J. Software Engineering & Applications, **2009, 2: 283-287**
doi:10.4236/jsea.2009.24036 Published Online November 2009 (http://www.SciRP.org/journal/jsea)

Research on the Trust Model Based on the Groups' Internal Recommendation in E-Commerce Environment

Nan REN[1], Qin LI[2]

School of Economics and Management, Jiangsu University of Science & Technology, Jiangsu, China.
Email:[1]rennan_hb@sohu.com, [2]lei731@gmail.com

Received June 30th, 2009; revised August 2nd, 2009; accepted August 7th, 2009.

ABSTRACT

The trust plays an extremely important role in online shopping. In order to make online shopping trusty, this paper puts foreword a new trust model in e-commerce environment GIR-TM (Groups' Internal Recommendation Trust Model). First, it regarded the network as a combination of groups, and then did the internal recommendation based on these groups. The GIR-TM, in the process of recommendation, distinguished clearly between the trust degrees of recommendation node and the trust degrees of recommended node, and then calculated the integrated credibility value of the recommended node according to the weight of recommendation node in the group, the partial trust degree and the degree of recommendation when the recommendation node recommends the recommended node, and the overall credibility value of recommended node as well. Lastly through listing the experimental data and comparing with the HHRB-TM (History and Honest Recommendation Based Trust Model) on the same condition, it is verified that GIR-TM is feasible and effective.

Keywords: *E-commerce, Groups, Internal Recommendation, the Credibility Value*

1. Introduction

Trust is the basis of co-operation, and it plays an extremely important role in online shopping. At present, there are still some issues in peer-to-peer trust model, such as over-reliance on the recommendations of others, trust calculations' inaccuracy, difficulty of dealing with the united malicious attacks, dynamic strategy malicious nodes and so on [1]. In order to promote e-commerce to develop stably and quickly, researchers around the world have done some researches in the field of trust model: M. H. Hanif Durad *et al.* [2] discussed how to utilize the trust management to strengthen its security in the grid environment. G. Liang *et al.* [3] discussed how to use the trust management system such as reputation systems to solve the trust problem among the users. F. Almenarez *et al.* [4] discussed how to use the auto-negotiation technologies to solve the dynamic trust management in general environment. Jøsang A *et al.* [5] pointed out that in the P2P environment, the core problem of the trust mechanism based on the reputation were that: in the given application, what trust factors are the most appropriately used to infer the measurement of trust and reputatition? How to generate, acquire and aggregate the information about these trust factors? Whether the trust mechanisms can resist various attacks which are controlled by strategic individuals? Li Wen [6] put forward a History and Honest Recommendation Based Trust Model in Peer-to-Peer Networks, and improved the evaluation algorithm of trust. Chen Xiaoliang [7] classified the impact factors, built the calculation model of initial trust, and figured out that Consumers had distrust of web sites and online stores which is a bottleneck in e-commerce development.

To solve the core problem that consumers are lacking in trust of e-commerce currently, this paper establishes a trust model based on the groups' internal recommendation in E-commerce environment, in which the comprehensive credibility value of recommended node is calculated by the weight of recommendation node in the group, the partial trust degree when recommendation node recommends recommended node, and the degree of recommendation and the overall credibility value of recommended node. The calculated result can supply the basis for restraining malicious acts effectively (such as joint defamation, malicious exaggeration, providing false information, etc.).

2. GIR-TM

2.1 Group Mechanisms

2.1.1 Group's Structure

First of all, according to the credibility value of every node, the peer-to-peer network can be divided into three small collections [8]:

$$WholeN = \{Good, Bad, \phi\}$$

In which: *Good* is a collection of nodes with good credibility value gained through the good service provided to others.

Bad is a collection which is composed of malicious nodes;

ϕ is a collection of nodes whose credibility are unsure.

When a node p joins in the network, it is put into the collection ϕ, and its credibility value is 0. The nodes with good performance can increase their credibility value into a particular value until it is placed into the collection *Good*. On the contrary, if the node performs badly and its credibility value will be less than 0, then it will be moved to the collection *Bad*, meanwhile, the information about its bad performance will be notified in the whole network. As received the notice, the nodes will not trade with the notified node any more and then cut off the connection with it.

Then, the nodes in collection *Good* will be grouped. Some nodes in this collection have a certain credibility value, higher reliability and stability, which compose the group called Trusted Group (TG), and we assume that its scale is Q. When the credibility value of a node in collection *Good* reaches a certain degree, it can set up its own trust group or apply to join in the existing groups. Those nodes that have not joined in the TG are put into another group (*AG*).

The administrator of a TG is a node which creates the group initially. Administrators must maintain a connection with all the nodes inside of group, and we assume that each node in group maintains k as external connection. Administrators can choose which node to join in, while the node can also choose its trust group. In order to clarify the information of each trade and the credibility value of each node in trading, we suggest that it is necessary to establish a Node's Information (NI) for each node in the net to record its own series of activities, just as shown in Table 1.

After a node establishes its own TG, the node needs to notify its information to the nodes which do not belong to any TG and the administrators of other trust groups (TGs). After the administrator of another TG receives the notice, it will inform the message to the nodes in its own group.

According to the above strategy, the entire network is divided into n TGs, collection *Bad*, collection ϕ, as well as *AG*. As shown in Figure 1, we assume that all nodes in collection *Good* have entered the trust group, just as the two trust groups TG_1 and TG_2 in Figure 1, and A, B respectively represent the administrators of TG_1 and TG_2, and the number of their foreign connection is K (K = 1, 2 ... n).

2.1.2 Connection of Nodes

After the node's credibility value in collection ϕ reaches a certain trust degree R_ϕ (the credibility value of collection ϕ) through the good behavior, it will be moved into collection *Good* according to the principle "two-way choice", that is, the node can choose trust group, and the administrator selects a node, while the node can choose to stay in *AG*, join in or build a TG.

As shown in Figure 1, through transacting with other nodes, node C's credibility value satisfies $R_C \geq R_\phi$, then it can enter the collection *Good*. When the node C decides to join in the TG_1, it needs to send application information to the administrator A, the information includes its ID and the kinds of commodities S_c .After receiving the application, the administrator A must carry out the following steps:

Step1: First of all, calculate the number of the nodes in TG_1, if the number reaches Q, reject the node C's connection, otherwise continue to Step 2;

Step2: Judge that whether the node c is a malicious node or not, if it is, refuse its connection, otherwise continue to Step 3;

Step3: The administrator reviews the node C's credibility value, R_{TG_1} is the credibility value of TG_1, if $R_{TG_1} > R_c \geq R_\phi$, reject the node C's connection, otherwise continue to Step4;

Step4: The node p belongs to TG_1, if $\forall$ p$\in$ TG_1, the kinds of commodities of p satisfies $S_p \neq S_c$, the node C is allowed to joining in, continue to Step5;

Table 1. The Node's Information (NI)

Group ID	Group Administrator	Value of credibility	Transaction node				
			Node's ID	Number of successful	Number of failure	Credibility Value	Integrated credibility value
			……				
			……				

Step5: The administrator allows the node C to join in TG_1, and establishes a connection with the node C;

Step6: C creates connection with all the nodes in this group and its own NI table.

After C receives the refused news, it can choose other TG, and repeat the above steps. If it is rejected by all administrators, it can set up its own group or stay in *AG*.

2.1.3 Departure of Nodes

Nodes' departure has two ways: one is active departure, and the other is passive departure. Active departure can withdraw from the peer-to-peer actively when the node completes the transactions. If the node is also the administrator, before it leaves, it will choose the node with the highest credibility value in the group as administrator, and copy the information of the group to it. Passive departure happens when a node's credibility value is less than the credibility value of the group, and the administrator ejects it out of the trust group, and puts it into collection *Bad*.

2.2 Internal Recommendation Mechanisms

2.2.1 Recommendation Ideas

As same as the real life, and on the basis of the Trust Group, the basic framework of GIR-TM is established, as shown in Figure 2,

In the Figure 2, the closed circle equals to a TG, in which each node (A, B, and C…) has its own transaction nodes. In order to clarify the information of each transaction and the credibility value of each transaction node, we proposed to establish a table called Node's Information (table NI) for every node. The table NI includes the ID, administrators of the group where the node stays, and the credibility value of node, as well as the transaction information such as the ID of other transactions nodes, the number of successful transactions and one of failed transactions, the credibility value of other nodes and the integrated credibility value (the calculation of the integrated credibility value is referred to the following section) after transacting. Assuming that A has transacted with the node E and with the completion of each transaction, the node A will refresh its own NI table (this NI table is to be shared, the shared region is the integrated credibility value with a recommendation tip sign), and then through comparing to judge whether the integrated credibility value of E meets the requirements or not, that is, if the integrated credibility value of E is greater than the overall credibility value of the group which includes node A, it will be signed with the recommended tip, which will be shared by the other nodes in this group, otherwise, giving up their recommendation.

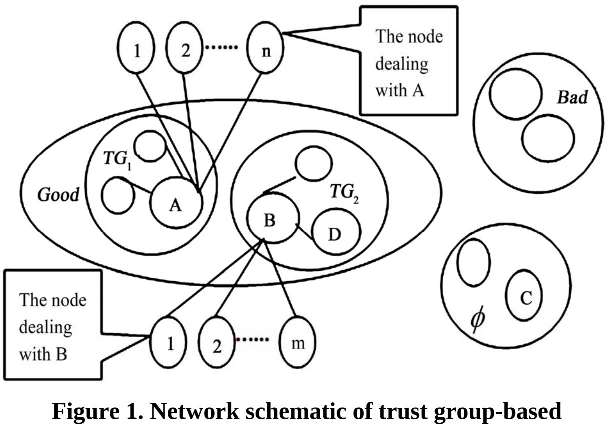

Figure 1. Network schematic of trust group-based

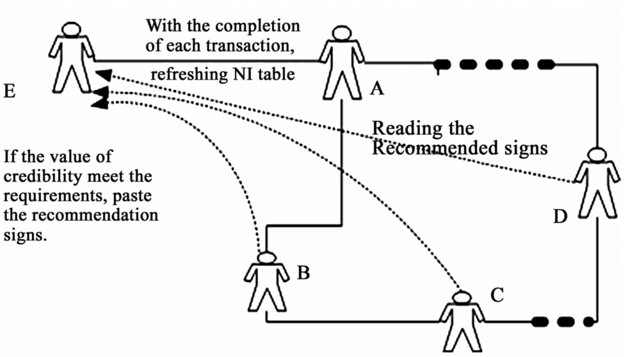
With the completion of each transaction,
refreshing NI table
E
A
Reading the Recommended signs
If the value of credibility meet the requirements, paste the recommendation signs.
D
B
C

Figure 2. Basic framework of groups' internal recommendation trust model

2.2.2 Calculation of the Integrated Credibility Value

In order to calculate the Integrated Credibility Value of GIR-TM in Figure 2, we firstly introduced the following 3 definitions [9] about the partial trust, the degrees of recommendation, and the integrated credibility value:

Definition2.1 partial trust: $L_{u\to v}$ represents the partial view of the node U on node V, which directly comes from the historical transaction experience between them, given that

$$L_{u\to v} = \frac{S_{UV}}{Nuv} \qquad (1)$$

In which, S_{uv} represents the number of successful transaction with node V in view of U;

N_{uv} represents the number of total transactions between U and V within the last interval time Δt (Δt is illustrated that the trust model pay more attention to the time limit of the nodes' behavior). If N_{uv} = 0, then $L_{u\to v}$ = 0.

Definition 2.2 the degrees of Recommendation: the degrees of recommendation how node X recommends the node V is calculated as follows:

$$R_{x\to v} = \frac{S_{xv} - F_{xv}}{S_{xv} + F_{xv}} \qquad (2)$$

In which, F_{uv} represents that in node U's view, the number of failure transaction with node V. If $S_{xv} + F_{xv}$ =0, then set $R_{x\to v}$=0. Or if $S_{xv} - F_{xv}$ <0, then set $R_{x\to v}$=0. As shown in definition 2.2, if the nodes perform badly in the trading, and gain poor assessment from others, then his credibility value will not be increased, but drastically reduced. So to some extent, this way can restrain the malicious acts of malicious nodes.

Definition 2.3 the integrated credibility degree: set $G_{u\to v}$ representing the projection of the trust level which node U trusts node V (U$\neq$V) in the trust scope λ:

$$G_{u\to v} = [\alpha\ L_{u\to v} + (1-\ \alpha)T_v] \times \lambda \quad (3)$$

Here T_v is the overall credibility degree of the node V, $T_v < 1$. In which, α is a constant and $0 < \alpha < 1$, and λ is the trust scope, $\lambda > 1$.

Based on the quantitative description of the trust mentioned above, Document [6] put forward a HHRB-TM (History and Honest Recommendation Based Trust Model) in Peer-to-Peer Networks, and the corresponding integrated trust credibility value is calculated as the Formula (4):

$$G_{u\to v} = \omega_u\ L_{u\to v} + (1-\ \omega_u) \times (\sum_{i=1}^{N} R_{x\to v} \times Cr_x) \quad (4)$$

In which, Cr_x is the credibility value of node X, ω_u [10] is a weight factor about node U referring to its own direct history transaction experience. ω_u is dynamic, and changes with the time or the number of transactions.

But the Formula (4) does not consider the weight of recommendation node, and the role of the node with high credibility value does not play completely. Aiming at such problem, this paper put forward the definition of comprehensive weights, and the calculation formula is:

Definition 2.4 comprehensive weights: set Gt_x as comprehensive weights of a trust group, and the calculation formula is:

$$Gt_x = \frac{Cr_x}{\sum_{i=1}^{m} Cr_i} \quad (5)$$

Here Cr_x is the credibility value of node X, $\sum_{i=1}^{m} Cr_i$ is the sum of the credibility value of all the nodes in the group in which node X is included.

According to the principle of the higher credibility value, the higher credibility, the more accurate recommendation information, and then the bigger contribution rate, the weight of recommendation node is added into the calculation of the credibility value of recommended node, just as:

$$Ct_v = Gt_x \times R_{x\to v} \times Cr_x \quad (6)$$

In which, Gt_x is comprehensive weight of the trust group in which the recommendation node X is included;

$R_{x\to v}$ is the recommending evaluation that recommendation Node X puts foreword on the recommended node V;

Cr_x is the overall credibility value of recommended node.

Ct_v is gained by the feedback information about the Node V's recommendation, $Ct_v \le 1$;

Combining the partial trust with recommendation trust through (7):

$$G_{u\to v}' = \omega_u\ L_{u\to v} + (1-\omega_u)\, Ct_v \quad (7)$$

In which, $G_{u\to v}$'is the integrated credibility value to represent how the node U recommends node V;

$L_{u\to v}$ represents accumulated direct history transaction experience when the node U transacts join with node V;

So, the integrated credibility value is as follows:

$$G_{u\to v}' = \omega_u\ L_{u\to v} + (1-\omega_u)\, Gt_x \times R_{x\to v} \times Cr_x \quad (8)$$

3. Model Validations

We compared HHRB trust model with the trust model GIR in this article in the same experiment situation. In order to verify the model, enumerating 20 groups of experimental data, and assuming S_{uv}=380, N_{uv}=430, ω_u=0.9.

These 20 groups of experimental data include the number of successful transactions S_{xv}, the number of failure transactions F_{xv} and the credibility value of each node Cr_x. Each group of experimental data is listed randomly, because the GIR-TM is based on the TG. We could think the nodes in the group are reliable, and the failure rata is smaller, and then we could abide the principle that the listed data of the failure transactions number is always less than the successful transactions number, in addition, the failure transactions number needs to be much less. And the Cr_x of each node needs to be more than 0.5 (because every node is in the TG and should have a higher credibility value, and we assume that the threshold value of each TG's credibility value is 0.5). As the real life, the reputable people will form a group, and they are all reliable to have much more possibility to transact each other successfully. In generally, these experimental data are realistic and are shown in Table 2:

The experimental results in Figure 3 are calculated according to Table 2. As shown in Figure 3 (GN is group number), although the integrated credibility value of the HHRB model fluctuates sometimes, the integrated credibility values obtained by the HHRB model and the GIR model are more or less the same, just between 0.8825 and 0.8838. So it can be concluded that the GIR-TM is verified to be feasible and effective.

Table 2. Experimental data

	S_{xv}	F_{xv}	Cr_x		S_{xv}	F_{xv}	Cr_x		S_{xv}	F_{xv}	Cr_x		S_{xv}	F_{xv}	Cr_x
1	250	3	0.6	6	79	1	0.91	11	31	0	0.65	16	283	2	0.95
2	60	1	0.7	7	301	3	0.68	12	173	0	0.92	17	291	3	0.98
3	80	1	0.57	8	123	2	0.73	13	92	1	0.835	18	68	1	0.74
4	99	0	0.73	9	161	1	0.88	14	182	2	0.72	19	136	0	0.9
5	59	1	0.82	10	83	1	0.79	15	259	2	0.935	20	197	1	0.54

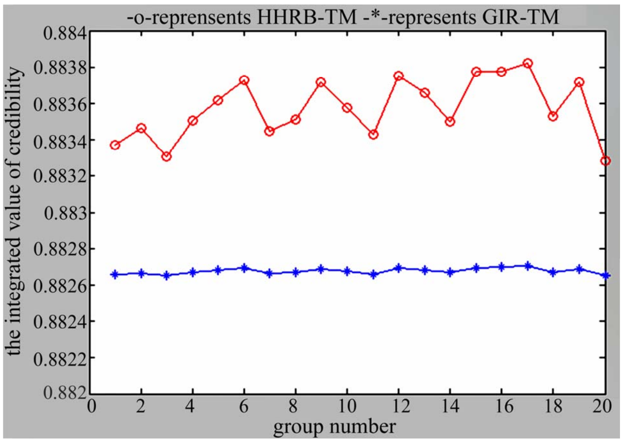

Figure 3. Comparing the integrated credibility value between $G_{u\to v}$ and $G_{u\to v}$

4. Summary and Prospect

The paper puts forward a Trust Model Based on the Groups' Internal Recommendation by analyzing the current issue of trust in electronic commerce. The model is composed of Trust Group and internal recommendation mechanism. Generally speaking, the achievements are as follows:

1) Put forward the GIR model based on the TG;

2) Put forward the algorithm of the integrated credibility value of the GIR model by improving the algorithm of the integrated credibility value of the HHRB;

3) Verify the effectiveness of the GIR model by comparing it with HHRB model.

Theoretically, the model can provide a good trading environment for customers, and reduce the occurrence of malicious actions. However, besides effectiveness verification of the GIR model, the model needs to be verified in the following aspects:

1) Verify the fairness of the transaction and the accuracy of the algorithm described in the model;

2) Further improve the model according to tested results;

3) Based on this paper, study on the rewarding and punishment mechanism to reward the reputable people and punish the malicious node.

5 Acknowledgments

This research was supported by Qing Lan Project of Jiangsu Province of China.

REFERENCES

[1] X. Li and L. Liu, "A reputation-based trust model for peer-to-peer e-commerce communities[C]," Proc of IEEE Conference on E-Commerce, ACM Press, California, pp. 275–284, 2003.

[2] M. H. Hanif Durad and C. Yuazlda, "A vision for the trust managed grid [A], Proceedings of the sixth IEEE International Symposium on Cluster Computing and the Grid [C], IEEE Computer Society Washington, DC, USA, 2006.

[3] G. Liang, L. Junzhou, and X. Yaobin, "Developing and managing trust in peer-to-peer systems [A]," proceedings of the 17th International Conference on Database and Expert Systems Applications[C], IEEE Computer Society Washington，DC，USA，2006.

[4] F. Almenarez, A. Marin, D. Diaz，and J. Sanchez, "Developing a model for trust management in pervasive devices [J]," 2006.

[5] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision [J]," Decision Support Systems, Vol. 43, No. 2, pp. 618−644, 2007.

[6] W. Li, "A history and honest recommendation based trust model in peer-to-peer Networks [D]," Hunan University, pp. 28–29, September 2007.

[7] X. L. Chen, "Research on the modeling and application of initial trust for e-commerce[D]," Huazhong University of Science and Technology, 2008.

[8] A. Gummadi and J. P. Yoon. "Modeling group trust for peer-to-peer access control," Database and Expert Systems Applications, Proceedings 15th International Workshop, pp. 971–978, 2004.

[9] W. Dou, H. M. Wang, and Y. Jia, "A recommendation-based peer-to-peer trust model [J]," Journal of software, Vol. 15, No. 4, pp. 571–583, 2004.

[10] G. Zacharia and P. Maes, "Trust management through reputation mechanisms [J]," Applied Artificial Intelligence, Vol. 14, No. 9, 2000.