International Journal of Hybrid Information Technology
Vol. 7, No. 6 (2014), pp. 411-422
http://dx.doi.org/10.14257/ijhit.2014.7.6.35

A Event Weight Based Trust Search Algorithm with Subjective Logic

Junfeng tian and Peipei Zhang

College of Mathematics and Computer,
Hebei University, Baoding 071002, China
tjf@hbu.edu.cn, 843073490@qq.com

Abstract

The traditional search of trust, mostly uses the flooding method. This algorithm has low efficiency and high computational cost. It also cannot solve the issue of overlapping of friends-circle. To solve these issues, a new trust search algorithm was proposed. The influence of event weight to node's recommended qualifications was fully considered in the new algorithm by the improvement of subjective logic theory, the path dependence and trust-circle caused by the overlapping of friends-circle were solved effectively by the strategies of dual-threshold screening and set added. The experiments results showed that the complexity of trust network was reduced, the efficiency of trust search was improved, and the accuracy of trust evaluation was increased through the new algorithm.

Keywords: *Subjective logic; Trust search; Event weight; Dual-threshold screening; The overlapping of friends-circle*

1. Introduction

With the widely used of large-scale distributed system(such as grid computing, pervasive computing, peer-to-peer computing, Ad Hoc, *etc.*), people not only enjoy the sharing of resources and high usage rate, but also face many security threats. On the one hand, Nodes in the distributed system lack some constraints, it makes the nodes in the environment have more freedom, which is more advantageous to the interactions between nodes. On the other hand, in the open distributed environment, the source node often needs to interact with the unknown or even completely strange nodes. However, due to the lack of trust between nodes, a large number of malicious nodes commit fraud or provide untrusted services. Trust mechanism is an effective means to solve the issues above. By the trust mechanism, we can make an estimate of other node's integrity and reliability before the interaction, thus ensuring the reliability and safety of interaction.

In recent years, the domestic and international scholars have studied trust mechanism based on different mathematical theories [1-8]. In trust model, trust relationship is built between nodes through the direct interaction. When the lack of direct interaction, trust is built between nodes through the trusted third party, thus forming the trust network diagram from the source node to the destination node. Based on the trust network diagram, the comprehensive trust evaluation of source node on destination node is obtained through the trust transitivity and aggregation. Therefore, as the basis and premise for trust model research, trust search algorithm is the key to ensure that the comprehensive trust evaluation accord with the objective reality.

ISSN: 1738-9968 IJHIT

2. Related Works

In the research of trust transitivity and aggregation, most of existing trust models [5-8] are based on the flooding search. Su and other scholars proposed a recommendation mechanism based on trust network in literature [5]. The recommended chains were obtained by flooding search, these chains were summarized three relationships and three strategies were given to solve the issue of fully dependent. Recommendation mechanism based on trust network, to some extent, reduced the recommended behaviors of malicious nodes. Jiang and other scholars proposed a research on trust transitivity and aggregation in evidential trust model by combing D-S evidence theory and graph theory in literature [6]. The concept of trust sub-graph was introduced and the dependencies between recommended chains were eliminated by EDTR algorithm. This model is also based on the flooding search. Qin and other scholars proposed a research on selective trust-path search and aggregation in distributed environment in literature [7]. By the control parameters, the searches of unnecessary trust-paths were stopped and the search of paths which containing effective information were performed. Besides, Jøsang and other scholars proposed the subjective logic based on D-S evidence theory [8-13]. Moreover, Jøsang proposed an optimized network analysis with subjective logic in literature [14]. A new specification chart was obtained by split the trust relationships which were obtained from the flooding search, and new independent trust paths were obtained in the algorithm by split the dependency relationships between original trust paths. But on looking the matter more closely, we find some issues in the algorithm, upcoming paper will describe these issues in much more detail.

Jøsang's model made some researches about trust transitivity and aggregation based on the flooding search. Although the path dependence [15] caused by flooding search was considered in the model, but only a simple algorithm about path optimization and the elimination of dependency was given. The model did not consider the cause of path dependence fundamentally-that is the overlapping of friends-circle [16-17]. Therefore, this algorithm has low search efficiency and it is difficult to resist the recommendations from the malicious nodes, and then makes the comprehensive trust evaluation inaccurate. Besides, node's recommended qualifications are influenced by the importance of event, the model did not consider it. When the importance of event is high, some nodes that have low trust evaluation cannot provide services with high credibility, then these nodes should not have recommended qualifications at this time.

Therefore, in this paper, a new trust search algorithm is proposed, which is an improvement of the simple flooding search. In the new algorithm, the strategies of dual-threshold screening and set added are designed to solve the overlapping of friends-circle.

3. A Event Weight based Trust Search Algorithm with Subjective Logic

3.1. Related Concepts

Trustor: The source node in the trust network who initiate the search. It needs to calculate the trust evaluation.

Trustee: The destination node in the trust network who terminate the search. It needs to be calculated the trust evaluation.

Recommended entity: The intermediate nodes in the trust network who provide the recommendations.

Neighbor node: Node who has direct interactions to the specific node.

Friends-circle: All neighbor nodes of one node constitute the friends-circle of that node.

Trust evaluation: Quantify the value of trust between nodes. It is composed by belief, disbelief and uncertainty, we can write $w = \{b, d, u\}$.

Event: A series of behaviors which cause the change of node's expectation value.

Event weight: The importance of current event.In this paper. The symbol 'V' is used to designate it, where $V \in [0,1]$. The more important the event, the higher the event weight. The calculation rules refer to literature[18]. In this paper, all events are divided into the following three conditions, the demarcation points V_1 and V_2 are selected based on the concrete application environment :

$$\begin{cases} V \in [0, V_1] & \text{Current event has low importance of event;} \\ V \in (V_1, V_2) & \text{Current event has general importance of event;} \\ V \in [V_2, 1] & \text{Current event has high importance of event} \end{cases} \quad (1)$$

In addition, all nodes are divided into the following four categories according to their expectation values:

Absolute trust node: Based on the experiences from the long-term interactions between nodes, we judge these nodes have high credibility whether to provide services or recommendations. All absolute trust nodes in the trust network constitute the set of absolute trust nodes.

General trust node: Based on the experiences from the interactions between nodes, we judge these nodes have general credibility whether to provide services or recommendations. All general trust nodes in the trust network constitute the set of general trust nodes.

Critical trust node: Based on the experiences from the interactions between nodes, other nodes have no good reasons to judge the credibility of the specific node, whether the node provides services or recommendations. All critical trust nodes in the trust network constitute the set of critical trust nodes.

Untrusted node: Based on the experiences from the long-term interactions between nodes, we judge these nodes have no credibility whether to provide services or recommendations. All untrusted nodes in the trust network constitute the set of untrusted nodes.

Untrusted node, critical trust node, general trust node and the absolute trust node corresponding to the following four expectation value ranges respectively: $0 \le E < E_1$, $E_1 \le E < E_2$, $E_2 \le E < E_3$ and $E_3 \le E \le 1$. Among them, E_1, E_2, E_3 are determined by the concrete application environment.

3.2. The Issues of Flooding Search in Jøsang's Model

1. In Jøsang's model, the trust network is obtained by the flooding search. However, due to the overlapping of friends-circle in the trust network, some trust networks may be appeared as follows:

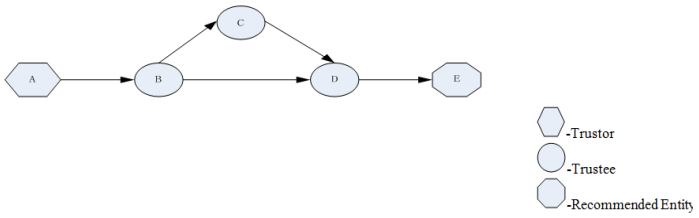

Figure 1. The Path Dependence in the Trust Network

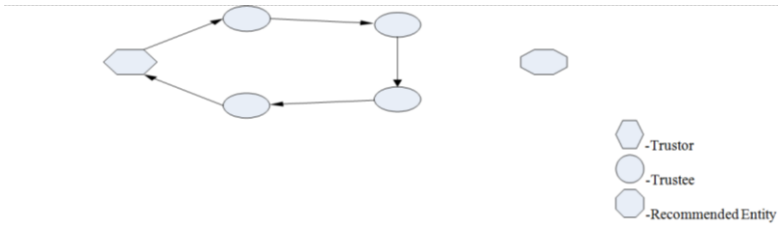

Figure 2. The Trust-circle in the Trust Network

With the trust relationship in Figure 1 analysis, there is a path dependence in the trust network. Jøsang consider that the trust evaluation between two nodes does not rely on the recommendation from third party when they exist the direct interaction. With the trust relationship in Figure 2 analysis, a trust-circle is formed which not contain the trustee.

2. There are multiple paths from trustor to trustee in the trust recommend diagram. At this time, a challenging issue is how to find the optimal paths to produce the most reasonable trust evaluation.

3. The algorithm in literature [14] also has the issue of high computational cost, although we can get the trust recommend diagram through the search.

3.3. A Event Weight based Trust Search Algorithm with Subjective Logic

In this paper, we assume that the trust relationships are stored in the form of table. In Figure 1, for example, the trust relationships are stored as follows:

Table 1. The Store of Trust Relationships

Source	Target	Belief	Disbelief	Uncertainty	Direct Interaction
A	B	b_B^A	d_B^A	u_B^A	1
B	C	b_C^B	d_C^B	u_C^B	1
C	D	b_D^C	d_D^C	u_D^C	1
B	D	b_D^B	d_D^B	u_D^B	1
D	E	b_E^D	d_E^D	u_E^D	1

At the beginning of search, we can get the simplified trust network relationships by the dual-threshold screening. Specific operations as follows:

The first is the node-threshold screening. Nodes who participate the recommendations need to reach the certain expectation value, only if they would have the recommended qualifications. Therefore, we set the node-threshold E_0, all nodes are classified according to their expectation value *E*. In generally, $E_0 \geq 0.5$.

The following is the event-threshold screening. In this paper, we screen the set of nodes based on event weight V to get the final sets which can participate the recommendation. After the screening, the following correspondence is obtained:

$$\begin{cases} \text{The set of absolute trust nodes, the set of general trust nodes, the set of critical trust nodes,} & When V \in [0, V_1]; \\ \text{The set of absolute trust nodes, the set of general trust nodes,} & When\ V \in (V_1, V_2); \\ \text{The set of absolute trust nodes,} & When V \in [V_2, 1] \end{cases} \quad (2)$$

After the dual-threshold screening, the valid nodes who can participate the recommendations are obtained, then enter the search phase. At first, the path nodes set *S(P)* and the path depth variable *D(P)* are defined.

Path nodes set *S(P)*: $S(P_i)$ is the set of nodes on the path i-th($i \in [1, n]$),and $S(P_i) = \{v_{i0}, \ldots v_{ij}, \ldots v_{im}\}$ ($j \in [0, m]$). Wherein v_{i0} is the initiate node, v_{im} is the terminate node, v_{ij} is the j-th node on the i-th path. Initially $S(P_i) = \{v_{i0}\}$. When the search is beginning, the nodes who get from each successful search are added into the set $S(P_i)$ and the nodes within the set no longer receive messages in the future.

Path depth variable *D(P)*:The maximum path depth which allow search. According to the six of separation theory [19], it considers that the depth of trust path which more than 6 do not have the recommended qualifications. So we set *D(P)*=6 initially. After each of successful search, *D(P)* should be minus one. When the trustee is successful searched, the search is complete. Otherwise the search continues, the search fails until *D(P)* is reduced to zero, then search is over.

At the beginning of algorithm description, the path mark variable *Q* is first defined, where *Q*={0,1}, and the path mark value *q* is defined. When *q*=0, it means that there is no valid trust paths in the current search. When *q*=1, it indicates that the current search is success and valid paths from trustor to trustee are formed, then the search stops. Initially, the path mark value q is set to be zero.

Specific steps are as follows:

Step 1. Trustor v_{i0} broadcasts the enquiring message to his neighbor nodes who have the recommended qualifications, and sends the initial nodes set information of each path, the initial path depth information and the current path flag value simultaneously.

Step 2. When neighbor node receives the message, they first check themselves whether is trustee v_{im} . If it is, then we add this node into the set *S(P)*, the variable *D(P)* makes minus one operation and make the path mark value *q* changes to one, the search ends, the trust path is formed. If not, then these nodes check themselves whether exist the recommended informations about trustee. If it exists, then we add the node into the set *S(P)*, the variable *D(P)* makes minus one operation and we keep the path mark value *q*=0.

Step 3. Checking the variable *D(P)* whether is 0, if it is, then the broadcast stops, the path search fails. If not, then the current node continue to forward the enquiring message to the neighbor nodes who have recommended qualifications and not add into the path nodes set, then go to step 2.

When the trust search is complete, the trust recommends diagram which contains n trust paths from trustor to trustee is formed. As shown below:

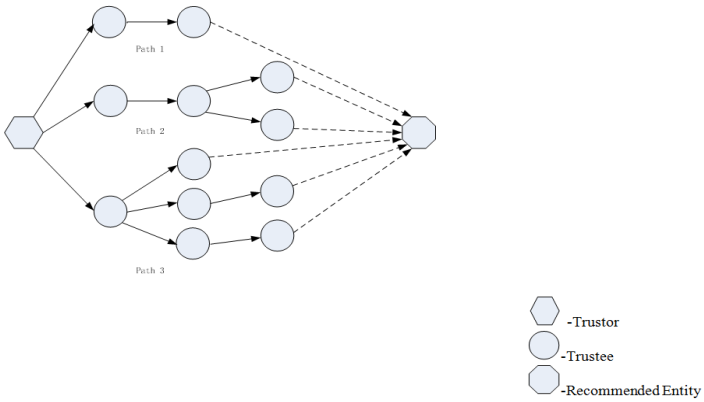

Figure 3. The Trust Recommend Diagram

As shown in Path 1, if only one node is added into the nodes set in each search process, that is to say:

$$\left|S(P_i)\right| = 7 - D(P_i) \tag{3}$$

We consider that the trust path is a acyclic path when the set *S(P)* and the variable *D(P)* satisfy the Equation (3). Acyclic trust path calculate the trust evaluation gradually in accordance with the trust transitivity rules.

As shown in Path 2 and Path 3, if not only one nodes are added into the nodes set in each search process, that is to say:

$$\left|S(P_i)\right| > 7 - D(P_i) \tag{4}$$

We consider that the trust path is a ring-path when the set *S(P)* and the variable *D(P)* satisfy the Equation (4). For the ring-trust path, we first partial transitivity, then partial aggregation.

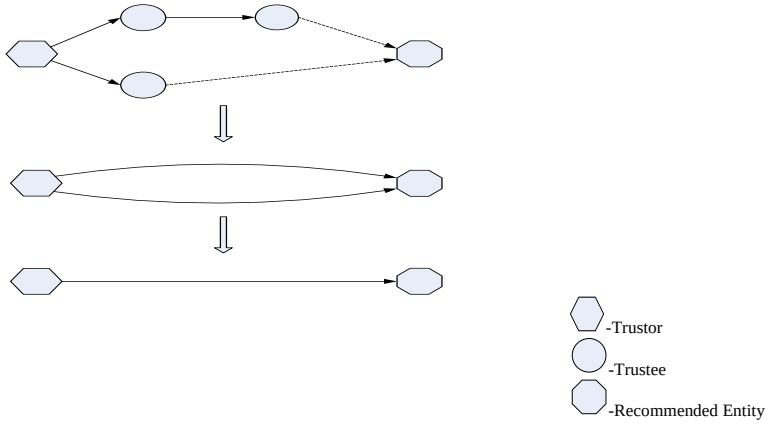

Figure 4. The Computation Rule of Ring Trust Path

An effective trust recommends diagram is obtained through the search of trust network. Based on the diagram and the calculation rules of trust evaluation in Jøsang's model, we can calculate the trust evaluation of each transitivity path by the discounting operator, and then get the comprehensive evaluation from trustor to trustee by the consensus operator.

3.4. Analysis of Time Complexity

The time complexity of trust search algorithm is determined by the number of nodes who participate the recommendations and the complexity of paths. Firstly, we assumes that the total number of nodes in the trust network is x and the expectation value of nodes presents the normal distribution $N(0.5, \sigma^2)$. If the current event weight is V $(0.5 < V < 1)$, then the proportion of number of nodes which expectation value greater than the event weight V accounts for $f(V)$ $(0 < f(V) < 1)$. When the event weight is V, the number of nodes who participate the recommendations in the network is x in general algorithm. The strategy of dual-threshold screening is designed in new algorithm, so the number of nodes is $f(V)x$. Compared two figures we illustrate that the new algorithm reduces the number of nodes greatly when the event weight is high. Secondly, the nodes who have received the message are added into the nodes set *S(P)*, the nodes who added into the set does not receive

other messages again. It simplifies the complexity of trust paths. Furthermore, we assume the average number of neighbors for each node in the trust network is *N*, the average number of overlapping neighbor nodes for each two nodes is *M*(*M*<*N*), the average depth of trust network paths is *L*. In general algorithm, all neighbors of each node must be receive the message, the average depth is *L*, so the time complexity of general algorithm is $O(N^L)$. In new algorithms, the overlapping neighbor nodes are added into the special set, so the time complexity of new algorithm is $O((N-M)^L)$, two figures illustrate that the new algorithm has lower time complexity than the general algorithm.

4. Experiments

In this paper the experiments carried out in the PeerSim simulation environment, and some contrast experiments were made between subjective logic trust model used the new algorithm and Jøsang's algorithm model [14]. In the experiments we compared the success rate of interaction, the node's expectation value and the computational cost. In addition, we set the number of nodes in the network is 1000, the total number of files is 1000 and the files are distributed on the nodes randomly, the degree (the number of neighbor nodes) of each node is 10, each interaction contains the files download 20 times, trustor select a node randomly to download the file each time, the number of successful interactions divided by the total number of interactions constitutes the success rate of this time interaction. Initially, the proportion of absolute trust node, general trust node, critical trust node and untrusted node is 5%, 15%, 30% and 50% respectively. Parameters and their values as follows:

Table 2. Parameters and Their Values

	V	V_1	V_2	E_1	E_2	E_3	E_0	V_0
CASE 1	0.15	0.30	0.70	0.50	0.75	0.90	0.50	0.15
CASE 2	0.50	0.30	0.70	0.50	0.75	0.90	0.50	0.50
CASE 3	0.85	0.30	0.70	0.50	0.75	0.90	0.50	0.85

4.1. Analysis of Success Rate of Interaction

Figure 5 shows the influence of malicious nodes to the success rate of interaction. In the experiment, we assume the malicious nodes commit fraud, and always provide false files in the proportion of 50% . Specific experimental dates as follows:

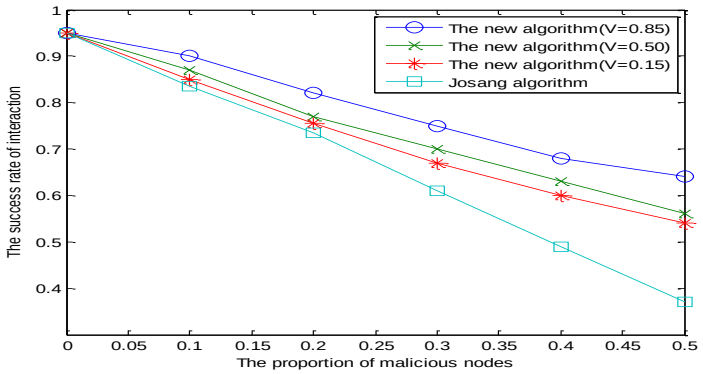

Figure 5. The Success Rate of Interaction Changes with the Proportion of Malicious Nodes Increasing

With the dates above analysis we can see that, trust models used two search algorithms have high success rate of interaction when the original proportion of malicious node is 0. Because at this time all nodes in the network are trusted to provide authentic files, so the recommendations have high credibility. As the proportion of malicious nodes increases, the success rate of interaction about two algorithm models show downward trends and Jøsang's algorithm model has a greater decline than the new algorithm model. Because the dependence paths caused by the overlapping of friends-circle are only split in Jøsang's algorithm, the path dependence is not eliminated fundamentally and the influence of event weight to the node's recommended qualifications is not considered. The new algorithm solves the issue of path dependence completely and it simplifies the complexity of trust relationships by the strategy of set added. Besides, the event-threshold is designed to ensure the nodes who participate the recommendation have high credibility, the nodes with low trust evaluation are removed. Two strategies ensure the new algorithm model has higher success rate of interaction then Jøsang's model at the same time.

Further, Figure 6 shows the success rate of interaction changes with the growth of event weight:

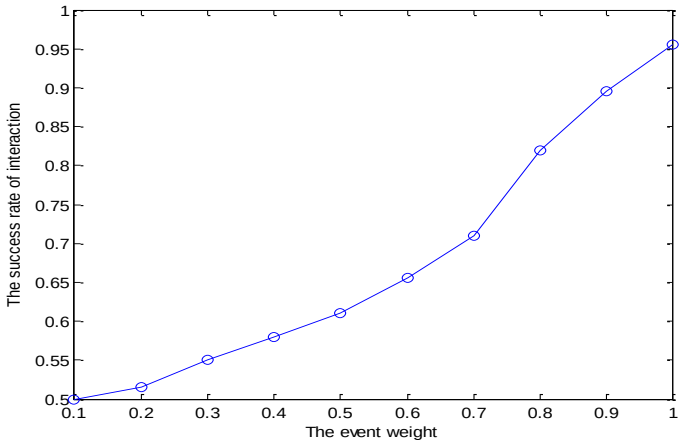

Figure 6. The Success Rate of Interaction Changes with the Growth of Event Weight

As shown above, the success rate of interaction changes with the growth of event weight. Because the event-threshold is designed in the new algorithm, which removes the nodes with low credibility effectively and ensures the services offered by the nodes have high credibility, thus ensuring the model has high success rate of interaction when the event weight is high. In addition, at first, the curve grows slowly, but steepens later. Because with the increasing of event weight, the event becomes more important and the credibility of nodes who participate recommendation also increases. All of them ensure the new algorithm has higher success rate of interaction when the event weight is higher.

4.2. Analysis of Node's Expectation Value

When the simulation experiments beginning, the initial expectation value of four types of nodes is set to be 0.50. Moreover, absolute trust node has high degree of credibility and high success rate of interaction. General trust node has general degree of credibility. Critical trust node has instability degree of credibility, high and low. Untrusted node always provide false

information, it does not have credibility. Figure 7 reflects the expectation value of four types of nodes changes with the increasing of the number of interactions:

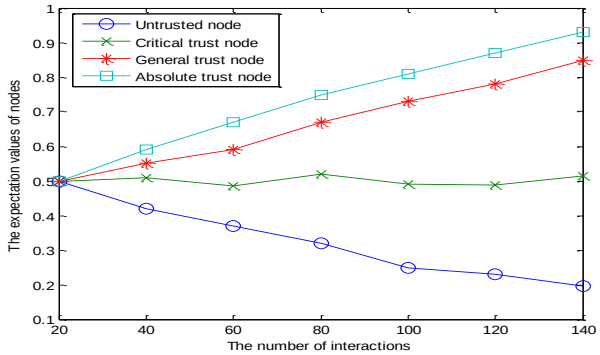

Figure 7. The Expectation Value Changes with the Number of Interactions Increasing

Simulation experiment dates show that: The expectation value of absolute trust node is increasing with the number of interactions increasing, and it grows rapidly. The expectation value of general trust node is also increasing with the number of interactions increasing, but the trend is gentler than the absolute trust node's. The expectation value of critical trust node reveals a trend of fluctuations, ups and downs. The expectation value of untrusted node shows a downward trend. Because trust evaluation between nodes stems from the number of positive events and negative events past observations in subjective logic. In the new algorithm, the dual-threshold screening is designed to guarantee the nodes with high credibility continue to participate the interaction and nodes with low credibility are removed. Therefore, with the number of interactions increasing, the expectation value of four types of nodes present above trends, which effectively distinguish four types of nodes and prevent the cheat from malicious nodes.

4.3. Analysis of Computational Cost

An important cause of the computational cost is the search of trust recommend diagram. The more nodes who participate the recommendation, the higher the computational cost. Therefore, it is critical to simplify the trust relationships reasonably and effectively. Figure 8 reflects the analysis of computational cost in different event weight when the total number of nodes is constant:

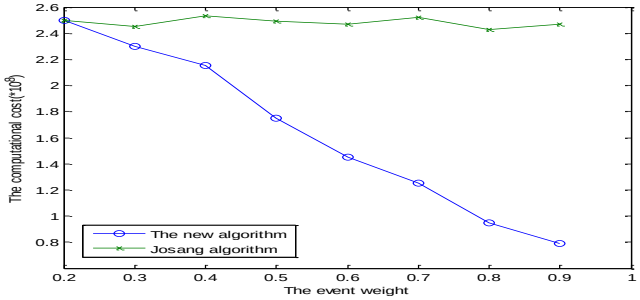

Figure 8. The Computational Cost Changes with the Growth of Event Weight

The influence of event weight is not considered in Jøsang's model, so a node whether involve in the interaction only depends on the history trust evaluation. In the new algorithm model, with the increasing of event weight, we consider that the nodes with low history trust evaluation cannot provide reliable information, so these nodes no longer involve in the interaction. Therefore, the dual-threshold screening is designed to ensure the nodes who participate the recommendation have high credibility. The higher the event weight, the fewer the number of nodes who participate the recommendation, the simpler the trust network. The new algorithm not only ensures the recommendations have high credibility, but also inhibits the malicious nodes offer the recommendations effectively, thus making the trust evaluation more in line with the actual situation.

5. Conclusion

In this paper, the influence of event weight to the node's recommended qualifications was fully considered, and a new trust search algorithm was proposed. The strategies of dual-threshold screening and set added were designed in the new algorithm. Simulation experiments showed that the new algorithm solved the path dependence and trust-circle caused by the overlapping of friends-circle. New algorithm also reduced the computational cost, inhibited the recommendations from malicious nodes effectively, and improved the success rate of interaction. Next step we will improve the discounting operator and consensus operator in Jøsang's model.

Acknowledgements

This work was supported in part by The National Natural Science Foundation of China (61170254, 60873203), the university of Hebei province science and technology research program (ZH2012029) and the Natural Science Foundation of Hebei province (F2014201117).

References

[1] T. Beth, M. Borcherding and B. Klein, Springer, Berlin Heidelberg **(1994).**
[2] G. Lin, Y. Bie, M. Lei and K. F. Zheng, "International Journal of Computational Intelligence Systems", Ahead-of-print **(2013).**
[3] K. Shao, F. Lou, N. X. Mei and Z. T. Tian, "Journal of Software", vol. 12, no. 23, **(2013).**
[4] A. Singh, "International Journal of Engineering Research and Applications", **(2012).**
[5] J. D. Su, H. Q. Guo and Y. Gao, "Journal of South China University of Technology (Natural Science Edition), vol. 4, no. 36, **(2008).**
[6] L. M. Jiang, K. Zhang, J. Xu and H. Zhang, "Journal on Communications", vol. 8, no. 32, **(2011).**
[7] Y. L. Qin, X. P. Wu and J. X. Gao, "Journal on Communications", z1, vol. 33, **(2012).**
[8] A. Jøsang, P. C. G. Costa and E. Blasch, "Determining Model Correctness for Situations of Belief Fusion [C]", Proceedings of the 16th International Conference on Information Fusion, **(2013)** July 9-12, Istanbul, Turkey
[9] A. Jøsang, "Subjective Logic [J]", Book Draft, **(2011).**
[10] A. Jøsang, G. Guo, M. S. Pini, F. Santini and Y. Xu, "Combining Recommender and Reputation Systems to Produce Better Online Advice [C]", Proceedings of the 10th International Conference on Modeling Decisions for Artificial Intelligence, **(2013)** November 20-22; Barcelona, The Kingdom of Spain
[11] A. Jøsang, Editor. Multi-Agent Preference Combination using Subjective Logic [C]", Proceedings of the 11th Workshop on Preferences and Soft Constraints, **(2011)** September 12, Perugia, Italy.
[12] A. Jøsang, T. Ažderska and S. Marsh, "Trust Transitivity and Conditional Belief Reasoning [M]", Proceedings of the 6th IFIP International Conference on Trust Management, **(2012)**May 21-25; Surat, India
[13] A. Jøsang, "Artificial Intelligence", vol. 1, no. 141, **(2002).**
[14] A. Jøsang and T. Bhuiyan, Editors. Optimal Trust Network Analysis with Subjective Logic[C]. Proceedings of the Second International Conference on Emerging Security Information, Systems and Technologies. **(2008)**August25-31, Cap Esterel, France.

[15] A. Jøsang, R. Hayward and S. Pope, "Trust Network Analysis with Subjective Logic [C]", Proceedings of the 29th Australasian Computer Science Conference. **(2006)**January 16-19, Hobart, Australian
[16] X. P. Xue, Y. T. Tan, Z. H. Wang, Y. R. Bi and Y. N. Min, "Application Research of Computers, vol. 3, no. 28, **(2011).**
[17] Z. L. Xiong, W. J. Jiang and G. J. Wang, "Computer Engineering", vol. 8, no. 39, **(2013).**
[18] Q. Jiang, L. L. Liu, X. Su and K. Cai, "Journal of Computer Applications", vol. 5, no. 29, **(2009).**
[19] S. Milgram, "Psychology Today", vol. 1, no. 2, **(1967).**

Authors

Junfeng Tian, he was born in 1965. He is a full professor and has been working on teaching and scientific research for many years. His research interests are in distributed trusted computing, network security.

Peipei Zhang, she was born in 1989. Her research interests are in distributed trusted computing, trust management.