Management Node Selection Based on Cloud Model in a Distributed Network

Hanyi Tang[1,2(✉)], Qibo Sun[1], and Jinglin Li[1]

[1] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, China
thyideyx@gmail.com, {qbsun,jlli}@bupt.edu.cn
[2] CETC Key Laboratory of Aerospace Information Applications, Beijing, China

Abstract. Network has become an indispensable part of people's lives. However, network insecurity still has negative impact on the development of network. Trust evaluation is becoming the core of network security enhancement. In distributed network, the node with the highest trust value is often selected as the subnet management node. The traditional distributed trust evaluation frameworks cannot achieve the best effect because of the ignorance of trust value stability of each node. To address this problem, this paper proposes a management node selection method based on cloud model. This method employs the cloud model to analyze the stability of network nodes, and selects the optimal node based on the three numerical features of cloud model. The experiment results show the effectiveness of our method.

Keywords: Trust evaluation · Network security · Cloud model

1 Introduction

With the development of network technology, distributed network is wildly used in reality. A lot of fraud problems appear for malicious node behavior. Network trust evaluation becomes a key technology in the field of network security.

In the distributed network environment, there is no centralized trust management node to calculate the trust of other nodes in the network. In traditional trust evaluation management system, the network are divided into clusters and the node with highest trust currently is selected as the trust management node. However, the behavior of nodes in a distributed environment is dynamic, and the trust of nodes changes over time. Therefore, dynamic trust evaluation node selection is an important method in a trust evaluation management system. A new trust evaluation node is selected when the trust of current trust evaluation node descends. However, the trust management node may change continually. Therefore, it is better to select a more stable node as the trust evaluation management node. We will tackle the problem by considering the node trust and stability of node trust in evaluation management node.

The paper presents a trust evaluation management node in distributed computing. Cloud model is extensively employed in this paper to solve the problem [12–14]. Firstly, backward cloud model is employed to evaluate the stability of each node. Then, an algorithm based on forward cloud model is proposed to select the trust evaluation

I. Romdhani et al. (Eds.): CollaborateCom 2017, LNICST 252, pp. 176–185, 2018.
https://doi.org/10.1007/978-3-030-00916-8_17

management node. Experiment results illustrate that our method is more accurate than other method.

The remainder of the article is organized as follows. We summarize the previous work in Sect. 2. Our management node selected method is described in detail in Sect. 3. We evaluate our method in Sect. 4. Conclusions are finally drawn in Sect. 5.

2 Related Work

The research in [3] proposes a trust evaluation model in cloud computing environment. The feedback factor and feedback density factor are introduced into the model to evaluate the trust of feedback. A trust computing model which based on experience and probabilistic statistical explanation is proposed in [4]. The concept of experience which is used to measure trust is introduced in the model. The derivation of credibility and comprehensive calculation formulation which are derived from empirical recommendations is presented. It is crude that use arithmetic mean of trust value can't prevent malicious network nodes from attacking reputation system. Based on Bayesian, a trust model which uses prior knowledge to obtain estimation parameters and posterior probabilities is proposed in [5]. However, the trust model did not consider the dynamically change of trust. Subjective trust management model based on fuzzy set theory is proposed in [6]. The concept of membership degree in fuzzy set theory is introduced to describe the fuzziness of trust.

All the above methods focus on the trust evaluation. However, for a large scale distributed network, it is unable to authorize a centralized trust management node to calculate the trust of other nodes in the network. We need to divide the network into clusters and select a trust evaluation management node for each cluster. We will address the problem in this paper.

Based on probability theory and fuzzy set theory, cloud model is proposed by [9] to qualitatively evaluate the uncertainty transformation model. Cloud model have widely used in many fields such as intelligent control, fuzzy evaluation, and evolutionary computation. In this paper, we propose a trust evaluation management node selection method based on cloud model.

3 Management Node Selection Based on Cloud Model

Our management node selection framework is shown in Fig. 1. Our management node selection method consists of three modules. Firstly, the trust value of the candidate nodes is obtained (Sect. 3.1). Secondly, the backward cloud model is extensively employed to evaluate the stability of the candidate nodes (Sect. 3.2). Finally, based on forward cloud model, a management node selection algorithm is proposed (Sect. 3.3).

3.1 Node Trust Calculation Based on Historical Behavior Data

Our paper focus on how to select the optimal management node rather than node trust evaluation. Therefore, this paper will use the trust evaluation method proposed in [10].

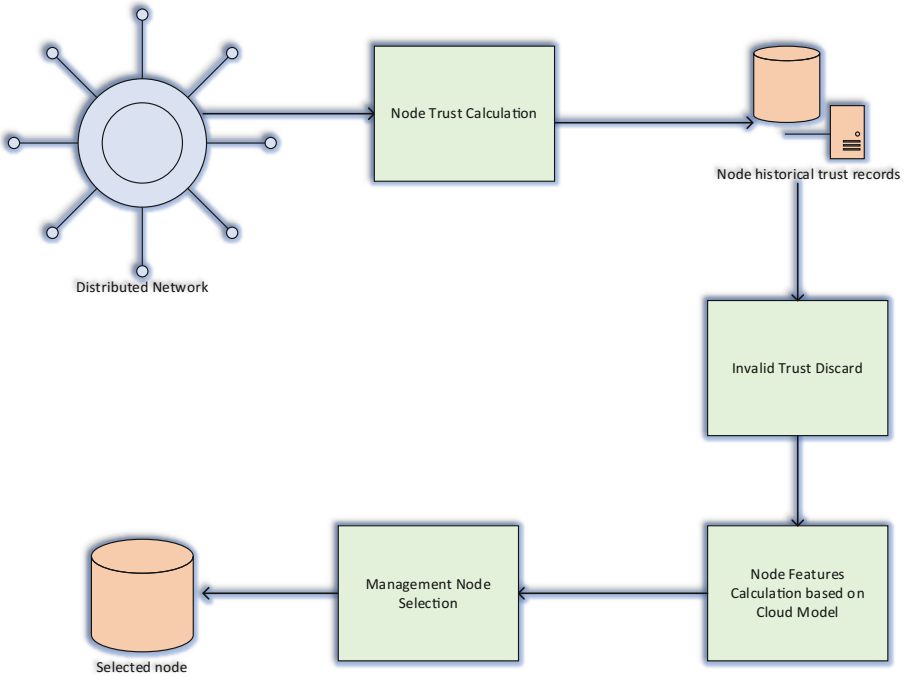

Fig. 1. Management node selection framework based on cloud model

Suppose $CN = \{cn_1, \ldots cn_i \ldots cn_{\max}\}$ denotes all the candidate nodes. Suppose that the behavior properties are $I = \{I_1, I_2, \ldots, I_m\}$. The trust value of the node of node cn_i in time t is calculated as follows:

$$NT_i^t = \sum_{p=1}^{m} w_p \times \tau_t\left(I_p(cn_i)\right) \tag{1}$$

where w_p represents the weight of behavior properties, $\tau_t\left(I_p(cn_i)\right)$ represents the value of the behavior property.

The replacement of node trust calculation method does not affect the performance of the management node selection method.

3.2 Node Stability Evaluation Based on Cloud Model

Cloud model [11] is a famous model to describe the transition between the qualitative concept and the quantitative values. Based on probability theory and fuzzy set theory, cloud model is developed with serious considering of the relation between randomness and fuzziness.

Definition 1 cloud and droplet. Suppose that U is a quantitative domain, and C is the qualitative concept of U. If quantitative value $x \in U$ and x is a stochastic

implementation of the qualitative concept C, $\mu(x) \in [0, 1]$, which denotes the certainty from x to C, is a random number with a stable tendency:

$$\mu : U \to [0, 1], \forall x \in U, x \to \mu(x) \tag{2}$$

Then the distribution of X in the domain U is called cloud, which is denoted by $C(X)$. Each x in X is called a droplet.

In cloud model, the features of the droplets are expressed three numerical value of the cloud. Cloud model employs three numerical features expectation (Ex), entropy (En), and hyper-entropy (He) to represent the stability of a node, as $C(Ex, En, He)$. Ex is the expectation of the distribution of the droplets. En represents the uncertainty of Ex. He is used to measure the uncertainty of entropy, which is determined by the randomness and fuzziness of entropy.

In this paper, all historical trust values of a specified node cn_i comprise a trust cloud as follows:

$$TC_{cn_i}(Ex^{cn_i}, En^{cn_i}, He^{cn_i})(0 \le Ex \le 1, 0 \le He \le 1) \tag{3}$$

Each trust value NT_i^t is a droplet. Ex is the expectation of all historical trust values as the basic trust. En is the entropy of trust, which reflect the uncertainty of trust relationship. He is the hyper entropy of trust, which reflect the uncertainty of En.

This paper extensively employ the backward cloud in [11] to evaluate the stability of trust values. Because the recent historical trust is more important than the old historical trust, we add a time-aware expectation, entropy, and hyper-entropy calculation method in backward cloud generator. In time-aware expectation, entropy, and hyper-entropy calculation, weights are assigned to the historical trusts. The weight of a trust is higher when the trust evaluation time is more near to current time. In our extended backward cloud, the features of the historical trust values is calculated as follows:

(1) The average value of historical trust values and the variance of historical trust values is calculated as follows:

$$\overline{T} = \frac{1}{n} \sum\nolimits_{t=t_1}^{t_n} \frac{(t - t_1)}{\sum\limits_j (t_j - t_1)} NT_i^t \tag{4}$$

$$A = \frac{1}{n} \sum\nolimits_{t=t_1}^{t_n} \frac{(t - t_1)}{\sum\limits_j (t_j - t_1)} \left| NT_i^t - \overline{T} \right| \tag{5}$$

$$B^2 = \frac{1}{n-1} \sum\nolimits_{t=t_1}^{t_n} \frac{(t - t_1)}{\sum\limits_j (t_j - t_1)} \left(NT_i^t - \overline{T} \right)^2 \tag{6}$$

(2) *Ex* is calculated as follows:

$$Ex = \overline{T} \tag{7}$$

(3) *En* is calculated as follows:

$$En = \sqrt{\frac{\pi}{2}} \times A \tag{8}$$

(4) *He* is calculated as follows:

$$He = \sqrt{B^2 - En^2} \tag{9}$$

$C(Ex, En, He)$ can be used to measure the uncertainty and stability of node trust. In the cloud model, *Ex* is the expectation of historical trust values, *En* is the uncertainty of trust, and *He* is the uncertainty of *En*. A node with smaller values of *En* and *He* is more stable in trust.

In addition, we will discard outdated historical trust values based on time window. As shown in Fig. 2, we keep a window with the size of T_w. If a trust value time is beyond the window, the trust is discarded in our method.

We will show how to select the optimal management node in the next section.

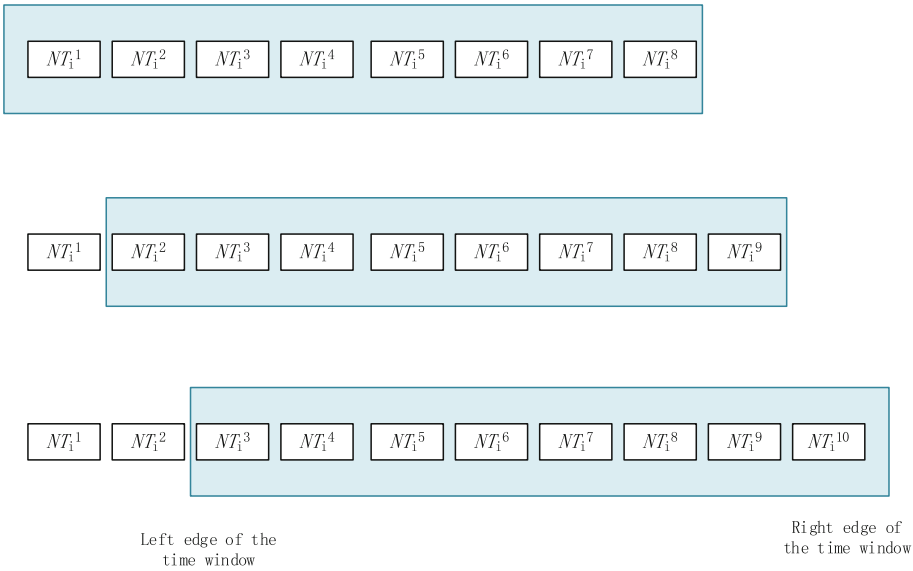

Fig. 2. Time window for invalid trust value discard

3.3 Management Node Selection

We will employ forward cloud to select the management node.

Firstly, we construct a benchmark cloud. The three features of the benchmark cloud are determined by the user, and are the largest values the user can accepted. We will select the management node by analyzing the distance between the trust cloud of candidate node and the trust benchmark cloud. This paper compares two trust cloud by the distance between the droplets. In this paper, the Euclidean distance is used to calculate the distance between two clouds.

Secondly, we use forward cloud generator to generate the normal cloud droplets of the benchmark cloud and the cloud of node cn_i. The normal cloud droplet is generated as follows:

(1) A normal random number En' with the expectation value En and the variance He is generated;
(2) A normal random number x_k with the expectation value Ex and the variance En' is generated;
(3) Calculate $y_k = e^{-\frac{(x_k - Ex)^2}{2(En')^2}}$ as degree of certainty
(4) Add Drop (x_k, y_k) as a droplet for node cn_i

The cloud distance calculation algorithm based on the forward cloud is shown in Algorithm 1.

Algorithm 1: The distance calculation of cloud

Input: $TC_b(Ex, En, He)$ of Benchmark trust cloud features, $TC_{cn_i}(Ex, En, He)$ of candidate nodes, the Number of cloud droplet N.

Output: The distance between two clouds *Distance*

1) Generate the normal cloud droplets by using forward cloud generator for the benchmark cloud $TC_b(Ex^b, En^b, He^b)$. Suppose the generated N droplets are denoted by $Drop(x_b^j, y_b^j)(1 \le j \le N)$.
2) Generate the normal cloud droplets by using forward cloud generator for the cloud of cn_i. Suppose the generated N droplets are denoted by $Drop(x_{cn_i}^j, y_{cn_i}^j)(1 \le j \le N)$.
3) Sort ($Drop(x_b^j, y_b^j)(1 \le j \le N)$) and $Drop(x_{cn_i}^j, y_{cn_i}^j)(1 \le j \le N)$ by x
4) for $j = 1$ to N do
5) $dis_{bi} = dis_{bi} + \sqrt{(x_b^j - x_{cn_i}^j)^2 + (y_b^j - y_{cn_i}^j)^2}$
6) return dis_{bi}

A smaller distance between the trust cloud of cn_i and the benchmark trust cloud means that the stability of cn_i is closer to the predefined ideal state. The higher the stability of the candidate node cn_i is, the better is it to be selected as a management node. On the contrary, a larger distance between the trust cloud of cn_i and the benchmark trust cloud indicates that the stability of the node bad and the node is excluded from the candidate nodes. We will select the node with the smallest distance as the management node.

4 Experiment and Analysis

The experiments conduct on the OMNET++ simulation software, and OMNET++ generates the historical interaction data of nodes and obtains the trusted value between nodes. We compare our dynamic trust evaluation management node selection method (DTE) with the static trust evaluation (STE) method which select the management node based on current node trust.

For visually show the sensitivity of the cloud model to the dynamic change of trust value, we illustrate the cloud model of nodes with varies behaviors. We will gradually add malicious behavior for a node with high trust. The experiment results are shown in Figs. 3, 4, 5, and 6. As shown in Figs. 3, 4, 5, and 6, the cloud model is very sensitive to the dynamic change of trust values. Cloud model will change a lot when each time to add the malicious behavior by 10% in this experiment.

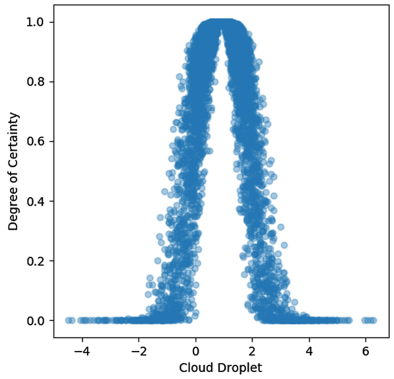

Fig. 3. Cloud drop distribution of node with high trust stability

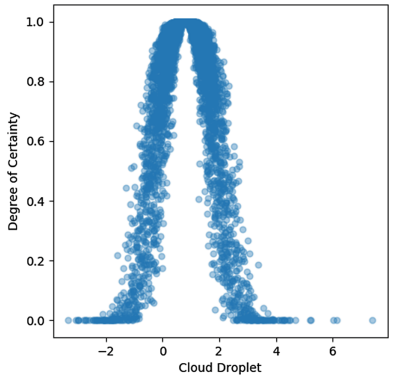

Fig. 4. Cloud drop distribution of node with general trust stability

In order to verify the validity of the cloud distance calculation based on Euclidean distance, we set the cloud generated by non-malicious node as the benchmark cloud. Then, we generate different clouds by adding different percent of malicious behaviors to destroy the stability of the non-malicious node. We calculate the distance between the generated clouds and the benchmark cloud. The results are shown in Fig. 7.

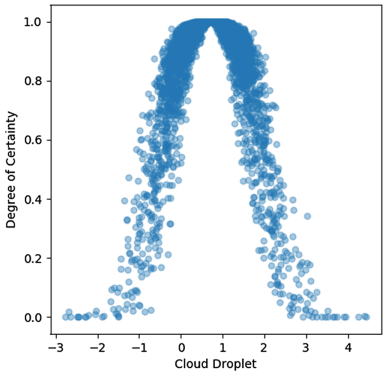

Fig. 5. Cloud drop distribution of node with low trust stability

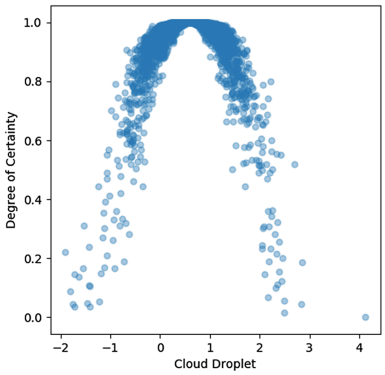

Fig. 6. Cloud drop distribution of extremely unstable node

From Fig. 7, we can clearly see that the distance increases when the behavior of a node become more unstable.

In experiment 3, we evaluate DTE and STE that a fixed node is chosen as the evaluation node by comparing the two methods in management node selection. Suppose there is a none-malicious node cn_j. The methods need to select a node cn_i to evaluate the trust value of cn_j. The experiment results are shown in Fig. 8. As shown in Fig. 8, the x-axis represents the ratio of malicious nodes, and the y-axis represents the evaluation result of cn_j.

We can see clearly through Fig. 8 that the trust of cn_j drops rapidly in STE with the increase of the proportion of malicious nodes in the network. However, the trust of cn_j in DTE is relatively stable. The experiment results show the effectiveness of our proposed management node selection approach.

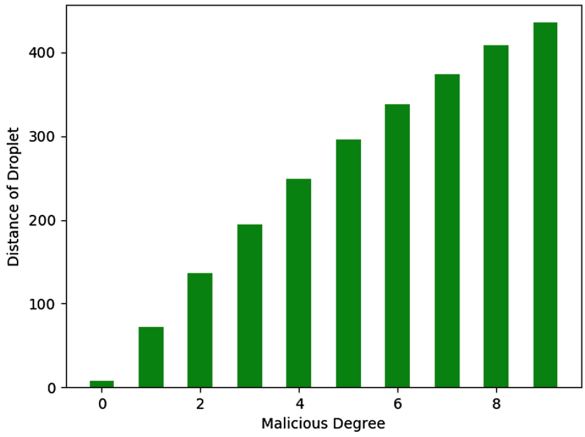

Fig. 7. Distance between benchmark cloud and trust cloud with different stability

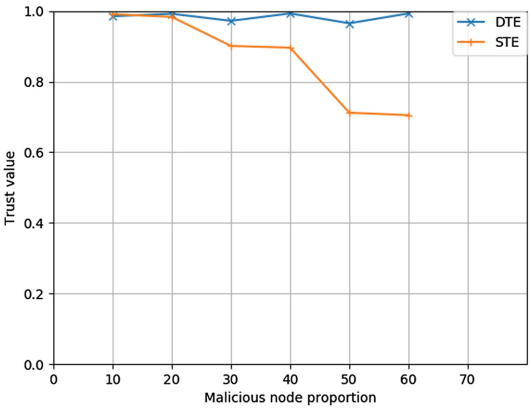

Fig. 8. Experiment results of STE and DTE

5 Conclusion

We propose a trust evaluation management node selection method in this paper. The core idea of the proposed method is to analyze the stability of nodes based on the historical behavior data and cloud model. The experiment results in simulated network illustrate the effectiveness of our method.

Acknowledgment. The work is supported by NSFC (61571066), and CETC key laboratory of aerospace information applications open project fund.

References

1. Foster, I., Kesselman, C.: The Grid: Blueprint for a New Computing Infrastructure. Morgan Kaufmann, San Francisco (1999)
2. Stoica, I., Morris, R., Karger, D., et al.: Chord: a scalable peer-to-peer lookup service for internet applications. San Diego, California, United States (2001)
3. Wang, Y., Peng, X.G., Bian, J., Dong-Lai, F.U.: Research on trust feedbacks credibility evaluation model for cloud computing. J. Comput. Eng. Des. **06**, 1906–1910 (2014)
4. Beth, T., Borcherding, M., Klein, B.: Valuation of trust in open networks. In: Gollmann, D. (ed.) ESORICS 1994. LNCS, vol. 875, pp. 1–18. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-58618-0_53
5. Wang, Y., Vassileva, J.: Bayesian network trust model in peer-to-peer networks. In: Moro, G., Sartori, C., Singh, M.P. (eds.) AP2PC 2003. LNCS (LNAI), vol. 2872, pp. 23–34. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-25840-7_3
6. Tang, W., Hu, J., Chen, Z.: Research on a fuzzy logic-based subjective trust management model. J. Comput. Res. Dev. **42**(10), 1654–1659 (2005)
7. Li, D., Liu, C., Du, Y., Han, X.: Uncertainty artificial intelligence. J. Softw. **15**(11), 1583–1594 (2004)
8. Li, D., Liu, C.: On the universality of the normal cloud model. J. Eng. Sci. **6**(8), 28–34 (2004)

9. Li, D.: Uncertainty Artificial Intelligence. National Defend Industry Press, Beijing (2005)
10. Yang, G., Sun, Q., Zhou, A., Li, J., Yuan, X., Tang, H.: A context-aware trust prediction method based on behavioral data analysis in distributed network environments. In: IEEE, International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress, pp. 674–680. IEEE Press (2016)
11. Yuan, L., He, Z., Zeng, G.: A resource trade model based on trust evaluation for grid computing. In: Network and Parallel Computing Workshops, 2007. NPC Workshops. IFIP International Conference, pp. 506–510. IEEE Press (2007)
12. Chen, J.J., Zhang, S.B.: Study on trust evaluation model based on cloud model and trust chain. Appl. Res. Comput. **32**, 249–253 (2015)
13. Zhang, T., Yan, L., Yang, Y.: Trust evaluation method for clustered wireless sensor networks based on cloud model. Wirel. Netw. 1–21 (2016)
14. Ayadi, O., Halouani, N., Masmoudi, F.: A fuzzy collaborative assessment methodology for partner trust evaluation. Int. J. Intell. Syst. **31**(5), 488–501 (2016)