Advances in Computer Science Research, volume 80

International Conference on Computer Science, Electronics and Communication Engineering (CSECE 2018)

IoT Node Trust Authorization Model

Ruizhong Du, Chong Liu* and Fanming Liu

Cyberspace Security and Computer College, Baoding 071002, China

Key Laboratory on High Trusted Information System in Hebei Province, Baoding 071002, China

*Corresponding author

***Abstract*—Aiming at the characteristics of strong heterogeneity and limited computing ability of IoT nodes, this dissertation proposes a Trust Authorization Model based on detection feedback in IoT, combined with the current trust model of IoT and implement storage and other tasks by calculating and storing the cluster head node with strong ability to facilitate the data transmission and search for energy consumption, and help the local network be not limited by the computing power of the device. In terms of trust calculation, the threshold value is based on the recommendation. 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; trust evaluation; cluster

I. 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 pay 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. At present, many countries in the world also attach great importance to the Internet of Things such as the Japan's "wisdom earth" American's "IJPN" and EU's "Internet of Things Action According to expert estimates, billions of devices will be connected to the Internet over the next few years [1].

The Internet of Things is an open, intelligent system where most nodes are unmanaged and vulnerable to malicious attacks, In another way, the external environment will damage the IoT devices as well as , the IoT nodes with single function and limited computing resources are easily invaded and become malicious nodes, which are hidden inside the IoT network ,launch internal attacks with legal status and cause serious security risks. In the Internet of Things, network attacks will not only cause property damage, but also threaten life. Therefore, it is particularly urgent and important to formulate a security strategy in favor of the IoT environment.

At present, 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 using data encryption authentication to guarantee data security[2,3]. Traditional secure authentication methods and commonly used encryption calculation are too complicated for limited resources and large-scale deployment of IoT devices [4]. In addition, these complex encryption methods considerIoT as a heterogeneous network with the feature of multiple fusion.

The model adopts the idea of trust model. And the trusted computing and storage functions are given to edge devices or devices with higher computational capabilities, reducing the overall energy consumption; the threshold dynamic adjustment reduces manual intervention and the network structure is more intelligent and automatic.

II. RELATED WORK

At present, there has been some research on the trust evaluation mechanism under the Internet of Things. Chen [5] and his colleagues proposed a trust management protocol for IoT devices, and conducted trust evaluation using the trustworthiness, interaction and domain preferences as parameters. Nitti et al. [6] 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 reflects the objectivity of the model. However, it neglected the reliability of the recommended data of neighboring nodes and was prone to malicious recommendation. [7] It proposed a distributed dynamic trust management model considered trust reliability. The use of reliability to assess the degree of trust, to a certain extent, reduces the impact of malicious recommendation data. 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, and some devices may not operate normally. Xu Huan [8] conducted his research on the structure characteristics of IOT, adopted the clustering structure in the IoT perception layer, evaluated the trustworthiness of nodes by predicting the interaction possibility of nodes, reduced the energy consumption and solved the problem of weaker Node, but he didn't settle down the corresponding resistance for malicious nodes. Liu Wenmao et al. [9] 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.

III. TRUST AUTHORIZATION MODEL

A. 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-hours 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.

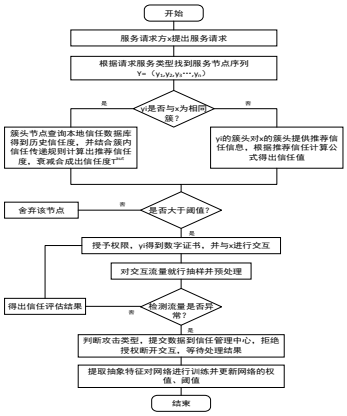

FIGURE I. SYSTEM FLOW CHART

(1)Cluster nodes: IoT composed of intelligent devices node with weak computing power .

(2)Cluster head nodes: Through the cluster head election algorithm, the nodes with strong computing power selected among cluster member nodes, Store and calculate the trust information of nodes in the cluster.

(3)Domain Trust management Center: comprehensive management and record of trust data 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.

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.

B. 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 subordinate proxy node selects and authorizes the sensor node according to the personality of the service type. For the purpose of this article Trust management module, the basis of authorization is the assessment of trust. These include two types of trust factors - historical statistics trust value, 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 The parameters include Flag, time, the corresponding historical trust and the address information of the interaction node (such as IPv6, EPC, etc.). For each time a node is selected, the local storage information is measured first, and if the flag in the latest interaction record is 0, the node is discarded directly. If 1 then continue to read the following information, its trust calculation. The time parameter is used to reflect the time decay of the data. The further the data is stored, the lower the reliability is. 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: Attenuate and synthesize for each node. Decay degree by the time function $\theta(t) = Q_t + e^{-N_t(t-t_i)}$ to represent, 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, ti is the time when hi is recorded.

In conclusion, the historical comprehensive trust of node A to node B is:

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

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

- recommendation trust.

Similar to the transmission of trust in human society, there also exists trust transfer and exchange between nodes in the Internet of Things, namely, recommendation trust. The model in this paper is based on the clustering trust model. 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 makes the assessment results to be more reliable. However, there are some safety issues in recommending trust, such as collaborative deception and malicious evaluation.

According to the cluster of the mutual nodes of both parties, it can be divided into a cluster recommendation and a cluster recommendation:

(1)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. Trust record in H_{rec} sequence as recommended trust data as $T^{rec}(A \to B)$.

(2) 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 a more relationship, that is, the mutual evaluation between the cluster heads of the two clusters.

From the above description, the recommended trust includes the following two cases:

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, if you add the cluster trust value to the cluster node as the data for the recommended trust calculation. The trust transfer mode between 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, formula 2 in step 3.

Step3: According to the record, the recommendation 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, $0 < i < r_n$. 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 follows:

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

Step4: Weightedly aggregate the recommended trust values provided by each recommended node initially 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 follows:

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

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), the weight of the outlier data in the recommendation trust can be reduced to a certain extent so as to reduce the malicious recommendation Impact.

$$\omega_i = \frac{\left|E_r(m_i) - m_i\right|}{\sum_{i=1}^{rn}\left|E_r(m_i - m_i)\right|}, \quad 0<i<rn \tag{4}$$

$E_r(m_i)$ is the mathematical expectation of overall recommendation trust.

$$E_r(m_i) = \frac{m_1 + m_2 + ... + m_{rn}}{rn} \tag{5}$$

- authorization response

The weight of the historical statistical trust value T^{his} 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 whether to grant authorization to the target node B for interaction.

$$T^{aut} = \alpha T^{his} + (1-\alpha)T^{rec} \tag{6}$$

The ∂ represents the historical statistical trust weight, which is obtained by the following formula:

$$\alpha = \frac{\frac{1}{D_h(hist)}}{\frac{1}{D_h(hist)} + \frac{1}{D_r(m)}} = \frac{D_r(m)}{D_h(hist) + D_r(m)} \tag{7}$$

$D(x)$ is the variance function, used to represent the degree of dispersion of the data. Weights α, the general trust model

often rely on expert experience, simulation results and other means to determine the results of this often lack the scientific, agile and adaptive. In this paper, 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 to be large, then the recommended trust occupies a greater proportion. If the recommended trust dispersion to be larger, then there is a greater share of historical trust.

IV. SIMULATION

The experimental environment is as follows: Inter (R) Core (TM) i5-2400 @ 3.10GHz, 4GB RAM, 500GB hard drive.

In this paper, we design five sets of experiments to verify the relationship between trustworthiness and interaction rate, the relationship between mutual success rate and the proportion of three types of nodes.

C. 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 two categories: normal node, malicious node. Normal node classes provide normal services, and malicious serving nodes are generally Refers 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. 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 initial trust of nodes are all 0.5, the normal node is used to initiate the service request, the service nodes are selected in four clusters, and the interactive process is analyzed experimentally.

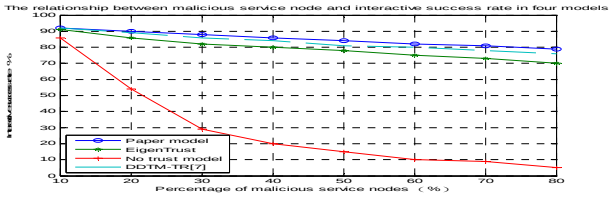

FIGURE II. THE RELATIONSHIP BETWEEN MALICIOUS SERVICE NODE AND INTERACTIVE SUCCESS RATE IN FOUR MODELS

Figure 2 describes the growth of malicious service nodes, interactive success rate changes. In contrast to the DDTM-TR model of the Eigentrust model and the literature [7], 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 EigenTrust model, 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. In addition, for over-dependent trust nodes, not only is there a risk of single point of failure but also for IoT nodes with limited computing power. There will be additional recommended trust overhead resulting in overloading. The model emphasizes the objectivity of the evaluation and avoids the selection of malicious service nodes by dynamically adjusting the weighting factors.

The main source of energy consumption for a typical trust assessment model is finding recommended trust data. Figure 6 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 that the nodes uniformly store and recommend the recommended information. For some computing devices with low computing capabilities (such as cameras and thermometers) May cause node overload or even paralysis. Although the TMA model in [11] 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 and 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.

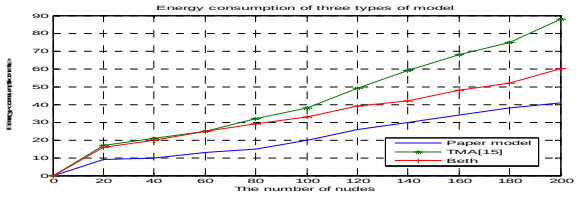

FIGURE III. ENERGY CONSUMPTION OF THREE TYPES OF MODEL

V. SUMMARY

Based on the classic theory of IoT, this paper regards trust as the basis of authorization and based on interaction records as the basis of trust evaluation to achieve a safe and 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 of failure but also improves the scalability of the network. Dynamic evaluation algorithms facilitate the management of a large number of IoT nodes and resist malicious recommendation attacks. The next research direction is for the characteristics of IoT nodes, combined with the development trend of attack means, customized custom parameters and higher trust evaluation algorithm.

REFERENCES:

[1] K. Bloede, G. Mischou, A. Senan, and R. Koontz, “The Internetof Things,”http://www.woodsidecap.com/wp-

content/uploads/2015/03/WCP- IOT- M and A- REPORT- 2015-3.pdf, Woodside Capital Partners,2015,accessed:2016-10-27.

[2] Liu yanbing, Hu Wenping. Internet of Things security model and key technologies [J]. Digital Communications, 010, 37 (4): 28-33,2010.

[3] Gong Xue Hong. Research on secure clustering mechanism of IoT-aware nodes based on trust [D]. Chongqing: Chongqing University of Posts and Telecommunications, 2014.

[4] 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.

[5] 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.

[6] 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.

[7] You Jing, Shangguan by Lun, Xu Shoukun and so on. A Distributed Dynamic Trust Management Model Considering Trust Reliability [J]. Journal of Software, 2017.

[8] Xu Huan. Research on the Trust Model of Internet of Things Based on Clustering [D]. Lanzhou Jiaotong University, 2017.

[9] Liu Wenmao, Yin Lihua, Fang Binxing and so on. Study on the trust mechanism under the Internet of things [J]. Chinese Journal of Computers, 2012,35 (5): 847-855.

[10] CROSBY G.V, HESTERL, PISSION N. Location-aware, trust-based detection and isolation of c ompromised nodes in w ireless sensor networks[J]. International Journal Network Security, 2011, 12(2): 107-117.