Available online at www.ijpe-online.com

International Journal of Performability Engineering

vol. 14, no. 3, March 2018, pp. 453-462
DOI: 10.23940/ijpe.18.03.p6.453462

Trust Authorization Monitoring Model in IoT

Ruizhong Du[a,b], Chong Liu[a,b,*], and Fanming Liu[a,b]

[a]*Cyberspace Security and Computer College, Baoding, 071002, China*
[b]*Key Laboratory on High Trusted Information System in Hebei Province, Baoding, 071002, China*

Abstract

With strong heterogeneity and the limited computing ability of IoT nodes, this dissertation proposes a Trust Authorization Model based on detection feedback in IoT that is combined with the current trust model of IoT as well as implement storage and other tasks. By calculating and storing the cluster head node along with its strong ability to facilitate the data transmission and search for energy consumption, it prevents the local network from being limited by the computing power of the device. In terms of trust calculation, the threshold value is based on the recommendation. At the same time, the BP neural network algorithm with self-learning function is periodically detecting the interactive data stream, detecting the attack nodes, quickly implementing the response measures, and meeting the actual situation of unmanned IoT of mass devices. Simulation results show that this model has lower energy consumption than other similar models, has good coping ability for attacks such as malicious recommendation and malicious slander, and has a higher detection rate and response rate to attack nodes.

Keywords: Internet of Things; BP neural network; trust evaluation

(Submitted on December 23, 2017; Revised on January 27, 2018; Accepted on February 24, 2018)

1. Introduction

Internet of Things is an important stage in the development of information age. With the continuous improvement of the level of social information, individuals and even countries have paid more attention to them. Because of huge market demand and broad prospects for its development, the Internet of Things is regarded as the next trillion-level market opportunity. Presently, many countries in the world also attach great importance to the Internet of Things such as the Japan's "wisdom earth", America's "IJPN", and the EU's "Internet of Things Action According to expert estimates, billions of devices will be connected to the Internet over the next few years" [2]. Furthermore, there are two main methods to ensure the security of perceived information: one is used by the similarity of perceptual nodes to deal with multiple data so that it eliminates false information sent by malicious nodes. The other is to ensure the authenticity of raw data and use data encryption authentication to guarantee data security [5,9]. Traditional secure authentication methods and commonly used encryption calculation are too complicated for limited resources and large-scale deployment of IoT devices [11]. In addition, these complex encryption methods consider IoT as a heterogeneous network with the feature of multiple fusion.

This model adopts the idea of a decentralized trust model. However, considering the weak computing characteristics of general nodes of IoT, the functions of trust computing and storage are given to edge devices or devices with higher computational capabilities, reducing the overall energy consumption. This gives the whole system more scalability and robustness. Massive IoT devices will be difficult to manage directly. In this model, the dynamic threshold adjustment automatically reduces the manual intervention and attacks on IoT devices using BP neural network. Learning attacks on the data stream testing, the network structure is more intelligent and automated.

2. Related Work

The traditional authorization mechanism mainly relies on the access control list and the IoT keeps deploying new devices on

* Corresponding author.
E-mail address: 273647459@qq.com

a large scale that cause devices to be very difficult for unfamiliar nodes to establish related links. Thus, it is not very suitable for establishing or maintaining complex tasks. The trust strategy in this domain is difficult to support across domains, which is bad for multi-network convergence and heterogeneous IoT. The centralized structure is vulnerable to attacks and paralyzes the entire network. Trust-based authorization connects unfamiliar nodes with each other through the recommended mechanism and continuously expanding the trust domain. The distributed architecture also makes the network less prone to single point of failure.

Currently, there has been some research on the trust evaluation mechanism under the Internet of Things. Chen [4] and his colleagues proposed a trust management protocol for IoT devices, and conducted trust evaluation using trustworthiness, interaction and domain preferences as parameters. Nitti et al. [10] put up a trust model that took into account the subjectivity and objectivity of SIoT (Social Internet of Tings), using the historical record of itself and neighboring nodes to calculate the trust of the trustee. This model used global feedback records to calculate trustworthiness to reflect the objectivity of the model. However, it neglected the reliability of the recommended data of neighboring nodes and was prone to malicious recommendation. [14] It proposed a distributed dynamic trust management model that considered trust reliability. The use of reliability to assess the degree of trust reduces the impact of malicious recommendation data to a certain extent. However, a large number of nodes with weak computing power in the Internet of Things environment are not suitable for P2P trust calculation, transmission and storage mode. Some devices may not operate normally. H. Xu [13] conducted his research on the structure characteristics of IOT, adopting the clustering structure in the IoT perception layer, evaluating the trustworthiness of nodes by predicting the interaction possibility of nodes, reducing the energy consumption and solving the problem of the weaker node. But, he did not settle down the corresponding resistance for malicious nodes.

Behavioral testing is the result of trust assessment and decides whether to authorize the interaction. It is not only used to consider the detection rate, but also to make the entire system in line with the structural characteristics of the Internet of Things. Bao [1] and others proposed a trust evaluation model based on intrusion detection to achieve dynamic detection of node behaviors. W. M. Liu et al. [8] proposed a hierarchical trust structure of the perception layer under the Internet of Things (IoT) environment. Based on the evidence theory, the trust of dynamic motion readers was deduced, which has the ability to detect the malicious nodes. The detection process does not consider the IoT node computing power requirements and low energy consumption. These complex algorithms for the introduction of new equipment are not friendly. B. B. Liu et al. [7] put forward a trust evaluation model and anomaly behavior detection algorithm based on node behavior detection for Internet of Things (IoT). Three kinds of trust factors are used to evaluate the trust behavior of nodes to avoid the malicious behavior of abnormal nodes in a relatively short period. But, it is still the overall evaluation conducted after the end of the interaction. It does not have the capability of real-time detection and cannot adopt appropriate security policies in time for obvious attacks. Zeehan Ali K [15] proposed a distributed intrusion detection mechanism based on IoT node trust. For IoT nodes under Low Power Lossy Routing Protocol (LLP), DODAG The Destination Oriented Directed Acyclic Graph node establishes a trust relationship with the neighbor node and uses the Josang subjective logic model [6] to evaluate the trust to guide the network to establish the interaction relationship.

In this paper, we propose a strategy model for the IoT infrastructure with weak computational power, multi-network convergence and large-scale features, adopt a clustering mechanism based on the limited resources of IoT nodes, and transfer most of the computational and storage burden to Cluster head node, making the whole network no longer limited by some computing power of weak equipment, giving it more scalability. For massive IoT devices in the absence of supervision, we propose a dynamic trust computing algorithm through automatic change of the threshold and weight to get the trust according to the actual situation, use the feedback neural network algorithm to periodically detect the interactive data stream and feedback the output to the trust database, and detect the attacking nodes and quickly implement the response measures.

3. Trust authorization model based on test feedback

3.1. Model design

Nodes in the IoT environment are quite different from the nodes in the previous distributed system. IoT nodes contain a wide range of sensor devices. Different device nodes generally have different computing, storage and communication capabilities. Those intelligence nodes and man-hour nodes are small. For these reasons, some of these nodes need to be satisfied with some additional requirements. It is particularly important to propose a more specific trust evaluation model for the Internet of Things. Since the user is unfamiliar with the sensor node, this node may be a safety hazard. To some extent, this problem can be resolved by building a trust model. The model described in this paper takes into account the heterogeneity of the network and the limited resources of the nodes. A clustering method is adopted to divide the network into several sub-areas according to the coverage of numerous management nodes. The transfer of trust values within and between clusters is the responsibility of the cluster head, and the trust information is passed to the trust management center.

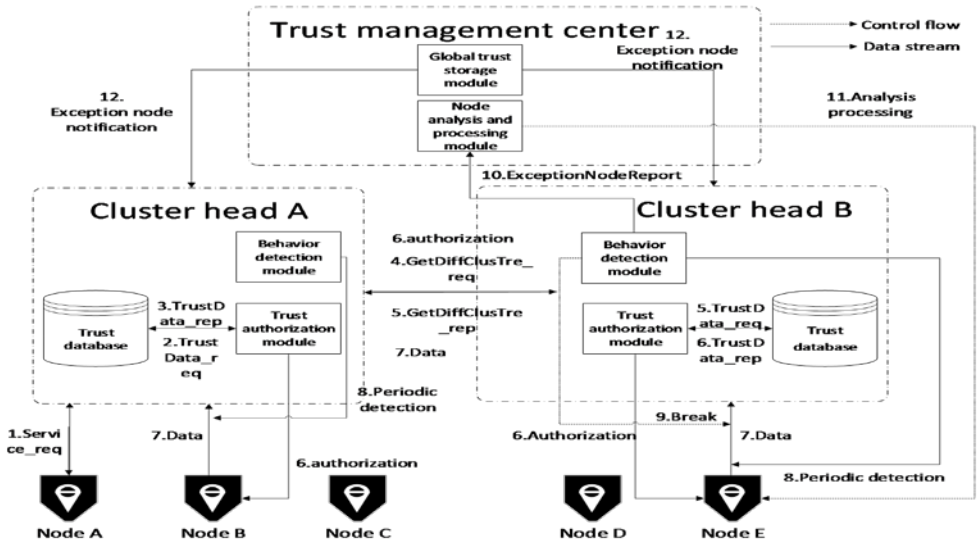

Figure 1. System flow chart based on trust model with feedback detection

Cluster nodes: In the Internet of Things, a series of intelligent sensing devices with computational processing capabilities and self-response capabilities generally have lower computational power.

Cluster head nodes: In the cluster with high computing power and credibility, maintenance of cluster trust list and the BP neural network detection results feedback update the list, which is the core node in the cluster.

Domain Trust management center: Comprehensive management and record of trust data is in this domain. The domain trust management center is a trusted anchor. The trust management center includes the global trust storage module, which keeps trust information of network nodes in the entire domain. It is generally held by the base station and other advanced network facilities.

By weighting the current trustworthiness weighted by the interactive history and the recommendation information of other nodes, it grants different authorities according to the trusting decision, classifies them through the trained neural network in the interaction process, and continuing the interaction by judging if the traffic is normal. Else, the classification is attacking traffic responds to the penalty policy, immediately disconnecting the link, setting the Flag of this node to 0, and provides a detailed report to the Trust Management node for processing. The physical structure of this model is shown in Figure 1, where node A is the service requester, nodes C and D are nodes that have been eliminated without exceeding the threshold, B and E are the nodes that are selected for interaction, and E is interacting. The process of sending malicious data stream was detected.

Traditional detection methods of intrusion detection system do not apply to the large-scale, heterogeneous IoT network. In this paper, we present a model of IoT based on trusted authoritative choice of nodes and mutual trustworthiness detection. According to historical mutual trust and recommendation trust, dynamic selection of authorization is carried out by periodically checking the behavior of authorized nodes. If the node behavior exceeds the specified threshold, the abnormal response measures will be executed in time. The model described in this paper has the characteristics of a fast response, friendly sensor nodes with low computational power and a certain degree of resistance to IoT internal attacks (such as DDoS attacks).

3.2. Trust authorization

When the core information management center of the Internet of Things receives the service request sent by the user, it sends the request data to the subordinate management node, and then the subordinate proxy node selects and authorizes the sensor node according to the personality of the service type. For the purpose of this trust management module, the basis of authorization is the assessment of trust. These include two types of trust factors - historical statistics trust value and recommended trust value. Through the weighted synthesis of two types of trust factors, the static trustworthiness of this interaction is calculated and compared with the threshold to decide whether to authorize or not.

- Historical statistics trust calculation.

The historical trust calculation is to directly evaluate the direct trust of the target node according to the historical interaction record stored by the local database of the trust management node. Each trust management node maintains a history

table that holds the history of trusts. In the mathematical expression of this model, the time decay function is used as the weight of the historical interaction trust. The trustworthiness value for the node after the previous interaction is recorded by the composite trust record. The address information of the interaction node is used to provide an addressing basis for the second phase of the trust evaluation - the response scheme of the node behavior evaluation. The trusted behavior detection module will be described in detail.

Step1: Read the history trust sequence stored locally in cluster head Q_{all}. Here, it is assumed that Q_b is the trust history of the target node B. $Q_b = \{q_1, q_2, q_3, ..., q_{dn}\}$, n is the number of historical interactions. One of the elements q_i (i> n) contains the flag, time, comprehensive trust and address information of the interactive node.

Step2: Check whether the flag of q1 is 0. 0 indicates that the trust management center has not processed the abnormal node; if so, discard the node directly. If not 0, then continue.

Step3: Attenuate and synthesize for each node. Decay degree by the time function $\theta(t) = Q_t + e^{-N_t(t-t_i)}$ represents, where Q_t and N_t is greater than 0 parameters, according to the degree of the specific application to determine. t is the current time and t_i is the time when hi is recorded. If the flag = 0.5, do not participate in the synthesis of the attenuation of the calculation. It belongs to the node behavior abnormal record and implements the corresponding punishment mechanism.

In conclusion, the historical comprehensive trust of node A to node B is as Equation (1).

$$T^{his}(A \to B) = \sum_{i=1}^{n} \frac{\theta(t_i)}{\sum_{j=1}^{n} \theta(t_j)} hist_i, n > 0 \tag{1}$$

Where $hist_i$ represents the history of the first i stored time trust. When there is no interaction between the local record, n = 0, $hist_i$=0.5. It means that they trust and distrust the unfamiliar node. To a certain extent, this is similar to that of human society.

- Recommendation trust.

Our model is based on the clustering trust. All cluster heads form the upper nodes, and the cluster heads store the reputation values and related parameters of the nodes in the cluster. As a reference data of authorized trust evaluation, recommendation trust can reflect the reputation of nodes more comprehensively and make the assessment results more reliable.

The recommended trust in the cluster: the subject node and the target node belong to the same cluster, and the subject node A records in the cluster head that there is too much or no interaction with the target node B. In this case, the cluster head node selects the nodes with higher credibility value to form the sequence $H^{rec} = \{h_1, h_2, h_3, ..., h_{rn}\}$, and H^{rec} satisfies the condition that there are many interaction records with the target node B. Recommended trust among the clusters: the subject node and the target node are in different clusters. The nodes in different clusters need to communicate with each other through the cluster head node. Therefore, compared with the recommended trust relationship in the cluster, the recommended trust relationship among the clusters has more of a relationship. That is, the mutual evaluation between the cluster heads of the two clusters.

Step1: The cluster head node chooses the recommended node in the cluster, and the recommended node C satisfies the following conditions: it has interacted with the main node A and has a high degree of trust and interacts with the target node B to record it. Step 2: Determine whether the target node B is in the same cluster as the principal node A. If you skip step 2 for the same cluster, you add the cluster trust value to the cluster node as the data for the recommended trust calculation. The trust transfer mode clusters with the main body of cluster nodes of the node in the cluster nodes as a new subject. Target node in the cluster of cluster head nodes as recommended. The corresponding data generation into the calculation formula of recommendation trust. Step3: According to the record, the recommendation sequence $H_{rt} = \{m_1, m_2, m_3, ..., m_{rn}\}$ of the recommended node C for the target node B is selected, where r_n is the recommended node number, where m_i is the corresponding recommended node to the target node. The recommended trust is $0 < i < r_n$. Taking the recommended node C as an example in the cluster, the formula for calculating the mi corresponding to the recommended node C is as Equation (2).

$$m_i = T_i^{his}(A \to C) \times T_i^{his}(C \to B), 0 < i < m \tag{2}$$

Step4: Aggregate the recommended trust values provided by each recommended node to obtain a recommended trust value. Because T^{rec} is formed by aggregating multiple recommended nodes, deliberately raising or degrading the target node in consideration of existence of a malicious node forms a collaborative fraud. This model reduces the influence of outlier nodes on trust evaluation by using the expectation of actual trustworthiness and the dispersion of actual value as the weight of the recommendation trust. It is almost impossible for most recommended nodes to be malicious nodes. The formula is as Equation (3).

$$T^{rec}(A \to B) = \sum_{i=1}^{rn} \omega_1 \times m_i, 1 < i < m \tag{3}$$

Where ω_i is the lazy degree of the recommended trust provided by the i-th recommendation node and the expected overall recommendation trust, and as the weight in the formula (3). $E_r(m_i)$ is the mathematical expectation of overall recommendation trust. The formula is as Equation (4).

$$\omega_i = \frac{\left|E_r(m_i) - m_i\right|}{\sum_{i=1}^{rn}\left|E_r(m_i - m_i)\right|}, E_r(m_i) = \frac{m_1 + m_2 + ... + m_{rn}}{rn}, 0 < i < m \tag{4}$$

- Authorization response

The weight of the historical statistical trust value and the recommended trust value T^{rec} can be combined to obtain the authorized trust value T^{aut}, which is compared with the preset threshold value to obtain the decision of whether to grant authorization to the target node B for interaction. The ∂ represents the historical statistical trust weight, which is obtained by the formula Equation (5).

$$T^{aut} = \alpha T^{his} + (1-\alpha)T^{rec}, \alpha = \frac{\frac{1}{D_h(hist)}}{\frac{1}{D_h(hist)} + \frac{1}{D_r(m)}} = \frac{D_r(m)}{D_h(hist) + D_r(m)} \tag{5}$$

$D(x)$ is the variance function, which is used to represent the degree of dispersion of the data. In our model, the variance function of historical statistics trust and recommended trust reflects its degree of dispersion as the reliability of data to dynamically adjust the weight factor. If the historical statistical trust dispersion is large, then the recommended trust occupies a greater proportion. If the recommended trust dispersion is larger, then there is a greater share of historical trust.

3.3. Trusted behavior Detection

When the node is authorized, both parties begin to interact. However, it is not always reliable to judge the trustworthiness of a node only through previous interaction records. Therefore, our model proposes a trust evaluation model of static history and dynamic traffic behavior analysis combined with interactive data authorization.

- Node Trusted Behavior Detection Based on BP Neural Network.

In this paper, an artificial neural network based on BP algorithm is adopted to analyze and classify the collected data traffic so as to detect the attack data stream in time. BP neural network is a multi-layer feedforward neural network. The main characteristics of the network is the signal forward and the error backpropagation. If the output layer cannot get the desired output, it will go back to the second part to propagate backwards. According to the error, the weight and threshold of the whole network are adjusted so that the predicted output keeps close to the expected output.

Suppose that the vector $X = \{x_1, x_2, ..., x_n\}$ is the input vector of the BP neural network. $Y = \{y_1, y_2, ..., y_m\}$ is the output vector of BP neural network. w_{ij}, w_{jk} represents the connection weight between the input layer, hidden layer and output layer neuron nodes. We adopt a supervised learning method by first selecting a large number of suitable training samples to train BP neural network. As the way of network attacks evolves and the number of Internet of Things nodes is huge and heterogeneous, the BP network continuously classifies and discovers the abnormal behavior discovered and updates its own anomaly information

database according to the abnormal information. In this way, under the background of continuous evolution and complexity, the BP network can also update its own trust evaluation system in time. By weighted calculation of the input information and bringing it into the activation function, the output value is finally obtained and the output value is compared with a preset threshold value. The malicious node is considered as a malicious node below the threshold value.

- Behavior Detection and Trust Assessment Module.

In order to meet the requirements of establishing a neural network model, first determine the number of hidden layers and nodes. If it is too small, then the linear function of the classification cannot meet the accuracy requirements. On the contrary, when the number of hidden nodes is too large, not only will the computing resource utilization rate increase exponentially, but the output randomness also increases. Therefore, we should find a way to choose a node with a common hidden layer. We propose using the empirical formula [12] to determine the number of neurons in the hidden layer. Empirical formula is a general formula proposed by researchers through a large number of experiments on hidden layer features. The formula is as Equation (6).

$$l = \sqrt{n \times m} + a \tag{6}$$

With l is the number of hidden layer nodes, m is the dimension of the input eigenvector, n is the dimension of the output layer, and a is an adjustment constant between 1 and 10. After setting up the network, we need to input the training samples to learn and get a model that can evaluate the trust of the sampled data streams. Select the k-th eigenvector group. BP neural network learning steps are as Equation (7).

Step1: Network initialization. The various connection weights in the interval [-1,1] were randomly assigned. Given a calculation precision value e and maximum number of learning M .

Step2: Select samples k and corresponding expected output as Equation (7).

$$\begin{aligned} X(k) &= (x_1(k), x_2(k), ..., x_s(k)) \\ d_o(k) &= (d_1(k), d_2(k), ..., d_q(k)) \end{aligned} \tag{7}$$

Step3: According to the input vector of X(k), the corresponding connection weights of $w_{ij,}$ hidden layer threshold calculation of hidden layer, and output of $ho_h(k)$. Where $f(\bullet)$ is the hidden layer excitation function to convert the linear relationship of the sample function $f(x) = \frac{1}{1+e^{-x}}$ to a non-linear relationship. This model uses the sigmoid function as the stimulus. The sigmoid function value range is [0,1], and is also in-line with the scope of the trust value.

Step4: Error calculation. According to BP neural network prediction output $y_o(k)$ and expected output $d_o(k)$ network prediction error e.

Step5: Weight update. Update network connection weights w_{ih}, w_{ho} based on prediction error e. Aiming at the shortcoming of slow convergence in BP neural network learning process, the additional momentum method is used to accelerate the convergence of previous experience accumulation. The formula is as Equation (8).

$$w(t) = w(t-1) + \Delta w(t) + a[w(t-1) - w(k-2)] \tag{8}$$

Among them the $w(t), w(t-1), w(t-2)$ respectively were t, t - 1, and the value of t - 2 times a is momentum vector.

For the weights between the hidden layer and output layer, use the partial derivative of output layer neurons of $\delta_o(k)$ and the output of hidden layer neurons to calculate the update as Equation (9)

$$\Delta w_{ho}(k) = \eta \delta_o(k) ho_h(k), \quad \Delta w_{ih}(k) = \eta \delta_h(k) x_i(k) \tag{9}$$

In order to solve the vector in the process of learning the oscillation of η leads to the problem of slow convergence speed and difficultly to stabilize. The variable vector learning algorithm is as Equation (10).

$$\eta(t) = \eta_{\max} - \frac{t(\eta_{\max} - \eta_{\min})}{t_{\max}} \tag{10}$$

The t is the current number of iterations, $t_{\max}$ is the largest number of iterations.

Step6: At this time, determine whether the network error meets the requirements and stop the iteration when the error reaches the precision or exceeds the maximum number of learning, and then end the algorithm; otherwise, return to Step3 for the next round of learning.

The network learning process is completed by the above steps. The network that has undergone learning and training has a higher capability of detecting malicious behaviors and can timely evaluate the behavior of the nodes. Because the sigmoid function has a value range of [0,1] and its function curve is a S-curve that better reflects changes in confidence. The output yo_o of the output layer is used as the trustworthiness of the trust assessment of the trusted activity detection module, and logs into the local trust database.

4. Simulation

In order to validate and evaluate the performance of the model in this paper, a simulation system of virtual IoT nodes based on Java language is established to further validate the model to adjust it. The experimental environment is as follows: Inter (R) Core (TM) i5-2400 @ 3.10GHz, 4GB RAM, 500GB hard drive.

4.1. Simulation of trust authorization module

According to the clustering-based hierarchical framework, the nodes in IoT are abstractly processed. To verify this model, four clusters, Cluster1 ~ Cluster4, are set up. Each cluster has 25 nodes, including cluster head nodes. Cluster interaction and trust assessment. According to the behavior characteristics of nodes, it is divided into three categories: NormalNode, MaliciousNode, and AttackNode. Normal node classes provide normal services, and malicious serving nodes are generally referred to the cluster of malicious nodes, including cluster heads, raising the trust of nodes in their own clusters and devaluating the trust of other cluster nodes. Attack node refers to a type of node that attacks user nodes in the process of interaction. In this paper, DoS attack nodes is an example for simulation experiments. The distribution of three types of nodes in the system is shown in Table 1. According to the function of nodes, it is divided into two categories: IntraClusterNode and ClusterHeadNode, in which the clusterhead node is responsible for maintaining a trust list including the trust between nodes and the nodes in the cluster.

The first type of malicious nodes (malicious service nodes) need to be protected from the level of trust authorization. Once the node is granted permission, the subsequent defense is difficult to detect legitimate data sent by legitimate nodes. The second type of malicious nodes (attack nodes) are mostly first through the legitimate authorization. In the interaction process and then attack, such attacks through the detection module can be more effectively detected.

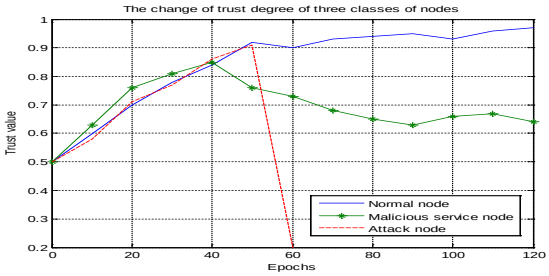

Figure 2. The change of trust degree of three classes of nodes

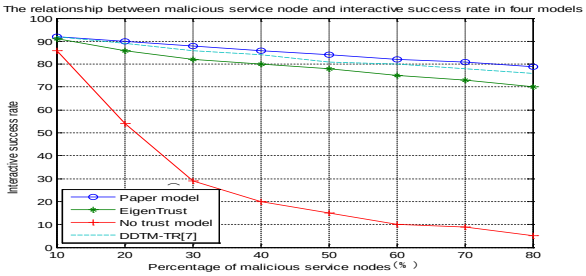

Figure 3. The malicious service node and interactive success rate

Figure 2 verifies the trustworthiness of the three types of nodes with the interactive cycle under the model in this paper. In the 120 interaction cycles, there is no periodic record. It can be seen that the interaction period of the first type of node is an upward trend, and its upward trend gradually becomes smaller and eventually approaches the maximum value of 1. The initial trust of the second type of nodes increases rapidly due to the cooperation and exaggeration. The trend of increasing

trust tends to be gentle because such nodes exaggerated the degree of trust and the quality of service cannot achieve a reasonable degree of trust, resulting in decreased overall trust. Although there is continued implementation of exaggerated strategy, the weight is smaller. The third type of node is similar to the first type of node at the beginning, but attack is detected in the 60th cycle, and the trust rate rapidly drops to the threshold (0.3) The following is therefore judged as attack nodes. Figure 3 describes the growth of malicious service nodes and interactive success rate changes. In contrast to the DDTM-TR model of the Eigentrust model and the literature [14], it is evident that the trust model has considerable advantages for the prevention of malicious service nodes. The interaction success rate of this model is higher than that of the EigenTrust model, and slightly higher than that of DDTM-TR. This is because the EigenTrust model relies excessively on subjective evaluation, and subjectivity is often not as accurate as expected. The model emphasizes the objectivity of the evaluation and avoids the selection of malicious service nodes by dynamically adjusting the weighting factors.

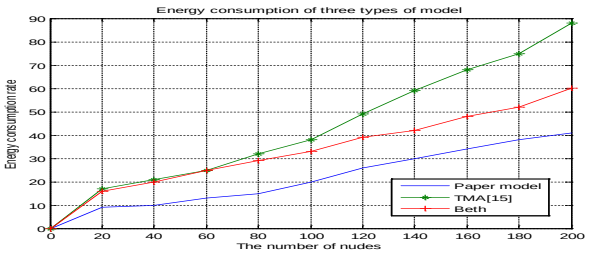

Figure 4. Energy consumption of three types of model

The main source of energy consumption for a typical trust assessment model is finding recommended trust data. Figure 4 shows the energy consumption of the model. The Beth model does not take into account the heterogeneity of the IoT network and the limited resources of most nodes, so the nodes uniformly store the recommended information. Some computing devices with low computing capabilities (such as cameras and thermometers) may cause node overload or even paralysis. Although the TMA model in [3] reduced the computational complexity compared with the Bath model, the common node is also regarded as the main body of the recommended trust, resulting in high overall energy consumption. It is unfriendly to some IoT nodes with low computational capabilities. The goal of the Internet of Things is the Internet of Everything, which is bound to develop into an unprecedentedly large network. For iterative methods, the consumption of computing resources will increase exponentially. In this paper, we transfer the trust storage and delivery tasks to the cluster head nodes with powerful computing ability. And, the number of cluster nodes can be dynamically allocated according to the different computing capabilities of cluster heads, which greatly reduces the computational overhead and enhances the robustness of the model.

4.2. Behavior simulation monitoring module

In order to verify the convergence of the detection rate and false detection rate of BP algorithm, some data in KDD CUP99 dataset are selected and brought into the algorithm. The matlab 7.0 is used to simulate the algorithm. In order to verify the relevance of the model, DoS attacks on the anomalous data types in the dataset include ping-of-death, syn flood, smurf and so on. The distribution of training sets and test sets is shown in Table 1.

Table 1. Table Type Styles

Attack type		DoS
Training set	Number	13485
	Species	syn flood, smurf and so on.
Test set	Number	29853
	Species	Apache2

The original 14 network parameters in the data set are abstracted and five categories including source IP, destination IP, packet length, sending interval and length change rate are selected. Therefore, only five nodes in the input layer are selected because only the detection of DoS attacks. So, the output layer 1 node, according to the formula (8), can be calculated:

Table 2. The Situation of Setting Training Parameter

Parameter name	Value
net.trainparam.show Display the result every many steps	50
net.trainparam.epochs Maximum allowed training steps	1000
net.trainparam.goal Minimum error of training target	0.01
net.trainParam.lr Initial learning rate	0.01

According to the initial parameter settings in Table 2, the convergence of the model detection algorithm in this paper is simulated and is compared to the traditional gradient descent algorithm and the momentum gradient descent algorithm. Figure 5 is the gradient descent algorithm learning process. Figure 6 is a momentum gradient descent algorithm learning process. It can be clearly seen that the learning algorithm in this paper (Figure 7) is more convergent. This is because the BP neural network algorithm in this paper takes the minimum time cost according to the specific conditions when choosing the hidden layer nodes. Moreover, the algorithm itself adopts the variable learning rate algorithm to solve the problem that the convergence speed is too slow to stabilize due to too small concussion.

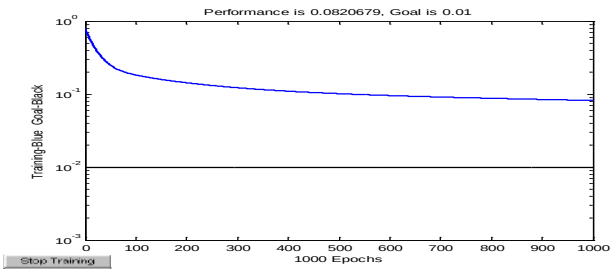

Figure 5. Convergence of gradient descent method

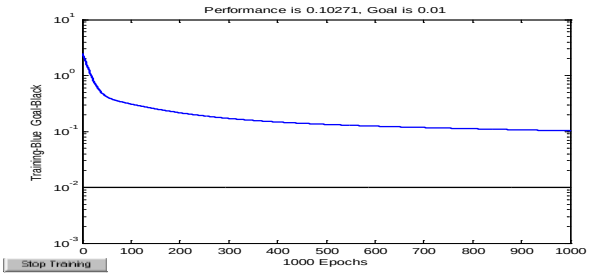

Figure 6. The convergence of the momentum gradient descent method

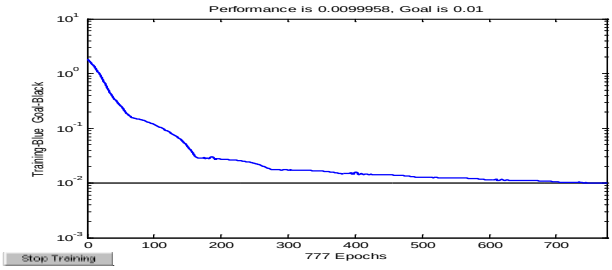

Figure 7. The convergence of the algorithm is studied in this paper

Table 3 lists the three kinds of algorithms of detection rate, false detection rate, and time consuming. Its computation formula is as follows:

Detection rate = number of correct detection/total number of samples is checked × 100%;

Error detection rate = inspection number/total number of samples by mistake × 100%.

Table 3. Comparison of Experimental Results

Learning algorithm	Detection rate（%）	False rate（%）
Algorithm	93.34	2.33
Momentum gradient descent method	87.02	4.27
Gradient descent method	80.53	7.56

Experimental results show (Table 3) the detection algorithm in this paper, and both detection rate and false positive rate have great advantages. This is because the detection algorithm dynamically sets the number of hidden layer nodes, reducing the time cost and improving the detection rate. The constant dynamic learning of a large number of training samples also improves the accuracy of the detection.

5. Conclusions

Based on the classic layered theory of IoT, this paper makes use of the topology of clustering to evaluate trust in the model of the whole network system by combining trust authorization detection and interactive abnormal behavior detection to achieve a secure, reliable network. In view of the heterogeneity and low power consumption of IoT nodes, the computational tasks are concentrated on cluster head nodes, which not only avoids the risk of single-point failure, but also increases the scalability of the network. In the trust and authorization module, in order to facilitate the management of a large number of IoT nodes, the algorithm objectivity is emphasized and the algorithm has some self-learning capabilities to deal with malicious recommendations. The behavior detection module, although experimentally demonstrated a good performance, only tested against DoS attacks. In fact, facing more kinds of attacks requires establishing more neural network nodes, which will greatly increase the computational complexity and in theory reduce the detection rate. The next research direction is aimed at the characteristics of IOT nodes, combined with the development trend of attack means, tailor-made targeted parameters and higher convergence learning algorithm.

References

1. F. Bao, R. Chen, M. J. Chang, et al. “Trust-based Intrusion Detection in Wireless Sensor Networks” [A]. 2011 IEEE International Conference on Communications (ICC)[C]. Kyoto, Japan, 2011.1-6.
2. K. Bloede, G. Mischou, A. Senan, and R. Koontz, “The Internet of Things,” Available at http://www.woodsidecap.com/wp-content/uploads/2015/03/WCP- IOT- M and A- REPORT- 2015-3.pdf, Last accessed:2016-10-27.
3. G. V. Crosby, L. Hester, and N. Pissinou, “Location-aware, Trust-based detection and Isolation of Compromised Nodes in Wireless Sensor Networks” [J]. International Journal Network Security, 2011, 12(2): 107- 117.
4. I. R. Chen, F. Bao, and J. Guo, “Trust-based Service Management for Social Internet of Things Systems,” IEEE Trans. Dependable Secur. Dependable Secur. Comput., vol. 5971, no. c, pp. 1–1, 2015.
5. X. H. Gong. “Research on Secure Clustering Mechanism of IoT-aware Nodes Based on Trust” [D]. Chongqing: Chongqing University of Posts and Telecommunications, 2014.
6. A. Jøsang, “A Logic for Uncertain Probabilities,” International Journal of Uncertainty, Fuzziness and Knowledge-based Systems, vol. 9, pp.279–311, 2001.
7. B. B. Liu, X. H. Gong. “Trust Assessment Method Based on IoT Node Behavior Detection” [J]. Journal of Communications, 2014,35 (5): 8-15.
8. W. M. Liu, L. H. Yin, B. X. Fang and so on.” Study on the Trust Mechanism Under the Internet of Things” [J]. Chinese Journal of Computers, 2012,35 (5): 847-855.
9. Y. B. Liu, W. P. Hu “Internet of Things Security Model and Key Technologies” [J]. Digital Communications, 010, 37 (4): 28-33,2010.
10. M. Nitti, R. Girau, and L. Atzori, “Trustworthiness Management in the Social Internet of Things,” IEEE Trans. Knowl. Data Eng., vol. 26, no. 5, pp. 1253–1266, 2014.
11. ROMANA. R, ZHOUA. J, LOPEZB. J. “On the Features and Challenges of Security & Privacy in Distributed Internet of Things” [J]. Computer Networks, 2013, 57 (10):2266-2279.
12. Srinivas Mukkamala, Andrew H. Sung. “Identifying Significant Features for Network Forensic Analysis Using Artificial Intelligent Techniques” [J], International Journal of Digital Evidence, Winter 2003,4:63-69.
13. H. Xu. “Research on the Trust Model of Internet of Things Based on Clustering” [D]. Lanzhou traffic University, 2017.
14. J. You, Shangguan Lun, Xu Shoukun, et al. “A Distributed Dynamic Trust Management Model Considering Trust Reliability” [J]. Journal of Software, 2017.
15. A. K. Zeeshan, H. Peter, “A Trust Based Distributed Intrusion Detection Mechanism for Internet of Things”, In 2017 IEEE 31st International Conference on Advanced Information Networking and Applications. IEEE, 2017, pp.1169-1176