Wang *et al. Compu Social Networls (2016) 3:2*
DOI 10.1186/s40649-016-0027-x

Computational Social Networks

RESEARCH Open Access

A game theory-based trust measurement model for social networks

Yingjie Wang[1], Zhipeng Cai[3,4*], Guisheng Yin[3], Yang Gao[2], Xiangrong Tong[1] and Qilong Han[3]

*Correspondence:
zcai@gsu.edu
[4] Department of Computer Science, Georgia State University, Atlanta 30303, Georgia
Full list of author information is available at the end of the article

Abstract

Background: In social networks, trust is a complex social network. Participants in online social networks want to share information and experiences with as many reliable users as possible. However, the modeling of trust is complicated and application dependent. Modeling trust needs to consider interaction history, recommendation, user behaviors and so on. Therefore, modeling trust is an important focus for online social networks.

Methods: We propose a game theory-based trust measurement model for social networks. The trust degree is calculated from three aspects, service reliability, feedback effectiveness, recommendation credibility, to get more accurate result. In addition, to alleviate the free-riding problem, we propose a game theory-based punishment mechanism for specific trust and global trust, respectively.

Results and conclusions: We prove that the proposed trust measurement model is effective. The free-riding problem can be resolved effectively through adding the proposed punishment mechanism.

Keywords: Service reliability, Feedback effectiveness, Recommendation credibility, Game theory, Punishment mechanism

Background

With the current popularity of online social networks, more and more information is distributed through social network services [2]. Participants in online social networks want to share information and experiences with as many reliable users as possible [3–5]. Trust is a basis of social network services. However, the modeling of trust is complicated and application-dependent [6–8]. Modeling trust needs to consider interaction history, recommendation, user behaviors and so on. Therefore, modeling trust is an important focus for online social networks [9–11].

In online social websites, such as Amazon, eBay, and FilmTrust, the existing trust models are mainly constructed based on nodes' global trust. However, these models fail to filter false feedback and distrustful recommendation, which leads to inaccuracy of the measurement results. Because it is common that nodes intend to be selfish, the free-riding phenomenon often occurs in social networks, resulting in the decrease of network performance [12]. For free-riding, the so-called free-riders attempt to benefit from network resources of others without offering their own resources in exchange [13]. The goal of our work is to build an effective trust measurement model that can benefit social network services, such

as controlling feedback, recommendation, and strategy selection. In an effort to resolve the above problems, the main contributions of our work are summarized as follows.

1. To more accurately measure trust degree of a node, we introduce three novel evaluation factors which are service reliability, feedback effectiveness and recommendation credibility.
2. Another practical problem considered in this paper is the free-riding problem. We propose punishment mechanisms for specific trust and global trust, respectively, which is different from the existing works where statistic methods are commonly used. In our punishment mechanism, we employ the evolutionary game theory which is more flexible and effective.

The rest of the paper is organized as follows: "Related works" section reviews the related works and presents the motivation for our work. "The proposed trust measurement model" section introduces the proposed trust measurement model for social networks. "Simulations and performance analysis" section illustrates our simulation results and analysis of the results. Conclusions and future work are shown in "The proposed trust measurement model" section.

Related works

Much effort has been spent on trust measurement models to depict trust behaviors in complex networks. Trust measurement methods under open network environment and trust measurement methods based on Agent synergy are the most important trust measurement methods.

Trust measurement methods under open network environment

Beth et al. [14] first proposed a trust measurement method under open network environment. In their work, trust is regarded as direct trust and recommendation trust, and a probabilistic method is adopted to represent trust. The PeerTrust model [15] uses the transaction and the community background as the source of reputation feedback. It can act as a defense against some of the subtle malicious attacks, e.g., a seller develops a good reputation by being honest for small transactions and tries to make a big profit by being dishonest for large transactions. The EigenRep model [16] assumes that if the direct trust between a node and the destination node is higher, the recommendation trust is more reliable. The model uses direct trust to calculate the global trust. This model can effectively solve the bad effect caused by the malicious recommendation. Wang et al. [17] proposed a trust model based on Bayesian network. This model investigates how to describe different aspects of trust to obtain various properties of entities according to different scenes. Wang et al. [18] solved the problem of recommendation trust based on the Bayesian method. This method calculates recommendation trust based on experts' experience. Lu et al. [19] proposed an evaluation method of software reliability. It is a bottom-up calculation process of trust level that can decompose and synthetically derive a parallel structure, so that the trust value of a system can be calculated accurately. However, there are still some shortages about this kind of models. They only adopt probabilistic model to establish subjective trust model. In other words, subjectivity and uncertainty of trust are equivalent to randomness.

They also adopt the averaging method to calculate recommendation trust, which cannot reflect the real situations of a trust relationship.

Trust measurement methods based on Agent synergy

In Agent synergy, trust means that a collaborative agent can properly and nondestructively predict subjective possibility of a collaborative activity. The source of prediction is the goal service behavior that previous agent observes. Prediction results are affected by evaluation of important degree from the agent, such as key collaborative activities and secondary collaborative activities [20, 21]. The eBay trust model is one of the most successful cases. In this model, the entities evaluate each other after each transaction. The structure of this system is straightforward, and the computation cost is small. Because trust between agents is associated with other entities' subjective understanding and fuzziness, it cannot be described and managed by conventional and accurate logic. Subjective trust as a cognitive phenomenon, whose subjectivity and uncertainty present fuzziness, is often managed by Fuzzy Set-based methods. It not only reflects fuzziness of agent trust, but also describes the trust mechanism between agents with intuitive and concise semantics. Tang et al. [22] first proposed the definition and evaluation of trust based on the fuzzy set theory. They gave formalization and deducted rules of trust to construct a complete subjective trust management model. However, this kind of model fails to consider the cooperative cheating behaviors, which cannot detect the community of cooperative cheating.

In addition, some recent works are also remarkable. Shi et al. [23] proposed a dynamic P2P trust model based on the time-window feedback mechanism. The model considers the inherent connection among trust, reputation and incentive and the effect of time factor on the trust computation. Gan et al. [24] proposed a reputation-based multi-dimensional trust (RMDT) algorithm which makes use of a self-confident coefficient to synthesize the direct and recommendation trust to evaluate the nodes in a network. A multi-dimensional trust mechanism is also introduced to improve sensitivity of RMDT on a single attribute. Meng et al. [25] proposed the @Trust model. Bedi et al. [26] proposed a trust-based recommender system using ant colony for trust computation. Zhang et al. [27] proposed a trust evaluation method based on the cloud model.

These models have promoted the development of trust measurement models. However, most of the existing models failed to filter false feedback and distrustful recommendation, which leads to inaccuracy of measurement results. In addition, free-riding problem was not comprehensively considered in most of the existing trust measurement models. Considering these problems, this paper proposes a game theory-based trust measurement model for social networks. The proposed model introduces three novel evaluation factors which are service reliability, feedback effectiveness and recommendation credibility to more accurately measure the trust degree of a node.

The proposed trust measurement model

To describe the trust degree more accurately, this paper divides nodes into four categories, which are service nodes, feedback nodes, recommendation nodes and managed nodes. In social networks, *trust* represents the level of confidence about the reliability and correctness of entity's behaviors. *Service reliability* indicates the trustworthiness of service that service nodes provide; *feedback effectiveness* represents the trustworthiness

of feedback that feedback nodes return; *recommendation credibility* expresses the trustworthiness of recommendation that recommendation nodes give. In this paper, the global trust of the node i, denoted as T_i, is the probability of i being correct. The service reliability is denoted as ST ; the feedback effectiveness is denoted as FT ; and the recommendation credibility is denoted as CT .

In this paper, let i be a service node, j be a feedback node and k be a recommendation node; and M_i, M_j, M_k are the managed nodes of i, j, k, respectively.

When feedback node j requests a specific service s, the managed node M_j searches for the trust node which can provide service s. If there exists such a node, say node i, node j requests the service from node i. If not, M_j searches for the recommendation node k. Then, node k recommends a service node i with the maximum trust degree that can provide service s to node j. If there does not exist a recommendation node k, the transaction fails.

The trust measurement process

In this model, the specific feedback value $f_{v_{j,i}}$, given by the feedback node j, is known by the system. Therefore, we obtain the calculation method of service reliability based on the specific feedback value $f_{v_{j,i}}$, which is shown by Eq. (1).

$$\mathrm{ST}_i = \frac{\sum_{j\in \mathrm{set}(i)} f_{v_{j,i}} \cdot \lambda(j,i)}{\sum_{j\in \mathrm{set}(i)} \lambda(j,i)}, \quad \mathrm{FT}_j \geq \theta \tag{1}$$

In Eq. (1), set(i) is the set of feedback nodes that communicated with service node i, and θ is the threshold of feedback effectiveness. $\lambda(j,i)$ presents the influence effect of node j on node i. In addition, FT_j represents the feedback effectiveness of node j.

In social networks, some feedback nodes may evaluate some trust nodes maliciously and praise some distrustful nodes. Therefore, we should also evaluate the trust degree of $f_{v_{j,i}}$. In this paper, we calculate the feedback effectiveness based on similarity of specific feedback values. The feedback effectiveness of node j can be derived through a similarity formula as shown by Eq. (2).

$$\mathrm{FT}_j = \frac{\sum_{i\in \mathrm{set}(j,r)} f_{v_{j,i}} \cdot f_{v_{r,i}}}{\sqrt{\sum_{i\in \mathrm{set}(j,r)} f_{v_{j,i}}^2} \cdot \sqrt{\sum_{i\in \mathrm{set}(j,r)} f_{v_{r,i}}^2}} \tag{2}$$

In Eq. (2), set(j, r) presents the node-pair set that both nodes communicated with node i. Similar with the calculation method of service reliability, the recommendation credibility of node k is computed by Eq. (3).

$$\mathrm{CT}_k = \frac{\sum_{i\in \mathrm{Rset}(k)} \mathrm{ST}_i \cdot \lambda(k,i)}{\sum_{i\in \mathrm{Rset}(k)} \lambda(k,i)} \tag{3}$$

In Eq. (3), Rset(k) is the node set recommended by recommendation node k before. $\lambda(k,i)$ presents the influence effect of node k on node i. There are two factors affecting the value of $\lambda(k,i)$. One is the time interval $T = t_n - t_p$, t_n presents the current time, and t_p presents the time that node k recommends node i. Another is the connection degree $\omega_{k,i}$ of the relationship between node i and node k. Thus, $\lambda(k,i)$ is shown as Eq. (4).

$$\lambda(k,i) = \frac{1}{t_n - t_p} \cdot \omega_{k,i} \tag{4}$$

In this paper, how to determine the connection degree $\omega_{k,i}$ is considered. According to the successful transaction $\mathrm{Tr}_{\mathrm{suc}}$ and the number of total transactions $|Tr|$ between node k and node i, we determine the connection degree $\omega_{k,i}$, which is shown as Eq. (5). In Eq. (5), successful transaction $\mathrm{Tr}_{\mathrm{suc}}$ is an indicative function, if CT> Threshold, $\mathrm{Tr}_{\mathrm{suc}} = 1$, otherwise, $\mathrm{Tr}_{\mathrm{suc}} = 0$.

$$\omega_{k,i} = \frac{\sum_{m=1}^{|Tr|} \mathrm{Tr}_{\mathrm{suc}}}{|Tr|} \tag{5}$$

According to the above analysis, the global trust degree is shown in Eq. (6). In Eq. (6), α, β and γ are weights for service reliability, feedback effectiveness and recommendation credibility, and $\alpha + \beta + \gamma = 1$.

$$T_i = \alpha \cdot \mathrm{ST}_i + \beta \cdot \mathrm{FT}_i + \gamma \cdot \mathrm{CT}_i \tag{6}$$

If a service node provides distrust service, i.e. the service reliability is less than the service threshold ρ, the node will enter the service punishment cycle. In the service punishment cycle, a node should not provide any service. If a feedback node provides distrust feedback, i.e. the feedback effectiveness is less than the feedback threshold θ, the node will enter the feedback punishment cycle. In the feedback punishment cycle, a node should not request any service. If a recommendation node provides distrust recommendation, i.e. the recommendation credibility is less than the recommendation threshold δ, the node will enter the recommendation punishment cycle. In the recommendation punishment cycle, a node should not provide any recommendation.

The process of direct interaction is summarized in Algorithm 1. In this direct interaction algorithm, the service reliability ST and the feedback effectiveness FT_j will be output.

Algorithm 1 The process of direct interaction.

Input:
The feedback value from node j, $fv_{j,i}$;
The set of feedback nodes that communicated with service node i, $set(i)$;
The node-pair set that both nodes communicated with node i, $set(j,r)$;
The time interval, T;
The connection degree of the relationship between node j and node i, $\omega_{j,i}$;
Output:
Service reliability, ST_i;
Feedback effectiveness, FT_j;
1: A feedback node j requests service s. The managed node M_j of node j searches for a trusted node i that can provide service s. If there exists such a node i, go to 2. Otherwise, go to 7.
2: M_j requests service from the managed node M_i of node i. M_j checks that whether node j is in the feedback punishment cycle. If so, go to 7. Otherwise, go to 3.
3: Node i provides service for node j. Node j computes the service reliability of service s.
4: M_j computes whether the feedback from node j can be trusted. If the feedback effectiveness is larger than θ, go to 5. Otherwise, go to 8.
5: M_j sends the trust degree of service s to M_i. M_j updates the feedback effectiveness of node j. If the service reliability is larger than ρ, go to 6. Otherwise, go to 7.
6: M_i updates the service reliability of node i. Node i enters the service punishment cycle. Then go to 9.
7: M_i updates the service reliability of node i. Then go to 9.
8: M_j updates the feedback effectiveness of node j. Node j enters the feedback punishment cycle.
9: **return** ST_i and FT_j.

If there is not a trusted service node i that has interacted with the feedback node j directly, it needs a recommendation node k to recommend a trusted node j for service node i. Thus, the process of indirect interaction is summarized in Algorithm 2.

Algorithm 2 The process of indirect interaction.

Input:
The feedback value from node j, $fv_{j,i}$;
The set of feedback nodes that communicated with service node i, $set(i)$;
The node-pair set that both nodes communicated with node i, $set(j,r)$;
The node set recommended by recommendation node k before, $Rset(k)$;
The time interval, T;
The connection degree of the relationship between node j and node i, $\omega_{j,i}$;

Output:
Service reliability, ST_i;
Feedback effectiveness, FT_j;
Recommendation credibility, CT_k;

1: A feedback node j requests service s. The managed node M_j searches for the recommendation node k which can recommend node i that can provide service s. If there exists a recommendation node k, go to 2. Otherwise, go to 7.
2: Node k requests from the managed node M_i of node i. M_i checks that whether node j is in the feedback punishment cycle. If so, go to 7. Otherwise, go to 3.
3: Node i provides service s for node j. Node j computes the service reliability of service s.
4: Node j computes the recommendation credibility of the recommendation node k. M_k updates the recommendation credibility of node k. If the recommendation credibility of node k is less than δ, k enters the recommendation punishment cycle. In addition, M_j computes whether the feedback from node j can be trusted. If the feedback effectiveness is larger than θ, go to 5. Otherwise, go to 8.
5: M_j sends the service reliability of service s to M_i. M_j updates the feedback effectiveness of node j. If the service reliability of node i is larger than ρ, go to 6. Otherwise, go to 7.
6: M_i updates the service reliability of node i. Then go to 9.
7: M_i updates the service reliability of node i. Node i enters the service punishment cycle. Then go to 9.
8: M_j updates the feedback effectiveness of node j. Node j enters the feedback punishment cycle.
9: **return** ST_i, FT_j and CT_k.

The punishment mechanisms

To resolve free-riding problem in social networks, two punishment mechanisms are proposed for specific trust and global trust degree, respectively. According to specific trust (service reliability, feedback effectiveness and recommendation credibility), this paper designs three punishment cycles, so that to restrain the specific trust behaviors of nodes. According to global trust, this paper gives a game theory-based punishment mechanism [28] to resolve the free-riding problem for social networks.

For specific trust, we design a specific punishment mechanism and divide punishment cycles into service punishment cycle, feedback punishment cycle and recommendation punishment cycle. Once a node has selfish behaviors, the node will enter punishment cycle. In the period of punishment cycle, the node must be cooperative and honest to restore its reputation. In addition, other nodes reject to provide services to this node. After the punishment cycle, the node can replay transactions. According to different selfish behaviors, this paper gives different punishment strategies, which are shown as followings.

1. Service punishment cycle. If the service reliability $\mathrm{ST}_i < \rho$, node i will enter service punishment cycle. In the service punishment cycle, a node cannot provide service for other nodes and cannot request any service.
2. Feedback punishment cycle. If the feedback effectiveness $\mathrm{FT}_i < \theta$, node i will enter feedback punishment cycle. In the feedback punishment cycle, a node cannot request any service. However, it can provide service for other nodes.
3. Recommendation punishment cycle. If the recommendation credibility $\mathrm{CT}_i < \delta$, node i will enter recommendation punishment cycle. In the recommendation pun-

ishment cycle, a node cannot recommend any node. However, it can request and provide service for other nodes.

According to global trust, this paper proposes a punishment mechanism based on multi-strategy game to inspire nodes to select the strategies with high trust degree. T indicates the whole trust degree of node i. We divide trust degrees into five levels as shown in Table 1.

The five-strategy matrix is shown in Table 2. In Table 2, pr_A^{ij} is the profit value that node A obtains, if A game with B that A adopts strategy i, and entity B adopts strategy j. And pr_B^{ij} is the profit value that B obtains, if B game with A that B adopts strategy i, and A adopts strategy j. Through game analyzing nodes' behaviors in social networks, we can know that the multi-strategy game matrix is a symmetric matrix. In the analysis for dynamics model, this game is performed repeatedly. At the end of each stage of multi-strategy game, any participant's strategy as a historical information can be known by other participants. In addition, all participants select and update their strategies for next stage of game based on historical information.

To prevent selfish nodes from selecting the strategy with low trust degree to be their preferred strategy for getting more benefits, i.e. to restrain the free-riding phenomenon, a punishment mechanism is established to inspire nodes to select the strategies with high trust degree based on the multi-strategy game. In the case of $i < j$, the calculation method of benefits after adding punishment mechanism is shown by Eq. (7). When $i = j$, the calculation method is shown by Eq. (8).

$$\begin{aligned} \mathrm{PR}_A^{ij} &= \mathrm{pr}_A^{ij} + \mu \cdot (\mathrm{pr}_A^{ij} + \mathrm{pr}_B^{ij}), \quad i < j \\ \mathrm{PR}_B^{ij} &= \mathrm{pr}_B^{ij} - \mu \cdot (\mathrm{pr}_A^{ij} + \mathrm{pr}_B^{ij}) \end{aligned} \tag{7}$$

$$\mathrm{PR}_A^{ij} = \mathrm{pr}_A^{ij}, \quad i = j \tag{8}$$

Table 1 The division of trust levels

T_i	Trust
[0.8,1]	Trust 1
[0.6,0.8)	Trust 2
[0.4,0.6)	Trust 3
[0.2,0.4)	Trust 4
[0,0.2)	Trust 5

Table 2 The initial five-strategy game matrix

Trust level	Trust 1	Trust 2	Trust 3	Trust 4	Trust 5
Trust 1	$\mathrm{pr}_A^{11}, \mathrm{pr}_B^{11}$	$\mathrm{pr}_A^{12}, \mathrm{pr}_B^{12}$	$\mathrm{pr}_A^{13}, \mathrm{pr}_B^{13}$	$\mathrm{pr}_A^{14}, \mathrm{pr}_B^{14}$	$\mathrm{pr}_A^{15}, \mathrm{pr}_B^{15}$
Trust 2	$\mathrm{pr}_A^{21}, \mathrm{pr}_B^{21}$	$\mathrm{pr}_A^{22}, \mathrm{pr}_B^{22}$	$\mathrm{pr}_A^{23}, \mathrm{pr}_B^{23}$	$\mathrm{pr}_A^{24}, \mathrm{pr}_B^{24}$	$\mathrm{pr}_A^{25}, \mathrm{pr}_B^{25}$
Trust 3	$\mathrm{pr}_A^{31}, \mathrm{pr}_B^{31}$	$\mathrm{pr}_A^{32}, \mathrm{pr}_B^{32}$	$\mathrm{pr}_A^{33}, \mathrm{pr}_B^{33}$	$\mathrm{pr}_A^{34}, \mathrm{pr}_B^{34}$	$\mathrm{pr}_A^{35}, \mathrm{pr}_B^{35}$
Trust 4	$\mathrm{pr}_A^{41}, \mathrm{pr}_B^{41}$	$\mathrm{pr}_A^{42}, \mathrm{pr}_B^{42}$	$\mathrm{pr}_A^{43}, \mathrm{pr}_B^{43}$	$\mathrm{pr}_A^{44}, \mathrm{pr}_B^{44}$	$\mathrm{pr}_A^{45}, \mathrm{pr}_B^{45}$
Trust 5	$\mathrm{pr}_A^{51}, \mathrm{pr}_B^{51}$	$\mathrm{pr}_A^{52}, \mathrm{pr}_B^{52}$	$\mathrm{pr}_A^{53}, \mathrm{pr}_B^{53}$	$\mathrm{pr}_A^{54}, \mathrm{pr}_B^{54}$	$\mathrm{pr}_A^{55}, \mathrm{pr}_B^{55}$

When two nodes game with each other, for the node with higher trust degree, system will increase its rewards; for the node with lower trust degree, system will decrease its earnings. μ is a punishment parameter. Because the game matrix is a symmetric matrix, the punishment parameter is symmetric too. In this paper, if the value of (Trust i − Trust j) is bigger, μ will increase.

Complexity analysis

In this trust measurement model, we need to compute service reliability, feedback effectiveness and recommendation credibility for one node. According to a node's service reliability, the computational complexity is $O(l)$, where l represents that this node has provided services for l nodes ever before. According to a node's feedback effectiveness, the computational complexity is $O(m)$, where m indicates that m nodes provided feedbacks for this node. According to a node's recommendation credibility, the computational complexity is $O(n)$, where n represents that n nodes were recommended by this node before. Therefore, the computational complexity of a node's global trust is $O(l + m + n)$. The proposed trust measurement model can be computed in polynomial time, thus it is computationally efficient.

Simulations and performance analysis

In this section, we present the simulation results to verify the effectiveness of the proposed model. The hardware simulation environment is: Intel Core (TM) Duo 2.66 GHz CPU, 2GB Memory, Windows XP operating system, and Matlab 7.0 simulation platform. We simulate real online social networks in our experiments. In simulations, 1000 nodes are simulated. There are two kinds of nodes, normal nodes and malicious nodes. There are two types of normal nodes which are completely trustful nodes that can provide trustful service, feedback and recommendation, and mix-type trustful nodes that provide trustful feedback and recommendation, but random service quality. 20 % of files have low quality, i.e. malicious files. Malicious nodes include three types which are completely malicious nodes that provide questionable service, feedback and recommendation, random malicious nodes that provide questionable service, feedback and recommendation with a certain probability (in the simulations, the probability is 50 %), and disguised malicious nodes that provide trustful service and recommendation but questionable feedback. In the simulations, there are 1000 nodes, including 30 % completely trustful nodes, 30 % mix-type trustful nodes, 10 % completely malicious nodes, 20 % random malicious nodes, and 10 % disguised malicious nodes. The simulation setting is shown in Table 3 where 1 represents completely trustful, 0 represents completely questionable, and ε represents randomly trustful.

Table 3 The simulation setting

The style of nodes/trust	Service	Feedback	Recommendation
Ct	1	1	1
Tt	ε	1	1
Cm	0	0	0
Rm	ε	ε	ε
Dm	1	0	1

Experimental verification for specific trust

We measure the evolution of trust degree according to service reliability, feedback effectiveness and recommendation credibility respectively. Figure 1 presents the initial evolution trend of service reliability without any punishment mechanism. From Fig. 1, it can be seen that there exists free-riding problem. The proportions of completely malicious nodes (Cm) and random malicious nodes (Rm) increase steadily in first 50 generations. After that, network tends to be stable. Therefore, if there is not any punishment mechanism, malicious nodes will dominate the evolutionary direction of the whole network. Figure 2 shows the ideal condition by adopting punishment mechanism. From Fig. 2, it can be seen that completely trustful nodes (Ct) will dominant the evolutionary direction of the whole network with the proposed punishment mechanism. However, the proportion of any other type of nodes will decrease to 0. In this case, only completely trustful nodes (Ct) can survive in network. It will cause new nodes entering network to be dead, because they do not have any historical trust information. To resolve this problem, we adjust the strength of punishment to avoid cold boot problem, as shown in Fig. 3. From Fig. 3, it can be seen that the proportions of completely trustful nodes (Ct) and disguised malicious nodes (Dm) increase steadily, and tend to be stable in the end. It is because that disguised malicious nodes (Dm) can provide trustful service so that they can survive in network.

Figures 4, 5 and 6 show the evolution trend of feedback effectiveness. Figure 4 presents the initial evolution trend of feedback effectiveness without any punishment mechanism. From Fig. 4, it can be seen that the free-riding problem occurs. The proportions of completely malicious nodes (Cm), random malicious nodes (Rm) and disguised malicious nodes (Dm) increase steadily in first 50 generations. After that, network tends to be stable. Since disguised malicious nodes (Dm) provide distrustful feedback, they will obtain more benefits than the nodes that provide trustful feedback without any punishment mechanism. Figure 5 shows the ideal case by adopting punishment mechanism. From Fig. 5, it can be seen that

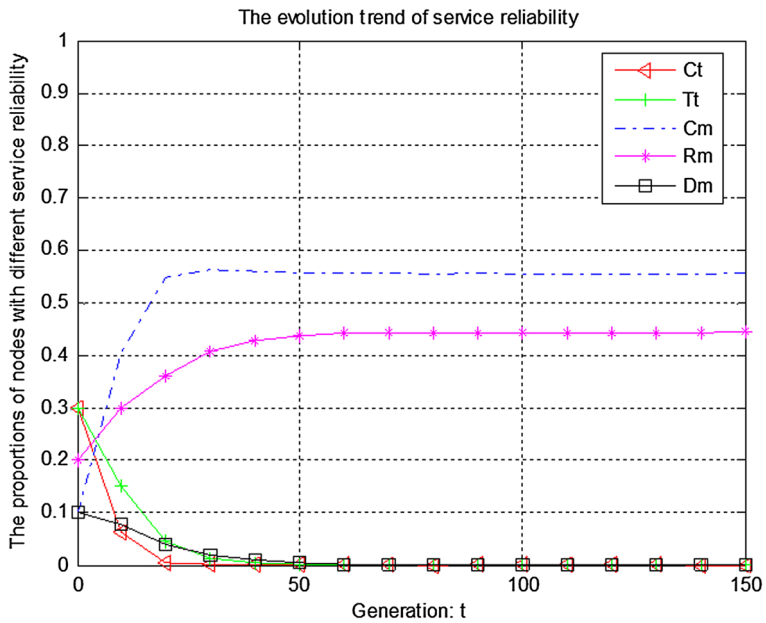

Fig. 1 The initial evolution trend of service reliability without punishment

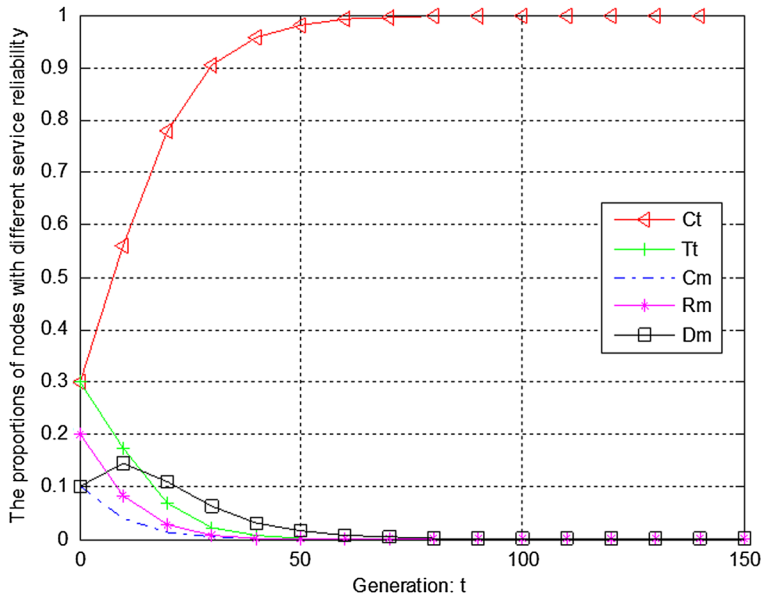

Fig. 2 The evolution trend of service reliability with punishment

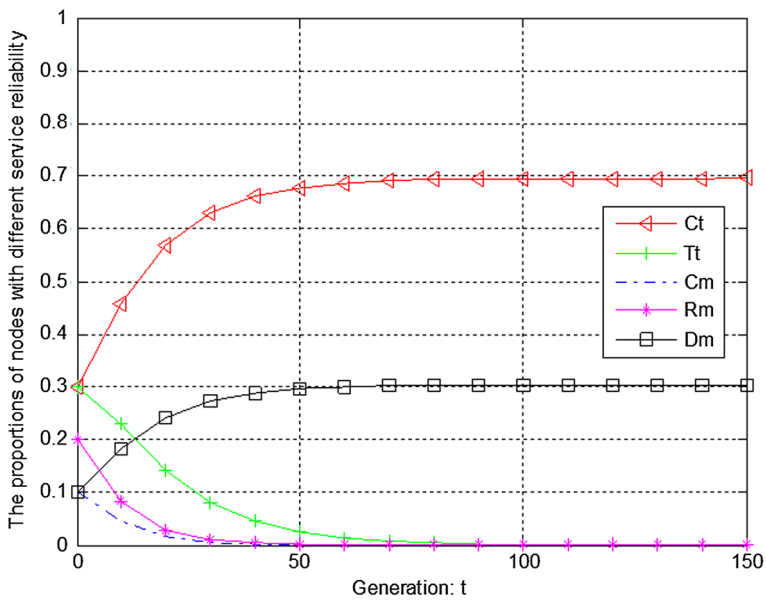

Fig. 3 The evolution trend of service reliability with adjusted punishment

completely trustful nodes (Ct) will dominate the evolutionary direction of the whole network with the proposed punishment mechanism. However, the proportion of any other type of nodes will decrease to 0. In this case, only completely trustful nodes (Ct) can survive in network. Figure 6 shows the evolutionary results after adjusting the strength of punishment. It can be seen that the proportions of completely trustful nodes (Ct) and mix-type trustful nodes (Tt) increase steadily, and tend to be stable in the end. This is because that mix-type trustful nodes (Tt) can provide trustful feedback, and they will survive in network.

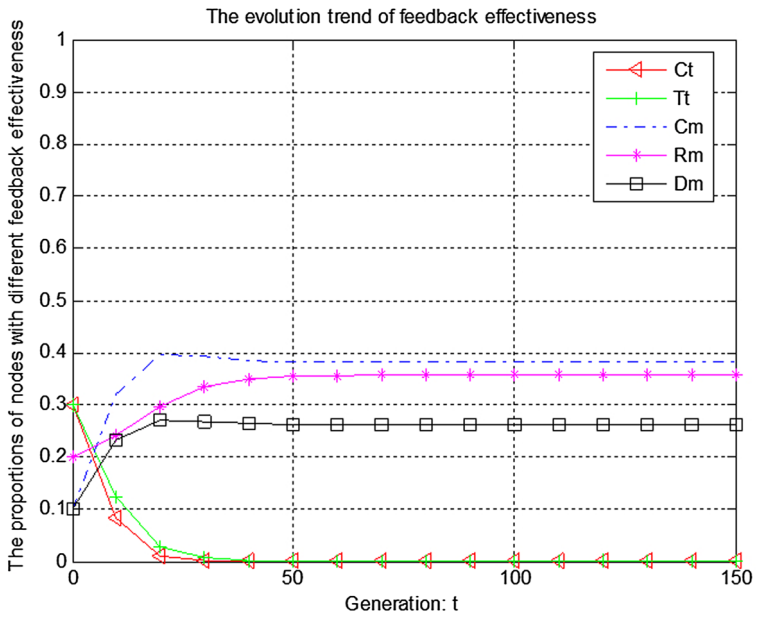

Fig. 4 The initial evolution trend of feedback effectiveness without punishment

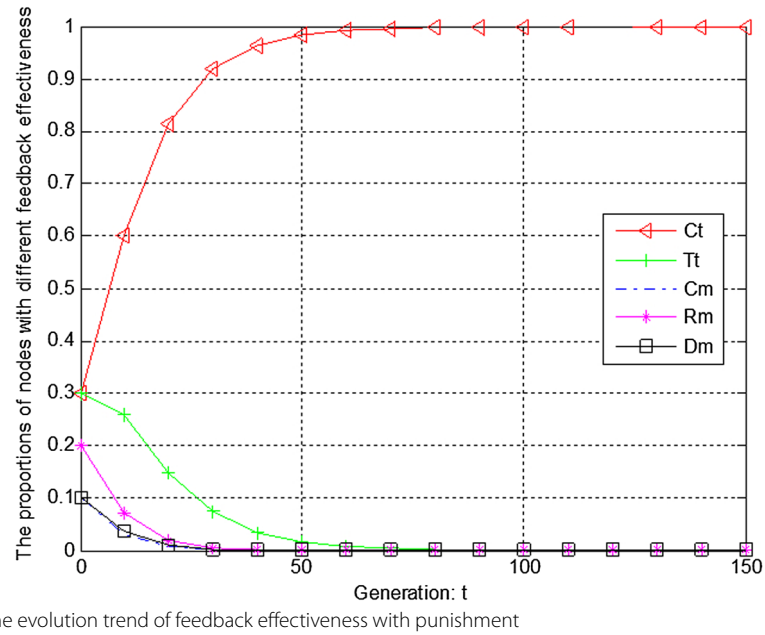

Fig. 5 The evolution trend of feedback effectiveness with punishment

Figures 7, 8 and 9 show the evolution trend of recommendation credibility. Figure 7 presents the initial evolution trend of recommendation credibility without any punishment mechanism. From Fig. 7, it can be seen that there is free-riding problem in network. The proportions of completely malicious nodes (Cm) and random malicious nodes (Rm) increase steadily in first 50 generations. After that, network tends to be stable. Figure 8 shows the ideal case by adopting punishment mechanism. From Fig. 8, it

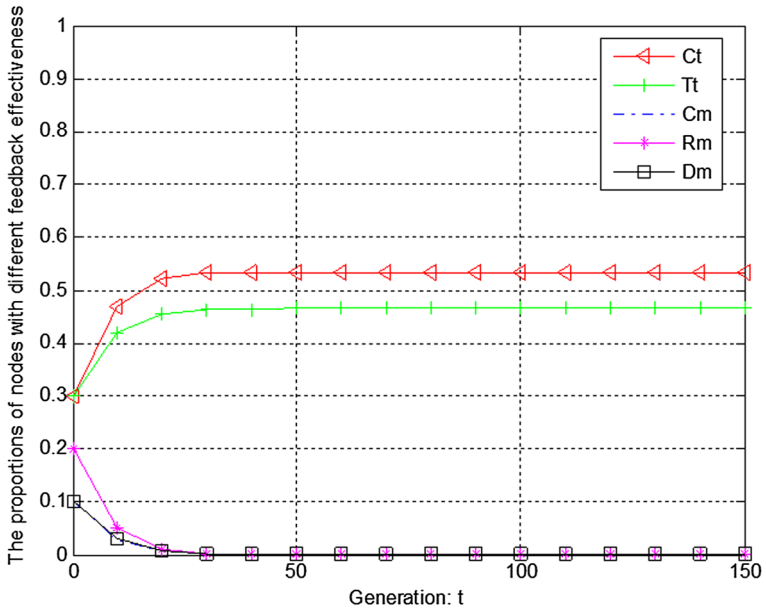

Fig. 6 The evolution trend of feedback effectiveness with adjusted punishment

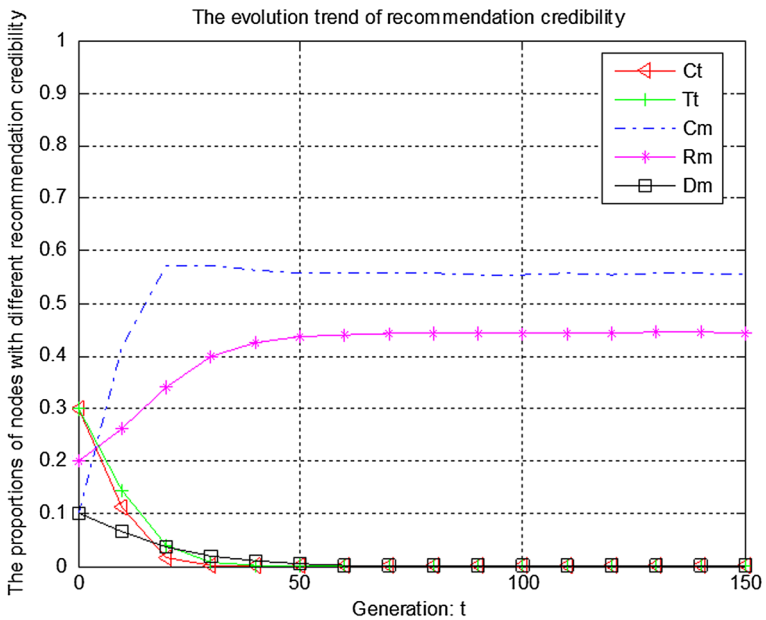

Fig. 7 The initial evolution trend of recommendation credibility without punishment

can be seen that completely trustful nodes (Ct) will dominate the evolutionary direction of the whole network with the proposed punishment mechanism. However, the proportion of any other type of nodes will decrease to 0. In this case, only completely trustful nodes (Ct) can survive in network. Therefore, Fig. 9 shows the evolutionary results after adjusting the strength of punishment. It can be seen that the proportions of completely trustful nodes (Ct) and mix-type trustful nodes (Tt) increase steadily, and tend to

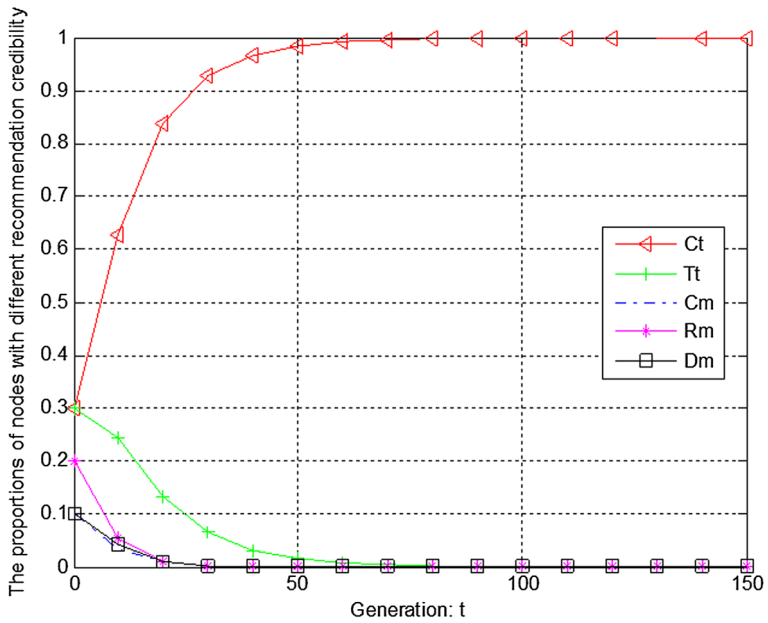

Fig. 8 The evolution trend of recommendation credibility with punishment

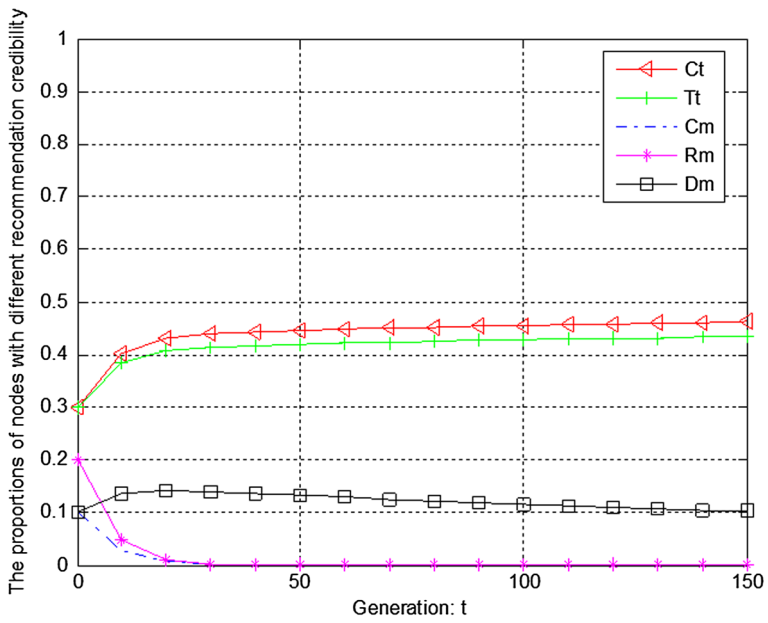

Fig. 9 The evolution trend of recommendation credibility with adjusted punishment

be stable in the end. The reason is that mix-type trustful nodes (Tt) can provide trustful recommendation, and they will survive in network.

Experimental verification for global trust

We also verify the effectiveness for global punishment mechanism. According to the simulations for specific trust, this section combines the measurement results of service

reliability, feedback effectiveness and recommendation credibility to measure the trust evolution of the whole network. Figure 10 shows the initial evolution results. From Fig. 10, we can see that if there is not any punishment mechanism, the free-riding phenomenon will occur. The free-riding problem can be resolved by employing global punishment mechanism as shown in Fig.11.

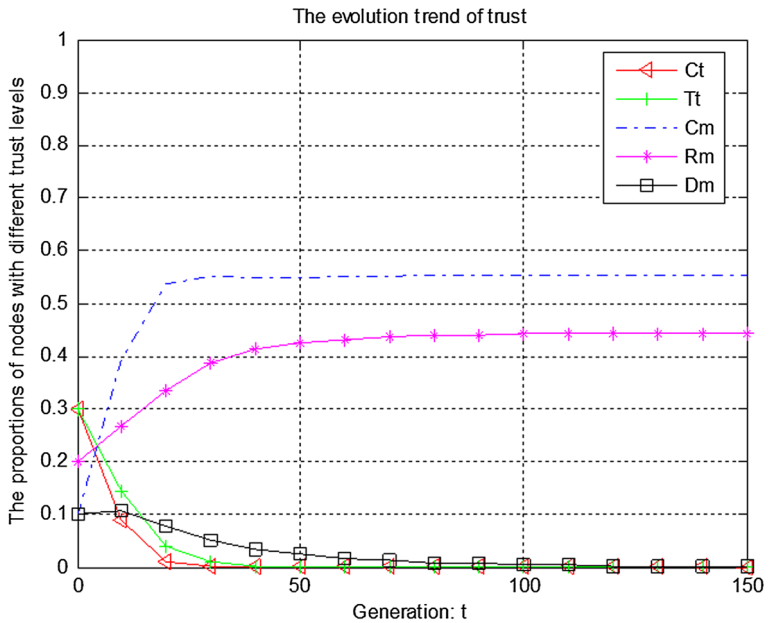

Fig. 10 The initial evolution trend of trust without punishment

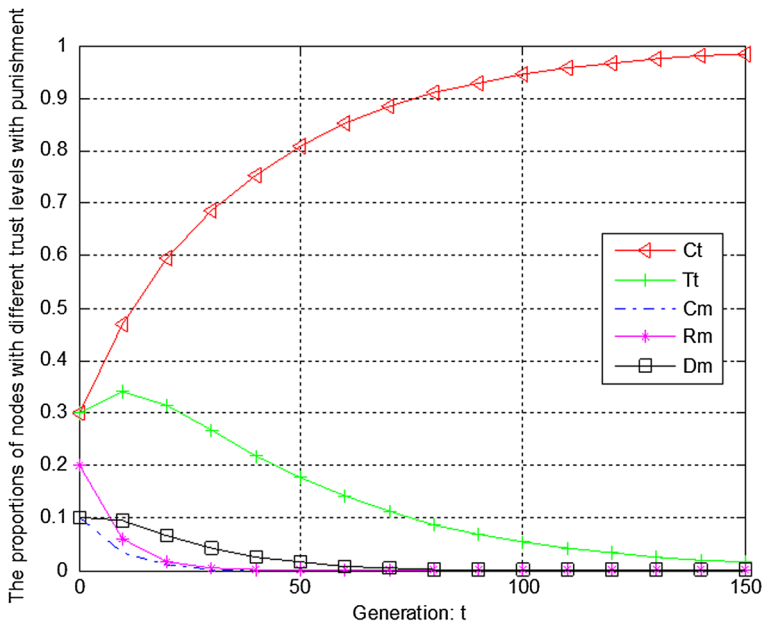

Fig. 11 The evolution trend of trust with punishment

Conclusion

In social networks, trust relationships between nodes are the basis of service transactions. However, the establishment of trust relationship is a complex progressive process depending on interaction history, trust recommendation, trust management and so on. Therefore, modeling trust relationship needs to take into account multiple decision factors. Considering the existing problems of trust models, this paper proposes a game theory-based trust measurement model for social networks where trust degree is determined by three aspects, which are service reliability, feedback effectiveness, and recommendation credibility. Based on game theory, we propose punishment mechanisms according to specific trust and global trust respectively to resolve free-riding problem. The simulation results show the effectiveness of the proposed trust measurement model. It also shows that the proposed punishment mechanisms can prevent free-riding phenomenon effectively. As a future work, we will further investigate more specific trust relationships between nodes, e.g., family, best friends, and classmates. We plan to study how to find ordered trust node set in social networks.

Authors' contributions

YW designed the proposed trust measurement model, performed the experiments analysis and drafted the manuscript. ZC conceived of the study, and participated in its design and coordination and helped to draft the manuscript. GY participated in the design of the study, and helped to direct the research contents. YG carried out the acquisition of data, and helped to perform experiments. XT helped to analyze the performance of the proposed trust measurement model. QH helped to analyze the feasibility of the proposed trust measurement model. All authors read and approved the final manuscript.

Author details

[1] School of Computer and Control Engineering, Yantai University, Qingquan Road, Yantai 244005, China. [2] School of Mathematics and Information Science, Yantai University, Qingquan Road, Yantai 244005, China. [3] College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China. [4] Department of Computer Science, Georgia State University, Atlanta 30303, Georgia.

Acknowledgements

This work is supported by the National Natural Science Foundation of China under Grants No. 61502410, No. 61572418, No. 61370084, No. 61502116, the Natural Science Foundation of Shandong Province under Grants No.ZR2013FQ020, ZR2014FQ026, ZR2013FQ023 and ZR2015PF010.

The short version of this manuscript is in CSoNet 2015 [1].

Competing interests

The authors declare that they have no competing interests.

Received: 25 September 2015 Accepted: 10 May 2016
Published online: 20 May 2016

References

1. Wang Y, Cai Z, Yin G, Gao Y, Pan Q. A trust measurement in social networks based on game theory. In: The 4th international conference, CSoNet 2015 (2015).
2. Al-Oufi S, Kim H-N, Saddik AE. A group trust metric for identifying people of trust in online social networks. Expert Syst Appl. 2012;39:13173–81.
3. Han M, Yan M, Cai Z, Li Y. An exploration of broader influence maximization in timeliness networks with opportunistic selection. J Netw Comput Appl. 2016;63:39–49.
4. Li J, Cai Z, Yan M, Li Y. Using crowdsourced data in location-based social networks to explore influence maximization. In: The 35th annual IEEE international conference on computer communications (2016).
5. He Z, Cai Z, Wang X. Modeling propagation dynamics and optimal countermeasures of the social network rumors. In: The 35th IEEE international conference on distributed computing systems (2015).
6. Wang Y, Yin G, Cai Z, Dong Y, Dong H. A trust-based probabilistic recommendation model for social networks. J Netw Comput Appl. 2015;55:59–67.
7. Zheng X, Cai Z, Li J, Gao H. An application-aware scheduling policy for real-time traffic. In: The 35th IEEE international conference on distributed computing systems (2015).
8. Enembreck F, Barthes J-PA. A social approach for learning agents. Expert Syst Appl. 2013;40:1902–16.
9. Wang Q, Wang J, Yu J, Yu M, Zhang Y. Trust-aware query routing in p2p social networks. Int J Commun Syst. 2012;25:1260–80.

10. Zhang L, Wang X, Lu J, Ren M, Duan Z, Cai Z. A novel contact prediction based routing scheme for dtns. Trans Emerg Telecommun Technol. 2014;. doi:10.1002/ett.2889.
11. Zhang L, Cai Z, Lu J, Wang X. Mobility aware routing in delay tolerant networks. Pers Ubiquit Comput. 2015;19:1111–23.
12. Wang X, Lin Y, Zhao Y, Zhang L, Liang Y, Cai Z. A novel approach for inhibiting misinformation propagation in human mobile opportunistic networks. Peer-to-Peer Netw Appl. 2016;9:1–18.
13. Feldman M, Chuang J. Overcoming free-riding behavior in peer-to-peer systems. Newsl ACM SIGecom Exch. 2005;5:41–50.
14. Beth T, Borcherding M, Klein B. Valuation of trust in open networks. In: Lecture notes in computer science, vol. 875; 1994; p. 1–18.
15. Xiong L, Liu L. Peertrust: supporting reputation-based trust in peer-to-peer communities. IEEE Trans Data Knowl Eng. 2004;16:843–57.
16. Kamvar S, Schlosser M. Eigenrep: reputation management in p2p networks. In: Proceedings of the 12th international world wide web conference. 2003. p. 123–34.
17. Wang Y, Lv J, Feng X, Zhang L. A trust measurement and evolution model for internetware. J Softw. 2006;17:1–2.
18. Wang Y, Vassileva J. Bayesian network-based trust model. In: Proceedings of the IEEE computer society WIC international conference on web intelligence. 2003. p. 372–78.
19. Lu W, Xu F, Lv J. An approach of software reliability evaluation in the open environment. Chin J Comput. 2010;33:452–62.
20. Zhu M, Jin Z. Approach for evaluating the trustworthiness of service agent. J Softw. 2011;22:2593–609.
21. Chang Z, Mao X, Qi Z. Component model and its implementation of internetware based on agent. J Softw. 2008;19:1113–24.
22. Tang W, Chen Z. Research of subjective trust management model based on the fuzzy set theory. J Softw. 2003;14:1401–8.
23. Shi Z, Liu J, Wang Z. Dynamic p2p trust model based on time-window feedback mechanism. J Commun. 2010;31:120–9.
24. Gan Z, Ding Q, Li K, Xiao G. Reputation-based multi-dimensional trust algorithm. J Softw. 2011;22:2401–11.
25. Meng X, Ding Y, Gong Y. @trust: A trust model based on feedback-arbitration in structured p2p network. Comput Commun. 2012;35:2044–53.
26. Bedi P, Sharma R. Trust based recommender system using ant colony for trust computation. Expert Syst Appl. 2012;39:1183–90.
27. Zhang S, Xu C. Study on the trust evaluation approach based on cloud model. Chin J Comput. 2013;36:422–31.
28. Chen J, Kiremire AR, Brust MR, Phoha VV. Modeling online social network users' profile attribute disclosure behavior from a game theoretic perspective. Comput Commun. 2014;49:18–32.