International Journal of Database Theory and Application
Vol.8, No.1 (2015), pp.235-244
http://dx.doi.org/10.14257/ijdta.2015.8.1.24

Designs and Simulations of Multi-factor in Trust Evaluation

Zhao Bin [1,2], He Jingsha[1,3,*], Huang Na[1], Zhang Yixuan[1], Zhou Shiyi[3] and Ji Jie[2]

[1]*School of Software Engineering, Beijing University of Technology, Beijing 100124, China*
[2]*Department of Computer Science, Jining University, Qufu, Shandong 273155, China*
[3]*Information Technology Department, Beijing Development Area Co., Ltd, Beijing 100176, China*
** jhe@bjut.edu.cn*

Abstract

Trust Model is an efficient way of resolving the trust problems in open networks in which trust evaluation is a key issue to be addressed in trust management. According to the design rules of trust models, the problem of the lack of dynamic adapt ability in trust evaluating, the lack of effective aggregation of trust and the lack of considerations to incentive mechanisms and so on, this paper introduced the bonus-penalty factor which shows how reliable is the direct trust of the recommend entities to the subject and evaluation reliability of the recommend entities which is used to decide whether the access object would adopt the recommendation of the recommend entities during the calculation of the recommend trust. The measurement of integrated trust solves the weight problem between direct trust and recommendatory trust by introducing balanced weight factor. Finally, we present designs of bonus-penalty function and balanced weight factor and simulations by Matlab software.

Keywords: *Trust Evaluation; Bonus-penalty Factor; Evaluation Reliability; Balanced Weight; Simulation*

1. Introduction

As the development of communication and network technologies makes current and future networks become more open, trust has been playing an increasingly more important role in access control in such networks. In network interactions of various kinds, results from trust evaluation can more realistically reflect the degree of multi-domain heterogeneity, high level of dynamics and uncertainty of open networks. Trust has thus become a key technology for secure and effective access control in open networks [1-2].

In open network environment, no a central authority being trusted, not getting all information about requestors, the outcome of granting requestors may be harmful, then results in trustworthiness and uncertainty or risk. And facing with characteristics of heterogeneous and dynamic in open network-oriented information, resources or services access security needs, introducing trust into open and dynamic network access control, studding key technologies in access control model based on dynamic trust [3], are important for the warranty information, resources or services requesters and providers to achieve the expected benefits, visit the act itself dynamic response and risk, discretionary access behavior to solve the security implications of great significance.

* Corresponding Author

ISSN: 2005-4270 IJDTA

Trust Model is an efficient way of resolving the trust problems in open networks in which trust evaluation is a key issue to be addressed in trust management. According to the design rules of trust models, the problem of the lack of dynamic adapt ability in trust evaluating, the lack of effective aggregation of trust and the lack of considerations to incentive mechanisms and so on, this paper introduced the bonus-penalty factor which shows how reliable is the direct trust of the recommend entities to the subject and evaluation reliability of the recommend entities which is used to decide whether the access object would adopt the recommendation of the recommend entities during the calculation of the recommend trust. The measurement of integrated trust solves the weight problem between direct trust and recommendatory trust by introducing balanced weight factor. Finally, we present designs of bonus-penalty function and balanced weight factor and simulations by Matlab software.

2. Design Principle of Classic Trust Model

According to design principle of classic trust model, we present trust principle of trust model from the following six aspects:

Accuracy

This requires that trust-based methods be able to distinguish between honest access and hostile access accurately and reliably so that access control can make the right decision and is also able to respond to dynamic changes in the network. An integrated trust value can be calculated through the combination of direct trust and recommendation trust to guarantee the accuracy and fault-tolerance of the result so that evaluation made by access control and measurement from the trust model would match with each other.

Self-adaption

This means that a trust method should consider the dynamic nature of networks, choose the best strategy for evaluation, analysis and calculation based on network conditions, automatically adjust calculation parameters, methods and restrictions to make the measurement of trust and the expectation of evaluation consistent with each other. Since there could be many spatial and temporal factors that would change along with time in open networks and the number of interactive entities could be different at different times, information, services and resources that can be provided by the networks could also change at all times. Moreover, any change in the number of network entities could also impact trust evaluation. Thus, the dynamic characteristics of open networks must be considered.

Dynamic

Since the number of interactive entities in open networks changes dynamically, the evaluation of trust is a very dynamic process that could involve complicated computations based on multiple factors. In the interactive process of open networks, entities exchange information all the time, making the measurement of trust very dynamic as the result of the occurrence of interactive actions and the change of trust relationships. Moreover, interactions inside the networks are very complicated, which requires that trust models be dynamic.

Robustness

The open and dynamic characteristics of open networks could bring danger to users while offering convenience. Hostile entities in open networks are expected to make hostile access or recommendation. Therefore, the trust value of an entity should not be determined only by some fixed set of entities, but by all relevant entities in the same network to resist hostile

actions. A trust model must be robust and the calculation of the trust value has to consider multiple factors so that attacks from hostile entities can be tolerated. Robustness has become very important in the evaluation of trust evaluation models.

Universality

This is also called extendibility, which means the ability of the trust model to adapt to the expansion of open networks. Since open networks could become larger as time goes by to involve more entities and the relationships between entities could become more sophisticated, there is a need for more storage space, higher communication cost and more calculation to maintain trust relationships. Universality of trust models mainly faces the issues of variable network entities, bandwidth efficiency, load balancing, routing topology and the burden and storage of the calculation results to maintain low cost.

Encouragement

Trust models should provide appropriate bonus-penalty mechanisms to encourage network entities to provide honest services and to punish the hostile access. The purpose is to make network entities get what they need while realizing the long-term goal of the networks, *i.e.*, to decrease hostile actions and increase honest actions to improve the security of the networks.

Encouragement means trust model provides appropriate bonus-penalty mechanism by taking some strategies to make network nodes provide honest service, *e.g.*, making just evaluation and recommendation about interactive nodes, and to impel them access honestly and punish the fraudulent access. The fundamental purpose of the encouragement principle is to correctly lead network nodes to get its own need while realizing histrionic goal, increase the satisfy to the network while decreasing hostile actions, and increase honest actions to make the network harmonious.

3. Related Works

Blaze *et al.*, first introduced the concept "Trust Management" [4] in 1996, Afterwards, trust was introduced into open networks and a lot of work has been conducted on trust management in open networks [5-11].

Based on the trust model of social relationship network, the weight factor **Error! Reference source not found.** is introduced into the EigenTrust model [5], and through the distributed calculation method based on DHT, the global trust value of each entity node is quantized using iteration. As a trust model using social network, the EigenTrust model considering the influence on trust computing by the behavior of malicious entity, but it ignored bonus-penalty and security of network interaction entities. The PowerTrust model [6] is improved in the decision of the set of trustable nodes and the convergence speed of trust iteration. It dynamically selects small number of power nodes that are most reputable using a distributed ranking mechanism. The Regret [7], a model of reputation based on fuzzy logical reasoning, and this kind of trust models uses the fuzzy in language to represent trust, the trust level which nodes belong to is expressed with fuzzy function. The work in [8] presents a new fuzzy-logic approach to aggregating peer reputation using public-domain trace data. According to the inner security issue of Peer-to Peer networks, the work in [9] presents a trust model based on direct transaction and recommendation in P2P network. Parameters of direct transaction information, rating confidence degree of recommendation information and dynamic balance weight were applied in the model. The model described peer's integration trust simply and accurately. The work in [10] presents a trust evaluation model based on dynamic Bayesian network associating with time factor. Based on interpersonal trust model in

sociology, the trusted relationship between network nodes was researched [10]. The work in [11] presents a dynamic access control model based on scenario trust, applying fuzzy cluster algorithms and information entropy theory, an allocation algorithm of each factors' balanced weight was designed, to achieve objective quantization of scenario trust.

In Section 4.1 and 4.2, we only introduce the concepts of bonus-penalty factor and the reliability of evaluation of the recommending entities without involving recommendation trust evaluation model. We perform some experiment by choosing different values for the bonus-penalty factor to evaluate the effectiveness in Section 5.1. When two entities engage in an interaction for the first time, due to the lack of direct interaction experience, the evaluation of global trust depends more on the recommendation trust from by third parties. As the number of interactions grows, direct trust accumulates and will become more important while the importance of recommendation trust goes down. In Section 4.3, we introduce the notion of the balanced weight in global trust evaluation which is used to express the relative weight of the direct trust vs. the recommendation trust. We also perform some experiment to evaluate balanced weight in global trust evaluation and analyze the results in Section 5.2.

4. Multi-factors in Trust Evaluation

4.1. The Bonus-Penalty Factor

Bonus-penalty factor: It expresses how reliable the recommending entities are during the calculation of the recommendation trust, i.e., the level of acceptance of the recommendation trust by the object.

The bonus-penalty factor shows how reliable the trust from the recommending entities is to the object during the calculation of the recommendation trust. The bonus-penalty factor would be used to reward honest access and punish hostile access. In network interactions, if the trust levels of the feedback reliability X include **Error! Reference source not found.**, which means total distrust, critical trust, total trust, the space of trust levels is L, **Error! Reference source not found.**, **Error! Reference source not found.** and **Error! Reference source not found.**, the bonus-penalty function f(x) can be expressed as follows:

Error! Reference source not found.,

where the values of **Error! Reference source not found.** change dynamically as the application environment changes.

4.2. Evaluation of Reliability

Reliability of evaluation of the recommending entity: during the calculation of the recommendation trust, the reliability of the recommending entities must be considered.

During the calculation of recommendation trust, the reliability of evaluation of the recommending entities could be used to determine whether object O should accept the recommendation from the recommending entities. The object gains the evaluation reliability of the recommending entities by considering the recommendation trust of the recommending entities. Then, object O gets the trust evaluation on subject S through the set of entities E. Object O would judge the trust evaluation on subject S performed by E and the result is reflected through a weight.

If all the entities in set **Error! Reference source not found.** have performed evaluation on the subject, then the value of **Error! Reference source not found.** is the number of elements in set **Error! Reference source not found.**. Each and every recommending entity would have an honest factor called c whose value is the ratio of the number of satisfied

recommendations to total recommendations, that is, the probability of success is P. The initial value of P can be 0.5, namely, the honest factor of recommendations is 0.5 by default when the first recommendation comes.

The calculation model of the reliability of evaluation of the set **Error! Reference source not found.** of entities given by object O is:

Error! Reference source not found.

where the initial value of **Error! Reference source not found.** is 0.5 and the number of elements in set **Error! Reference source not found.** is 0.

In the calculation of trust from recommending entities in open networks, reliability of evaluation is the basis for the calculation of global recommendation trust. The object considers the influence of reliability of evaluation on the subject given by recommending entities so that it can resist access from hostile entities.

4.3. The balanced Weight

The balanced weight: it balances the weight of direct trust and recommendatory trust in the calculation of global trust.

The balanced weight shows the degree of confidence of the access object nodes, and its value changes from 0 to 1. The value of balanced weight **Error! Reference source not found.** depends on the acceptance to the access subject in direct trust and recommendatory trust.

The calculation model of the balanced weight is as below:

$$\varphi = \frac{1}{2} + \frac{1}{\pi}\arctan\left(10 \times \frac{k-\mathrm{int}(N)}{N}\right),$$

Where K represents the interactive times between the subject and the object, and N is the number of access which changes dynamically according to the demand of system safety and interactive network.

5. Simulation Experiment

Our experiment environment is set as follows: the hardware is a Lenovo PC(CPU i3-3240@3.4GHZ, DDR3 4GB, operating system Windows 7), and the Matlab(R2009b)7.9.0 is used to analyze the result.

5.1. The Choice of Bonus-penalty

In the process of evaluating the recommendation trust, the value of the bonus-penalty factor represents the acceptance degree of trust from the recommending entities. In open networks, the value of **Error! Reference source not found.** would change dynamically in response to application environments. With the space for the trust values being **Error! Reference source not found.**, the reflection function between feedback reliability and bonus-penalty is shown in Figure 1-a while Figures 1-b, 1-c and 1-d display the results for **Error! Reference source not found.**, **Error! Reference source not found.** and **Error! Reference source not found.**, respectively.

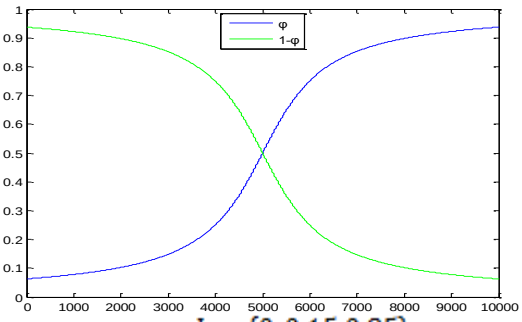

Figure 1-a. $L = \{0, 0.15, 0.85\}$

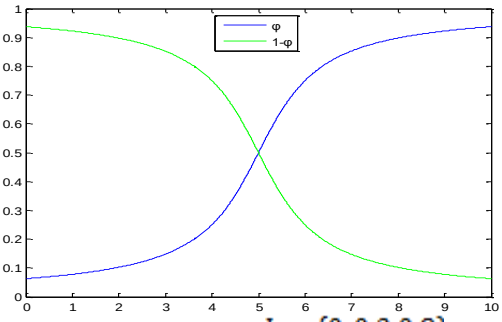

Figure 1-b. $L = \{0, 0.2, 0.8\}$

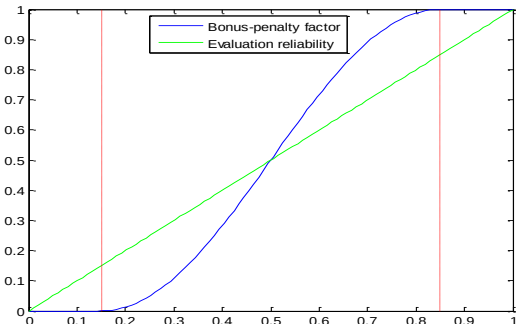

Figure 1-c. $L = \{0, 0.1, 0.9\}$

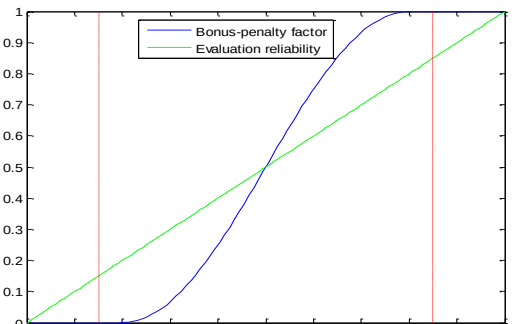

Figure 1-d. $L = \{0, 0.05, 0.95\}$

Figure 1. Reflection Relationship between Feedback Reliability and Bonus-Penalty

We can see from Figure 1 that the bonus-penalty factor changes dynamically as the space of trust values changes, which is determined by the network environments. That is, bonus-penalty would differ in different network environments. When the feedback reliability is higher than 0.5, the bonus-penalty shows a good effect and the degree of adoption would improve as the interaction between entities continues. When the feedback reliability is lower than 0.5, the bonus-penalty shows a less favorable effect and the degree of reward and punishment would decrease by a large margin. When bonus-penalty becomes 0, hostile entities can be recognized and recommendations from hostile entities are resisted so that the reliability of recommendation trust can be reached.

5.2. The Choice of Balanced Weight

The value of balanced weight and the change of interaction number are shown in figure 2. As it says, the bigger the k and **Error! Reference source not found.** are, the bigger proportion the direct trust evaluation of the access subject has, and the other recommendatory trust of recommendatory entities has a lower proportion, while **Error! Reference source not found.** increases with the amplification of interactions between the subject and the object. In Figure 2-a, the N is 10, in Figure 2-b, the N is 100, in Figure 2-c, the N is 100, and in Figure 2-d, the N is 10000.

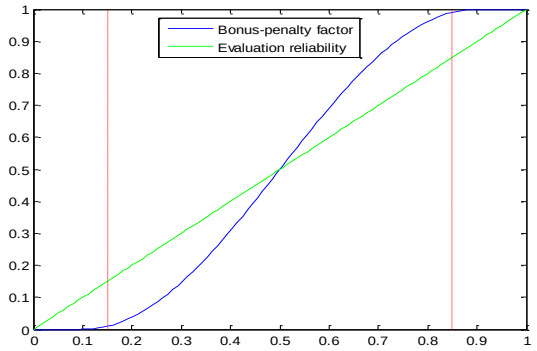

Figure 2-a. N=10

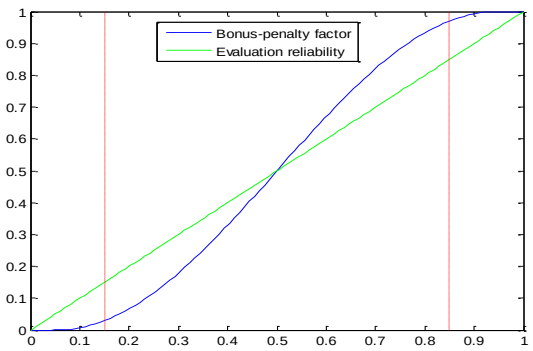

Figure 2-b. N=100

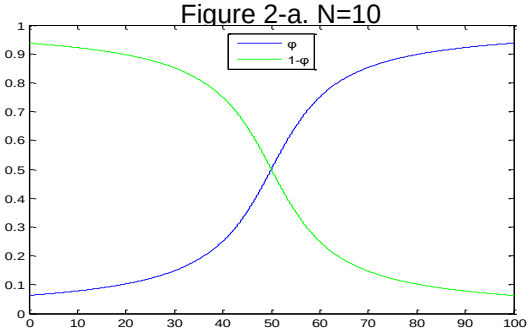

Figure 2-c. N=1000

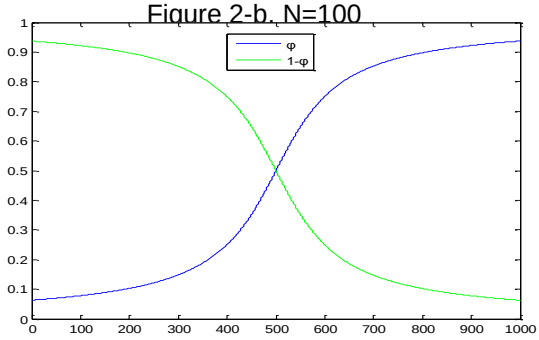

Figure 2-d. N=10000

Figure 2. Balanced Weight Changes as the Number of Interactions Increases

The balanced weight shows the degree of confidence of the object, during the interaction between the object and the subject, since the known information is not enough, the direct experience is short, and it tends to depend on recommendatory trust, so the initial value of **Error! Reference source not found.** is small, but with the number of interactions between the subject and the object increasing, the object prefers to believe its own direct interactive historical experience. So **Error! Reference source not found.** changes dynamically with the change of interactions.

6. Conclusions

In this paper, we introduced the bonus-penalty factor which shows how reliable is the direct trust of the recommend entities to the subject and evaluation reliability of the recommend entities which is used to decide whether the access object would adopt the recommendation of the recommend entities during the calculation of the recommend trust. The measurement of integrated trust solves the weight problem between direct trust and recommendatory trust by introducing balanced weight factor. Finally, we present designs of bonus-penalty function and balanced weight factor and simulations by Matlab software.

Focusing on the problem that current recommend trust relationship is too complex, our next work is to simplify it and improve the accuracy and convergence of trust evaluation and quantization.

Acknowledgements

The work in this paper has been supported by National Natural Science Foundation of China (61272500), Beijing National Science Foundation (4142008), Shandong National Science Foundation (ZR2013FQ024) and Pre-launch of Beijing City Government Major Tasks and District Government Emergency Projects (Z131100005613030).

References

[1] J. Griffin, T. Jaeger and R. Perez, "Trusted Virtual Domains: Toward Secure Distributed Services", Proceedings of 1st Workshop on Hot Topics in Systems Dependability, Yokohama, Japan,June **(2005)**, pp. 1-6.
[2] F. Feng, C. Lin, D. Peng and J. Li, "A Trust and Context Based Access Control Model for Distributed Systems", Proceedings of 2008 10th IEEE International Conference on High Performance Computing and Communications, Washington, DC, USA, Sept, **(2008)**, pp. 629-634.
[3] G. Han, J. Jiang, L. Shu, J. Niu, and H. C. Chao, "Management and applications of trust in Wireless Sensor Networks: A survey", Journal of computer and system sciences, vol. 80, no. 3, **(2014)**, pp. 602-617.
[4] M. Blaze, J. Feigenbaum and J. Lacy, "Decentralized Trust Management". Proceedings of 17th Symposium on Security and Privacy, Oakland, CA, USA, **(1996)**, pp. 164-173.
[5] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The EigenTrust algorithm for reputation management in P2P networks", Proceedings of the 12th International World Wide Web Conference, Budapest, Hungary, **(2003)**, pp. 640-651.
[6] R. F. Zhou, and K. Hwang, "PowerTrust: A Robust and Scalable Reputation System for Trusted Peer to Peer Computing", IEEE Transactions on parallel and distributed systems, vol. 18, no. 4, pp. 460-473.
[7] J. Sabater, and C. Sierra, "REGRET: A reputation model for gregarious societies", Proceedings of the 4 th International Workshop on Deception, Fraud and Trust in Agent Societies, Bologna, Italy, **(2001)**, pp. 61-69.
[8] S. Song, R. Zhou, K. Hwang,and Y. Kwok, "Trusted P2P transactions with fuzzy reputation aggregation". IEEE Internet Computing, vol. 9, no. 6, **(2005)**, pp. 24-34.
[9] S. Chen, "Trust model based on weight factor in P2P network". Journal of computer Applications, vol. 33, no. 6, **(2013)**, pp. 1612-1614.
[10] H. Liang, W. Wu, "Research of trust evaluation model based on dynamic Bayesian network", Journal on communications, vol. 34, no. 9, **(2013)**, pp. 69-76.
[11] S. Ma, J. He and X. Shuai, "An Access Control Method based on Scenario Trust", International Journal of Computational Intelligence Systems, vol. 5, no. 5, **(2012)**, pp. 942-952.

Authors

Zhao Bin is currently a Ph.D. student in the School of Software Engineering at Beijing University of Technology in China. His research focuses on network security, cloud computing and information forensics and he has published several papers in scholarly journals and international conferences in the above research areas.

He Jingsha received his B.S. degree from Xi'an Jiaotong University in Xi'an, China and his M.S. and Ph.D. degrees from the University of Maryland at College Park in USA. He is currently a professor in the School of Software Engineering at Beijing University of Technology in China. Professor He has published over 170 research papers in scholarly journals and international conferences and has received nearly 30 patents in the United States and in China. His main research interests include information security, network measurement, and wireless ad hoc, mesh and sensor network security.

Zhang Yixuan is a Ph.D candidate in the College of Software Engineering at Beijing University of Technology, Beijing, China. She received her B.S. degree in Beijing University of Technology in 2011. Her research interests include network security, access control, game theory and distributed network technology.