehensive consideration of opinions from every representative using a fuzzy-logic theory [15][16][17][18].

The rest of the paper is organized in the following way. In Section 2, reputation and trust managements in different virtual environments, e.g. e-commerce, P2P and grids, are summarized. Section 3 provides detailed information on VOMES, including a reputation calculation system and a committee based decision-making using fuzzy method. Simulation results to evaluate VOMES performance from various aspects are demonstrated in Section 4. We conclude our work and give a brief discussion on further work in Section 5.

2. Related Work

There are three typical virtual communities on the Internet, including e-comment, P2P and grids. How to characterize member behavior patterns and help members establish appropriate trust relationships is a significant challenge for all virtual communities. Reputation system is wildly used to represent member behavior pattern and help members in virtual communities make decisions on interactions. Different communities have different policies and topologies, leading to different trust models and distinct ways of establishing trust relationships among members.

2.1. Trust Models for E-commerce

E-commerce is a centralized, open and huge scale virtual community which requires high trust insurance and accurate and stable reputation system. As a trade platform for both consumers and good providers, e-commerce emphasizes on providing accurate and simplified reputation schemes for consumers to conduct successful trades and inhibit malicious and cheating behaviors [19]. Consumers can evaluate good providers according to their reputation values [20] and make a trade decision personally. How to provide accurate and stable reputation values to characterize member behavior patterns is a significant challenge for e-commerce administrators.

Generally speaking, trust models for e-commerce can be classified into two categories: accumulated models and average models. In an accumulated model, feedbacks from consumers on evaluation of providers are accumulated as the current reputation value. Positive feedbacks due to successful trades increase a provider's reputation value and negative ones decrease the value. This type of trust models cost little computational resources and storage; on the other hand, it ignores many other factors, for example successful trade rate and is not accurate enough. Some existing online markets, e.g. eBay [21][22], Yahoo! and TaoBao [23], all adopt the accumulated trust model. The average trust model also accumulates all feedbacks of consumers on a provider, though divided by the number of feedbacks. The divided value is the average reputation value of the corresponding provider. The average model costs more and can not separate different reputation levels of providers distinctly. Both Amazon and AuctionSoup adopt the average trust model.

2.2. Trust Models in P2P Environment

A peer-to-peer (P2P) environment which usually focuses on resource discovering and data transferring applications is an open, self-organized and decentralized system. The trust relationship is also established based on member reputation values and individual judgments. There is no central member to maintain member reputation values due to the P2P topology. However, a global reputation evaluation is still required for judgment and inhibition of selfish and malicious behaviors. When a data transfer occurs between two members, a feedback to the file provider is also produced but maintained by the user. Since there is no central member with global information, P2P system usually adopts a mechanism to aggregate distributed feedbacks over the system to calculate global reputation of a certain member [24].

For a small scale P2P system, it is possible to collect feedbacks from all other members. But in most cases, a P2P system may include tens of thousands of members. How to choose members who can contribute their feedbacks about a given member and calculate all these feedbacks as the global reputation of that member becomes a key challenge. There are many mechanisms helping users to obtain feedbacks of most trustable members, such as PowerTrust [25], Gossip Trust [26][27] and EigenTrust [28]. In a P2P environment, trust models mainly are proposed to ensure the efficiency of collecting trustable members for feedbacks, for the collecting procedure would consume more time and storage as scales of P2P systems increase.

2.3. Trust Models in Grid

Once established, a grid environment is already a trustable and centralized virtual community [29][30]. All members in a grid, Users or RPs, already have achieved agreements on resource sharing before the grid is established. They maybe know each other very well in real world projects or collaborations. The grid is just an enabling technology for implementation of this achieved agreement and resource sharing policies on the Internet. If a new member wants to join in a grid, he must be verified by grid representatives personally and manually. Since a grid is already a virtual community with high trustable and secure level and a new member is usually verified in real world, generally speaking, grid doesn't need a reputation system to evaluate its members.

2.4. Trust Models for CI

CI is an open and partly-centralized virtual community that provides a public platform for establishing grid-like VOs and sharing resources among members dynamically. Members establish trust relationships through VOs and CI provides tools and services for VO management and maintenance. One VO forms one trust domain. Members can share resources with each other only if they belong to the same trust domain, i.e. in the same VO.

One member can belong to different VOs for resource sharing, with different trust levels applied. Different VOs or trust domains can be established and maintained using VOMES, making it possible to satisfy various scientific demands while other virtual communities all have only one trust domain. Table 1 shows the difference from other virtual communities.

Table 1. Comparison of CI with Other Virtual Communities

Virtual Communities	Trust Domains	Trust Relationships
E-commerce	Members belong to the same domain.	Establish trust relationship only between two members.
P2P	Members belong to the same domain.	Establish trust relationship only between two members.
Grid	Members belong to the same trust domain.	All the members have trust relationships among each other.
CI	Members belong to different trust domains.	Members in the same VO have trust relationships.

VOMES focuses on establish and maintain a specific trust domain for a given scientific project dynamically and is in charge of providing membership management services. VOMES provides a whole scheme including a reputation system and a committee based fuzzy comprehensive decision making scheme to help CI members verify VO applicant to establish specific VOs for application specified requirements. Detailed information is given below.

3. VOMES

VOMES consists of two components: a layered reputation system and a committee based fuzzy decision–making method. The reputation system associates reputation values with member behavior patterns and are also input values for the committee to make a decision. A committee is proposed to make a comprehensive decision on a given member according to reputation values and VO configurations.

3.1. Key Concepts

Task Request Time (TRT): Expected time a task should be completed on a given resource, denoted as *Tr*. The user evaluates the complexity of the program and resources assigned to him in order to estimate an expected execution time for his program.

Task Completing Time (TCT): TCT is the actual time from submitting the task to receiving the corresponding report. The report would be task outputs if the task is successfully completed or an error record if the task is failed. TCT value is denoted as *Tc*.

Interaction Quality (IQ): Denoted as *Q* to represent three different situations: task is finished in time (i.e.$Tc \leq Tr$), beyond the request time (i.e.$Tc>Tr$) or task is failed, with different follow-up impacts on members. We assign different values to these three IQ levels to encourage successful interactions and punish failures.

Reference Member (RM): This is a perfect member only exists in theory. Since the interaction quality is influenced by both participants, it is hard to ascribe a failure to either participant. The reference member is an ideal member that provides perfect service to others. So interaction quality between a reference member and any given member is only up to the real member, which can reflect its behavior pattern independently.

Member Behavior Pattern (MBP): We describe a member behavior pattern with three possibilities $P=\{p_1,p_2,p_3\}$, representing possibilities of three IQ levels, respectively.

Reputation Value (*PCMM*): After an interaction is finished, a score is calculated, according to the T*RT* and IQ of this interaction to present its impact to the reputation. The T*RT**IQ value can be accumulated and divided by the sum of corresponding T*RT*, which is taken as the reputation value (RV).

Theoretical Reputation Value (*TRV*): If we already know the actual MBP of a member, we can calculate an overall expectation value of its reputation, *QP*, as the theoretical reputation value (TRV) of a member. We use the TRV to represent the member behavior pattern for simplicity in this paper.

Global Reputation (GR): This reputation, denoted as *Gr*, is maintained by the CI Management Center (CIMC), tracking historical behaviors of a member since he joins in the CI. This reputation represents member interaction behavior patterns with all other members in CI.

Local Reputation (LR): This reputation, denoted as is *Lr*, is maintained by members themselves, recording historical interactions between specific members. This reputation represents one member's individual judgment about the behavior pattern of a given member.

Independent Malicious Behavior (IMB): Members may decrease the quality of interactions deliberately. If an independent malicious member is a user, he may submit unexecutable tasks or unreasonable expected time *Tr* and so all. If it is a RP, he may not allocate sufficient resources and privileges to run the program. This behavior may disarrange ordinary interactions and the reputation system, which should be prohibited.

Collusive Malicious Behavior (CMB): Members cheat for a very high global reputation value by bogus successful interactions with collusive members. The two members may interact using empty tasks and result reports in order to cheat for high global reputation.

3.2. Reputation Calculation

3.2.1 Global Reputation Calculation Algorithms

Assuming a member M_j (j=1,2,……,m) (a User or RP) has interacted with other members for n times, Q_i (i=1,2,……,n) is IQ of the i^{th} interaction, and Tr_i and Tc_i are T*RT* and TCT of the i^{th} interaction, respectively.

$$Q_i = \begin{cases} 1 \quad if \quad \text{task is completed} \quad and \quad Tc_i \le Tr_i \\ 0 \quad if \quad \text{task is completed} \quad and \quad Tc_i > Tr_i ,\left(i=1,2,......,n\right) \\ \text{-1} \quad if \quad \text{task is failed} \end{cases} \tag{1}$$

Given the definition of Q above, we can calculate the TRV using the MBP of a member:

$$TRV = QP = [1,0,-1]\begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} = p_1 - p_3 \tag{2}$$

After *n* interactions, the accumulated Q-weighted T*RT* for member M_j is denoted as $V_j(n)$ while the accumulated T*RT* is denoted as $S_j(n)$.

$$V_j(n) = \sum_{i=1}^{n} Tr_i * Q_i, \left(j = 1, 2, ..., m \right) \tag{3}$$

$$S_j(n) = \sum_{i=1}^{n} Tr_i, \left(j = 1, 2, ..., m \right) \tag{4}$$

Because quality of interactions is determined by behavior patterns of both participants, we use the switch calculator to approximate each of behavior patterns, assuming they both have equal responsibility for the interaction quality. The validity of the algorithm is provided in Section 4.

$$Gr_j(n) = \sqrt{\frac{V_j(n)}{S_j(n)}} = \sqrt{\frac{\sum_{i=1}^{n} Tr_i Q_i}{\sum_{i=1}^{n} Tr_i}}, \left(j = 1, 2, ..., m \right) \tag{5}$$

However, Formula (5) does not consider the time factor: the latest interaction record can represent current behavior pattern changes more accurately. We propose an attenuation index β ($0 \leq \beta \leq 1$), to reflect the time influence on the record reference value. Considering time attenuation influence to the global reputation, $Gr_j(n)$ is calculated as follows:

$$Gr_j(n) = \sqrt{\frac{V_j(n)}{S_j(n)}} = \sqrt{\frac{Tr_n Q_n + \beta V_j(n-1)}{Tr_n + \beta S_j(n-1)}}, \left(j = 1, 2, ..., m \right) \tag{6}$$

Initial values of $V_j(0)$ and $S_j(0)$ are configured according to requirements when a member joins in CI.

3.2.2 Local Reputation Calculation Algorithms

Local reputation is similarly defined as global reputation but only based on the past interactions between two specific members. *Lr* represents a member's individual judgment on a given member based on the interaction history between the two while *Gr* is the general judgment about a member of CI. We denote $Lr_{jk}(n)$ as the local reputation the member M_j assigns on M_k at *n* times interaction with M_k, which can be calculated similarly as follows:

$$Lr_{jk}(n) = \sqrt{\frac{Tr_n Q_n + \beta V_{jk}(n-1)}{Tr_n + \beta S_{jk}(n-1)}}, (j, k = 1, 2, ...m) \tag{7}$$

Compared with global reputation, local reputation is more flexible and personalization. The local reputation value calculated by Formula (7) is just for reference, since it is maintained locally by the member himself so can be changed personally. One member can assign a very low value to the local reputation of another member to prevent future interactions with that member. Local reputation is designed to reflect individual judgment, compared with global reputation.

3.3. Membership Evaluation

In the last section, we propose a whole scheme to calculate global and local reputation to describe member behavior patterns on different aspects. In general, an applicant should be approved by all existing members in the VO before he joins in. We can not just simplify the issue by using uniform reputation thresholds to evaluate members, which is widely used in P2P and e-commerce virtual communities, since different members may have different judgments for a given applicant. Another difficulty is that for both the applicant and VO members, it is not feasible to carry out the approval process between the applicant and every member because the member number of CI can be very large.

In this work, a committee-based fuzzy decision-making is proposed. The committee consists of part of members in a VO, called representatives, to present the various requests of all members and can reduce the approval process time. The fuzzy decision-making method can express fine-grained judgments of representatives compared with voting mechanisms [31][32] and make a comprehensive decision automatically, which dramatically simplifies the approval process.

The committee based fuzzy decision-making method, including verification and reviews, are designed to insure the trust level of a VO and minimize malicious behaviors appearing aperiodically. New applicant has to be verified and members in the VO are reviewed periodically in order to prohibit possible malicious behaviors, for collusive malicious members may cheat in or the behavior pattern of a member may change after joining. In this section, we introduce the committee based fuzzy decision-making method in details and the performance of the two processes is evaluated in the next section.

3.3.1 Fuzzy Inference

There are two reasons to adopt fuzzy inference. One reason is that reputation values always have different meanings for different members, for example, a member with reputation value 0.7 means reliable enough for some Users but may not for others. The membership vector can eliminate this difference and provide a uniform opinion description to the committee. Second reason is that fuzzy logic is robust to deal with uncertainty and inaccuracy of CI reputation values. Fuzzy inference can map accurate and absolute reputation values to membership degrees belonging to a fuzzy set using a function $\mu(x)$ ($0\leq\mu(x)\leq1$). The positive 1 presents fully belonging to the given set and 0 means nothing to do with the given fuzzy set.

Firstly we calculate a comprehensive reputation value, which is actually a weighted average of local and global reputation values. Denote the comprehensive reputation value M_j assigns on M_k as Cr_{jk}:

$$Cr_{jk} = \alpha Lr_{jk} + (1-\alpha)Gr_k, 0 \leq \alpha \leq 1 \ , \tag{8}$$

, where α is configured by M_j. The higher α is the more important Lr_{jk} is. In extreme cases that α equals to 1, M_j only trusts his own judgment. If α equals to 0, M_j totally trusts global reputation.

And then we use a membership function maps absolute comprehensive reputation values to membership degrees to different sets. We divide members into three sets: reliable members (RLM), indeterminate members (IDM) and unreliable members (URM). The judgment M_j makes on M_k is described by the membership vector, denoted as V_{jk}=(v_1,v_2,v_3), respectively representing membership degree M_j regard M_k as RLM, IDM and URM.

A generally used membership function is provided to calculate the membership degree. Assuming membership function for v_1, v_2 and v_3 are $\mu_1(Cr_{jk})$, $\mu_2(Cr_{jk})$ and $\mu_3(Cr_{jk})$. Figure 1 shows the three membership functions over Cr_{jk} and corresponding formulations are also included below.

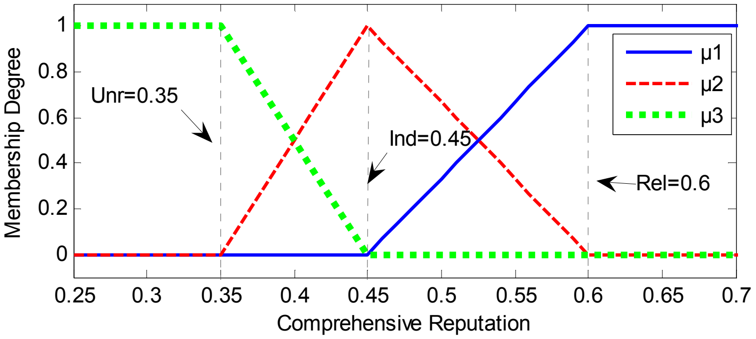

Figure 1. Membership Functions for Fuzzy Inference

$$\mu_1(Cr_{jk})=\begin{cases} 0, & Cr_{jk}\le Ind \\ \dfrac{Cr_{jk}-Ind}{Rel-Ind}, & Ind<Cr_{jk}<Rel \\ 1, & Cr_{jk}\ge Rel \end{cases}$$

$$\mu_2(Cr_{jk})=\begin{cases} 0, & Cr_{jk}\le Unr \quad or \quad Cr_{jk}\ge Rel \\ \dfrac{Cr_{jk}-Unr}{Ind-Unr}, & Unr\le Cr_{jk}\le Ind \\ \dfrac{Rel-Cr_{jk}}{Rel-Ind}, & Ind\le Cr_{jk}\le Rel \end{cases} \tag{9}$$

$$\mu_3(Cr_{jk})=\begin{cases} 1, & Cr_{jk}\le Unr \\ \dfrac{Ind-Cr_{jk}}{Ind-Unr}, & Unr<Cr_{jk}<Ind \\ 0, & Rel\le Cr_{jk} \end{cases}$$

In Formula (9), *Rel* is the threshold for reliable members while *Unr* is the threshold for unreliable members. *Ind* represents typical indeterminate members. The membership degree vector V_{jk}={$\mu_1(Cr_{jk})$, $\mu_2(Cr_{jk})$, $\mu_3(Cr_{jk})$} can totally represent the opinion of the representative M_j on the applicant M_k. A VO administrator receives all these judgments from representatives of the committee and integrates them to a final decision using the fuzzy comprehensive decision-making model described below.

3.3.2 Fuzzy Comprehensive Decision-making Method

There are two reasons for choosing the fuzzy comprehensive decision-making model: capability to handle uncertainty, fuzziness, and incomplete information adaptively and capability to make comprehensive decisions by integrating multiple factors [33][34][35].

Assuming the number of representatives in the committee is *p*, the complete fuzzy comprehensive decision-making model consists of four elements: the factor set

$$U = \{u_l \mid l = 1, 2, \ldots\ldots, p\},$$

is a list of factors concerning with decision-making. In our case, every representative has influence on decision-making, so they are all regarded as factors. Corresponding weight vector

$$A = \{a_l \mid l = 1, 2, \ldots\ldots, p\},$$

can be used to describe different importance and influence of representatives in the committee: a_l represents the weight of representative u_l in decision-making. The evaluation set

$$V = \{v_h \mid h = 1, 2, 3\}$$

represents three different sets members are divided into. The factor judgment vector

$$f(u_l) = \{r_{lh} \mid h = 1, 2, 3\}, \sum_{h=1}^{3} r_{lh} = 1, l = 1, 2, \ldots\ldots, p,$$

is membership degrees a member belongs to v_h, which is given by M_l.

We adopt the $M(\wedge \vee)$ model, namely the max-min model, to calculate the comprehensive decision. Let B be the judgment matrix:

$$R = \begin{bmatrix} f(u_1) \\ f(u_2) \\ \vdots \\ f(u_p) \end{bmatrix} = \begin{bmatrix} r_{11} & r_{12} & r_{13} \\ r_{21} & r_{22} & r_{23} \\ \vdots & \vdots & \vdots \\ r_{p1} & r_{p2} & r_{p3} \end{bmatrix}$$

Use $M(\wedge \vee)$ model to calculate judgment vector *B* and its normalization *B'*.

$$B = A \circ R = \{b_h \mid h = 1, 2, 3\}$$

$$b_h = \max_l(\min(a_l, r_{lh})) \qquad l = 1, 2, \ldots\ldots, p, h = 1, 2, 3 \tag{10}$$

$$b_h^{'} = \frac{b_h}{\sum_{h=1}^{3} b_h}, h = 1, 2, 3 \tag{11}$$

b'_h represents the percentage degree the committee prefer the judgment of v_h. The VO administrator can configure a threshold for b'_h: if there is a b'_h higher than the threshold, the VO administrator will adopt the decision v_h, since he believes this decision can represent the majority view of the committee or VO members. If there is no b'_h higher than the threshold, the VO administrator will check the applicant personally.

4. Simulation and Evaluation

In this section, we evaluate the accuracy and robustness of reputation calculation and the performance of verification procedure and review procedure.

4.1. Reputation Analysis

4.1.1 Performance Metrics

A good and robust reputation system should rapidly and exactly reflect member behavior patterns, has distinct degrees to differentiate various behavior patterns and can eliminate malicious behaviors. We define three performance metrics, including Reputation Standard Variance (*RSV*), Stable Reputation Value (*SRV*) and Rising Time (*RT*) over different behavior patterns and different Percentages of Malicious Members (*PMM*), consisting of Percentage of Independent Malicious Members (*PIMM*) and Percentage of Collusive Malicious Members (*PCMM*).

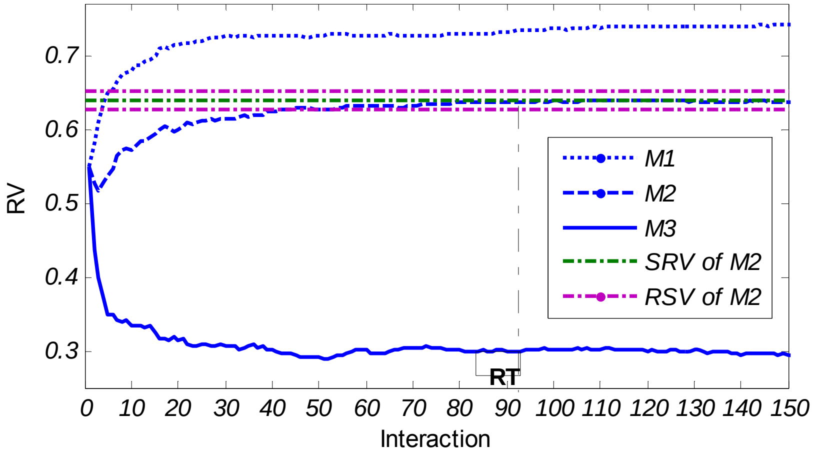

Figure 2. Dynamic Processes of Reputation Calculation – Performance Metrics

Figure 2 shows how reputation changes over interactions in a VO with 100 members and 5% malicious members. Three curves respectively represent members with three different behavior patterns: reliable, unreliable and an ordinary member between the two extreme cases. The TRV of three members are 0.9, 0.7, and 0.3, respectively. Since interactions in a simulated VO environment are all based on probability, all the data is an average value of 100 simulation results in this section.

As shown in Figure 2, the rising time *RT* is defined as the first time the reputation reaches the *SRV*. *RT* reflects the rate reputation value reflect the member behavior pattern. The faster the reputation reaches the stable value, the more sensitive the reputation system is. However, higher sensitivity of the reputation system always leads to unstable reputation values. The reputation value may oscillate dramatically near the *SRV* though the member behavior pattern is fixed. *RSV* is used to evaluate the stableness of the reputation system.

Three curves final reach stable values, which we hope can reflect actual TRV. *SRV* is used to analyze the reputation accuracy.

From the simulation, the rise time *RT* varies little over different behavior patterns but is greatly influenced by initial values of $V_j(0)$ and $S_j(0)$. Because in most cases, statistic initial values for all the members are fixed in CI, so the *RT* changes a little and we just focus on analyzing *RSV* and *SRV* changes over different situations below.

4.1.2 Simulation Environment

Our simulation environment is a VO with 100 members with TRV from 0.6 to 0.75. The malicious member is defined as the member that has distinct low TRV from 0.2 to 0.3. We put a member with assigned behavior pattern in the VO and track its global reputation after every interaction. In the experiment of analyzing the performance over different behavior patterns, the percentage of malicious members is fixed at 5% and the TRV of tracked member changes from 0.2 to 1. In the experiment of analyzing the performance over different percentages of malicious members, TRV of tracked member is fixed at 0.7 and the percentage of malicious members changed from 0 to 50%.

Because both independent and collusive malicious members have low TRV and the only difference is that collusive malicious members cheat for high global reputation through bogus interactions with accomplice, we just consider how the low TRV affects the reputation system and the issue of bogus high global reputation is addressed in Section 4.2. As the local reputation involves too much subjective factors and has similar calculation formula as the global reputation, we just analyze performance metrics for global reputation in the following sections.

4.1.3 Performance over Different Behavior Patterns

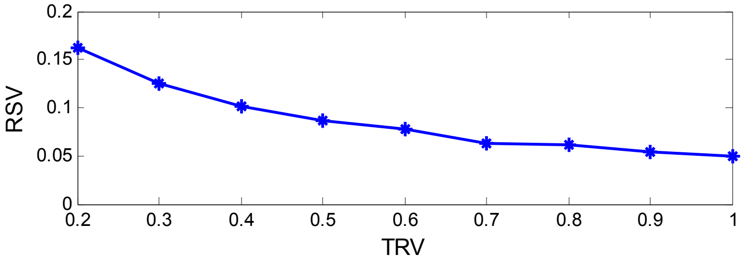

Figure 3. Performance Evaluation - *RSV* over *TRV*

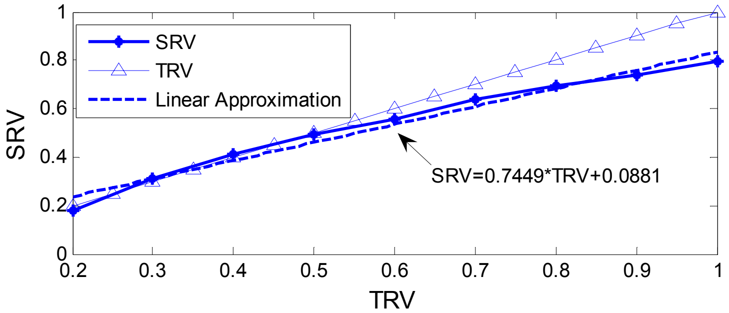

Figure 4. Performance Evaluation - *SRV* over *TRV*

As shown in Figure 3, it is obvious that *RSV* is limited to sufficient low values, no matter TRV is. Reputation values of malicious members (with low TRV) have higher *RSV* which indicates that their reputation value change more easily. This is because malicious members always have low reputation values and are easily influenced by randomicity of interaction quality.

Reputation values should also reflect actual behavior patterns of members, which can be evaluated using *SRV*. Figure 4 shows three curves, the global *SRV* calculated by the reputation system, linear approximation for the calculated *SRV* and the actual TRV.

It is obvious that the calculated *SRV* is an approximate linear line. Linearly mapping the actual TRV to *SRV* can insure the reputation value having sufficient differential degree to classify members with different behavior patterns. The linearity relationship between *SRV* and TRV can ensures the *SRV* accuracy and differential degrees.

4.1.4 Performance over Different Percentages of Malicious members

Another performance aspect of reputation calculation is robustness to malicious behaviors. Malicious members lead to failed interactions which decrease and disorder reputation values of actual reliable members. A good reputation calculation scheme should minimize influence of malicious behaviors to a reasonable scope and ensure stableness and accuracy of reputation values of other members.

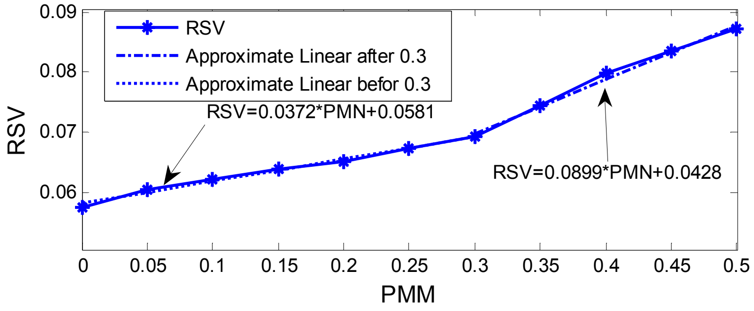

Figure 5. Performance Evaluation - *RSV* over *PMM*

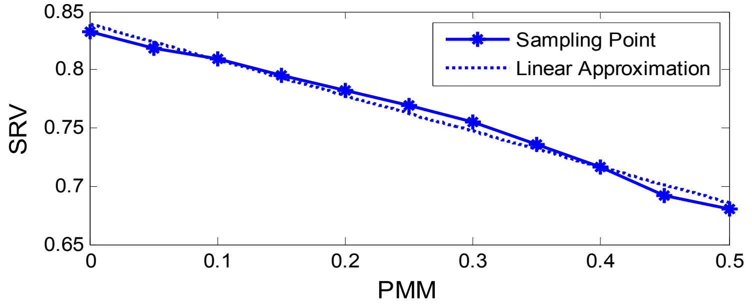

Figure 6. Performance Evaluation - *SRV* over *PMM*

Figure 5 shows how the *RSV* of a member with TRV=0.7 changes over different *PMM* in the VO. It is shown in the figure that *RSV* increases linearly as the *PMM* increases. There is a turning point at *PMM*=0.3: *RSV* increases faster if *PMM* is bigger than 30%. So it is better to keep *PMM* in a VO below 30%. When *PMM* equals to 50%, the *RSV* reaches the maximal point.

Figure 6 shows how malicious members affect the *SRV*. The *SRV* decreases linearly when *PMM* increases and the slope is -0.27. *SRV* keeps stable if there are only a small number of malicious members in the VO and the verification procedure can limit the percentage of malicious members in a VO, which is introduced in Section 4.2.

In this section, we evaluate the reputation system using three performance metrics, *RSV*, *SRV* and *RT*. We examine how *RSV* and *SRV* changes over different TRV and *PMM* in CI. From the results, we can conclude that our reputation calculation system can linearly, rapid and stably reflect various member behavior patterns and greatly defense malicious members in a VO with no more than 30% *PMM*.

4.2. Committee Performance

Verification occurs when an applicant joins in the VO and reviews are carried out periodically to identify both independent and collusive malicious members and maintain the VO trust level in time. In this section, we analyze the performance of the two processes over different *PMM*. The committee has great influence on the verification performance. So we also test how the scale of the committee affects the verification performance in 4.2.5.

4.2.1 Performance Metrics

Two performance metrics are used to evaluate performance of verification and reviews: errors of classifying malicious members as reliable ones and errors of classifying reliable members as malicious ones. We define the two types of errors as Positive Errors (*PE*) and Negative Errors (*NE*) respectively.

PE = (Number of malicious members regarded as reliable) / (Number of malicious members);

NE = (Number of reliable members regarded as malicious) / (Number of reliable members).

4.2.2 Simulation Environment

Table 2. Simulation Parameters

m	200	*Ind*	0.6
p	10	Number of Members in CI	1000
α	0.4	Reliable Member Behavior Pattern	(0.9:0.067:0.33)
β	0.99	Malicious Member Behavior Pattern	(0.7:0.2:0.1)
Rel	075	Initial Value $V_j(0): S_j(0)$	3:10
Unr	0.67	Collusive Malicious Member Initial Value $V_j(0): S_j(0)$	9:20

The actual environment is always unstable, in which MBP changes aperiodically and RV always locates in the transition phase from the initial to stable reputation values. A series of interactions among members are simulated in CI before the experiment starts to make all member RVs transient. Because we assume in the environment MBP don't change as the interaction happens, we keep all the members staying in the transition phase by controlling the number of interactions before the experiment.

In the environment, both independent and collusive malicious members have to be identified. Both of them have low TRV and the only difference is that collusive malicious members have high bogus global reputation values but independent malicious member do not. Two types of reputation, global reputation and local reputation are calculated as input values of committee based fuzzy decision-making method. Detailed experiment configurations are described in Table 2.

4.2.3 *PE* and *NE* of Verification

The global reputation of independent malicious members decreases with interactions while collusive malicious members may cheat for high global reputation. But local reputation values assigned to both types of malicious members by representatives decrease to reflect actual behavior patterns if malicious members interact with representatives. Our fuzzy comprehensive decision-making can aggregate the two kinds of information from all representatives in a committee and make a decision according to membership vectors and weight vector automatically. In the experiment, the committee verifies all the members in CI and classifies them into three types: reliable, unreliable and indeterminate. We hope the committee can classify the member to the corresponding sets: actual malicious members into unreliable class, the members with high TRV into reliable class and the members between the two into indeterminate class which need to be further verified.

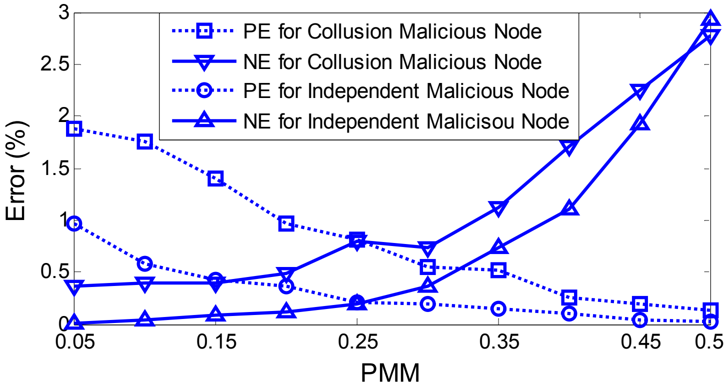

Figure 7. Performance Evaluation – *NE*/*PE* over *PMM*

Figure 7 shows the *PE* and *NE* curves over different *PIMM* and *PCMM*. From that figure, it is obvious that the committee can verify most of malicious members and reliable members, for *PE* is no more than 0.02 while *NE* is lower than 0.03. Collusive malicious members may have high global reputation by giving high feedbacks with each other. This high bogus global reputation may cheat the committee to approve actual malicious members. In this case, local reputation representatives assigned on the given member should be considered. The final decision is based on the weighted average of global reputation and local reputation. As illustrated in Figure 7, it is more difficult to identify collusive malicious members from reliable members than independent malicious members, which makes higher *PE* and *NE* values. But *PE* and *NE* for collusive malicious behaviors are still low enough. No matter how strict the verification is, we can never ensure that all malicious members are identified and rejected when applicants reach the VO committee. So performance of periodical reviews is also of importance.

4.2.4 *PE* and *NE* of Reviews

This experiment is carried out based on a VO environment consists of three types of members: reliable members, independent and collusive malicious members. Every review selects some members that are regarded as malicious ones, which may contains both actual malicious members and reliable members. *PE* and *NE* values after 10 rounds of reviews are calculated respectively to evaluate its performance. Since most of independent malicious members are rejected during verification and are much easier to be identified than collusive malicious members, we only consider review performance of identifying collusive malicious members from reliable ones in the VO. In this experiment, reviews occur once every 50 interactions.

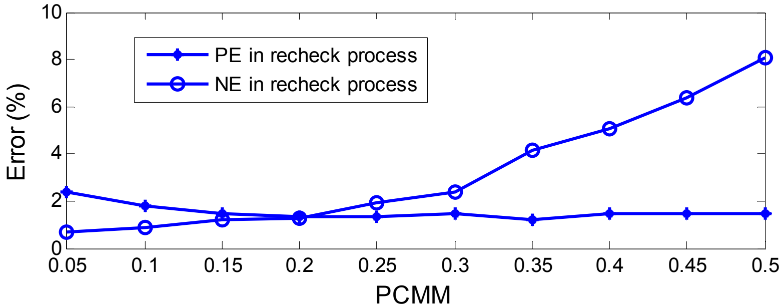

Figure 8. Performance Evaluation – *NE/PE* over *PCMM*

Figure 8 shows curves of *PE* and *NE* over different number of collusive malicious members. It is obvious that *PE* is stably limited to a very low level, which means most of collusive malicious members can be identified from reliable members, no matter how many collusive malicious members there are. *NE* increases with the number of collusive malicious members. That is because the malicious may bring failed interactions with reliable members, which decreases global reputation values of both sides and disorders other VO regular interactions. However, the number of reliable members regarded as malicious members is 1.93% at most if the number of malicious members is no more than 50.

In this section, we evaluate performance of committee based verification and reviews. Two performance metrics, *PE* and *NE*, are proposed to evaluate accuracy and effectiveness of the two processes. From simulation and analysis results, it can be concluded that both processes can identify the two types of malicious members from reliable members with very low *PE* and *NE* values. Collusive malicious members are more difficult to be identified compared with independent ones. Considering the behavior pattern changes after a member joins in a VO, we need reviews to trace member behavior patterns periodically and remove malicious ones in real time. Verification ensures only small number of malicious members have probability to cheat in the VO while reviews are essential to maintain the VO trust level. Simulation results show that the combination of verification and reviews ensure that only reliable members can be the VO member at any time.

4.2.5 *PE* and *NE* of Different Committees

The number of representatives in a committee has significant impact on the classification performance. Intuitively, more representatives are in the committee, more accurate the verification of the committee is, since more knowledge about an application is collected by the committee from representatives. It is quite similar with that in practical world. In this section, we test the effectiveness of the representatives through a simulated experiment.

In the experiment, the CI and VO environment configurations are listed in Table 2, assuming 200 VO candidates requiring to be verified. We assume there are 50 collusive malicious members in these 200 candidates. Verification performances of different scales of committees are shown in Figure 9.

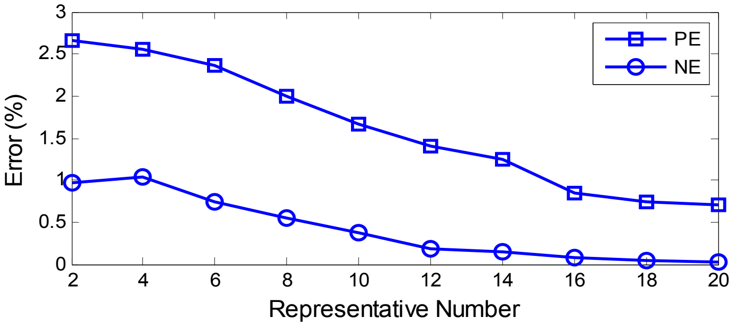

Figure 9. *PE* and *NE* of Different Number of Representatives

As show in Figure 9, verification errors, *PE* and *NE* decrease as the representative number increases. That is to say that expanding the scale of the committee in a VO can enhance the verification accuracy for a new applicant. And a new representative joining into the committee always has an obvious positive effectiveness for the CAVM performance. It is an expandable way to enhance the verification accuracy if the VO administrator or other members have high secure requirements.

But it does not mean that we can expand the committee without any limitation to continuously enhance the verification accuracy. Two reasons impede the extension. The first one is that it is infeasible to select large number of trustable and experienced nodes from CI as representatives, for the knowledge of the VO administrator is limited. Generally, only a few numbers of members are trusted by the VO administrator and empowered as representatives to verify a new applicant. Another reason is that expanding the scale of the committee will increase the complexity of the verification process. If *PE* and *NE* are lowered to an acceptable scope, it is unnecessary and inefficient to increase the number of representatives in the committee.

5. Conclusions

In this paper, we propose a VO Membership Evaluation System, consisting of a layered reputation system and a committee based fuzzy comprehensive decision-making method, to help Users and RPs establish a VO with insurance of trustiness and robustness. Simulation experiments are carried out to analyze and evaluate the proposed VOMES using different aspects of performance metrics. The contributions of VOMS are summarized as follows.

- A layered reputation system. There is no existing work addressing reputation and trust issues in CI currently. Our reputation system can rapidly, stably and accurately reflects actual behavior patterns of VO members and provides significant differential degrees to classify different behavior patterns.

- Committee based fuzzy decision-making. A committee based decision-making method is proposed in our work. Experienced representatives in the committee represent various requests of the whole VO to verify new applicants and review memberships periodically. This mechanism obviously reduces malicious behaviors and maintains the VO trust level automatically. Besides that, VO administrator can simply enhance the accuracy of the verification through extending the committee scale, namely empower new member as the representative to join in the decision-making process.
- Membership reviews. Because the committee based fuzzy decision-making method is carried out automatically, it is possible to review the memberships in a VO periodically. It can maintain the VO trust level in real time and obviously identify malicious behaviors.

The above components and method makes VOMES stably and accurately verify new applicant, defeat potential independent and collusive malicious behavior and expansive to enhance its performance. Currently, performance of VOMES is analyzed and evaluated in a simulation environment. Future works include deployment of VOMES in real-world grid and CI environments so that performance of VOMES can be further improved.

Acknowledgement

This work is supported by National Science Foundation of China (grant No. 60803017) and Ministry of Science and Technology of China under National 973 Basic Research Program (grants No. 2011CB302505 and No. 2011CB302805).

References

[1] D. E. Atkins et al. Revolutionizing Science and Engineering through Cyberinfrastructure, National Science Foundation Blue – Ribbon Advisory Panel on Cyberinfrastructure, January 2003.

[2] Open Science Grid (OSG), http://www.opensciencegrid.org.

[3] Enabling Grids for E-science (EGEE), http://www.eu-egee.org/.

[4] TeraGrid, http://www.teragrid.org/.

[5] NSF Cyberinfrastructure Council, NSF's Cyberinfrastructure Vision for 21st Century Discovery, Version 7.1., National Science Foundation, July 2006.

[6] G. Fox, E-science Meets Computational Science and Information Technology, Computing in Science & Engineering, July-Aug, 2002.

[7] T. Znati, Challenges and Future Research Directions in Large-Scale Complex Systems, Proceedings of 28th International Conference on Distributed Computing Systems, pp.17-20, June. 2008.

[8] C. P. Holland, Business Trust and the Formation of Virtual Organizations, Proceedings of 31st Hawaii International Conference on System Sciences, pp.602-610, Jan. 1998.

[9] S. Y. Pu, M. K. O. Lee, L. S. Yi, Virtual Organizations: the Key Dimensions, Proceedings of Academia/Industry Working Conference on Research Challenges, pp.27-29, April. 2000.

[10] I. Foster, C. Kesselman, The Grid: Blueprint for a New Computing Infrastructure, Morgan Kaufmann, San Francisco, 1998.

[11] R. Buyya, D. Abramson, J. Giddy, Nimrod/G: an Architecture for a Resource Management and Scheduling System in a Global Computational Grid, Proceedings of 4th International Conference/Exhibition on High Performance Computing, pp.283-289, May. 2000.

[12] VOMS Monitoring Documentation, http://voms-monitor.grid.iu.edu/cgi-bin/index.cgi.

[13] GUMS, https://www.racf.bnl.gov/Facility/GUMS/1.2/index.html.

[14] OSG VO Registration Policy and Procedure, OSG DocDB Document 737v2, http://www.opensciencegrid.org, April 14, 2008.

[15] G. J. Klir, U. St. Clair, B. Yuan, Fuzzy Set Theory: Foundations and Applications, Prentice Hall, 1997.

[16] S. Song, K. Hwang, R. Zhou, Y.-K. Kwok, Trusted P2P Transactions with Fuzzy Reputation Aggregation, IEEE Internet Computing, Nov.-Dec. 2005.

[17] L. A. Zadeh, Fuzzy Logic, Neural Networks and Soft Computing, ACM Communications, Vol. 37, No. 3, pp.77–84, 1994.

[18] H. Yano, An Interactive Fuzzy Decision Making Method for Decentralized Multiobjective Programming Problems, IFSA World Congress and 20th NAFIPS International Conference, pp.98-103, 2001.

[19] G. Zacharia, A. Moukas, P. Maes, L ab. Media, Collaborative Reputation Mechanisms in Electronic Marketplaces, Proceedings of 32nd Annual Hawaii International Conference on System Sciences, pp.7, 1999.

[20] W. Yan, L. Kwei-Jay, Reputation-Oriented Trustworthy Computing in E-Commerce Environments, IEEE Internet Computing, pp.55-59, 2008.

[21] C. Dellarocas, Analyzing the Economic Efficiency of eBay-like Online Reputation Reporting Mechanisms, Proceedings of 3rd ACM Conference on E-Commerce, 2001.

[22] P. Resnick, R. Zeckhauser, Trust among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System, The Economics of the Internet and E-Commerce, 2002.

[23] Q. Li, Z. Liu, Research on Chinese C2C E-Business Institutional Trust Mechanism: Case Study on Taobao and Ebay, International Conference on Wireless Communications, Networking and Mobile Computing, pp.3787-3790, 2007.

[24] K. Aberer, Z. Despotovic, Managing Trust in a Peer-2-Peer Information System, Proceedings of 10th International Conference on Information and Knowledge Management, 2001.

[25] R. Zhou, K. Hwang, PowerTrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing, IEEE Transactions on Parallel and Distributed Systems, 2007.

[26] R. Zhou, K. Hwang, M. Cai, GossipTrust for Fast Reputation Aggregation in Peer-to-Peer Networks, IEEE Transactions on Knowledge and Data Engineering, 2008.

[27] R. Zhou, K. Hwang, Gossip-based Reputation Aggregation for Unstructured Peer-to-Peer Networks, Proceedings IEEE International Symposium of Parallel and Distributed Processing, pp.1-10, 2007.

[28] S. D. Kamvar, M. T. Schlosser, H. Garcia-Molina, The Eigentrust Algorithm for Reputation Management in P2P Networks, Proceedings of 12th International Conference on World Wide Web, 2003.

[29] Grid Toolkits Project, http://www.globus.org.

[30] E. Cody, et. al., Security in Grid Computing: A Review and Synthesis, Decision Support Systems, pp.749-764, 2008.

[31] D. Venkaiah, P. Jalote, An Integer Programming Approach for Assigning Votes in a Distributed System, Proceedings of 14th Symposium on Reliable Distributed Systems, pp. 128-134, 1995.

[32] S. Yacoub, X. Lin, S. Simske, J. Burns, Automating the Analysis of Voting Systems, Proceedings of 14th International Symposium on Software Reliability Engineering, pp. 203-214, 2003.

[33] H. G. Shakouri, M. B. Menhaj, A Systematic Fuzzy Decision-Making Process to Choose the Best Model Among a Set of Competing Models, IEEE Transaction on Systems, Man and Cybernetics Part A, pp.1118-1128, Sept.2008.

[34] H. Chen, Z. Ye, Research of P2P Trust based on Fuzzy Decision-making, Proceedings of 12th International Conference on Computer Supported Cooperative Work in Design, pp.793-796, 2008.

[35] N. Baldo, M. Zorz, Cognitive Network Access Using Fuzzy Decision Making, IEEE International Conference on Communications, pp.6504-6510, 2007.