International Journal of Security and Its Applications
Vol. 9, No. 6 (2015), pp. 101-114
http://dx.doi.org/10.14257/ijsia.2015.9.6.11

Research on Application of Hierarchical Trust Mechanism in Internet of Things

Deng Xian-Rui[1], Mu Jingqin[2] and Wei Ping[3]

[1, 2]*Department of Computer Science, Tangshan Normal University, Tangshan, China*
[3]*College of Geophysics and Information Engineering, China University of Petroleum, Beijing, China*
[1]*xianruideng@sina.com*

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 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 [1, 2]. 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.*, [3]. In recent years, the research of the trust model of the Internet of Things has also drawn more and more attentions [4, 5]. 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 [6]. Therefore, the trust model becomes a powerful supplement to improve the security of the system.

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 [7]. 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 [8, 9]. 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

ISSN: 1738-9976 IJSIA

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 [11, 12], 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 [13]. 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 [14].

2. Trust Architecture in the Internet of Things

2.1. Trust Evaluation based on VCID

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.

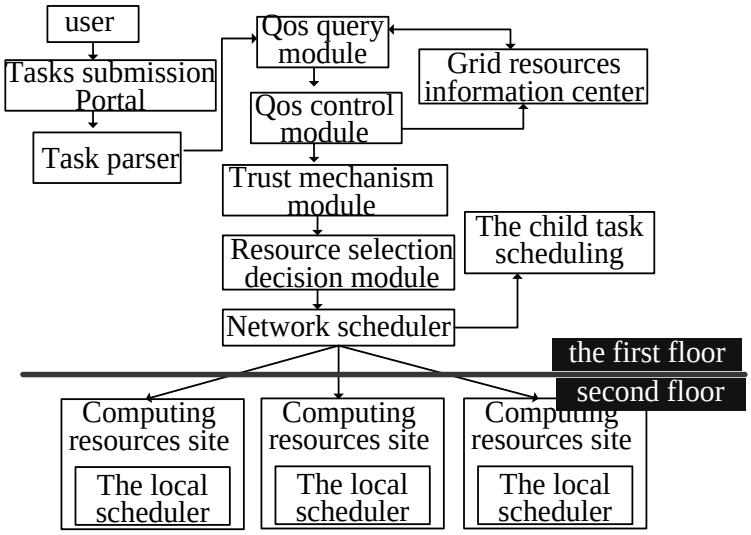


Figure 1. The Schematic Diagram of the Trust Architecture

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.

Table 1. Types of the Reader's Trust

Type of trust	Behavior
Authorized trust Tt	Terminal node abandons the order or the data Terminal node falsifies the order or the data Terminal node replaces or forges the order or the data Effectiveness of the ternimal node's information

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.

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.

Table 2. The Derivation Rules of Abandoning Data

Event	Hypothesis of event	Hypothesis	Knowledge (derivation rules)	Uncertainty degree of the knowledge
terminal node abandons data packet	Node does not abandon the data packet and is detected by the neighbor node	B_0	$A_5 \rightarrow B_0$	CF_0
	Node does not abandon the data packet but is not detected by the neighbor node	B_1	A_6 OR $A_5 \rightarrow B_1$	CF_1
	Node abandons the data packet because it can get connected to the neighbor node	B_2	$A_5 \rightarrow B_{52}$	CF_2
	Node maliciously abandons the data packet	B_3	A_7 AND $A_5 \rightarrow B_3$	CF_3

In Table 2, 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 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:

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

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.

Table 3. The Event Lists of the Reader Network

Type of hypothesis	Hypothesis	Mark
Event (the terminal node falsifies the data packet)	The node does not modify the data packet	B_4
	The node does not modify the data packet, but the network transmission is false	B_5
	The node has a abnormal work and modifies the data packet during the forwarding	B_6
	The node maliciously modify the content of the data packet	B_7
Event (the terminal node forges or replaces the data packet)	The node does not replace the data packet, because the contents of the former and latter data packets are the same	B_8
	The node replaces the data packet and transmits it to the institution that is not the destination	B_9

After the neighbor nodes discover the abnormal events of node R, they need to report to the institution. Because one event may be captured by more than one node, the institution OA checks regularly to find out all the reports {Tevent} related to the event, then orthogonally calculates the comprehensive trust degree of each event, and calculates the uncertainty degree of Bi.

$$m(B_i) = m_{x_1}(B_i) \oplus m_{x_2}(B_i) \oplus \cdots \oplus m_{x_n}(B_i) \quad (4)$$

$$T'_{event} = (m(B_i), B(B_i), P(B_i)) \quad (5)$$

$$GER(B_i) = Bel(B_i) + \frac{Pl(B_i)}{|D|} \quad (6)$$

The process that the institution gives the authorization of interaction is shown in Figure 2. After reader R = Rn – 1 discovers tag T, it sends the request of TAG_HEADER_REQ. And tag T responses to TAG_HEADER_REP, which includes the information such as number T, the affiliated institution O and so on. Then, R sends the authorization request of AUTH_ REQ to institutions O, and after R identifies that R is reliable, it passes the authorization and returns AUTH_REP. After R obtains the authorization, it shows the authorization certificate to T. Finally, T can carry out the interactions of data or orders with R.

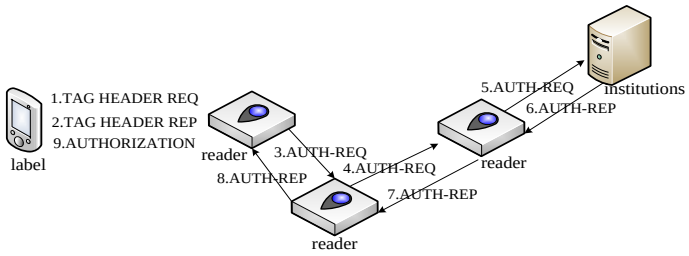


Figure 2. The Schematic Diagram of the Dynamic Authorization

Then, in Tn-1 time, after the interaction between T and Rn-1, T records (Rn-1, Tn-1, opn - 1), in which opn- 1 is the digest of the operation type of the interaction. In the next moment Tn, when T goes by the terminal reader Rn and sends the data packet D to the institution O, it adds the interactive information in Tn-1 time to the data packet. The data packet changes into M = (certT, rsT, seq, Rn-1, Tn-1, opn- 1, D, h), in which h = hash(certT, seq, Rn-1, Tn-1, opn – 1, rsT) is the hashed value of the field combination. To ensure the integrity of M, certT is the certificate of T, rsT is the random number of T, and seq is the serial number of D. After Rn receives M, M = (certT, rsT, seq, Rn-1, Tn-1, opn – 1, D, h, certRn, rsRn, h') is forwarded, in which there is h' = hash(certRn, rsRn, h), certRn and rsRn is respectively the certificate and random number. Therefore, M' contains the signature of Rn, and the intermediate reader will verify h and h ' during the routing, if it fails, then the forwarding is declined, otherwise the forwarding is continued until it reach O.

Finally, the institution O maintains a hash table C ={ seq→(M ' − D) } for each T. At the same time, it uses the hash table B = { R→{ c} } to save the detected information of the nodes with malicious authorization, in which c is the certainty factor of each abnormal event. After the institution O receives M', it checks whether if M' has malicious behavior for authorization, which is shown in Figure 3.

```
if h' ≠ hash(cert_{R_n}, rs_{R_n}, h) ∥ valid(cert_T)==false
return
seq_max = max(seq, seq_max)
seq_min = min(seq, seq_min)
C[seq] = (cert_T, rs_T, seq, R_{n-1}, T_{n-1}, op_{n-1}, h)
if (currentTime% checkTimeout = 0)
  foreach (cert_T, rs_T, seq, R_{i-1}, T_{i-1}, op_{n-1}, h) ∈ values(C) and
      seq_min ≤ seq ≤ seq_max
    if (h ≠ hash(cert_T, seq, R_{n-1}, T_{n-1}, op_{n-1}, rs_T))
      B[R_n].add(c_1)
    else if (seq -1 ∉ keys(C))
      B[R_{n-1}].add(c_2)
    else if (op_{n-1} is invalid)
      B[R_{n-1}].add(c_3)
    endif
  endforeach
endif
```

Figure 3. The Digest Checking Process of the Institution

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

(1) Because the intermediate node checks the integrity of the data packet, if the check of institution O on h' successes, then it can be sure that M' does not been modified after being send from Rn, otherwise the intermediate node will abandon the data packet that fails the checking, thus, it can guarantee the security of the routing.

(2) The checking of institution O on h can ensure that Rn does not falsify M. Therefore, when the label data goes by the reader network, its integrity can be ensured. In addition, T adds random number rsT and timestamp Tn – 1 to the data packet, which can ensure that Rn can not replace or forge M.

(3) The reader obtains the authorization before the interaction with T, and the routing path is clear. If the institution cannot find the seq-1 key in C, then it shows that the institution does not receive the data packet of the previous interaction at last. The data packet is likely to be abandoned by Rn – 1, and then O can mark that Rn – 1 has a malicious behavior.

(4) The operation summary before the moment of the checking is opn-1, the institution can audit whether if the reader properly uses the authorization and without illegal operations.

However, this approach carries the risk of omission, namely there will be the situations that the interactive readers both are malicious nodes or the data packet loses due to the changes of the network, then the institution will only know the losing of the data packet, but can not learn the serial number of the reader. Because VCID only reduces the reputation of the institution according to the identified malicious events, it will not affect the normal institutions, so it is acceptable. In addition, the verification of the authorization can be designed as the exclusive or operation, which can satisfy the computing power of the label.

The verifiable caching interaction digest method needs to save the digest information. On the one hand, the label will save the digest of this interaction during the interaction, and it will upload and abandon the digest during the next interaction, so there only needs to one digest. On the other hand, the server needs to save the digests uploaded by all the tags within *check_timeout* time. Although the storage and checking of a single tag cost little, for the large-scale application, it may need to use the parallel computation and storage.

2.2. 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.

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.

Institution OA regularly inspects the events in evidence theory or the events of cross validation in VCID, when it finds the abnormal status of node R after the orthogonal calculation, it reports to G. And the process is shown in followings.

1. *For the status of each node in TR, set the trust threshold *, the likelihood threshold *, the abnormal authorization threshold t and the biggest abnormal authorization threshold c*
2. *Aggregate all the interactive reports according to the report nodes, and obtain **

3. *Calculate the state assumption of node R * according to table 4*
4. *If there exists *, which makes there are * and *, determine the state of R **
5. *Calculate the abnormal number of authorization **
6. *If there is *, then **
7. *If R is abnormal, then add * to **
8. *QA sends the abnormal report E of node to G*

Trust Management of the Trust Management Institution

When the cache of the trust management institution receives the status reports of the nodes, it checks the reports regularly. The specific steps are shown followings.

1. *Hash the reports of the institutions according to the nodes, each node corresponds to one list **
2. *Count the report number of the normal nodes, faulted nodes, faulted environment and malicious nodes in *, and treat the largest type as the final state type of R to eventually generate the state list of all the nodes*
3. *Carry out the hash to Lo according to the institution R belongs to, each institution org corresponds to one list **
4. *Count the report number of the normal nodes, faulted nodes, faulted environment and malicious nodes in *, which is respectively marked as *, *, * and **
5. *Calculate and update the reputation value * after the forgetting of the malicious events, in which f is the forgetting factor, To is the initial reputation, * is the reputation of the institution at the former moment, and the obtained final reputation value of the institution is *, in which * is the penalty factor of the node faulty, and * is the penalty factor of the malicious node*
6. *G publishes **

2.3. Trust Transmitting between the Institution and the 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.

$$T(R_n) = \alpha T_{O_A}(R_n, O_B) + (1-\alpha) T_G(O_B) \tag{7}$$

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.

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.

$$T_n(R) = \delta T_{n-1}(R) \tag{8}$$

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

2.4. 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), 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.

$$MTR_{i,ij} = (MCT(i,ij), P_{i,ij}) \tag{9}$$

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

$$Trust - MT(i,ij) = MCT(i,ij) / Trust(i,ij) \tag{10}$$

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).

$$F_{i,ij} = \alpha \times Trust - MT(i,ij) + (1-\alpha) \times P_{i,ij} (0 \le \alpha \le 1) \tag{11}$$

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.

3. Experimental Simulation and Analysis

3.1. 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.

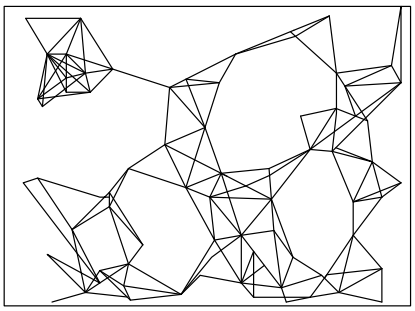


Figure 4. The Simulation Environment

3.2. Results Analysis

(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.

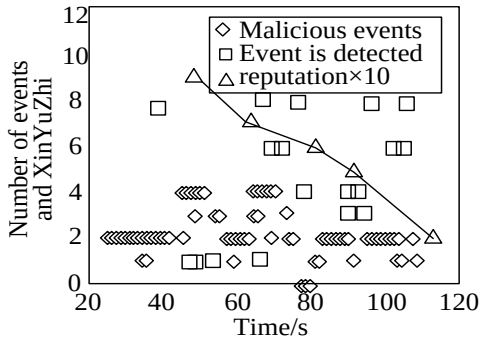


Figure 5. The Comparison between Malicious Events and Detected Events in the Environment with 0% Moved Nodes

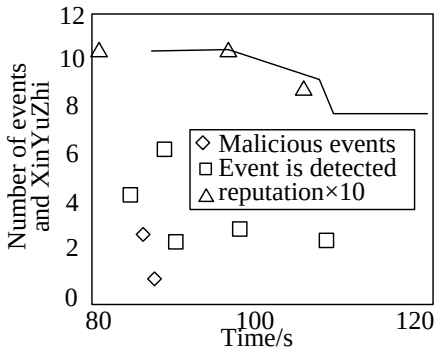


Figure 6. The Comparison between Malicious Events and Detected Events in the Environment with 30% Moved Nodes

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.

(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.

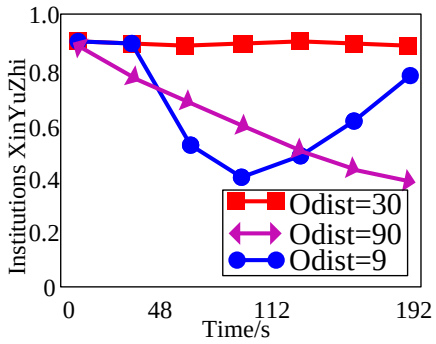


Figure 7. The Influence of the Communication Distance between Tags on the Reputaion of Institution

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:

$$\overline{N} = \frac{odist^2 \bullet \pi \bullet n}{w \bullet h} \tag{9}$$

When there is odist = 30 m, then the value of N is 0.21. At this moment, the tags are the same with the readers, it is hard to meet other readers to carry out the monitoring. It can be seen that the evidence theory has a relatively poor performance with a relatively short communication distance between the tags.

(3) Convergence Rate of the Evidence Theory

For the hierarchical trust mechanism, the malicious events of the nodes at the bottom converge to the reputation of the institution on the top, and the convergence rate of trust is an important evaluation standard. In order to assess the convergence

of the routing trust, the network area of the reader is set to 800 × 600 mm, and the others remain the same. The experiment results are shown in Figure 10.

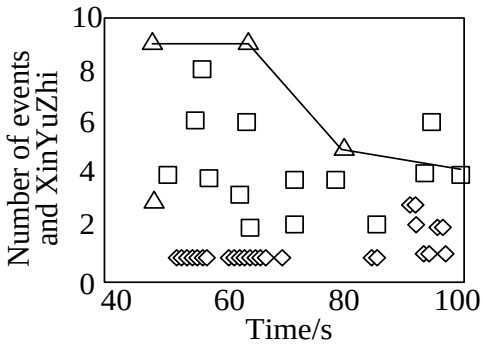


Figure 8. The Convergence Rate of the D-S Method

The initial reputation value of the institution is 0.9, before t = 48s, there is no malicious events, and after it the malicious events begin to appear. If there are successive three abandoning events after t = 50s, then after Δt = max (recv _ timeout, check_timeout), namely the next checking moment or the maximum timeout of receiving the data packet, the neighbor nodes detect the malicious events. Therefore, when t =55 s, there are six reports of the malicious events, and eight reports in the next second. Because a malicious event can be captured by multiple nodes, so there are multiple corresponding reports. Then the malicious reports gather up, but at this time, the reputation value of the institution has not been updated, thus when there is t = 64s, the reputation value of the institution is still 0.9. After the next checking moment of the trust management institution t = 80 s, the reputation of the malicious institution begins to reduce, and continues to reduce with the increasing of the reports. It can be seen that the hierarchical structure of trust can feedback the behavior of the nodes at the bottom to the trust of the institution within a relatively short period of time. The larger the scale of the application, the more the nodes will be, or the more the malicious behavior of the nodes will be, then the faster the feedback of the trust will be.

(4) Convergence Rate of the VCID

In the authorized trust, use the caching previous interaction digest method to detect the malicious terminal nodes, which also can effectively detect the malicious nodes, even in the environment that the density of the reader is not dense. Three groups of experiments are designed, among which, group 1 and group 2 respectively uses the evidence theory and the bayesian decision, namely to deduce the malicious events by using the nodes to detect the behavior of the neighbor nodes to the tags, and group 3 adopts the verifiable caching interaction information method. Each group selects 40, 60 and 80 nodes, there are 9 experiments in total. The results are shown in Figure 11.

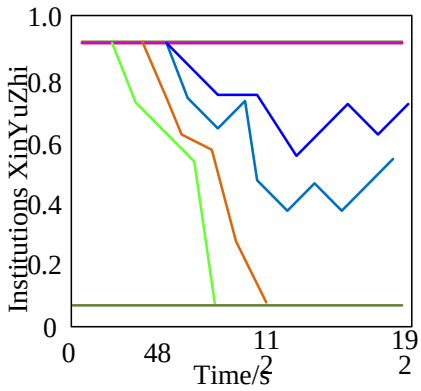


Figure 9. The Convergence Rate of the VCID

In the experiment that adopts the evidence theory, because it is relatively sparse between the nodes, the malicious events cannot be detected. Therefore, when the number of nodes is 40 and 60, the reputation of the malicious institution is always the same, and when the number of nodes is 80, the reputation value begins to decline. The results obtained by using the bayesian decision are similar to the results obtained by using the evidence theory, but its success rate of detection reduces. Other methods such as the cloud model and the method based on the entropy model are both adjust the trust degree of the nodes by capturing the behavior of the neighbor nodes, which will be restricted by the short communication distance between the tags in the detecting of the interaction between the readers and the tags, thus, their influences on the reputation of the institution are similar to the experiment results of the two groups.

On the contrary, in the experiment that uses VCID, it also can timely detect the malicious events, even if the number of nodes is 40. And since then, with the increasing of the density, the number of the contact beween the malicious nodes and the tags increasing, and the reputation value of the malicious institution declines faster. It can be seen that by adopting the verifiable caching previous interaction information method, the relatively faster convergence speed can be obtained, and the influence of the node deployment can be avoided.

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.

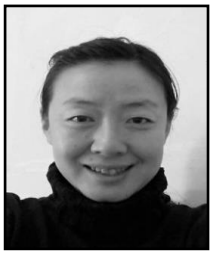
Acknowledgement

This research work is supported by the Hebei province science and technology plan project, under Grant No. 13220319D and the Doctor Foundation of Tangshan Normal University under Grant No. 07A01.

References

[1] M. J. Mirza and N. Anjum, "Association of Moving Objects Across Visual Sensor Networks", Journal of Multimedia, vol. 7, no. 1, **(2012)**.
[2] H. Huang, H. Chen, R. Wang, Q. Mao and R. Cheng, "(t, n) Secret Sharing Scheme Based on Cylinder Model in Wireless Sensor Networks", Journal of Networks, vol. 7, no. 7, **(2012)**.
[3] X. Huang, X. Ma, B. Chen, A. Markham, Q. Wang and A. W. Roscoe, "Human Interactive Secure ID Management in Body Sensor Networks", Journal of Networks, vol. 7, no. 9, **(2012)**.
[4] Y. Grenier, "Time-dependent ARMA modeling of nonstationary signals", IEEE Trans. Acoust., Speech, Signal Processing, vol. 31, no. 8, **(1983)**.
[5] M. Jachan, G. Matz and F. Tfarma, "Models: Order Estimation And Stabilization", Proceedings of 2005 International Conference on Acoustics, Speech, and Signal Processing, Philadelphia, USA, **(2005)** March 19-23.
[6] X. Ma and C. L. Nikias, "Parameter estimation and blind channel identification in impulsive signal environments", IEEE Transactions on Signal Processing, vol. 43, no. 12, **(1995)**.
[7] M. Shao and C. L. Nikias, "Signal processing with fractional lower order moments instable processed and their applications", Proceedings of the IEEE, vol. 81, no. 7, **(1993)**.
[8] J. He, Y. Geng and K. Pahlavan, "Modeling Indoor TOA Ranging Error for Body Mounted Sensors", Proceedings of IEEE 23nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), Sydney, Australia, **(2012)** September 11-14.
[9] Y. Geng, J. Chen and K. Pahlavan, "Motion detection using RF signals for the first responder in emergency operations", A PHASER project. Proceedings of 24nd International Symposium on Personal Indoor and Mobile Radio Communications; London, Britain, **(2013)** September 8-11.
[10] S. Li, Y. Geng, J. He and K. Pahlavan, "Analysis of Three-dimensional Maximum Likelihood Algorithm for Capsule Endoscopy Localization", Proceedings of 5th International Conference on Biomedical Engineering and Informatics, Chongqing, China, **(2012)** October 16-18.
[11] T. H. Liu and J. M. Mendel, "A Subspace-Based Direction Finding Algorithm Using Fractional Lower Order Statistics", IEEE Transactions On Signal Processing, vol. 49, no. 8, **(2001)**.
[12] E. N. Kuruoglu, "Signal Processing in α Stable Noise Environments: A Least lp-Norm Approach", Department of Engineering, University of Cambridge, Britain, **(1998)**.
[13] Z. Lv, L. Feng, H. Li and S. Feng, "Hand-free motion interaction on Google Glass", Proceedings of SIGGRAPH Asia 2014 Mobile Graphics and Interactive Applications, Shenzhen, China, **(2014)** December 3-6.
[14] C. Zhong, S. M. Arisona, X. Huang, M. Batty and G. Schmitt, "Detecting the dynamics of urban structure through spatial network analysis", Proceedings of International Journal of Geographical Information Science, vol. 28, no. 11, **(2014)**.
[15] W. Li, J. Tordsson and E. Elmroth, "An aspect-oriented approach to consistency-preserving caching and compression of web service response messages", Proceedings of 2010 IEEE International Conference Web Services, Miami, USA, **(2010)** July 5-10.
[16] M. Shao and C. L. Nikias, "Signal processing with fractional lower order moments: stable processes and their applications", Proceedings of the IEEE, vol. 81, no. 7, **(1993)**.
[17] S. Wang and X. Zhu, "α spectrum estimation method for ARMA $S\alpha S$ process based on FLOC", Journal on Communications, vol. 28, no. 7, **(2007)**.

Authors



Deng Xian-Rui, received PhD in Control Theory and Control Engineering in 2007 from the Institute of Automation, Chinese Academy of Sciences, Beijing, China. She is currently associate professor in the Computer Science Department of Tangshan Normal College, Tangshan, Hebei, China. Her research interests include Internet of Things and computer simulation.

Mu Jingqin, received is master degree in Computer Sciences in 2004 from the China University of Geosciences, Beijing, China. She is now a teacher in department of computer science in Tangshan normal university. Her research interests are imaging processing and software formalization.

Wei Ping, received PhD in Control Theory and Control Engineering in 2006 from the Institute of Automation, Chinese Academy of Sciences, Beijing, China. She is currently a teacher in the College of Geophysics and Information Engineering, China University of Petroleum. Her research interests include Internet of Things and algorithm.