Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 13 (13): 2532-2537, 2013
ISSN 1812-5654 / DOI: 10.3923/jas.2013.2532.2537

A Trust Model in P2P Based on Fuzzy Set Theory

[1,2]Hao Yan and [1]Ying Zhang
[1]College of Information Technology,
Jinling Institute of Technology,
[2]Jiangsu Information Analysis Engineering Laboratory, JiangSu, NanJing, 211169, China

Abstract: In P2P, trust is the basic of effective interactions between nodes but because of the anonymity and dynamic characters, it is difficulty to establish and maintain the trust relationships in the network. In fact trust is not objective but has subjectivity and ambiguity, so this study gives a new distributed trust model based on fuzzy sets theory for evaluating the trust values of nodes which considers multiple network factors, different weights, different interaction results and finally proposes a general algorithm for calculating node's trust. Specifically, this trust model incorporates both direct trust and indirect trust and provides a flexible method to combine the two different parts. At last, by simulations we can see that this trust model can distinguish good nodes and malicious nodes, and give great help for nodes to effectively select appropriate interaction partners.

Key words: P2P network, trust, fuzzy set, satisfaction

INTRODUCTION

P2P network is an open, dynamic environment, its characters of anonymity and no center determine that it can be widespreadly used in e-commerce, distributed-computing and so on (Yu and Singh, 2002). Since the open network, the external trust security between nodes in distributed applications has disappeared mostly. So, for the dynamic distributed environment, how to establish and maintain trust relationships between the nodes in order to ensure the safe operation on distributed applications has became to be a fundamental issue (Dellarocas, 2004).

As a human cognitive phenomena, trust has the subjectivity, uncertainty and ambiguity. Many researchers have do a lot work to give the formalization of the trust, for example Beth model and J Ø sang model are the most representative models. And also Sepanar gave a global reputation-based model EigenTrust, LiXiong raised a trust model called PeerTrust based on reputation, and so on (Beth *et al*., 1994; Josang, 1996; Spanek and Tuma, 2006; Xiong and Liu, 2004). Each model has its advantages on solving the problem of node turst but each model has its flaws either. For example some of them are not considering of the fuzziness of trust but simplely put its subjectivity and uncertainty equivalent to randomness; some models ignore the private and dynamics characters of trust, not giving consideration to the context of each interaction and the solution of how to store the trust values (Hao, 2013).

Fuzziness of trust is not the performance of two values (yes or no), it can be the middle of this two sides (Wan *et al*., 2007). Trust models depend on transactions between nodes through a period of success and failure satisfaction and dissatisfaction to quantify the direct trust value. The result of each transaction is calculated as equal on the final impact on trust which does not match trust in social networks because the trust may change with time. Additionally, the network interactions, such as the values of the information provided, the transfer speed, transfer contents of the authenticity of the transaction and other factors will directly affect the level of satisfaction. So, simply using the successes and failures of this two-valued logic to describe the trust contents of a transaction between nodes is not precise (Schlosser *et al*., 2004).

The study proposes a new trust model in P2P base on fuzzy theory which considers the direct trust, recommendation trust, interaction time, transfer speed and other factors to get the finally trust value. The model can dynamically get the trust value of the nodes, accurately distinguish the good nodes or bad nodes in order to improve the network security.

BASIC CONCEPTS

Trust is a subjective judgment, based on the experiences or interactions, all of the which are inherently subjective. Trust itself is not facts or evidences but the knowledge of the facts observed. At the same time its

Corresponding Author: Hao Yan, College of Information Technology, Jinling Institute of Technology, JiangSu, NanJing, 211169, China

subjectivity comes from observers, so different observers may have different ideas on the same target. Trust relationship is essentially based on faith, with subjectivity, uncertainty and ambiguity which can not accurately be described and validated (Song *et al*., 2005).

Similar to the interpersonal trust of human society, P2P network also has a trust concept between nodes based on the experience of direct or indirect contact with each other on the basis of the credibility on the subjective view which is subjective, dynamic and mainly shows credibility of the behavior of nodes in the network (Repantis and Kalogeraki, 2006). So, in P2P the trusts between nodes are divided into two types of direct trust and indirect trust. Direct trust only deals with the nodes which have transaction records between each other and the degree can be calculated by these records; Indirect trust means there are no transaction records before, so the trust value should be got by querying other nodes (Khambatti *et al*., 2004). That is if the node wants to evaluate the trust of another, it should send requests for asking the node's credibility to its friends and wait for the response result for their trust value. If the friend still has no records, it can continue to make requests to other nodes. With all the result of the friends, the nodes get the final trust value of the target node.

Because of the complexity of network, except the direct result of transactions, the trust can be influenced by many factors, such as network speed, transfer content etc, so trust model must take into account various factors in the transaction process in order to obtain more realistic and effective trust (Kamvar *et al*., 2003). The study fully considers of the process of all transactions and the ambiguity of trust, based on the fuzzy theory proposes a new trust model for improving the accurate assessment of the nodes and preventing collusion attacks, cheating and other bad behaviors.

TRUST MODEL ON FUZZY

Before interactions nodes should firstly get assessment of trust value of the interaction target, if the outcome of the assessment shows the node trustworthy, the interaction can be executed, otherwise refused. In order to obtain more accurate trust values, the trust model should give attentions to both of direct trust and indirect trust (Zhang and Zhao, 2009).

In order to describe the trust model presented in this paper more clearly, the study first introduces the basic concepts of fuzzy set theory.

Fuzzy theory

Definition 1

Membership: Set up a non-empty set X, x is one element of X, give the following mapping for any $x \in X$, $X \to [0, 1]$, $x|\to\psi_T(x) \in [0, 1]$, the set T composed of ordered couples $T = \{(x|\psi_T(x))\}\ \forall x \in X$ is one fuzzy subset of X and function $\psi_T(x)$ is the membership function for x to X. For any specific x, its membership is the value of $\psi_T(x)$ (Wen and Chen, 2003).

Membership $\psi_T(x)$ presents the degree of x belonging to X. If $\psi_T = 1$, x belongs to X entirely; if $\psi_T = 0$, x does not belongs to X entirely. For the $\psi_T(x)$ more closer to 1, the degree of x belonging to X is more deep, to the contrary more closer to 0, the degree of x not belonging to X is more deep.

Using the trust vector composed of the concept of fuzzy set membership to evaluate the trust value of a node, the process is a simple fuzzy comprehensive evaluation. In which there are four basic elements for one trust evaluation:

- Factor set $P = \{p_1, p_2, \cdots p_n\}$, in which every element presents one factor considered between the transaction for evaluating the trust value of a node, such as 'content', 'network speed' and so on
- Interaction feedback value set $f = \{f_1, f_2, \cdots f_n\}$ which presents the satisfaction for each factor after the completion of the transaction
- Factor evaluation matrix $F = (f_{ij})_{n\times m}$, in which f_{ij} denotes the membership of node f_i 's the evaluation result towards f_i, so for n factors, the evaluation matrix is:

$$R = \begin{pmatrix} f_{11} & \cdots & f_{1n} \\ \vdots & \ddots & \vdots \\ f_{m1} & \cdots & f_{mn} \end{pmatrix}$$

- Weight set $W = \{w_1, w_2, \cdots w_n\}$. Factors will take different affects for the evaluation, so they have different weights (Wang *et al*., 2011)

So the calculation of the trust value of nodes based on fuzzy theory is a transform of the factor weight set with the fuzzy evaluation matrix $V = W \circ R$.

Trust evaluation: In P2P network environment, trust of each subject is determined by a number of factors, for example interaction context, transaction time etc which must be considered for assuring the trust vectors, so secondly we should further clarify the definition of the assessment of the P2P network objects.

Define 2

Trust objects: Define a multiple attribute group O = (O_1(t), O_2(t),···O_n(t)), in which (O_1(t),(O_2(t),(O_3(t) denote at time t the trust vector evaluation of the nodes on a particular transaction context O. we can set O to the quantity of resources, computing capabilities, data processing capabilities and so on.

Then the direct trust we can get by the following steps. We use the symbol DT to denote the direct trust value which has the range of [0, 1], 0 means no trust at all, 1 means absolutely trust, higher the value, greater the degree of trust. We use symbol RT to denote the result of one interaction, failure or success, using 0 and 1 to stand for them respectively. Assuming there all n impact factors are considered between each transaction, then all these factors constitute a transaction factor set:

$$P = \{p_1, p_2, \cdots, p_n\}$$

each factor has a respective weight, then the weight collection is:

$$W = \{w_1, w_2, \cdots, w_n\}$$

so we can get the matrix of every membership $S = (s_{ij})_{n\times m}$, $I\in[1, n]$, $j\in[2, m]$, then the weighted average operator:

$$p_i = \oplus\sum_{i=1}^{n} w_i p_{ij}$$

To reduce the complexity, we normalize the weights w_i, then the weighted average operator can be simplified as:

$$p_i = \sum_{i=1}^{n} w_i p_{ij}$$

Assuming the evaluation vector $TV_{ij}(o,) = (t_1, t_2, \cdots t_n)$, the level quantitative vector is $Q = (q_1, q_2, \cdots q_n)$, then the new direct trust can be calculated by the equation:

$$DT^{(t)} = \begin{cases} \sum_{i=1}^{n} t_i * q_{ij} & RT = 1 \\ 0 & RT = 0 \end{cases} \quad (1)$$

Define 3

Decay of trust: With time going, P2P trust values between nodes will decay always. Obviously the more near transaction is, the greater impact on current trust value. And also the trust value has a limited life cycle, in which the value is useful but when time out the older trust value will have no impact of the current interaction. So, in this trust model, we defined a valid time period T and the decay function can be defined to:

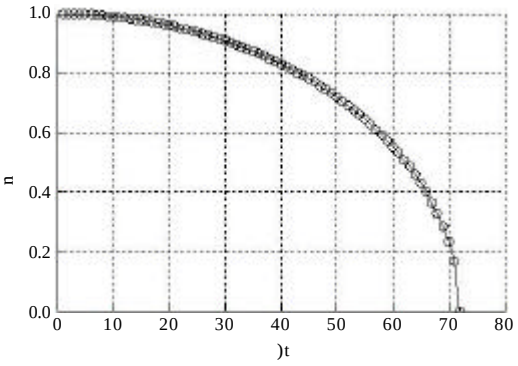

Fig. 1: Decay function of trust

$$\varphi = \sqrt{1-\left(\frac{\Delta t}{T}\right)^2} \quad (2)$$

in which, Δt denotes the time interval from the time of the transaction happened to right now. Assuming T = 72 h, Fig. 1 shows the trust value delay rate.

From the Fig. 1 we can see that with time going, the influence of old trust is decreasing and also the rate of decrease is becoming faster, that is the naturely reflecting of human forgotten line.

According to the above definitions, the direct trust value of node N_b after m interactions with node N_a can be obtained by the equation:

$$DT'_{ab} = \alpha * DT'_{ab} + \beta * \frac{\sum_{i=1}^{m-1} \varphi * DT^i_{ab}}{\sum_{i=1}^{m-1} \varphi} \quad (3)$$

In which, α is the weight of the last interaction trust feedback for impact on the direct trust value and β is the weight of all others interaction for calculating the current trust, both parameters can be adjusted dynamically by user according to conditions.

Indirect trust: To assess the degree of trust between nodes, besides considering the direct transactions, also should consider the reputation of the node in the whole network (Teacy *et al*., 2006) which can be got from node's friends by the recommendation way shown in Fig. 2. From Fig. 2 we can see the way of recommendation trust, node 1 has not transact with node 4 directly, so it can take the evaluation trust of node 4 by his friends node 2 and node 3 which called indirect trust.

Define 4

Indirect trust: Indirect trust value is calculated based on the (denote by RT) recommendations by friends, so the credibility of the friend nodes themselves will have a

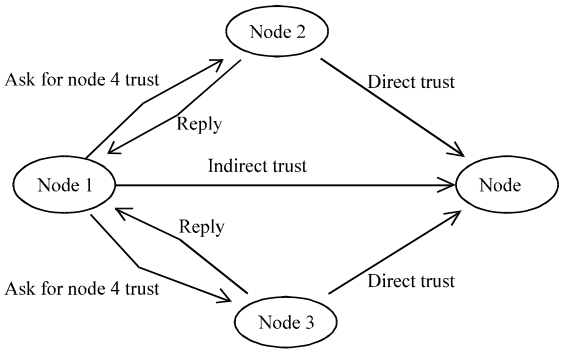

Fig. 2: Recommendation trust process

direct impact on its recommended trust value. If the node itself is not trustful, its recommended credibility trust can not be trustful and at the same time resulting in waste of bandwidth for network queries. So in this model, the node will choose his neighbors with high reputation beyond the setted threshold η. If the nodes don't have suitable friends, system set the target with the original trust value which is just equal to trust threshold. So the indirect trust value can be calculated by:

$$RT = \frac{\sum_{i=1}^{m} T_i * RT_{ai}}{\sum_{i=1}^{m} T_i} \quad (4)$$

in which, m denotes the number of friend nodes. RT denotes the total recommendation trust value of one friend node, RT_α denotes the recommendation value of node N_i to node N_α, T_i is the trust value of node N_i.

The recommendation trust value is real time, that means when the node need, it send request to it's friends and then calculates the value, the node does not store the value. So recommendation trust does not decay with time. At the same time, the friend nodes take into account the decay of trust when feedback its recommended trust value, therefore the decay of the recommendation trust of the nodes are actually contained in the recommended trust values.

Final trust and threshold: The final trust value of nodes insisting of direct trust and indirect trust can be calculated easily based on the above two comprehensive trust algorithm. Assuming that the comprehensive trust of node N_a for node Tab is N_a, So T_{ab} is:

$$T_{ab} = \varepsilon \times DT_{ab} + (1-\varepsilon) \times RT_{ab} \quad (5)$$

in which, ε represents the weight of direct trust which can be adjusted according to actual situation and (1-ε) represents the weight of recommendation trust. In real network environment, if nodes have many direct interaction records, it can set the ε more bigger, otherwise more smaller.

By the Eq. 5, we can get the trust value of the node and normally before this work, we should first choose a threshold value of the trust which is the basic line for judging the node is trustful or not trustful. If the outcome of the trust assessment shows the node is trustworthy, the interactions can be executed, otherwise refused.

SIMULATION AND ANALYSIS

Assuming a node A want to get the file of node B, firstly A should evaluate the trust value of node B. We set factor set O = {'file size', 'download speed', 'file 'version',' interesting'}, the weight set W = {0.2, 0.5, 0.1, 0.2}, the feedback result set is F = {'absolutely trust', trust, 'normal', 'trust a little', 'not trust}, then we get the membership matrix:

$$R = \begin{bmatrix} 0.1 & 0.2 & 0.3 & 0.3 & 0.1 \\ 0.3 & 0.1 & 0.2 & 0.2 & 0.2 \\ 0 & 0.4 & 0.1 & 0.4 & 0.1 \\ 0.5 & 0.2 & 0.1 & 0 & 0.2 \end{bmatrix}$$

and the trust evaluation vector is V = (0.27, 0.17, 0.19, 0.2, 0.17). At last we can get the direct trust is 69. 6 with the quantitative index [96, 80, 60, 55, 45]. If the trust threshold is setted to 65, then the node B is trustful.

And then we do some simulations to verify the correctness and feasibility of this trust model using matlab10. We suppose there are 500 nodes in the network environment with the weight ε = 0. 6 and T = 60 sec.

The first simulation is that we set all the 500 nodes with the random trust value in [0. 5, 0. 7] with the distribution in Fig. 3. Among all the nodes, we set 20% malicious nodes who will supply bad service, 50% normal nodes supplying success and fail service randomly and 30% good nodes supplying excellent services. After 500 cycles, the nodes trust values distributed as Fig. 4, in which green points present good nodes, blue points present normal nodes and gray nodes presents malicious nodes. From the figure we can see that with the transaction the trust values of good node is ascending and almost beyond 0.7 and the trust values of normal nodes have a big range from 0.45 to 0.8, at the same time the trust values of malicious nodes almost below 0.4. So the trust model can give a right evaluation trust value of all nodes.

Secondly, to check the ability of resist collusion and cheating attacks of this trust model we record the simulation cycles and the successful interaction ratios in

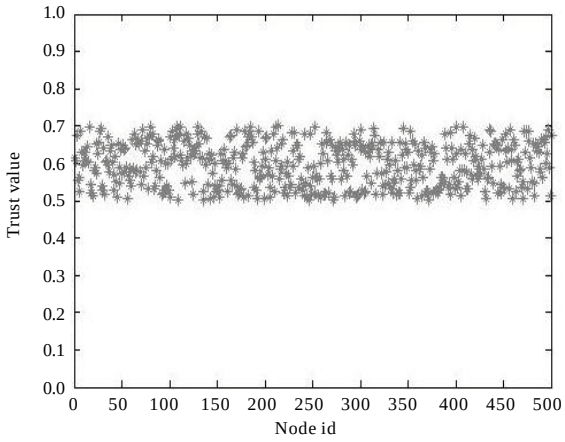

Fig. 3: Initial trust values

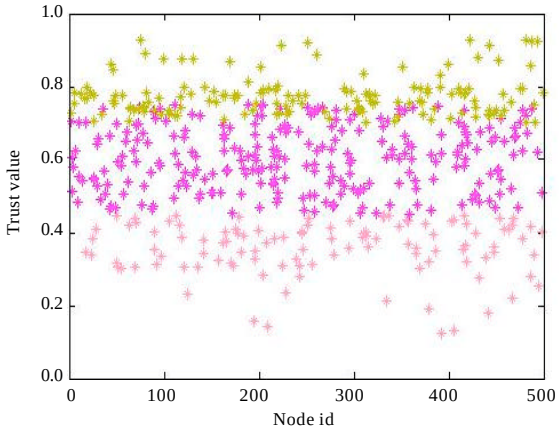

Fig. 4: After 500 cycles

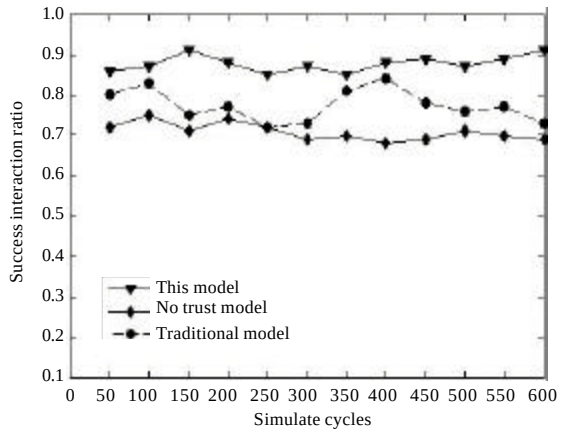

Fig. 5: Comparison of three enviroment

different trust models. The result of this simulation is shown in the Fig. 5. We can see that compared to no trust model and traditional model, this trust model will get a higher successful interaction ratio, that's because the trust model will distinguish good node or bad node and then prevent the interaction if the target node is not trustworthy.

CONCLUSION

Security is a mostly hot issue of P2P network, researching the trust relationship in P2P is a sensely work for the real world. In this study, we propose a new trust model in P2P based on fuzzy theory which can accurately assess the trust between nodes, restrain the cheating and other harmful behaviors and get rid of malicious nodes. It can supply effective decision support for the development of new network, improve the security of the P2P network.

ACKNOWLEDGMENT

Project supported by the College and University Natural Science Foundation of the Ministry of Education, Jiangsu (13KJD520004, 12KJD510006).

REFERENCES

Beth, T., M. Borcherding and B. Klein, 1994. Valuation of trust in open networks. Proceedings of the 3rd European Symposium on Research in Security, (ESORICS'94), Springer-Verlag, Brighton, pp: 3-18.

Dellarocas, C., 2004. Sanctioning reputation mechanisms in online trading environments with moral hazard. MIT Sloan Work. Paper, 3: 1-43.

Hao, Y., 2013. Research of a new distributed trust model in P2P. Inform. Technol. Appl. Ind., 263-266: 1085-1090.

Josang, A., 1996. The right type of trust for distributed systems. Proceedings of the 1996 New Security Paradigms Workshop, September 17-20, 1996, Lake Arrowhead, pp: 119-131.

Kamvar, S.D., M. T. Schlosser and H. Garcia-Molina, 2003. The eigentrust algorithm for reputation management in p2p networks. Proceedings of the 12th International Conference on World Wide Web, May 20-24, 2003, Budapest, Hungary, pp: 640-651.

Khambatti, M., P. Dasgupta and K.D. Ryu, 2004. A role-based trust model for peer-to-peer communities and dynamic coalitions. Proceeding of the 2nd IEEE International Information Assurance Workshop, April 8-9, 2004, Charlotte, NC, Pages: 141.

Repantis, T. and V. Kalogeraki, 2006. Decentralized trust management for ad-hoc peer-to-peer networks. Proceedings of the 4th International Workshop on Middleware for Pervasive and Ad-Hoc Computing, (MPAC 2006), New York, Pages: 6.

Schlosser, M.T., T.E. Condie and S.D. Kamwar, 2004. Simulating a file-sharing P2P network. Proceedings of the 1st Workshop on Se-mantics in P2P and Grid Computing, October 2004, Budapest, pp: 69-80.

Song, S., K. Hwang, R. Zhou and Y.K. Kwok, 2005. Trusted P2P transactions with fuzzy reputation aggregation. IEEE Internet Comput., 9: 24-34.

Spanek, R. and M. Tuma, 2006. Securegrid-based computing with social-network based trust management in the semantic web. Neural Network World, 16: 475-488.

Teacy, W.T.L., J. Patel, N.R. Jennings and M. Luck, 2006. TRAVOS: Trust and reputation in the context of inaccurate information sources. J. Autonomous Agents Multi-Agent Syst., 12: 183-198.

Wan, J., R.T. Zheng and X.H. Xu, 2007. Research of incentive mechanisms in P2P network. J. Comput. Appl., 27: 2202-2205.

Wang, T.C., Y.L. Luo, K.Z. Zuo and B. Jie, 2011. Dynamic trust model based on trade weight for P2P network. Appl. Res. Comput., 28: 300-303.

Wen, T. and Z. Chen, 2003. Research of subjective trust management model based on the fuzzy set theory. J. Software, 14: 1401-1408.

Xiong, L. and L. Liu, 2004. PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities. IEEE Trans. Knowledge Data Eng., 16: 843-857.

Yu, B. and M.P. Singh, 2002. An evidential model of distributed reputation management. Proceedings of the 1st International Joint Conference on Autonomous Agents and Multiagent Systems, July 15-19, ACM, New York, pp: 294-301.

Zhang, J.A. and H.Q. Zhao, 2009. Research on fuzzy trust model for P2P network. Microelect. Compu., 26: 158-162.