Dynamic trust evaluation model based on bidding and multi-attributes for social networks

Gang Wang*

Department of Computer Science and Technology,
Xi'an University of Finance and Economics,
No. 2 Weichang Road,
Chang'an District, Xi'an, 710100, China
and
Institute for Cyber Security,
University of Texas at San Antonio,
NPB 3.122, UTSA Main Campus,
San Antonio, TX 78249, Texas, USA
Email: wg.only@gmail.com
*Corresponding author

Jaehong Park

College of Business Administration,
University of Alabama in Huntsville,
301 Sparkman Drive, Huntsville, AL 35899, USA
Email: jae.park@uah.edu

Ravi Sandhu

Institute for Cyber Security,
University of Texas at San Antonio,
NPB 3.122, UTSA Main Campus,
San Antonio, TX 78249, Texas, USA
Email: ravi.sandhu@utsa.edu

Jun Wang

Department of Electronic Commerce,
Xi'an University of Finance and Economics,
No. 2 Weichang Road, Chang'an District, Xi'an, 710100, China
Email: wj1229@vip.163.com

Xiaolin Gui

Department of Electronics and Information Engineering,
Xi'an Jiaotong University,
No. 28 Xian ning Road, Xi'an, 710049, China
Email: xlgui@mail.xjtu.edu.cn

Abstract: Mutual trust is the most important basis in social networks. However, many malicious nodes often deceive, collaboratively cheat, and maliciously recommend other nodes for getting the more benefits. Meanwhile, because of lacking effective incentive strategy, many nodes are neither to evaluate nor to recommend. Thus, malicious actions have been aggravated in social networks. To solve these issues, we designed a bidding strategy to incentivise nodes to do their best to recommend or evaluate service node. At the same time, we also employed TOPSIS method of selecting a correct service node for system from networks. To guarantee reliability of service node selected, we brought recommendation time influential function, service content similarity function and recommendation acquaintance function into the model to compute general trust of node. Finally, we gave an update method for trust degree of node and experiments analysis.

Keywords: dynamic trust; trust evaluation model; bid; multi-attributes; TOPSIS; information entropy; recommendation trust; direct trust; Markov chain.

Reference to this paper should be made as follows: Wang, G., Park, J., Sandhu, R., Wang, J. and Gui, X. (2019) 'Dynamic trust evaluation model based on bidding and multi-attributes for social networks', *Int. J. High Performance Computing and Networking*, Vol. 13, No. 4, pp.436–454.

Biographical notes: Gang Wang works as an Associate Professor in the Xi'an University of Finance and Economics. He received his PhD in Computer Science and Technology from the Xi'an Jiaotong University in 2013. He worked as a Visiting Scholar in the University of Texas at San Antonio, July 2015 to July 2016. His current research interests include trust management, privacy security and social networks computing, cloud computing and internet of things.

Jaehong Park works as an Associate Professor in the University of Alabama in Huntsville, Alabama, USA. He received his PhD in Information Technology from the George Mason University. His research interests include data and application security and privacy, access and usage control, cloud computing security, secure provenance and social computing.

Ravi Sandhu is the Founding Executive Director of the Institute for Cyber Security at the University of Texas San Antonio, and holds an Endowed Chair. He is an ACM, IEEE and AAAS Fellow and inventor on 29 patents. He is past Editor-in-Chief of the *IEEE Transactions on Dependable and Secure Computing*, past founding Editor-in-Chief of *ACM Transactions on Information and System Security* and a past Chair of ACM SIGSAC. He founded ACM CCS, SACMAT and CODASPY, and has been a leader in numerous other security conferences. His research has focused on security models and architectures, including the seminal role-based access control model. His papers have accumulated over 26,000 Google Scholar citations, including over 6,400 citations for the RBAC96 paper.

Jun Wang works in the Xi'an University of Finance and Economics. He received his PhD in Northwestern Polytechnical University in China. He received his PhD degree in Computer Science and Technology from Northwestern Polytechnical University in 2011. His current research interests include strategic management and incentive to innovation.

Xiaolin Gui works as a Professor in the Xi'an Jiaotong University. He received his PhD in Xi'an Jiaotong University. He received hid PhD degree in Computer Science and Technology from Xi'an Jiaotong University in 2001. His current research interests include dynamic trust management theory, cloud computing and internet of things.

1 Introduction

With the boom and flourish of social networks, mutual trust has become one of prerequisites of all services in social networks. Because the establishment of trust relationship is a complicated and progressive process which includes interaction history, service contents, trustworthy recommendation, trust management (TM), emotion and psychology, etc., TM system must also be a complex system of involving multi-factors. Therefore, how to build a completed trust evaluation model becomes one of the most important works for the current social networks.

However, we met a series of serious issues in process of trust relationship building on social networks. Firstly, many nodes are neither to evaluate quality of service of service nodes, nor to recommend right service nodes for system after service finished because of the lack of effective incentive strategy. Secondly, because there is related benefits relationship among a few nodes, these nodes often cheat collaboratively and recommend maliciously, for example, many nodes combine or consult each other in private for improving their trust degree or get more rewards in order to get more service chances and extra-rewards. So it is worth asking whether their recommendation is credibility. Thirdly, it is a difficult thing for system to select a right service node from a lot of cyber service nodes.

In this paper, we established a trust evaluation model based on bidding and multi-attributes for social networks. We firstly designed a bidding strategy so as to incentivise cyber nodes to evaluate and recommend other right nodes actively. In this way, nodes' enthusiasm will be activated enough and these participants will also get corresponding rewards, more service resources and chances. In the meantime, we employed TOPSIS method as selecting right service node in order to overcome the defect of randomly selecting service nodes in past trust models, in which we used entropy weight to insure that selecting service attributes are objective and accurate. Moreover, system can compute the best order of service nodes by TOPSIS. In addition, the accuracy of node selected is ensured by the credibility of node service. To assure the credibility of node service, we brought recommendation time influential function, service content similarity function and recommendation acquaintance function into the model for computing general trust of nodes. Besides these, we also proposed an updating method of recommendation trust based on multi-attributions.

The rest of the paper is organised as follows. Section 2 reviews the recent researches in this field. Sections 3 and 4 discuss bidding strategy, trust computation model and selection method of service node based on entropy weight and TOPSIS. Section 5 is comprehensive trust computation

of service nodes and the credibility evaluation of node recommended. Section 6 gives updating method of recommendation trust. Section 7 is to simulate experiments and results analysis. Finally, conclusions are drawn in Section 8.

2 Relate works

TM, firstly proposed by Blaze et al. (1996), is aimed at solving trust issues in large-scale distributed computing. Later, the corresponding TM system PolicyMaker and KeyNote (Blaze et al., 1998) were designed on this basis.

Sabater and Sierra (2001) proposed a trust system called *REGRET* which computes the final trust value of nodes by integrating varied reputation with a graded ontology structure and social networks analysis.

Gan et al. (2011) proposed a multi-dimensionalities reputation computing method in electronic commerce by dividing trust into four dimensions and building utility function as one of the computing direct trust weight. Meanwhile, distinguishing recommendation trustworthiness and scale of recommendation nodes by relationship between recommendation nodes improves accuracy and objectivity of trust computing. However, the trustworthiness of recommendation is hardly fixed because of the lack of comparison of recommendation transaction contents and the lack of rewards and punishment mechanism probably leads to the embryo of oligarchy.

Al-Oufi et al. (2012) proposed a group trust metric for identifying people of trust in online social networks in which evaluating method was from Advogato (http://www.advogato.org/) evaluated credibility of individual user in online social networks. Unlike Advogato method, that authors' method extended Advogato looked for the trustable users of each individual in social networks by integrating social relationship. While the extended trust measure propagation mechanism disseminated the capability of each node along a chain of social connections into successive nodes and designed capacity-first maximum flow in order to identify local trusted users and rank them in their trust level. Meanwhile, a sequential reliable user set was setup to block distrusted users to access personal network and so as to protect personal information.

Kim and Phalak (2012) proposed a trust prediction framework in rating-based experience sharing social networks without a web of trust. Authors adopted the Rigg's algorithm to compute quality of service content and the user's trust degree of providing content because the clarity trust rank for credible websites is not always useful and is typically sparse.

Zolfaghar and Abdollah (2011) proposed evolution of trust networks in social web applications using supervised learning. In order to predict the probability of trust relationship, the paper maps the current issue on formal link prediction problem and solves it with supervised learning. Although exponential functions were adopted in computing time weight in the model, the method lacked powerful support of theory. Jiang et al. (2012) proposed a SWTrust trustworthiness framework, instead of a complete trust evaluating model, which computes a trust graph in a large-scale online social networks and incorporates it in current trust model to enhance validation and practicality of trust model.

Zhan and Fang (2011) proposed a novel computing method through incorporating three different components: profile similarity, information reliability, and social opinions. Whether the user is trustworthy depends on fusing computing of above-mentioned three components in networks, but how to determine the weight of the three components lacks theory foundations and proofs.

Chen et al. (2009) proposed a bidding idea to improve trust query efficiency and trust-updating method of recommending nodes, which mainly adopted idea of the subjective logic-based trust model proposed by Jøsang (2001). This model decided trust degree of object evaluated with three standards of credibility, incredibility and uncertainty by imported uncertain factors in evaluating experience. However, because there is not the explicit incentive strategy in bidding mechanism, many nodes are unwilling to do their best to bid. Meanwhile, system could not distinguish which recommendation is credible and which is not because of lacking evaluation for credibility of recommendation.

EigenRep model is a typical global reputation model that specifies the trust computing under the P2P environment (Kamvar and Schlosser, 2003). Dou et al. (2004) proposed a global trust model that is intended to avoid the lack of security consideration in *EigenRep* Model, for instance, feigning, slandering and lack of punitive measures. Meanwhile, this model effectively solves the problem of trust recommendation.

Wang et al. (2008) proposed a new trust model under the P2P e-commerce environment, which accelerates the direct trust by voting, in other words, stimulating nodes to vote positively to improve the reliability of trust. Zhang et al. (2006) discussed the dependent and restrictive relationship of between resource incentive mechanism and distribution mechanism, and proposed self-adaptive trust-incentive resource distribution mechanism in the view of economics and trust. Zhang et al. (2006) proposed dynamic value adjustment strategy of resource providers in the light of economics-based general equilibrium theory, and self-adaptive trust-incentive distribution strategy was drawn up according to supply and demand and load of current resource status.

Wang et al. (2010) proposed a trust model based on transaction content similarity, and the model represents the trust degree of recommendation by taking advantage of service content similarity, and improved the reliability of trust recommendation. Due to the absence of appropriate incentive and punishment mechanism, there were still defects in reducing malicious recommendation.

Amoretti and Zanichelli (2016) proposed a distributed reputation management system for service-oriented P2P networks, which exploits voting and effectively copes with trust misrepresentation attempts.

Wang and Wu (2011) proposed a TM called *MeTrust* which can ensure the judgment from trust characteristic aspect by dividing influential evidence of trust into three different layers: node layer, path layer and graphic layer.

A few trust models adopted multi-dimension trustworthiness evaluation method (Blaze et al., 1996; Sabater and Sierra, 2001; Dou et al., 2004; Denko et al., 2011; Griffiths, 2005; Wang et al., 2007) which had certain effect on refraining malicious cheat, but system could randomly select service nodes from networks just and efficiency was so low. At the same time, the incompletion of trust analysis and computation method led poor efficiency in restraining malicious recommendation and malicious collaboratively recommendation, and updating recommendation trust.

From analysed above, we found there are four general issues in the current method of trust evaluation as follows:

1 The past trust models ignored how to select an appropriated service node in a large-scale social networks, as the past general practice, they randomly selected service nodes and assessed these nodes in experiments, but which did not agree with the reality.

2 The existing models seldom assessed service recommendation nodes, and assumed that recommendation of the higher trust is more trustworthy. But actually trustworthiness of recommendation could not be ensured.

3 In the networks, the recommending credibility of node does not equal to service credibility of node, but the trust models do not distinguish between them.

4 The current trust models lacked effective incentive strategies and methods to guarantee enthusiasm of recommending nodes. As the time elapsed, it leads that nodes loss the interest of recommendation and the scale of recommendation is gradually shrinking, which causes large deviation of recommendation trust computing and cannot assure the objectivity and accuracy of recommendation, and then this will affect comprehensive trust computing of nodes.

To solve these issues, we proposed a new trust evaluation model.

3 Trust evaluation model based on bidding and multi-attributes

3.1 Structure of trust evaluation model

We firstly give a structure of trust model in Figure 1.

The framework consists of four sections in which the part (1) represents bidding process of service nodes; the part (2) represents selection of ideal service nodes; the part (3) is to compute recommendation trust (3-1), which gets comprehensive trust value of service nodes (3-2) by fusing direct trust and recommendation trust with service influence function of including multi-attributes; the part (4) is the updating computation of recommendation trust for recommendation nodes.

Figure 1 Structure of trust evaluation model for service nodes (see online version for colours)

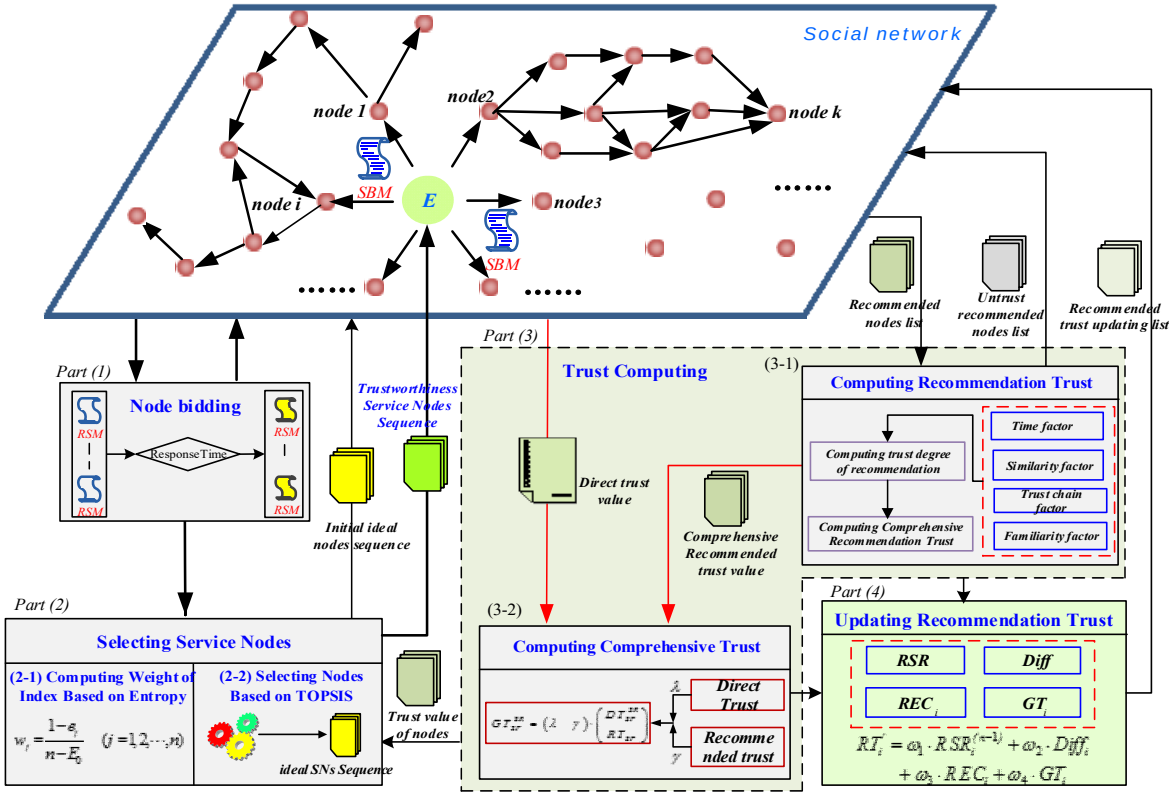
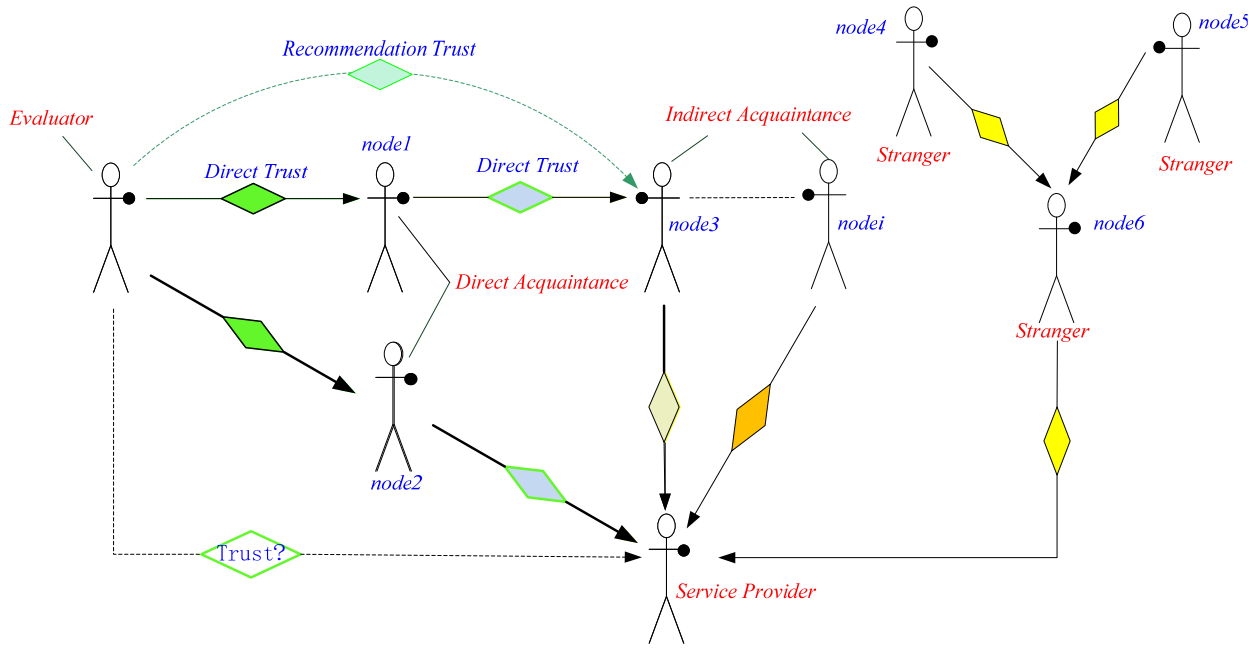


Figure 2 Trust relationship between recommendation nodes (see online version for colours)



The logical relationship of the four parts is described as follows, firstly, evaluation nodes, VIZ. resource request nodes, send request information, the others will respond after they receive request information of evaluation nodes in social networks, and replying nodes complete bidding in part (1), so that inappropriate bidding nodes will be gotten rid of. Secondly, part (2) selects interactive node sequence by evaluating candidates and make an announcement of the node set. Thirdly, part (3) computes trust degree of selected nodes and obtains ideal interaction nodes. Finally, part (4) is responsible for updating and maintaining of trust recommendation.

The paper firstly introduces several concepts as follows:

Definition 1: Service provider, also known as target node or service node, refers to the node which provides resource service, and its trustworthiness will be evaluated by service requestor in social networks, denoted by SP.

Definition 2: Service recommendation node refers to the node which provides recommendation of service source for the service requestor in social networks in order to gain related economic interests and trust degree, denoted by SR.

Definition 3: Service requestor, also known as evaluator, is the node which evaluates trust of service provider in social networks, denoted by *E*.

Meanwhile, in order to easily understand formulas mentioned later, we use formalisation method to represent interaction among nodes, which is detailed as follows, when node *i* interacts with node *j*, where we use X_j^i, where *X* is direct trust or interaction content *C*, etc., represents their relationship, e.g., DT_{SP}^E represents the trust value according to interaction history between evaluator *E* and service provider *SP*, the same as others.

From the view of behaviour cognitive, that we find that reliability and credibility of recommendation depend on familiarity between recommendation and evaluating nodes to a great extent. Thus, if there exists direct interaction experience between recommending and evaluating nodes, their recommending reliability is usually higher than reliability of recommending nodes without direct interaction experience, i.e., reliability of acquaintance recommendation is higher than stranger's reliability, and reliability of direct acquaintance recommendation is higher than indirect acquaintance's reliability. So it forms a trust recommending chain among evaluating node, recommending node and service node in social networks. Meanwhile, the closer recommending node is to evaluating node, the more trustworthy recommending node is (Lou and Dai, 2015).

In Figure 2, *node 1* and *node 2* are called direct recommendation nodes; *node 3* is called indirect recommendation node; *node 4*, *node 5* and *6* are un-acquaintance recommendation nodes. In consideration of human cognition, the evaluation is dependent on acquaintance degree between service nodes and evaluating nodes to a certain extent. In other words, the recommendation from *node 1* usually has higher credibility than *node 4*, *node 5* and *6*, and is even higher than *node 3* and *node i*.

From the perspective of social value, for aiming to get benefits from social activities no matter what nodes are malicious or not (assuming that all nodes in networks are rational nodes). Taking this into account, we introduced bidding method to guarantee higher interests of normal service than the interests of abnormal service (here, we have two classes of the resource service and the recommendation service). The rewards as bidding include two parts of gaining payments and reputation. The former is equivalent to 'hard incentive system' and the latter refers to 'soft

incentive system' (Zhang et al., 2006). With the bidding method, the incentivised nodes can do their best to do services for networks.

Therefore, we defined the related concepts as follows:

Definition 4: Service bidding messages (SBM) is defined as the following tetrad.

$$\boldsymbol{SBM} = (Evaluator\_ID, ServiceContents, TimeStrap, \mathrm{Re}ward)$$

Among this, *Evaluator_ID* is equivalent to evaluating node; *ServiceContents* is the content of service and *TimeStarp* is the bidding-time window. *Reward* is a benefit to resource nodes and recommendation nodes after service, which consists of two aspects, the rewards and the trust evaluation. On the contrary, the phony recommendation and service nodes have to take the consequences.

Definition 5: Resource service messages (RSM) is defined as the following triple.

$$\boldsymbol{RSM} = (Resource\_Service\_ID, ServiceContents, Response\_Time)$$

Among this, *Resourece_Service_ID* is equivalent to resource service bidding node; *ServiceContents* is content of service and *ResponseTime* is response time.

3.2 Bidding strategy and trust evaluation algorithm

Our bidding strategy and trust evaluation algorithm are as follows.

Input: Initialise network nodes

Output: a list of trusted nodes and a list of excellent recommendation nodes

Step 1 The evaluator sends service bidding messages (SBM) and receives the resource service application from resource nodes in return. Then system starts preliminary screening with the SBM conditions and acquires the corresponding resource service node sequence $SP_1 > SP_2 > \cdots > SP_n$.

Step 2 Making an announcement of the bidding node sequence $SP_1 > SP_2 > \cdots > SP_n$ fed back to the network and recommending nodes according to sequence.

Step 3 Evaluating the bidding nodes' entropy weight from the announcement and arranging them by TOPSIS method. Then system will get the corresponding sequence in quality order like $SP_1' > SP_2' > \cdots > SP_n'$.

Step 4 Computing the recommended nodes in four dimensions, by fusing their recommendation trust getting the comprehensive recommendation trust value $\overline{\boldsymbol{RT}_i}$ $(i = 1, 2, \cdots, n)$.

Step 5 Computing Comprehensive Trust by Fusing Recommendation Trust $\overline{\boldsymbol{RT}_i}$ $(i = 1, 2, \cdots, n)$ and Direct Trust $\boldsymbol{DT}_i$ $(i = 1, 2, \cdots, n)$. And then system selects the most trustworthy node from the global trust value $\boldsymbol{GT}_i$ $(i = 1, 2, \cdots, n)$ as the target node according to Comprehensive Trust value.

Step 6 After the interaction between evaluation nodes and service nodes finished, system will update the trust value of recommendation nodes according to four key attributes which are respectively the probability of service success, the evolutionary level of recommendation capability, the trustworthiness itself, and the divergence of between the comprehensive recommendation value and the trustworthy value of target node R_τ^i. At the same time, system will release an announcement of a list of untrust recommendation nodes to networks.

4 Selection method of service node based on entropy weight and TOPSIS

4.1 Information entropy of evaluation indexes

Supposing that there are m bidding nodes and n evaluators, we have y_{ij} for the j^{th} evaluation value of the i^{th} bidding nodes, then we represent the evaluation value matrix of evaluation node as $\boldsymbol{Y} = (y_{ij})_{m\times n}$. Considering that dimension of each index value is different in the matrix, we standardise the value as formula (1),

$$d_{ij} = \frac{y_{ij}}{\sqrt{\sum_{i=1}^{m} y_{ij}^2}} \quad (i = 1, 2, \cdots, m;\ j = 1, 2, \cdots, n) \tag{1}$$

Information entropy value of j^{th} index of the evaluation matrix Y is:

$$e_j = -k \sum d_{ij} \ln d_{ij} \quad (j = 1, 2, \cdots, n) \tag{2}$$

Let $k = 1/\ln m$, while the number of resource bidding nodes is certain, k will be a constant in order to guarantee $0 \le e_j \le 1$.

The general entropy is $E_0 = \sum_{i=1}^{n} e_j$, we define the deviation of j^{th} index as formula (3),

$$h_j = 1 - e_j \quad (j = 1, 2, \cdots, n) \tag{3}$$

From the entropy weight method we know information that evaluation algorithm with a higher deviation and a lower entropy weight provides is the more effective. Meanwhile, we would pay more attention when there is obvious difference among the evaluating algorithms. The higher an indicator's entropy value is, the smaller the difference among evaluating methods is for the indicator, at the same time, the smaller influence to evaluation result is. Hence, the weight factor of the j^{th} indicator can be defined as follows:

$$w_j = \frac{1 - e_j}{n - E_0} \quad (j = 1, 2, \cdots, n) \tag{4}$$

From formula (2)~(4) and the entropy core, we concluded that the entropy value e_j reaches a maximum when $d_{i1} = d_{i2} = \ldots = d_{in}$. At the same time, $w_j = 0$ means the j^{th} index does

not provide any information about nodes *SP* to nodes *E*. Thus, we remove the index.

4.2 Selecting bidding nodes with TOPSIS method

TOPSIS (Hwang and Yoon, 1981) method is a simple and efficacious multi-attributions comprehensive evaluation method which evaluates the quality of finite objects and sorts them according to the closeness degree between current object and ideal targets. Its principle is if there are the shortest distance between evaluating object and optimum solution and the longest distance between evaluating object and the worst solution, the object is the best choice, and vice versa. Among this, value of each index of the ideal solution is the best value of the current evaluating index, and vice versa.

If there exists *m* bidding nodes and *n* evaluating indexes, we define an evaluating index decision matrix $Y = (y_{ij})_{m\times n}$ and weighted normal decision matrix *X*, where elements x_{ij} is

$$x_{ij} = w_j \times d_{ij} \quad (i = 1, 2, \cdots, m;\ j = 1, 2, \cdots, n).$$

The ideal solution X^+ and the negative ideal solution X^- are as follows:

$$\begin{aligned} X^+ &= \{x_1^+, x_2^+, \cdots x_n^+\} \\ &= \{(\max x_{ij} \mid j \in J_1), (\min x_{ij} \mid j \in J_2), (i = 1, 2, \cdots, n)\} \end{aligned} \tag{5}$$

$$\begin{aligned} X^- &= \{x_1^-, x_2^-, \cdots x_n^-\} \\ &= \{(\min x_{ij} \mid j \in J_1), (\max x_{ij} \mid j \in J_2), (i = 1, 2, \cdots, n)\} \end{aligned} \tag{6}$$

in which J_1 is the profitable index collection represents the best value of the i^{th} index; and J_2 is the consuming index collection represents the worst value of the i^{th} index. The bigger the profitable index is, the smaller the consuming index is. In this case, it represents the evaluating result is the better and vice versa.

We compute the distance of resource node evaluation value from the best and worst evaluation value collections (ideal solution and negative ideal solution) by *n*-dimensional Euclidean formula:

$$s^+ = \sqrt{\sum_{j=1}^{n} (x_{ij} - x_j^+)^2} \quad (i = 1, 2, \cdots, m) \tag{7}$$

$$s^- = \sqrt{\sum_{j=1}^{n} (x_{ij} - x_j^-)^2} \quad (i = 1, 2, \cdots, m) \tag{8}$$

Thus, the closeness degree between the resource service nodes and the ideal resource service nodes can be computed as follows:

$$c_i = \frac{s_i^-}{s_i^+ + s_i^-} \quad (i = 1, 2, \cdots, m) \tag{9}$$

Among this, c_i reflects the closeness to ideal and negative ideal resource service of the i^{th} resource service nodes. Apparently, when $0 < c_i \le 1$, the greater c_i is, the higher priority resource service node is. While $c_i = 1$, the i^{th} resource service node is the optimum.

5 The comprehensive trust computation and evaluating of recommending credibility

The trust evaluation of service provider has two parts, which one is the direct trust between evaluator and service provider, and the other is recommending trust that is recommending nodes gave an evaluated value to service provider. It actually represents whether service provider is credibility from the view of recommendation nodes. So the comprehensive credibility of service provider can be computed by fusing direct trust and recommendation trust.

5.1 Direct trust

Direct trust is a trust value that obtained by evaluating the direct service of between evaluation node SR and resource service node SP. Direct trust computing involved with service successes, volume of service, etc. (Gan et al., 2011). However, the past computing method of indexes weigh existed defect of subjective assumption and the method is both trivial and uncertain. We find whether service is successful is the most direct and the manifest standard of evaluating SP in computing direct trust, direct trust is a trust value that obtained by evaluating the direct service between evaluation node *SR* and resource service node *SP*. Which means not only to solve defect of subjective assumption of index weigh, but also to reduce the volume of multi-dimensions computing. Meanwhile, the time influence factor is taken into account, which can improve the accuracy of direct trust.

The direct trust DT_{SP}^E represents direct mutual trust between evaluator *E* and resource service node *SP*, we represent it as formula (10):

$$\boldsymbol{DT}_{SP}^E = \frac{S_{SP}^E + 1}{S_{SP}^E + F_{SP}^E + 2} \tag{10}$$

In which, DT_{SP}^E is direct trust, while S_{SP}^E and F_{SP}^E, respectively represent the frequency of the successful and unsuccessful services between node *E* and resource service node *SP*. It is $S_{SP}^E = 0$, $F_{SP}^E = 0$ if there is no interactions between node *E* and resource service node *SP*, in the other words, the trustworthiness is equal to the untrustworthiness, VIZ $DT_{SP}^E = \frac{1}{2}$.

Actually, that credibility of a node which did not have any services in a long period should be attenuated with time, that is to say trust has time-attenuation. But it is hard to directly find out the relation between trust and time because trust involves too many factors, e.g., emotion, interaction history, mutual time and context environment, etc. However, it is as known that frequency of service is related to trust, and frequency of service is related to time, thus we

express the time-attenuation of trust with the relationship of service frequency and time.

Therefore, we introduce function $\boldsymbol{f}(N(t))$ with frequency of transaction $N(t)$ within time t, $N(t)$ meets the following terms:

1 $N(t) \geq 0$

2 Let $N(t)$ be a positive integer

3 If $s \prec t$, $N(s) \leq N(t)$, and $N(t) - N(s)$ is equivalent to number of transaction within $(s, t]$. i.e., stochastic $\{N(t), t \geq 0\}$ is counting process on temporal interval with length of t.

In conclusion, on interval t with arbitrary length, number of transaction $N(t)$ between node E and SP is Poisson distribution with (parameter), $\lambda t \succ 0$. We get $f(N(t))$ as formula (11):

$$\boldsymbol{f}\left(N(t)\right) = P\{N(t+s) - N(s) = k\} = e^{-\lambda t}\frac{(\lambda t)^k}{k!}, \quad k = 0, 1, 2, \cdots \tag{11}$$

k is number of transaction, $\lambda = \dfrac{E(N(t))}{t}$ represents the average times per unit time.

Thus, we get direct trust of node SP from node E on k.

$$\boldsymbol{DT}_{SP}^{E} = \boldsymbol{f}\left(N(t)\right) \cdot \boldsymbol{DT}_{SP}^{E} \tag{12}$$

5.2 Recommendation trust

The computing formula of recommending trust model was given by Wang and Gui (2012).

$$\overline{\boldsymbol{RT}_{SP}} = \sum_{\substack{i,j=1 \\ i \neq j}}^{n} \boldsymbol{Sim}\left(C_{SP}^{i}, C_{SP}^{j}\right) \cdot \left(\sqrt[3]{\alpha \cdot \omega_{SP}^{i} \cdot \boldsymbol{DT}_{SP}^{i}} + \sqrt[3]{\beta \cdot \omega_{SP}^{j} \cdot \boldsymbol{DT}_{SP}^{j}}\right) \Big/ n \tag{13}$$

$\overline{\boldsymbol{RT}_{SP}}$ is the comprehensive trustworthiness evaluation to service nodes SP, where i, j, SP are respectively the recommendation node, evaluator node and service node. C_{SP}^{i} is the content of between recommendation node i and service node SP, and C_{SP}^{j} is the content of between recommendation node j and service node SP.

$\boldsymbol{Sim}(C_{SP}^{i}, C_{SP}^{j})$ states the similarity of C_{SP}^{i} and C_{SP}^{SR}; ω_{SR}^{i} and ω_{SR}^{j}, respectively represent the weight of acquaintance recommendation node and strange recommendation node.

Among this, we initialise weight of strange node is $\omega_{SR}^{j} = 0.5$ which represents the half of the trust degree when strange nodes join into networks.

We declare a trust degree called α, which is credibility of service node in the view of acquaintance:

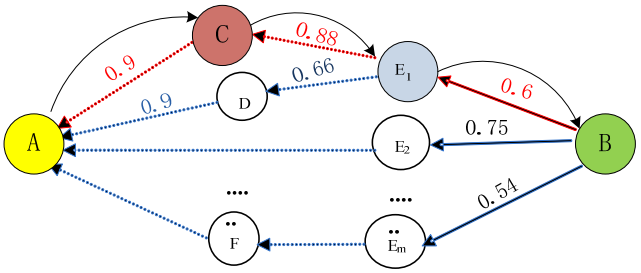
$$\begin{cases} \alpha = DT_{SP}^{i} & \text{if } SR_i = DASR_i \\ \alpha = \dfrac{1}{n}\displaystyle\sum_{N=1,\, i \neq j \neq k}^{n} \prod PT_{SP}^{i} * PT_{SP}^{j} & \text{if } SR_i = IASR_i \\ \quad = PT_{j}^{i} \times PT_{SP}^{j} \times PT_{l}^{SP} \times \cdots & \end{cases} \tag{14}$$

Since the recommending path might intercross while the recommending node i is indirect acquaintance recommending node. To solve this problem, we set a threshold ε, and we will give up the node iff $\alpha < \varepsilon$. ε is the difference empirical values according to the difference context.

β is credibility of service node in the view of strange recommending node. We set $\beta = \dfrac{1}{n}\displaystyle\sum_{i=1}^{n} DT_{SR}^{i}$. The node could be a new or dormancy node while $\displaystyle\sum_{i=1}^{n} DT_{SR}^{i} = 0$.

Actually, in the process of recommending, because there existed two different paths which are respectively independent path and crossed path. We would select a recommendation path with the highest credibility in the crossed path. For instance, we select $A \rightarrow C \rightarrow E_1 \rightarrow B$ as the optimal path in Figure 3.

Figure 3 Selecting trust recommendation path (see online version for colours)



5.2.1 Computing similarity degree of service content

The computing method of service content similarity is actually a complicated computing process involving multi-attributes, though Wang and Gui (2012) proposed the computing method of service-similarity degree, it did not consider multi-attributes factor of service-similarity, which will lead to coarse-grained issue of service-similarity computing.

We use $\vec{\mathbf{a}}_i = (x_{i1}, x_{i2}, \cdots, x_{in})$ as the i^{th} service vector that service provider gave recommending node in the period, and use $\vec{\mathbf{b}}_j = (x_{j1}, x_{j2}, \cdots, x_{jn})$ as the current service vector that service provider gives evaluating node. Therefore, we use the cosine similarity with $\vec{\mathbf{a}}_i$ and $\vec{\mathbf{b}}_j$ represents service content similarity.

$$\boldsymbol{Sim}\left(C_{SP}^{i}, C_{SP}^{j}\right) = \frac{\vec{\boldsymbol{a}} \bullet \vec{\boldsymbol{b}}}{|\vec{\boldsymbol{a}}| \bullet |\vec{\boldsymbol{b}}|} \tag{15}$$

Since recommendation service content involves different indicators in different scenarios, how to abstract related indicators is an important work. Through analysing, we found that the successful ratio of recommending service is the most important indicator of recommending service quality in recommending trust. Likewise, recommending service content is outstanding indicator of recommending service content indicators, recommending service cost is the most remarkable indicator of value cost of recommending service, recommending service time is one of the striking important indicators for recommending credibility, and recommending service responding time shows attitude indicator of recommending node. Besides these, recommending service is related with the other contexts. To ensure recommending trust computing is overall and simple as soon as possible, we selected five trust-interrelated indicators, they are respectively *ServiceSuccess*, *ServiceContents*, *ServiceTime*, *ServiceCost* and *ResponseTime*, Therefore, the service can be abstracted as an indicator set, and the service vectors $\vec{\mathbf{a}}_i$ and $\vec{\mathbf{b}}_j$ are standardised as

$$\vec{\mathbf{a}}_i = (x_{i1}, x_{i2}, x_{i3}, x_{i4}, x_{i5}), \vec{\mathbf{b}}_j = (x_{j1}, x_{j2}, x_{j3}, x_{j4}, x_{j5}),$$
$$0 \le i,\ j \le m.$$

Among this, (x_{i1}, x_{i2}, x_{i3}, x_{i4}, x_{i5}) and (x_{j1}, x_{j2}, x_{j3}, x_{j4}, x_{j5}), respectively represent (*ServiceSuccess*, *ServiceContents*, *ServiceTime*, *ServiceCost*, *ResponseTime*).

The weight of service vector indicator ϖ_τ can be computed by an entropy weight-based method.

Supposing that the evaluating index sample data matrix $\boldsymbol{X} = (x_{i\tau})_{m\times n}$, let $\boldsymbol{Z}_{i,\tau} = (Z_{i\tau})_{m\times n}$, $Z_{i\tau} = x_{i\tau} \Big/ \sum_{i=1}^{m} x_{i\tau}$. Among this, i is the amount of recommendation nodes, and τ is evaluation index and $\tau \le n$, (n = 5). We can get the entropy weight of indexes according to information entropy concept:

$$e_\tau = -k\sum_{i=1}^{m} Z_{i\tau} \ln Z_{i\tau},\ \tau = 1, 2, \cdots, n \tag{16}$$

In which, $k = (\ln m)^{-1}$, $0 \le e_\tau \le 1$. The weight of each index can be computed by the following formula:

$$\varpi_\tau = (1-e_\tau) \Big/ \sum_{\tau=1}^{5} (1-e_\tau),\ \tau = 1, 2, \cdots, n \tag{17}$$

Among this, $0 \le \varpi_\tau \le 1$ and $\sum_{\tau=1}^{5} \varpi_\tau = 1$.

From the analysis above, the service similarity degree can be computed as follows:

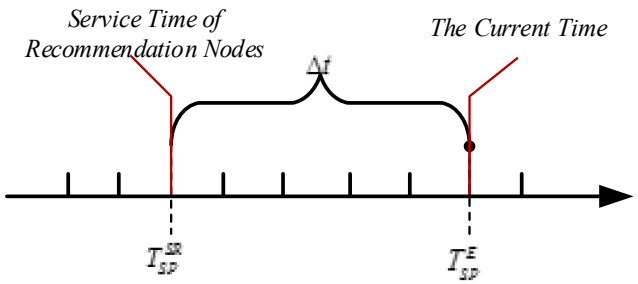
$$\boldsymbol{Sim}\left(C_{SP}^{i}, C_{SP}^{j}\right) = \frac{\sum_{\tau=1}^{5} \varpi_\tau x_{i\tau} \bullet \varpi_\tau x_{j\tau}}{\sqrt{\left(\sum_{\tau=1}^{5} \varpi_\tau x_{i\tau}\right)^2 \bullet \left(\sum_{\tau=1}^{5} \varpi_\tau x_{j\tau}\right)^2}} \tag{18}$$

In which, ϖ_τ is equivalent to the weight of the τ^{th} index.

5.2.2 *Evaluating of recommendation credibility*

Recommendation credibility is the trustworthiness degree for recommendation nodes which is evaluated by other nodes in the network. Wang et al. (2007) proposed that recommendation trustworthiness is closely related to two aspects among the numerous factors: On one hand, from the perspective of service itself, the recommendation trustworthiness depends on the similarity between evaluator's request content and service content that service node has proposed to recommending nodes on a large-scale. On the other hand, considering the human cognition, the synthesis trustworthiness of evaluated object is related to the familiarity between recommendation nodes and evaluation nodes. In the practical situations, the recommendation trustworthiness also depends on the service timing and frequency of service between service nodes and recommending nodes.

Figure 4 Time influence factor of recommendation trustworthiness (see online version for colours)

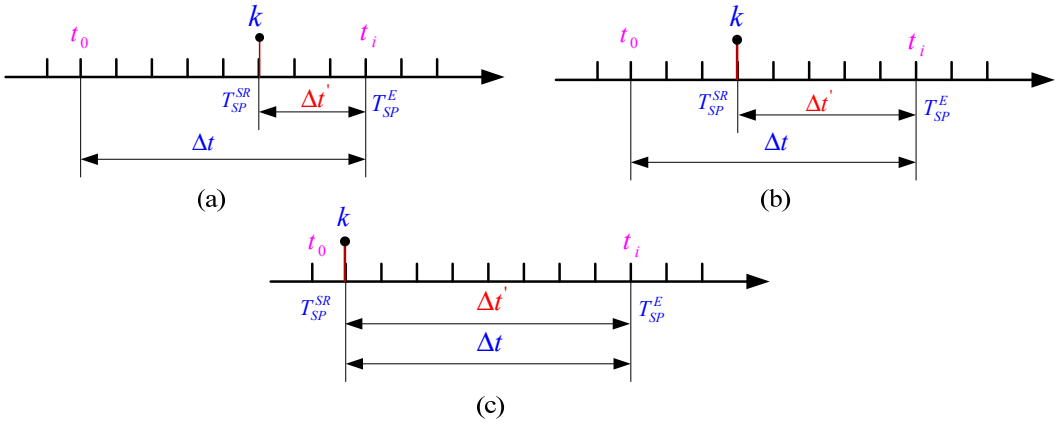


In Figure 4, T_{SP}^{E} is the service time between evaluation node and service node; T_{SP}^{SR} between recommendation node and service node is the closest history service time to T_{SP}^{E}. We can conclude that the shorter the interval between T_{SP}^{SR} and T_{SP}^{E} is, the higher the recommendation trustworthiness is within Δt.

A shorter interval between T_{SP}^{E} and T_{SP}^{SR} can define a higher recommendation trustworthiness, whereas the recommendation trustworthiness declines while the service time moving forward.

In Figure 5, Δt is the time interval [t_0, t_i], $\Delta t'$ is the interval between T_{SP}^{SR} and T_{SP}^{E}; k is for the number of service. We can reach the conclusion that k is in inverse proportion to $\Delta t'$ in [t_0, t_i], which means the higher k is, the shorter $\Delta t'$ is, VIZ. the closer T_{SP}^{SR} and T_{SP}^{E} are. Thus, recommendation trustworthiness is related to the service frequency in a period, that is to say, the high-frequency service leads to the shorter distance to T_{SP}^{E}.

Figure 5 Relationship between the number of service and time of service for recommendation nodes (see online version for colours)



From the mentioned above, it is the service frequency of node that concerns the recommendation trustworthiness of recommendation node in that period. The time-sensitive functions have been proposed in the previous trust models, and the relevant mathematical expressions have been given. For instance, Gan et al. (2011) proposed a time-sensitive function according to time window of each service. However, relationship between the time sensibility and credibility is not a simple linear or exponent relation. Obviously, Gan et al.'s (2011) thinking to the time-sensitive function has remarkable subjectivity. So we gave a following theorem to determine the recommendation time influence function.

We consider $N(t)$ as number of service provided by service nodes and recommendation nodes on interval $[0, t)$, $t \geq 0$. Let $\{N(t), t \geq 0\}$ be a stochastic process called counting progress, which has a status of non-negative integers and continuous time.

Figure 6 Sample function chart of the number of recommendation

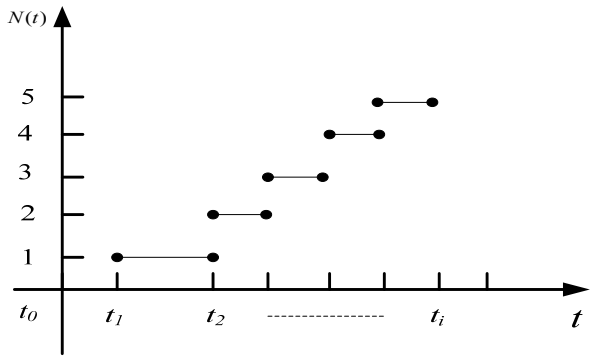


Figure 6 is an illustration of sample function $N(t)$. We consider $N(t) - N(t_0) \triangleq N(t_0, t)$, $0 \leq t_0 < t$, $N(t)$ is the number of services of arbitrary recommendation node on $[0, t)$.

There are k times of services on $[t_0, t)$, i.e., $\{N(t_0, t_i) = k\}$ is an event.

Theorem 1: Let us define k services of recommendation node SR_i on period $[t_0, t_i]$, and consider $\{N(t_0, t_i) = k\}$ as an event with probability $P_k(t_0, t_i) = P\{N(t_0, t_i) = k\}$ $k = 1, 2, \cdots$. The recommendation time-influence function $f(t_0, t_i)$ of recommendation nodes satisfy a Poisson distribution of λ on $[t_0, t_i]$, i.e.,

$$\boldsymbol{f}(t_0, t_i) = P_k(t_0, t_i) = \frac{[\lambda(t_i - t_0)]^k}{k!} e^{-\lambda(t_i - t_0)}, \quad t > t_0, k = 0, 1, 2, \cdots \tag{19}$$

If

1 $N(0) = 0$.

2 The increments of non-overlapped intervals are independent.

3 To consider sufficiently small Δt, $P_1(t, t + \Delta t) = P\{N(t, t + \Delta t) = 1\} = \lambda \Delta t + o(\Delta t)$. In which, the constant λ refers to the intensity and $\lambda > 0$, and $o(\Delta t)$ is the infinitesimal of higher order of Δt since $\Delta t \to 0$. λ is the expected value of services quantity of unit interval.

4 To consider sufficiently small Δt, $\sum_{j=2}^{\infty} P_j(t, t + \Delta t) = \sum_{j=2}^{\infty} P\{N(t, t + \Delta t) = j\} = o(\Delta t)$, i.e., compared with the probability of service quantity of 1 in $[t, t + \Delta t)$, the probability of service quantity of two or more is negligible.

Because the repeating services can weaken influence of time-attenuation by collaborative recommendation in a certain period, we introduce the service content similarity and acquaintance between recommendation nodes and evaluators to guarantee trustworthiness of recommendation. Recommendation reliability (RR_i) can be calculated by the following formula.

$$\begin{cases} RR_i = \sqrt[4]{f(t_0, t_i) Sim(C_{SP}^i, C_{SP}^j) \cdot \alpha \cdot \omega_{SR}^j}, \\ \quad \text{if } i \text{ is accquaintance node} \\ RR_i = \sqrt[4]{f(t_0, t_i) Sim(C_{SP}^i, C_{SP}^j) \cdot \beta \cdot \omega_{SR}^j}, \\ \quad \text{if } j \text{ is stranger node} \end{cases} \tag{20}$$

In which, $f(t_0, t_i)$ is time-influence function, $Sim(C_{SP}^i, C_{SP}^j)$ is the service content similarity between recommending nodes and evaluators, α, β and ω are as above.

So formula (13) is changed as following equation.

$$\overline{\boldsymbol{RT}_{SP}} = \sum_{\substack{i,j=1 \\ i\neq j}}^{n} \left(\sqrt{RR_i \cdot \boldsymbol{DT}_{SP}^i} + \sqrt{RR_j \cdot \boldsymbol{DT}_{SP}^j} \right) \Big/ n \tag{21}$$

5.3 Comprehensive trust

Computing method of comprehensive trust is as follows:

$$\boldsymbol{GT}_{SP}^{SR} = (\lambda \quad \gamma) \cdot \begin{pmatrix} \boldsymbol{DT}_{SP}^{SR} \\ \overline{\boldsymbol{RT}_{SP}} \end{pmatrix} \tag{22}$$

Among this, $\lambda + \gamma = 1$, $\lambda, \gamma \in [0, 1]$, λ and γ are the weight factors of direct trust and recommendation trust. In view of social relations, the trust gained from direct interaction is higher than indirect interaction's. With the increase of mutual among nodes, the resource requestors prefer the target nodes with high direct interaction trust, i.e., λ and γ dynamically change along with the interaction frequency. A greater λ and a smaller γ demonstrate that the direct trust will take larger proportion with the increase of k while the recommendation trust has a smaller proportion. At the same time, it is only 50-50 that evaluator trusts an arbitrary evaluated strange service node, thus a service influence function $\lambda(k)$ was introduced as follows:

$$\lambda(k) = 1 - \left(\frac{1}{2}\right)^{\frac{k}{n-k}} = \begin{cases} 1 - \left(\frac{1}{2}\right)^{\frac{k}{n-k}}, & n-k \neq 0 \\ 1, & n-k = 0 \end{cases} \tag{23}$$

Among this, $\lambda(k)$ is a dynamic function which has a variable of k. While $n - k = 0$, i.e., $k = n$, indicates that there are direct interactions between resource requestor and target nodes. In the case, there is not recommendation from other nodes, and $\lambda = 1$. While $k = 0$, i.e., $\lambda(k) = 0$, indicates that the comprehensive trust computing relies on the recommendations from other nodes and there is no direct trust among the nodes.

6 Updating recommendation trust values based on multi-attributes for recommendation nodes

In social networks, a node is both service node and recommending node, so a node has both comprehensive trust value and recommendation trust value. We knew though two kinds of trust are related to each other, they are largely different. When we say that a node had a higher credibility, we would distinguish the node is as a content service node or as a recommending node. Because a higher trust value does not indicate a higher recommendation trust.

We consider four key attributes for updating recommending trust: successful recommendation ratio, evolution degree of recommending capability, credibility of recommending nodes and deviation between recommending credibility and comprehensive trust. The updating method can be applied to recommending credibility computation.

The recommendation trust RT' can be expressed as a tetrad $RT' = (RSR_i^{(n\text{-}1)}, REC, Diff, GT)$. Among this, $RSR_i^{(n-1)}$ is equivalent to the successful recommendation ratio, REC represents evolution degree of recommendation capability, GT shows the service credibility of recommendation nodes and Diff is the deviation between recommendation credibility and comprehensive trust. Thus, the formalised computing formula of RT' is:

$$\boldsymbol{RT}_i' = \omega_1 \cdot RSR_i^{(n-1)} + \omega_2 \cdot Diff_i + \omega_3 \cdot REC_i + \omega_4 \cdot GT_i \tag{24}$$

Among this, $\sum_{i=1}^{4} \omega_i = 1$, and ω_i can be computed in entropy-based. Likewise, we no longer discuss about it.

6.1 Difference degree of recommendation trust

$$Diff = \frac{\left| \overline{RT_{SP}} - R_i \right|}{\overline{RT_{SP}}} \tag{25}$$

R_i is the recommendation trust value of the i^{th} nodes, and $\overline{RT_{SP}}$ is for the comprehensive trust value of SP.

6.2 Evolution degree of recommendation capability

Definition 6: Evolution degree is the improvement of recommendation capability of service nodes, and it concerns several indices (recommendation accuracy, successful recommendation ratio, etc.), which vary with the increase of recommendations.

Instead of experiences, the evolution degree of recommendation capability mainly concerns the recommendation contribution to network. Therefore, we put forward recommendation evolution computing method based on Markov process theory.

A Markov chain (discrete-time Markov chain or DTMC) named after Andrey Markov is a random process that undergoes transitions from one state to another on a state space (https://en.wikipedia.org/wiki/Markov_chain). The mathematical concepts are as follows:

Definition 7: Let a stochastic progress $\{\boldsymbol{X}(t), t \in T\}$ with n arbitrarily values of time $t_1 < t_2 < \cdots$, t_n, $n \geq 3$, $t_i \in T$ within state-space I. The distribution function of $X(t_n)$ remains the same while the condition $\boldsymbol{X}(t_i) = x_i$, $x_i \in I$, $(i = 1, 2, \cdots, n-1)$ turns into $\boldsymbol{X}(t_{n-1}) = x_{n-1}$, namely that,

$$\begin{aligned} &\boldsymbol{P}\left\{ \boldsymbol{X}(t_n) \leq x_n \,\middle|\, \boldsymbol{X}(t_1) = x_1, \boldsymbol{X}(t_2) \right. \\ &= x_2, \cdots, \left. \boldsymbol{X}(t_{n-1}) = x_{n-1} \right\} \\ &= P\left\{ \boldsymbol{X}(t_n) \leq x_n \,\middle|\, \boldsymbol{X}(t_{n-1}) = x_{n-1} \right\} \end{aligned} \tag{26}$$

In conclusion, the process $\{X(t), t \in T\}$ has Markov properties, which can be referred to as Markov process. The

Markov process with discrete time and discrete status is called Markov chain.

The computing steps of recommendation improvement capability are as follows:

Step 1 Evaluation rank

To evaluate the recommendation capability of nodes, the paper establishes a rank of evaluation and represents the level with evaluation indexing set $V\{v_1, v_2, v_3, \ldots, v_n\}$.

Step 2 Ranking proportions

To count the evaluation recommendation nodes of different levels, M_i is brought in to represents the number of nodes in the i^{th} level, and s_i' is referred to as the corresponding proportion, that is

$$\sum_{i=1}^{n} M_i = N,\ S_i' = \frac{M_i}{N}.$$

Step 3 State transition

The vector $\boldsymbol{S}_w^t = (S_1^t, S_2^t, \cdots, S_j^t)$ is defined to express evaluation status of recommendation capability of nodes w, state for short, and parameter t (t is a discrete magnitude) represents time, then S_w^k expresses the k^{th} state of w. The state changes with t, which is called state transition.

Step 4 Service probability matrix

If S_w^k is the current evaluation state, S^{k-1} is the state vector of previous evaluation. Given Chapman-Kolmogorov equation (Zhang et al., 2008; El-Damcese and Temraz, 2015), $\boldsymbol{S}_w^{k-1} \times \boldsymbol{P}_w = \boldsymbol{S}_w^k$. In which, $\boldsymbol{P}_w$ is the 1-step transition probability matrix.

$$\boldsymbol{P}_w = \begin{pmatrix} P_{11} & P_{12} & \cdots & P_{1n} \\ P_{21} & P_{22} & \cdots & P_{2n} \\ \cdots & \cdots & P_{ij} & \cdots \\ P_{n1} & P_{n2} & \cdots & P_{mn} \end{pmatrix} \tag{27}$$

Among this, P_{ij} is referred to as the transition probability from state i to j,

$$0 \le P_{ij} \le 1 \quad (i, j = 1, 2, \cdots, n),\ \sum P_{ij} = 1,\ (i = 1, 2, \cdots, n)$$

The given progress results x_1, x_2, ⋯, x_n can quantify the recommendation capability as $\boldsymbol{F}_w$, i.e.,

$$\boldsymbol{F}_w = \sum_{i=1}^{n} S_i x_i \tag{28}$$

The Markov chain is said to be ergodic then $\boldsymbol{S}_w^{t-1} = \boldsymbol{S}_w^t = \boldsymbol{S}_w^k$ as $t \to \infty$ (Wang, 1987). As long as steady-state $\boldsymbol{S}_w = (S_1, S_2, \cdots, S_n)$ is worked out, it can be used to calculate improvement of w, which can be figured out by the following formula:

$$\begin{cases} S_w \times P_w = S_w \\ \sum_{i=1}^{n} S_i = 1 \end{cases} \tag{29}$$

Instead of recommendation capability score, F_w is referred to as the improvement degree during this period. Larger F_w represents larger improvement comparing with the previous.

6.3 Case illustration of evolution of recommendation capability

Let w_1, w_2 as recommendation nodes, where establishes a rank of 5 levels (high degree of confidence, trust basic trust, distrust, a high degree of distrust), respectively referred to as (*HT*, *T*, *BT*, *DT*, *HDT*). The nodes of each level and transition state of w_1, w_2 are shown as Table 1 and Table 2.

- Previous actual state:

$$\boldsymbol{S}_{w_1} = (5/30, 21/30, 4/30, 0, 0),$$
$$\boldsymbol{S}_{w_2} = (2/30, 26/30, 2/30, 0, 0)$$

- Current actual state:

$$\boldsymbol{S}_{w_1'} = (6/30, 21/30, 3/30, 0, 0),$$
$$\boldsymbol{S}_{w_2'} = (4/30, 25/30, 1/30, 0, 0)$$

Table 1 Evaluation of node w_1

The number of nodes	*This evaluation*						*Total*
	Rank	*FT*	*T*	*BT*	*NT*	*NFT*	
Previous evaluation	FT	4	1	0	0	0	5*
	T	2	18	1	0	0	21
	BT	0	2	2	0	0	4
	NT	0	0	0	0	0	0
	NFT	0	0	0	0	0	0
Total		6	21	3	0	0	30

Notes: The meaning of '*' figure represents that there are five evaluators giving FT in previous evaluation, in the current evaluation, four of them give 'HT', one of them gives 'T'. The others are same argument.

Table 2 Evaluation of node w_2

The number of nodes	*This evaluation*						*Total*
	Rank	*FT*	*T*	*BT*	*NT*	*NFT*	
Previous evaluation	FT	1	1	0	0	0	2*
	T	2	24	0	0	0	26
	BT	1	0	1	0	0	2
	NT	0	0	0	0	0	0
	NFT	0	0	0	0	0	0
Total		4	25	1	0	0	30

Notes: The meaning of '*' figure represents that there are five evaluators giving FT in previous evaluation, in the current evaluation, four of them give 'HT', one of them gives 'T'. The others are same argument.

The 1-step transition probability P_{w_1}, P_{w_2} :

$$\boldsymbol{P}_{w_1} = \begin{bmatrix} 4/5 & 1/5 & 0 & 0 & 0 \\ 2/21 & 18/21 & 1/21 & 0 & 0 \\ 0 & 1/2 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\boldsymbol{P}_{w_2} = \begin{bmatrix} 1/2 & 1/2 & 0 & 0 & 0 \\ 1/13 & 12/13 & 0 & 0 & 0 \\ 1/2 & 0 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

The steady-state of w_1, w_2 can be worked out by $(I - \boldsymbol{P}_w)^T \boldsymbol{S}_w^T = 0$.

The steady-state of w_1 can be calculated by the following formula,

$$\begin{bmatrix} 1/5 & -1/5 & 0 & 0 & 0 \\ -2/21 & 1/7 & -1/21 & 0 & 0 \\ 0 & -1/2 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} S_1 \\ S_2 \\ S_3 \\ S_4 \\ S_5 \end{bmatrix} = 0$$

Thus, $\boldsymbol{S}_{w_1} = (10/33, 7/11, 2/33, 0, 0)$.

Similarly, $\boldsymbol{S}_{w_2} = (2/15, 13/15, 0, 0, 0)$.

If the specific scores of different levels are defined as FT = 90, T = 80, BT = 60, NT = 50, NFT = 30, the recommendation capability scores of w_1 and w_2 are $\boldsymbol{F}_{w_1} = 81.8$ and $\boldsymbol{F}_{w_2} = 81.3$, which means that recommendation capability of w_1 is better than recommendation capability of w_2.

7 Simulation experiment and result analysis

The design and verification of the simulation experiment on interaction node selection and trust relation computing has been given in the following contents. The simulation experiments are designed to verify the authenticity of selected ideal interaction nodes and to identify the strategy-cheating nodes and malicious nodes. Meanwhile, the restraint on malicious or collaborative cheating can be judged by recommendation capability, recommendation accuracy and successful recommendation ratio.

Because *EigenRep* model is a typical global reputation model that specifies the trust computing under the P2P environment, we select *EigenRep* compared with other models in order to show experiment results of our algorithm.

We carry out experiment to simulate the recommendation service algorithm and verify its effectiveness. 1,000 nodes and 1,000 kinds of services were set. These services are assigned to the nodes at random, and every node at least has one service content. The simulation experiment is composed of several periods and every node interacts during each period. Let the initial trustworthiness be of 0.5.

The simulation experiment is based on Java; CPU is 3.0 G and the memory is 2 G in the running environment.

Experiment 1: The analysis and comparison of strategy deceptions.

To recognise the intermittent strategy cheating, the paper measures the perception capability of this method for strategy cheating, which differs from *EigenRep* model and general model (interactions are regarded as the unique condition).

The experiment simulates the intermittent cheating of malicious nodes, which gained high trustworthiness during a period through successful interactions.

Figure 7 Trust changes curve with the increase of service cycle (see online version for colours)

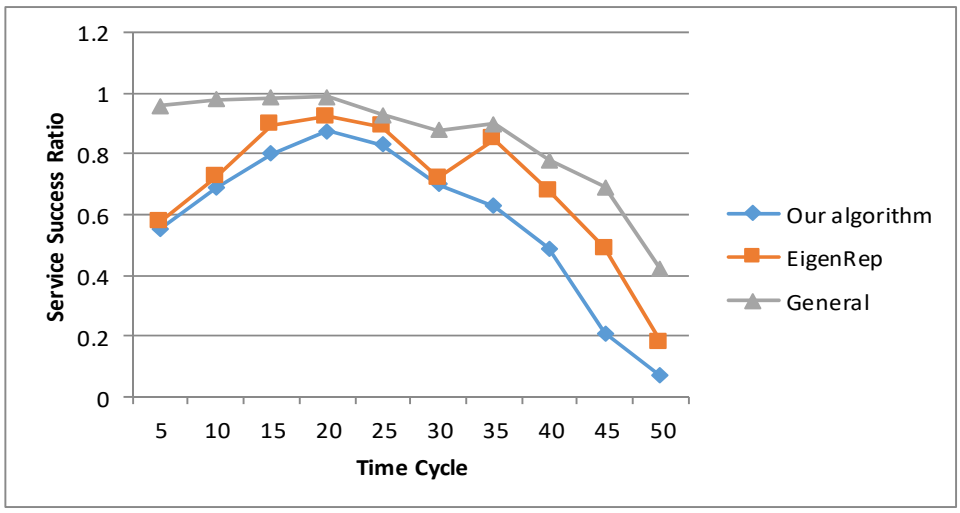


Figure 8 Success ratio of service with malicious nodes changing (see online version for colours)

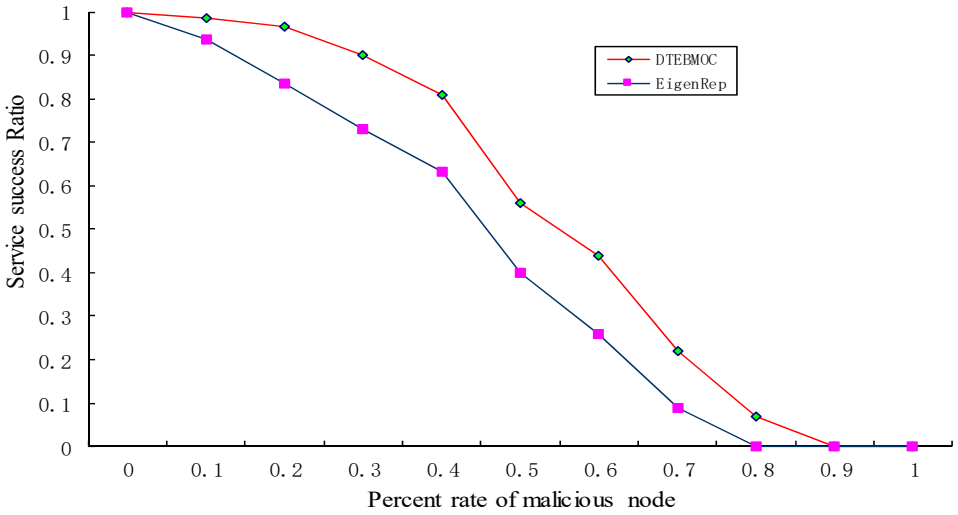
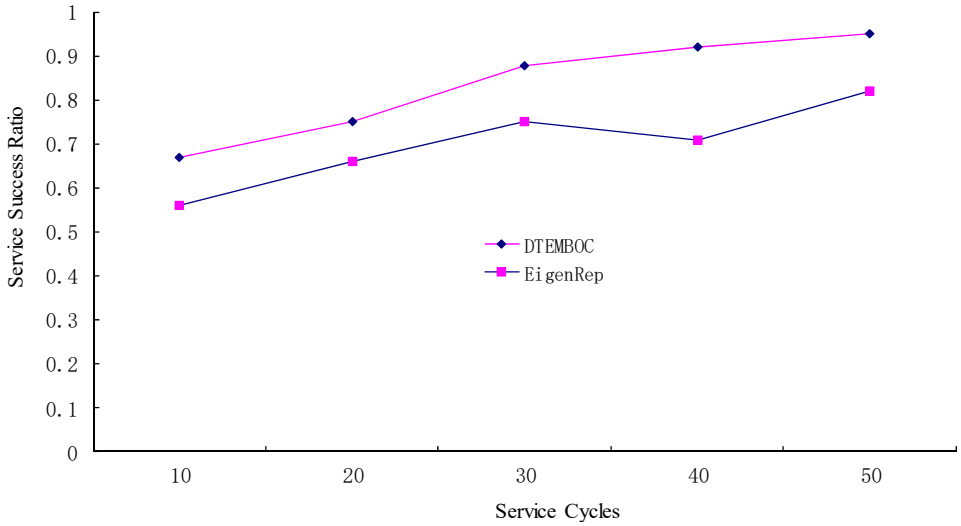


Figure 9 Success ratio of service with the increase of service cycles (see online version for colours)



In Figure 7, in the less service cycles, we can see clearly that general model has a low recognition ratio of strategy cheating nodes. From 5th to 10th cycle, the method we proposed makes trustworthiness of strategy cheating nodes is 55.3%~68.9%, which is lower than both *EigenRep* model's (57.7%~72.3%) and general model's (96%~98%).

It is indicated that strategy cheating is easily recognised by our method and *EigenRep* model at beginning. With the increasing number of transaction cycles, the malicious nodes take strategy measures to improve successful service ratio, which enhance its trustworthiness in *EigenRep* model and our method.

Strategy malicious cheating occurred along with the trustworthiness of malicious nodes reaching a certain degree on the 25th cycle. Compared with the slightly decreased trustworthiness in general model and *EigenRep* model, the trustworthiness of malicious nodes is decreased dramatically in our method.

On the 30th cycle, we can find that the malicious nodes deceive general model and *EigenRep* model to improve their trustworthiness by interacting as good nodes, but the deception is recognised by our method.

After the 40th cycle, the trustworthiness of malicious is decreased more rapidly in our method than general model and *EigenRep* model. According to the experiment results, compared with *EigenRep* model and general model, the recommendation trust model is more sensitive to the unexpectedly alteration. While the intermittent deception occurred, the trustworthiness decline rapidly; with the time elapsing, the velocity of decline is much greater than restoration, i.e., the method we proposed is good at identifying strategy deception nodes.

Experiment 2: Analysis and comparison in different malicious recommendation nodes.

In Figure 8, with the increasing of malicious nodes, it is clear that the method we proposed is more effective for its great improvement of successful interaction ratio than the *EigenRep* model. When the percentage of malicious node is less than 40%, the successful interaction ratio is inversely proportion to the number of malicious nodes. However, the

successful interaction ratio in our method is decreased more slowly than *EigenRep* model.

The percent rate of malicious node is from 40% to 60%, the restraint on malicious nodes in our method is more effective than *EigenRep* model. Compared with the *EigenRep* model, our recommendation trust algorithms has kept a high successful service ratio even when the percentage of malicious nodes reaches 60%. The model restrains the malicious node effectively no matter it is a pure or collaboration malicious node.

Experiment 3: Analysis and comparison in the fixed malicious nodes.

It can be discovered that the dynamic service in the paper can indicate a higher successful interaction ratio with the increasing interaction cycles under the circumstance which has a fixed amount of malicious service nodes of 40%.

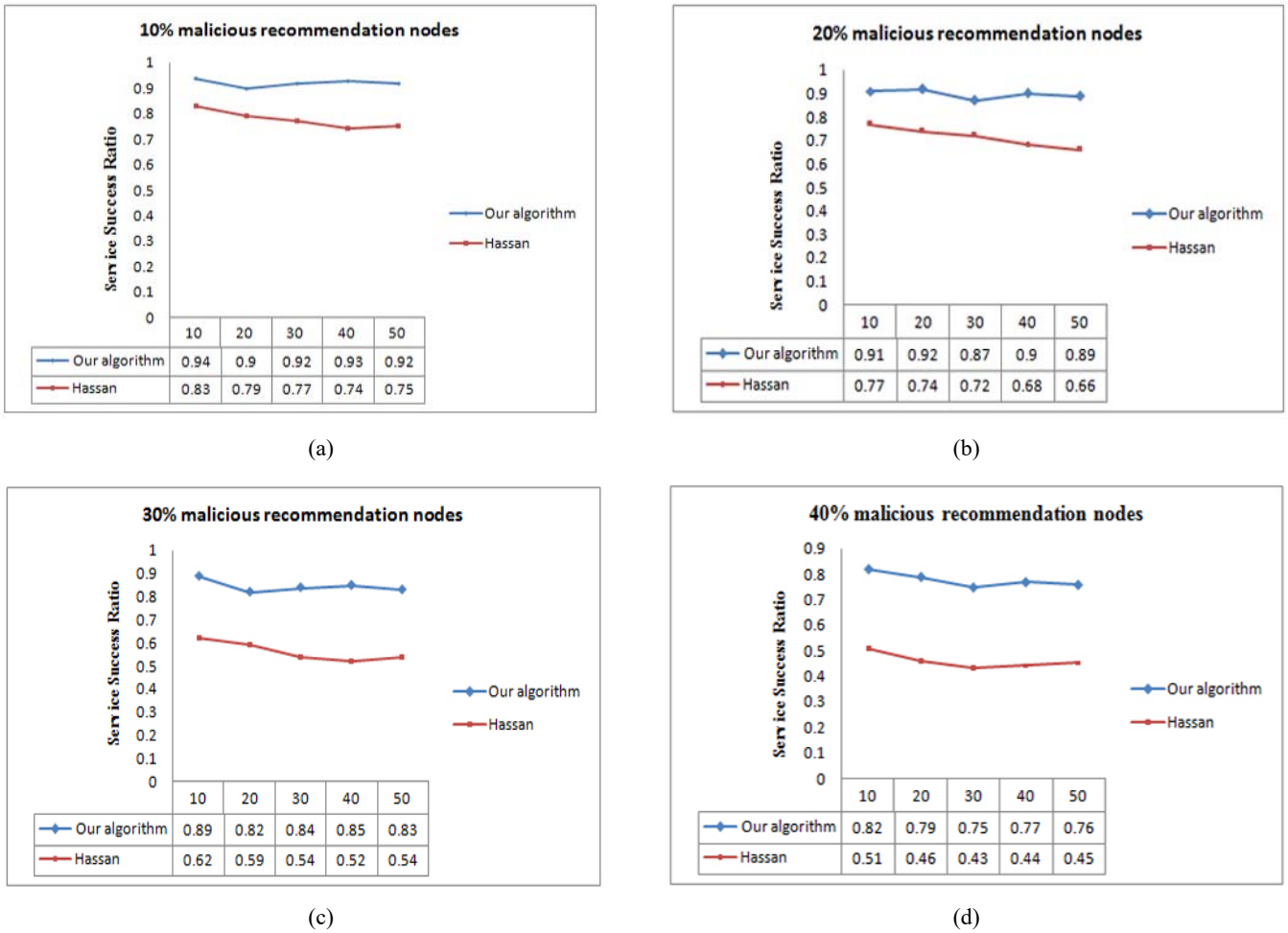
Experiment 4: Analysis and comparison of malicious collaborative recommendation.

In Figure 10, the increasing rate of malicious recommendation nodes and the decreasing accuracy of trust computing can lead to the more failed interactions and lower successful interaction ratio. While the percentage of malicious recommendation nodes increases, the successful interaction ratio decreases because of each malicious recommendation, which is related to its trustworthiness and keeps reducing its recommendation trustworthiness. Although Hassan model (Jameel et al., 2005) has certain restraint capability, it assumes that recommendation nodes have high trustworthiness, at the same time, it lacks punishment mechanism. Therefore, the dishonest recommendation influence cannot be weakened easily and the successful interaction frequency decreases rapidly.

The model we propose can decelerate the decline of successful service ratio by keeping honest nodes on the recommendation path away from the dishonest nodes while the percentage of dishonest recommendation nodes increases. The recommendation service evaluation algorithm proposed by us can adjust trustworthiness dynamically by introducing service content similarity and enhancing recommendation competence with incentive measures. Compared to Hassan model our method can identify malicious nodes to make recommendation information more accurate.

Experiment 5: Analysis and comparison of recommendation trustworthiness of nodes.

Figure 10 Success ratio of services under difference ratio of malicious collaborative recommendation nodes (see online version for colours)



We design experiments respectively on three vital attributions of recommendation service of nodes.

In the service accuracy experiment of recommendation, the average accuracy of whole service has been introduced because of the random distribution and selection. In the evolution level experiment of recommendation service ability, a node of higher trustworthiness of 80% and a node of lower trustworthiness of 60% (which gained the basic trust) are selected as static recommendation nodes. Thus, we get the recommendation evolution ability of each period and the success rate of recommendation service according to service cycles is also designed in the experiment.

7.1 The average recommendation accuracy experiment of nodes

In Figure 11, the *EigenRep* has a certain value of recommendation while the service periods increases, i.e., the transaction content similarity of recommendation nodes cannot be evaluated. Therefore, we cannot evaluate its trustworthiness efficaciously with *EigenRep* model and it goes against the reality. Compared with the EigenRep model, the current algorithm shows practical quality, that is to say, the recommendation accuracy changes with the changing of service periods. It is indicated that the recommendation accuracy declines while the recommendation content is different from service content.

Considering the mention above, the algorithm we proposed in this paper is in accordance with the reality.

7.2 The experiment on evolution degree of recommendation capability

In this experiment, a node of higher trustworthiness and a node of lower trustworthiness are selected as referential static recommendation nodes to evaluate the recommendation capability evolution level. Thus, we can draw the conclusion easily: the corresponding change has been taken place while the service periods increase of these two nodes.

Figure 12 shows the evolution level of recommendation ability of two nodes, in which TON: 80% represents the trustworthiness of one node is 80%, and TON: 60% represents the trustworthiness of the other node is 60%. From result of the experiment, we can see progress degree of recommendation capability of node where TON is 80% is lower than the other node's in the former 30 service periods, with the increase of service cycles, and the recommendation evolution degrees of the two nodes are approaching to each other. The result represents the ratio of recommendation successful of two nodes is also increasing when the trustworthiness of the two recommendation nodes has been improved and their trustworthiness is close. The results of our experiment conform to actual situation.

Therefore, we can ensure the fairness between competitive bidding nodes because their recommendation evolution degrees are almost equal, which means our algorithm is in accordance with reality.

7.3 The experiment on successful recommendation ratio

Figure 13 shows changing of the successful recommendation ratio in different malicious recommendation rate while the service period increases. In which, RMRN is ratio of malicious recommendation nodes, and RMRN: 20% represents ratio of malicious recommendation nodes is 20%, likewise. The lower the ratio of malicious nodes is the higher ratio of the successful recommendation is.

Figure 11 Average accuracy of recommendation with the increase of service cycles (see online version for colours)

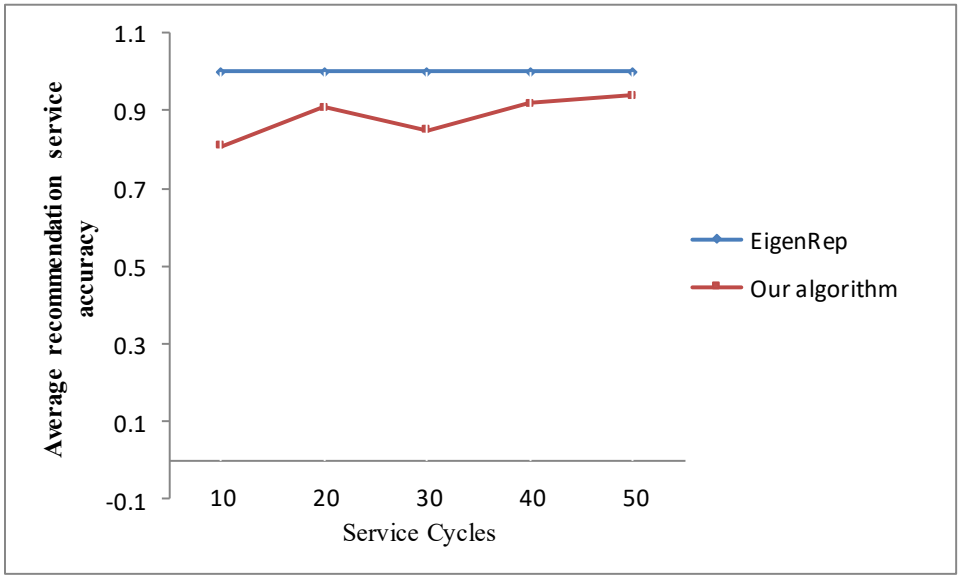
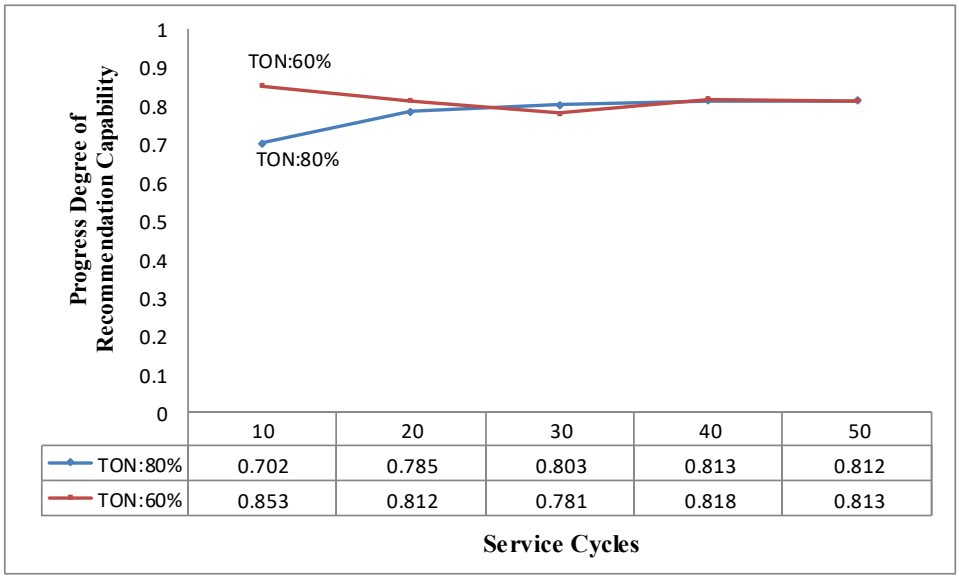
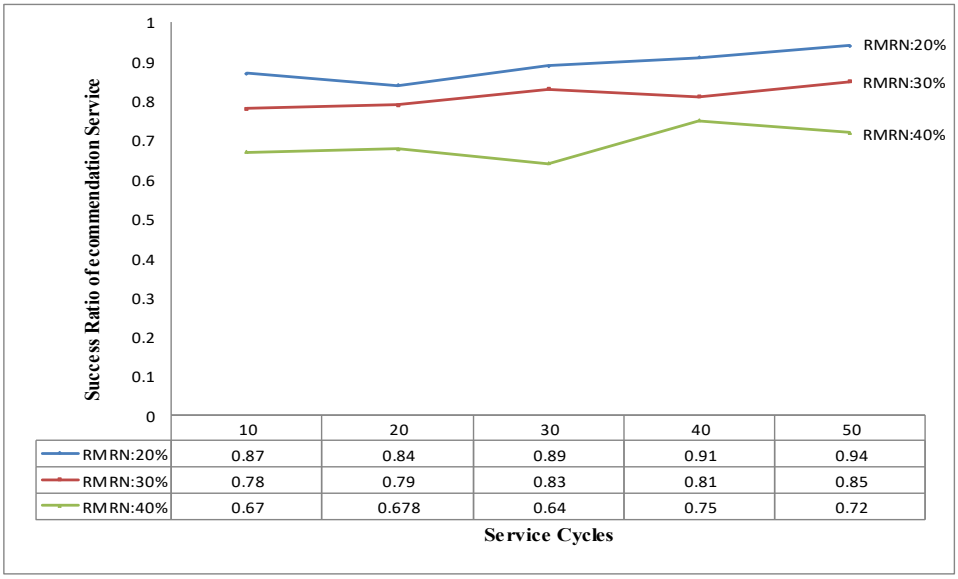


Figure 12 Evolution degree of recommending capability with the increase of service cycles in different trust nodes (see online version for colours)



	10	20	30	40	50
TON:80%	0.702	0.785	0.803	0.813	0.812
TON:60%	0.853	0.812	0.781	0.818	0.813

Figure 13 Success ratio of recommendation with the increase of service cycles in different malicious recommendation nodes (see online version for colours)



	10	20	30	40	50
RMRN:20%	0.87	0.84	0.89	0.91	0.94
RMRN:30%	0.78	0.79	0.83	0.81	0.85
RMRN:40%	0.67	0.678	0.64	0.75	0.72

The successful recommendation ratio stays 64% with our algorithm in the percentage of malicious recommendation nodes of 40%, i.e., our algorithm has a preferable robustness in coping with attacks from malicious recommendation nodes.

8 Conclusions and next works

In the paper, a dynamic trust model based on bidding and multi-attributes in social networks is presented. Through the model several significant issues in networks are solved effectively. Firstly, a bidding strategy built by the paper copes with laziness question of nodes in order to make nodes active. Secondly, by TOPSIS method, model can select a few the correct service node avoiding the defection of random selecting service node; thirdly, the model can also distinguish between recommending trust and service trust. Experiment results prove that the model can effectively restrain cheat of nodes, malicious recommendation of nodes and collaborative cheat, etc.; at the same time, experiment analysis also represented that the model can incent nodes to do the best to join recommendation and evaluation.

However, our model has still some weaknesses, for example, our solution will cause an issue of performance overhead with expansion of networking, specifically in large-scale networking environment. We found that operating efficiency of the system dropped when the number of nodes was over 500, and then operating efficiency of the system dropped sharply when the number

of nodes was over 1,000. Therefore, we selected 1,000 nodes in our experiments as a compromise.

Moreover, our algorithm also has other two limitations, in which one is that we supposed the shifting probability is a constant variable in the process of Markov and the other is that we supposed time is infinite. In fact, the shifting probability is ever changing and time is also finite.

To deal with these issues, we will keep going on studying by optimising our algorithm and finding other solutions in order to improve performance of system in further. At the same time, we are going to research the relationship between access control and trust in big data and large-scale networking environment.

Acknowledgements

The Project Supported by Natural Science Basic Research Plan in Shaanxi Province of China (Program No. 2014JM2-6099) and Project of Education Department of Shaanxi Province of China (No. 2013JK1193) and National Natural Science Foundation of China (No. U1261111).

References

Advogato [online] http://www.advogato.org/ (accessed 1 January 2013).

Al-Oufi, S., Kim, H-N. and El Saddik, A. (2012) 'A group trust metric for identifying people of trust in online social networks', *Expert Systems with Applications*, Vol. 39, No. 18, pp.13173–13181.

Amoretti, M. and Zanichelli, F. (2016) 'Distributed reputation management for service-oriented peer-to-peer enterprise communities', *International Journal of Computational Science and Engineering*, Vol. 13, No. 2, pp.147–157.

Blaze, M., Feigenbaum, J. and Keromytis, A.D. (1998) 'Keynote: trust management for public-key infrastructures', in Christianson, B., Crispo, B., William, S. et al. (Eds.): *Cambridge 1998 Security Protocols International Workshop*, Springer-Verglag, Berlin, pp.59–63.

Blaze, M., Feigenbaum, J. and Lacy, J. (1996) 'Decentralized trust management', in *Proc. 17th IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, Oakland, CA, USA, pp.164–173.

Chen, C., Wang, R-C., Zhang, L. and Deng, Y. (2009) 'A kind of trust appraisal model based on bids in grid', *Journal of NanJing University of Posts and Telecommunications (Natural Science)*, Vol. 29, No. 5, pp.59–64.

Denko, M.K., Sun, T. and Woungang, I. (2011) 'Trust management in ubiquitous computing: a Bayesian approach', *Computer Communications*, Vol. 34, No. 3, pp.398–406.

Dou, W., Wang, H-M., Jia, Y. and Zhou, P. (2004) 'A recommendation-based peer-to-peer trust model', *Journal of Software*, in Chinese, Vol. 15, No. 4, pp.571–583.

El-Damcese, M. and Temraz, N. (2015) 'Analysis of availability and reliability of k-out-of-n: F model with fuzzy rates', *International Journal of Computational Science and Engineering*, Vol. 10, Nos. 1/2, pp.192–201

Gan, Z-B., Ding, Q., Li, K. and Xiao, G-Q. (2011) 'Reputation-Based multi-dimensional trust algorithm', *Journal of Software*, in Chinese, Vol. 22, No. 10, pp.2401–2411.

Griffiths, N. (2005) 'Task delegation using experience based multi-dimensional trust', in *Proc. of the 4th Int'l. Joint Conf. on Autonomous Agents and Multiagent Systems*, ACM Press, Utrecht, Netherlands, pp.621–628.

Hwang, C.L. and Yoon, K. (1981) *Multiple Attribute Decision Making: Methods and Applications*, Springer-Verlag Press, New York.

Jameel, H., Hung, L.X., Kalim, U., Asjjad, A., Lee, S.Y. and Lee, Y.K. (2005) 'A trust model for ubiquitous systems based on vectors of trust values', in Werner, B. (Ed.): *Proc. of the 7th IEEE Int'l. Symp. on Multimedia*, IEEE Computer Society Press, Washington, Irvine, CA, USA, pp.674–679.

Jiang, W., Wang, G. and Wu, J. (2012) 'Generating trusted graphs for trust evaluation in online social networks', *The International Journal of Grid Computing and eScience, Future Generation Computer Systems*, in Press, Corrected Proof, Available online 26 June 2012.

Jøsang, A. (2001) 'A logic for uncertain probabilities', *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, Vol. 9, No. 3, pp.279–311.

Kamvar, S.D. and Schlosser, M.T. (2003) 'EigenRep: reputation management in P2P networks', in *Lawrence S. Proc. of the 12th Int'l. World Wide Web Conf.*, ACM Press, Budapest, pp.123–134.

Kim, Y.A. and Phalak, R. (2012) 'A trust prediction framework in rating-based experience sharing social networks without a web of trust', *Information Sciences*, Vol. 191, No. 3, pp.128–145.

Lou, C.X. and Dai, W. (2015) 'Optimal and stable supply chain services system: integrating management services with robust optimisation modelling', *International Journal of High Performance Computing and Networking*, Vol. 8, No. 1, pp.71–80.

Markov chain [online] https://en.wikipedia.org/wiki/Markov_chain (accessed 20 May 2012).

Sabater, J. and Sierra, C. (2001) 'REGRET: reputation in gregarious societies', in *Proc. of the 5th Int'l. Conf. on Autonomous Agents*, ACM Press, Montreal, Que., Canada, pp.194–195.

Wang, G. and Gui, X. (2012) 'DRTEMBB: dynamic recommendation trust evaluation model based on bidding', *Journal of Multimedia*, Vol. 7, No. 4, pp.279–288.

Wang, G. and Wu, J. (2011) 'Multi-dimensional evidence-based trust management with multi-trusted paths', *Future Generation Computer Systems*, Vol. 27, No. 5, pp.529–538.

Wang, G., Gui, X. and Wei, G. (2010) 'A recommendation trust model based on e-commerce transactions content-similarity', in *2010 International Conference on Machine Vision and Human-machine Interface*, Kaifeng, pp.105–108.

Wang, R.X. (1987) *Random Process*, Xian Jiaotong University, Xi'an, in Chinese.

Wang, X.S., Liang, P., Ma, H.D., Xing, D. and Wang, B.Z. (2007) 'A P2P trust model based on multi-dimensional trust evaluation', in *Proc. of the Bio-Inspired Computational Intelligence and Applications*, Springer-Verlag, Shanghai, China, pp.347–356.

Wang, Y., Zhao, Y-l. and Hou, F. (2008) 'A new security trust model for peer-to-peer e-commerce', in *Management of e-Commerce and e-Government ICMECG'08*, Jiangxi, pp.399–402.

Zhan, J. and Fang, X. (2011) 'A novel trust computing system for social networks', in *2011 IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing*, Boston, pp.1284–1289.

Zhang, X.C., Li, J. and Wei, G. (2008) *Economic and Applied Mathematics Tutorial*, Nankai University Press, in Chinese.

Zhang, Y., Lin, L., Huai, J-P., Li, X-X. and Zhong, L. (2006) 'A resource allocation mechanism providing trust and incentive in grid', *Journal of Software*, in Chinese, Vol. 17, No. 11, pp.2245–2254.

Zolfaghar, K. and Abdollah, A. (2011) 'Evolution of trust networks in social web applications using supervised learning', in *World Conference on Information Technology, WCIT-2010*, Elsevier, Istanbul, Turkey, Vol. 3, pp.833–839.

Appendix

Theorem 1 proof

Let $P_n(t) = P\{N(t) = n\} = P\{N(t) - N(0) = n\}$, $n \geq 1$ then

$$P_n(t+\Delta t) = P\{N(t+\Delta t) = n\} = P\{N(t+\Delta t) - N(0) = n\}$$
$$= P\{N(t) - N(0) = n,\ N(t+\Delta t) - N(t) = 0\}$$
$$+P\{N(t) - N(0) = n-1,\ N(t+\Delta t) - N(t) = 1\}$$
$$+\sum_{j=2}^{n} P\{N(t) - N(0) = n-j,\ N(t+\Delta t) - N(t) = j\}$$

By condition (2)~(4), the following is obtained.

$$P_n(t+\Delta t) = P_n(t)P_o(\Delta t) + P_{n-1}(t)P_1(\Delta t) + o(\Delta t)$$
$$= (1-\lambda\Delta t)P_n(t) + \lambda\Delta t P_{n-1}(t) + o(\Delta t)$$

Thus,

$$\frac{P_n(t+\Delta t) - P_n(t)}{\Delta t} = -\lambda P_n(t) + \lambda P_{n-1}(t) + \frac{o(\Delta t)}{\Delta t},$$

let $\Delta t \to 0$,then.

$$P_n'(t) = -\lambda P_n(t) + \lambda P_{n-1}(t)P_1(\Delta t)$$
$$\therefore e^{\lambda t}\left[P_n'(t) + \lambda P_n(t)\right] = \lambda e^{\lambda t} P_{n-1}(t)$$
$$\therefore \frac{d}{dt}\left[e^{\lambda t} P_n(t)\right] = \lambda e^{\lambda t} P_{n-1}(t)$$

By the induction method, we can proof that

$$f(t_0, t_i) = P_k(t_0, t_i) = \frac{\left[\lambda(t_i - t_0)\right]^k}{k!} e^{-\lambda(t_i - t_0)}$$

Supposing that formula (5.10) is true, when $n = n - 1$. Thus, by formula (1), we can obtain that

$$\therefore \frac{d}{dt}\left[e^{\lambda(t-t_0)} P_n(t_0, t_i)\right] = \lambda e^{\lambda(t_i - t_0)} \frac{\left[\lambda(t_i - t_0)\right]^{n-1}}{(n-1)!} e^{-\lambda(t-t_0)}$$
$$= -\lambda \frac{\left[\lambda(t_i - t_0)\right]^{n-1}}{(n-1)!}$$

Thus, by integral

$$e^{\lambda(t_i - t_0)} P_n(t_0, t_i) = \frac{\left[\lambda(t_i - t_0)\right]^n}{n!} + c$$

Let $P_n(0) = P\{N(0) = n\} = 0$ substitute into the above equation, then

$$P_n(t_0, t_i) = e^{-\lambda(t_i - t_0)} \frac{\left[\lambda(t_i - t_0)\right]^n}{n!}$$

Under condition (2), we could infer that

$$P\{N(t_i) - N(t_0) = k\} = \frac{\left[\lambda(t_i - t_0)\right]^{k-1}}{(k-1)!} e^{-\lambda(t_i - t_0)},\ n = 0, 1, \cdots$$

Q.E.D.