Research on the Application of Internet of Things based on Structural Data System Trust

Hean LIU
Hunan City University, Yiyang, Hunan, 413000, China

Abstract: In order to determine the conditions for the application of the dynamic authorization problem in the Internet of things, a reliable trust mechanism must be established between the institution, the reader and the tag. it proposes the improved method of evidence theory according to the characteristics of the readers, which can deduce the routing trust of the reader. The experimental results show that the hierarchical trust mechanism has a very good convergence of trust, and the algorithm in this paper can effectively detect the malicious terminal nodes.

Keywords: Node; Cluster; Things Network

1. Introduction

In the network system, in addition to the benign nodes, there may also exists some malicious nodes and selfish nodes, who try to interfere with the normal operation of the network. In order to obtain the reliable communication services and enhance the security of the system, researches of the subjective trust have been conducted in many areas, such as e-commerce, P2P network, etc. In recent years, the research of the trust model of the Internet of Things has also drawn more and more attentions. However, the traditional security algorithm is difficult to be applied to the dynamic network environment, and the main reason is that these algorithms are too complex. Therefore, the trust model becomes a powerful supplement to improve the security of the system.

In the reader network, there exist the phenomena of the increasing or decreasing or movement of a large number of nodes, while the identity- based method has the fixed structure and higher cost of computing, and the credibility- based method requires the subject to survive for a long time, thus both of them are not applicable to the dynamic environment. In the research of the ad-hoc network, the collaboration between the nodes is often adopted to update their trust values of each node, so as to eventually deduce the malicious nodes. Therefore, when the subject of the reader is evaluating the trust value of the object, it mainly investigate its behavior, this is why it is called the behavior- based trust. In the specific calculation of trust and the derivation process of the node status, there are a variety of models, such as the D-S evidence theory used in literature [1-3], The experiment in literature [4-6] shows that this kind of certainty in the rapidly changing network leads to the undesirability of the report rate of the malicious incident, and when the threshold value of trust is relatively small, the false positive rate of the malicious incident is relatively high, and the Bayesian prior probability and conditional probability need expert knowledge, and are often difficult to determine. In addition, the trust model based on entropy theory and the method based on cloud model both use the uncertainty to description trust, but is the trust path between the subject and the object is too long, the uncertainty will be amplified. Thus, both of them have slower convergence in the multistage trust chain, and the trust based on the semi-ring algebra theory also has the same problem. With the increasing of the hops of the path, the convergence speed of trust of the above models will become slow, and its extendibility will fail.

It can be seen that each kind of trust model has different characteristics of rewards and punishments, convergence speed and extensible ability, and the single trust architecture or trust computing model cannot meet the trust demands of all the subjects in the Internet of things.

2. Trust Architecture in the Internet of Things

In the trust system that studies the environment of the Internet of things, because the scale, the ability and stability of each subject are not the same, if discuss all the trust relationships together, the complexity of the system will be increased. Thus, the trust system is divided into three layers: the institutional layer, the reader layer and the object layer, which is shown in figure 1. Use the long-term credibility to deal with the trust degree of the institution in the institutional layer of the Internet, make use of the neighbors to monitor the behavior of the node in the reader layer, and adopts the interactive information of the cache to detect the interaction between the node and the tag in the object layer. At the same time, there exists the transmission of the trust flow between the layers, the calculation of the trust degree of the reader can refer to the credibility of the institution that the node belongs to, and the behavior of the reader is fed back as the reputation value of its affiliated institution. The hierarchical trust mechanism can simplify the complexity of the trust interaction in the Internet of things, and meet the trust demands of different subjects.

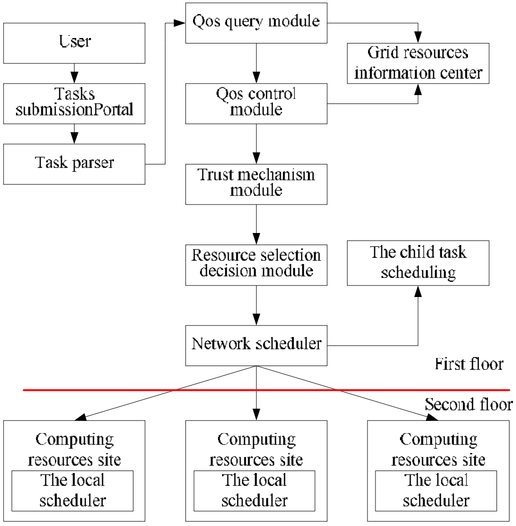

Figure 1. The Schematic diagram of the trust architecture

2.1. Trust of the reader

This section describes the method based on using the evidence theory to deduce the trust of the reader and analyzes its defects, so as to propose the VCID method.

The premise of using the evidence theory is the collaboration between the nodes, and that the neighbor nodes can detect the interaction between the objects and the reader. However, the communication between the object and the terminal reader adopts the RFID communication, which has a shorter distance and may not be learned by other nodes. Moreover, if the distribution of the readers is too sparse, it will also lead to the low detection efficiency.

The verifiable caching previous interaction digest method proposed in this paper keeps the evidence for the terminal node's usage of the authorization in the object layer, and verifies the previous interaction digest provided by the objects in the institutional layer to complete the audit of the authorization, which avoids the influence of the distribution of the readers and the communication distance between the tags.

Set the corresponding derivation rules according to the assumptions in table 2, and deduce the probability of the assumptions through the phenomena observed by the node. For example, when node x receives the data packet whose destination is node X, type is command and object is tag T in T time, while node N does not be observed to send the corresponding order in the next moment, and it is found that the recent movement speed of tag T is relatively fast, then it can be concluded that the label moves too fast, which leads to the node fails to send the demand.

The probability distribution function of B2 is as follows:

$$A=\{(x_i,y_i): i\le m, x_i\le 1, y_i\le 1\} \tag{1}$$

Among which, CER (Ai) is the uncertainty degree of each phenomenon, the trust function and the likelihood function of the event is respectively as follows:

$$y=\frac{R_1}{R_2}=\frac{yIn\Omega_1}{yIn\Omega_2}=\frac{In\Omega_1}{In\Omega_2} \tag{2}$$

$$R=yIn\Omega \tag{3}$$

Among which, there is D = {Bi}.

2.2. Trust evaluation based on VCID

The premise of using the evidence theory is the collaboration between the nodes, and that the neighbor nodes can detect the interaction between the objects and the reader. However, the communication between the object and the terminal reader adopts the RFID communication, which has a shorter distance and may not be learned by other nodes.

The verifiable caching interaction information method can guarantee the institution to complete the authorized trust, which is show as follows:

2.3. Hierarchical trust algorithm

When selecting the resource sites, the algorithm proposed in this paper is called the computing resources selection-scheduling algorithm, which comprehensively considers the total execution time of prediction and the price factor. It will choose the resource sites with the smallest total execution time, the highest trust value and the lowest price, according to the dynamically choices of the users.

3. Experimental Simulation and Analysis

3.1. Experimental environment and settings

The reader network is dynamic, and the unstable nodes will change the network topology and the interaction time, these unstable factors will affect the recognition of malicious events. Design to use the movements of the two experimental nodes of the method that based on the evidence theory to study the performance of the trust institution. In the first experiment (figure 7), the nodes are stationary, while in the second experiment (figure 8), 30% nodes move at the speed of 10 m/s. In the figure, the square points represent the occurred malicious incidents, and the diamond points the detected malicious events. If no malicious events happen or are detected at some moment, then there is no mark, the reputation value of the institution at some moment is multiplied by 10 and marked in the figure 2 for comparison.

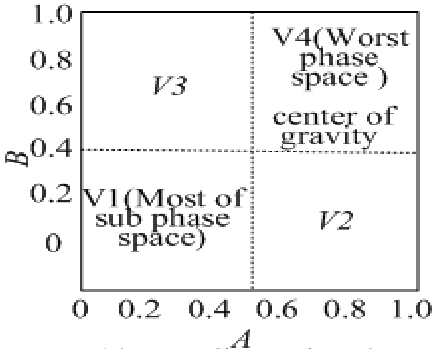

Figure 2. The Comparison between Malicious Events and Detected Events in the Environment with 0% Moved Nodes

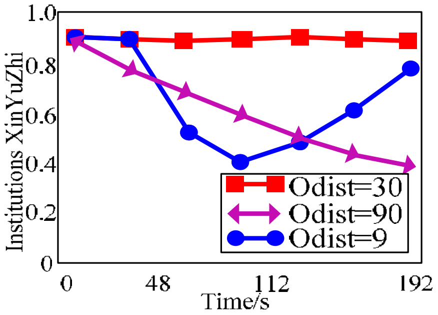

Figure 3. The Comparison between Malicious Events and Detected Events in the Environment with 30% Moved Nodes

4. Conclusion

In order to solve the conditions for the dynamic authorization problem to be applied to the Internet of things, a reliable trust mechanism must be established among the institution, the reader and the tag. Therefore, this paper proposes a hierarchical trust mechanism, and puts forward a verifiable caching interaction digest algorithm. The trust model has a relatively fast convergence and extensibility, and is suitable for the applications in the distributed and large-scale Internet of things. The experiments show that the hierarchical architecture in this paper makes the reader has a relatively rapid convergence, and it has a good performance.

References

[1] Muhammad J. Mirza, Nadeem Anjum. Association of Moving Objects Across Visual Sensor Networks. Journal of Multimedia, Vol 7, No 1 (2012) pp. 2-8

[2] Haiping Huang, Hao Chen, Ruchuan Wang, Qian Mao, Renyuan Cheng.(t, n) Secret Sharing Scheme Based on Cylinder Model in Wireless Sensor Networks. Journal of Networks, Vol 7, No 7 (2012) pp. 1009-1016

[3] Xin Huang, Xiao Ma, Bangdao Chen, Andrew Markham, Qinghua Wang, Andrew William Roscoe. Human Interactive Secure ID Management in Body Sensor Networks. Journal of Networks, Vol 7, No 9 (2012), 1400-1406

[4] Guang Yan, Zhu Yue-Fei, Gu Chun-Xiang, Fei Jin-long, He Xin-Zheng, A Framework for Automated Security Proof and its Application to OAEP. Journal of Networks, Vol 8, No 3 (2013), 552-558

[5] Muhammad J. Mirza, Nadeem Anjum.Association of Moving Objects Across Visual Sensor Networks.Journal of Multimedia, Vol 7, No 1 (2012), 2-8

[6] Muhammad J. Mirza, Nadeem Anjum.Association of Moving Objects across Visual Sensor Networks. Journal of Multimedia, Vol 7, No 1 (2012), 2-8