International Journal of Intelligent Information and Management Science
ISSN: 2307-0692, Volume 6, Issue 5, October, 2017

Research on Application of Hierarchical Trust Mechanism in Internet of Things

Haogui Chen
Hunan City University, Yiyang, 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. Thus, this paper proposes a hierarchical trust mechanism, and puts forward a verifiable caching interaction digest schema at the same time. At first, this paper analyzes the features of the application and the trust demands of different subjects in the Internet of things, the credibility of the detaching mechanism and the reader trust. Then, it proposes the improved method of evidence theory accoording 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, Verifiable Cache, Rate of Convergence

1. Introduction

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 [1-4], which calculates the local trust according to the interaction with the object, and through a Trust Net network to combine with the local trust of the other node to the object to carry out the composition, so as to obtain the comprehensive trust. 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 [5].

This paper mainly has development and innovation works in the following aspects:

In order to further verify the correctness and effectiveness of the trust mechanism and algorithm proposed in this paper, the simulation experiments on the influences of the unstable reader, of the communication distance between the labels, of the convergence speed of the evidence theory and the proposed trust mechanism are carried out. The experimental simulation results show that the trust mechanism and the algorithm in this paper both are suitable for the unstable reader network, but in the tag- terminal reader environment with a relatively close communication distance, the algorithm in this paper has an obviously better performance. The hierarchical architecture in this paper makes the reader have relatively faster trust convergence and good performance.

1.1. Institutional trust

Before the authorization of the reader, it is necessary to examine the trust of the institution that the reader belongs to. The trust of the institution is stable, and it can be obtained by the evaluation of the third party to its reputation value, and is mainly implemented in the institutional layer. Considering that the number of the institutions is far less than the number of the readers and tags, and at the same time, there often exist entities in the institution, which is stable. Thus, the trust management based on the trust management institution is proposed.

1.2. Trust management based on cluster

In the distributed application, it can be divided according to the geographical area to form the administrable cell cluster. In the cluster, the reputations of the ordinary institutions are centrally managed by a trust management institution G, which maintains the reputation of the institution according to the reports of the institutions in the cluster. While the ordinary institutions decide whether to authorize the reader, reference to the reputation value of the institution released by G.

1.3. Trust-transmitting between the institution and the reader

1.3.1. Dynamic authorization reader

Before the reader Rn needs to carry out the interaction with the tag, it needs to obtain the authorization of the institution OA that the tag belongs to. Rn sends the authorization request to OA, after OA receives the request of the reader Rn, it will calculate the trust degree of the reader Rn.

$$T(R_n) = aT_{O_A}(R_n, O_B) + (1-a)T_G(O_B) \quad (1)$$

Among which, TOA(Rn， OB) is the direct trust that based on previous interaction experience, TG(OB) is the indirect trust, namely the reputation of the institution OB that Rn belongs to, which can be obtained from the trust management institution G, and α is the proportional adjustment factor. If T (Rn) is less than the threshold Tmin, then the authorization is refused. Otherwise, it is passed.

1.3.2. Trust feedback

Influenced by the initial value and the convergence of the trusted model, the authorization of the institution to the node may not be reasonable, thus the trust feedback becomes an important method to correct the mistakes. The institution obtains the behavior credibility of the node from the interaction digest provided by the tag, updates the authorization of the node, and feedback to the reputation value of its belonged institution. If an authorized node has faulty or malicious behavior, it will report to institution O, and O will reduce the trust value of the node.

$$T_n(R) = dT_{n-1}(R) \quad (2)$$

If there is Tn (R) < Tmin, then the institution revokes the authorization.

1.4. 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.
The algorithm is simply described as follows:
For a large task, after the task resolver, the obtained task subset is T= {t1, t2…tm}. According to the requirements of the task QoS, it is divided into four types of tasks based on the scheduling strategies, and this paper firstly selects the task subset T' = (t1, t2…tk) 苘 k ≤ m in the task set QoS (hh). Then carries out the following five basic operations successively to the task subsets in QoS (hl), QoS (lh) and QoS (ll), until all the task subsets T ' comprehensively choose the proper resource sets.
1) For each task ti, collect and calculate the corresponding measuring index vector of each resource site rij in the available resources Ri.

$$MTR_{i,ij} = (MCT(i,ij), P_{i,ij}) \quad (3)$$

2) For task ti, bring in the trust mechanism to calculate the minimum completion time of the prediction. And the formula is as follows:

$$Trust - MT(i,ij) = MCT(i,ij) / Trust(i,ij) \quad (4)$$

Among which, Trust (I,ij) is the trust degree of node ti to the computing node rij.
3) For each subtask ti in the T ', calculate the corresponding comprehensive measure function of each available computing resource rij according to the following formula (11).

$$F_{i,ij} = a \times Trust - MT(i,ij) + (1-a) \times P_{i,ij} (0 \le a \le 1) \quad (5)$$

4) After the above steps, the set of the one-to-one corresponding target computing resources {r1k1,r2k2, ,rmkm} to the set of the subtasks T' ={t1，t2，….tk} is finally obtained. And riki(ki ∈ (1,2,….ni)) is the computing resource site selected by the subtask ti.
5) Update the trust value and the weight information, and send the subtasks to the corresponding computing resource sites, then carry out the scheduling of the second floor, and place them to each execution node for the parallel execution.

2. Experimental Simulation And Analysis

2.1. Experimental environment and settings

The experiments use the simulation to carry out the verification, and the environment is shown in figure 6. Among which, the points begin with O is the objects, the points begin with R is the readers, the colors represent the belonged institutions, and the line between the nodes shows that the two nodes are in the communication. The simulation uses the event-driven. If the following experiment does not have attached instructions, then the network area of the reader in the environment is 1200 x 900mm, the number of the reader nodes is 80, the communication distance is 200m, the communication distance between the tags is 60m, and the simulation time is 200s. The influences of the unstable reader on the happening if the malicious events and the effects of the communication distance between the tags on the detection of the events are analyzed in the following, and the influences are compared with the convergence efficiency performance of the evidence theory and VCID.

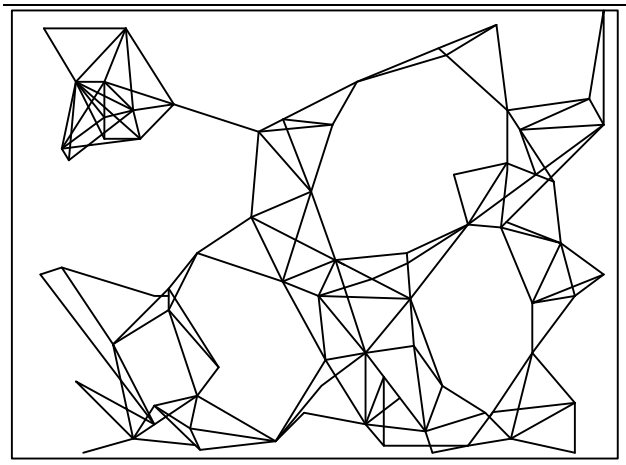

Figure.1. The Simulation Environment.

2.2. Influence of the communication distance between The tags

The communication distance between the tags also has influence on the detection of the malicious events. Different RFID tags, such as the passive tags and the active tags, have different communication distances, and the communication distance between the tags directly determines number of the neighbor nodes that can monitor the interaction between the tags and the terminal reader.

There are three experiments, and the communication distance between the tags is respectively 30m, 60m and 90m, the changes of the institution's reputation are shown in figure 9. When the communication distance between the tags is 30m, the reputation value of the institution does not change, and when the communication distance between the tags increases to 60m, the reputation value of the institution decreases, and the reports without detecting the malicious events after a period of time start to pick up. And when the communication distance between the tags increases to 90m, the reputation value of the institution quickly reduce to a minimum and remains unchanged.

Set the communication distance between the tags to odist, the number of the readers to n, and the network area of the reader to S = w·h, then the average number of the readers that the tags met is as follows.

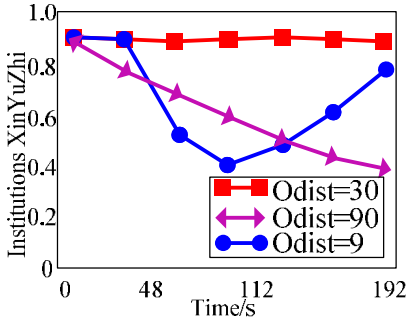

Figure.2. The Influence of the Communication Distance between Tags on the Reputaion of Institution.

3. 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] Yingyue Zhang, Evan Mintzer, and Kathryn E. Uhrich, Synthesis and Characterization of PEGylated Bolaamphiphiles with Enhanced Retention in Liposomes, Journal of Colloid and Interface Science, 2016, 482, 19-26.

[5] Jonathan J. Faig, Alysha Moretti, Laurie B. Joseph, Yingyue Zhang, Mary Joy Nova, Kervin Smith, and Kathryn E. Uhrich, Biodegradable Kojic Acid-Based Polymers: Controlled Delivery of Bioactives for Melanogenesis Inhibition, Biomacromolecules, 2017, 18(2), 363-373.