Dynamic Evaluation of Recommendation Trust in Open Networks

Yu Zhang[1,2], Guangmin Sun[1,*], Peng He[3], Peng Zhai[1] and Yuge Sun[4]

[1]*Faculty of Information Technology, Beijing University of Technology, Beijing, China*
[2]*Department of Computer Science, Jining University, Qufu, China*
[3]*College of Computer and Information Technology, China Three Gorges University, Yichang, China*
[4]*School of Electrical and Electronic Engineering, the University of Manchester, Manchester, United Kingdom*
E-mail: gmsun@bjut.edu.cn
[*]*Corresponding Author*

Received 09 September 2020; Accepted 21 October 2020;
Publication 23 December 2020

Abstract

Trust evaluation is a key issue in the interaction between network entities in open networks. The attacks of malicious entities have become a major obstacle to the development of open networks. Few traditional trust models have considered incorporating incentive mechanisms to reduce the influence of recommendation values from malicious entities in trust evaluation. This paper proposed a dynamic evaluation of recommendation trust model, considering the interaction procedure between entities, introducing reward-punishment factor and evaluation reliability factor. The function of reward-punishment factor is to reward honest interactions between entities while punishing fraudulent interactions. The evaluation reliability factor is used to decide whether to accept the recommendations from the recommending entities. Simulation results show that the model could effectively reduce the influence

Journal of Web Engineering, Vol. 19_7–8, 1173–1192.
doi: 10.13052/jwe1540-9589.197811

of malicious entities in trust evaluation. The proposed model could accurately and reliably identify the access behaviour of malicious entities, and adopt appropriate processing countermeasure to ensure the accuracy and fault tolerance of calculation.

Keywords: Open networks, recommendation trust, dynamic, evaluation.

1 Introduction

1.1 Research Background

The characteristics of open networks are openness, anonymity, self-organization and so on, and make it widely used in instant messaging, file sharing, distributed computing and other fields. This also shows that the security and reliability services provided by network entities cannot be ignored. The issue of trust between entities has become a major obstacle to the further development of open networks applications. In the current open networks, there are mainly the following types of malicious entities attacks: oscillating entity attacks, malicious entity uses multiple small-scale transactions to increase trust to obtain trust of other entities, and provides false transactions in a large-scale transaction, a group is formed between malicious entities, within the group entities exchange and give satisfactory evaluations to enhance mutual trust in order to conduct false transactions with other entities. In addition, there is a class of malicious entities that seriously affect the availability and robustness of open networks, that is, selfish entities that only download and do not share resources. This selfish behaviour of entities severely affects the service availability of open networks. In order to improve the traditional trust model to deal with the problem of insufficient malicious entities, this paper proposed a method for the evaluation of recommendation trust by considering the interaction procedure between entities and by introducing a bonus-penalty factor as well as the reliability of trust evaluation.

1.2 Method of This Paper

To solve the problem resulting from the lack of incentive mechanisms in the classic trust models and to minimize the influence of the recommendations from malicious entities in trust evaluation, we provide a method for the evaluation of recommended trust by incorporating the interaction procedure between entities in the process of trust evaluation. In this paper, the notions

of incentive factor and the credibility of evaluation were taken into consideration. We will also perform some experiments to evaluate the effectiveness and to validate the advantages of our proposed method over some existing methods.

1.3 Organization of This Paper

The rest of this paper is organized as follows. In the next section, we introduce several key concepts that are critical in our work. In Section 3, we propose the method for evaluation of recommendation trust in which we will first describe the interaction procedure, the reward-punishment factor and credibility of evaluation. Subsequently we present the formula that is the centre of our method. In Section 4, we describe the analysis of our proposed model. In Section 5, we describe our experiment and analyse the results to evaluate and validate the effectiveness of our proposed method as well as to compare and show the advantages of our method over an existing method. Lastly, in Section 6, we conclude this paper.

2 Related Research

Trust can better reflect the multi-domain heterogeneity, high dynamism and uncertainty of open networks, thus trust management is a key technology for access control in network security [1–3]. Among the conventional trust models, EigenTrust was a very authoritative trust algorithm. However, the EigenTrust model used the service trust value to define the recommended trust value, which could not perfectly reflect the authenticity of the actual recommendation information of the node. Although the EigenTrust model considered the influence of malicious entities, it ignored the reward-punishment factor as well as the security of the network interaction entities.

In order to improve the P2P trust model's ability of inhibiting malicious nodes, by means of grouping nodes in the network according to the level, using the basic fuzzy inference rule, combining trust value and contribution value, limiting the resource access according to the level of node, the Grouping P2P Trust Model could effectively inhibit the attack of malicious nodes, and successful rate of file download was higher than EigenTrust model [4]. Because a fundamental consideration in design of trust model in a peer-to-peer system was the self-interest of individual peers, Abrams et al. [5] proposed a strategy proof partition mechanism that provided incentives for

peers to share files, avoided manipulation by selfish interests, approximated trust scores based on EigenTrust. Comparing with EigenTrust model, the DHTrust model made significant improvement in convergence speed and aggregation accuracy [6].

With the in-depth study of various large-scale distributed applications based on internet, system was represented by a dynamic collaboration model composed of multiple software services. In order to overcome the problem of inadequate handling capacity for multi-source behaviour data in traditional trust model, rough set theory and information entropy theory were combined and applied to the study of distributed dynamic trust measurement and prediction model based on behaviour data [7]. Because cross-domain secure access was required in heterogeneous environments, Li et al. [8] proposed a trust attribute-based access control algebraic system of policies composition. To resolve the risk problem of transaction in P2P network, by simulating interpersonal interactive process in society network, Zhang et al. [9] proposed a trust management model based on dynamic recommendation. In order to meet the requirements of the real-time response, privacy and security, Deng et al. [10] proposed a resource/user comprehensive trust evaluation system model aiming at user experience quality. Fang et al. [11] discussed and analysed the existing problem, current research situation and development trend in the preparation and executing stage of ABAC. In order to ensure that the node could provide reliable resources and good service, Zhao et al. [12] proposed a P2P network trust model based on time series, builded trust relationship between peers, introduced a time decay function. The model could improve credibility to P2P network because it had better dynamic self-adaptability and better ability to check the malicious peers than EigenTrust. These models above considered interest, behaviour, environment, trust attribute, user experience, time series and so on, but they lacked of punishment mechanism and recommendation trust evaluation was not accurate enough.

Based on Attribute-Based Access Control, Shi et al. [13] proposed a dynamic and adaptive access control model. On the basis of fuzzy theory, Liu et al. [14] proposed a Task-based access control model of peer-to-peer network. Concerning the problems of Attribute-Based Encryption(ABE) such as high computational consumption and lack of flexibility in mobile Internet, Chen et al. [15] proposed a Ciphertext-Policy ABE(CP-ABE) access control scheme based on dynamic trust level. On the basis of a continuous process, Shao et al. [16] proposed a recommendation trust model for describing indirect trust. Nie et al. [17] proposed an optimization

technology of attribute access control based on trust evaluation in cloud computing environment. Huang et al. [18] proposed a new trust evaluation model which related to the trust of the individual partner, the explicit and implicit trust relationship among partner services. Woongsup [19] proposed a trust model which was used to ensure the credibility of service providers. Through indicating the credible extent of service providers, a service was determined to be credible or not. Naima et al. [20] proposed a defence mechanism for filtering out dishonest recommendations based on a measure of dissimilarity function between two subsets. A subset of recommendations with the highest measure of dissimilarity was considered as a set of dishonest recommendations. In order to solve the problem of recommended trust evaluation in trust-based access control, Zhao et al. [21] proposed a model of recommended trust evaluation based on the gray correlation analysis. These models above considered application of indirect recommendation trust, but they lacked of comprehensive consideration of reward-punishment factor, evaluation reliability factor and balance weight factor.

3 Relevant Concepts

Trust: it expresses one entity's expectation regarding the honesty, trust, ability, reliability, etc. on another entity to engage in an interactive activity during a certain period of time and within a certain context.

Recommended trust (TR): it describes the situation that interactive entities haven't reached a desired level of trust directly and the establishment of a trust relationship needs to be aided by recommendations from other entities. It can also be called indirect trust.

Direct trust (TD): it expresses one entity's level of trust on another entity based on direct, historical interactive experiences between the two entities.

Domain recommendation trust (TDR): it expresses the situation in which the two interactive entities have no direct interactions and the trust is established based on recommendation information from entities within a domain such as an organization or a community.

Global trust (TG): it expresses an aggregated trust value by applying appropriate weights to the direct and recommendation trust. The aggregated trust reflects the global view of one entity's trust on another entity in a certain network interaction under a certain network environment.

Reward-punishment factor: it indicates the incredible level of recommending entity's trust value during calculation of recommendation trust. In another word, it can express how degree the acceptance of a recommending entity is.

Reliability of evaluation from recommending entities: during the measurement of recommendation trust, the reliability of the recommending entities must be considered when the recommendation trust values are utilized.

We can infer that an effective evaluation of trust among interactive network entities is to combine the direct trust and indirect trust. In this paper, we focus on the evaluation of recommended trust, and we consider the factors of reward and punishment and the reliability of the evaluation. The purpose of this method is to enhance the effectiveness of trust evaluation.

4 Recommendation Trust Measurement Model

4.1 The Interaction Procedure

The behaviour of entities during an interaction is one of the main factors. In open networks, the behaviour determines whether the interaction will be successful. The different network interactive environments also influence the success of the interactions. For example, in a social network, not only the username and password, but also the age, sex, hobby, etc. of the users are needed for successful interactions. In a financial management platform, every activity affecting the trading volume would generate an alert so that the system would check whether information in affected accounts still remains correct and consistent. Trust between people in the real world has been applied to the research on trust measurement and evaluation in the information and network world. The complexity of trust can thus be modelled and described using multi-dimension service attributes that would influence the trust in many angles and dimensions so that the results of trust measurement and evaluation are reasonably useful.

A model of the interaction procedure is depicted in Figure 1 in which we could see that the global trust is comprised of direct trust and recommendation trust. The global reliability of entities as well as the multi-dimensional attributes can be obtained by calculating direct trust and indirect trust. This indirect trust is recommendation trust. The formation of the recommended domain of entities is the foundation of trust calculation. The calculation of recommendation trust is restricted to the recommended domain of entities. The value of recommendation trust of entities and attributes is the result of evaluating recommendation trust from the recommending domain.

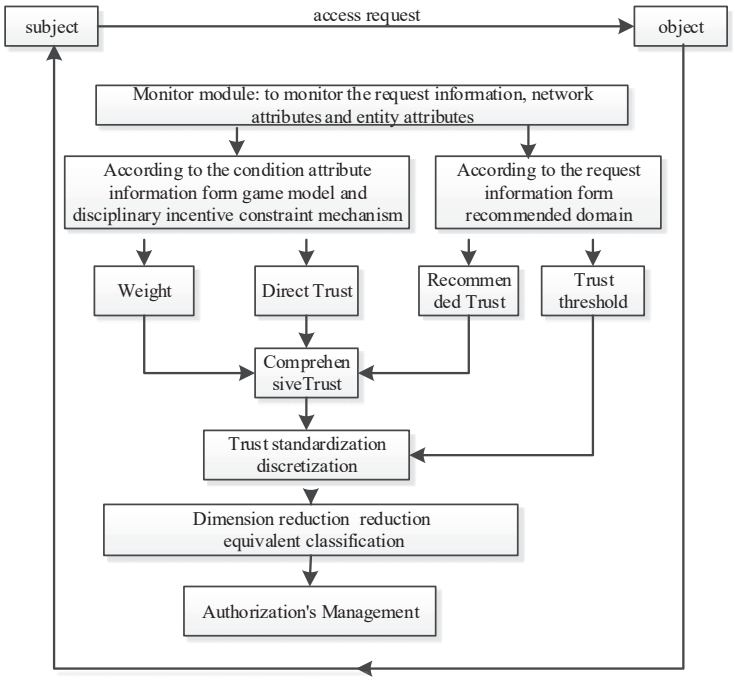


Figure 1 The interaction procedure between entities in open networks.

4.2 The Reward-Punishment Factor

The reward-punishment factor is introduced to indicate reliable degree of the trust value of recommendation trust. The purpose of Reward-punishment is to reward honest interactions between entities while punishing fraudulent interactions. In network interactions, the trust levels of the feedback reliability x include $\varepsilon_1, \varepsilon_2, \varepsilon_3$ to respectively express total distrust, conditional trust and total trust. The space of the trust levels is called L, $L = \{\varepsilon_1, \varepsilon_2, \varepsilon_3\}$, $\varepsilon_i \bigcap \varepsilon_j = \phi(i \neq j)$ and $\varepsilon_1 < \varepsilon_2 < \varepsilon_3$. Thus, the reward-punishment function $f(x)$ is defined as follows:

$$f(x) = \begin{cases} 0 & (0 \leq x \leq \varepsilon_1) \\ \dfrac{\sin\left(\frac{x-\varepsilon_1}{\varepsilon_2-\varepsilon_1} \cdot \pi - \frac{1}{2}\pi\right) + 1}{2} & (\varepsilon_1 \leq x \leq \varepsilon_2) \\ 1 & (\varepsilon_2 \leq x \leq 1) \end{cases} \tag{1}$$

Where the values of $\varepsilon_1, \varepsilon_2, \varepsilon_3$ would change dynamically as the application environment changes.

4.3 Reliability of Evaluation

In the calculation of recommendation trust, the reliability of evaluation of the recommending entities is used by the primary entity to decide whether to accept the recommendations from the recommending entities. The primary entity obtains the reliability of evaluation of the recommending entities by considering the recommendation trust from the recommending entities.

Suppose entity O obtains the trust evaluation of another entity S through a third entity E. Entity O would judge the trust evaluation of entity S given by entity E and, through related calculations, derive a weight value for the recommendation trust.

If set $U_{e,o}$ contains the entities that have interacted with entities O and E in the past and have performed evaluation on entity S, then the value of $num(U_{e,o})$ is the number of elements in set $U_{e,o}$. Each recommending entity has an honest factor for its own recommendation which, denoted as c, is the ratio of the number of satisfied recommendations to the total number of recommendations. This can be expressed as the probability of success P with an initial value of, say, 0.5 (i.e., 50%) to avoid any bias. That is, the honest factor of any recommendation is always 0.5 in the first recommendation.

The model for calculating the reliability of evaluation for the set $U_{e,o}$ of entities E given by entity O is thus:

$$\eta_{U_{E,O}} = \frac{1}{2num(U_{e,o})} \sum_{X \in U_{E,O}} |TD_{e \to x} - TD_{o \to x}| + p(x) \tag{2}$$

Where the initial value of η_e is 0.5 and the number of elements of set $U_{e,o}$ is 0.

During the calculation of trust from the recommending entities in an open network, the reliability of evaluation serves as the basis for the calculation of the global recommendation trust, which reflects the reliability of recommendation trust relationship. In order to resist fraudulent recommendations from dishonest or malicious entities, the primary entity considers the influence of recommending entities.

4.4 Measurement of Recommendation Trust

By considering the influence of the reward-punishment factor, the reliability of evaluation from the recommending entities and the recommendation trust in the calculation of recommendation trust, the model for recommendation

trust of the entities in set $U_{e,o}$ is as follows:

$$TR_{e\to s} = \frac{1}{2}\left(\left(val(r_{e\to s})\cdot\eta_{e\to s} + \frac{f(x_{e\to s})}{\sum_{i\in U_{e\to s}} f(x_{i\to s})}\right)\cdot TD_{e\to s}\right) \quad (3)$$

In the network, entities have interacted with each other. An entity would consult the recommendation trust of other entities and calculate the global recommendation trust by considering the combination factors. The combination factors include reward-punishment, the reliability of evaluation of recommending entities and the recommendation trust values.

Thus, The calculation model of the global recommendation trust value is as follows:

$$TDR_{U_{e\to s}} = \frac{1}{2}\sum_{i\in U_{e\to s}}\left(\left(val(r_{i\to s})\cdot\eta_{i\to s} + \frac{f(x_{i\to s})}{\sum_{i\in U_{e\to s}} f(x_{i\to s})}\right)\cdot TD_{i\to s}\right) \quad (4)$$

Where $val(r_{i\to s})$ is the ratio of the amount of successful interactions over the total amount of interactions by all the entities. These entities have interacted with the entity being evaluated.

5 Experiment and Analysis

5.1 Experimental Environment and Parameter Settings

We have performed some experiments to evaluate our proposed method for calculating recommendation trust. The environment of experiment is as follows: the computer used is a Lenovo PC, the software is an open source one developed by Stanford University called Query Cycle Simulator and the Java language is used in the programming to simulate the recommendation trust model. Then, Matlab is used to analyse the results.

Query Cycle Simulator could be used to simulate the classic shared network of P2P file resources and it provides the basic evaluation function. The core idea is to take network entities as self-adapting smart entities based on some simple rules that originate from the abstraction and simplification of human behaviours.

5.2 Choice of the Reward-Punishment Factor

In the evaluation of recommendation trust, the choice of the reward-punishment factor expresses the degree of acceptance of the trust values from

recommending entities. In the process of interactions in an open network, the values of $\varepsilon_1 < \varepsilon_2 < \varepsilon_3$ change dynamically along with the application environment. The relationship between reliability and reward-punishment can be seen in Figure 2 when the space of trust levels in the experiment are set as $L_1 = \{0, 0.15, 0.85\}$, $L_2 = \{0, 0.05, 0.95\}$ respectively.

The results in Figure 2 show that the level of reward and punishment is expressed by reward-punishment factor. The level of reward and punishment changes dynamically along with values of trust levels. Furthermore, the values of trust levels change according to the network interaction environment.

Therefore, reward-punishment changes dynamically as the network environment changes. When the value of reliability is higher than 0.5, the reward-punishment factor takes a positive effect and the degree of adoption will improve as interactions take place between entities. When the value of reliability is lower than 0.5, however, the reward-punishment factor takes a negative effect and the degree of reward and punishment would decrease by a large margin. When the value of reliability is 0, malicious entities can be effectively filtered out, resulting in recommendations from such malicious entities to be recognized and resisted so as to insure the reliability of recommendation trust.

5.3 Effectiveness of Recommendation

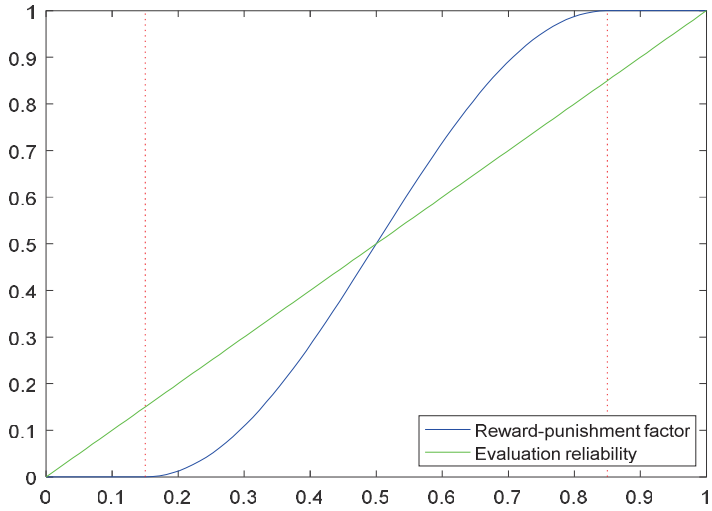
We define the interaction satisfaction ratio as the ratio of satisfied interaction amount over the total amount of interactions from all entities. The interaction satisfaction ratio is expressed as SP (expressed in percentile).

The parameters in the experiment are as follows: the trust level space $L_1 = \{0, 0.15, 0.85\}$, the number of entities E is between 100 and 1000, the initial network topology is random, the percentage of normal entities is 100% and thus that of malicious entities is 0% and the threshold for being trusted is [0.5–1]. In addition, in our comparison analysis, we assume the same number of entities in our proposed trust model (MyRTrust) and the EigenTrust model.

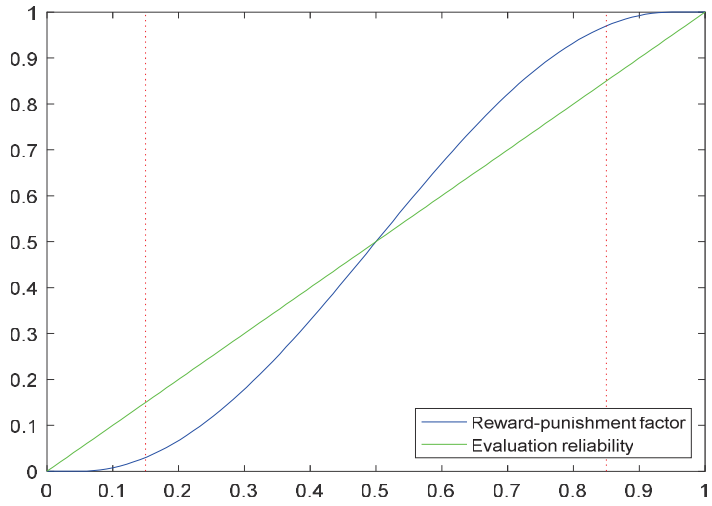
There is no interaction behaviour in networks at first. For the sake of performing the evaluation in an objective and useful manner, we start the analysis from the 51th period of the interactions, in which we don't take into consideration of the influence of direct trust.

Experiment 1: Percentage of malicious entities varies between 0% and 50%.

Figure 3(a) shows the results for 10 periods in an environment in which there is no malicious entity. During each period, each entity would send an

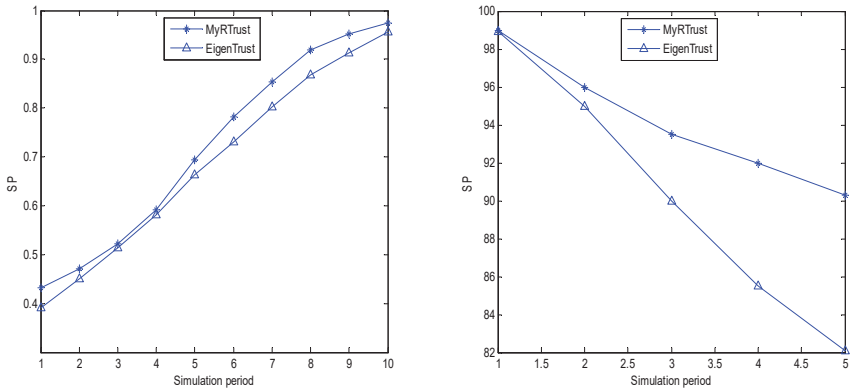


(a) Space of the trust levels are set as $L_1 = \{0, 0.15, 0.85\}$



(b) Space of the trust levels are set as $L_2 = \{0, 0.05, 0.95\}$

Figure 2 Relationship between reliability and reward-punishment when the space of trust levels are set as different values.



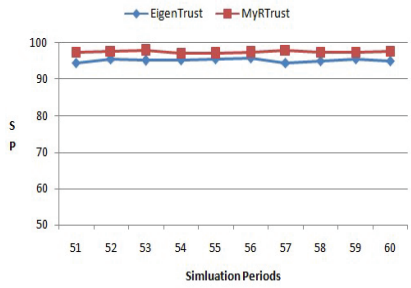
(a) There is no malicious entity

(b) There are varying numbers of malicious entities

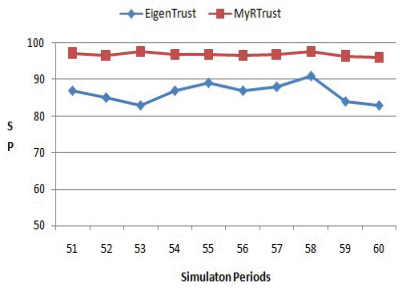
Figure 3 Comparison of SPs whether there are malicious entities or not.

interactive service request, which generates a proper response to the request. As can be seen in the Figure 3(a), the speed of evaluation and clustering of recommendation trust in MyRTrust is faster than that in EigenTrust in all the 10 periods.

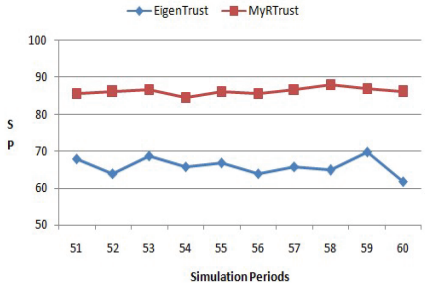
When there are malicious entities in the network, the interaction satisfaction ratio SP would be affected by the percentage of such malicious entities. Figure 3(b) shows the results in which the amount of network entities is invariant in the experiment. However, the percentage of malicious entities varies between 0% and 50% with an increment of 10%. In this experiment, we carry out a total number of 100 simulation periods for each of the above scenarios that corresponds to the percentage of malicious entities and the SP value is the average of the interaction satisfaction ratios for the 51–100th periods. As can be seen in the Figure 3(b), the percentage of malicious recommending entities increases along with the increasing number of interactions. And the accuracy of evaluation of global recommendation goes down continuously resulting in reduction in the number of successful interactions as well as a decrease for SP to some degrees. Since every fraudulent recommendation from a malicious recommending entity would also affect the trust on itself by other entities in future interactions, the recommendation trust that it provides will become less effective as the result. Thus, this reward and punishment mechanism plays an important role in the model. Because of not having the mechanism above, the EigenTrust model, however, is not able to lower the influence of trust evaluation from such malicious entities, causing the SP to drop very dramatically.



(a) Percentage of malicious entities is 0%



(b) Percentage of malicious entities is 10%



(c) Percentage of malicious entities is 30%

Figure 4 Influence of different proportion of malicious entities on SP.

Experiment 2: Percentage of malicious entities remains unchanged.

In the experiment, the number of preset entities in MyRTrust and EigenTrust model remains the same and unchanged. The simulation experiment parameters set the percentage of malicious entities to 0%, 10% and 30%. Each entity sends out an interactive service request in each cycle. For the authenticity and objectivity of the simulation, since there is no network interaction information between entities during network initialization, the data analysis of Experiment 2 is also performed from the 51thperiod of the interactions.

Figure 4 shows the results of the simulation experiment, in which Figure 4(a), (b) and (c) respectively indicate that, when the ratio of malicious entities is 0%, 10% and 30%, the interaction satisfaction ratio changes as the percentage of malicious entities changes.

Figure 4(a) shows that, under the condition that all network entities are honest, the interaction satisfaction rate of the MyRTrust model is higher than EigenTrust model, and the curves of two models are smooth.

Figure 4(b) shows that,under the condition that the percentage of malicious entities is 10%, there is no significant impact on the interactive satisfaction rate of the MyRTrust model, but the interactive satisfaction rate of the EigenTrust model decreases to a certain extent and its curve has changed somewhat.

Figure 4(c) shows that,under the condition that the percentage of malicious entities is 30%, the interactive satisfaction rate of above two models both decrease to a certain extent and the curves both become no longer smooth.

It can be seen from the changes of the curves in Figure 4 that the interaction satisfaction rate of the MyRTrust model is significantly higher than EigenTrust model. As the percentage of malicious entities increases, the number of access failures increases. At the same time, the interaction satisfaction rate of the two models is obviously reduced. In MyRTrust model, the malicious entities may be blocked by the recommendation of other entities in the process of recommendation.

Therefore, when the percentage of malicious entities is small, the interaction satisfaction rate of the MyRTrust model is less affected than that of the EigenTrust model, indicating that the MyRTrust model can effectively weaken the impact of malicious entity recommendation on entity trust evaluation.

6 Model Analysis

6.1 Accuracy

In the process of quantitative calculation of trust measurement, the influence parameters of trust are considered comprehensively in our proposed trust model. Historical interaction information is considered in the measurement process of direct trust. Not only reward-punishment factor but also reliability of evaluation are considered. Therefore, our proposed trust model can accurately and reliably identify the access behaviour of malicious entities, and adopt appropriate processing methods to ensure the accuracy and fault tolerance of calculation.

6.2 Dynamic Adaptability

In the process of quantitative calculation of trust measurement, the dynamic influence parameters are considered from multiple aspects. In the process of quantitative calculation of the comprehensive trust measurement, the balance

weight factor is introduced to solve the weight proportion of direct and indirect trust. In the process of network interaction, the balance weight factor changes dynamically along with amount of interactions. This mechanism reflects the dynamic adaptability.

6.3 Incentive

In the process of recommendation measurement, reliability of evaluation of the recommendation entity is used to determine whether the access object adopts the recommendation of the recommendation entity, and the reward-punishment factor is introduced as the trust degree for the access object to evaluate the direct trust of the recommendation entity. This network environment encourages network entities to accumulate trust and provide integrity services. Whether the choice of reward-punishment factor is appropriate, directly determines the magnitude of incentives, that is, the level of reward-punishment standards, directly affects the effect of incentives. Inappropriate reward-punishment standards not only do not play an incentive role, and sometimes even counterproductive, resulting in the distortion of trust calculation and the occurrence of dishonest access behaviour.

7 Conclusion

We propose a dynamic evaluation of recommendation trust model, considering the interaction procedure between entities, introducing reward-punishment factor and reliability of evaluation factor. In the process of quantitative calculation of trust measurement, the calculation of trust measurement of entity comprehensively considers the influence factors such as direct trust, indirect trust and feedback credibility, which can effectively identify and resist the recommendation of malicious entities, resist active or passive attacks by malicious entities, and ensure the reliability of the recommended trust value. Simulation experiments results show that our proposed trust model would effectively reduce the influence of recommendation trust values from malicious entities. The model can be used in a variety of network system access control scenarios.

The trust quantification method in our proposed model has reference value for the evaluation and quantification of trust in open network environment. Future work is to simplify the overly complex recommendation trust relationship, improve the accuracy and convergence, establish perfect incentive mechanism for untrustworthy network access behaviour between

entities, establish the entity-oriented multi-dimensional attribute dynamic game trust evaluation model in the universal environment, and amplify the universality of trust evaluation and quantification against the deficiencies of various models.

Acknowledgments

The study was been supported by National Natural Science Foundation of China (Grant: 11527801, 61305026) and A Project of Shandong Province Higher Educational Science and Technology Program (Grant: J17KA048).

References

[1] W. Sherchan, S. Nepal, C. Paris., 'A Survey of Trust in Social Networks', ACM Computing Survey, 45(4), pp. 119–228, 2013.
[2] G. Han, J. Jiang, L. Shu, et al., 'Management and Applications of Trust in Wireless Sensor Networks: A Survey', Journal of Computer and System Sciences, 80(3), pp. 602–617, 2014.
[3] B. Zhao, J. He, Y. Zhang, et al., 'Dynamic trust evaluation in open networks', Intelligent Automation & Soft Computing, 22(4), pp. 631–638, 2016.
[4] X. Cao, X. Shao, Z. Lu., 'Grouping P2P Trust Model Based on Dual Attribute Values', Computer Engineering, 41(3), pp. 130–135, 2015.
[5] Z. Abrams, R. McGrew, S. Plotkin, 'A non-manipulable trust system based on EigenTrust', ACM SIGecom Exchanges, 5(4), pp. 21–30, 2005.
[6] W. Xue, Y. Liu, K. Li, et al., 'DHTrust: a robust and distributed reputation system for trusted peer-to-peer networks', Concurrency and Computation: Practice & Experience, 24(10), pp. 1037–1051, 2012.
[7] X. Y. Li, X. L. Gui, Q. Mao, et al., 'Adaptive Dynamic Trust Measurement and Prediction Model based on Behaviour Monitoring', Chinese Journal of Computers, 32(4), pp. 664–674, 2009.
[8] Y. Li, H. Guo, W. Peng, et al., 'Trust attribute-based access control policies composition', Application research of Computers, 33(7), pp. 2175–2180, 2016.
[9] J. A. Zhang and X. E. Guo, 'Trust Model based on Dynamic Recommendation in P2P Network', Computer Engineering, 36(1), pp. 174–176+180, 2010.

[10] X. Deng, P. Guan, Z. Wang, et al., 'Integrated Trust Based Resource Cooperation in Edge Computing', Journal of Computer Research and Development, 55(3), pp. 449–477, 2018.
[11] L. Fang, L. Yin, Y. Guo, et al., 'A Survey of Key Technologies in Attribute-Based Access Control Scheme', Chinese Journal of Computers, 40(7), pp. 1680–1698, 2017.
[12] Z. Zhao, B. Tan, S. Xia, et al., 'P2P network comprehensive trust model based on time series', Computer Engineering and Applications, 53(15), pp. 127–131, 2017.
[13] G. Shi, H. Wang, Y. Ci, et al., 'Dynamic and adaptive access control model', Journal on Communications, 37(11), pp. 49–56, 2016.
[14] H. Liu, L. Zhang, Z. Chen, 'Task-based access control mode of peer-to-peer network based on fuzzy theory', Journal on Communications, 38(2), pp. 44–52, 2017.
[15] D. Chen, S. Yang, 'Dynamic trust level based ciphertext access control scheme', Journal of Computer Applications, 37(6), pp. 1587–1592, 2017.
[16] K. Shao, F. Luo, N. X. Mei, et al., 'Normal Distribution based Dynamical Recommendation Trust Model', Journal of Software, 23(12), pp. 3130–3148, 2012.
[17] J. Nie, D. Zhang, 'Research on Resource Trust Access Control Based on Cloud Computing Environment', Communications in Computer and Information Science, 873, pp. 394–404, 2017.
[18] L. T. Huang, S. G. Deng, Y. Li, et al., 'A Trust Evaluation Mechanism for Collaboration of Data-intensive Services in Cloud', Applied Mathematics & Information Sciences, 7(1), pp. 121–129, 2013.
[19] K. Woongsup, 'A Trustworthy Service Computing Framework through a Semantic Messaging Model', Applied Mathematics &Information Sciences, 7(2), pp. 729–739, 2013.
[20] I. Naima, G. Abdul, Z. Uzman, 'A Mechanism for Detecting Dishonest Recommendation in Indirect Trust Computation', EURASIP Journal on Wireless Communications and Networking, pp. 189, 2013.
[21] B. Zhao, J. He, Y. Zhang, et al., 'The Method of Recommended Trust Evaluation Based on Grey Correlation Analysis', Acta Scientiarum Naturalium Universitatis Pekinensis, 53(2), pp. 314–320, 2017.

Biographies

Yu Zhang was born in China in 1978. He is currently a doctoral candidate in the Faculty of Information Technology at Beijing University Of Technology. He received his B.Sc. and M.Sc. degrees in physics from Qufu Normal University, China in 2002 and 2005, respectively. His research interests include neural networks and network security.

Guangmin Sun was born in China in 1960. He received his B.Sc. degree in electronic engineering from Beijing Institute of Technology, China in 1982, his M.Sc. degree in communication and information systems from Nanjing University of Science and Technology, China in 1991, and his Ph.D. degree in communication and information systems from Xidian University, China in 1997. Currently, he is a professor with Beijing University of Technology. His research interests include neural networks, image processing and pattern recognition.

Peng He was born in China in 1965. He received his B.Sc. degree in computer application from Hefei University Of Technology, China in 1986, and his M.Sc. degree in measurement and control from Chinese Academy of Sciences, China in 1989. Currently, he is a professor with China Three Gorges University. His research interests include deep learning and network security.

Peng Zhai was born in China in 1978. He is currently a doctoral candidate in the Faculty of Information Technology at Beijing University Of Technology and an associate professor with Jining University, China. He received his M.Sc. degrees in Shandong University of Science and Technology, China in 2005. His research interests include network security and blockchain.

Yuge Sun was born in China in 1997. He received his B.Sc. degree in electrical and electronic engineering from The University of Manchester, UK in 2018. His research interests include image processing and artificial intelligence.