CNTE: A Node Centrality-Based Network Trust Evaluation Method

Xiang Yuan[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
{yuanxiangsky, qbsun, jlli}@bupt.edu.cn
[2] CETC-Key-Laboratory-of-Aerospace Information Applications, Beijing, China

Abstract. Network trust evaluation is an important mechanism in improving network security. Network trust is determined by the node trust and the topology of the network. To improve the evaluation accuracy and efficiency, we propose a node centrality-based network trust evaluation method. Firstly, the node trust is calculated by employing the node behavior analysis. Secondly, node centrality in the network is calculated based on coefficient variation. Finally, the network trust is calculated based on the above-mentioned steps. Experiment results show that our proposed method can improve the evaluation accuracy.

Keywords: Network trust · Trust evaluation · Node behavior
Node centrality

1 Introduction

The scale of network is now growing continuously. On the one hand, because of the complexity of the network, the network confronts various internal security threats. On the other hand, due to the improper operation of the users, the malicious attacks from hackers expose the network to serious external security threats. However, the traditional identity-based network security mechanism is unable to solve this problem effectively. Therefore, network trust evaluation based on the node behavior has attracted the attentions from the researchers [1].

The traditional trust model evaluates the trust of the network node by constructing the trust relationship among the entities of the network and quantifying the interactive information between the network nodes. There is a trust relationship between people in sociology, and the trust of each of them will affect the trust of the groups of these people. Compared to groups in social relations, where the trust of each node constituting the subnet is known, the trust value of the entire subnet can be evaluated and quantified. When the information in the network needs to go through a subnet, we can assess the trust value of the network to determine whether the information is transmitted through this network. The ambiguity of trust relationships and the uncertainty of node behaviors are the greatest challenge of current trust evaluation research. At present, the researchers put forward a variety of evaluation models [3–12], including the Bayesian theory-based model, Fuzzy set theory-based model, DS evidence

I. Romdhani et al. (Eds.): CollaborateCom 2017, LNICST 252, pp. 186–196, 2018.
https://doi.org/10.1007/978-3-030-00916-8_18

theory-based model and so on. These models can effectively promote the development of network trust evaluation and improve the network security. However, the existing model also has some of the following problems:

(1) Most of the trust evaluation methods focus on the node trust evaluation, and the solution for the trust evaluation of the entire network is lacking.
(2) The existing network trust evaluation methods that combine the node trust based on average trust of all node do not consider the characteristics of the entities in the network and the location of the entity itself.

To solve the above problems, a trust evaluation method based on node centrality is proposed on the basis of previous ideas. The proposed method makes the trust evaluation objective and fair by taking into account the topological position of the network nodes. The experiment results show the effectiveness of our method.

The remainder of the article is organized as follows. The Sect. 2 gives a brief review of related work. Section 3 gives definitions of relevant problems. In Sect. 4, the experiment results are given. Section 5 gives a summary of the article.

2 Related Work

Trust evaluation is the key technology to support the construction of network trust system. Many scholars and experts have studied the evaluation of trust. As early as 1996, Blaze [1] and others put forward the concept of trust management in order to solve the problem of service security in Internet. Trust is considered as an important information that helps the user to make a judgment about a network entity or a network. Then, the Chinese scholar Lin Chuang et al. [2] put forward the concept of trusted network. The basic properties of trusted network and the problems to be solved are discussed.

In recent years, many scholars try to quantify the dynamic trust relationships in the network. In the paper [3], a Bayesian network-based approach is proposed to compute the trust value of network entities. The method considers the impact of authentication and network interaction behavior on trusted metrics. Time window and time factor are introduced to improve the timeliness and dynamic adaptability of the model. The method in paper [4] is proposed based on fuzzy decision analysis. Multiple user behaviors evidence is considered, and ordered binary comparison theory is employed to get the optimal weights. A trust evaluation method based on cloud model is proposed in paper [8]. By introducing penalty mechanism and attenuation function, the method can make up the deficiency of dynamic change of cloud model in pervasive trust environment. The method based on cloud model takes full account of the diversity and uncertainty of trust objects, and the results are more accurate than traditional methods.

These trust evaluation models focus on the trust evaluation of a single network entity, but there is not much discussion about the relationship between entities and the overall topology of the network. We will address the problem in this paper (Fig. 1).

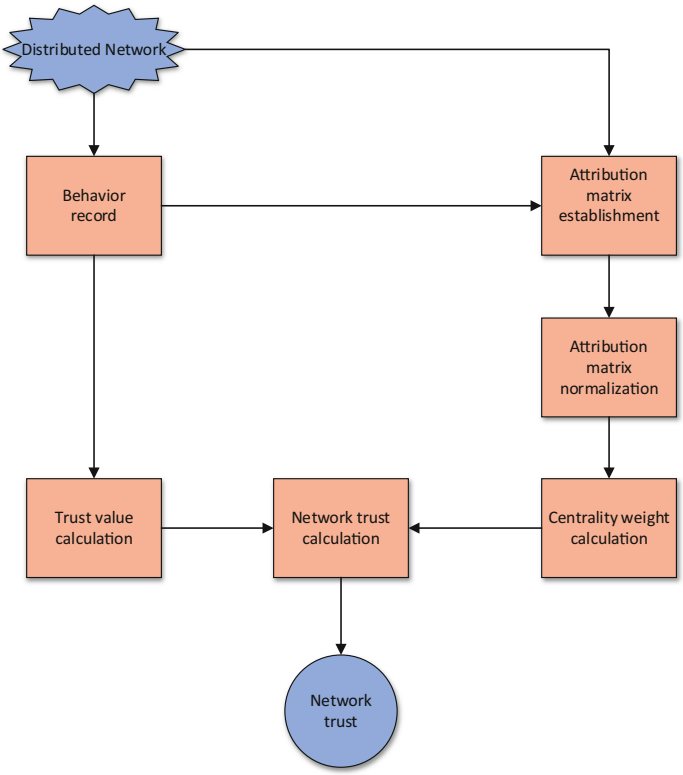

Fig. 1. Framework of network trust evaluation method

3 Proposed Network Trust Evaluation Method

3.1 Node Trust Calculation

Let $v_1, v_2, v_3, \ldots v_n$ represent network entities (nodes or resources) in a network, $\alpha_1, \alpha_2, \alpha_3, \ldots \alpha_n$ represent the trust values of corresponding node in the network. The network trust is determined by the trust of all nodes in the network. Therefore, we firstly need calculate node trust. In this paper, we focus on network trust calculation. For the generality of the scheme, the node trust calculation method is replaceable, and the effectiveness of our method is not influenced. Therefore, this paper employs the method in [15] to calculate the node trust value.

3.2 Attribution Matrix Establishment

The contribution of different node to network trust varies. We employ centrality to evaluate the different contribution. In order to guarantee the completeness, we select two global centrality attributes and two local centrality attributes to evaluate the node

centrality. These four centrality attributes are closeness centrality, betweenness centrality, semi centrality, and interaction centrality. The closeness centrality describes the average minimum distance of a node to other nodes. The betweenness centrality describes the number of shortest paths through the node. These two properties reflect the global centrality of the node. The semi local centrality reflects the number of the first and the second nearest neighbors in the network. The more number of neighbors of a node, the greater the influence of the node is. The interaction centrality reflects the interaction times of the network nodes. These two properties reflect the local centrality of the node. The proximity centrality, betweenness centrality, and semi local centrality are defined in the paper [14]. The interaction centrality is defined as follows.

Definition 1 Interaction centrality. Entities in the network interact with each other to transfer data. Interaction centrality is defined as follows:

$$C = C_t + \sum_k C_k d(k) \tag{1}$$

Because the node interaction is a continuous process, the attenuation factor δ is introduced. δ is a time decay function. The closer the interaction time to the current time is, the more important the interaction is to the evaluation. The attenuation function is defined as follows:

$$\delta(k) = \frac{k}{t-1} \tag{2}$$

where k is the timestamp, and the $t-1$ is the longest time interval considered in the current system.

Definition 2 Semi centrality. For a node n_i, the $Nei(n_i)$ is defined as the number of all neighbors that can be reached within 2 steps from the n_i, and then we defined

$$Q(n_j) = \sum_{n_i \in p(n_j)} Nei(n_i) \tag{3}$$

where $n_i \in p(n_j)$ represents the set of the number of all neighbors that can be reached within 1 step from n_j. Thus, the semi centrality of the node n_i can be obtained

$$semi(n_i) = \sum_{w \in P(i)} Q(w) \tag{4}$$

The semi local centrality reflects the number of the first and two order neighbors of the corresponding node in the network. The more number of neighbors of a node is, represents the greater the influence of the node is.

Definition 3 Closeness centrality. We defined d_{ij} as the length of the shortest path between the node n_i and the node n_j. Then the average length of the shortest path from a node to other nodes is:

$$d_i = \frac{1}{n-1}\sum_{i \neq j} d_{ij} \tag{5}$$

A smaller d_i denotes that n_i is closer to other nodes in the network. The closeness centrality is defined as:

$$Closeness(n_i) = \frac{1}{d_i} = \frac{n-1}{\sum\limits_{i \neq j} d_{ij}} \tag{6}$$

Definition 4 Betweenness centrality. Betweenness centrality is defined as the percent of shortest path that pass through n_i. The betweenness centrality is defined as

$$Betweenness(n_i) = \sum_{i \neq s, i \neq d, s \neq d} \frac{sp^i_{s,d}}{sps, d} \tag{7}$$

where sp_{sd} is the number of the shortest path from the source node n_s to the destination node n_d, and sp^i_{sd} is the number of the shortest path passing through *ni* from the source node n_s to the destination node n_d.

Suppose the number of centrality indicator is n. Then the centrality vector of the *i-th* node is $X_i = [x_{i1}, x_{i2}, \ldots\ldots, x_{in}]$. Where $x_{i1}, x_{i2}, \ldots x_{\mathrm{in}}$ is the centrality indicator of the *i-th* node. Now we construct a matrix for node centrality evaluation. The centrality evaluation matrix of the network is as follows:

$$X = \begin{Bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \cdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{Bmatrix} \tag{8}$$

where $x_{11},\ x_{21} \ldots x_{n1}$ is the centrality vector of the first node, and there are m network nodes. In this paper, four centrality indicators are used to evaluate the node centrality. Among them, x_{i1} represents the semi centrality indicator of the *i-th* node, and x_{i2} represents the closeness centrality indicator of the *i-th* node; x_{i3} represents the betweenness centrality indicator of the *i-th* node, and x_{i4} represents the Interaction centrality indicator of the *i-th* node. The evaluation indicator vector of *i*th node is $X_i = [x_{i1}, x_{i2}, x_{i3}, x_{i4}]$.

3.3 Attribution Matrix Normalization

As for the centrality indicator in the matrix, the dimensions of the centrality indicators are different. Therefore, it is necessary to normalize the centrality evaluation matrix so

that the dimensions of the centrality indicators are in the same level. The maximum-minimum method is used to normalize the data. The maximum-minimum method is as follows:

$$x_{ij} = \frac{x_{ij} - \{\min(x_{1j}, x_{2j}, \ldots, x_{mj})\}}{\{\max(x_{1j}, x_{2j}, \ldots, x_{mj})\} - \{\min(x_{1j}, x_{2j}, \ldots, x_{mj})\}} \tag{9}$$

3.4 Centrality Weight Calculation

We employ the coefficient variation method, which is an objective method, to calculate the weight of the centrality indicator. Firstly, the mean and variance are calculated by the following:

$$\overline{x_i} = \frac{1}{n}\sum_{j=1}^{j=m} x_{ji}, i = 1, 2 \ldots n \tag{10}$$

$$s_i = \frac{1}{n}\sqrt{\sum_{j=1}^{j=m} \left(x_{ji} - \overline{x_i}\right)^2}, i = 1, 2 \ldots n \tag{11}$$

Based on the mean and variance, the coefficient variation of each centrality indicator can be calculated by the following:

$$CV(i) = \frac{\overline{x_i}}{s_i}, i = 1, 2..n \tag{12}$$

After getting the coefficient variation of each centrality indicator, the centrality weight χ_i of each centrality indicator is calculated by the following:

$$\chi_i = \frac{CV(i)}{\sum_{k=1}^{n} CV(k)}, i = 1, 2 \ldots n \tag{13}$$

In this method, n equal to 4, which represents that there are 4 centrality indicators.

Node centrality calculation comprehensively consider the node position in the network, and current node statement. Based on the weight of the centrality indicator, the centrality of each node is calculated as follows:

$$p(i) = \sum_{j=1}^{j=n} x_{ij} * \chi_j = 1, 2 \ldots m \tag{14}$$

3.5 Network Trust Evaluation

Based on the node centrality, we now calculate the contribution weight of each node to the network trust. A node with higher node centrality contributes more to network trust. Therefore, the contribution weight of each node to the network trust is calculated as follows:

$$\varpi_i = \frac{p(i)}{\sum_{k=1}^{k=m} P(k)}, i = 1, 2 \ldots m \tag{15}$$

Suppose $v_1, v_2, v_3, \ldots v_n$ is the nodes in the network. The overall network trust is calculated as follows:

$$\Gamma(v_1 \ldots v_n) = \sum_{i=1}^{N} \omega_i \alpha_i \tag{16}$$

4 Experiment and Analysis

We experiment on a discrete event simulation platform named OMNET++, which is an open source and multi-protocol network simulation software. It can simulate all kinds of network environment effectively. We experiment on two networks: (1) start network. Star network topology is shown in Fig. 2. (2) BUPT campus network. The BUPT campus network topology is shown in Fig. 3. For the two networks, the interaction between nodes is simulated and the interaction records between nodes are recorded. In the experiment, we compare CNTE (node centrality-based network trust evaluation method) with MBEM (mean-based evaluation method, the network trust is the average of the node trust).

The first experiment is conducted on the start network. Firstly, we want to see how the two methods act when the behavior of a central node changes. Therefore, we increase the number of successful interactions of node 1. The experiment results are shown in Fig. 4. Secondly, we want to see how the two methods act when the behavior of a non-central node changes. Therefore, we increase the number of successful interactions of node 2. The experimental results are shown in Fig. 5. As can be seen in Figs. 4 and 5, the accuracy of our method is higher than the compared method.

The second experiment is conducted on the BUPT campus network. Firstly, how the two methods act when the behavior of a central node changes is evaluated. We increase the number of successful interactions of node 1. The experiment result is shown in Fig. 6. Secondly, how the two methods act when the behavior of a non-central node changes is evaluated. We increase the number of successful interactions of node 31. The experimental results are shown in Fig. 7. Experiment results show that the network trust ascends quickly when the trust of a core node increases. Otherwise, the network trust changes slowly. Therefore, our approach has a good response to the impact of different network nodes on the overall network trust.

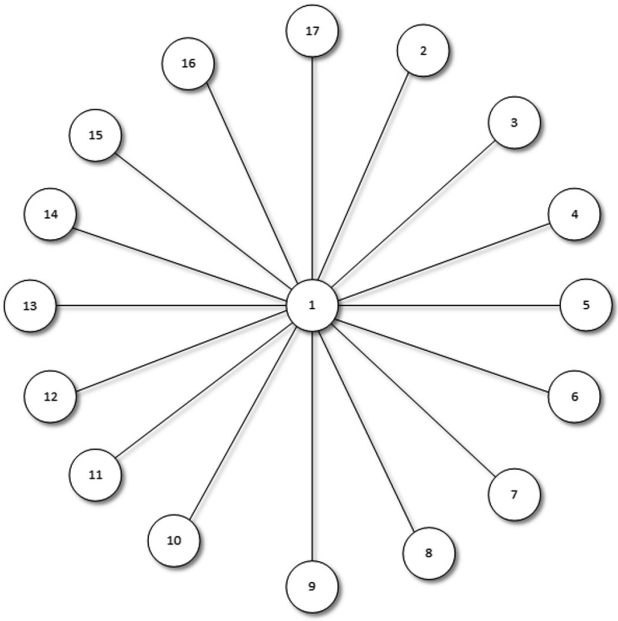

Fig. 2. Star network topology

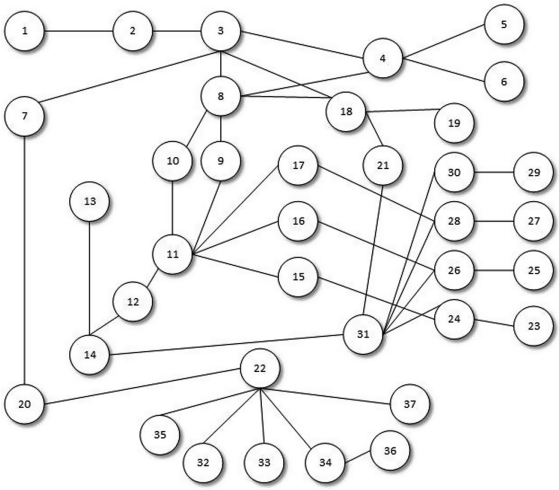

Fig. 3. BUPT campus network topology

In the experiment, the relationship between the performance of the algorithm and the network complexity is discussed. The network topology is abstracted as a graph, and the network complexity is described by the number of nodes N and the number of edges M in the network. In Fig. 8, the relationship between the efficiency of the

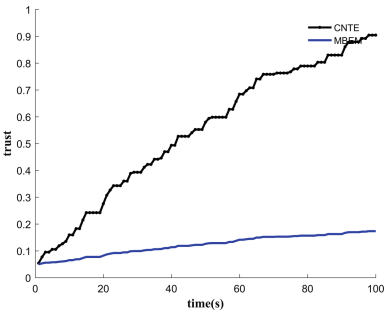

Fig. 4. Results in star network when the behavior of node 1 changes

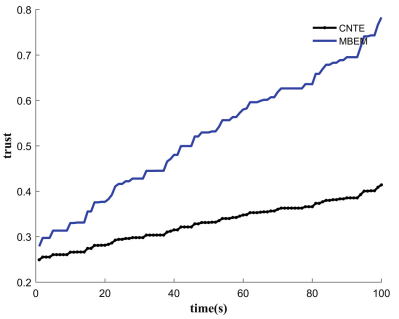

Fig. 5. Results in star network when the behavior of node 2 changes

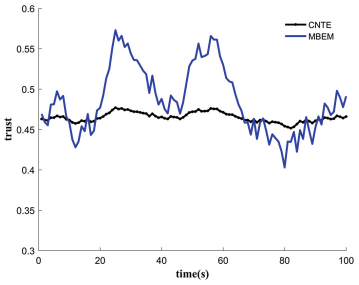

Fig. 6. Results in campus network when the behavior of node 1 changes

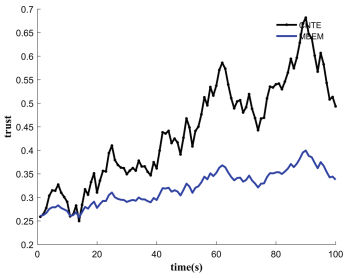

Fig. 7. Results in campus network when the behavior of node 31 changes

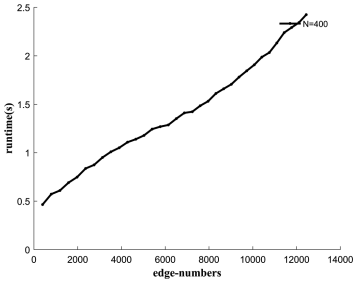

Fig. 8. Algorithm execution time and the number of different edges

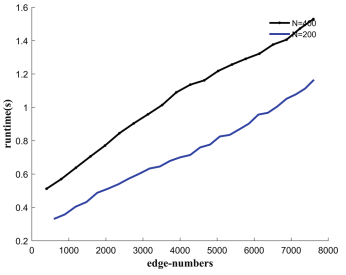

Fig. 9. Algorithm execution time under two quantitative nodes

algorithm and the edges of the network is given when N = 400 is used. With the increase of the number of edges, the execution time of the algorithm is increasing. Figure 9 compares the execution time in the N = 300 and N = 500 networks as the M continues to increase. From the experiment, we can see that the execution efficiency of the algorithm is less than 1 s in $N < 400$ and $M < 4000$. The experiment show that the execution time of the algorithm increases with the complexity of the network, but the algorithm has higher efficiency when the network size is small.

5 Conclusions and Future Work

In this paper, we propose a method of network trusted evaluation based on network centricity. This method is used to evaluate the trust value of subnets composed of network nodes. This approach solves the problem of evaluation of the entire subnet trust. The network trust is calculated based on the node trust and the network topology. Firstly, we calculate the trust value of each node in the network based on the node behavior. Then, based on the network topology, the node centrality is calculated by using the coefficient variation. Finally, based on the node centrality, our method combines the node trust to calculate the network trust. Experiments show that the proposed method has high performance and availability. The method has good performance in the case of small network size, but it is also worth optimizing for large networks.

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

References

1. Blaze, M., Feigenbaum, J., Lacy, J.: Decentralized trust management. IEEE Computer Society, p. 164 (1996)
2. Lin, C., Peng, X.: Research on trustworthy network. Proc. Chin. Soc. Comput. **28**(5), 751–758 (2005)
3. Liang, H., Wu, W.: Research on credible measurement model based on dynamic Bayesian networks. J. Commun. **9**, 68–76 (2013)
4. Melaye, D., Demazeau, Y.: Bayesian dynamic trust model. In: Pěchouček, M., Petta, P., Varga, L.Z. (eds.) CEEMAS 2005. LNCS (LNAI), vol. 3690, pp. 480–489. Springer, Heidelberg (2005). https://doi.org/10.1007/11559221_48
5. Gao, Y., Liu, W.: BeTrust: a dynamic trust model based on bayesian inference and Tsallis entropy for medical sensor networks. J. Sensors **2**, 1–10 (2014)
6. Liang, H.Q., Wu, W.: Research of trust evaluation model based on dynamic Bayesian network. J. Commun. **34**(9), 68–76 (2013)
7. Sun, Q.: Research on P2P network reputation model based on cloud model and trusted recommendation source. University of Science & Technology China (2010)
8. Wang, J., Yang, J., Yang, W., et al.: Research on trust mechanism based on cloud model in P2P networks. Comput. Eng. **40**(5), 124–128 (2014)
9. Ren, K., Li, T., Wan, Z., et al.: Highly reliable trust establishment scheme in ad hoc networks. Comput. Netw. Int. J. Comput. Telecommun. Netw. **45**(6), 687–699 (2004)
10. Ma, J., Zhao, Z., Ye, X.: Evaluation of user behavior in trustworthy networks based on fuzzy decision analysis. Comput. Eng. **37**(13), 125–127 (2011)
11. Feng, R., Xu, X., Zhou, X., et al.: A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory. Sensors **11**(2), 1345–1360 (2011)
12. Ganeriwal, S., Srivastava, M.B.: Reputation-based framework for high integrity sensor networks. In: DBLP, pp. 66–77 (2004)

13. Ahmed, A., Bakar, K.A., Channa, M.I., et al.: A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks. Front. Comput. Sci. **9**(2), 280–296 (2015)
14. Ren, X., Linyuan, L.: A survey of network important node ranking methods. Sci. Bull. **13**, 1175–1197 (2014)
15. Lu, X.: Research on trust evaluation model of mobile ad hoc networks. Anhui University (2014)