Scholar Publishing Group
Distributed Processing System
https://doi.org/10.38007/DPS.2020.010305
ISSN 2790-0916 Vol. 1, Issue 3: 37-45

Open Distributed System Based on Trust Relationship Model

Logeshi Sainin[*]

Philippine Christian University Center for International Education, Philippines

[*]*corresponding author*

Keywords: Trust Relationship Model, Open, Distributed System, System Analysis

Abstract: With the rapid development of network technology and the continuous improvement of information resources, the network equipment mode has developed rapidly from centralized to distributed. In the distributed network environment, the security information is insufficient and uncertain: the nodes in the distributed network do not know each other's identities, resulting in the inability to obtain security related information in many cases. Therefore, this paper proposes a trust relationship(TR) model, analyzes the open distributed system(ODS), discusses the calculation method of trust degree, evaluates the validity and correctness of the model in terms of time correlation and consistency through simulation experiments, and evaluates the robustness of the model against common trust system attack methods through a group of experiments. The experimental results verify the effectiveness of the TR model.

1. Introduction

The dynamic, heterogeneous and widely distributed characteristics of the distributed system make the management of things in the distributed environment no longer centralized, closed and controllable, thus increasing the security threat of the distributed system. Traditional network security systems pay attention to privacy and information security, and implement security strategies through identity authentication, password technology, authorization, access control and other technologies to improve system security. However, there is no guarantee that the companies joining the network are real entities and the security requirements of the shared system.

With the continuous expansion of network scale, many computing modes based on large-scale distributed network environment, such as distributed computing, pervasive computing, grid computing and cloud computing, have been widely studied and applied. The amount of information processed in the network is more huge, the type of information is more complex, sharing and collaboration are more common, information is more changeable in its life cycle, and the access rights of resources are diversified and personalized, The user relationship has become complex, which brings severe challenges to authorization management [1]. In view of the new characteristics and new security requirements of the open network environment, this paper analyzes the ODS based on the TR model. The main feature of the system is that it combines the security credentials with subjective trust concepts such as experience and recommendation, evaluates the trust in all aspects, realizes fine-grained authorization and access control based on the trust evaluation results, and dynamically manages user attributes and user permissions [2].

Some typical trust management models put forward in recent years use continuous value method to express the degree of trust. In order to accurately express the dynamic change of trust, this paper chooses continuous value method to express the degree of trust. Firstly, this paper gives a comprehensive introduction to ODS and TR, and points out the shortcomings of TR establishment and TR management; The ODS based on trust relation model is analyzed; The effectiveness and correctness of the model in terms of time correlation and consistency were evaluated through simulation experiments, and good results were achieved [3-4].

2. Analysis of ODS based on TR Model

2.1. ODS

Distributed network has unique advantages in comprehensive performance, distributed computing and resource sharing, large-scale parallel computing, network application model and so on.

Analysis of trust problem in distributed file system: Generally speaking, according to the implemented functions, the protocol of P2P network is divided into several layers, and each layer performs relatively independent functions. At present, different researchers differ in the specific details of the division. P2P network can be basically divided into four layers, which are network connection layer, P2P intermediate layer, P2P service layer and P2P application layer from bottom to top [5-6]. As shown in the following table:

Table 1. P2P network architecture

P2P application layer (tools applications services etc.)
P2P Service layer (security reliability resource aggregation
P2P middle layer (discovery locating routing etc.)
Network connection layer (TCP/CP Bluetooth WLAN etc.)

2.2. TR

Trust is a complex concept. The research on trust mainly includes the establishment and management of trust relations. Trust is an important relationship between entities and is the premise for entities to communicate with each other. The proposal of trust puts forward new ideas for solving security problems in large-scale network environment. Trust based security mechanism is gradually considered as an effective method to solve security problems in open network environment [7-8]. However, the existing research still has some shortcomings in the definition of trust, the dynamic description of trust, the description of trust management and the evaluation of trust:

Formal definition of trust. At present, there is no unified standard for the definition of trust, and the definition of trust is not formalized, and it is mostly described in natural language. For example, "when subject a assumes that subject B will act exactly as it expects, it is said that a trusts B". There are some fundamental problems with such a definition. Because natural language is rich in meaning and everyone's understanding of natural language is not necessarily the same, all of them often lead to inconsistent understanding of trust [9].

Dynamic characterization of trust. In the open network environment, the trust policy of each system changes frequently, resulting in frequent changes in the TR of each entity. At different times, the TR between each entity is often different. In practical applications, due to the establishment and revocation of trust relations, the formulation and change of trust policies and other events, the trust relations between entities often change at any time and on demand, and the description of trust should also change with time and demand. Therefore, the description of trust must be dynamic [10].

Evaluation of trust. At present, the research on trust evaluation mainly focuses on the evaluation of objective trust, that is, the establishment of trust relations through the analysis and judgment of certificates, without considering the comprehensive evaluation of objective trust and subjective trust. In the open network environment, subjective trust can not be ignored for the establishment of trust relations. Only by combining objective trust and subjective trust can we make a reasonable Comprehensive and more reliable assessment [11-12].

2.3. Analysis of ODS based on TR Model

The trust between entities can be quantitatively analyzed, so the TR between entities can be associated with a metric value. Trust can be measured in a way similar to some information or knowledge, and the degree of trust is the quantitative expression of this degree of trust. The trust degree is used to measure the size of the TR [13-14].

Binary value method: in this expression method, two values of 0 and 1 are used to express trust. That is, the trust object or the trust object is expressed by 1; Or the untrusted is represented by 0. This representation is common in objective trust management models. This expression method is simple and direct, and can also be conveniently used in the automated trust management system. However, this method is too extreme for the measurement of trust and cannot express the dynamic and subjective nature of trust relations [15].

Continuous value method continuous value method defines the quantitative measurement space of trust degree as a continuous quantity within a certain range. For example, the trust degree is distributed in the interval [0,1] or [- 1,1]. This expression method has a fine granularity and can accurately reflect the dynamic change process of trust [65], so it has been widely used in recent years [16]. In this paper, the trust space is a real number in the range of [0,1]. That is, a trust degree of 0 indicates that the trust degree of the trust object is the lowest and completely untrusted; A trust degree of 1 indicates that the trust object has the highest degree of trust and is completely credible; A trust degree of 0.5 indicates that there is no confidence in the trust degree of the trust object, and this value is also used as the initialization of the trust degree. If two entities first contact each other, the trust degree of each other is set to 0.5. Of course, the above three expression methods are not completely isolated, and the other two expression methods of trust space can also be conveniently mapped to the trust space expression method selected in this paper [17].

After selecting the above expression method of trust degree, the trust evaluation value deduced in this model is actually the expected probability of whether the trust subject will act according to his own expectation of the future. That is, when the trust degree is 1, the trust subject thinks that the trust object will take actions according to its own expectations. And a trust degree of 0 indicates that the trust subject believes that the trust object will not act according to its own expectations [18]. A trust degree of 0.5 indicates that the trust subject has no confidence in the future behavior of the trust object. According to the trust degree set by this continuous value method, the trust degree can be easily applied to the decision-making behavior of the trust subject.

3. Calculation of Trust

The main task of the trust model is to calculate and obtain the trust evaluation value. Considering that in an open distributed environment, it is difficult for an entity to interact directly with all other entities, or even do not know other entities at all. Therefore, according to the previous definition, our trust model uses two trust information sources to calculate the trust evaluation value: historical interaction knowledge (direct trust) and recommendation information (indirect trust).

When entity a needs to evaluate the trust of entity B, a will first find out the direct trust information of entity B in its own history. Direct trust comes from past direct interaction experience. If an entity has a history of interaction with another entity, the trust degree of another entity can be judged according to the results of these interactions. This forms direct trust. If there is no direct interaction between two entities in history, in our model, the direct trust is set to the default value of 0.5. As explained in the previous section on measurement methods of dynamic trust relations, a trust degree of 1 indicates that the trust object will act according to our expectations, while a trust degree of 0 indicates that the trust object will not act according to our expectations, and a trust degree of 0.5 indicates that there is no confidence in the future behavior of the trust object, that is, there is no TR with the trust object.

The calculation of the trust degree in the trust model must comprehensively consider the characteristics of two dynamic trust relations: trust should be difficult to obtain, but easy to lose; The past interaction experience should be time related, that is, the later the behavior occurs, the greater the impact on trust. According to the above thought, we introduce forgetting factor into the construction of trust model β, Its definition is shown in formula (1):

$$\eta = \begin{cases} \dfrac{s^{\Delta t_{\max}} - s^{t-t'}}{s^{\Delta t_{\max}-1}} & when t - t' \le \Delta t_{\max} \\ 0 & whenelse. \end{cases} \tag{1}$$

Here, T represents the present time, and t 'represents the time when the past behavior occurred. Δ Tmax is a definable parameter, which is used to indicate the allowable time window size, that is, after how long, the past experience is considered to be completely worthless. In this way, when the time of historical interaction is outside the allowable time window length, the forgetting factor η Is 0, i.e. past experience is worthless. And the closer t 'is to the current time t, η The closer the value is to 1, the more valuable the past experience is.

Using the direct trust, indirect trust and forgetting factor, the time-dependent trust calculation process is defined as follows: the trust evaluation of trust subject a to trust object B at time t is:

$$T^{t}(A,B) = \eta \times DT^{t'}(A,B) + (1-\eta) \times IT^{t}(A,B) \tag{2}$$

That is, at a certain time t, when the trust subject a needs to interact with the trust object B, the trust subject a will evaluate the trust degree of the trust object B at the current time in real time, instead of directly using the historical trust degree evaluation value. This real-time trust evaluation process consists of two parts: the trust evaluation value recorded in the history is used as the direct trust degree, which represents the direct interaction experience in the past; The recommendation information from other recommendation entities obtained in real time is synthesized into an indirect trust degree for use. At the same time, the forgetting factor is used as a configurable parameter to determine the weight of the direct trust. When the experience is too long, η 0, the model can only rely on the indirect trust degree of the recommendation information to evaluate the trust object. And the experience occurrence time is the current time, η 1 indicates that the current trust evaluation value is directly used to evaluate the trust object, and there is no need to collect the recommendation information again.

4. Simulation Experiment and Data Analysis

In order to evaluate the effectiveness of the TR model proposed in this paper and its adaptability to the characteristics of the ODS environment, this paper uses the evaluation method of experimental simulation. The interaction between nodes in P2P network is simulated by Java program. A group of nodes are set up in the simulation environment to interact with each other. By specifying one node as the trust subject and the other node as the trust object, the performance of the trust model proposed in this paper is tested by observing the changes of the trust subject's trust degree caused by different behaviors of the trust object. This proves the validity of the trust model and verifies that the model can meet the characteristics of the trust model in large-scale distributed computing environment.

First, our model is distributed for trust evaluation, and all trust evaluation processes are completed independently in the entity. Even for the same trust object at the same time, completely inconsistent trust evaluation results will be caused by the experience of the trust subject and the recommendation information of different recommendation entities. Then, two groups of experiments will be conducted to evaluate the validity and correctness of the model in terms of time correlation and consistency, and one group of experiments will be conducted to evaluate the robustness of the model in the face of common trust system attack methods.

4.1. Time Correlation Experiment

For example, the description of time dependence in the characteristics of trust model, the model must express the time dependence of TR, that is, the TR should change with the passage of time; The influence of the factors influencing the TR on the TR will also change with the passage of time. In Experiment 1, we mainly designed the model for the time correlation, that is, we mainly investigated the influence of forgetting factors introduced in the model on trust evaluation.

Experiment 1 is divided into two parts. First, the relationship between the trust evaluation value of the trust object and time is investigated in the case that other factors have not changed. In our model, the trust evaluation value is composed of the historical experience recorded in the trust subject and the recommendation information from other recommendation entities at the current time. We assume that the trust evaluation value of the trust object is 1 at the time t = 0. At time t ', a new trust evaluation value will be synthesized according to the trust evaluation value at time t and the current recommendation information from other recommendation entities. Assuming that the recommendation information is the same, the synthesized indirect trust evaluation value is 0.6. Investigate the relationship between Δ Tmax and trust evaluation value at different times. The test results are shown in Table 2 and figure 1.

Table 2. Data table of trust over time

	0	1	2	3	4	5	6	7	8	9	10
Δt_{max}=4	1	0.97	0.94	0.85	0.6	0.6	0.6	0.6	0.6	0.6	0.6
Δt_{max}=6	1	0.99	0.98	0.96	0.92	0.83	0.6	0.6	0.6	0.6	0.6
Δt_{max}=10	1	0.99	0.99	0.98	0.97	0.98	0.97	0.97	0.95	0.88	0.6

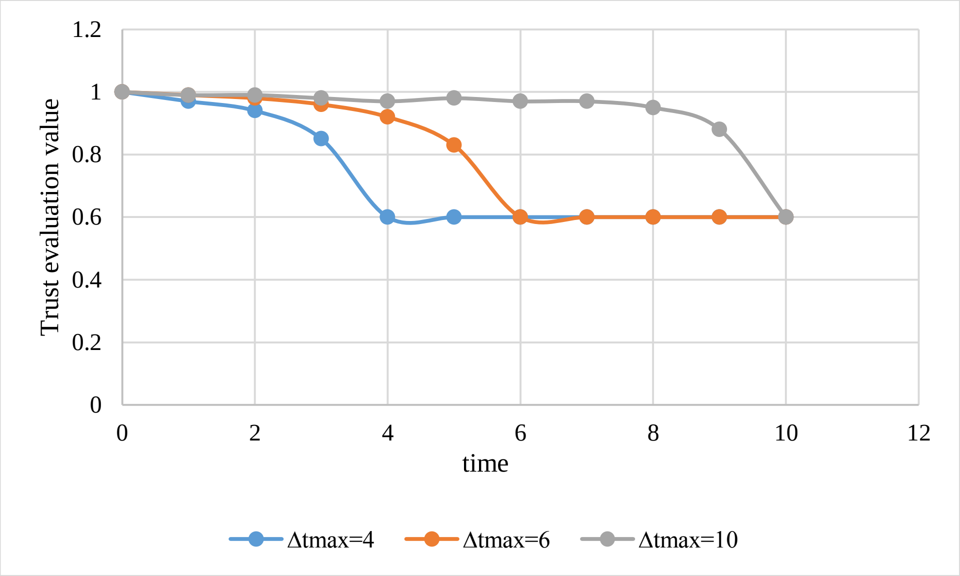

Figure 1. Change of trust over time

The above experimental data show the experimental results. The experimental results show that our model has good time correlation. The influence of past experience will gradually weaken with the passage of time and eventually disappear. Within the time window Δ Tmax, the impact of past experience initially decreases slowly, and then decreases rapidly when it approaches the size of the time window. Finally, once it exceeds the allowable range of the time window, the trust subject will completely rely on indirect trust to calculate the trust evaluation value.

The second part of Experiment 1 is to investigate the impact of the time difference between the past historical experience and the current behavior when updating the entity's trust evaluation value according to the entity's behavior results. When updating the trust evaluation value of the trust object according to the behavior result of the trust object, the model in this paper also uses the forgetting factor, so the change relationship between the trust evaluation value and the update time is consistent with the situation shown in Fig. 1.

4.2. Consistency Test

In the experiment, we mainly investigate how the behavior value of the trust object changes with the behavior of the trust object. For simplicity and generality, we ignored the influence of forgetting factor in this experiment and assumed forgetting factor at every moment η= 0.25, and the history window H = 4. We set three behavior modes of entities:

Consistent good model: we simulate the process of an entity improving its own trust evaluation value by adhering to consistent positive behavior; Consistent poor model: we simulated the process in which the entity's behavior is negative and thus loses its reputation; Behavior shock mode: we simulate the process of trust shock attack by the entity alternately implementing positive and negative behaviors. The changes of trust under different behavior modes are shown in Table 3 and Figure 2.

Table 3. Trust degree change data table

	0	1	2	3	4	5	6	7	8	9	10
Through	0.5	0.68	0.72	0.77	0.76	0.79	0.81	0.82	0.83	0.84	0.84
Penetration difference	1	0.61	0.49	0.42	0.40	0.38	0.35	0.29	0.26	0.25	0.22
Behavior shock	1	0.5	0.8	0.42	0.68	0.41	0.61	0.40	0.59	0.38	0.51

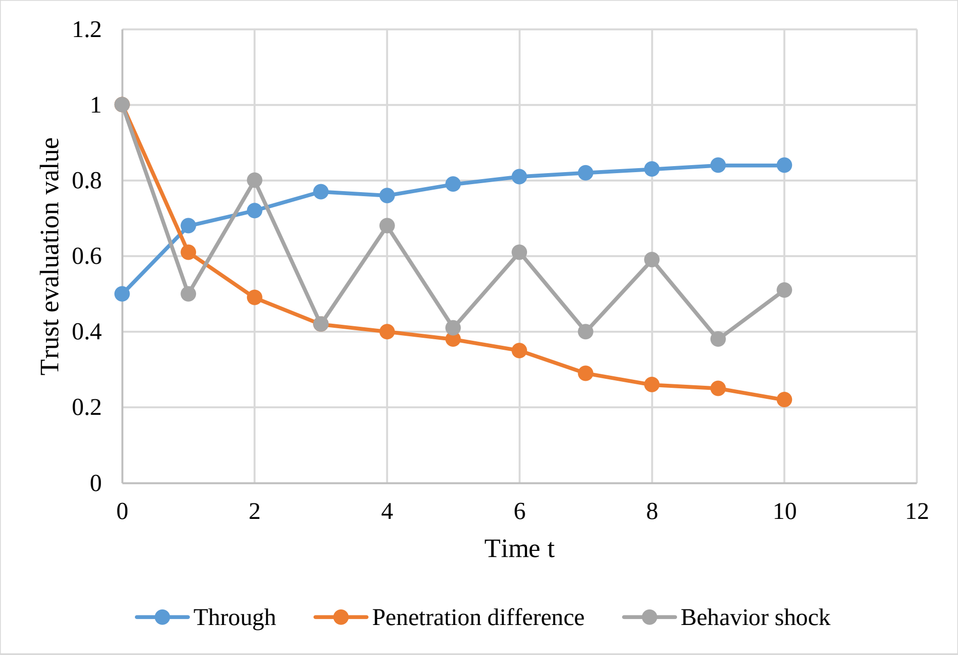

Figure 2. Changes in trust under different behavior patterns

The experimental results show that our model better reflects the consistency of trust. Entities can gradually improve their trust evaluation value by adhering to positive behaviors. And the negative behavior will make the trust evaluation value of the entity decrease rapidly. Our model can also correctly handle this kind of attack when confronting the shock attack behavior with strategic behavior change, so that the trust evaluation value of the attacker tends to decrease as a whole with the shock behavior, and ultimately destroys his reputation.

The experimental results also show that our model can quickly detect the negative behavior of the entity, and the trust evaluation value will drop below the default value after two negative behaviors. At the same time, as there is a malicious behavior threshold in the model, when the negative behavior of the entity is lower than the preset parameter, the system will directly set the trust evaluation value of the entity to 0. This can quickly respond to malicious attacks and other behaviors.

5. Conclusion

This paper analyzes the ODS based on the TR model, and puts forward the trust model and authorization strategy of the resource entity of the distributed decision support system. However, because the TR management mechanism is very complex, the research in this paper is only a beginning, and there are some problems. The next step needs to further study the TR, especially the expression and measurement of trust, and the related characteristics of TR, This is very important for modeling TRs. At the same time, we need to further enhance the security of the trust model, and improve the anti attack ability of the trust model through the design of new trust evaluation algorithms and the application of existing security means. Therefore, in the future work, we should also devote ourselves to the research of ODS combined with relationship.

Funding

This article is not supported by any foundation.

Data Availability

Data sharing is not applicable to this article as no new data were created or analysed in this study.

Conflict of Interest

The author states that this article has no conflict of interest.

References

[1] Yusuke, SATO, Satoshi, et al. Proposal of Sustainable Relief Goods Supply System for Large Scale Disaster -Autonomous Distributed System Based on the Response Threshold Model for Ant Colonies–. Journal of Japan Society for Fuzzy Theory and Intelligent Informatics, 2019, 31(1):586-591.

[2] Yang X, Zhang L, Xie W, et al. Sequential and Iterative Distributed Model Predictive Control of Multi-Motor Driving Cutterhead System for TBM. IEEE Access, 2019, PP(99):1-1.

[3] Kaaria S K, Njuguna R. Organizational Attributes and Implementation of Enterprise Resource Planning: A Case of Kenya Medical Research Institute, Kilifi County. International Journal of Current Aspects, 2019, 3(II):231-242.

[4] Turner K M, Nelson C A, Pestka D L, et al. Identification of critical factors for forming collaborative relationships between physicians and pharmacists. American journal of health-system pharmacy: AJHP: official journal of the American Society of Health-System Pharmacists, 2019, 76(16):1238-1247.

[5] Asim Y, Malik A K, Raza B, et al. A trust model for analysis of trust, influence and their relationship in social network communities. Telematics & Informatics, 2019, 36(MAR.):94-116.

[6] Li R, Wan Y. Analysis of the Negative Relationship between Blockchain Application and Corporate Performance. Mobile Information Systems, 2020, 2020(7):1-18.

[7] Barhoun R, Ed-Daibouni M, Namir A. An Extended Attribute-Based Access Control (ABAC) Model for Distributed Collaborative Healthcare System. International Journal of Service Science, Management, Engineering, and Technology, 2019, 10(4):81-94.

[8] Jahn U, Wolff C, Schulz P. Concepts of a Modular System Architecture for Distributed Robotic Systems. Computers, 2019, 8(1):25-25.

[9] Carvallo J P, Taneja J, Callaway D, et al. Distributed Resources Shift Paradigms on Power System Design, Planning, and Operation: An Application of the GAP Model. Proceedings of the IEEE, 2019, PP(99):1-17.

[10] Garcia-Torres, Felix, Bordons, et al. Optimal Economic Schedule for a Network of Microgrids With Hybrid Energy Storage System Using Distributed Model Predictive Control. IEEE Transactions on Industrial Electronics, 2019, 66(3):1919-1929.

[11] Kruesi L, Burstein F, Tanner K. A knowledge management system framework for an open biomedical repository: communities, collaboration and corroboration. Journal of Knowledge Management, 2020, 24(10):2553-2572.

[12] Muzammal M, Qu Q, Nasrulin B. Renovating blockchain with distributed databases: An open source system. Future Generation Computer Systems, 2019, 90(JAN.):105-117.

[13] Mingnan, Zhou, Dahai, et al. An Efficient Code-defect Testing Distributed System. IOP Conference Series: Materials Science and Engineering, 2019, 490(4):42038-42038.

[14] Hajjaj M, Miki M. Distributed Intelligent Lighting System by Performing New Model for Illuminance and Color Temperature in the Workplace. Intelligent Control and Automation, 2019, 10(1):1-12.

[15] Dhingra S, Gupta S, Bhatt R. A Study of Relationship Among Service Quality of E-Commerce Websites, Customer Satisfaction, and Purchase Intention. International Journal of E-Business Research, 2020, 16(3):42-59.

[16] Ellen, G, Engelhardt, et al. Is There a Relationship between Shared Decision Making and Breast Cancer Patients' Trust in Their Medical Oncologists?:. Medical Decision Making, 2019, 40(1):52-61.

[17] Hassan H, El-Desouky A I, Ibrahim A, et al. Enhanced QoS-Based Model for Trust Assessment in Cloud Computing Environment. IEEE Access, 2020, PP(99):1-1.

[18] Mirzaee F, Dehghan M. A Model of Trust within the Mother-Midwife Relationship: A Grounded Theory Approach. Obstetrics and Gynecology International, 2020, 2020(5):1-7.