Research Article

Modeling Dynamic Trust and Risk Evaluation Based on High-Order Moments

Yan Gao,^{1,2} Zhiyong Dai,^{1,2} and Wenfen Liu^{1,2}

¹ Zhengzhou Information Science and Technology Institute, Zhengzhou 450001, China

² State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China

Correspondence should be addressed to Yan Gao; gaoyan_yangao@163.com

Received 16 April 2014; Revised 5 August 2014; Accepted 14 August 2014

Academic Editor: Alessandro Palmeri

Copyright © 2015 Yan Gao et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This paper proposes a dynamic trust and risk evaluation model based on high-order moments. The credibility of an entity is measured with trust degree and risk value comprehensively. Firstly, considering the dynamic and time decay characters of trust, a time attenuation function is defined, and direct trust is further expressed. Subsequently, in order to improve the accuracy of feedback trust, a filter mechanism is constructed to eliminate the false feedback, combining coefficient of skewness with hypothesis test. More importantly, the weights of direct trust and feedback trust are derived subjectively and adaptively with the moments and frequency of direct interactions. Furthermore, risk is evaluated with direct risk and feedback risk, which are obtained by mainly using coefficient of variation and coefficient of kurtosis. Risk value can be used to measure the stability of providing services. Simulation results show that the proposed model not only has high accuracy, but also resists effectively collusive attacks and strategic malicious behaviors.

1. Introduction

With the rapid development of network technology, peer-to-peer networks have been widely applied in a variety of distributed application systems, such as P2P file sharing, electronic commerce [1], and cloud computing, which make Internet applications simpler and more efficient. However, to guarantee the security and credibility of these network application environments is very difficult due to the openness, anonymity, and high dynamic. Therefore, there are very serious technical challenges to provide the safe and reliable services. Trust management has become a kind of effective technology of “soft security” in solving the existing network security issues related to trust [2].

In recent years, trust relationships under different application conditions have been analyzed [3], and many scholars have established trust models to study dynamical trust relationship with different mathematical methods and tools [4], which typically have EigenTrust [5], PeerTrust [6], PowerTrust [7], GossipTrust [8], and so on.

At present, the weighted average method is used to quantify trust in most of the literatures. Li et al. [9] presented

trust management in large-scale P2P networks, where direct trust and feedback trust were computed considering time decay and distance attenuation, respectively, and the corresponding weights can be adjusted adaptively. On this basis, [10] analyzed five factors related to trust relationship, history, availability, feedback, motivation, and risk, and constructed a trust model based on the idea of multisource information fusion, in which their weights were assigned by WMA-OWA algorithms. Xue et al. [11] put forward a robust reputation system for structured P2P networks; the reputation managers were only responsible for local information, rather than global reputation, which can resist effectively collusion attack. In addition, by distinguishing the abilities of providing service and recommending, it makes trust quantification more accurate and reliable.

Except for the weighted average method, trust models are presented using probability and statistical methods. Wang et al. [12] proposed a robust linear Markov (RLM) reputation model with Kalman aggregation method through prediction variance, which is against malicious attacks by using EM algorithm to calibrate the dynamic parameters autonomously. Ayday and Fekri [13] attribute the reputation

management problem to an inference problem of calculating the marginal distribution and present a centralized iterative method using the factor graph and belief propagation. Considering that trust is a dynamic process related to the context, Liu and Datta [14] established a context aware trust model using hidden Markov chain, in which the interaction results are the states of the Markov chain and the characteristics of context information are viewed as the observation sequence. The experiment shows that this model has lower positive false and negative false rates.

Although much new progress has been made in the existing researches, there are still some problems, which mainly are reflected in the following respects. First, dynamic is the biggest challenge in the evaluation and forecasting of trust relationship, due to the fact that trust relationship changes dynamically over time and has the time attenuation character in which interaction information further from current time has the weaker influence to trust relationship. Therefore, how to depict the time decay precisely and improve the accuracy and dynamic adaptation is a very difficult job. Secondly, false feedback filter is prerequisite to guarantee the correctness of feedback trust. At present, attacks against trust systems emerge endlessly in [15, 16]; malicious entities may provide false interaction information about a target entity to the requestor. The existing models only identify and defend simple attacks and fraud but lack protection mechanisms against complex attacks such as collusion, spying, and strategic attacks, which leads to the poor security and robustness. Further, in constructing quantitative models with weighted average methods, it is key to set the corresponding weight of direct trust and feedback trust. The existing setting methods are with strong subjectivity, less flexibility, and difficulty in being adjusted dynamically, which leads to lack adaptability and affect the trust decision ultimately. Lastly, risk evaluation is viewed as an objective preference to trust computation. The researches on trust at present often ignore the impact of risk, which makes trust computation not fully reflect the credibility of the entity behavior.

According to the above problems, this paper models behavior trust and risk evaluation using high-order moments. First of all, a time attenuation function is defined to characterize dynamic and time decay of trust more flexibly. Based on this, the direct trust is computed combined with the moments and frequency of direct interactions between entities. Subsequently, before calculating feedback trust, feedback interaction information is filtered through establishing a statistical model with standard coefficient of skewness and hypothesis testing, eliminating the false feedback. Then the feedback trust is calculated with the time attenuation function. Next, according to the basic principles, considering the number and moments of direct interactions, we give a weight setting method which is adaptive and dynamically adjusted as the interaction continues. On this basis, in order to fully study its ability to provide service, the stability of target entity behavior is measured by analyzing the discrete and sharp degree with coefficient of variation and standard coefficient of kurtosis of two samples: direct interactions and real feedback information. Further, risk evaluation model is given with the weighted average method. To measure

the ability of the target entity, the values of trust and risk evaluation are both taken into account so as to make a trust decision.

The remainder of this paper is organized as follows. Section 2 presents a trust quantitative model through computing direct trust, feedback trust, and their own weight, respectively. A risk evaluation model is established in Section 3 by measuring direct risk and feedback risk comprehensively. Section 4 discusses the accuracy, dynamic, and robustness of the proposed model under several attacks and compares it with related work in simulation experiments. Finally, the summary analysis carries on.

2. A Quantitative Model for Trust

This section mainly gives the computational expressions of direct trust and feedback trust, and then total trust is ultimately quantified with the weighted average method. Set entity i and j as any service requester and service provider, respectively. Denote $T_{i,j}(t)$ to be the total trust of entity i for j at the moment t ; then it can be calculated as follows:

$$T_{i,j}(t) = \omega_1 \times DT_{i,j}(t) + \omega_2 \times FT_{i,j}(t), \quad (1)$$

where $DT_{i,j}(t)$ represents the direct trust computed with the direct interactions between the two entities and $FT_{i,j}(t)$ is the feedback trust obtained through the interactions between other entities and entity j . $\omega_1, \omega_2 \in [0, 1]$ is the weight of $DT_{i,j}(t)$ and $FT_{i,j}(t)$, respectively, and $\omega_1 + \omega_2 = 1$. The following are the computation methods of $DT_{i,j}(t)$, $FT_{i,j}(t)$, and ω_1 . For the sake of simplicity, every (t) in (1) is omitted hereinafter.

As we know, trust has the characteristics of time decay; that is, the interactions results farther from the current time have the weaker influence on the current trust value. Consequently, those interactions only in a certain period close to the current time are necessary to be analyzed so as to obtain the current trust degree. Given Δt ($0 < \Delta t \leq t$) and $l, l^* = \lfloor t/\Delta t \rfloor$, the time range in which these interactions are considered is specified as

$$[u\Delta t, t) = [l^*\Delta t, t) \bigcup \sum_{h=u}^{l^*-1} [h\Delta t, (h+1)\Delta t), \quad (2)$$

where $u = \max\{l^* - l, 0\}$. For convenience, set

$$\Delta t_h = \begin{cases} h\Delta t, & u \leq h \leq l^* \\ t, & h = l^* + 1, \end{cases} \quad (3)$$

and $\Lambda_h = [\Delta t_h, \Delta t_{h+1})$, $u \leq h \leq l^*$.

2.1. Direct Trust Computing. For any $u \leq h \leq l^*$, assume that there were N_h interactions in the interval Λ_h between entity i and j , denoted by

$$\Omega_{i,j}^h = \{r_{d,h}^1, r_{d,h}^2, \dots, r_{d,h}^{N_h}\}, \quad (4)$$

where $r_{d,h}^c \in [0, 1]$ is the satisfaction degree of entity i at the c th interaction, $1 \leq c \leq N_h$. Then

$$DT_{i,j}^h = \frac{1}{|\Omega_{i,j}^h|} \sum_{c=1}^{N_h} r_{d,h}^c. \quad (5)$$

Based on (5), $DT_{i,j}$ can be represented as $DT_{i,j} = f(DT_{i,j}^u, \dots, DT_{i,j}^{l^*})$, where $f(\cdot)$ is a function with $l^* - u + 1$ variables. Accordingly, the key is to determine $f(\cdot)$ in order to obtain $DT_{i,j}$. Considering the dynamic and time decay of trust, a time attenuation function is first introduced before $f(\cdot)$ is given.

Definition 1 (time attenuation function). Consider

$$\alpha_\delta(t^*) = \frac{1}{2} + \frac{1}{\sqrt[3]{e^{t-t^*} + 1}}, \quad 0 \leq t^* < t, \quad (6)$$

where the parameter $\delta > 0$ is used to adjust the attenuation speed.

Through analysis, it is known that $1/2 < \alpha_\delta(t^*) \leq 1$ and $\alpha_\delta(t^*)$ is a strictly monotonously increasing function of t^* . The function α_δ is specified in Figure 1.

From Figure 1, the rates of descending differ with different δ . As a result, the relative influence of interactions in each interval Λ_h is distinguished. Additionally, the selection that $\alpha_\delta(t^*) > 0.5$ is adopted mainly for the purpose of meeting the requirements of weight setting presented in Section 2.3.

Combining the direct interactions $\{D_{i,j}^h, u \leq h \leq l^*\}$ with time attenuation function (6), the computation expression for direct trust $DT_{i,j}$ is as follows.

Definition 2 (direct trust $DT_{i,j}$). For any $u \leq h \leq l^*$, define $f(\Lambda_h, DT_{i,j}^h) = (\alpha_\delta(\Delta t_{h+1}) \cdot DT_{i,j}^h) / (\sum_{h=u}^{l^*} \sqrt[3]{\alpha_\delta(\Delta t_{h+1})})$, $\rho > 1$, and then

$$DT_{i,j} = \sum_{h=u}^{l^*} f(\Lambda_h, DT_{i,j}^h) = \sum_{h=u}^{l^*} \frac{\alpha_\delta(\Delta t_{h+1}) \cdot DT_{i,j}^h}{\sum_{h=u}^{l^*} \sqrt[3]{\alpha_\delta(\Delta t_{h+1})}}. \quad (7)$$

Set $DT_{i,j}^h = 0.5$ if $\Omega_{i,j}^h = \phi$. For any $u \leq h \leq l^*$, due to $\alpha_\delta(\Delta t_{h+1}) < \sqrt[3]{\alpha_\delta(\Delta t_{h+1})}$ and $DT_{i,j}^h \in [0, 1]$, $0 \leq DT_{i,j} \leq 1$. Specially, if $\rho = 1$ in (7), it is similar to the expression for direct trust in [9]. It is worth mentioning that an entity is able to choose the appropriate parameter ρ according to its own situation, which more reflects the personalization character of trust.

2.2. Feedback Trust Computing. After entity i receives the interactions about j recommended from several entities, it is necessary to filter this information, eliminate the false interaction information, and retain the true ones, which is a precondition to correctly compute the feedback trust $FT_{i,j}$. The storage and distribution of interaction information, filter mechanism, and feedback trust are introduced in the following.

FIGURE 1: Time attenuation function α_δ .

2.2.1. Storage and Distribution of Feedback Information. This model adopts the storage and distribution means based on DHT for the interaction information of any entity. In order to more effectively resist malicious attacks, overlay network is used similar to DHTON presented in [11]; that is, all the interactions about j are stored in several managers and each manager is responsible only for storage and distribution of local interactions.

The Chord network is first described. In a Chord network, every entity is represented by a W -bit identifier and all entities are lined in the Chord circle in the clockwise direction. Set $\mathbb{C} = \{v : 0 \leq v < 2^W\}$ and denote $\mathbb{C}_{\text{exist}}$ by entity set in the Chord circle; then $\mathbb{C}_{\text{exist}} \subset \mathbb{C}$. We might set $\mathbb{C}_{\text{exist}} = \{v_1, v_2, \dots, v_{|\mathbb{C}_{\text{exist}}|}\}$, $0 \leq v_1 < v_2 < \dots < v_{|\mathbb{C}_{\text{exist}}|} < 2^W$. Hence, there exists z ($1 \leq z \leq |\mathbb{C}_{\text{exist}}|$) to make $j = v_z$ and $\mathbb{C}$ except that j is divided into W subsets:

$$\mathbb{C}_k = \{(j + 2^{k-1}) \pmod{2^W}, \dots, (j + 2^k - 1) \pmod{2^W}\}, \quad 1 \leq k \leq W. \quad (8)$$

For any $1 \leq k \leq W$, define

$$\mathbb{C}_{\text{exist}}^k = \mathbb{C}_{\text{exist}} \cap \mathbb{C}_k. \quad (9)$$

When $\mathbb{C}_{\text{exist}}^k \neq \phi$, the entity in the front in the clockwise direction is just the finger entity of $\mathbb{C}_{\text{exist}}^k$, which is responsible for the storage and distribution of interaction information between j and all the entities in $\mathbb{C}_{\text{exist}}^k$. Set $U = \{k : 1 \leq k \leq W, \mathbb{C}_{\text{exist}}^k \neq \phi\}$ and $\eta = (\eta_1, \eta_2, \dots, \eta_{|U|})$, $\eta_\tau \in U$, $\eta_1 < \eta_2 < \dots < \eta_{|U|}$, $1 \leq \tau \leq |U|$; then the set of all managers of entity j is $V_\Sigma = \{v_{z+1}, v_{z+1+\Sigma_1}, \dots, v_{z+1+\Sigma_{|U|-1}}\}$, where $\Sigma_m = \sum_{\tau=1}^m |\mathbb{C}_{\text{exist}}^{\eta_\tau}|$. Entity i needs to send requests to the entities in V_Σ to obtain the interaction information about j .

There is not distinction between direct trust and feedback trust in the algorithm of computing trust in [11] where

the direct interactions between i and j are not separated from all of the feedback information. However, considering that their own experience is often more inclined in the trust relationship, it is necessary to differentiate the two. For $1 \leq \tau \leq |U|$ and $\Sigma_0 = 0$, denote Ω^τ by the interaction information from the manager $v_{z+1+\Sigma_{\tau-1}}$; then the set of interactions used to compute feedback trust is $\Omega_F = \bigcup_{\tau=1}^{|U|} \Omega^\tau \setminus \Omega^i$, where Ω^i is the interactions between i and j .

2.2.2. False Feedback Filter. According to the time instant of each interaction, Ω_F is divided into $l^* - u + 1$ groups. For any $u \leq h \leq l^*$, denote

$$\Omega_F^h = \{r_{F,h}^1, r_{F,h}^2, \dots, r_{F,h}^{B_h}\}, \quad (10)$$

where B_h and $r_{F,h}^b$ are the number of feedback interactions and satisfaction degree at the b th interaction in the interval Λ_h , respectively, $1 \leq b \leq B_h$. Therefore, $\Omega_F = \bigcup_{h=u}^{l^*} \Omega_F^h$.

In each time interval Λ_h , if the ability of providing service of entity j is regarded as a random variable Y_h whose value range is $[0, 1]$, the feedback interactions Ω_F^h are just the samples. Assume the providing service ability of entity j is stable in each interval, and then the samples should approximately obey the normal distribution without the presence of attacks. If the attacks want to affect the computing result of trust degree on the whole, it is vital for malicious entities to return most false interactions to the requester. This false feedback is over high (collusive boost) or too low (collusive defaming), and its corresponding interaction moments should be close to the present moment. Through the above analysis, it can be judged that when there exists collusive defaming (boost) attack, the shape characteristics of the samples will be clearly to the left (right).

In order to filter the false feedback effectively, standard coefficient of skewness and hypothesis testing are used to analyze the feedback information. In statistics, coefficient of skewness is a measurement to reflect the skewness condition of sample distribution, including the degree and direction of skewness.

Definition 3 (standard coefficient of skewness [17]). Suppose $x_1, x_2, \dots, x_n$ are the samples from population X and $\bar{x} = (1/n) \sum_{l=1}^n x_l$ and $s^2 = (1/(n-1)) \sum_{l=1}^n (x_l - \bar{x})^2$ are the sample mean and variance, respectively; then

$$Sk = \sqrt{\frac{1}{6n}} \sum_{l=1}^n \left(\frac{x_l - \bar{x}}{s} \right)^3 \quad (11)$$

is the standard coefficient of skewness. $Sk = 0$ states that the sample distribution is symmetrical; $Sk > 0$ means that the distribution has a positive skewness; otherwise, the sample distribution has a negative skewness. The larger the absolute value of Sk , the higher the degree of skewness.

The false feedback filter method is given using Definition 3 and hypothesis testing in the following.

Based on Definition 3, the standard coefficient of skewness of the samples $\{r_{F,h}^b, 1 \leq b \leq B_h\}$ is computed as

$$Sk_h = \sqrt{\frac{1}{6B_h}} \sum_{b=1}^{B_h} \left(\frac{r_{F,h}^b - \bar{r}_{F,h}}{s_{F,h}} \right)^3, \quad (12)$$

where $\bar{r}_{F,h} = (1/B_h) \sum_{b=1}^{B_h} r_{F,h}^b$, $s_{F,h}^2 = (1/(B_h - 1)) \sum_{b=1}^{B_h} (r_{F,h}^b - \bar{r}_{F,h})^2$.

Set a threshold value $\Gamma_1 > 0$. After Sk_h is obtained by (12), if $|Sk_h| > \Gamma_1$, it can be judged that there is false feedback in the samples. Moreover, for any $1 \leq b \leq B_h$, we get the following.

Case 1. It is when $Sk_h < -\Gamma_1$, $r_{F,h}^b$ is regarded as false feedback and will be eliminated from Ω_F^h if and only if $r_{F,h}^b \in (0, \bar{r}_{F,h} - s_{F,h})$.

Case 2. When $Sk_h > \Gamma_1$, if $r_{F,h}^b \in (\bar{r}_{F,h} + s_{F,h}, 1)$, the feedback $r_{F,h}^b$ will be eliminated from Ω_F^h .

2.2.3. Feedback Trust. For any $u \leq h \leq l^*$, after the false data in each set Ω_F^h are eliminated, denote Ω_{HF}^h by all of the honest feedback, and then $\Omega_{HF}^h \subseteq \Omega_F^h$. The following is the computing expression for feedback trust.

Definition 4 (feedback trust $FT_{i,j}$). Using the real feedback interactions $\{\Omega_{HF}^h, u \leq h \leq l^*\}$ and time attenuation function (6), the computing expression for $FT_{i,j}$ is

$$FT_{i,j} = \frac{\sum_{h=u}^{l^*} \alpha_\delta(\Delta t_{h+1}) FT_{i,j}^h}{\sum_{h=u}^{l^*} \sqrt[\rho]{\alpha_\delta(\Delta t_{h+1})}}, \quad (13)$$

where $FT_{i,j}^h = (1/|\Omega_{HF}^h|) \sum_{r \in \Omega_{HF}^h} r$.

2.3. Weight Setting Method. To calculate the total trust with weighted average method, the weight setting needs to follow the following two principles at least:

- (i) the weight of direct trust should be not less than the weight of feedback trust; that is to say, $\omega_1 \geq 0.5$;
- (ii) lowering the weight ω_2 properly can reduce the negative impact of malicious feedback and improve the accuracy so as to obtain good performance [18].

Based on the above principles, a theorem is first proven before the computing method of the weights is derived.

Theorem 5. For any $u \leq h \leq l^*$, set $g(h) = \sum_{h=u}^{l^*} \alpha_\delta(\Delta t_{h+1}) / \sum_{h=u}^{l^*} \sqrt[\rho]{\alpha_\delta(\Delta t_{h+1})}$, $\rho > 1$; then $g(h)$ is a strictly monotonously increasing function of variable h and $0.5 < g(h) < 1$.

Proof. For any $u \leq h \leq l^*$, α_h is short for $\alpha_\delta(\Delta t_{h+1})$ for convenience.

For any $u \leq h \leq l^*$, $1/2 < \alpha_h < 1$, and $1/2 < \alpha_u < \dots < \alpha_{l^*} < 1$ from Definition 1,

$$g(h) = \frac{\sum_{h=u}^{l^*} \alpha_h}{\sum_{h=u}^{l^*} \sqrt[\rho]{\alpha_h}} > \frac{1}{l^* - u + 1} \sum_{h=u}^{l^*} \alpha_h > 0.5. \quad (14)$$

And, for any $\rho > 1$, $\alpha_h < \sqrt[\rho]{\alpha_h}$; hence,

$$g(h) = \frac{\sum_{h=u}^{l^*} \alpha_h}{\sum_{h=u}^{l^*} \sqrt[\rho]{\alpha_h}} < \frac{\sum_{h=u}^{l^*} \alpha_h}{\sum_{h=u}^{l^*} \alpha_h} = 1. \quad (15)$$

In addition, for any $u + 1 \leq h \leq l^*$,

$$\begin{aligned} gh - g(h-1) &= \frac{\sum_{k=u}^h \alpha_k}{\sum_{k=u}^h \sqrt[\rho]{\alpha_k}} - \frac{\sum_{k=u}^{h-1} \alpha_k}{\sum_{k=u}^{h-1} \sqrt[\rho]{\alpha_k}} \\ &= \frac{\sum_{k=u}^{h-1} \alpha_k + \alpha_h}{\sum_{k=u}^{h-1} \sqrt[\rho]{\alpha_k} + \sqrt[\rho]{\alpha_h}} - \frac{\sum_{k=u}^{h-1} \alpha_k}{\sum_{k=u}^{h-1} \sqrt[\rho]{\alpha_k}} \\ &= \frac{(\sum_{k=u}^{h-1} \alpha_k + \alpha_h) \times \sum_{k=u}^{h-1} \sqrt[\rho]{\alpha_k} - \sum_{k=u}^{h-1} \alpha_k (\sum_{k=u}^{h-1} \sqrt[\rho]{\alpha_k} + \sqrt[\rho]{\alpha_h})}{\sum_{k=u}^h \sqrt[\rho]{\alpha_k} \times \sum_{k=u}^{h-1} \sqrt[\rho]{\alpha_k}} \\ &= \frac{\alpha_h \times \sum_{k=u}^{h-1} \sqrt[\rho]{\alpha_k} - \sqrt[\rho]{\alpha_h} \times \sum_{k=u}^{h-1} \alpha_k}{\sum_{k=u}^h \sqrt[\rho]{\alpha_k} \times \sum_{k=u}^{h-1} \sqrt[\rho]{\alpha_k}} \\ &= \frac{\sqrt[\rho]{\alpha_h} \times (\sum_{k=u}^{h-1} \alpha_k^{1-1/\rho} \times \sqrt[\rho]{\alpha_k} - \sum_{k=u}^{h-1} \sqrt[\rho]{\alpha_k} \times \alpha_k^{1-1/\rho})}{\sum_{k=u}^h \sqrt[\rho]{\alpha_k} \times \sum_{k=u}^{h-1} \sqrt[\rho]{\alpha_k}} \\ &= \frac{\sqrt[\rho]{\alpha_h} \times (\sum_{k=u}^{h-1} \sqrt[\rho]{\alpha_k} \times (\alpha_k^{1-1/\rho} - \alpha_k^{1-1/\rho}))}{\sum_{k=u}^h \sqrt[\rho]{\alpha_k} \times \sum_{k=u}^{h-1} \sqrt[\rho]{\alpha_k}} > 0. \end{aligned} \quad (16)$$

For any $u \leq k \leq h-1$, $\alpha_h > \alpha_k$, that is, $\alpha_h^{1-1/\rho} - \alpha_k^{1-1/\rho} > 0$, $g(h) - g(h-1) > 0$. Therefore, $g(h)$ is a strictly monotonously increasing function of variable h . $\square$

Based on the principles of the weight setting, combining the conclusion of Theorem 5 with the moments and frequency of the direct interactions, the weights w_1 and w_2 are derived as follows:

$$w_1 = \frac{\sum_{h=u}^{l^*} \alpha_h (\Delta t_{h+1})}{\sum_{h=u}^{l^*} \sqrt[\rho]{\alpha_h} (\Delta t_{h+1})}, \quad w_2 = 1 - \frac{\sum_{h=u}^{l^*} \alpha_h (\Delta t_{h+1})}{\sum_{h=u}^{l^*} \sqrt[\rho]{\alpha_h} (\Delta t_{h+1})}. \quad (17)$$

From Theorem 5, $w_1 > 0.5$ and w_1 is significantly greater than 0.5 with the increase in the direct interactions; that is, w_2 is reduced as much as possible. Particularly, the weights can be updated as the interaction continues, and then they can be adjusted dynamically and adaptively.

To sum up, substituting (7), (13), and (17) into (1), we can obtain the total trust:

$$\begin{aligned} T_{i,j} &= w_1 \times DT_{i,j} + w_2 \times FT_{i,j} \\ &= \frac{\sum_{h=u}^{l^*} \alpha_h (\Delta t_{h+1})}{\sum_{h=u}^{l^*} \sqrt[\rho]{\alpha_h} (\Delta t_{h+1})} \times \sum_{h=u}^{l^*} \frac{\alpha_h (\Delta t_{h+1}) \cdot DT_{i,j}^h}{\sum_{h=u}^{l^*} \sqrt[\rho]{\alpha_h} (\Delta t_{h+1})} \\ &\quad + \left(1 - \frac{\sum_{h=u}^{l^*} \alpha_h (\Delta t_{h+1})}{\sum_{h=u}^{l^*} \sqrt[\rho]{\alpha_h} (\Delta t_{h+1})} \right) \times \frac{\sum_{h=u}^{l^*} \alpha_h (\Delta t_{h+1}) FT_{i,j}^h}{\sum_{h=u}^{l^*} \sqrt[\rho]{\alpha_h} (\Delta t_{h+1})}. \end{aligned} \quad (18)$$

3. Risk Evaluation Model

In the open and dynamical network environment, trust and risk are the important factors to make security decisions. Trust computing can provide guidance for safety decision-making and risk evaluation is an objective reference for trust computation [19]. The existing researches on trust often ignore the impact of risk, which makes trust computation not fully reflect the credibility of entity behavior.

In this paper, we use the stability of providing this service of entity j to represent the risk value. The higher the stability, the smaller the risk. The stability can be measured by analyzing the dispersion and sharpness of two samples: the direct interactions $\Omega_d = \{\Omega_{i,j}^h, u \leq h \leq l^*\}$ and honest feedback $\Omega_{HF} = \{\Omega_{HF}^h, u \leq h \leq l^*\}$. In statistics, the coefficient of variation and coefficient of kurtosis can indicate the two statistical characteristics. Therefore, the coefficient of variation and coefficient of kurtosis are used to establish a risk quantification model in the following and it is comprehensively measured with direct risk and feedback risk.

Definition 6 (coefficient of variance [17]). Set $C_v = s/\bar{x}$ as the coefficient of variance of $x_1, x_2, \dots, x_n$, where $\bar{x}$ and s are the same as given in Definition 3.

Although the coefficient of variance can measure the dispersion degree of the sample, two samples with the same coefficient of variance have different kurtosis in many cases. Therefore, the standard coefficient of kurtosis is further used to reflect the sharpness of the sampling distributions.

Definition 7 (standard coefficient of kurtosis [17]). Denote

$$\text{Kur} = \sqrt{\frac{n}{24}} \left(\frac{1}{n} \sum_{k=1}^n \left(\frac{x_k - \bar{x}}{s} \right)^4 - 3 \right) \quad (19)$$

to be the standard coefficient of kurtosis of the sample $x_1, x_2, \dots, x_n$, where $\bar{x}$ and s are the same as those in Definition 3. $\text{Kur} = 0$ shows that the sharpness degree of the sample distribution is equivalent to the normal distribution. $\text{Kur} > 0$ and $\text{Kur} < 0$ mean the sharpness degree of the sample distribution is higher and lower than the normal distribution, respectively.

Using Definitions 6 and 7, the coefficient of variance and standard coefficient of kurtosis of two samples Ω_d and Ω_{HF} are computed. The coefficients of variance of the two samples are

$$C_1 = s_D / \overline{DT}, \quad C_2 = s_H / \overline{FT^H}, \quad (20)$$

where

$$\begin{aligned} \overline{DT} &= \frac{1}{|\Omega_d|} \sum_{r \in \Omega_d} r, & s_D^2 &= \frac{1}{|\Omega_d|} \sum_{r \in \Omega_d} (r - \overline{DT})^2, \\ \overline{FT^H} &= \frac{1}{|\Omega_{HF}|} \sum_{r \in \Omega_{HF}} r, & s_H^2 &= \frac{1}{|\Omega_{HF}|} \sum_{r \in \Omega_{HF}} (r - \overline{FT^H})^2. \end{aligned} \quad (21)$$

And the standard coefficients of kurtosis of the two samples are

$$\begin{aligned} \text{Kur}_1 &= \sqrt{\frac{|\Omega_d|}{24}} \left(\frac{1}{|\Omega_d|} \sum_{r \in \Omega_d} \left(\frac{r - \overline{DT}}{s_D} \right)^4 - 3 \right), \\ \text{Kur}_2 &= \sqrt{\frac{|\Omega_{HF}|}{24}} \left(\frac{1}{|\Omega_{HF}|} \sum_{r \in \Omega_{HF}} \left(\frac{r - \overline{FT^H}}{s_H} \right)^4 - 3 \right). \end{aligned} \quad (22)$$

The larger the coefficient of variation, the higher the dispersion degree of a sample, which shows that the ability of providing service is more unstable. The larger the standard coefficient of kurtosis, the higher the concentration degree, which shows that the ability of providing service is more stable. Therefore, the larger the coefficient of variance, the lower the coefficient of kurtosis, and the risk of selecting j as a target entity to provide service is higher.

The two coefficients of kurtosis Kur_l ($l = 1, 2$) range in $(-\infty, +\infty)$. Because the risk value is a monotonously decreasing function of the coefficient of kurtosis, the relationship between the two can be calculated as follows:

$$\Theta(\text{Kur}_l) = 1 - \frac{1}{\pi} \left[\arctan(\text{Kur}_l) + \frac{\pi}{2} \right]. \quad (23)$$

From the properties of $\arctan x$, $\Theta(\text{Kur}_l) \in [0, 1]$ and, when $\text{Kur}_l = 0$, $\Theta(\text{Kur}_l) = 0.5$.

For the two coefficients of variance C_l ($l = 1, 2$), the risk value is a monotonously increasing function about the coefficient of variance:

$$\Psi(C_l) = 1 - e^{-C_l}. \quad (24)$$

From (24), $\Psi(C_l) \in [0, 1]$.

Based on the above analysis, the direct risk Rk_D and feedback risk Rk_F are computed, respectively, by

$$\begin{aligned} \text{Rk}_D &= \frac{1}{2} [\Theta(\text{Kur}_1) + \Psi(C_1)], \\ \text{Rk}_F &= \frac{1}{2} [\Theta(\text{Kur}_2) + \Psi(C_2)]. \end{aligned} \quad (25)$$

To sum up the risk value is given using (25):

$$\begin{aligned} \text{Rk}_{i,j} &= \omega_1 \text{Rk}_D + (1 - \omega_1) \text{Rk}_F \\ &= \frac{\omega_1}{2} \cdot [\Theta(\text{Kur}_1) + \Psi(C_1)] \\ &\quad + \left(\frac{1}{2} - \frac{\omega_1}{2} \right) \cdot [\Theta(\text{Kur}_2) + \Psi(C_2)]. \end{aligned} \quad (26)$$

Substituting (17), (23), and (24) into (26), the risk value $\text{Rk}_{i,j}$ is obtained.

In conclusion, the credibility of entity j is measured with a two-dimensional vector $(T_{i,j}, \text{Rk}_{i,j})$.

4. Simulation and Performance Analysis

We make the simulation to analyze the performance of the proposed model based on Peersim, a popular simulator of the P2P network. In the network, there are 2000 entities and 10000 kinds of services, in which 8000 are normal, 1000 are fake, and the remainders are vicious. We first use the RMS error to measure the accuracy of the proposed model. Subsequently, the dynamic is verified as the behavior of an entity changes over time. Furthermore, the percentage of successful interactions and the pass ratio of malicious services are adopted to analyze the performance of resisting the collusive attack and strategic malicious attacks.

4.1. Evaluation of Accuracy. We verify the accuracy through computing the root-mean-square (RMS) of the aggregated total trust of all entities [11]. The RMS error can be used to evaluate the effectiveness of the proposed model against various malicious behaviors. The smaller the RMS error, the higher the accuracy. The RMS error is given as follows:

$$\text{RMS error} = \sqrt{\frac{\sum_{k=1}^{N_e} ((T'_k - T_k) / T'_k)^2}{N_e}}, \quad (27)$$

where N_e is the total number of entities and T_k and T'_k are the evaluated and actual total trust of entity k , respectively.

It can be observed that the RMS error of our model is lower than the DHTrust and PowerTrust in Figure 2. This result emerges mainly due to three aspects. One is that we distinguish the direct trust and feedback trust and their weights in the proposed model are flexible and personalized. Another important point is the filtering mechanism proposed in Section 2.2.2, which eliminates the fake feedback so as to guarantee the correctness of the available feedback interactions. Moreover, different from only considering the trust degree, the trust and risk values are used comprehensively to reduce the RMS error.

4.2. Evaluation of Dynamic. The experiment is conducted to verify the dynamic of the proposed model. Assume that the behavior of an entity changes as time evolves. It can provide good services in the first 5 time intervals. Subsequently, it becomes unstable and provides honest services with probabilities of 0.9 and 0.8 from the 6th to 10th time interval and

FIGURE 2: RMS errors with different percentages of malicious entities.

FIGURE 3: The trust degree of a dynamical entity.

from 11th to 15th time interval, respectively. Next, it returns the good state. Trust degree of the entity changes as specified in Figure 3.

When the entity changes from good to bad, trust degree descends quickly and, after 2 time intervals, the evaluated trust degree can reflect the real situation. However, trust degree grows slowly if it varies from bad to good and it takes almost 5 intervals to reach the real value. This phenomenon shows that it is necessary to take a long time to accumulate trust degree and it can be viewed as the punishment for the unstable behaviours before.

4.3. Analysis of Collusive Attacks. In the existing attack models, collusive attack is generally considered as the biggest threat aiming at the trust systems. This attack model mainly includes full collusion and spies. In the “full collusion” model, all entities of a malicious collective provide bogus services

and create false positive feedback recommendation to all the other entities of the collectives. In the model “spies,” the malicious collective is divided into two groups: spies and malicious. The spies provide honest services to obtain a high reputation and simultaneously give false positive feedback to the malicious part of the collective. In order to analyze the performance of the proposed model to resist the collusive attack, two measurement indexes are first given as follows.

Definition 8. Set $MR(n)$ as the service request times of malicious entities and $PC(n)$ the pass count among these malicious requests in the n th simulation cycle; the pass ratio of malicious service is defined as $PR(n) = PC(n)/MR(n)$. It represents the ability to identify such malicious entities.

Definition 9. Set $TI(n)$ as the total number of interactions and $SI(n)$ the successful interactions in the n th simulation cycle; the ratio of successful interactions is $SR(n) = TI(n)/SI(n)$.

To measure the effect of collusive malicious entities, it is assumed that the percentages of malicious ones are 10% and 20%, respectively, half of which are spies. In this simulation experiment, 300 cycles are conducted and there are several services in every cycle. The comparisons of the proposed model with DHTrust and EigenTrust are detailed in Figures 4 and 5.

The left parts of Figures 4 and 5 represent the $PR(n)$ and $SR(n)$ corresponding to the three trust models when the percentage of malicious entities is 10%, and the $PR(n)$ and $SR(n)$ are reflected in the right parts when the percentage is 20%. From the above graphs, the $PR(n)$ s and $SR(n)$ s of the proposed model are distinctly lower and higher than DHTrust and EigenTrust, respectively. In the proposed model, $PR(n)$ is almost less than 0.1 until $n > 250$ and it tends to 0.05 as the interactions continue. Accordingly, $SR(n)$ floats around 0.95. A similar situation exists when the percentage is 20%. Such a result is obtained mainly due to the filtering mechanism in the proposed model. Because the filtering method is based on the statistics characteristics of several feedback entities, it is very effective to identify the malicious entities so as to resist the collusive attacks. And the experiment results precisely illustrate this point.

4.4. Analysis of Strategic Malicious Behaviors. The performance of the proposed model when strategic malicious entities exist in the network is analyzed in this subsection. Such malicious entities can be divided into two kinds in general. One kind is to promote trust degree with small deals and provide the fake services or malicious attacks for the big deals. The other is to provide the normal service when its credibility is low and give the fake services or malicious attacks after trust is improved.

In this experiment, we assume that the percentages of strategic malicious entities are 10%, 20%, and 30% and each half of such entities takes the two strategies, respectively.

The curves in Figure 6 show the changes of $SR(n)$ when the percentages are 10%, 20%, and 30% in order, respectively.

FIGURE 4: Pass ratio of malicious services.

FIGURE 5: The ratio of successful services.

It can be found that $SR(n)$ becomes greater than 0.95 after a few cycles and the asymptotic values do not have much difference as the interactions continue. This result reflects that the correctness of the proposed model is very high even in the presence of strategic malicious entities.

5. Conclusions

In this paper, a dynamic trust and risk quantitative model is established. The credibility of an entity is measured by two indicators: total trust and risk value. Total trust is obtained

FIGURE 6: The ratio of successful services.

with the weighted average method through considering direct interactions and feedback information comprehensively. In order to ensure the accuracy, a feedback filter model about feedback information based on coefficient of skewness and hypothesis test is proposed. Additionally, the weights allocation mechanism is adaptive. Furthermore, risk value is used to describe the stability of providing services, which is modeled with coefficient of variation and coefficient of kurtosis. Through simulation experiments, it is verified that the proposed model makes significant improvement in accuracy and dynamic and then it is robust to collusive malicious attacks and strategic malicious attacks.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The authors would like to express their sincere appreciation to the anonymous reviewers for their insightful comments, which have greatly aided them in improving the quality of the paper. This work is supported by the National Basic Research Program of China (973 Program) (nos. 2012CB315905 and 2012CB315901).

References

- [1] L. Chang, Y. Ouzrout, A. Nongillard, A. Bouras, and Z. Jiliu, "The reputation evaluation based on optimized Hidden Markov model in E-commerce," *Mathematical Problems in Engineering*, vol. 2013, Article ID 391720, 11 pages, 2013.
- [2] R. Falcone and J. Kim, "Soft security: isolating unreliable agents from society," in *Proceedings of the International Workshop on Trust, Reputation and Security: Theories and Practice (AAMAS '02)*, R. Falcone, S. Barber, L. Korba, and M. Singh, Eds., Lecture Notes in Computer Science, pp. 224–233, Springer, 2003.
- [3] L. Liu and W. Shi, "Trust and reputation management," *IEEE Internet Computing*, vol. 14, no. 5, pp. 10–13, 2010.
- [4] F. Mármol and G. Pérez, "Trust and reputation models comparison," *Internet Research*, vol. 21, no. 2, pp. 138–153, 2011.
- [5] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The EigenTrust algorithm for reputation management in P2P networks," in *Proceedings of the 12th International Conference on World Wide Web (WWW '03)*, pp. 640–651, May 2003.
- [6] L. Xiong and L. Liu, "PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities," *IEEE Transactions on Knowledge and Data Engineering*, vol. 16, no. 7, pp. 843–857, 2004.
- [7] R. Zhou and K. Hwang, "PowerTrust: a robust and scalable reputation system for trusted peer-to-peer computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 18, no. 4, pp. 460–473, 2007.
- [8] R. Zhou, K. Hwang, and M. Cai, "GossipTrust for fast reputation aggregation in peer-to-peer networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 20, no. 9, pp. 1282–1295, 2008.
- [9] X. Li, F. Zhou, and X. Yang, "Scalable feedback aggregating (SFA) overlay for large-scale P2P trust management," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 10, pp. 1944–1957, 2012.
- [10] X. Li, F. Zhou, and X. Yang, "A multi-dimensional trust evaluation model for large-scale P2P computing," *Journal of Parallel and Distributed Computing*, vol. 71, no. 6, pp. 837–847, 2011.
- [11] W. Xue, Y. Liu, K. Li, Z. Chi, G. Min, and W. Qu, "DHTrust: a robust and distributed reputation system for trusted peer-to-peer networks," *Concurrency and Computation: Practice and Experience*, vol. 24, no. 10, pp. 1037–1051, 2012.
- [12] X. Wang, L. Liu, and J. Su, "RLM: A general model for trust representation and aggregation," *IEEE Transactions on Services Computing*, vol. 5, no. 1, pp. 131–143, 2012.
- [13] E. Ayday and F. Fekri, "Iterative trust and reputation management using belief propagation," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 3, pp. 375–386, 2012.
- [14] X. Liu and A. Datta, "Modeling context aware dynamic trust using hidden markov model," in *Proceedings of the 26th AAAI Conference on Artificial Intelligence*, pp. 1938–1944, July 2012.
- [15] E. Koutrouli and A. Tsalgaidou, "Taxonomy of attacks and defense mechanisms in P2P reputation systems-lessons for reputation system designers," *Computer Science Review*, vol. 6, no. 2–3, pp. 47–70, 2012.
- [16] A. Jøsang, "Robustness of trust and reputation systems: does it Matter?" in *Proceedings of the 6th IFIPTM International Conference on Trust Management (IFIPTM '12)*, vol. 374, pp. 253–262, Springer, Berlin, Germany, 2012.
- [17] H. Gao, *Statistics Computation*, Peking University Press, Beijing, China, 1995.
- [18] Z. Liang and W. Shi, "Analysis of ratings on trust inference in open environments," *Performance Evaluation*, vol. 65, no. 2, pp. 99–128, 2008.
- [19] F. Lu, K. Zheng, X. Niu, and Y. Yang, "Construct a risk-aware peer-to-peer security trust model," *Journal of Beijing University of Posts and Telecommunications*, vol. 32, pp. 22–32, 2011.