Dynamic Trust Model Based on Extended Subjective Logic

Tian Junfeng[1], Zhang Jiayao[1], Zhang Peipei[1] and Ma Xiaoxue[2]
[1]School of Computer Science and Technology, Hebei University
Baoding 071000, Hebei -P.R. China
[e-mail: tjf@hbu.edu.cn]
[e-mail: 2218624065@qq.com]
[e-mail: zhangjiayao13@sina.com]
[2]Computer instruction, Hebei University
Baoding 071000, Hebei -P.R. China
[e-mail: 861465099@qq.com]
*Corresponding author: Zhang Jiayao

Received July 2, 2017; revised January 23, 2018; accepted March 12, 2018;
published August 31, 2018

Abstract

In Jøsang's trust model, trust evaluation is obtained through operators, but there are problems with the mutuality and asymmetry of trust and the impact of event weight on trust evaluation. Trust evaluation is updated dynamically and continuously with time and the process of interactions, but it has not been reflected in Jøsang's model. Therefore, final trust evaluation is not accurate, and malicious fraud cannot be prevented effectively. This causes the success rate of interaction to be low. To solve these problems, a new dynamic trust model is proposed based on extended subjective logic (DTM-ESL). In DTM-ESL, the event weight and the mutuality of trust are fully considered, the original one-way trust relationship is extended to a two-way trust relationship, discounting and consensus operators are improved, and trust renewal is designed based on event weight. The viability and effectiveness of this new model are verified by simulation experiments.

Keywords: Extended subjective logic, Dynamic trust model, Two-way trust relationship, Trust search, Event weight

This work has been supported by National Natural Science Foundation of China (61170254,60873203).

http://doi.org/10.3837/tiis.2018.08.021 **ISSN : 1976-7277**

1. Introduction

Trust is a type of belief or expectation. Trust in trading refers to the honesty, recognition, and authenticity of services in the trading process [1]. As the prerequisite and basis for trading, trust determines the results of trading. Successful trading requires trust whether in the traditional trading environment or in the e-commerce trading environment. If trust is lacking on both sides of the trade, people will take actions that are beneficial to themselves, so trust is a necessary condition for successful trading. Trust in the traditional trading environment is the result of understanding. Both sides understand each other through a history of direct interactions, and they directly establish trust relationships that influence trading.

With the rapid development of information technology, e-commerce is gradually increasing. The traditional trust mechanism does not meet the requirements because trading is no longer face-to-face, and we cannot evaluate trust directly through a history of direct interactions. The static trust process based on Certificate Authority [2-3] is proposed to solve the corresponding problems. With the further expansion of large-scale distributed application systems (e.g., grid computing, pervasive computing, peer-to-peer computing, Ad Hoc), the system is an autonomous network that is composed of nodes, and the information on the nodes in the network can be shared.

However, some malicious nodes may be hidden in the network to commit fraud or provide malicious recommendations, resulting in great risk in the interactions between nodes. A static trust mechanism based on proofs cannot effectively prevent malicious behavior, and cannot adapt to the development of a large-scale distributed network [4]. Therefore, it is very important to establish an effective dynamic trust management mechanism for the healthy development of e-commerce that can forecast a node’s behavior before an interaction and update the trust evaluation after the interaction.

The concept of trust management was first proposed by Blaze et al. [4]. The basic idea was to recognize the incompleteness of security information in the current system. To ensure the system can make security decisions, we must rely on additional security information that is provided by a trusted third party. In addition, from the perspective of trust, the content and degree of trust were divided by Rahman et al. [5], and a corresponding trust model was established to evaluate the trust.

Based on the state and behavior of entities, a dynamic trust metric of a trusted network was proposed by Li et al. [6]. The trust information was obtained through analysis of the association of the state and behavior of entities. Malicious attacks were effectively solved with this model, but the dynamic changes of context were not considered. A super-peer-based trust model for peer-to-peer networks was proposed in [7]. The problem of the trust relationship between nodes being hard to build was solved, and a node classification and feedback filtering algorithm were designed in the model. Both ensure the model can not only resist malicious attacks effectively but also accomplishes this at low cost.

Wang et al. [8] proposed an evaluation method of subjective trust based on a cloud model. This model was used to describe and measure the degree of trust and uncertainty. The fuzziness and randomness of trust between entities were considered in the model, and a trust change cloud was structured through the history of a subjective trust cloud, which ensures the method can provide effective auxiliary support to the trust decision. Jiang proposed a comprehensive and efficient trust model of WSN. The reliability and familiarity of trust were defined to improve the accuracy of recommended nodes. The trust value of sensor nodes was more accurate and reliable [9].

Taking the dynamics and uncertainty of trust into account, Jøsang et al. [10-15] proposed a method of subjective logic to model the trust relationship based on the Dempster/Shafer evidence theory. In Jøsang's model, the concepts of evidence space and opinion space were introduced to describe and measure the trust relationship, and a series of subjective logic operators were provided to calculate the trust evaluation. Contrary to the single value that was previously used to describe trust, Jøsang's model emphasized the subjectivity and uncertainty of trust and adopted the uncertainty u, which can better reflect the characteristics of trust.

However, this model is not perfect, and there are still some problems in Jøsang's model. Jøsang's model ignored some factors: trust is mutual, asymmetrical, dynamic, and influenced by the importance of current events. Feng proposed a trust management mechanism based on Bayesian model, in which the trust value was calculated by using the RFSN trust value calculation method to calculate the direct trust and indirect trust. The model introduced the time sliding window to update the trust value [16]. You considering the dynamic trust and rewards and punishment mechanism, has the strong ability of self-adjusting, can rapidly improve the reliability of the trust evaluation, did not consider the weight of the recommended event [17].

To solve this problem, we make the following improvements to some models.

1. The original one-way trust relationship is extended to a two-way trust relationship, and designs three trust decision schemes of relative trust evaluation between two nodes.
2. Discounting and consensus operators are improved.
3. Trust updates, such as penalties and rewards, and trust network searches are fully considered by the impact of event weights.

2. Subjective logic and problems in Jøsang's model

In Jøsang's model, the evidence space consists of a series of observable events produced by the entity. These events can be divided into positive events and negative events. The opinion space consists of a series of subjective trust evaluations about declarative statements, and it is represented by the triplet w = {b, d, u}. Assuming the trust evaluation between entity A and entity B is $w_B^A = \{b_B^A, d_B^A, u_B^A\}$, the triplet satisfies

$$b_B^A + d_B^A + u_B^A = 1 \text{ and } b_B^A, d_B^A, u_B^A \in [0,1] \tag{1}$$

where b_B^A, d_B^A and u_B^A represent belief, disbelief, and uncertainty of entity A to entity B. Trust evaluation is determined by the mapping function from the evidence space to the opinion space. The values r, s, and C represent the number of positive events, negative events, and uncertain factor (in subjective logic, the default value is 2) in evidence space. The mapping function is

$$\begin{cases} b_B^A = \dfrac{r_B^A}{r_B^A + s_B^A + C} \\ d_B^A = \dfrac{s_B^A}{r_B^A + s_B^A + C} \\ u_B^A = \dfrac{C}{r_B^A + s_B^A + C} \end{cases} \tag{2}$$

The formula of expectation value E of entity *A* to entity *B* is as follows:

$$E_B^A = b_B^A + a_B^A u_B^A \tag{3}$$

where *a* is the prior probability to show past experiences.

The discounting and consensus operators are given below.

Discounting operator: Node *A* wants to know the trust evaluation of node *T* when there is no direct interaction between them, so *A* needs a recommendation from node *B;* thereby a recommended path from node *A* to node *T* is formed through node *B*. Assuming node *A* trusts node *B*, the trust evaluation is denoted by $w_B^A = \{b_B^A, d_B^A, u_B^A\}$. Node *B* also trusts node *T*, and the trust evaluation is denoted by $w_T^B = \{b_T^B, d_T^B, u_T^B\}$. The symbol "$\otimes$" is used to designate the discounting operator. Thus, we can write $w_T^{A:B} = w_B^A \otimes w_T^B$.

$$\begin{cases} b_T^{A:B} = b_B^A b_T^B \\ d_T^{A:B} = b_B^A d_T^B \\ u_T^{A:B} = d_B^A + u_B^A + b_B^A u_T^B \end{cases} \tag{4}$$

Consensus operator: Node *A* wants to know the trust evaluation of node *T* when both *B* and *C* have recommended information about node *T*. Two opinions from *B* and *C* must be aggregated. Assuming node *B* trusts node *T*, the trust evaluation is denoted by $w_T^B = \{b_T^B, d_T^B, u_T^B\}$. Node *C* also trusts node *T*, and the trust evaluation is denoted by $w_T^C = \{b_T^C, d_T^C, u_T^C\}$. The symbol "$\oplus$" is used to designate the consensus operator. Thus, we can write $w_T^{B\Diamond C} = w_T^B \oplus w_T^C$.

$$\begin{cases} b_T^{B\Diamond C} = (b_T^B u_T^C + b_T^C u_T^B)/k \\ d_T^{B\Diamond C} = (d_T^B u_T^C + d_T^C u_T^B)/k \\ u_T^{B\Diamond C} = (u_T^B u_T^C)/k \end{cases} \tag{5}$$

where $k = u_T^B + u_T^C - u_T^B u_T^C$.

However, studies found that there are still many problems in Jøsang's trust model:

(1) The mutuality and asymmetry of trust are not considered in Jøsang's model. The trust evaluation is mutual between nodes. The trust evaluation of node *A* to node *B* determines the degree of subjective trust to services that are provided by node *B*. The trust evaluation of node *B* to node *A* decides the credibility degree of the recommended information.

(2) Trust evaluation between two nodes is influenced by the importance of current events. In general, the more important the current event, the more cautiously nodes evaluate each other. Jøsang's model ignores the importance of events.

(3) Trust evaluation is dynamic. That is to say, the trust evaluation is updated dynamically and continuously as time goes on and processes interact. Jøsang's model does not take this into consideration.

(4) With the analysis of the discounting operator, we can see that the final trust evaluation of node *A* to node *B* is decided by the parameters b_B^A, b_T^B, and d_T^B, and it is not associated with the parameter d_B^A. When the belief of node *A* to node *B* is fixed and the values of d_B^A and u_B^A satisfy the equation $d_B^A + u_B^A = 1 - b_B^A$, then the changes of d_B^A and u_B^A have no influence on

the final trust evaluation. However, the trust evaluation of node A to node B is determined by the parameters b_B^A and d_B^A together, and the final trust evaluation obtained from Jøsang's model will inevitably deviate from the objective.

(5) The importance of the event is also not considered in the consensus operator.

3. Dynamic trust model based on extended subjective logic

In view of the existing problems in Jøsang's model, we developed a new trust model (DTM-ESL), in which the mutuality of trust and the importance of events to the trust evaluation are fully considered. The new model is an improvement to and extension of Jøsang's original model. Our main work is as follows:

(1) The original one-way trust relationship is extended to a two-way trust relationship, and three trust strategies based on the importance of current events are given.

(2) The discounting and consensus operators in Jøsang's model are improved to make them more in line with the actual situation.

(3) According to the dynamism of trust, trust renewal is designed based on event weight.

In the following four sections, we introduce the related concepts, the construction of a two-way trust relationship, the improvement of discounting and consensus operators, and the design of trust renewal.

3.1 Related concepts

For ease of description, we define related concepts with regard to DTM-ESL.

Trustor: The source node that initiates the search in the trust network. It must calculate the trust evaluation.

Trustee: The destination node that terminates the search in the trust network. Its trust evaluation must be calculated.

Recommended entities: The intermediate nodes that provide recommendations in the trust network.

Neighbor node: A node that has direct interaction with one specific node.

Trust evaluation: Quantifies the trust value of node *A* to node *B*. It is composed of belief, disbelief, and uncertainty. We can write $w_B^A = \{b_B^A, d_B^A, u_B^A\}$.

Relative trust evaluation: Quantifies the trust value between node *A* and node *B*. It is also composed of belief, disbelief, and uncertainty. We can write $w_{A,B} = \{b_{A,B}, d_{A,B}, u_{A,B}\}$.

System: An application scenario for models.

Event: A series of behaviors that cause the node's expectation value to change.

Event Weight: The importance of a current event. In this paper, the symbol *V* is used to designate it, where $V \in [0,1]$. The more important the event, the higher the event weight [18]. The calculation rules refer to reference. The demarcation points V_1 and V_2 are selected based on a system that divides all events into the following three categories:

$$\begin{cases} V \in [0, V_1] & \text{Current event has low importance of event;} \\ V \in (V_1, V_2) & \text{Current event has general importance of event;} \\ V \in [V_2, 1] & \text{Current event has high importance of event} \end{cases} \tag{6}$$

3.2 Two-way trust relationship and three trust strategies

In general, trust is mutual and asymmetrical. As shown in **Fig. 1**, assuming node *A* is the trustor, node *B* is a recommended entity. Node *A* trusts node *B*, and the trust evaluation is denoted by $w_B^A = \{b_B^A, d_B^A, u_B^A\}$. Correspondingly, node *B* also trusts node *A*, and the trust evaluation is denoted by $w_A^B = \{b_A^B, d_A^B, u_A^B\}$. Nodes have trust evaluations about each other, and the trust evaluations are asymmetrical. The trust evaluation of node *A* to node *B* determines the degree of subjective trust for services provided by node *B*. The trust evaluation of node *B* to node *A* determines the credibility degree of the recommended information. Balancing the difference between them becomes the key to determining the interaction result. The original one-way trust relationship is extended to a two-way trust relationship, and the relative trust evaluation $w_{A,B}$ between *A* and *B* is used. All operation rules mentioned later are based on the premise of relative trust evaluation.

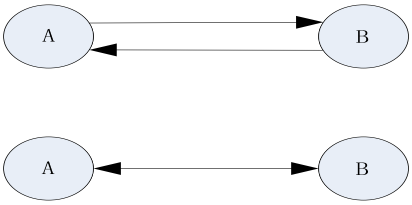

Fig. 1. Two-way trust relationship

In general, it is not easy for node *A* to know the real trust evaluation about itself by node *B*. Sometimes, for its own interests, node *B* may make a trust evaluation that does not agree with the real situation, which means $w_A^B\ _{real} \neq w_A^B\ _{evaluate}$. In this case, the relative trust evaluation $w_{A,B}$ between node *A* and node *B* is used.

In this paper, three trust strategies for the relative trust evaluation are proposed. The selection of strategies is determined by the event weight. In general, the more important the current event, the higher the event weight, and the more cautious the corresponding evaluation. Suitable demarcation points V_1 and V_2 are selected by the current system:

$$\begin{cases} \text{Optimistic strategy} & V \in [0,\ V_1]; \\ \text{Neutral strategy} & V \in (V_1,\ V_2); \\ \text{Pessimistic strategy} & V \in [V_2, 1] \end{cases} \tag{7}$$

The three trust strategies are as follows:

1. Optimistic strategy: when the current event weight is low ($v_i \in [0, v_1]$) and the risky situation can be chosen.

$$\begin{cases} b_{A,B} = \max(b_B^A, b_A^B) \\ d_{A,B} = \min(d_B^A, d_A^B) \\ u_{A,B} = 1 - b_{A,B} - d_{A,B} \end{cases} \tag{8}$$

2. Pessimistic strategy: when the current event weight is high ($v_i \in [v_2, 1]$) and the current choice requires caution.

$$\begin{cases} b_{A,B} = \min(b_B^A, b_A^B) \\ d_{A,B} = \max(d_B^A, d_A^B) \\ u_{A,B} = 1 - b_{A,B} - d_{A,B} \end{cases} \tag{9}$$

3. Neutral strategy: when the current event weight is ordinary ($v_i \in (v_1, v_2)$) and the choice is neutral.

$$\begin{cases} b_{A,B} = \alpha b_B^A + \beta b_A^B \\ d_{A,B} = \alpha d_B^A + \beta d_A^B \\ u_{A,B} = 1 - b_{A,B} - d_{A,B} \end{cases} \tag{10}$$

where α、β satisfy $0 \le \alpha \le 1$, $0 \le \beta \le 1$, and $\alpha + \beta = 1$. The values are $\alpha = \beta = 0.5$.

3.3 Construction of the trust network

In DTM-ESL, the trust network analysis method is used according to [19]. By splitting the trust relationships from the flooding search, a new specification chart is obtained that consists of a number of independent trust paths from trustor to trustee. Based on the diagram of the trust network recommendation and the calculation rules of trust evaluation in DTM-ESL, the trust evaluations of trustor to trustee can be obtained assuming the trust relationships are stored in the form of a table. In **Fig. 1**, for example, the trust relationships are stored as follows:

Table 1. Store of trust relationships

Source	Target	Belief	Disbelief	Uncertainty	Direct Interaction
A	B	b_B^A	d_B^A	u_B^A	1
B	A	b_A^B	d_A^B	u_A^B	1

There are usually many paths from the trust subject to the trust object in the trust network recommendation graph. So how to find the best path of trust to produce the most trusted evaluation results? In this paper, a method of double-threshold filtering is proposed to select the nodes with higher trust rating and control the number of nodes in order to get the optimal trust path. Before conducting a trust search, a simplified trust network recommendation is obtained through double-threshold filtering. The following is the detail:

First filter the nodes based on thresholds. In other words, the nodes that provide recommendations need to reach a certain level of expectations before they have the recommended qualifications. If the expected value of a node is too low, it is considered that the trustworthiness of the node is not high, which leads to a high degree of untrusted recommendation and the formation of the transfer path is invalid.

Second, filter the events based on thresholds. In other words, the more important the current events, the more we must ensure that the nodes that provide recommendations have high expectations, thus forming a trust network with high credibility.

3.4 Improvement in discounting and consensus operators

3.4.1. Trust transitivity: Trust evaluations between nodes are different under different event weights. For example, when the current event weight is low, *A* thinks *B* can recommend a good result. However, when the event changes and the event weight increases, it does not mean that *A* trusts *B* to recommend a good result as before. Therefore, the impact of event weight on the current trust evaluation must be considered when calculating the trust transitivity. Since the final trust evaluation is irrelevant to the unbelief of node *A* to node *B* for the original operator, we made improvements to it. The trust transitivity is shown below:

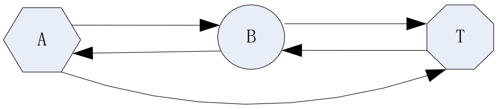

Fig. 2. Trust transitivity

where node *A* is the trustor, node *B* is a recommended entity, and node *T* is the trustee. Trust is mutual and asymmetric between *A* and *B*, and between *B* and *T*. Through the recommendation of node *B*, node *A* can get a one-way trust evaluation of node *T*.

The new transfer operator is divided into three steps below:

1. The relative trust evaluations between nodes are used. For the three trust strategies, see 3.2.

2. The impact of event weight on the trust evaluation is considered. The impact factor is set as η, and η acts between *A* and *B*.

Assuming the current event is the *i*-th event and the event weight is V_i ($i \in [1,n]$), V_j ($i \neq j$ and $j \in [1,n-1]$) is the maximum event weight in previous events *i-1* so, $V_j = \max\{V_1, V_2, \cdots V_{i-1}\}$, $V_j = 0$ if $i = 1$. Comparing V_j with V_i , we can get two consequences: first, if $V_i \leq V_j$, this means the current event is not more important than past events, and the trust evaluation under high event weight also applies to the event that has low weight. Second, if $V_i \geq V_j$, this means the current event is more important than all past events. The trust evaluation under low event weight does not apply to the event that has high weight, and the current event weight has some influence on the trust evaluation.

Thus, η has the following values:

$$\eta = \begin{cases} V_j / V_i, & V_i > V_j, V_j \neq 0; \\ 1, & V_i \leq V_j or V_j = 0 \end{cases} \tag{11}$$

Trust evaluation after considering the event weight is as follows:

$$\begin{cases} b^1_{A,B} = \eta b_{A,B} \\ d^1_{A,B} = \eta d_{A,B} \\ u^1_{A,B} = 1 - b_{A,B} - d_{A,B} \end{cases} \tag{12}$$

3. Discount calculation. The trust evaluation is discounted after transference. Because of the recommendation of node *B*, the direct trust evaluation between *B* and *T* changes to the indirect trust evaluation of *A* to *T*. Assuming the trust evaluation of node *A* to node *T* is $w^A_T = \{b^A_T, d^A_T, u^A_T\}$ and the discount factor is *M*,

$$\begin{cases} b^A_T = M b_{B,T} \\ d^A_T = M d_{B,T} \\ u^A_T = 1 - b^A_T - d^A_T \end{cases} \tag{13}$$

where $M = E^1_{A,B}$.

In Jøsang's model, the discount factor is b^A_B, which is the belief of node *A* to node *B*. Jøsang thinks that the presence of uncertainty u is caused by the unfinished events or a lack of complete evidence, and *u* will eventually be assigned to *b* or *d* with deepening understanding. If b^A_B is set to be the discount factor, the impact of potential *b* to decision-making is apparently not considered. The expectation value *E* ($E = b + au$) represents the maximum possible credibility between *A* and *B*. It is more reasonable than b as a discount operator.

These views are illustrated by the following comparative examples. Alice and Bob are customers, and Tim is a repairer. There is no trade between Alice and Tim. Bob repaired his car at Tim's, so Alice wants to get the result from Bob before repairing. In scene one, there are failed transaction records between Alice and Bob, so the belief is low from Alice to Bob. In scene two, there are few transaction records between Alice and Bob, and Alice has no clear judgment on Bob, so the uncertainty is high from Alice to Bob. The prior probability *a* is set to be 0.8 for two sets of dates.

Table 2. Comparison of two operators in situation 1

	b	***d***	***u***
Trust evaluation between node *A* and node *B*	0.15	0.80	0.05
Trust evaluation between node *B* and node *T*	0.90	0.10	0
Jøsang's discounting operator	0.135	0.015	0.85
Transfer operator in this work	0.171	0.019	0.81

Table 3. Comparison of two operators in situation 2

	b	***d***	***u***
Trust evaluation between node *A* and node *B*	0.15	0.05	0.80
Trust evaluation between node *B* and node *T*	0.90	0.10	0
Jøsang's discounting operator	0.135	0.015	0.85
Transfer operator in this work	0.711	0.079	0.21

Assume that the trust relationships between node A and node B are different between situations 1 (**Table 2**) and 2 (**Table 3**). In the first situation, the disbelief d is high between node A and node B, and the expectation value is low ($E = b + au = 0.19$). In the second situation, the uncertainty u is high between node A and node B, and the expectation value is high ($E = b + au = 0.79$).

Belief b is high between node B and node T in two situations. In principle，the final belief b of node A to node T should be high. Jøsang's discounting operator does not fit the regular pattern. In addition, the situations of the two groups are different, but the results calculated by Jøsang's discounting operator are the same, which is inconsistent with common sense. The results show that the new operator is reasonable.

3.4.2. Trust aggregation: The impact of event weight is not considered in a consensus operator. To solve this problem, a new aggregate operation is proposed, and three strategies are contained in the new aggregate operator: pessimistic strategy, optimistic strategy, and neutral strategy. See Eqs. (8), (9), and (10).

3.5 Trust renewal

The trust evaluation is updated dynamically as time goes on and as processes interact. Only then can we ensure that the trust evaluation is time sensitive and more in line with reality.

3.5.1. Time decay of trust evaluation: With the passage of time, the trust evaluation of trustor to trustee will decay [20]. The older the trust evaluation, the smaller the impact of this trust evaluation on decision-making. The newer the trust evaluation, the more authentic the trust evaluation, and the greater the impact of this evaluation on decision-making.

The time decay factor in a certain period is set to be λ:

$$\lambda = e^{-k\left\lfloor \frac{t-t_0}{T} \right\rfloor} \tag{14}$$

where k is the regulatory factor to regulate the speed of decay, which is decided by the system, t is the current time, t_0 is the point in time when the trust evaluation is generated, and T is the time period of evaluation, which is decided by the evaluation.

Assuming the trust evaluation of trustor to trustee is $w_0 = \{b_0, d_0, u_0\}$ at time t_0, then the trust evaluation after the decay is $w = \{b, d, u\}$:

$$\begin{cases} b = \lambda b_0 \\ d = \lambda d_0 \\ u = 1 - \lambda(b_0 + d_0) \end{cases} \tag{15}$$

3.5.2. Trust reward and punishment: The direct trust evaluation of trustor to trustee is obtained from direct interaction. The trust evaluation of trustor to recommended entity should also be updated accordingly.

The trust renewal of trustor to trustee is based on the final interaction results. The latest *r* and *s* are obtained after the completion of direct interactions. In this case, the direct trust evaluation of trustor to trustee is obtained based on the mapping function [Formula (2)].

The trust renewal of trustor to recommended entity is also based on the final interaction results. If the interaction results are in the range of expectations, which means the latest r and s satisfy the intervals $(r+s)b \le r \le (r+s)(b+u)$ and $(r+s)d \le s \le (r+s)(d+u)$, then the interaction is successful, and the recommended behaviors that are provided by the recommended entities conform to expectations. At this time, the trustor rewards the recommended entity by the reward factor. If the interaction results deviate from expectations, which means the latest r or s do not satisfy the intervals above, then the interaction is regarded as a failure, and the recommended behaviors that are provided by recommend entities do not conform to expectations. The trustor punishes the recommended entity by the penalty factor.

The trust reward is as follows:

$$\begin{cases} b' = b + u\theta \\ d' = d \\ u' = 1 - b' - d' \end{cases} \tag{16}$$

where the reward factor is θ. The value of θ is a piecewise function, and the segments are divided based on the event weight:

$$\begin{cases} c_1, V \in [0, V_1]; \\ c_2, V \in (V_1, V_2); \\ c_3, V \in [V_2, 1] \end{cases} \tag{17}$$

The values of demarcation points V_1 and V_2 depend on the current system. When $0 \le c_1 < c_2 < c_3 \le 1$, the values of c_1, c_2, and c_3 depend on the system. In general, the higher the event weight, the greater the magnitude of the reward.

The trust punishment is as follows:

$$\begin{cases} b' = b \\ d' = d + u\sigma \\ u' = 1 - b' - d' \end{cases} \tag{18}$$

where the penalty factor is σ, and $\sigma = c_4 a^{(V-1)}$. However, the control factor c_4 is used to control the maximum punishment in the current system, $c_4 \in [0,1]$ and the value of c_4 depend on the system. The regulatory factor a is used to adjust the steepness of the current curve, a is a constant value that depends on the current system, and V is the current event weight. In general, the higher the event weight, the greater the magnitude of punishment.

4. Experiments

The experiments are carried out in a PeerSim simulation environment [21], and some contrast experiments are conducted between DTM-ESL and Jøsang's model. In the experiments, the success rate of interaction and the node expectation value are compared. The number of nodes in the network is set to be 1000, the total number of files is set to be 1000, and the files are distributed on the nodes randomly. The degree (the number of neighbor nodes) of each node is set to be 10, and each interaction downloads files 20 times.

The trustor selects nodes randomly to download the file each time. Dividing the number of success interactions by the total number of interactions constitutes the success rate of this interaction. The parameters and their values are shown in **Table 4**. The parameters under three different weights are set. The weights for the three cases are 0.15, 0.5, and 0.85, respectively. The demarcation points V_1 and V_2 are 0.3 and 0.7 respectively. Select the neutral strategy to analyze the cases, so the values are set $\alpha = \beta = 0.5$. In each case, two sets of reward and penalty factors are set to different values in order to analyze the success rate of interaction in different situations. the regulatory factor k and the time period of evaluation T are set to 1.

Table 4. Parameters and their values

Parameters	V	v_1	v_2	α	β	θ	σ	**k**	**T**
CASE 1	0.15	0.3	0.7	0.5	0.5	0.20	0.30	1	1
						0.15	0.30		
CASE 2	0.5	0.3	0.7	0.5	0.5	0.50	0.40	1	1
						0.45	0.60		
CASE 3	0.85	0.3	0.7	0.5	0.5	0.80	0.60	1	1
						0.75	0.80		

4.1 Analysis of success rate of interaction

First, the impact of the two-way trust relationship and event weight to the success rate of interaction are considered. Using three event weights, the success rate of the interaction changes as the number of interactions increases, as shown in **Fig. 3:**

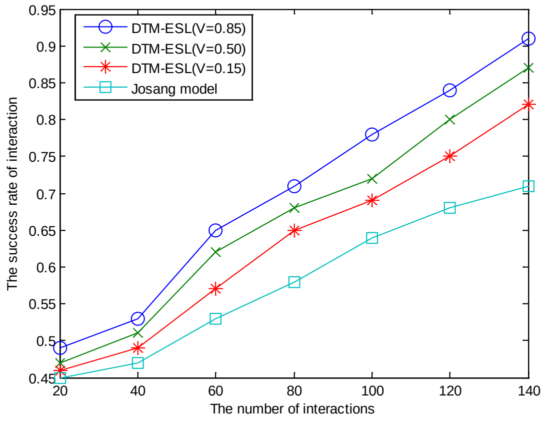

Fig. 3. Success rate of interaction changes as number of interactions increases

As shown above, the success rates of interaction for the two models indicate upward trends as the number of interactions increases, the understanding between nodes becomes deeper, and the uncertainty u becomes smaller. This makes the trust evaluation more in line with the actual situation, and the success rates of interaction of the two models show upward trends. Comparing the success rates of interaction of the two models when the number of interactions is constant, we can see that the DTM-ESL has higher success rates than Jøsang's model. This is because the mutuality and asymmetry of trust is considered in our model, and the original one-way trust relationship is extended to a two-way trust relationship.

Compared with the one-way trust relationship, the relative trust evaluation is more in line with the real situation, so DTM-ESL has a higher success rate than Jøsang's model. An analysis of the DTM-ESL dates indicates that the success rate of interaction is related to the event weight when the number of interactions is constant. The higher the event weight, the higher the success rate of interaction. Because trust renewal is designed in DTM-ESL, the nodes that participate in the recommendation are rewarded or punished according to the results of the interactions. The higher the event weight, the greater the magnitude of reward or punishment that effectively restrains malicious fraud. This gives the nodes that participate in the recommendations high credibility, thus ensuring the recommended information has high credibility. This credibility also guarantees that the DTM-ESL has a higher success rate of interaction than Jøsang's model. **Fig. 4** shows the success rate of interaction changes with the growth of event weight.

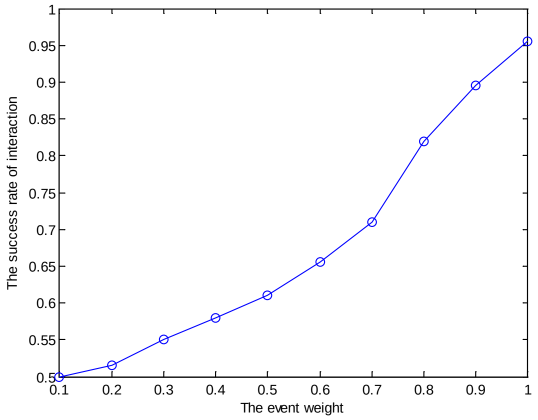

Fig. 4. Success rate of interaction changes as event weight increases

From the analysis of **Fig. 4**, we can see that the success rate of interaction changes with the growth of event weight. This is because the trust renewal in DTM-ESL is designed to ensure that the nodes that prompt the interactions to succeed are rewarded, and the nodes that prompt the interactions to fail are punished, thus effectively eliminating the node with low credibility and ensuring a high success rate of interaction.

When the experiment starts, the curve is flat. With the growth of event weights, the curve steepens because punishment increases with the increase of event weight. This ensures the credibility of nodes that participate in the recommendation becomes higher. Thus, DTM-ESL has a higher success rate of interaction when the event weight is high.

When malicious nodes are present, the comparison of the success rate under three event weights is shown below. We assume the information provided by the malicious nodes does not have full credibility, and that malicious nodes always provide 50% false files. DTM-ESL 1 represents the curve with a smaller reward factor. DTM-ESL 2 represents the curve with a larger reward factor at the same time weight. The results are as follows:

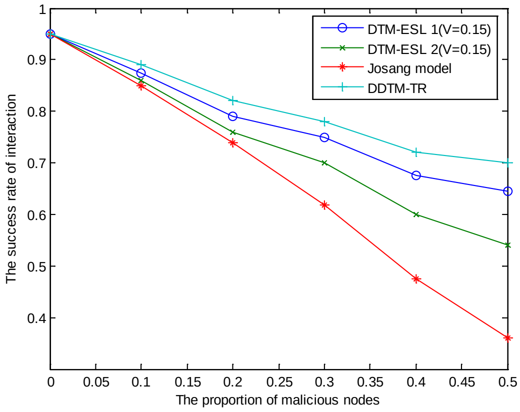

Fig. 5. Success rate of interaction changes with proportion of malicious nodes increasing when V = 0.15

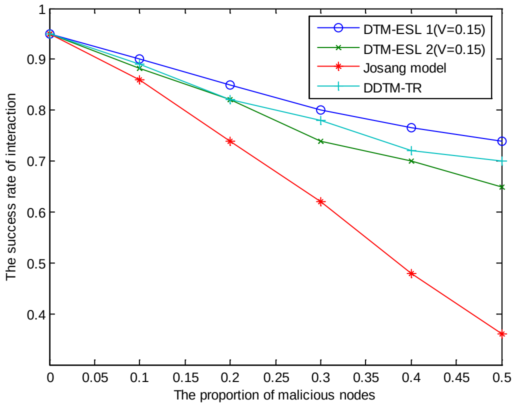

Fig. 6. Success rate of interaction changes with proportion of malicious nodes increasing when V = 0.50

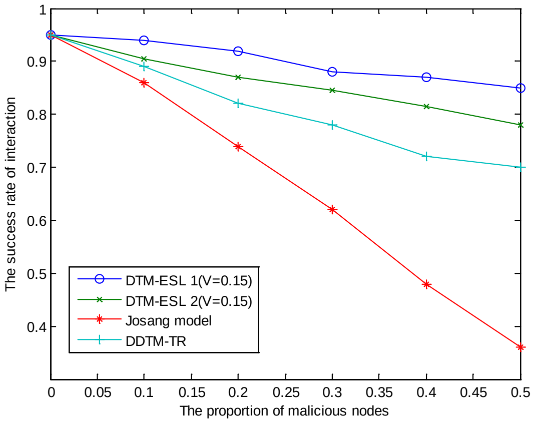

Fig. 7. Success rate of interaction changes with proportion of malicious nodes increasing when V = 0.85

From the analysis of **Figs. 5-7**, we can see that all trust models have a high success rate of interaction when the ratio of malicious nodes is close to zero. This is because all nodes in the network are trusted to provide authentic files at this time, and the recommended information has high credibility. With an increase in the proportion of malicious nodes, the success rate of interaction shows downward trends, and the trend of decline for Jøsang's model is larger than that for DTM-ESL.

Because the punishment for malicious nodes is not considered in Jøsang's model, some malicious nodes continue to provide services in following interactions even though they prompted the interactions to fail in previous interactions, thus causing repeated failures of interactions. By contrast, trust renewal is designed in DTM-ESL, and trust evaluation is updated according to the interaction results. The recommended nodes that promote interactions to succeed are rewarded to give them a high credibility, and the recommended nodes that promote interactions to fail are punished to reduce their credibility.

Through trust renewal, malicious nodes are effectively removed. The credibility of recommended information and the authenticity of services are ensured, thus giving DTM-ESL a high success rate of interaction. Through analysis of the impact of reward and penalty factors in DTM-ESL, we can see that when the event weight is constant, the greater the punishment and the higher the success rate of interaction. Because punishment makes the nodes that provide services have high accuracy, services have a high success rate of interaction. Through the calculation and analysis of credibility, the DDTM-DR model filters some malicious recommendation or outdated direct experience. After the interaction ends, the model adjusts and updates the trust through the feedback algorithm in order to further improve the reliability of the follow-up trust evaluation, but did not consider the impact of events weight. Comparing the four models, we illustrate that when the malicious nodes are at a certain proportion (the ratio is greater than 0), the success rate of interaction is related to the event weight. The higher the event weight, the higher the success rate of interaction because when the event weight is high, the trust evaluation between nodes is cautious, which is more in line with the actual situation.

4.2. Analysis of node's expectation value

When the reward factor θ is 0.20 and the penalty factor σ is 0.60 in the simulation experiments, we randomly tag the nodes whose initial expectation value is 0.50. The expectation values of these nodes are recorded in the following interactions. After repeated experiments, the expectation values of the tagged nodes present the following four trends:

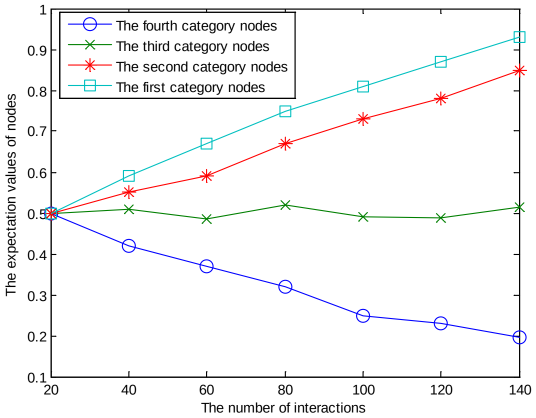

Fig. 8. Expectation value changes with number of interactions increasing

With analysis of **Fig. 8**, we can see that the expectation value of first category nodes grows when the number of interactions increases, and the growth is rapid. The expectation value of the second category nodes grows when the number of interactions increases, but the trend of growth is more gentle than for the first category nodes. The expectation value of the third category nodes presents a fluctuating trend. The expectation value of the fourth category nodes rapidly falls. This is because trust renewal is designed in DTM-ESL, which ensures that the nodes that prompt interactions to succeed are rewarded, and the nodes that prompt interactions to fail are punished. This distinguishes the four categories of nodes and prevents malicious fraud.

In the simulation experiments, we tag the nodes randomly whose initial expectation value is 0.70, and the expectation values of tagged nodes are recorded over time. In the experiments, the time interval is set to be T. The interactions fail owing to malicious fraud in the fifth time period, while interactions succeed in the rest of the time periods. **Fig. 9** shows the expectation value of tagged nodes changing for DTM-ESL and Jøsang.

First, with the analysis of dates, we can see that the four curves show upward trends during the first four time periods, and that the trends are flat. Three curves for DTM-ESL show downward trends in the fifth period, and the trends are steep. This is because trust renewal is designed in DTM-ESL, which ensures that the nodes that prompt interactions to succeed can be rewarded, and the nodes that prompt interactions to fail can be punished, so the curves present the above trends.

When the event weight is constant, based on the functions of reward and penalty factors, the magnitude of punishment from the failed interaction is much larger than the magnitude of reward from the successful interaction. This is why the downward trend is more precipitous than the upward trend in these curves.

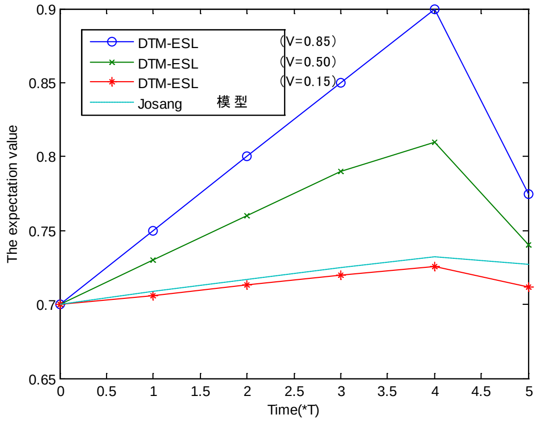

Fig. 9. Expectation value changes over time

Second, comparing the three curves at the same time, we see that the magnitude of change in expectation value is related to the event weight. The higher the event weight, the greater the corresponding magnitude of change. This is because according to the functions of the reward and penalty factors, the magnitude of change for the expectation value is related to the current event weight. When the event weight is high, a failed interaction has a dramatic impact on the nodes, resulting in a sharp decrease in credibility between nodes, so the current trust evaluation is more cautious. When the event weight is low, a failed interaction may have an impact on the nodes, but the impact is less than when the event weight is high.

Third, compared with the other three curves, we can see that the curve of Jøsang is close to the curve of DTM-ESL (V = 0.15) during the first four time periods, but Jøsang's curve drops slowly in the fifth period. This is because for Jøsang's model, If the interaction fails, just let the number of positive events increase by one, which makes expectation value change smaller.

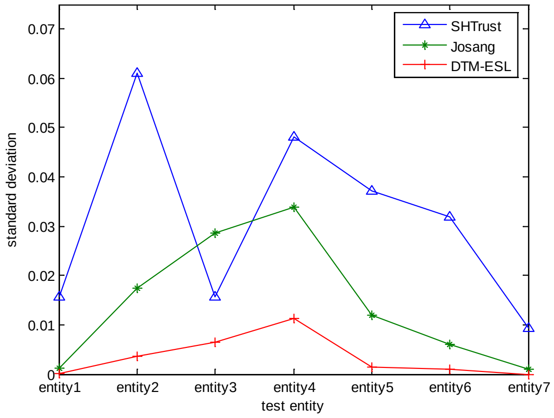

Fig. 10. Standard deviation of expectation value

The paper analyzes seven entities given by the SHTrust model. From entity 1 to entity 7, the trust value becomes lower and lower. Using the data given by the SHTrust model, **Fig. 10** gets the expectation value of each entity for the SHTrust model, Jøsang model, and DTM-ESL model after a period of time. The smaller the standard deviation, the higher the accuracy of the predicted results. As shown in **Fig. 10**, the standard deviation of the trust value of the DTM-ESL model is significantly smaller than the standard deviation of the other two models.

Under normal circumstances, the greater the impact of events, the greater the weight. The greater the weight of the event, the greater the rate of rewards and punishments. In addition, most of the invaders will choose important events to invade. The reward and punishment of important events is large, so the expectation value of each entity quickly achieve stability with the progress of the interaction.

4.3. model's analysis of time complexity and computational cost

The time complexity of trust network search is determined by the size of the network nodes participating in the recommendation and the complexity of the path. Assuming that the total number of nodes in the current trust network is X and its expected value is a normal distribution of N (0.5, σ^2).If the weight of the event is V (0.5 <V <1), the proportion of the number of nodes whose expected value is greater than the event weight V is $f(v)=1-\Phi(\frac{V-0.5}{\sigma})=1-\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{V} e^{-\frac{(t-0.5)^2}{2\sigma^2}}dt$ .Under the weight of this event, the size of network nodes participating in the general algorithm is X.

The dynamic trust model based on extended subjective logic adopts double threshold screening strategy, the size of network nodes participating in the general algorithm is f(V)X. The comparison of the two figures shows that the double-threshold strategy set by this algorithm reduces the number of nodes under the high event weight, and then the network size becomes smaller.

Assuming that each node in the trust network has N neighbor nodes, the neighbor nodes whose weight is greater than the current event are O(*Nf (v))*, and the average depth of the trust network is L. The neighbor node of each node in the general algorithm should accept the request, So its time complexity is NL. Dynamic trust network search algorithm based on extended subjective logic first filter nodes, so the time complexity is O((*Nf (v)*) $^{L)}$. The comparison of two figures shows that the trust network search algorithm based on extended subjective logic has lower time complexity than the general algorithm.

The search behavior of the trust network recommendation relationship is an important reason for the computational cost of the model. The more nodes that provide recommendations in the trust network, the greater the computational cost. Therefore, it is very important to simplify the network recommendation relationship reasonably and effectively.

As shown in **Fig. 11**, it is the comparison of the computational cost of each model with different event weights when the total number of nodes is constant.

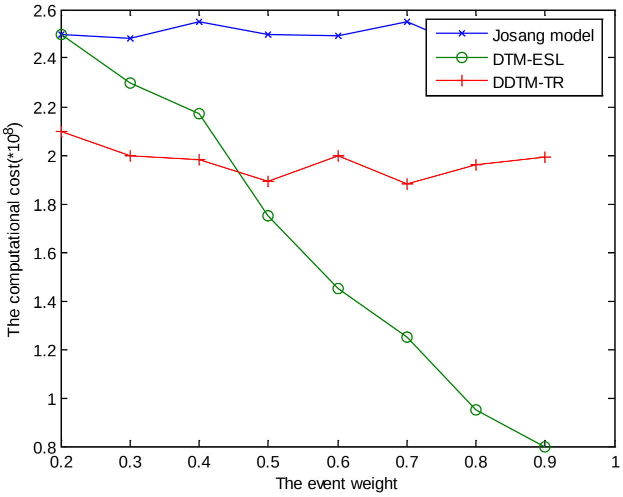

Fig. 11. The impact of event weight on cost.

the impact of event weight on trust evaluation is not reflected in Jøsang's model. Therefore, it relies only on the historical trust evaluation to determine whether the nodes are involved in the interaction in Jøsang's model. In the DDTM-TR model, calculating the recommended trust using only locally stored recommendations and a limited number of recommended nodes greatly reduces computational cost. However, the model does not consider the impact of event weights. In the DTM-ESL model, it is considered that nodes with lower historical trust evaluation cannot provide reliable recommendation information as the weight of events increases, and such nodes no longer have the recommended qualifications. The double threshold screening strategy ensures that all nodes that provide recommendations are highly reliable. The higher the event weight, the fewer the nodes that provide recommendations, and the simpler the recommendation relationship of the corresponding trust network, which not only ensures the high credibility of the recommended behavior but also effectively suppresses the malicious node's recommendation behavior. The final trust evaluation is more in line with the actual situation, but also reduces the calculation overhead.

5. Conclusion

In this paper, the traditional one-way trust relationship in Jøsang's model is extended to a two-way trust relationship, and three trust strategies concerning the relative trust evaluation between two nodes are presented. A new trust model (DTM-ESL) based on extended subjective logic is proposed. In DTM-ESL, the impact of event weight is fully considered, the original operators are improved, and a trust renewal process is designed. The validity of the new model is verified by simulation experiments. To achieve higher accuracy, we will further focus on the setting of related parameters.

References

[1] Azzedin F, Maheswaran M, "Towards trust-aware resource management in grid computing systems," in *Proc. of Cluster Computing and the Grid, 2002. 2nd IEEE/ACM International Symposium on. IEEE*, pp.452-452, 2002. Article (CrossRef Link).

[2] William E. Burr, "Public Key Infrastructure (PKI) Technical Specifications Part A: Technical Concept of Options," in *http://csrc/nist.gov/nist.gov/pki/twg/baseline/pkicon20b.pdf*, 1998. Article (CrossRef Link).

[3] Linn J, "Trust models and management in public-key infrastructures," in *RSA Laboratories*, pp.20, 2000. Article (CrossRef Link).

[4] M. Blaze, J. Feigenbaum and J. Lacy, "Decentralized trust management," in *Proc. of Proceedings of the 17th Symposium on Security and Privacy. Oakland, CA: IEEE Computer Society Press*, pp.164-173, 1996. Article (CrossRef Link).

[5] Abdul-Rahman A, Hailes S, "A distributed trust model," in *Proc. of Proceedings of the 1997 workshop on New security paradigms*， pp. 48-60, 1998. Article (CrossRef Link).

[6] Li D F, Yang Y X and Gu L Z, "Study on dynamic trust metric of trusted network based on state and behavior associated," *Journal on Communications*, pp.12-19, 2011. Article (CrossRef Link).

[7] Tian C Q, Jiang J H and Hu Z G, "A Novel Super-peer Based Trust Model for Peer-to-Peer Networks," *Chinese Journal of Computers*, pp: 345-355, 2010. Article (CrossRef Link).

[8] Wang S X, Zhang L and Li H S, "An Evaluation Approach of Subjective Trust Based on Cloud Model," *Journal of Software*, pp.1341-1352,2010. Article (CrossRef Link).

[9] Jiang J, Han G, Wang F, "An efficient distributed trust model for wireless sensor networks," *IEEE Trans on Parallel and Distributed Systems*, 2015, 26(5):1228-1237. Article (CrossRef Link).

[10] Jøsang A, Costa P C G and Blasch E, "Determining model correctness for situations of belief fusion," in *Proc. of Information Fusion (FUSION), 2013 16th International Conference on. IEEE*, pp. 1886-1893, 2013. Article (CrossRef Link).

[11] Jøsang A, "Subjective logic," *Book Draft*, 2011. Article (CrossRef Link).

[12] Jøsang A, Guo G and Pini M S, "Combining Recommender and Reputation Systems to Produce Better Online Advice," in *Proc. of The 11th International Conference on Privacy, Security and Trust*, pp.10-12, 2013. Article (CrossRef Link).

[13] Jøsang A, "Multi-Agent Preference Combination using Subjective Logic," in *Proc. of 11th Workshop on Preferences and Soft Constraints*, pp.61, 2011. Article (CrossRef Link).

[14] Jøsang A, Aždersk a T, Marsh S, "Trust Transitivity and Conditional Belief Reasoning," *Trust Management VI*, pp.68-83, 2012. Article (CrossRef Link).

[15] Jøsang A, "The consensus operator for combining beliefs," *Artificial Intelligence*, pp. 157-170, 2002. Article (CrossRef Link).

[16] Feng R, Han X, Liu Q, et al. "A credible bayesian-based trust management scheme for wireless sensor networks," *International Journal of Distributed Sensor Networks*, 2015(2): 1-9, 2015. Article (CrossRef Link).

[17] W Liu，Z Dai，Y Gao, “Distributed dynamic trust management model based on trust reliability,” *Journal of Sichuan University*, 46 (4), pp. 61-66, 2014. Article (CrossRef Link).
[18] Jiang Q, Liu L L and Su X, “Test path generation approach for GUI based on event weight,” *Journal of Computer Applications*, pp.1382-1384, 2009. Article (CrossRef Link).
[19] Jøsang A, Bhuiyan T, “Optimal trust network analysis with subjective logic,” in *Proc. of Emerging Security Information, Systems and Technologies, 2008. SECURWARE'08. Second International Conference on. IEEE*, pp.179-184, 2008. Article (CrossRef Link).
[20] Shi Z G, Liu J W and Wang Z L, “Dynamic P2P trust model based on time-window feedback mechanism,” *Journal on Communications*, pp.120-129, 2010. Article (CrossRef Link).
[21] http://peersim.sourceforge.net/

Tian Junfeng was born in 1965. He received the Ph.D. degree from China University of Technology. He is now a Ph.D. candidate of Hebei University. His research interests include information security and trusted computing.

Zhang Jiayao (corresponding author) was born in 1991. He is a master graduate student of Hebei University. His research interests include cloud computing and trusted computing. (Email: 2218624065@qq.com)

Zhang Peipei was born in 1989. She received the master degree in Hebei University. Her research interests include Information security and trusted computing.

Ma Xiaoxue was born in 1974.She received the master degree in Hebei University. Her research interest is network technique.