Research on Trust Mechanism Algorithm based on Internet of Things

Shuaili Wang
Hunan City University, Yiyang Hunan 413000, China

Abstract: According to the defects in the Internet of things, this paper proposes a trust mechanism algorithm based on the Internet of things. Through the use of the algorithm, the authentication algorithm is analyzed, the results show that the algorithm is faster and more accurate than the traditional

Keywords: Algorithm; Trust mechanism; Mechanism; Authentication

1. Introduction

The evidence theory usually has good convergence of calculation and scalability, but its Dempster synthesis has risk of conflict, because the orthogonal synthesis considers the same part of the different reports, if there is the report of a node totally different from the real situation, the synthesis results will be affected, and the conflict is especially obvious in the environment of a forged node report. Similar to the evidence theory, the hypothesis of the method proposed by Song and others, which is based on the Bayesian decision theory model, does not have the fuzziness, and the behavior of the node is always either yes or no. The experiment in literature [1-3] 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 [4-5].

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

The trust mechanism under the environment of the Internet of things is an important problem needs to be studied. In this paper, the hierarchical architecture of trust under the environment of the Internet of things meets the trust demands of different subjects, and separates the credibility of the institution from the reader trust. The usage of the method that based on the evidence theory to deduce the trust of the dynamically moved reader leads to the relatively poorer detection efficiency of the malicious events due to the relatively shorter communication distance between the labels, therefore, this paper puts forward the method that can verify the previous interaction digest of the caching, which can effectively detect the malicious terminal reader. Use the reputation mechanism to maintain the trust of the institution in a stable institutional layer, then the trust interactions between the layers form the circulation of “credible phenomenon–credible node –credible institution–credible authorization”, which makes the trust get fast convergence and feedback.

1.1. 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.

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.

$$m(B_i) = m_{x_1}(B_i) \oplus m_{x_2}(B_i) \oplus \cdots \oplus m_{x_n}(B_i) \tag{1}$$

$$T'_{event} = (m(B_i), B(B_i), P(B_i)) \tag{2}$$

$$GER(B_i) = Bel(B_i) + \frac{Pl(B_i)}{|D|} \tag{3}$$

1.2. 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. 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.

When the institution obtains the authorization request of the reader, it determines whether to allow to give the authorization or not, through the credibility of its organization. After the authorization, in order to prevent its abuse, the institution needs to monitor the follow-up interactions, and the concrete process is as follows: during the interaction, the objects cache the relevant information of each other, and submit the information to the institution in the next interaction, in this way, the institution can determine whether the interaction is reasonable or not. Therefore, the verifiable caching previous interaction digest method includes three steps: the institution gives the authorization of interaction, the tags cache the digest of each other and the institution audits the authorization.

The process that the institution gives the authorization of interaction is shown in Figure 1. 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.

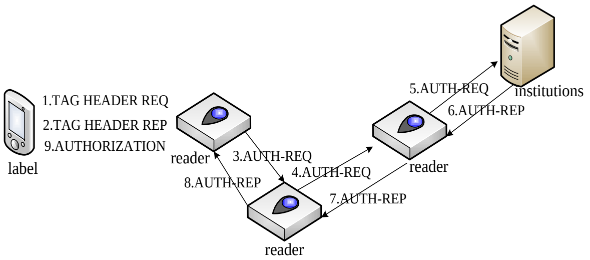

Figure 1. The schematic diagram of the dynamic authorization

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 figure2.

```
if $h' \neq \mathrm{hash}(cert_{R_n}, rs_{R_n}, h)$ □ $valid(cert_T)$==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 $(cert_T, rs_T, seq, R_{i-1}, T_{i-1}, op_{n-1}, h) \in values(C)$ and
      $seq_{\min} \leq seq \leq seq_{\max}$
    if $(h \neq \mathrm{hash}(cert_T, seq, R_{n-1}, T_{n-1}, op_{n-1}, rs_T))$
      $\mathrm{B}\left[R_n\right].add(c_1)$
    else if $(seq - 1 \notin keys(C))$
      $\mathrm{B}[R_{n-1}].\mathrm{add}(c_2)$
    else if ($op_{n-1}$ is invalid)
      $\mathrm{B}[R_{n-1}].\mathrm{add}(c_3)$
    endif
  endforeach
endif
```

Figure 2. 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 numbers T 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. Experimental Simulation and Analysis

2.1. 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 3.

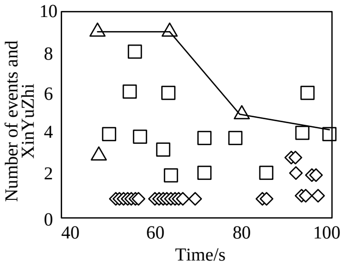

Figure 3. The convergence rate of the D-S method

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.

2.2. 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 4.

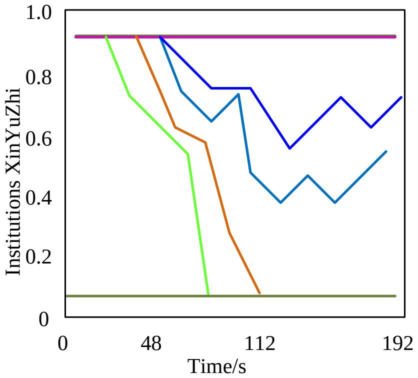

Figure 4. The convergence rate of the VCID

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.

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.

3. Conclusion

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 between the malicious nodes and the tags increases, 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.

References

[1] Lv, Z., Halawani, A., Feng, S., Li, H., &Rẻhman, S. U. (2014). Multimodal hand and foot gesture interaction for handheld devices. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 11(1s), 10.

[2] Yizheng Chen, Fujian Tang, Yi Bao, Yan Tang, *Genda Chen. A Fe-C coated long period fiber grating sensor for corrosion induced mass loss measurement. Optics letters, 41(2016), pp. 2306-2309.

[3] Yang Du, Yizheng Chen, YiyangZhuang, Chen Zhu, Fujian Tang, *Jie Huang. Probing Nanostrain via a Mechanically Designed Optical Fiber Interferometer. IEEE Photonics Technology Letters, 29(2017), pp. 1348-1351.

[4] Weisen Pan, Shizhan Chen, ZhiyongFeng. Automatic Clustering of Social Tag using Community Detection. Applied Mathematics & Information Sciences, 2013, 7(2): 675-681.

[5] Yingyue Zhang, Qi Li, William J. Welsh, Prabhas V. Moghe, and Kathryn E. Uhrich, Micellar and Structural Stability of NanoscaleAmphiphilic Polymers: Implications for Anti-atherosclerotic Bioactivity, Biomaterials, 2016, 84, 230-240.