Hindawi Publishing Corporation
Journal of Electrical and Computer Engineering
Volume 2016, Article ID 4361719, 10 pages
http://dx.doi.org/10.1155/2016/4361719

Research Article

The Comparison of Distributed P2P Trust Models Based on Quantitative Parameters in the File Downloading Scenarios

Jingpei Wang and Jie Liu

Information Security Research Center, China CEPREI Laboratory, Guangzhou 510610, China

Correspondence should be addressed to Jingpei Wang; wjpbupt@163.com

Received 26 December 2015; Revised 29 April 2016; Accepted 9 June 2016

Academic Editor: Arash Habibi Lashkari

Varied P2P trust models have been proposed recently; it is necessary to develop an effective method to evaluate these trust models to resolve the commonalities (guiding the newly generated trust models in theory) and individuality (assisting a decision maker in choosing an optimal trust model to implement in specific context) issues. A new method for analyzing and comparing P2P trust models based on hierarchical parameters quantization in the file downloading scenarios is proposed in this paper. Several parameters are extracted from the functional attributes and quality feature of trust relationship, as well as requirements from the specific network context and the evaluators. Several distributed P2P trust models are analyzed quantitatively with extracted parameters modeled into a hierarchical model. The fuzzy inferring method is applied to the hierarchical modeling of parameters to fuse the evaluated values of the candidate trust models, and then the relative optimal one is selected based on the sorted overall quantitative values. Finally, analyses and simulation are performed. The results show that the proposed method is reasonable and effective compared with the previous algorithms.

1. Introduction

Due to the openness of distributed networks, security issue becomes one of the most important challenges when deploying these networks into application. Traditional strategies, such as traditional encryption and access control, because of their poor scalability, are no longer suited for resolving security issues of distributed P2P system. Trust management resolves the security issues in semantic and behavioral levels and filters malicious nodes based on their real-time behaviors between transactions. Trust mechanism can transfer between heterogeneous mixed networks seamlessly, and the researches of trust management are of considerable interest in recent years [1, 2].

The researches of trust in computer network have emerged several years ago. However, there are no uniform definitions of trust related issues. First, we give our definition of trust and trust management in this paper.

Trust. Trust has been interpreted as opinion, reputation, probability, and so forth. In the trust management based on trust degree, trust is defined as subjective expectations that denote the uncertainty in collaboration between the subjects and agents.

Trust Model. Trust model defines the method and procedure of trust modeling and trust evaluation.

Trust Management. Trust management is a service mechanism that self-organizes a set of items based on their trust status to take an informed decision.

The core issue of trust management is constructing reliable trust models, and a wide range of P2P trust models for distributed P2P network is proposed during the last decades [3–14]. One problem is that there are no evaluating criteria for comparing these varied models, making it difficult for an interested party to decide upon an optimal trust model to implement. We give a P2P scenario as follows.

One user (service requester) performs the file download in P2P network, supposing that varied trust models are

available for computing the trust values of the target service provider. The user should ask some questions firstly:

(1) Which trust model is the most consistent to compute and guide the trust flows?

(2) Which trust model can assist in providing more qualified service in this application context?

(3) The diverse requirements from decision maker would influence the results of choosing the optimal trust model; what is the degree of this influence?

In order to resolve the above quandaries, it is necessary to develop a quantitative method to analyze some trust models and induce choosing the most proper one according to the application context and multiple requirements of user.

In this paper, a method for comparing trust models based on hierarchical model of parameters is proposed. The evaluated parameters are extracted from the trust related concepts, network context, and the requirements of users. The evaluated values of trust models are obtained by quantitative calculation of the parameters model with the Delphi and fuzzy inference methods. The optimal trust model is selected based on the sorted quantized values. Analysis and simulation results show that the proposed algorithm is reasonable and effective.

The rest of the paper is organized as follows. Section 2 presents the related works. Section 3 outlines the parameters and gives qualitative analysis. In Section 4, hierarchical parameter modeling and formal quantization are proposed. Further, parameter fusion and trust model evaluation are given in Section 5. Section 6 presents analysis and simulation, followed by the conclusions in Section 7.

2. Related Works

Various trust models have been proposed for the P2P in the past decade [3–14]. From the aspect of trust measurement and modeling method, the trust models can be divided into hybrid distributed approach [5], trust model based on weighted average method [6, 7], trust model based on game theory [8], multiple factors trust model [9, 10], Bayesian trust model [11], fuzzy inferring trust model [12, 13], trust model based evidence theory [14], and so forth. However, there are rare sound researches on how to compare trust models. Some researchers focus on the qualitative analysis or guidance of the trust models; some others focus on the quantitative evaluation.

Wojcik et al. introduced a set of criteria to analyze trust models [15]. The criteria consist of four parts: trust establishment, trust initialization, trust updating, and trust evaluation. Each part is followed by some suggestions. It provided a common framework for the development of a sound trust model, though there is no concrete realization. Rodriguez-Perez et al. discussed the main issues that a reputation framework must address and analyzed the most representative reputation systems in fully distributed peer-to-peer systems [16]. They also discussed the main advantages and drawbacks of each proposal in relation to peer-to-peer reputation system requirements. Mármol and Pérez described several trust and reputation models for distributed and heterogeneous networks and compared to provide an evaluation of the most relevant works [17]. They suggested that certain security threats and the specific features of the distributed network where a model is to be deployed should be considered carefully to improve the evaluation accuracy. He and Wu discussed the theory basics, applications, advantages, and disadvantages of some reputation systems [18]. They considered that aggregation overhead, storage efficiency, and reputation accuracy are three key issues in the design of reputation for P2P network. Azzedin proposed a reputation assessment process and used it to classify the existing reputation systems [19]. He focused on the different methods in selecting the recommendation sources and collecting the recommendations. These two phases can contribute significantly to the overall performance owing to precision, recall, and communication cost. All the above methods take the right direction to analyze trust model, but there is no concrete algorithm to compare the investigated trust models to select an optimal one to implement.

Schlosser et al. presented a formal model for describing reputation systems [20]. Based on the formal model, a generic simulation framework was implemented. The defects of this simulation framework are shortage of theoretical analysis for parameter settings and that only reputation systems are taken into account. Yang et al. proposed a method to evaluate the trust model by treating the trust model as a black box and comparing the output with the input [21]. Their work is similar to software testing in software engineering. The evaluated results are compared with two parameters: sensibility and foreseeability. However, it is difficult to model the overall features of trust models using merely two measurable parameters. In a word, the existing methods have some deficiencies, and trust model evaluation remains an open issue.

3. Parameters Extracting and Qualitative Analysis of Trust Models

3.1. Parameters Extracting. From the user perspective, the P2P can be considered as a service supporter and trust management is an integral mechanism of the network system that assists the system in providing qualified service. There are some parameters existing in trust relationship and trust models.

Subjectivity. From the definition of trust we can see that trust is a subjective concept. It is provided by observers based on their subjective judgment. Different observer, different period, different mood, and different scenario may induce different judgments. Notice that reputation is not subjective as it is based on the historical behavior. Also, not all parameters are subjective; there are some QoS parameters that can be perfectly quantified (delay, jitter, etc.)

Fuzziness. Trust is a blurry concept. Three factors induce the fuzziness: uncertainty, inaccuracy, and no clarity. A proper

trust model should be able to express these blurry concepts in trust establishing and measurement. However, most trust models proposed are based on numerical computing and the methods of quantization and inference of the fuzzy relationship varied from one to another. How to express, quantize, and infer fuzzy relationship also belongs to the scope of the fuzziness.

Time Decay. Trust should decay as time passes by. For example, trust relationship formed 3 years ago is less credible than that formed 3 days ago. However, the decayed amplitude and range have no unified conclusion in varied trust models. Whether to introduce the decay factor and what decayed range is reasonable need evaluation for the trust models.

Robustness. There are malicious attacks in distributed system, including unintentional attacks, for example, data transmission delay and block induced denial of service, and malicious attacks, for example, false feedback, collusive cheating, and malicious calumniation. An excellent trust model should be able to resist various attacks and avoid the malicious nodes from transactions.

Reward and Punishment. In a trust system, various nodes have different performance according to their ability and wish. Trust models should provide a proper mechanism to reward nodes with high trust values to encourage them to provide better service. Meanwhile, punish nodes with malicious performance by reducing their trust values or forbidding their transaction.

Sensitivity. This feature reflects the evolution speed of the trust relationship with the disturbance of the network behaviors. The evaluated factors of sensitivity include the changing speed of trust value, handing speed of malicious attack, and the speed of searching. Moreover, sensitivity is associated with application scenario; that is, higher sensitivity is suited for high precision network (i.e., military network), while lower sensitivity is popular with tolerant network.

Transitivity. When an entity needs to judge the globe trust value of another entity within the domain or in the distance, the trust transitivity is necessary. Trust or reputation transmitted mainly through recommended mechanism from a series of middle nodes. However, this recommended relationship is not always true; if node A trusts node B and node B trusts node C, we cannot infer that node A always trusts node C. A good trust model should include recommended mechanism as well as the reasonable disposal of asymmetric recommendation.

Scalability. This parameter mainly depicts the relationship between network size and network load in dealing with the trust relationship. The calculation complexity remains low or increases slowly with the increase of network nodes meaning better scalability. Specifically, trust model with lower time complexity, lower space complexity, and more efficient transmission pattern is a better model.

Other parameters could be considered in deciding the performance of a trust model, for example, the assessment or evolution of trust, usability, variable assignments.

3.2. Qualitative Analysis of Trust Models. In this section, we will address the characteristics of some traditional P2P trust models based on the extracted functions.

Rodriguez-Perez et al. [5] proposed a superpeer reputation framework for P2P network. There are single peer and sure-peer. The peers always maintain their own local reputation database; the system is fault tolerant to sure-peer unavailability. Surework introduces incentives in order to promote that nodes with higher capabilities become superpeers and assume more tasks than normal peers. Reciprocity is also promoted by encouraging peers to provide better services to most reputable client peers. Therefore, the robustness and reward-punishment are obvious. Malicious actions can be found by local reputation and clusters' opinion quickly, which reflects some sensibility. Reputation can be calculated and transferred to other sure-peers and clusters. The drawbacks of surework are increasing system complexity and computational cost, the scalability being not very good, and the other parameters being not mentioned.

EigenTrust [6] is a trust and reputation model for P2P networks where each peer is assigned a global trust value based on its transaction history. The trust value changes gradually, and the trust level determines the different transaction chance. The subjectivity, fuzziness, and time decay are not found in this model, as it adopted objective calculation of transaction results and did not consider the time decay factor. An important feature of this model is the presence of some pretrusted peers that help to break up malicious collectives, and peers can avoid transactions with partial malicious peers, so the robustness and punishment mechanism are qualified, whereas the handing speed of malicious attack and the changing speed of trust value are not obvious, which mean lower sensitivity. The transitivity is clearly presented though the asymmetric recommendation is not considered. The pretrusted peers change the convergence and achieve a significant reduction of overhead in the system, so the performance of scalability is acceptable.

PeerTrust [7] is a reputation based trust model, where more factors are introduced to compute trust value for each peer. The feedback-based evaluation, satisfaction of transaction, participating degree, community context, credibility, and so forth are considered in the trust evaluation. The subjectivity is presented with the participation of the peers' judgment of satisfaction and credibility. PeerTrust algorithm also proposed an adaptive time window-based algorithm to reflect the most recent behaviors, so time decay is considered. Good feedback will gain better results and bad feedback will be found, which means the presence of reward-punishment mechanism. The robustness and transitivity are improved compared with EigenTrust, whereas the scalability is decreased as complexity computation.

Harish et al. designed and analyzed a game theoretic model for P2P trust management [8]. The trust framework incorporated self-experience and reputation to calculate trustworthiness of a peer. Various strategies like game

tree strategy, dynamic strategy, and auditing strategy were proposed for selecting peers for doing job. The method addressed the problem of the selfish behavior; different entity uses different strategy. The intelligent entity can update the reputation values of other interactive nodes; and reward and punishment are performed directly by the payoff. Therefore, subjectivity, transitivity, and reward-punishment are obvious. It can avoid internal malicious behaviors and the robustness is presented, but the calculation of reputation and strategies and their evolution induce larger overhead. Fuzziness, time decay, and sensitivity are not mentioned.

Li et al. proposed a multidimensional trust model for large scale P2P computing [9]. It involves many factors, that is, assumptions, expectations, behaviors, and risks, to reflect the complexity of trust. Moreover, the weights of these factors are dynamically assigned by series of objective algorithms. The subjectivity, fuzziness, and time decay are not mentioned. This model gave a scene where malicious feedback is changing while the accuracy and the adaptability maintain a proper level, which means good robustness. The reward-punishment of trust value as well as sensitivity is not obvious, the transitivity is mentioned, and finally the scalability is excellent with the mechanism of direct trust tree.

Wang and Vassileva proposed a Bayesian trust model in P2P networks [11], it takes trust as a multifaceted concept, and peers need to develop differentiated trust in different aspects of other peers' capability. Bayesian network provides a flexible method to combine different aspects of trust. The subjectivity is obvious, and the calculation of differentiated trust is rapid, though the final results are measured by the number of transactions meaning low sensitivity. The transitivity is considered and the scalability is excellent as the lower load of computation. However, the fuzziness, time decay, robustness, and reward-punishment mechanism are not mentioned in this model.

There are other trust models proposed by different methods, for example, fuzzy trust model [13] and D-S evidence trust model [14]. The analysis procedure is the same as that of the above trust models and omitted here. The results of qualitative analysis are shown in Table 1. In this table, "$\surd$" stands for trust models having responding parameters and "$\times$" means not having related parameters or the merits of related parameters are not obvious. From the analysis we can see that the investigated trust models all have their advantages and disadvantages from the aspect of the parameters. And it can be inferred that the degree for one parameter owned by several trust models differs from one to another; for example, EigenTrust and PeerTrust both have robustness, whereas the intensity of robustness is varied as adopting different mechanism. The subjectivity between Jøsang model and Bayesian model is varied as different number of factors is adopted in each model.

In a word, parameter distribution and parameters degree among trust models are unbalanced, making it difficult for an interested party to decide upon a particular trust model to implement. Nevertheless, we can find the relatively optimal trust model through quantitative comparison in a concrete scene. In the next section, a quantized evaluation is addressed.

4. Hierarchical Parameters Modeling and Formal Quantization

4.1. Hierarchical Modeling of Parameters. On one hand, it is difficult to analyze trust models using more than eight parameters directly and simultaneously. Some parameters are conflicted; for example, complicated algorithms are used to deal with attacks, which increase robustness but deteriorate scalability. Some parameters are correlative; better punishment mechanisms would lead to better robustness. Moreover, different parameters concern different aspects of service, and sometime the same parameters may concern more than one aspect; for example, scalability is involved in network structure, and robustness concerns the service reliability as well as network structure.

On the other hand, there are other decision factors, such as network scene and individual policy of observer. According to previous definition, trust management is a third-party auxiliary mechanism assisting the system in providing qualified service. From the service perspective, we can extract some factors of the quality of service with a trust model: function conformance, reliability, the adaptability for network context, and the specific requirement of a user, each of which is followed by some parameters; for example, function conformance includes transitivity and flexibility which reflect the reasonability of trust modeling. The performance of each factor can be evaluated by some low-level parameters.

A natural method is establishing a hierarchical structure to combine the above two aspects; the parameters and their upper factors (criteria layer) can be considered comprehensively. It can distribute conflicting parameters to different decision criteria layer, and correlative parameters can be laid into one layer for coordinate evaluation. Then, a fusion method is designed to fuse these parameters and criteria layer to obtain the overall performance of trust models. In this paper, the decision factors in criteria layer are described as follows.

Function Conformance. This layer mainly focuses on the reasonability of trust representation, the conformance of trust attributes, and the mechanism of performing the service task properly. The most obvious functions of trust management are measuring the uncertainty of the nodes' behaviors and self-organizing a set of objects to perform the task (e.g., routing or transmitting data). Whether the uncertainty can be measured properly or not will be evaluated in this layer. Subjectivity, fuzziness, time decay, and transitivity will be used to characterize the conformance of trust mechanism and be distributed to this layer.

Service Reliability. This layer estimates whether the service provided by trust mechanism is reliable. Trust management is a third-party auxiliary mechanism. The provided service should be qualified. The robustness describes how the trusted cooperators resist malicious attacks or shield from the malicious node to maintain the stability of service. The reward and punishment (with more reasonable resource distribution) and sensitivity (reflecting the reaction speed of attacks and

Table 1: The distribution of parameters of some P2P trust models.

Trust model	Parameters							
	Subjectivity	Fuzziness	Time decay	Robustness	Reward & punishment	Sensibility	Transitivity	Scalability
EigenTrust	×	×	×	√	√	×	√	√
PeerTrust	√	×	√	√	√	×	√	×
Surework	×	×	×	√	√	√	√	×
Harish et al. [8]	√	×	×	√	√	×	√	×
Li et al. [9]	×	√	×	√	×	×	√	√
Wang and Vassileva [11]	√	×	×	×	×	√	√	√
Wang et al. [12]	√	√	√	×	×	√	×	√
Tian and Yang [14]	×	√	√	√	×	×	√	×

the sensitive degree of the changeable trust value) will be evaluated in this layer.

Structure Adaptability. This layer mainly evaluates the dynamic relationship between the trust model and network environment. The structure, size, topology, and the dynamics of the target network all will influence the execution of task. A reasonable model should be able to adjust to the change of network structure. The scalability should maintain excellent state with the expansion of nodes, the transitive path is available with the change of structure, and the reaction is timely when important nodes change or immediate service is needed. Therefore, scalability, transitivity, and sensitivity are related to this layer.

Strategies Differences of Observer. The observer may have different requirement and secure policies and even different interest and preferences, in using the trust model for certain context. In addition, it also includes some performance index, such as the usage of resource (overhead or scalability), disposal speed and quality of service of trust mechanism, the ability of surviving (mainly robustness), and the special need of sensitivity (i.e., higher accurate application).

Other criteria will be populated to add in criteria layers. The detailed hierarchical structure of parameters and factors are shown in Figure 1. Parameters act as basic layer, middle service factors act as criteria layer, and the top layer is goal layer.

The comprehensive assessment of the trust models for performing a specific task in a certain context can be derived from reasonable evaluation of the following criteria layer and basic layer in succession.

4.2. Formal Evaluation of Trust Model. The extracted parameters characterize the basic functional feature of a trust model, $P = \{p_1, p_2, \ldots, p_n\}$ denote the set of parameters, and n is the number of parameters. In order to perform quantitative analysis, we quantify the parameters and select an algorithm to fuse these parameters; that is $C :\mapsto (\mathrm{TM}, P, I)$, where TM is a trust model, I denote an integration algorithm, and C is evaluation result. A direct evaluation can be modeled into a functional form, as shown in

$$C(\mathrm{TM}) = f_I(f_1(p_1), f_2(p_2), \ldots, f_n(p_n)), \quad (1)$$

where $f_i(p_i)$, $i \in [1, n]$, denotes the quantization of ith parameter. In order to achieve the overall unified value, the normalization is embedded in the quantization of $f_i(p_i)$; in other words $Q(P) = (f_1(p_1), f_2(p_2), \ldots, f_n(p_n))$ is a dimensionless vector. $f_I(\cdot)$ denote an integrating function. A simple integration is weighted average of $Q(P)$. A more complicate but rational method is fuzzy fusion that will be used in this paper.

4.3. Quantization of Parameters. There exists a mapping f between the impact factors and the quantified value of each parameter for a given trust model. In our algorithm, the quantitative procedure of a parameter includes extracting the impact factors of each parameter, scoring the impact factors, and performing normalization and fuzzy integration of the impact factors to obtain the quantitative value of single parameter.

For a single parameter p_i, C denotes the factor set: $C = \{c_1, c_2, \ldots, c_m\}$, and m is the number of factors. The factor is extracted based on three considerations: the definition of parameter, evaluated points, range of parameter and some experience of experts. For example, scalability is related to time complexity, space complexity, transmission, and efficient storage of data; the impact factors of sensitivity include the changing speed of trust value and handing speed of malicious attack and the speed of searching and timely reaction when network topology changes.

For a single impact factor c_j, $j \in [1, m]$, we evaluate it with specific measure, range. A simple method is using fuzzy theory to determine the range and level of the evaluated factor according to the experience of observer (i.e., for the rationality, irrational, default, and lowest rationality, medium rationality, favorable rationality, and highest rationality, denoted as five intervals from 0 upper to 1, resp.; quantized step is 0.2 that denotes the uncertainty). Considering that there are some manufactured discrepancies for each factor, Delphi method can be introduced to collect and filter the divergent answers and obtain the quantified value.

The Delphi method is an interactive forecasting method that relies on a group of experts. The experts answer questions in two or more rounds. It is believed that, after several rounds, the range of the answers will decrease and the group will converge towards the "correct" answer. Finally, the process is stopped after a predefined stop criterion (e.g., stability). In

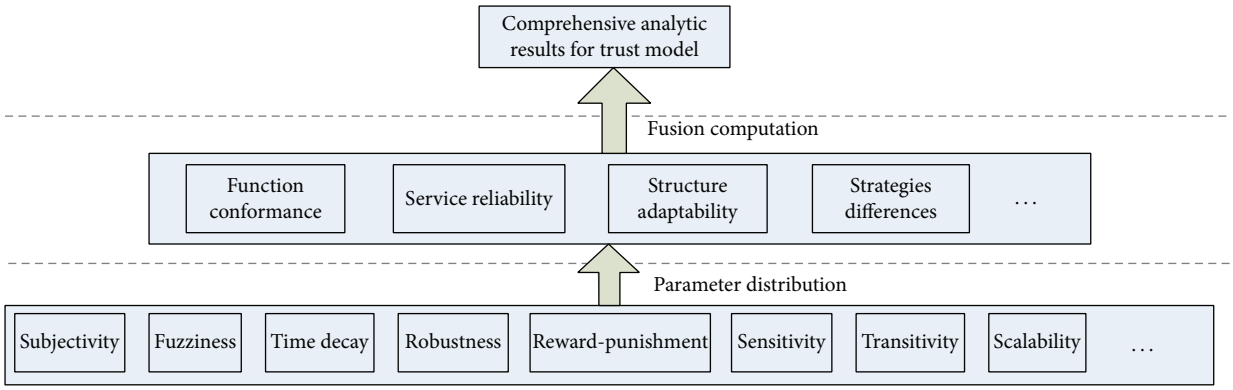


Figure 1: Hierarchical structure of parameters for trust models.

this paper, several questions are defined firstly based on the multiple factors of a particular c_j. Each question is followed by certain options that denote the level of possible answers (i.e., rationality, from being irrational to highest rationality). These questionnaires are provided to several experts. After several rounds, the final correct feedback will be determined, and the final quantized value of a factor $Q(c_j)$ can be obtained. Repeat above quantization until all m factors are quantized, denoted as $Q(C) = \{Q(c_1), Q(c_2), \ldots, Q(c_m)\}$.

Notice that m elements in $Q(c_j)$ may be measured in different unit; take the scalability as an example; the units of time complexity and space complexity are time (ms) and capacity (kb). Firstly, we normalize these different units. The popular method of normalization is max–min method:

$$Q_m\left(c_j\right) = \frac{Q\left(c_j\right) - \min\left(Q\left(c_j\right)\right)}{\max\left(Q\left(c_j\right)\right) - \min\left(Q\left(c_j\right)\right)}, \quad j \in [1, m], \quad (2)$$

where $\max(Q(c_j))$ and $\min(Q(c_j))$ are the maximum quantized value and the minimum value determined by the range of jth factor. $Q_m(c_j)$ is a numeric value between 0 and 1 after normalization. Repeat above disposal until all m factors are normalized, denoted as $Q_m(C) = \{Q_m(c_1), Q_m(c_2), \ldots, Q_m(c_m)\}$.

The final procedure is integrating the impact factors to obtain the overall quantized value of single parameter. As the impact factors are independent of each other, a simple integration is weighted sum of the quantized value of each factor. The integral is defined as follows:

$$\begin{aligned} Q\left(p_i\right) &= \sum_{j=1}^{m} w_{c_j} Q_m\left(C_j\right) \\ &= w_{c_1} Q_m\left(C_1\right) + w_{c_2} Q_m\left(C_2\right) + \cdots \\ &\quad + w_{c_m} Q_m\left(C_m\right), \end{aligned} \quad (3)$$

where w_{c_j}, $j \in [1, m]$, denote the weight of $Q_m(c_j)$ and satisfy $w_{c_1} + w_{c_2} + \cdots + w_{c_m} = 1$. The weights are determined by the experience of the experts in consideration of importance degrees of evaluation criteria. The final integration is finished through (3), and the quantized value of parameter p_i is obtained, denoted as $Q(p_i)$.

Repeat all the above procedures until all n parameters are quantized, denoted as

$$\begin{aligned} Q(P) &= \left(f_1\left(p_1\right), f_2\left(p_2\right), \ldots, f_n\left(p_n\right)\right) \\ &= \left(Q\left(p_1\right), Q\left(p_2\right), \ldots, Q\left(p_n\right)\right), \end{aligned} \quad (4)$$

where $f_i(p_i)$ is a quantification function with all the above procedures and varied for different parameter.

5. Parameter Fusion and Trust Model Evaluation

A fusion algorithm based on fuzzy inference is proposed to combine the parameters in hierarchical structure in Figure 1.

5.1. The Weights of Distributive Parameters. In Figure 1, the middle criteria layer and lower parameters have certain relation. Several parameters are related to one or more factors in criteria layer. As the parameters are dependent on each other, fuzzy integral in (3) is inappropriate. Without loss of generality, we suppose that one factor in criteria layer is related to all the parameters, and the goal layer is related to all the factors in criteria layer. Firstly, the weights of parameters to single factor in criteria layer and the weights of factors in criteria layer to the goal layer are calculated. The entropy-weight coefficient method is a quantitative objective method and will be applied in our paper.

Entropy-weight coefficient method is a quantitative risk evaluation method [22]. The relative importance of a risk factor to an evaluated system can be measured by its entropy, which is calculated by the fusion of probability values denoting the supporting degree of risk factors to indexes of evaluation set for the system. In this paper, the parameters are considered as risk factors; one factor in the criteria layer is considered as evaluated object. Set several statuses for the evaluated object, give the probability of each parameter at each status, and apply entropy-weight coefficient method calculating the relative importance (weight) of each parameter to one upper factor. The statuses can be set based on certain evaluation set (i.e., rationality, from being irrational to highest rationality) used in previous parameter

quantitation, and the probabilities that each parameter stay at certain status of the evaluation set can be determined by the same experts that used the Delphi method in Section 4.3. The detailed procedure of entropyweight coefficient method is referred to in related book (i.e., [22]) and omitted here.

Repeat the above calculation until all the weights are obtained. The weight of parameters of kth ($k \in [1, s]$, s being the number of factors in criteria layer) factor in middle criteria layer is denoted as $W_{pk} = \{w_{k1}, w_{k2}, \ldots, w_{kn}\}$, where n is the number of parameters. For the sake of simplicity, discard the weights that equaled 0 (e.g., time decay has no relation with structure adaptability of a trust model; the probability density function of status is always 0), and obtain effective weights, denoted as $W_k = \{w_{k1}, w_{k2}, \ldots, w_{kb}\}$, where $b \in [1, n]$. Repeat the above filtering; the weights of parameters to one factor in criteria layer and the weights of factors in criteria layer to the goal layer are obtained.

5.2. The Fusion of Parameters Based on Fuzzy Inference. The evaluated values of single factor in criteria layer and the evaluated value of goal layer will be fused by fuzzy inference in succession. In fuzzy set theory, a variable $V_T = \{v_1, v_2, \ldots, v_b\}$, v_k ($k = 1, 2, \ldots, b$) denoting the value of object T at the point k (k-level value) according to the defined membership functions in a given discourse domain, and the problem is how to obtain V_T under a given tree (i.e., Figure 1).

We evaluate kth factor in the criteria layer followed by b parameters. Set a discourse domain for the kth factor (e.g., reliability, from the least reliable to the most reliable and 5 levels are divided as the least reliable, little reliable, medium reliable, favorite reliable, and the most reliable and $V_q = \{0, 0.2, 0.4, 0.6, 0.8, 1\}$ stands for quantitative border value). The membership function is a trapezoidal function; the prototype is shown below:

$$\mu_T(x) = \begin{cases} \left(\dfrac{x-t}{1-t}\right)^2, & 0 \le x \le \dfrac{a+1}{2} \\ 1 - \left(\dfrac{x-t}{1-t}\right)^2, & \dfrac{a+1}{2} \le x \le 1, \end{cases} \quad (5)$$

where a is a defined threshold and t ($t \in [0, 1]$) is the offset of positive x and is set to 0.2 to form 5 curves.

The quantitative values of b parameters have been achieved in Section 4.3; each value can be mapped to a membership degree according to membership function, eventually formed into an evaluation matrix $R = (r_{gh})_{b \times l}$. The weighted vector is $W_k = \{w_{k1}, w_{k2}, \ldots, w_{kb}\}$, and then the overall vector of the kth factor is denoted as

$$V_T = \{v_1, v_2, \ldots, v_l\} = (w_{k1}, w_{k2}, \ldots, w_{kb}) \times \left(r_{gh}\right)_{b \times l}. \quad (6)$$

Define the evaluated value of the kth factor: $V_k = \max(V_T)$, where $\max(V_T)$ is the maximum membership degree of V_T.

Repeat the above procedure until all the evaluated values of the factors in the criteria layer are obtained. Based on the evaluated value of the factors in the criteria layer and the weights of factors in middle layer to the final goal layer, the fuzzy comprehensive judgment is performed with the same method as that used in calculating the evaluated value of the kth factor V_k to obtain the comprehensive analytic value for a trust model.

Then, the observer can compare the eventual evaluated value with the threshold to judge whether the trust model is qualified. The threshold is set based on some factors, for example, accuracy and fee. We can evaluate a set of trust models, sort the evaluated values, and choose an optimal trust model (usually the model with maximal evaluated value) for implementation.

5.3. The Outline of the Evaluated Procedure. The main steps of the proposed method are summarized:

(1) Based on the structure in Figure 1, apply entropy-weight coefficient method to calculate the weights of parameters to factors in criteria layer and the weights of factors in criteria layer to goal layer. Meanwhile, determine the distributive b parameters for kth factor in criteria layer.

(2) Parameter quantitation: for a trust model, quantize the extracted parameters with a series of procedures described in Section 4.3, and obtain the vector $Q(P) = (f_1(p_1), f_2(p_2), \ldots, f_n(p_n))$.

(3) Parameter fusion: the evaluated value of a trust model is calculated by the fusion of quantitative values and weights of parameters by fuzzy inference described in Section 5.2. And judge whether the given model satisfies the request according to the defined threshold.

(4) Select a set of trust models, repeat step (2) and step (3), calculate and sort the overall evaluated values, and choose an optimal trust model for implementation.

6. Method Analysis and Simulation

In this section, some discussion, a concrete evaluation experiment, and the effectiveness of the proposed method are addressed in Sections 6.1, 6.2, and 6.3, respectively.

6.1. Some Discussion of the Proposed Method. Consider the following:

(1) Notice that the hierarchical model is an open structure that other parameters and decision factors can be integrated into this model, which reflect the flexibility of the proposed method. Moreover, the hierarchical model is a reference model, and more than three layers might exist when subfactors are being linked to the parameters or the factor in criteria layer.

(2) The weights calculated by our method are stable under the condition that distributed scene and individual policy are determined. And the quantized values of parameters varied from one trust model to another.

6.2. A Concrete Evaluation Experiment. A concrete evaluation experiment is performed. Six traditional trust models

Table 2: Sorted results of evaluated trust models.

Overall score	0.79	0.78	0.65	0.63	0.62
Sorted models	MdTrust	Bayesian	EigenTrust	GTM	PeerTrust

analyzed in Section 3.2 are selected: EigenTrust, PeerTrust, game theory model (GTM for short) [8], multidimensional trust (MdTrust for short) model [9], and Bayesian model [11]. Some conditions are set as follows:

(1) A concrete scene: one user (service requester) performs the file download in P2P network. And the service requester pays more attention to the speed and quality of file download.

(2) The eight parameters and four factors in the middle layer are all considered.

(3) The number of statuses of the four factors is set to 5 (measured by rationality, I-irrational, L-lowest rationality, M-medium rationality, F-favorable rationality, and H-highest rationality); the probabilities of each status for parameters are determined by the same 7 experts in parameter quantitation with Delphi method; the range of quantized value of parameters is 0-1, with quantized step being 0.2.

According to the procedures in Section 5.3, the evaluated values of the 6 trust models are shown in Table 2.

From Table 2, we can see that multidimensional trust model reaches the highest score, as it has more parameters than others, and the robustness and scalability receive higher score in quantitation. PeerTrust compared to EigenTrust, although with better transitivity; worse scalability eventually leads to a smaller overall evaluated score, as the weight of scalability is larger than that of transitivity under the service requester policy.

We can see that none of the candidate trust models satisfies all the parameters. If the threshold is 0.8, then no trust model is qualified. Nevertheless, we can select the relatively optimal trust model (i.e., one received the highest evaluated value) to implement for a special application.

6.3. The Effectiveness of the Method. In this section, we will analyze the effectiveness of the proposed method.

The efficiency of the proposed method: for a given model, for n parameters, suppose that there are m factors mostly. Seven experts carry out two rounds of consultation, each of which needs time t_1, and the combination of m factors costs $O(m)$. The overall time complexity is $n \times (2t_1 \times m + O(m))$, m being small (around 3–5 for each parameter), so the time complexity is controlled. For the weights of parameters, it is needed to calculate the process of the entropy-weight coefficient, time complexity being $O(n)$. Moreover, the weights can be reutilized for the same scene and task.

We further validate the effectiveness of the proposed method by comparing it with previous methods [15, 20, 21]. For the convenience, [15] is denoted as Wojcik's method and [20, 21] are Schlosser's method and Yang's method.

Firstly, the proposed method adopts multiple parameters to evaluate trust model; it is more comprehensive than other works in characterizing the trust issues. Wojcik introduced a series of factors classified into four aspects in establishing a trust model, but the parameter functions were not considered. Yang's method judged the performance of trust model with two parameters: sensibility and foreseeability. In Schlosser, three parameters were used to reflect trust. These methods had failed to reflect the comprehensive characteristics of a trust model.

Secondly, in terms of accuracy, Yang proposed a black box model and compared a set of trust history sequences in the input with the output and then determined the performance of the trust model with sensibility and foreseeability. Its accuracy depends on the initialization of trust and behavioral characteristic. Wojcik displayed entire process of establishing trust comprehensively, but no specific assessment is performed. Schlosser presented a formal model for describing multiple reputation systems, but only reputation systems are taken into account. In our proposal, objective disposal of parameters as well as fuzzy inference is used to quantify the evaluated value of a trust model, the results are more objective and with higher accuracy.

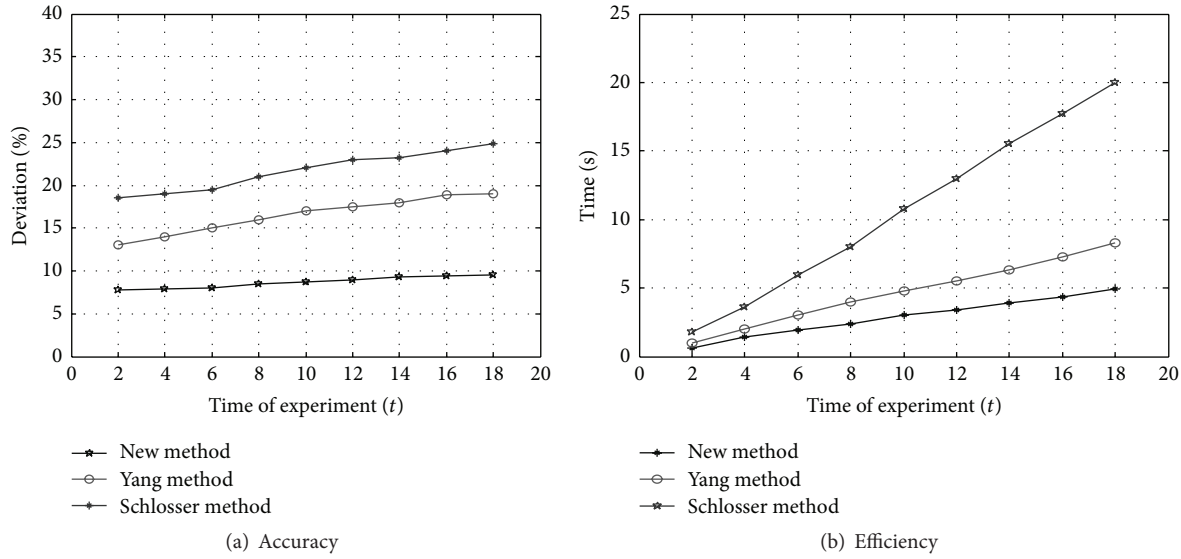
Thirdly, in terms of efficiency, the overhead for our method is controllable and man-made evaluation in Delphi method and the calculation of weights and the fuzzy inference contribute to the calculation load. Wojcik's method does not involve load, and the overhead varied with varied algorithms. Yang's method searched for the history scorings of trusted entities according to the defined behavior characteristics; the time complexity is about $O(n)$, where n is the number of behaviors collected. Schlosser simulated the reputation system in the performance of resisting attacks with the granularity of single node, and the consumption increases with the increase of nodes. The analysis results are shown in Table 3.

In Table 3, the proposed method is denoted as "new method"; the performance is denoted as three levels: good (high), medium, and bad (low). Table 3 explains the superiority of the proposed method.

Further, we present a quantitative comparison among Schlosser's method and Yang's method with simulation. The accuracy and efficiency are compared among three methods.

Accuracy simulation: reflect the change of deviation (y-axis) of evaluated results with the increasing experiment time (x-axis). The conditions are the same as that set in Section 6.2; the deviation is defined as $d = |d_e - d_t| \times 100\%$, where d_e is current evaluated value of the optimal trust model and d_t is the statistical average of its former values. We perform the experiment 20 times. The number of initial nodes of P2P network is 20, where malicious nodes are 20%. The network nodes increase by 5, where the malicious nodes increase with the same percentage (20%), when the experiment time increases by 1.

Efficiency simulation: reflect the relationship between resource consumption (i.e., time consumption) and the number of experiments. The initial number of evaluated trust models is 1 and increases by 1 when the experiment time increases by 1. The simulation results are shown in Figure 2.



(a) Accuracy (b) Efficiency

Figure 2: Simulation results.

Table 3: The comparison of the previous methods.

	Wojcik's method	Yang's method	Schlosser's method	New method
Comprehensiveness	Good	Medium	Medium	Very good
Accuracy	High	Medium	Low	Very high
Efficiency	Uncertain	High	Medium	High

Figure 2(a) describes the accuracy of the three methods. We can find that the deviation of the proposed method is smaller than Yang's method and Schlosser's method; the deviation is controlled within 10%. Therefore, the proposed method is more accurate.

Figure 2(b) describes the efficiency of the three methods; the calculation load increases with the increasing of evaluated models. The proposed method is similar to Yang's method, increasing linearly, but Schlosser's method increases rapidly. The results are in accord with analysis in Table 3.

7. Conclusions

A new method is proposed to compare and evaluate the trust models with quantitative parameters in P2P file downloading scene in this paper. The evaluated parameters are extracted from the trust related concepts and modeled into a hierarchical structure. The Delphi method, entropy-weight coefficient method, and fuzzy inference are applied to obtain a comprehensive evaluated value of a trust model. The optimal trust model is selected according to the sorted overall quantized values of candidate trust models. Analysis and simulation results show that the proposed evaluation algorithm is reasonable and effective. The proposed method resolves the individuality issues, assisting a decision maker in choosing an optimal trust model to implement in specific context. Moreover, the method also can be used to guide the newly generated trust model in theory so that it has better performance in parameter function and adaptability.

Competing Interests

The authors declare that they have no competing interests.

References

[1] Y. Zhong, B. Bhargava, Y. Lu, and P. Angin, "A computational dynamic trust model for user authorization," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 1–15, 2015.

[2] I.-R. Chen, J. Guo, and F. Bao, "Trust management for service composition in SOA-based IoT systems," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '14)*, pp. 3444–3449, Istanbul, Turkey, April 2014.

[3] E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, and P. Samarati, "Managing and sharing servants' reputations in P2P systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. 15, no. 4, pp. 840–854, 2003.

[4] L. Mekouar, Y. Iraqi, and R. Boutaba, "Detecting malicious peers in a reputation-based peer-to-peer system," in *Proceedings of the 2nd IEEE Consumer Communications and Networking Conference (CCNC '05)*, pp. 37–42, IEEE, Las Vegas, Nev, USA, January 2005.

[5] M. Rodriguez-Perez, O. Esparza, and J. L. Muñoz, "Surework: a super-peer reputation framework for p2p networks," in *Proceedings of the 23rd Annual ACM Symposium on Applied Computing (SAC '08)*, pp. 2019–2023, Fortaleza, Brazil, March 2008.

[6] 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, ACM, Budapest, Hungary, May 2003.

[7] L. Xiong and L. Liu, "A reputation-based trust model for peer-to-peer eCommerce communities," in *Proceedings of the ACM Conference on Electronic Commerce (EC '03)*, pp. 275–284, San Diego, Calif, USA, June 2003.

[8] M. Harish, N. Anandavelu, N. Anbalagan, G. S. Mahalakshmi, and T. V. Geetha, "Design and analysis of a game theoretic model for P2P trust management," in *Distributed Computing and Internet Technology: 4th International Conference, ICDCIT 2007, Bangalore, India, December 17–20. Proceedings*, vol. 4882 of *Lecture Notes in Computer Science*, pp. 110–115, Springer, Berlin, Germany, 2007.

[9] 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.

[10] L. Srour, A. Kayssi, and A. Chehab, "Reputation-based algorithm for managing trust in file sharing networks," in *Proceedings of the Securecomm and Workshops*, pp. 1–10, IEEE, Baltimore, Md, USA, September 2006.

[11] Y. Wang and J. Vassileva, "Bayesian network-based trust model in peer-to-peer networks," in *Proceedings of IEEE/WIC International Conference on Web Intelligence*, pp. 372–378, Halifax, Canada, 2003.

[12] Y. Wang, R. Wang, and Z. Han, "Dynamical trust construction schema with fuzzy decision in P2P systems," *Chinese Journal of Electronics*, vol. 18, no. 3, pp. 417–421, 2009.

[13] S. Song, K. Hwang, R. Zhou, and Y.-K. Kwok, "Trusted P2P transactions with fuzzy reputation aggregation," *IEEE Internet Computing*, vol. 9, no. 6, pp. 24–34, 2005.

[14] C. Tian and B. Yang, "A D-S evidence theory based fuzzy trust model in file-sharing P2P networks," *Peer-to-Peer Networking and Applications*, vol. 7, no. 4, pp. 332–345, 2014.

[15] M. Wojcik, H. S. Venter, and J. H. P. Eloff, "Trust model evaluation criteria: a detailed analysis of trust representation," in *Proceedings of the South African Telecommunications Networks and Applications Conference (SATNAC '06)*, Western Cape, South Africa, September 2006.

[16] M. Rodriguez-Perez, O. Esparza, and J. L. Muñoz, "Analysis of peer-to-peer distributed reputation schemes," in *Proceedings of the IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom '05)*, pp. 1811–1817, San Jose, Calif, USA, December 2005.

[17] F. G. Mármol and G. M. Pérez, "Trust and reputation models comparison," *Internet Research*, vol. 21, no. 2, pp. 138–153, 2011.

[18] C. He and M. Wu, "Comparison and analysis of different reputation systems for peer-to-peer networks," in *Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE '10)*, vol. 3, pp. V3-20–V3-23, IEEE, Chengdu, China, August 2010.

[19] F. Azzedin, "Taxonomy of reputation assessment in peer-to-peer systems and analysis of their data retrieval," *Knowledge Engineering Review*, vol. 29, no. 4, pp. 463–483, 2014.

[20] A. Schlosser, M. Voss, and L. Brückner, "Comparing and evaluating metrics for reputation systems by simulation," in *Proceedings of the IAT Workshop on Reputation in Agent Societies*, 2004.

[21] M. Yang, L. Wang, and Y. Lei, "Research on evaluation of trust model," in *Proceedings of the International Conference on Computational Intelligence and Security (CIS '08)*, vol. 1, pp. 345–349, Suzhou, China, December 2008.

[22] H. Su and C. Zhu, "Application of entropy weight coefficient method in evaluation of soil fertility," in *Recent Advances in Computer Science and Information Engineering*, vol. 126 of *Lecture Notes in Electrical Engineering*, pp. 697–703, Springer, Berlin, Germany, 2012.