Research on Trust based on Internet of Things

Jianjun Wu
Hunan City University, Yiyang, 413000, China

Abstract: This paper proposes a hierarchical trust system, which separates the different trust demands of the subjects in the heterogeneous environment. According to the weakness of the evidence theory, a verifiable caching interaction digest schema (VCID) is proposed, which constructs the circulation of "credible phenomenon –credible behavior–credible node –credible institution–credible authorization" in the architecture of trust to well integrate the reader trust and the reputation of the institution. The experiment shows that relative to the evidence theory, the proposed VCID algorithm can more effectively detect the malicious terminal nodes. In addition, the hierarchical architecture of trust has a very good trust convergence. The trust mechanism in this paper can meet the trust demands of different subjects, and has a relatively faster trust convergence and extensibility at the same time.

Keywords: Things, different subjects,effectively

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[1-3].

Trust is the phenomenon of human society, and Marsh uses the sociology and other disciplines of knowledge, and early changes the trust form into the concept of computing. Trust is the belief of a node that another node can perform the actions related to its own interests according to the agreed content in a certain period of time. And the trust degree is the quantitative of this belief. The trust relationship in this paper is divided into three categories: the local trust degree, the recommended trust degree and the global reputation[4-5]. The trust model of the e-commerce usually has two types: one is the identity-based full control, namely to confirm the identity through the certificates, and carry out the authorization according to the strategies in the unified administrative domain of trust, which can directly manage the nodes in the network and is more convenient for the calculation, but due to its fixed identity and trust policy, it is not suitable for the distributed environment. The other is the credibility-based trust management, namely when the subject is calculating the trust degree of the object, it also refers to the evaluation to the object of a third party except for using its own experience. In the calculation, a variety of models can be used, such as the average value, the Bayesian system, the vector mechanism and so on. It needs a much longer time to build and maintain the credibility, which conforms to the stable characteristic of the institution. At the same time, through collaboration, the mechanism can rapidly detect the malicious nodes in the distributed network, thus, the credit system can be applied to the institutions of the Internet. In the above calculation model, the updating of the object's credibility is mainly derived from the interactive feedback of the subject to the object, but in the actual application of the Internet of things, there are not too many interactions between the institutions, and the interactions mainly occur in the institution-reader and the reader – label. While the credibility of the institution is mainly the feedback of the behavior of the reader, therefore, when using the reputation system to evaluate the trust of the institution, the factors of the subordinate reader of the corresponding institution need to be taken into consideration.

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.

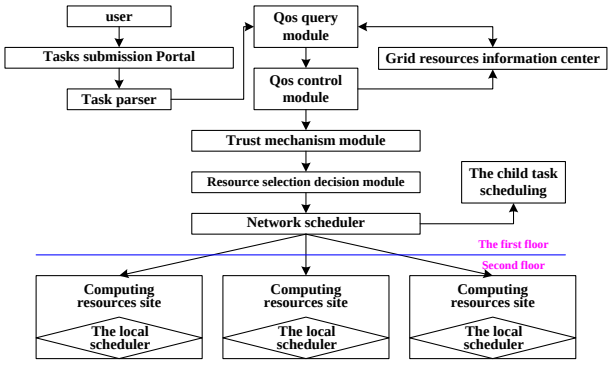

Figure.1. The Schematic Diagram Of The Trust Architecture.

Specifically, the reputation of the institution is affected by the behavior of its reader, and the behavior of the reader is mainly embodied in the interaction with the tag, namely for the authorized terminal reader, whether to faithfully forward the data and execute the demand or not. It is shown in Table 1, and the detailed description is presented in the following two sections.

3. Trust Derivation Based on Evidence Theory

1)The Evidence Theory

The evidence theory (D-S theory) is a kind of uncertain reasoning, which uses the existing knowledge and evidence to deduce the uncertainty of the hypothesis. According to the evidence theory to judge the trust degree of the reader needs to be analyzed in accordance with its behavior. With the formal expression, namely to assume that H represents the unlikelihood of node r, and the evidence in support of this hypothesis is that node r has malicious behavior, such as B1, B2,... Bn. And to judge whether these malicious behavior exist or not also needs to use the phenomenon A1, A2, ⋯Am observed by the neighbor nodes of node r to deduce, thus, there forms a derived chain of "phenomenon - behavior – state".

2) The Reasoning of the Malicious Behavior

Each type of the routing trust in table 2 can be divided into a number of assumptions, and then define the phenomenon and knowledge that deduce the hypothesis. Take "the intermediate node abandons the data packet" as an example, and respectively define the assumptions of the four events.

the{Ai} in the knowledge is the observed phenomenon by the node. In A1: Tn moment, node N receives the data packet P. and the destination of P is N. In A2: moment, the type of P is data, and the next hop is label Q. In A3: moment, during the interval of [Tn, Tn + 1], the monitoring node X receives the data packet C sent from node N, and its target is Q. In A4: moment, during the interval of [Tn, Tn + 1], the monitoring node X does not receive the data packet C sent from node N, and its target is Q. In A5: moment, the contents of C and P are the same. In A6: moment, during the interval of [Tn, Tn + 1], the movement of node N is relatively fast. In A7: moment, during the interval of [Tn, Tn + 1], the movement of node N is relatively slow. In A8: moment, the distance between node N and node X is relatively distant. In A9: moment, during the interval of [Tn, Tn + 1], the movement of node Q is relatively fast.

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 Tin 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:

$$m(B_2) = \min\{CER(A_1), CER(A_2), CER(A_4), CER(A_9)\} CF_2 \quad (1)$$

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:

$$Bel(B_2) = m(B_2) \quad (2)$$

$$Pl(B_2) = 1 - Bel(-B_2) = m(B_2) + m(D) \quad (3)$$

Among which, there is D = {Bi}.

The derivations of other events is similar to that of this event, due to the limited space they are not presented. And table 3 is the list for other events.

4. Results Analysis

4.1. Influence of the unstable reader

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 for comparison.

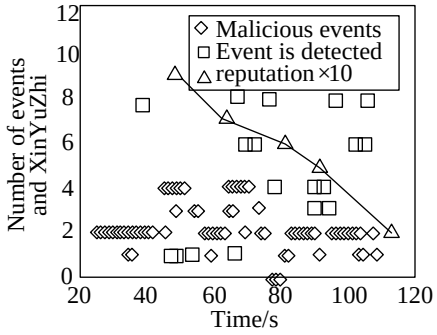

Figure.2. The Comparison between Malicious Events and Detected Events in the Environment with 0% Moved Nodes.

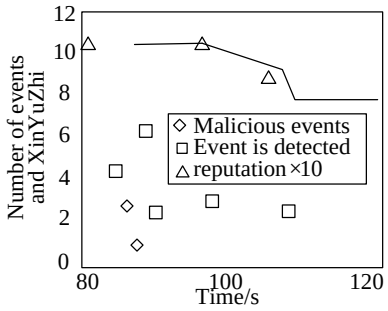

Figure.3. The Comparison between Malicious Events and Detected Events in the Environment with 30% Moved Nodes.

It can be seen that when the malicious nodes move fast, they have less contact with the tag, thus the malicious events are less. When all the nodes are stationary, there are 242 malicious events in total, and when 30% nodes are moving, there are only three malicious events. It can be seen that the movement of the nodes has a great influence on the happening of the malicious events. In the experiment, the distance between the tags is relatively longer, therefore, the three malicious events are all detected. The next experiment will analyze the influence of the communication distance between the tags on the detection of the malicious events.

5. 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] 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, 2012, 7(7): 1009-1016.

[2] Muhammad J. Mirza, Nadeem Anjum. Association of Moving Objects Across Visual Sensor Networks. Journal of Multimedia, 2012, 7(1): 2-8.

[3] Xin Huang, Xiao Ma, Bangdao Chen, Andrew Markham, Qinghua Wang, Andrew William Roscoe. Human Interactive Secure ID Managementin Body Sensor Networks. Journal of Networks, 2012, 7(9): 1400-1406.

[4] Weisen Pan, Shizhan Chen, Zhiyong Feng. Investigating the Collaborative Intention and Semantic Structure among Co-occurring Tags using Graph Theory. 2012 International Enterprise Distributed Object Computing Conference, IEEE, Beijing, pp. 190-195.

[5] Jennifer W. Chan, Yingyue Zhang, and Kathryn E. Uhrich, Amphiphilic Macromolecule Self-Assembled Monolayers Suppress Smooth Muscle Cell Proliferation, Bioconjugate Chemistry, 2015, 26(7), 1359-1369.