http://dx.doi.org/10.5755/j01.eee.19.4.4057 ELEKTRONIKA IR ELEKTROTECHNIKA, ISSN 1392-1215, VOL. 19, NO. 4, 2013

Dynamic Recommendation Trust Model Based on Information Entropy and Heuristic Rules in E-Commerce Environment

Gang Wang[1,2], Xiaolin Gui[1]
[1]*Department of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an, 710049, China*
[2]*School of Information, Xi'an University of Finance and Economics, Xi'an, 710100, China*
wg.only@gmail.com

***Abstract*—Under E-commence environment, because both parties of transaction lack the mutual basis of trust, transaction is facing the higher risk. We propose a dynamic recommendation trust model based on information entropy and heuristic rules. In the model, we take into account recommendation trustworthiness is related with acquaintance degree of between recommendation nodes and trust evaluator, and recommendation trustworthiness is also related with similarity of transaction contents at the same time. So we propose a novel computing method of concept similarity of transaction content based on trade goods ontology, in order to ensure objectivity and accuracy of computing, we adopt information entropy to avoid the defect of subjectivity of artificial weighted coefficient, and we adopt heuristic rules to resolve the problem that two concept similarity degree does not be distinguished while the number of information that two concept contains is the same. Based on experiments result analysis, slander and collaborative cheating of malicious nodes are restrained and held back by our model. In addition, experiment results show we propose concept similarity computing method is effective.**

***Index Terms*—Trust model, ontology, information entropy, heuristic rules.**

I. INTRODUCTION

With the rapid growth in computing and communications technology, the past decade has witnessed a proliferation of powerful e-commerce. However, the problems also follow it, in which, trust is a very important problem in e-commerce. Thus, how to build a secure, reliable and trustworthy trust evaluation system for e-commerce is a research hot spot nowadays.

At present, a number of scholars have already had rather in-depth studies in trust security, in which, trust models were divided policy-based and reputation-based models in terms of management mechanism [1]–[3]. From a structural perspective of trust, trust model is classified centralized trust management model and distribution-based trust management model [4]–[6]. *EigenRep* Model is a global trust model that could overcome feigning and slandering of malicious nodes [7]. Li Jingtao et al. proposed a similarity-based weighted trust model [8]. Despite that the concept of recommendation trust similarity is mentioned, and the reliability of trust has improved dramatically, it ignores that the interest of each node to service is different, and computing granularity is still too big [9].The Bayesian Trust Model [10] calculated the trust value of nodes according to contributing factor of each node, but it does not consider that the feedback reliability of the nodes is different, because these nodes have different interest similarity. In addition, the trust is dynamic changes with time and interests of nodes. Li Wen and the others gave the granularity classifications of trust based on *QoS* of nodes, and yet its classifications didn't consider to the similarity of service content among nodes [11]. Ying Weijin and others gave consideration to the similarity of service concept, but they ignore trust is dynamic change with time and the number of transaction [12] The author advocated an e-commerce recommendation trust model under P2P environment, the model introduces trust factors, such as transaction value, transaction evaluation and transaction time that affect trust degree, and solves the problem of computing local reputation. At the same time, global reputation enhances the counter attack capability of the trust mechanism [13].

In summary, we find existing trust models don't comprehensively consider influence factors of trust, so trust computing lacks universality in e-commerce nowadays. We propose a novel trust computing model based on information entropy and heuristic rules, in which, we adopt information entropy to compute the weight of all indexes for concept similarity, and it could assure weight of index is objectivity, and we adjust concept similarity by heuristic rules in order to meet actual application fact at the same time. Additionally, because items of goods or service in e-commerce are too more and their name often repeat each other, similarity computing for transaction content isn't accurate enough. Through computing ontology concept similarity, we could effectively avoid the problem.

Manuscript received March 19, 2012; accepted May 29, 2012.
This work was supported by a grant from National Science and Technology Major Project of the Ministry of Science and Technology of China (No.2012ZX03002001-004) and the National Natural Science Foundation of China (No. 60873071, No.61172090).

II. RECOMMENDATION TRUST MODEL

Definition1. Service requestor, (also known as Evaluator), refers to buyer in E-Commerce or service evaluation node in the network, denoted by *E*.

Definition2. Service recommendation node is the node that recommends service for evaluator, and its purpose is to gain related economic profits and trust, denoted by *SR*.

Definition3. Service Provider refers to buyer in E-Commerce or service-evaluated node in the network, denoted by *SP*.

From in the view of social psychology, the trustworthiness of recommendation of acquaintance node is generally higher than stranger nodes'. Moreover, the evaluation of direct acquaintance recommendation nodes is comparatively more reliable than indirect acquaintance recommendation nodes. So we find that global trust degree is closely related with the following two aspects:

Global trust of node *i* depends on the evaluation of other nodes in the network to *node i*, and objective and accurate of the evaluation is to depend to transaction content similarity.

In Fig. 1, $C_{a,d}$ is transaction content of between *a* and *d*. $C_{b,d}$ is transaction content of between *b* and *d*. $C_{c,d}$ is transaction content of between *c* and *d*. Thus, trust of *a* to *d* relies to similarity of between $C_{a,d}$ and $C_{c,d}$ and similarity of between $C_{a,d}$ and $C_{b,d}$.

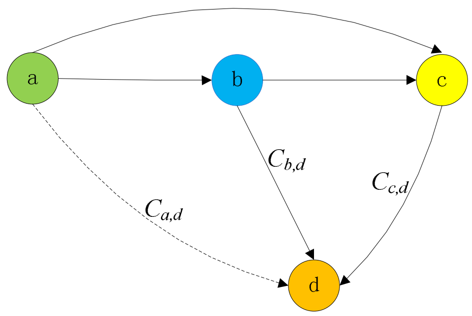


Fig. 1. Transaction content of network nodes.

Because recommendations trust of node *i* depend on acquaintance of between recommendation node and evaluator, the relationship shows a rank relationship or Chain relationship in the network, that is recommendation path. So recommendation trust of node *i* is the maximum of recommendation trust among these recommendation paths.

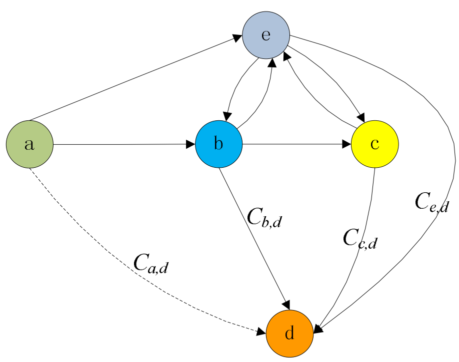


Fig. 2. Transaction content of network nodes.

In Fig. 2, recommendation paths of node *d* have *a-b-d*, *a-e-d*, *a-b-c-d*, *a-e-b-d*, *a-e-c-d*, and so on. Correspondingly, recommendation trust of node *d* will select the maximum trust values from these recommendation paths.

III. TRUST MODEL ALGORITHM

Input: Initializes *Node_Numbers*, *Product_Numbers*;

Output: Gets Transaction successful ratio;

Step 1. Initialization node transaction road map. At the onset of the network, the initial nodes are all individual nodes that have never had any transactions, and the numbers of network nodes and malicious nodes need to be initialized, and trades goods need to be distributed randomly. If one node is determined as malicious, then the trade goods assigned to that node will decrease by half, and the system will generate a transaction road map;

Step 2. Calculating Global Trust Comprehensive Value. Initializes ε, i, j, while number i is smaller than cycle numbers and trust value is smaller than ε, it abandons the traded road map;

Step 3. While number i is smaller than transaction path total numbers, and if the current path doesn't have malicious nodes, successNum equal to success Numbers and totalNum equals to total numbers;

Step 4. While number j is smaller than transaction path total numbers, and if node i and node j are not the same node, node i and node j carry out a transactions, and trade successful ratio is the number of successful transaction V.s the transactions total number; else node j to be abandoned, and go to Step 2.

A. Direct trust computing

Direct trust value determined by the history logs of transactions between evaluator and target nodes, in which *i* is the initiator for transaction, and *j* is the follower

$$DT_{i,j} = \frac{S_{i,j}}{G_{i,j}} = \frac{S_{i,j}}{S_{i,j} + F_{i,j}}, \quad (1)$$

where $DT_{i,j}$ represents direct trust value, $S_{i,j}$ represents the number of times that *i* and *j* have been happy with the transactions, i.e., the success rate; $G_{i,j}$ specifies the overall times of the transactions between *i* and *j*, $G_{i,j} = S_{i,j} + F_{i,j}$, $F_{i,j}$ refers the number of times that *i* and *j* have been unhappy with the transactions, or rate of failures. When $G_{i,j} = 0$, $DT_{i,j} = 0.5$. $DT_{i,j}$ and $DT_{j,i}$ are not equal.

B. Recommendation trust computing

$$\overline{RT}_k = \sum_{\substack{i,j=1 \\ i \neq j}}^{n} Sim(C_{ik}, C_{jk}) * (\sqrt[3]{\alpha * \omega_{ik} * DT_{i,k}} + \sqrt[3]{\beta * \omega_{jk} * DT_{j,k}}) / n, \quad (2)$$

where $\overline{RT}_k$ is the integration of recommendation trust evaluation value for *node* k, $Sim(C_{ik}, C_{jk})$ refers to the similarity of between C_{ik} and C_{jk}, in which refers to interaction content of *node* *i*, *j* and *node* *k*, and ω_{ik} and ω_{jk} respectively refer to acquaintance recommendation weight and stranger recommendation weight

$$\begin{cases} \omega_{ik} = DT_{i,k} \\ \omega_{jk} = 0.5 \end{cases}.$$

The weight of stranger recommendation is initially set at 0.5, meaning its half can be trusted and the other half couldn't be trusted. α refers to the recommendation weight of direct acquaintance node or indirect acquaintance, and this represents the trust degree of the recommending node for the recommended node; α is set at:

$$\begin{cases} \alpha = DT_{i,j}, & \text{if } i \text{ and } j \text{ have direct interaction,} \\ \alpha = \dfrac{1}{n}\sum_{N=1, i\neq j\neq k}^{n}\prod DT_{i,j} * DT_{j,k}, & \text{if } i \text{ and } k \text{ don't direct interaction.} \end{cases} \quad (3)$$

When $\alpha<\varepsilon$, the node shall be abandoned. ε is the threshold value of trust chain to be set by us.

β refers to stranger recommendation weight, and $\beta = \dfrac{\sum_{i=1}^{n} DT_{ij}}{n}$. If $\sum_{i=1}^{n} DT_{ij} = 0$, then the node is a newly joining node or a dormant node.

C. Global trust computing

Global Trust Degree is a synthesized trust degree that directs trust and recommendation trust weighted to target node

$$GT = \begin{cases} RT, & \text{if } s = 0, \\ DT, & \text{if } \tau = 0, \\ \rho * DT + (1-\rho) * RT, & \text{if } s \neq 0 \text{ and } \tau \neq 0, \end{cases} \quad (4)$$

where s represents to recommendation node numbers; τ represents to the direct transaction number of Trust evaluator and target node; ρ is the weight of trust evaluator and target node, and $1-\rho$ is recommendation trust weight, and $\rho(x)$ is a dynamic change function as interactive numbers x, and its computing equation is as following

$$\rho(x) = 1 - \left(\frac{1}{2}\right)^{\frac{x}{n-x}}, \; n - x \neq 0 \;, \quad (5)$$

where $n \in \{1,2,3, \ldots\}$, and x is the x-*th* interaction between trust evaluator and target node in a period of time. The larger x is, the larger ρ is. When trust evaluator is the first interaction with target node, due to the limited number of interaction, trust evaluator will pay more attention to recommendation trust of the others. With the increasing number of interaction, trust evaluator would be more willing to depend on own interaction experience to judge trust value of target node. Correspondingly, recommendation rate of the other recommendation nodes is falling gradually, and ρ will enlarge gradually with increase of interactive numbers.

IV. CONCEPT SIMILARITY COMPUTING OF TRADE GOODS ONTOLOGY

Similarity computing method that we adopt is concept similarity computing based on transaction content ontology. We propose a novel computing method of similarity based on information entropy and heuristic rules. To different from tradition methods of defining semantic distance with artificial weighting coefficient is that our method adopt statistical information entropy to define semantic distance and edges' weight between two nodes, so it could avoid the subjectivity of artificial weight method. Meanwhile, which we use heuristic rules enhances the fine distinction ability.

In the ontology structure, that concept c_i contains information satisfies the following formula

$$I(c_i) = I(c_i^{\sup erclass}) + I(c_i^{self} \mid c_i^{\sup erclass}). \quad (6)$$

Of which, $I(c_i^{\sup erclass})$ denotes the information of $c_i^{\sup erclass}$ that is parent class of c_i; $I(c_i^{self} \mid c_i^{\sup erclass})$ denotes self-information of c_i:

$$I(c_i^{self} \mid c_i^{\sup erclass}) = I(c_i) - I(c_i^{\sup erclass}), \quad (7)$$

$$p(c_i^{slef} \mid c_i^{\sup erclass}) = \frac{p(c_i)}{p(c_i^{\sup erclass})}, \quad (8)$$

where $p(c_i)$ is probability of concept c_i in ontology structure, since sub-concept can inherit information from parent concept, therefore

$$p(c_i) = \frac{\sum n(c_i^{subclass}) + 1}{n(o)}, \quad (9)$$

where $\sum n(c_i^{subclass})$ presents all sub-concepts of concept c_i in ontology O, $n(o)$ denotes all concepts numbers in ontology structure. Semantic distance of two concepts can be decided through two concepts contain information. hence, there is a following formula (10)

$$\begin{aligned} dis(c_i, c_j) = &\sum_{this=i}^{droot} f(c_{this}, c_{this}^{\sup erclass}) * (I(c_{this}) - I(c_{this}^{\sup erclass})) + \\ &+ \sum_{this=j}^{droot} f(c_{this}, c_{this}^{\sup erclass}) * (I(c_{this}) - I(c_{this}^{\sup erclass})), \end{aligned} \quad (10)$$

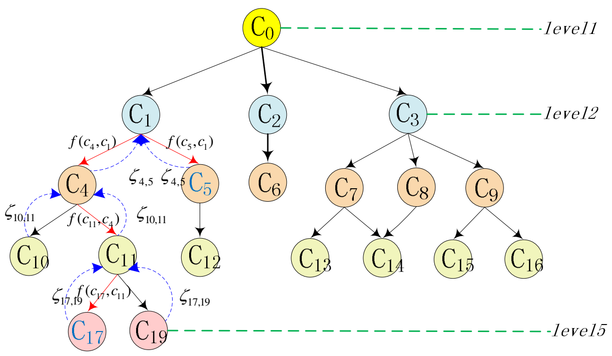
where $f(c_{this}, c_{this}^{\sup erclass})$ denotes weighting function of edge $c_{this} \rightarrow c_{this}^{\sup erclass}$, and c_{this} is the node in the current path, $c_{this}^{\sup erclass}$ is a parent node of c_{this}, computing formula as following

$$f(c_{this}, c_{this}^{\sup erclass}) = \frac{I(c_{this}^{\sup erclass}) - I(c_{this})}{I(c_{i,j}^{droot}) - I(c_\kappa)}, \quad (11)$$

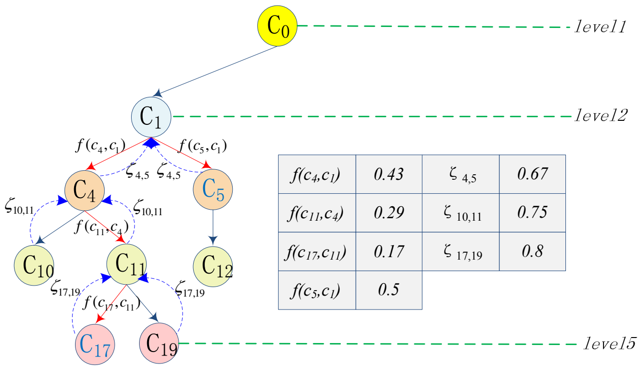
where $c_{i,j}^{droot}$ is the sharing parent node of two concepts c_i, c_j, with the different of concept, the sharing parent node is dynamic change on the shortest path between two concepts. c_κ denotes a node of the same side with concept node c_{this}, and c_κ is the one of two concept nodes of computing concept similarity.

For example, in Fig. 3, the shortest path between concepts c_{17} and c_5 is $c_{17} \rightarrow c_{11} \rightarrow c_4 \rightarrow c_1 \rightarrow c_5$, in which c_1 is the sharing parent node of concepts c_{17} and c_5, thus, $f(c_{11}, c_4) = \dfrac{I(c_4) - I(c_{11})}{I(c_1) - I(c_{17})}$, two concepts similarity computing formula is as following

$$sim(c_i, c_j) = \frac{1}{1 + dis(c_i, c_j)}. \tag{12}$$



(a)



(b)

Fig. 3. Concept ontology hierarchical structure (a) and the shortest path (b) between two concepts.

In computing similarity, while the number of information that two concept contains is the same, two concept similarity degree does not be distinguished, this paper creates heuristic rules in order to repair concept similarity. Heuristic rules as shown Table I.

TABLE I. HEURISTIC RULES.

Heuristic Rules	**Conditions**
R1	HasSameSuperclass()
R2	HasSameSiblingclass()
R3	HasSameSubclass()
R4	HasSameInstance()
R5	$\forall c_i^{subclass}$ *similarity X*, $\exists c_i^{superclass}$ *similarity X*
R6	$\forall c_i^{sibling}$ *similarity Y*, $\exists c_i$ *similarity Y*

To take heuristic rules R_1 for example: While two concepts have the same parent concept, concept similarity increases gradually along with hierarchy of ontology structure increases gradually, therefore, under the rule R_1, through increases similarity adjustment coefficient $\zeta_{i,j}$ between two concepts c_i and c_j, the concept similarity computing formula is as following

$$\zeta_{i,j} = \frac{level(c_{i,j}^{superclass})}{level(c_i, c_j)}, \tag{13}$$

where $level(c_{i,j}^{superclass})$ is the level of a common parent node of concept c_i and c_j among ontology hierarchical structure; $level(c_i, c_j)$ is the level of concept c_i and c_j in ontology hierarchical structure

$$sim'(c_i, c_j) = \zeta_{i,j} \bullet sim(c_i, c_j). \tag{14}$$

V. TRADE GOODS DOMAIN ONTOLOGY BUILDING

The existing building method of ontology is not yet mature and lacks an integrated and uniform methodology. We propose a graded hierarchical building method of domain ontology of trade goods attributions oriented. Trade Goods Ontology Building Process is as follows:

Step 1. Determining the purpose of domain ontology, content and scope;

Step 2. Determining concept ontology and classification system according to uses of goods;

Step 3. Determining class attribution and relationship among classes;

Step 4. Formalized definition and indication of ontology;

Step 5. Ontology coding;

Step 6. Ontology evaluation.

In which, formal representation of ontology is as follows:

Definition6: ontology represents by quintuple

$$O_{product} = \{C_{product}, R_r, A^{C_{product}}, A_{product}^{R_r}, X_{product}\}, \tag{15}$$

of which, $C_{product}$ is concept set; R_r is a relationship set; $A^{C_{product}}$ is a set to be composed by more attribution sets, and is also a concept attribution set; $A_{product}^{R_r}$ is a more attributions component set and is a relationship set among concepts; $X_{product}$ is a axiom set.

Definition7: if concepts $C_{product}^i$ and $C_{product}^j$ belong to concept $C_{product}$, denoted by $C_{product}^i, C_{product}^j \in C_{product}$, and values of R_r arranges from $C_{product}^i$ to $C_{product}^j$, that is $r = \langle C_{product}^i, C_{product}^j \rangle$. Concept $C_{product}^i$ and $C_{product}^j$ have relationship R_r, and denoted by $C_{product}^i R_r C_{product}^j$, then $C_{product}^j \in \{C_{product}^i\} \odot r$, $C_{product}^i \in r * \{C_{product}^j\}$.

In which, $\odot$ indicates $C_{product} \times R \rightarrow C_{product}$, $*$ indicates $R \times C_{product} \rightarrow C_{product}$, $C_{product}$ is concept domain, R is relationship domain. Inverse relationship of R_r denotes by R_r^{-1}, $r^{-1} = \langle C_{product}^j, C_{product}^i \rangle$, and then $C_{product}^i \in \{C_{product}^j\} \odot r^{-1}$, $C_{product}^j \in r^{-1} * \{C_{product}^i\}$.

Definition8: if concept $C_{product}^i$ belongs to concept $C_{product}$, and is denoted by $C_{product}^i \in C_{product}$ ($i \in N$), then $A^{C_{product}}$ is a set that is made up of more attributions, in which every attribution matches along with a concept.

$$A^{C_{product}} = \left\{ A^{C_{product}}(c_{product}^1), A^{C_{product}}(c_{product}^2), \cdots, A^{C_{product}}(c_{product}^i) \right\}. \tag{16}$$

Definition9: if concept $C^i_{product}$ and $C^j_{product}$ belong to concept $C_{product}$ and is denoted by $C^i_{product}, C^j_{product} \in C_{product}$, and $A^{C_{product}}(c^j_{product}) \subseteq A^{C_{product}}(c^j_{product})$, then $C^j_{product} \in is\_subclass\_of * \{C^i_{product}\}$ or $\langle C^j_{product}, C^i_{product} \rangle \in is\_subclass\_of$.

Definition10: if concepts $C^i_{product}$ and $C^j_{product} \in C_{product}$,and $A^{C_{product}}(c^i_{product}) \supseteq A^{C_{product}}(c^j_{product})$, then $C^i_{product} \equiv C^j_{product}$.

Definition11: if concepts $C^i_{product}$ and $C^j_{product}$ meet relation of $C^i_{product} \subseteq \neg C^j_{product}$, then $(C^i_{product}, C^j_{product}) \in Disjoint\,with$.

VI. SIMULATION EXPERIMENT AND RESULT ANALYSIS

We simulate the operation of our model through experiment and verify the results of the experiment by operating the model in a small-scale network. The experiment involves 15 nodes and 81 commodities. The trade goods ontology structures used in the experiment are respectively 1, 3, 3, 3 and 3. The goods are randomly assigned to each node, making sure that each node is assigned with at least one commodity but no more than 15. ε is set at 0.3, and the simulation experiment is conducted under Java environment.

A. Definition of node types

The nodes involved in the transactions fall into two types: good nodes and malicious nodes. Malicious nodes are further classified into purely malicious nodes and collaborative malicious nodes, the main purposes are summarized as follows:

Main purpose of pure malicious nodes has two aspects: one is to provide fake goods or service; the other is to defame good nodes.

Main purpose of collaborative Malicious Nodes has two aspects: one is adulation by each other among acquaintance nodes which means to magnify effect themselves; the other is slander to good nodes that traded with malicious nodes.

B. Performance evaluation indicators

The evaluation indicators for our model are based on the success rate of transactions. After each simulation experiment, success rate of transactions is calculated through counting up the number of successful transactions at good nodes and the total transaction times. The times of successful transactions and total transactional times here are the sum of transactions of good nodes as trade content provider and trade content demander.

C. Experiment analysis

Analysis of directing to scale of malicious recommendation nodes.

Result of the experiment1 shows (Fig. 4) that under the circumstance where the rate of malicious nodes continues to rise, the success ratio of transaction under our Model has improved impressively compared with *EigenRep* model, and under the circumstance where malicious nodes continues to rise, the success ratio of transaction decreases rapidly. When the number of malicious nodes gets above 60%, our Model can still maintain a quite high success ratio of transactions. Whether it is purely malicious nodes or collaborative malicious nodes, our Model demonstrates a good containing effect.

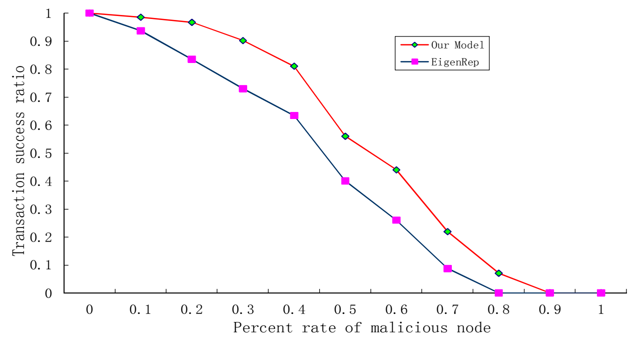


Fig. 4. Success ratio of when malicious nodes are changed.

Sensitivity analysis of directing to the number of times of transaction (Fig. 5).

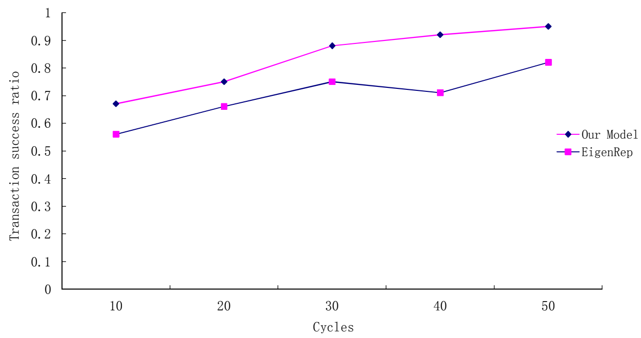


Fig. 5. Transactions success ratio of the cycle in a fixed malicious nodes rate.

In the experiment, when the rate of malicious nodes is set at 40%, success ration of *EigenRep* model is only 69.4%, and yet success ration of our model is 90.2%. Our model demonstrates a very good success ratio with the increase of transaction cycles.

Analysis of directing to malicious recommendation attack

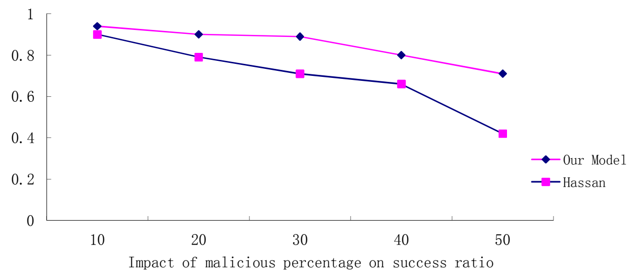


Fig. 6. Impact of malicious recommendation nodes percentage to Transaction success rate.

Fig. 6 shows that trust computing accurateness declines gradually with continually increase of dishonest node ratio, which leads to the increase of the number of transaction failure and the decreasing of the success ratio. Because each dishonest recommendation of recommendation node will influence trust value of self-node, and will lead to self trust value to be decreased, along with dishonest node ratio increasing, the decline magnitude of the success ratio of transaction is larger. Hassan model has a kind of resistant ability, but because Hassan assumes that recommendation nodes have the higher trust value, meanwhile, Hassan model lacks punishment mechanism, it cannot effectively weaken the influence of dishonest recommendation to trust, and the success ratio of transaction decreases rapidly.

Our model shows that the dishonest node can be shielded through the others honest nodes of recommendation path, so decline of transaction success ratio is lower than Hassan model. Therefore, in contrast with Hassan model, our model could filter malicious recommendation nodes more effectively and make recommendation information to be more accurate with the introduction of trade goods concept similarity and dynamic adjustment trust value.

VII. CONCLUSIONS

We propose a dynamic recommendation trust model based on information entropy and heuristic rules in the paper. By information entropy, we resolve one problem that weighted coefficient is determined by artificial, and by heuristic rules we resolve the other problem that two concept similarity degree does not be distinguished while the number of information that two concept contains is the same. At the same time, we adopt ontology concept similarity to avoid repeating naming of the same service or trade goods in e-commerce, and vice versa. Meanwhile, the model divides the evaluation of nodes into acquaintance node recommendation and stranger node recommendation, so that the model conforms to real application environment and guarantees that transactions can take place in a secure and reliable fashion under e-commerce context. From experiment result, we find the model is the more objective and reliable to trust evaluation of the nodes. Simulation experiments results also confirm that this model is effective in identifying and constraining attack and collaborative cheating of malicious nodes.

REFERENCES

[1] Yu Zhang, Hua Jun Cheng, Xiao Hong Jiang, "Trust Management Research Survey In E-Commerce", *Chinese Journal of Electronics,* vol. 36, no. 10, pp. 2011–2019, 2008.

[2] W. Nejdl, D. Olmedilla, M. Winslett, "Peer Trust: Automated trust negotiation for peers on the semantic web", in *Proc. of Workshop on Secure Data Management in a Connected World,* Berlin: Springer-Verlag, 2004, pp. 118–132. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-30073-1_9

[3] Y. Chu, J. Feigenbaum, B. La Macchia, P. Resnick, M. Strauss, "Referee: Trust management for web applications", *World Wide Web Journal,* vol. 2, no. 2, pp. 127–139, 1997.

[4] B. Yu, M. P. Singh, "An evidential model of distributed reputation management", in *Proc. of the First International Joint Conference on Autonomous Agents and Multiagent Systems,* New York: ACM Press, 2002, pp. 294–301. [Online]. Available: http://dx.doi.org/10.1145/544741.544809

[5] P. Resnick, R. Zeckhauser, "Trust among strangers in internet transactions: empirical analysis of eBay's reputation systems", *The Economics of the Internet and E-commerce,* vol. 11, pp. 127–157, 2002. [Online]. Available: http://dx.doi.org/10.1016/S0278-0984(02)11030-3

[6] G Zacharia, A Moukas, P Maes, "Collaborative reputation mechanisms in electronic marketplaces", *Decision Support Systems,* vol. 29, no. 4, pp. 371–388, 2000. [Online]. Available: http://dx.doi.org/10.1016/S0167-9236(00)00084-1

[7] S. Kamvar, D. Schlosser, M. T. Eigen, "Reputation management in P2P networks", in *Proc. of the 12th Int. World Wide Web Conf.,* Budapest: ACM Press, 2003, pp. 123–134.

[8] Jing-tao Li, Yi-nan Jing, Xiao-chun Xiao, Xue-ping Wang, "A trust model based on similarity-weighted recommendation for P2P environments", *Journal of Software,* vol. 18, no. 1, pp. 157–167, 2007. (in Chinese). [Online]. Available: http://dx.doi.org/10.1360/jos180157

[9] Wen Dou, Huai-Min Wang, Yan Jia, Peng Zou, "A Recommendation-Based Peer-to-Peer Trust Model", *Journal of Software,* vol. 15, no. 4, pp. 571–583, 2004.

[10] Y. Wang, J. Vassileva, "Bayesian network trust model in peer-to-peer networks", in *Proc of the 2nd Intel Workshop on Agents and Peer-to-Peer Computing,* Berlin: Springer-Verlag, 2004, pp. 23–34. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-25840-7_3

[11] Li Wen, Xie Dong-Qing, Wu Yong, "History and recommendation-based trustmodel in P2P environment", *Application Research of Computers,* vol. 25, no. 3, pp. 915–919, 2008.

[12] Jin. Yingwei, Zhang Yong, Wenyu Qu, "A Trust Model Based on Similarity Evaluation in P2P Networks", in *Proc. of the 2008 IEEE International Symposium on Parallel and Distributed Processing with Applications,* 2008, pp. 737–742. [Online]. Available: http://dx.doi.org/10.1109/ISPA.2008.55

[13] Shou-Xu Jiang, Jian-Zhong Li, "A Reputation-Based Trust Mechanism for P2P E-Commerce Systems", *Journal of Software,* 2007, vol. 18, no. 10, pp. 2551–2563. [Online]. Available: http://dx.doi.org/10.1360/jos182551