International Journal of Security and Its Applications
Vol. 10, No. 12 (2016), pp.389-398
http://dx.doi.org/10.14257/ijsia.2016.10.12.32

A Multi Dimension Service Trust Model in Social Network

Leiyue Yao*, Qianglai Xie

The Center of Collaboration and Innovation, JiangXi University of Technology, Jiangxi, 330098, China
special8212@sohu.com

Abstract

Trust is the precondition to provide users with efficient services in social network. We often use the evaluation information of other users, but doesn't use social network by the trust relationship. In this study, by using the trust network theory to obtain the evaluation reliability of user's feedback on the service, obtaining transaction context information through the transaction background, a comprehensive service trust computation model is put forward. It incorporates self-feedback, trust network neighbor feedback, feedback similarity and transaction context information. It can avoid the sparsity and cold start in traditional trust computation. The experimental results show that the model can effectively prevent social network dishonest feedback, and more accurate to reflect the service trust.

Keywords*: Social network service; Service trust; Trust network; Social network neighbor; Feedback similarity.*

1. Introduction

Social networks service (SNS) has a rapid development with the popularization of Internet users. It not only has an explosive growth of user number, but also has a large-scale emergence of various services. In recent years, a large number of new social network services continue to emerge, for example the twitter and micro blog, which is becoming a major social network form. Due to the social network directly in the face of consumer groups, propaganda is more direct, and more conducive to word-of-mouth publicity. Many companies believe it is an innovation of marketing mode. They can use social network to recommend the services; can effectively reduce the cost of enterprise marketing. Social network marketing can make the goal more accurate, so that the flexible strategy will certainly be in the enterprise service marketing model to occupy a very important position [1].

Different areas and various professional have different understanding on services. The service computing field defines it is an activity between at least a service provider and a service consumer for the business goals or solves the problem. This paper refers to the social networking service by using of social networks to provide users with a variety of services, such as user select interest points according to the current location and preferences, the evaluation of information (services such as restaurants, hotels, etc.), with a general sense of service. The current social network service providing system can recommend interest according to the user's context [2]. It has a shortcoming that it doesn't recommend service to the user according to the social relation network, and the friends don't play the guiding role of the substantive. But in real life, the recommendation by acquaintance is often important to user. How to find valuable services from the complicated social network? So service trust evaluation gradually becomes a key supporting technology in the social network marketing. Service trust calculation model is the base to provide efficient application services to users. Therefore, how to find the

ISSN: 1738-9976 IJSIA

trust service through the evaluation information of other users in the social network is the challenge for the further development of the social networking service.

2. Related Work

The concept of trust management initially proposed by M. blaze in 1996 [3]. Accordance with the modeling method of trust, it is divided into sociological theory based, statistics based, probability, semantic based, uncertainty theory based and fuzzy set based trust model. According to the view of Artz [4], there are two ways to obtain the trust: the first is according strategy and the certificate, and the second is based on reputation. The first trust mechanism includes public key infrastructure (PKI) and credential, which has unified trust management language, unified authorization decision engine and distribution of document management features. For example Policy-maker [5] is the typical application. Reputation based trust management is computed by local experience and other entities feedback. The trust level is defined by an accurate numerical value. Trust degree related with activities, and constantly revised in the activities. Reputation based trust management is used widely in Ad, Hoc, P2P, Sensor Networks and pervasive computing and other fields.

At present, there are a lot of researches on service selection problem in different field. For example, in the field of electronic commerce / recommendation [6,7], the user can make a judgment whether to buy according to the trust evaluation. However, it is different in the social network. On the one hand, it lacks substantive contact between users in the current e-commerce system, and doesn’t establish the social relationship networks, which lead to suspicion on credibility for some users’ feedback. On the other hand, all feedback evaluation weight is the same in the existing e-commerce system. In addition, research on service selection is also reflected in the field of Web services. Kalepu summarized the attributes of quality of service (QoS) required in web service selection [8]. Lindenberg analyzed trust relationship between human societies, and proposed the service selection algorithm based on trust relationship [9]. However, a large-scale system has sparse direct relationship. Hu puts forward a recommendation trust model based on weighted similarity between nodes [10]. It is inspired that the nodes have similarities in their recommendation, and the trust model can based on weighted similarity between nodes. Dai considered bad trading history in the calculation of reputation, and give the corresponding punishment [11]. Yang believed that some details behaviour in specific areas is hidden in the single trust value model, and cannot resist the malicious node attack strategy, so a P2P trust model based on interest similarity weighted recommendation is proposed [12]. Although there are some related researches in the network service recommendation and the service trust, it still doesn't solve the problem of the service trust in the social network. And there are serious deficiencies of trust relationship exists in the practical application of Web services in the industrial sector. Social networks can solve credibility of user’s feedback, transaction context, and user’s preferences in service selection, and provide users with high trustable service. The credibility of the feedback is based on social network with trust network theory to solve; trading context information can be obtained through transaction background.

Therefore, this paper presents a multi-dimension service trust computation model. The contribution of the comprehensive service trust model is that it introduces self-feedback, trust network neighbor feedback, feedback similarity and transaction context information, especially the feedback similarity of neighbor node in trust network. It has a high efficiency, and can avoid the sparsity and cold start in traditional trust computation. The model can effectively prevent dishonest feedback, and more accurate to reflect the service trust.

3. Idea for Design

3.1. Social Network Service Framework

Social networking service framework is as shown in Figure 1, when user A search service in network, he will access to a list of services; the system will search for trust evaluation evidence and use an evaluation model for service trust; then return the trust value to user; the user A will decide whether to transact.

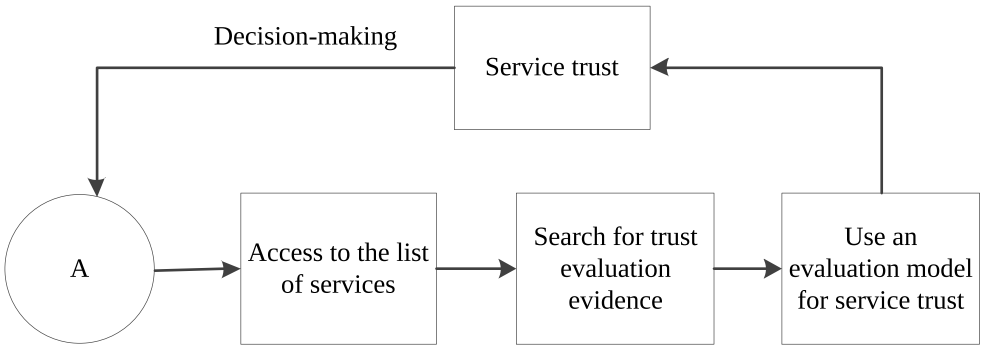

Figure 1. Social Networking Service Framework

3.2. Trust Network

The friends in social network will automatically converted to the user's self-network, which is a trust network connected by friend relations. For example, in Figure 2, the user A divided his friends into colleagues, students and relatives.

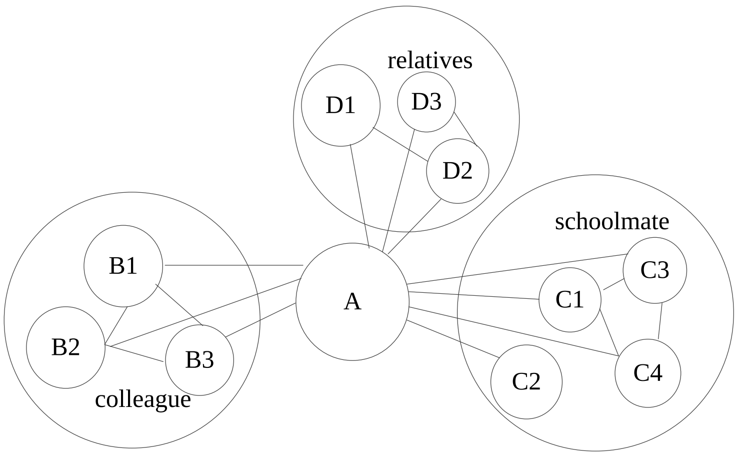

Figure 2. Trust Network

3.3. Dynamic Trust Level Computation Method

Service Trust compute process is divided into 4 steps:

Step 1: get the service list information, access to direct transaction history of user A, get direct transaction trust according to transaction information and feedback if there is the direct transaction.

Step 2: if there is no direct transaction, find the user's nearest neighbor nodes, send out requesting information. If the neighbor nodes have direct transactions, then calculate trust by neighbor's feedbacks.

Step 3: if there is no direct transaction of neighbors, extracting the target service transaction and feedback information, search the overlap service set between the nodes who give feedbacks to target service and neighbor nodes of A. If the set is empty, the transaction trust value is directly related to the service transaction and their feedback.

Step 4, if the set is not empty, computing feedback similarity of overlap trading service set between neighbor node set and feedback node set, use the similarity as the feedback reliability; combine with the transaction information to calculate the feedback trust value.

4. Trust Model

4.1. Select Neighbor Nodes

In a trust network, the user has a certain amount of trust users. From the trust network, we can directly get the trust neighbours of the target users, namely direct neighbours. Through the breadth first search can get trust users of direct neighbours, that is, indirect neighbours. Both them can constitute the user's initial neighbours. In order to avoid the interference of the long tail noise of a limited similar neighbour, a threshold value is set for the number of neighbours. For the users who have multiple neighbours, picked K neighbours closely linked with the user from the initial neighbour; and neighbour must at the layer n (n<=3). Then, set a threshold value of θ, the node can as the trust node of user A if trust degree is not less than θ. The trust value is reduced with transmission, and the trust value set TU of value for neighbour node t is as eq.1.

$$TU = \{t = \prod_{i=1}^{n} TU_i \mid t \geqslant \theta, n \leqslant 3\}$$

(1)

4.2. Feedback Similarity Calculation

The common methods of computing the similarity includes the cosine similarity cosine similarity, Pearson correlation. But in the face of sparse data, the common scoring service set is already small between two user‘s set, even the small set is very similar, it can’t make sure that they have high similarity. In order to solve this problem, a new similarity measure is proposed.

Define the equilibrium similarity of user set, which refers to the average feedback similarity between the neighbor sets U and feedback node set V to the overlap service set S.

The neighbor set U: $U=\{u_1, u_2...u_n\}$, and feedback node set V: $V=\{v_1, v_2...v_n\}$, service set S: $S=\{s_1, s_2...s_n\}$. Suppose u_1 make feedback score fu_1 on s_1. If there are *nu nodes* make feedback on s_1, the average feedback of U on s_1 is defined as eq.2.

$$\overline{fu_1} = \frac{1}{nu}\sum_{i=1}^{nu} fu_i$$

(2)

The average feedback of the U set to the S set is a combination of feedback FUS, and the average feedback of the V set to the S set is a combination of the feedback FVS.

Equilibrium similarity of user set $Sim(U,V)$ is

$$Sim(U,V) = \frac{FUS \quad FVS}{\sqrt{FUS^2} \quad \sqrt{FVS^2}}$$ Where $FUS = \{\overline{fu_1}, \overline{fu_1}..\overline{fu_n}\}$, $FVS = \{\overline{fv_1}, \overline{fv_1}..\overline{fv_n}\}$

(3)

If the common feedback score has a high similarity between two set, it indicates that the feedback set V has a similar propensity on service with the target user who request service. The feedback on target service is also worthy of trust. The feedback similarity and feedback reliability is positive.

4.3. Service Transaction Related Factors

Transaction trust of user *a* on the service *i* is computed by historical transaction information. It can use to predict the trust for user *b* in future. The main factors include history feedback, transaction time and number.

(1) Transaction feedback: allowing users to give a score on the transaction service, the corresponding score {0,0.1,0.2…1}, that is, the range of score is [0,1].

(2) The number of transactions: the number of transactions reflects the user's familiarity with the service, the introduction of transaction number *n* in the model is to obtain the average score in valid time.

$$\bar{f} = \frac{1}{n}\sum_{i=1}^{n} f_i \tag{4}$$

4.4. Service Trust Computing Model

The trust of user *A* on service *S* is eventually defined as *T*, according to the algorithm flow in 3.3 and the influence variables calculation method, the calculation method of trust *T* is obtained:

(1) If there is the direct transaction between user *A* and service *S*, that is $D \neq \Phi$. The trust *T(A,S)* follows the self-feedback trading trust rule, *An* represents the transaction number between *A* and *S* in effective time, f_{Ai} is feedback of user *A* in service *i*.

$$T(A,S) = \frac{1}{An}\sum_{i=1}^{An} f_{Ai} \tag{5}$$

(2) If there is no direct transaction of the user, but there is a direct transaction of neighbor node, that is $D = \Phi$, $DU = \Phi$. The trust *T(A,S)* follows the neighbor feedback. Among them, *j* is the neighbor node index, *m* is the number of neighbor nodes, Tu_j is the trust value of A on the neighbor node *j*, $T(u_j,S)$ is trust of the neighbor node *j* on service *S*. According to the transaction trust value calculation method, the trust is defined as follows:

$$T(A,S) = \frac{1}{m}\sum_{j=1}^{m} Tu_j \quad T(u_j,S), \text{ that is: } T(A,S) = \frac{1}{m}\sum_{j=1}^{m}(Tu_j \quad \frac{1}{n}\sum_{i=1}^{n} f_i) \tag{6}$$

(3) If the overlap service set is empty, that is $D = \Phi$, $DU = \Phi$, $IU = \Phi$. The trust *T(A,S)* follows the service transaction trust value, n represents the number of feedback in effective time, f_i is the *i-th* feedback score.

$$T(A,S) = \frac{1}{n}\sum_{i=1}^{n} f_i \tag{7}$$

(4) If the overlap service set is not empty, that is $D = \Phi$, $DU = \Phi$, $IU \neq \Phi$. The trust *T(A,S)* follows similarity feedback trust value. *Sim(U,V)*is the feedback similarity of neighbor node and feedback node on service *S*. T_U is the trust of user *A* on neighbor node, m is the number of neighbor node, then can get the average trust of user *A* on all neighbor nodes. *vn* is number of in feedback set V, f_{vi} is feedback of feedback node *i* on *S*, so the average of f_{vi} is the transaction trust value of set *V* on *S*. The equation of *T(A,S)* is as eq.8.

$$T(A,S) = Sim(U,V)\frac{1}{m}\sum_{j=1}^{m}(Tu_j \frac{1}{vn}\sum_{i=1}^{vn} f_{vi}) \tag{8}$$

So the comprehensive trust model is as eq.9.

$$T(A,S) = \begin{cases} \frac{1}{An}\sum_{i=1}^{An} f_{Ai} & D \neq \phi \\ \frac{1}{m}\sum_{j=1}^{m}(Tu_j \frac{1}{n}\sum_{i=1}^{n} f_i) & D = \phi \quad DU \neq \phi \\ \frac{1}{n}\sum_{i=1}^{n} f_i & D = \phi \quad DU = \phi \quad IU = \phi \\ Sim(U,V)\frac{1}{m}\sum_{j=1}^{m}(Tu_j \frac{1}{vn}\sum_{i=1}^{vn} f_{vi}) & D = \phi \quad DU = \phi \quad IU \neq \phi \end{cases} \tag{9}$$

5. Experiment

5.1. Experiment Description

In order to verify the accuracy of the trust model, we simulate a certain scale social network nodes and service experimental environment; the main experimental parameters are described as follows:

(1) Service types: supposed there are 20 services, 10 trusted services, and 10 untrusted services.

(2) Node type: supposed that there are 100 users in a social network, each user establish a social trust relationship with10 users, the value of trust is evenly distributed in the [0.8,1] for the neighbors have a high trust degree. Users are randomly assigned to services with a certain transaction, each service has transactions with 50 users, but the integrity user will only choose the untrusted service once time once they found deceived. In the experiment, we add a part of malicious user nodes, and they give the opposite feedback to service quality. In order to achieve malicious recommendation, the malicious node will transact with untrusted service no less than 4 times.

(3) Feedback score: the set of feedback score {0, 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1}, a total of 10 grades. 0.5 for neutral evaluation, below 0.5 said unreliable, service is more unreliable if the score is smaller; above 0.5 said reliable, and service is more reliable if the score is greater.

5.2. Experiment Index

Traditional trust (Tmodel) used mean value of all feedback. The multi-dimensional service trust model (Mmodel) has proposed algorithm in different situations, which can improve the trust computation efficiency. In order to verify the accuracy of the model trust calculation, the following error indicators are set as follows [13].

(1) MCE is the trust calculation error of the untrusted service *MS (Malicious Service)*, *m* is number of untrusted service, $T(S_i)$ is trust value of untrusted service *i*.

$$MCE = \frac{1}{m}\sum_{i=0}^{m} T(S_i) \tag{10}$$

(2) HCE is the trust calculation error of the trust service *HS (Honest Service)*, *h* is number of trusted service, $T(S_j)$ is trust value of trusted service *j*.

$$HCE = \frac{1}{h}\sum_{j=0}^{h}(1 - T(S_j)) \tag{11}$$

(3) GCE is global trust computation error :

$$GCE = \frac{1}{m+h}(\sum_{i=0}^{m}T(S_i) + \sum_{j=0}^{h}(1 - T(S_j))) \tag{12}$$

Obviously, if the *MCE*, *HCE*, *GCE* is smaller, the higher accuracy of the model calculation.

5.3. Experiment Result

Supposed that *MS* provide service with poor quality, the honest users give score value of 0, malicious nodes give score value of 1; *HS* provide service with high quality, the honest users give score value of 1, malicious nodes give score value of 0. In the experiment, the number of malicious nodes is gradually increased, ranging from 0 to 50, and observing two trust calculation errors of different services with the increase of these nodes. As shown in Figure 3, 4, when the number of malicious node is increasing, the trust calculation errors of *MS* and *HS* are increased in Tmodel and Mmodel. It mainly due to the trust models are rely on the collective feedbacks. When raising the proportion of malicious users to a certain extent, aggregation feedback will more likely to be interfered by false feedback.

Results of trust calculation error *MCE* for *MS* is shown in Figure 3. According to practical experience, experiment set honest user transact with untrusted service is not a fixed number, but only once a time. The malicious users will repeatedly transact with untrusted service to add feedbacks for a fraud. Therefore, the trust of untrusted service *MS* is more easily determined by the malicious user's feedback. The experiment also shows that with the increase of malicious users, the trust error of *MS* increased significantly. Due to the Mmodel access service trust value in priority in the trusted network, and when there is no evidence of a direct trust, it will consider the reliability of feedback. So the magnitude of increase in the *MS* trust evaluation is far lower than the Tmodel. Because the trust value of neighbor ranges from 0.8 to 1, there will be an initial certain trust evaluation error for a certain attenuation of trust transferring even in the absence of a malicious user.

Results of trust calculation error *HCE* for *HS* is shown in Figure 4. The experiment set transaction number is random in [1,4] between honest users and the trusted service. The malicious users will be shielded easily when they repeated transact with trusted service, so the experiment generally set transaction number is the average number of users. The trust of *HS* is decided by honest users and malicious users jointly. The result also shows that with the increase of malicious users, *HS* trust calculation error will increase in both model, but the Tmodel is increased obviously. Similar to the *MS* trust, *HS* trust evaluation also has an initial trust error in the absence of a malicious user.

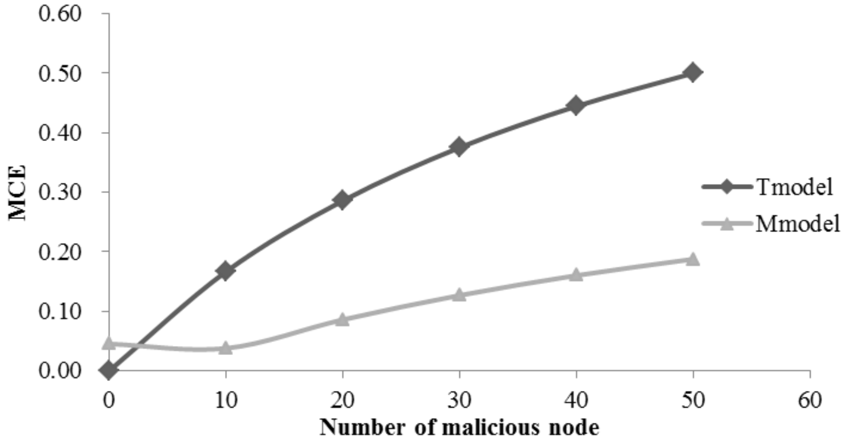

Figure 3. Result of Untrusted Service Calculation Error

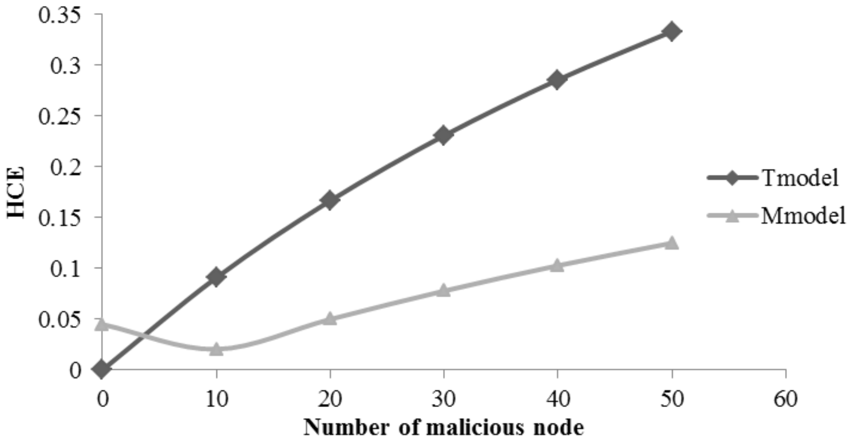

Figure 4. Result of Trusted Service Calculation Error

The experimental results for the global trust computation error *GCE* is shown in Figure 5. To sum up, for the two indicators of MCE and HCE, the Mmodel in this paper are lower than the contrast model, the global computing error GCE in Mmodel is the also lower too. The trust model integrated a variety of transactions services trust calculation rules in the social network , it is more conducive to remove accidental trust issues; it also take into account both the feedback reliability calculation, this also reduces the malicious nodes attempt by multiple transactions feedback to submerge honest feedback.

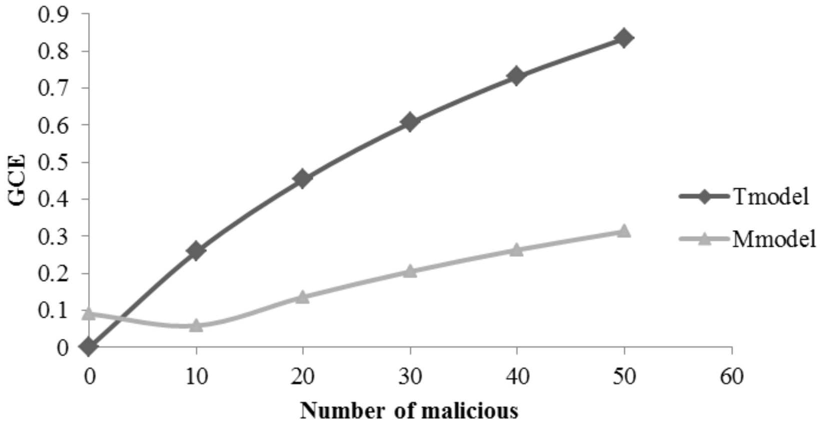

Figure 5. Result of Global Calculation Error

6. Conclusions

The social network can directly reflect the trust relationship between the users, and to form a trust network. The study has considered multiple situations in social network, includes service selection feature, user direct trading, neighbour direct trading, feedback similarity, transaction context. We design a comprehensive model of service trust, which can efficiently provide reliable service for the users. Especially introducing neighbour feedback similarity mechanism by the trust network, a comprehensively and accurately service trust evaluation is designed. Comparing with the traditional method, trust network and trust recommendation mechanism can avoids the sparsity and cold start problem. At meanwhile, the transaction time effectiveness, trusted friends circle in social network, can effectively inhibit the integrity of the service feedback. The mode is more close to the real world. But the study is lack of the influence factors of transaction context. We will pay more attention to the study on the dynamic and diverse transaction context in future, to improve the trust evaluation accuracy.

Acknowledgements

This work was supported by the Opening Project from “Mobile Internet Based Vehicle Communication System[HongKe[2016]96]” (Jiangxi University of Technology).

References

[1] S. Deng, L. Huang, G. Xu, 2014, “Social network-based service recommendation with trust enhancement”, Expert Systems with Applications, vol.41, no.18. **(2014)**, pp.8075-8084.

[2] X. Sui, Z. Chen, & J. Ma, “Location Sensitive Friend Recommendation in Social Network”, Web Technologies and Applications, **(2015)**, pp.316-327.

[3] M. Blaze, J. Feigenbaum, A. D. Keromytis, “Keynote: trust management for public-key infrastructures”, Infrastructures Lecture Notes in Computer Science, 1550, **(1999)**, pp.59--63.

[4] D. Artz, Y. Gil, “A survey of trust in computer science and the semantic web”, Web Semantics Science Services & Agents on the World Wide Web, vol.5, no.2, **(2007)**, pp.58-71.

[5] J. Cole, Z. Milosevic, K. Raymond. “Decentralized trust management”, Procs. of IEEE Conf. security & Privacy, vol.30, no.1, **(1996)**, pp.0164.

[6] G. Cheng, “Research on the recommending method used in C2C online trading”, International Conference on Web Intelligence and Intelligent Agent Technology (WI-IATW) **(2007)**, November 2-5, California, USA, pp.103-106,

[7] Y Zhao, C.Y. Feng, J. Yang, L.M. Wang, "Literature review of network public opinion about the e-commerce", Review of computer engineering studies, vol.2, no.2, **(2015)** , pp. 25-30.
[8] S. Kalepu, S. Krishnaswamy, S.W. Loke, "Verity: a QoS metric for selecting Web services and providers", International Conference on Web Information Systems Engineering Workshops (WISEW'03), **(2004)**, December 13, Roma, Italy, pp.131-139.
[9] J. Lindenberg, W. Pasman, K. Kranenborg, J. Stegeman, M.A. Neerincx, "Improving service matching and selection in ubiquitous computing environments: a user study", Personal & Ubiquitous Computing, vol.11, no.1, **(2007)**, pp.59-68.
[10] J.L. Hu, Q.Y. Wu, B. Zhou, J.H. Liu, "Robust feedback credibility-based distributed p2p trust model", Journal of Software, vol.20, no.10, **(2009)**, pp.2885-2898.
[11] Z.F. Dai, Q.Y. Wen, X.B. Li, "Recommendation trust model scheme for p2p network environment", Journal of Beijing University of Posts &Telecommunications, vol.32, no.3, **(2009)**, pp.69-72.
[12] L. Yang, Y. Zhang, C. Xing, T. Zhang, "A node Interest Similarity based P2P Trust Model", 12th IEEE International Conference on Communication Technology (ICCT) **(2010)**, November 11-14, Nanjing, China, pp.572 – 575.
[13] G. Lax, G.M.L. Sarne, "CellTrust: a reputation model for C2C commerce". Electron Commerce Research, vol.8, no.4, **(2008)**, pp.193-216.

Authors

Leiyue Yao, He is an associate professor in information science and engineering, and he is a senior engineer in information system development. He was born in July 1982 in Jiangxi in China. His major is computer application technology. He received his master's degree in Nanchang University in 2006. His research interests are in the pervasive computing, Mobile Commerce, system optimization.

Qianglai Xie, He is a lecturer in information science and engineering, and he is a Chief software Architect. He received his bachelor's degree in 2010 and major in network technology. His research interests are in information management system, Service Computing.

