Trust Prediction Model Based on Deep Learning in Social Internet of Things

Yuyao Wen, Zhan Xu, Ruxin Zhi(✉), and Jinhui Chen

Beijing Information Science and Technology University, Beijing 100192, China
wenyuyaol63@l63.com, zhiruxin@bistu.edu.cn

Abstract. The Social Internet of Things (SIoT) is the result of the development of Internet of Things from intelligence to socialization. In the social internet of things, different nodes can automatically establish social relationships through social networks to obtain the services they need. Trust management is very important to such an open environment. This paper proposes an improved trust management model for social internet of things, which is divided into two parts: the improved node-level trust model and server-level trust model. In this paper, we propose an innovative trust model at the SIoT server-level, by introducing the deep learning model to predict the trust value of the new nodes in the social internet of things, to solve the problem that the network delay may affect the trust value evaluation in the actual social internet of things network. The simulation results show that the model based on deep learning prediction can get more successful transaction experience, and it is still effective against the high proportion of malicious nodes. The system performance is significantly better than the model without deep learning.

Keywords: Social internet of things · Trustworthiness management · Deep learning

1 Introduction

With the rapid development of 5G in recent years, the internet of things is facing greater opportunities and challenges, and has attracted more and more attention [1, 2]. The internet of things makes the social form of human society not only occur to people, but also expand on a wider range of people to things, things to things. Because of this, the internet of things is also known as the future of the Internet. With the connection between a large number of objects and the intelligence of things, it is an inevitable trend to study the interaction method of social form among devices in the internet of things [3–5]. SIoT came into being. It is the combination of traditional internet of things and existing social networks [6].

In recent years, more and more attention has been paid to deep learning and learning model based on neural network. They are widely used in e-commerce, medical and other fields, and have brought great changes in various fields [7]. So is deep learning in 5G communication field. In the application scenario of the internet of things, the communication may not go well because the nodes are too sparse or too dense, which affects task delivery and trust to value evaluation. At this time, some new

B. Li et al. (Eds.): IoTaaS 2020, LNICST 346, pp. 557–570, 2021.
https://doi.org/10.1007/978-3-030-67514-1_44

nodes have little historical information about transaction with other nodes, which makes it difficult for other nodes to get effective trust evaluation. This problem is also known as the "cold start".

The overall structure of this paper is as follows: The second part introduces the related work of this paper; The third part introduces the improved node-level trust model and the SIoT server-level trust model; The fourth part proves the superiority of this model by simulation. The last part summarizes this paper.

2 Related Work

The original internet of things only considers the connection between things, while the concept of owner of each node is added to the social Internet of things. Each node establishes its own social relationship according to its owner's social network, and spontaneously finds other reliable nodes to deliver tasks. Each node can play the role of service provider or service requester. In such a social Internet of things network of frequent social behaviors, some nodes will face the risk of malicious attacks from the bad nodes because of their own interests, so it is important to evaluate the credibility of service providers in the social Internet of things.

There have been some trust models in the social internet of things before [8–11]. In [8], the author puts forward two parts of the trust model: subjective model from social network, each node calculates the credibility of its owner's friends according to its own experience and the opinions of friendly recommenders, and objective model from P2P (peer-to-peer computer network) communication network, in which each node stores the trust value to other nodes. Information is sent to its peers in a distributed hash table structure, so any node can use the same information. On the basis of [8, 12] proposed a new social internet of things model based on [13]. According to this model, a group of objects can be given social forms. For example, equipment in the same area can be defined as friendship, which is like living together or working together. Another type of relationship is defined as the object owned by the same user, which is called ownership object relationship, just like different intelligent devices in the same family owned by the same person, establishing friendship relationship is more convenient for their transaction.

A trust model named TMCOI-SIoT is proposed in [14]. In this model network, there is a SIoT server and several communities. Each community chooses the node with the highest reputation as its administrator according to the actual situation. Different task requester nodes can select the nodes in the corresponding community according to their own interests or task types of task transaction. In this model, all nodes that want to join or leave the community need the consent of the community administrator (that is, nodes with a trust value higher than the threshold value will be allowed to join the community by the administrator, and nodes with insufficient trust value will be kicked out of the community by the administrator, and all nodes must not leave the community without permission). Otherwise, the community administrator will add their information to the "blacklist" and inform the SIoT Servers and other community administrators. In [14], trust models are proposed at node-level and administrator-level. In the node-level trust model, two interactive nodes obtain the trust value evaluation through

the previous transaction experience; in the administrator-level, use Kalman filter model to predict and evaluate the trust value of unfamiliar nodes (nodes with insufficient transaction experience).

Based on [14] and deep learning model, this paper proposes an improved trust model for social internet of things, which is divided into improved node-level trust model and SIoT server-level trust model. The main innovations of this paper are as follows:

1) In the node-level trust model, we calculate the trust weight of the friendship nodes that provide indirect trust, that is, the higher the trust degree, the more valuable the advice provided by the nodes. This is more similar to the general situation of network trust calculation.
2) In the trust model of the SIoT server-level, aiming at the "cold start" problem mentioned above, this paper introduces the deep learning model to predict the trust value of the newly added nodes in the community in advance. Simulation results show that under the guidance of this prediction, the trust value convergence of the target node is faster than that without deep learning model, and the transaction success rate is higher in the total transaction process.

3 Trust Model

3.1 The Improved Trust Model of Node-Level

The purpose of trust management is to evaluate the credibility of nodes effectively, so as to find the malicious nodes that may provide malicious attacks in the network. Because different malicious nodes may launch a variety of malicious attacks in different situations, this paper divides the malicious node attacks into three types:

1) Malicious nodes destroy the reputation of a well-behaved node by providing wrong suggestions. And this will reduce the possibility of choosing this good node as a service provider. In this trust model, when a malicious node requests services from a good node, whether the service provided by the good node is good or bad, the malicious node gives it a lower trust value.
2) The malicious node can improve the reputation of another bad node by providing good suggestions, thus increasing the possibility of the bad node being selected as a service provider. This is also a collusive attack, that is, it can work with other bad nodes to improve each other's reputation. In this trust model, when a malicious node requests services from another malicious node, it will give a higher trust value, so as to carry out the collusion attack.
3) A malicious node can enhance its importance by providing a good service so that it can be selected as a service provider, but then it will provide a malicious service in an important transaction. In this model, when a good node requests services from a malicious node, the malicious node will provide good services to increase its trust in transactions of low importance, and provide poor services in important transactions.

In this paper, the trust value of a node is evaluated by the evaluation of node trust obtained by direct transaction between nodes (direct trust) and the reputation obtained by requesting service providers from friends (indirect trust). In this trust model, each node maintains its own set of trust evaluation for other nodes. In the experiment, each node dynamically updates its direct trust value and indirect trust value when interacting with other nodes (Table 1).

Table 1. List of parameters

Symbol	Meaning
i	Service requesting node
j	Service providing node
T_D	Direct trust value
T_{ID}	Indirect trust value
T	Total trust value
N	Corresponding transaction N times in total
h	Transaction factor

In order to deal with the above malicious attacks, the nodes in this model only request the corresponding node reputation from their friend nodes, and through the introduction of transaction factor h, classify the importance of different events, making it more difficult for malicious nodes to obtain high trust value from low transaction factor events. The specific model is as follows:

There are three kinds of social relations among the initial set nodes: ownership, location and community. If the trust value range is (0,1), and the trust value is 0, the node is completely untrusted; if the trust value is 1, the node is completely trusted. Among them, the initial trust value between nodes of the same owner is set to 0.9; the initial trust value between nodes of the same location relationship is set to 0.7; the initial trust value between nodes of the same community relationship is set to 0.6; the initial trust value between nodes without social relationship is set to 0.5.

In a real social network, two nodes in the same community or in the same location are more likely to succeed in transaction than non-social nodes. Therefore, in the simulation of this paper, the closer the social relationship between nodes will lead to a higher rate of successful transaction.

This model uses the trust model between nodes in [14] for reference to define the direct trust value between nodes: after node i requests services from and interacts with node j, node i calculates the direct trust value T_D of node j through the previous transaction experience with node j:

$$T_D = \frac{\alpha_{ij} + 1}{\alpha_{ij} + \beta_{ij} + 2} \tag{1}$$

$$\alpha_{ij} = R * \sum_{l=1}^{N} h_l \tag{2}$$

$$\beta_{ij} = P * \sum_{l=1}^{N} h_l \tag{3}$$

In formula (1), α_{ij} represents the successful transaction between node i and node j, and β_{ij} represents the failed transaction. In formula (2) (3), the calculation method of the two is given, where N represents the corresponding total number of transactions. h_l represents the transaction factor of the corresponding interaction between two nodes at the l th time. R (reward) is set to 1 and P (punishment) is set to 2. The purpose of double punishment for unsatisfied transactions is to deal with the third kind of malicious attack, that is, building trust is more difficult than losing trust. This prevents objects from performing well in low weight services to build good reputation, and then performing poorly in important services.

After the transaction, the node i sends a trust value request to its friend k, and calculates the indirect trust value T_{ID} by combining the trust value of its friends to the node j: (node i has n friends)

$$T_{ID} = \frac{\sum_{k=1}^{n} T_{kj} * T_{ik}}{\sum_{k=1}^{n} T_{ik}} \tag{4}$$

In [14], the indirect trust value acquisition method is to take the average number of recommended trust values of all recommenders, though this is defective in the actual network. Due to the different states of different nodes, the credibility of the recommended trust value given to the service requester is also different, so this model adds the weight of the service requester's trust value to each recommender here.

Finally, the total trust value of node i to node j is evaluated by formula (5):

$$T_{ij} = \lambda T_D + (1 - \lambda) T_{ID} \tag{5}$$

Where $\lambda \in [0,1]$ is used to weigh the direct trust value and the indirect trust value, and keep the total trust between 0 and 1.

Then, the total trust value of node i to node j is obtained by integrating the transaction experience of node i to node j:

$$T_{ij}(t) = (1 - \delta) T_{ij}(t - \Delta t) + \delta T_{ij}(t) \tag{6}$$

$T_{ij}(t - \Delta t)$ represents the total trust value of the last transaction between node i and j. $\delta \in [0,1]$ is used to weight the current and previous trust values.

3.2 Trust Model of SIoT Server-Level

This paper uses the model in [14] for reference, that is, there is a SIoT server and several communities in this social internet of things network, and each community has several nodes.

This paper mainly studies the trust value evaluation of unfamiliar nodes in the social internet of things network (taking the dense network as an example) where the communication may not go well due to the large delay. Therefore, in the simulation, we need to use the improved node-level trust model to simulate several transactions in the community before the trust value evaluation and prediction (10000 random transactions are simulated as training set data because there are many nodes in this paper).

In the simulation process of this model, each node selects the node with the highest trust value of its own trust value evaluation log for task interaction. For the node pairs with more than 10 successful transactions, the SIoT server collects the social relationship between node pairs, the ratio of the sum of transaction weights of previous successful transactions to the sum of transaction weights of all transactions, and the evaluation of the final trust value obtained after the corresponding target node interacts. The SIoT server inputs several groups of information collected as training sets into the DNN deep learning model as shown in Fig. 1.

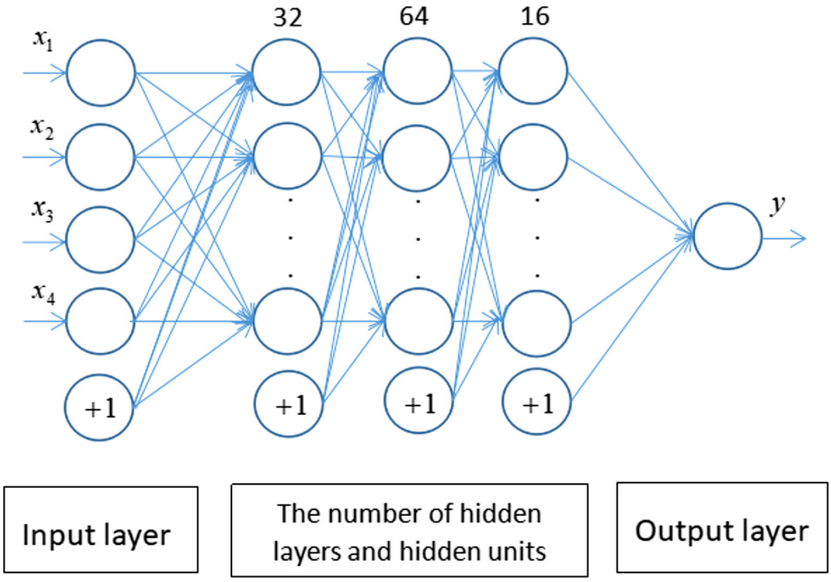

Fig. 1. Deep learning model used in this paper.

In the DNN deep learning model shown in Fig. 1, the input layer on the left is respectively: whether it is the friendship relationship (yes is recorded as 1, no as 0); whether it is the same location relationship; whether it is the same community relationship; the ratio of the sum of the transaction weights of the previous successful transactions of the corresponding interaction node to the sum of the transaction weights of all the transactions. The middle hidden layer is set as three layers: the first layer has 32 units; the second layer has 64 units; the third layer has 16 units. The final output value is the trust evaluation value of the predicted target node.

The social relationship can be expressed as a combination of numbers. For example, they are not only friendship relationship, but also the same location relationship and the same community relationship, which is recorded as 111. Therefore, after a number of random interactions to obtain training set data, all relationship node pairs with social relationships of 111, 110, 101, 100, 011, 010, 001 and 000 can be obtained. We record the ratio of the sum of the transaction weights of these nodes for the first three successful transactions to the sum of the total transaction weights of these three transactions (since the cold start problem often occurs between nodes with less interaction experience, set three times as training set data here), and use this ratio as the fourth input factor of the deep learning model. Finally, the simulation results including the trust value evaluation of the target node are input into the deep learning model shown in Fig. 1, and the model results are trained.

Table 2 shows the parameters of deep learning model:

Table 2. The parameters of training deep learning model

Machine memory	16.0 GB
Computer system	Win 10
Video card	GTX1060
Python version	3.7.4
Pytorch version	1.3.1
Hidden layers of deep learning model	3
The number of units in each hidden layer of deep learning model	32,64,16
Learning rate	0.1

In this model, a total of 100 groups of data of different social relationship node pairs are collected, of which 90 groups are training sets and 10 groups are test sets. The training process of deep learning model is about 5 s.

Through this model, the SIoT server can predict the trust value of the service requester node to the target node in the corresponding environment. In order to make the simulation results clear, when a new node is set to join the community, the service requester can request several services from it (take three times as an example). Then, by providing the corresponding input data for the prediction of deep learning model to the SIoT server, the service requester gets the trust value evaluation of the new node and saves it in its own log. In this way, the service requester node can have the corresponding trust value evaluation even in the face of unfamiliar nodes with poor interaction experience, so that the node with the highest trust value can be directly selected for transaction.

4 Simulation Analysis

In this simulation, the given service requester node is always in good condition. In addition to this node, the state of each other node is dynamic (in the simulation of this paper, there are only two states: good and malicious).

The simulation initially set 40 nodes, 4 different communities, 4 different locations and 4 different owners. The network topology is set in advance, and the ownership relationship, location relationship and community relationship are all randomly selected.

Before each transaction, the service requester randomly selects one of four task types from 1 to 4 and requests services from the relevant interested communities. After randomly selecting the service provider node with the highest trust value of all nodes in the interested community, we start the task of randomly selecting transaction factor as h (the value range of h is (0,1). The larger the value is, the more important the transaction is).

This paper takes dense network as an example. Due to the intensive transaction of nodes in the dense network, there may be too much network load and unsuccessful transaction. The success rate of transaction between nodes is set as 80%.

We do 20000 random transactions and all 40 nodes are good at the beginning. With the increase of interaction times, good nodes become malicious nodes at random, and the number of malicious nodes increases at a constant rate.

Trust value transfer is involved in indirect trust value calculation, and transitivity is one of the controversial properties in trust management related research [8]. At the same time, it has been proved in the simulation analysis of [14] that the use of higher λ value in trust value evaluation can help nodes quickly converge to the real node state. On the other hand, malicious nodes should not rely on their good history to conduct improper behavior, so when new transaction occurs, the proportion of old transaction should be reduced. Overall, this paper considers that the trust value of indirect trust is less reliable than that of direct trust, and in order to compare the simulation results with the model in [14] more clearly, so we use the same weight parameters as the model in [14]: the initial values of parameters λ and δ are set to 0.8.

In this paper, we select two nodes with node numbers of 5 and 22 (set both nodes as good nodes), that is, in 20000 random transactions, only the transaction events of node 5 and node 22 are recorded. In the low malicious node proportion environment (malicious node proportion is 20%) and high malicious node proportion environment (malicious node proportion is 80%), the node-level trust model in [14] is compared with the node-level trust model in this paper. The simulation results are as follows:

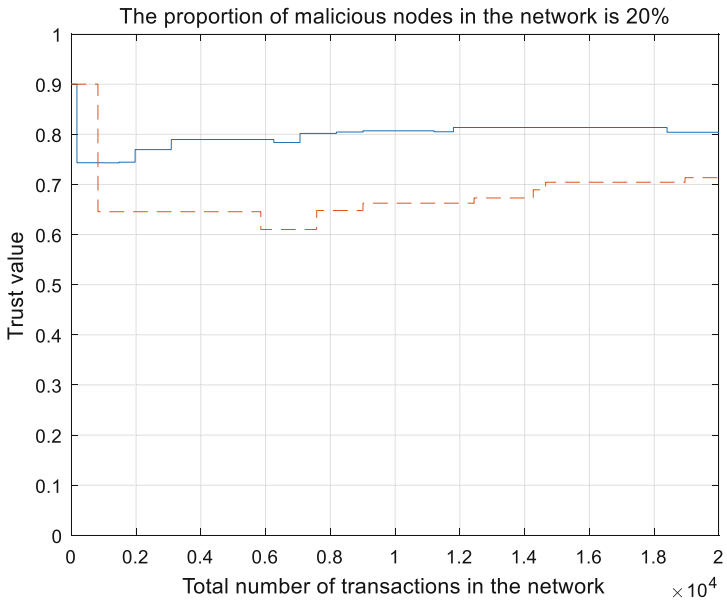

Fig. 2. Comparison of trust values at node-level between two models under the proportion of 20% malicious nodes.

The dotted line in Fig. 2 represents the node-level trust value in the model of [14], and the solid line is the model in this paper. As can be seen from Fig. 2, because the model in this paper gives weight to the trust value of the recommender, the trust value of the good nodes is higher than that of the model in [14] in most simulation time when the proportion of malicious nodes is not very high. A higher trust value also makes it easier for the service provider node to be selected as the next service provider.

The dotted line in Fig. 3 represents the node level trust value in the model of [14], and the solid line is the model in this paper. It can be seen from Fig. 3 that when the proportion of malicious nodes increases to a certain extent, because the indirect recommendation of node-level trust value in the model of [14] is only a simple average of the sum, so when the malicious recommendation increases, the trust value evaluation of a good node to another good node may appear a distrust state of less than 0.5, which makes the good node face the risk of being kicked out of the community and blacklisted by the community administrator. However, the trust model in this paper can still maintain a high level of trust value in the high proportion of malicious nodes.

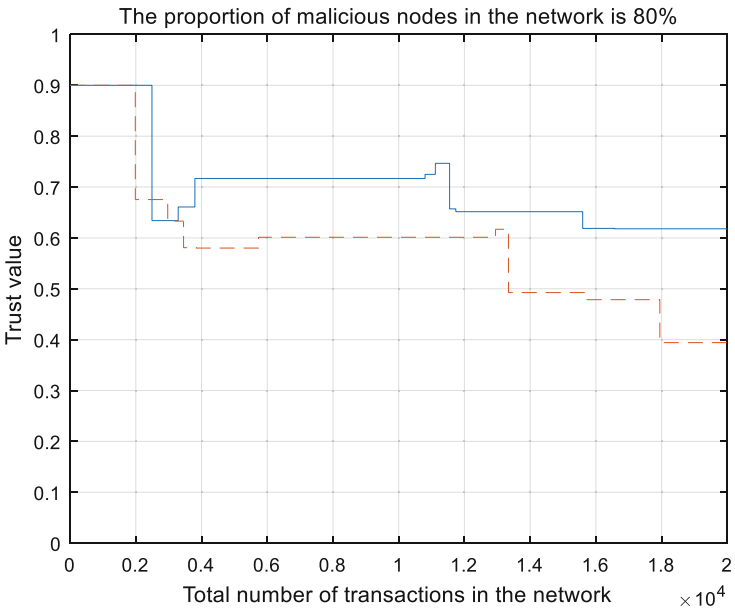

Fig. 3. Comparison of trust values at node-level between two models under the proportion of 80% malicious nodes.

The combination of Fig. 2 and Fig. 3 shows that the node-level trust model in this paper has better protection against malicious recommendation attacks from malicious nodes.

As described in Sect. 3, 10000 transactions are performed as a training set before the simulation starts. In the beginning of the formal simulation, all malicious nodes are initially set up because the malicious nodes have been generated in the training set collection process. New nodes are added to the model in this paper and the model in [14] at the same time to observe the trust evaluation of good nodes to new nodes. Take the proportion of 20% malicious nodes and 80% malicious nodes in the network as an example, we simulate the trust value calculation under the two models. In the simulation, we ensure that in different models of the same transaction, there is the same transaction factor and interested community selection. After each transaction, if the transaction evaluation is successful, it will be recorded as 1; if not, it will be recorded as 0. Count the total number of successful and failed transaction.

We set the node No. 5 and the newly added node as good nodes, and record the trust evaluation of node No. 5 to the new node in the simulation. After 20000 transaction experiments, the comparison results of the two trust models are shown in Fig. 4 and Fig. 5.

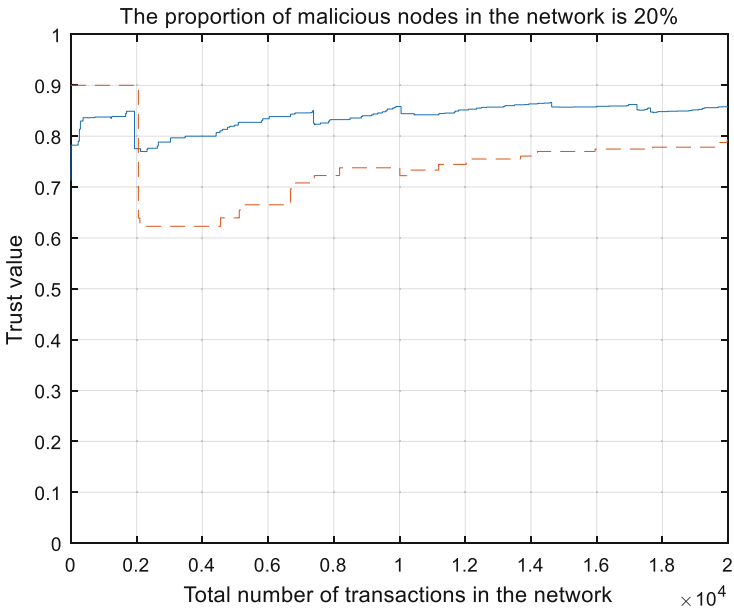

Fig. 4. Comparison of trust values between the two models under the proportion of 20% malicious nodes.

In Fig. 4, the solid line represents the trust value evaluation of the good node to the newly added good node in this model, and the dotted line represents the trust value evaluation of the good node to the newly added good node in the model of [14]. As can be seen from Fig. 4, the trust model in this paper has good trust value prediction, and always selects the node with the highest trust value as the service provider, so after the good node joins the community, it has more opportunities to provide tasks. Providing more good services in Fig. 4 shows that the trust value of the solid line can quickly converge to a higher value, and in most of the transaction process, the trust value evaluation is higher than the dotted line. According to statistics, the total number of successful transactions and failure transactions of this model in this simulation is 12016 and 801; the total number of successful transactions and failure transactions of the model in [14] is 10825 and 1950 (the sum of the number of successful transactions and the number of failure transactions is less than 20000, because when a malicious node requests a service from a good node or other malicious node, the service evaluation given is a fixed value of 0 or 1, regardless of whether the service is good or bad). The number of successful transactions of the model in this paper is significantly higher than that of the model in [14], and the number of failures is also much lower than that of the model in [14].

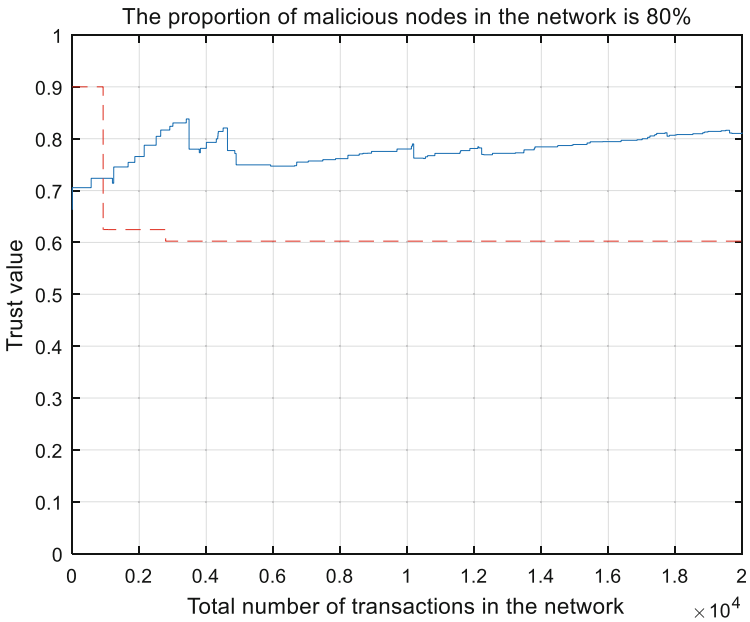

Fig. 5. Comparison of trust values between the two models under the proportion of 80% malicious nodes.

In Fig. 5, the solid line represents the trust value evaluation of the good nodes in this model to the newly added good nodes, and the dotted line represents the trust value evaluation of the good nodes in the model [14] to the newly added good nodes. Comparing Fig. 4 and Fig. 5, the trust model in this paper achieves a high trust value evaluation in the case of a high proportion of malicious nodes, although the trust value evaluation is slightly lower than that in the case of a low proportion of malicious nodes. In the model of [14], malicious recommendation attacks increase due to too many malicious nodes. After the newly added good node completes several transactions, the good node is kicked out of the community due to the malicious recommendation of other malicious nodes in the same community. Therefore, the trust value evaluation maintains the trust value state before being kicked out of the community after several transactions, which is the straight line in the Fig. 5. According to statistics, the total number of successful transactions and the total number of failed transactions in this model are 2420 and 683 respectively. In the model of [14], the total number of successful transactions is 1817, and the total number of failed transactions is 1422. Compared with the low proportion of malicious nodes, the number of successful transactions in the model of [14] is more less than that of the model in this paper.

The model in this paper always selects the node with the highest trust evaluation value for transaction, so good nodes in the model can get more transaction opportunities compared with the [14] model. The more transactions good nodes participate in, the higher the probability of successful transactions. At the same time, because the node with the highest trust evaluation value is always selected to transaction in the

model in this paper, it is difficult for the malicious node to appear as the service provider node after obtaining a low trust evaluation value. At this time, the malicious nodes have to quit the community, and because of the "blacklist" system in the administrator and SIoT server, such malicious nodes will have no chance to join the original community. At the same time, for some malicious nodes that may become good nodes, the system in this paper's model also gives them opportunities to transaction instead of directly kicking them out of the community as in the model [14].

5 Conclusion

This paper presents an improved trust prediction model for social internet of things. In view of the "cold start" problem that may occur in the networks with large delay, which may affect the trust value evaluation of new nodes due to the low communication success rate, this paper innovatively proposes the application of deep learning model in the SIoT server-level trust model to evaluate and predict the trust value of corresponding nodes, so that the good nodes can identify the new nodes with good trust value evaluation faster. It can effectively reduce the impact of malicious attacks from malicious nodes. Simulation results show that this model can effectively deal with the network with high proportion of malicious nodes.

Acknowledgements. This work was supported by the Beijing Science and Technology Project (No. Z191100001419001), Key Laboratory of Modern Measurement & Control Technology, Ministry of Education, Beijing Information Science & Technology University(No. KF202011 23202), Shipei Plan of Beijing Information Science & Technology University (2020), Beijing Excellent Talent Support Program (No. 2016000026833ZK08), and Support Plan for the Construction of High Level Teachers in Beijing Municipal Universities (No. CIT&TCD201704065).

References

1. French, A.M., Shim, J.P.: The digital revolution: internet of things, 5G, and beyond. Commun. Assoc. Inf. Syst. **38**(1), 840–850 (2016)
2. Militano, L., Araniti, G., Condoluci, M., Farris, I., Iera, A.: Device-to-device communications for 5G internet of things. http://www.researchgate.net/publication/283327011. Accessed 2015
3. Guinard, D., Fischer, M., Trifa, V.: Sharing using social networks in a composable Web of Things. In: Proceedings of the Pervasive Computing and Communications 2010, pp. 702–707, Mannheim, Germany (2010)
4. Atzori, L., Iera, A., Morabito, G., Nitti, M.: The social internet of things (SIoT) - when social networks meet the internet of things: concept, architecture and network characterization. Comput. Netw. **56**(16), 3594–3608 (2012)
5. Ortiz, A.M., Hussein, D., Park, S., Han, S.N., Crespi, N.: The cluster between Internet of Things and social networks: review and research challenges. IEEE Internet Things J. **1**(3), 206–215 (2014)
6. Mi, B., Liang, X., Zhang, S.: A survey on social internet of things. Chin. J. Comput. **41**(7), 1448–1475 (2018)

7. Geoffrey, H.: Deep learning—a technology with the potential to transform health care. JAMA J. Am. Med. Assoc. **320**(11),1101 (2018)
8. Nitti, M., Girau, R., Atzori, L.: Trustworthiness management in the social internet of things. IEEE Trans. Knowl. Data Eng. **26**(5), 1–11(2014)
9. Eleftherios, K., Orfefs, V., Theodora, V.: TRM-SIoT: a scalable hybrid trust and reputation model for the social internet of things. In: 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA), pp. 1–9, Berlin, Germany (2016)
10. Sherif, E.A.R., Ayman, A., Mohamad, A.: CBSTM-IoT: context-based social trust model for the internet of things. In: 2016 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT), vol.1, pp. 1–8, Cairo, Egypt (2016)
11. Saied, Y.B., Olivereau, A., Zeghlache, D., Laurent, M.: Trust management system design for the internet of things: a context aware and multi-service approach. Comput. Secur. **39**(B), 351–365 (2013)
12. Chen, I.R., Bao, F., Guo, J.: Trust-based service management for social internet of things systems. IEEE Trans. Dependable Secure Comput. **13**(6), 684–696 (2016)
13. Carminati, B., Ferrari E., Viviani, M.: Security and Trust in Online Social Networks. Morgan & Claypool, San Rafael (2013)
14. Oumaima, B.A., Mohamed, H.E., Leila, S.: TMCoI-SIoT: a trust management system based on communities of interest for the social internet of things. In: 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 747–752, Valencia, Spain (2017)