Intelligent Authentication Method for Trusted Access of Mobile Nodes in Internet of Things Driven by Cloud Trust

Shu Song[1] and Lixin Jia[2(✉)]

[1] Changjiang Polytechnic, Wuhan 430074, China
ss209809@126.com
[2] Jiangsu Fangtian Power Technology Co., Ltd., Nanjing 210096, China
lxj987600@126.com

Abstract. In order to solve the problem that traditional cloud trust-driven mobile nodes in the Internet of Things lack credible authentication, a cloud trust-driven intelligent authentication method for trusted access of mobile nodes in the Internet of Things is proposed. The mobile nodes in the Internet of Things are determined based on cloud trust-driven, relying on the processing of mobile nodes in the Internet of Things and the intelligent authentication of trusted access of mobile nodes in the Internet of Things. The cloud trust-driven Internet of Things migration is realized. Mobile node trusted access intelligent authentication. The experimental data show that the proposed intelligent authentication method can not only improve the credibility of the traditional authentication method, but also simplify and standardize the authentication process. It enhances the adaptability and flexibility of trusted access authentication of Internet of things driven by cloud.

Keywords: Cloud trust drive · Internet of Things · Mobile node · Intelligent authentication

1 Introduction

The Internet of Things (IOT) is a hybrid heterogeneous network composed of perceptual subnet, transmission subnet and application subnet. As an important part of the Internet of Things, wireless sensor has been widely used. Wireless sensor networks (WSNs) are composed of a large number of low-cost sensor nodes with weak computing and communication capabilities and limited power. After the sensor node collects the sensing data, the node sends the data to the background server of the base station in a mobile ad hoc manner, and the information acquisition, the processing and the analysis of a specific area at any time are realized [1]. In the future, there will be a large number of mobile nodes in the Internet of things, so it is necessary to deeply study the security of access authentication of mobile nodes in the Internet of things (Table 1).

The cloud platform of the Internet of things collects and uses data through the nodes of the Internet of things, performs data calculation and storage based on the cloud platform, improves the ability of the Internet of things to process data and the scope of data sharing, and enriches the content of cloud data. It promotes the

S. Liu and L. Xia (Eds.): ADHIP 2020, LNICST 348, pp. 232–241, 2021.
https://doi.org/10.1007/978-3-030-67874-6_22

penetration and integration of the Internet and the human world, and also brings new security issues. Due to the characteristics and limitations of IOT nodes, they are extremely vulnerable to attack. At present, scholars have carried out research on the node access of the Internet of things. Ben and others put forward the Internet of things chain is proposed to build trust in the Internet of things ecosystem. First, the system model is defined, including trusted Internet of things data server, authorization management server and semi trusted cloud re encryption proxy server. Secondly, describe the flow and algorithm of the system; finally, analyze and prove the security of pre-tuan. Based on proxy re encryption, pre-tuan will give full play to the computing power of the cloud. At the same time, ensure the security and reliability of Internet of things data sharing. In order to improve the efficiency of trusted proof of IOT nodes [2]. Gong and others proposed a threshold signature method for Internet of things based on credibility. When the sum of the credibility of the IOT nodes participating in the signature is greater than or equal to the threshold, the role of the nodes in the proof becomes greater, and vice versa. Security analysis and example analysis show that the scheme can resist the collusion attack of any member whose credibility sum is less than the threshold value, and can effectively reduce the burden of IOT nodes on the premise of ensuring the security of IOT [3].

This paper proposes an intelligent authentication method for trusted access of IOT mobile nodes driven by cloud trust. IOT mobile nodes are driven by cloud trust and determined by the processing of IOT mobile nodes and the intelligent authentication of trusted access of IOT mobile nodes. Realize the Internet of things migration driven by cloud trust. Intelligent authentication for trusted access of mobile nodes. Experimental data show that this method not only improves the reliability of traditional authentication methods, but also standardizes the authentication process.

2 Intelligent Authentication of Trusted Access of Mobile Nodes in Internet of Things Driven by Cloud

2.1 Mobile Node Determination of Internet of Things Based on Cloud Trust-Driven

In the perception subnet of the Internet of things, the roaming target domain of mobile nodes is usually random. In view of the future application trend of the Internet of things, the roaming phenomenon of mobile nodes is bound to exist in large quantities. After the mobile node joins the remote domain and passes the authentication, it can obtain all the network resources of the remote domain at will.In practical applications, the location of Internet of things mobile nodes based on cloud trust drive is generally unknown, so it is unreasonable to make the moving track of target nodes include all nodes, so it is necessary to determine the mobile nodes of Internet of things. Determining the location of each node is one of the fundamental problems in the field of wireless sensor networks. A two-step localization algorithm based on UKF filter and triangulation algorithm has been proposed. The algorithm uses a mobile node to traverse the whole network and periodically broadcasts information containing its current location. The self-localization process of the sensor node is realized by the target

tracking method of UKF [4]. This algorithm proves that it can improve the special requirements of the moving trajectory of mobile nodes, and is more suitable for the actual situation, and obtain a better positioning accuracy. Assuming that the mobile node based on cloud trust-driven Internet of things has the capability of RSSI ranging, then the schematic diagram of the Euclidean location algorithm is shown in Fig. 1. In the figure, the known unknown node B and C are known to have known BC distance or can be obtained by RSSI measurement within the wireless range of the target node L, and node A is adjacent to B, C. Then, for all the edges of the quadrilateral ABCL, and a diagonal BC, the length of the AL (the distance between node A and L) can be calculated according to the properties of the triangle. Using this method, when the unknown node obtains the distance from three or more target nodes, the mobile node based on cloud trust-driven Internet of things can be determined.

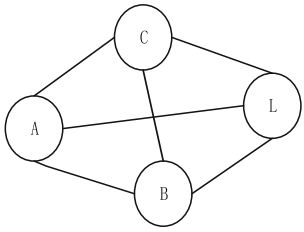

Fig. 1. Diagram of Internet of things mobile node determination based on cloud trust-driven

If a mobile node with the capability of RSSI ranging can move three times (or more) within the communication range of the sensor node and is not in a straight line, this is equivalent to meeting the requirements of the three target nodes in the Euclidean localization method [5].

The Euclidean distance-finding method uses mathematical calculation method to determine the mobile nodes of Internet of things driven by cloud trust. The mobile node determines the degree of deviation, assuming that X1, X2,. Xn is the mathematical expectation that the different mobile nodes, E (X) is a random variable, and the mobile node determination formula is as follows:

$$\mathrm{E}\ (\mathrm{X}) = \sum_{1=1}^{n} X_i \tag{1}$$

$[X_i - \mathrm{E}\ (\mathrm{X})]^2$ is the square deviation of mobile nodes, and the arithmetic mean of $[X_1 - \mathrm{E}\ (\mathrm{X})]^2$, $[X_2 - \mathrm{E}\ (\mathrm{X})]^2$, … $[X_i - \mathrm{E}\ (\mathrm{X})]^2$ is the average square deviation of this set of data., the expression formula is shown in formula 2:

$$\sigma = \frac{1}{n}\sum_{i=1}^{n} X_i[X_2 - \mathrm{E}\ (\mathrm{X})]^2 \tag{2}$$

σ is the standard deviation which measures the degree of dispersion between the measured value and the average value. The greater the standard deviation, the greater the degree of discretization of the random variables of the data, and the greater the degree of deviation in the determination of the moving nodes.

When the expected value is equal or close, the standard deviation can be used to compare the deviation degree directly [6]. If the expected value of the two groups of distributions is obviously different, the coefficient of variation should be used to compare it [7]. The coefficient of variation is the ratio of the standard deviation to the expected value and is expressed in formula 3:

$$V = \frac{\sigma}{\mathrm{E}\ (\mathrm{X})} \tag{3}$$

In the whole positioning and ranging process, the trilateral localization algorithm can only measure the position of ordinary sensor nodes. When the sensor node has the ability of RSSI ranging, it cannot measure its position, and the Euclidean algorithm can improve this situation very well. This paper combines UKF filtering to eliminate the noise interference, that is, the Internet of things mobile node processing. As a result, more accurate results are obtained.

2.2 Filtering Process of Mobile Node in Internet of Things

The cloud trust-driven mechanism is defined as follows: in an open cloud environment, when the addressing service AS1 of the Internet of things across the domain strictly adheres to certain specific constraints, and acts according to the trust value of the addressing service AS2 through the sensor protocol management mechanism [8]. When the whole system can cooperate dynamically and reach the uniform state of the underlying addressing and positioning standard, it is called the trust-driven relationship between the addressing service AS1 and the addressing service AS2 [9].

For the i(i = 1,⋯,I) mobile node of the Internet of Things driven by cloud trust, the state equation in the k(k = 1,⋯,K) iteration cycle is:

$$Xi = (k-1) + wi(k) \tag{4}$$

In the formula, $wi(k)$ represents the noise of the Internet of things mobile node system driven by cloud trust. There are two kinds of factors affecting the processing of the Internet of things mobile node. The first is the selection of the initial state vector and the other is the selection of the measurement noise. The distance between the sensor node and the moving target node is unpredictable [10]. The filtering process must require an objective equation of state to predict the next moment, so the equation of state shown in formula (4) generally believes that the position of the next moment is basically the same as the current position, however, when the initial value is close to the real value, the state prediction equation is close to true. Therefore, in order to obtain accurate filtering results, the requirements for the selection of initial values need to be improved. For the measured noise Q, it will affect the filtering speed of each step of the iterative filtering estimation [11]. Generally, when the moving target node changes

rapidly, a larger value should be taken, and a smaller value should be taken when the estimated value is close to the real value. For Q value, because the speed of moving node can be controlled, a moderate value can be set according to it. For the initial state setting, the Euclidean localization algorithm can usually be used.

2.3 Credit Value Evaluation and Processing Process of Internet of Things Mobile Node

The cloud trust value expresses the trust evaluation criterion of the underlying resource addressing service of the Internet of Things in the cloud environment, and the dynamic trust management model, the feedback-based trust driving mechanism, the trust benefit function (trust steepness function) heuristic algorithm can be adopted, The cloud-based trust evaluation algorithm is used to solve [12]. The credibility value depends on the dynamic information of the trust object which is difficult to capture, and it is difficult to verify the new time-effective weights of credit degree. To some extent, this affects the construction of trust relationship between cross-domain addressing services. In order to solve the above problems, Euclidean localization algorithm combined with cloud-based trust evaluation algorithm to improve the trust benefit function, and use the improved algorithm to solve the trust value.

According to the above discussion, the localization method can be divided into two steps: firstly, the initial position of sensor node is determined by Euclidean positioning and distance finding method, and then the UKF filtering method is used to locate the sensor node accurately. Since the work of each sensor is independent, for sensor I, the flow chart of each sensor is shown in Fig. 2 when the time threshold Tr meets certain conditions.

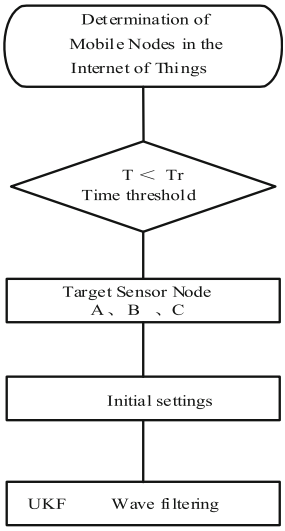

Fig. 2. Flow chart of Internet of things mobile node processing

This method reduces the requirements of moving trajectory of mobile nodes, and can obtain satisfactory positioning accuracy even if the nodes move at will. This method is improved at the expense of a certain amount of computation.

Based on the Euclidean positioning algorithm, the mobile node processing of the Internet of Things is finally realized by combining the cloud trust value. And lays the foundation for the trusted access intelligent authentication of the Internet of Things mobile node.

2.4 Intelligent Authentication of Trusted Access to Internet of Things Mobile Node

The intelligent authentication of trusted access of Internet of things is designed by determining the mobile node of Internet of things based on cloud trust drive and the processing of mobile node of Internet of things. On the basis of traditional authentication protocol of mobile node of Internet of things, intelligent authentication of trusted access of mobile node of Internet of things is carried out.

Traditional IoT mobile node authentication model mainly consists of Internet of things Management Center (CA-IoT), mobile aggregation terminal (Mobile Sink Node, MSN, base station (Base Station,BS), sensor node (Sensor) and Internet of things mobile node (Cluster Head,. CH) composition [13].

First, the traditional mobile node authentication protocol of the Internet of things is initialized. In the system initialization phase, when MSN registers with CA-IoT with its own real identity, CA-IoT provides a series of non-linked random pseudonym identity (PID),. PID = {pid1,pid2, …, pidn}. The local authentication server (Home Authentication Server,HAS) will be pre-assigned to each pseudonym identity Pidipid public key pkpidi and the corresponding private key skpidi and then CA-IoT will put all the tuples (pidi,pkpidi,skpidi) sent securely to MSN [14]. There has been a detailed and quantitative study of the storage space of the anonymous key and related certificate for long-term use of a pseudonym in advance. The pre-loaded pseudonym is applied and the storage overhead is within a reasonable range.

Modbus protocol is an important data to realize trusted access intelligent authentication of IoT mobile node, which determines the communication state of trusted access intelligent authentication of IoT mobile node [15]. If that communication protocol of the Modbus is not match with the trusted access intelligent authentication system of the Internet of Things mobile node, a separate remote communication can not be realized, and when the mobile node of the Internet of things is trusted to access the intelligent authentication response message, it is necessary to query in a broadcast mode, otherwise, no response message will be received. Since the Internet of things mobile node trusted access intelligent authentication response message is also composed of Modbus protocol, it is necessary to confirm the Internet of things mobile node trusted access intelligent authentication data and error detection domain. If the trusted access intelligent authentication of the Internet of things mobile node occurs in the process of receiving messages, then the trusted access intelligent authentication of the Internet of things mobile node will not execute its command, so it is necessary to establish the transmission process. Feedback the error message and send it out in a timely manner. The feedback circuit principle is shown in Fig. 3.

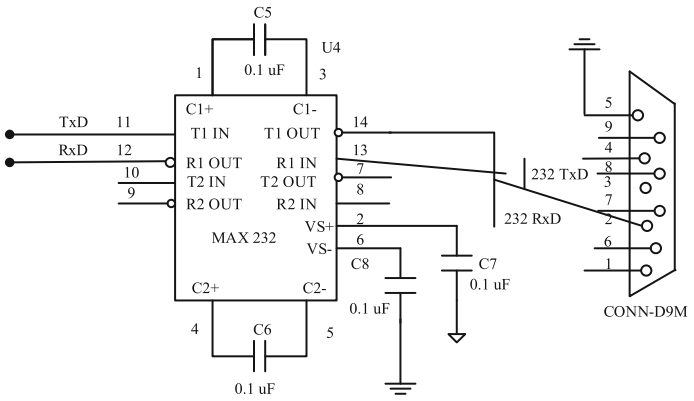

Fig. 3. Schematic diagram of error message feedback circuit

The application network makes the Modbus communication protocol match with the trusted access intelligent authentication of the Internet of things mobile node, so any action of the trusted access intelligent authentication of the Internet of things mobile node can be realized. In the process of trusted access intelligent authentication of Internet of things mobile nodes, the control system can be used not only as master system but also as slave system.

Improve the initial position accuracy of the filtering by using the Euclidean positioning method, thereby improving the processing effect of the Internet of Things mobile node, and simultaneously, on the basis of the traditional Internet of Things mobile node authentication protocol, conducting the intelligent authentication of the Internet of Things mobile node to the trusted access, And the trusted access intelligent authentication of the Internet of Things mobile node which is driven by the cloud trust is completed.

3 Results

In order to verify the validity of the proposed intelligent authentication method for trusted access of mobile nodes in Internet of things (IoT) driven by cloud trust, experiments are carried out to demonstrate and analyze the effectiveness of the proposed method. In order to ensure the accuracy of simulation test, the traditional iotchain: establishing trust in the Internet of things ecosystem using blockchain (reference [2] method) is used as the comparative experimental object, and the data generated by the two methods are given in the same data chart.

3.1 Experimental Environment and Test Data Setting

The specific experimental environment is as follows: Intel (R) core (TM) i5-6500 processor, 3.20 ghz CPU, 16 GB memory, windows 10 system version, 64 bit operating system.

In order to ensure the accuracy of the simulation test process, set the test parameters, first modify the address configuration mechanism of hierarchical mobile IP to make it use stateful address configuration, and access router 1 (AR1) in the home proxy (HA). AR2 and AR3 install dibbler software and package filtering software, and install RADIUS software on the server. It starts HMIPv6 program on MN, HMIPv6 program and DHCPv6 server program on HA, DHCPv6 server program and routing advertisement protocol on AR1, AR2 and AR3 respectively. In-service The AAA server-side program is started on the server. Where the user name option format, the password option format, and the authentication failure information are defined as follows:

Table 1. Lab parameter settings tabl

Identification	Character length
Username Option Identification (44)	Option Length (20 bytes)
User name (16 bytes)	
Password Option Identification (45)	Option Length (20 bytes)
Password ciphertext (16 bytes)	
Failure Information Option Identification (46)	Option Length (20 bytes)
Failure information (16 bytes)	

The experiment completes the access authentication of handoff process from home to AR1, AR2 in MAP1 and AR3 in MAP2, and the access authentication process from MAP1 to MAP2. If the user adopts the wrong user name or password, the IP address cannot be obtained during the handoff process, the access authentication fails, the handover process cannot be completed, and the MN is refused to join the phase. The network to which it is to be.

The simulated cloud trust-driven object-of-things mobile node, in the X–Y plane, the area[0, 1000 m] × [0, 1000 m], is randomly scattered by the airplane to the unknown sensor node and a movable, position-aware target node, and at the same time, it is assumed that the node can take off, then it will follow a predetermined trajectory, The sensor nodes on the air side to the ground periodically release their position information at a predetermined time interval. While the sensor node in the unknown position can measure its distance from the node. When the node is located with the GPS, it is assumed that the covariance mean value in the self-positioning of the moving target node is assumed in the simulation A positioning error of 50 m.

3.2 Analysis of Test Results

According to the setup of the experiment process, the experimental results of two kinds of authentication methods for mobile nodes of the Internet of things are obtained, and the experimental results are drawn into charts as shown in Fig. 4:

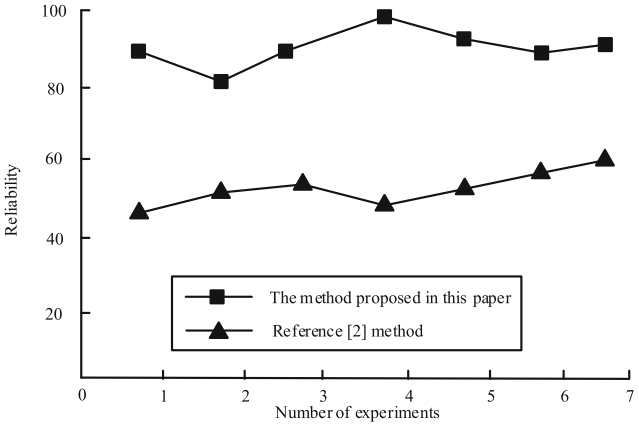

Fig. 4. Comparison table of experimental results

It is proved by experiments that when the server is secure and reliable, the configuration information of software and hardware of MSN platform will not be leaked to other legitimate users in the network, nor will it be leaked to CH, to effectively protect the privacy of the platform. This paper discusses the time needed to exchange information between the duplicate address detection process and the AAA protocol without increasing the additional delay and assigning a legal IP address to the MN as the online forwarding address when the authentication is successful.

The experiment and demonstration analysis show that the trusted access intelligent authentication method of the cloud trust-driven Internet-of-Things mobile node has high credibility, and at the same time, the self-adaptability and the flexibility of the trusted access authentication of the cloud trust-driven Internet-of-things mobile node are enhanced.

4 Conclusions

Because of the lack of trusted authentication in the traditional cloud trust driven mobile nodes in the Internet of things, the security and reliability of data processing in the Internet of things are improved. An intelligent authentication method for trusted access of mobile nodes in the Internet of Things driven by cloud trust is proposed. The method is based on the determination of mobile nodes in the Internet of Things driven by cloud trust, relying on the processing of mobile nodes in the Internet of Things and the intelligent authentication of trusted access of mobile nodes in the Internet of Things. Trusted Access Intelligent Authentication for Mobile Nodes of the Internet of Things Driven by Arbitrary. The experimental results show that the intelligent authentication method for trusted access of mobile nodes in Internet of things driven by cloud can effectively verify the validity of mobile nodes. While the authentication is successful, the mobile node (MN) is configured with a legal IP address, which can meet the needs of practical application and greatly reduce the hidden danger of information security.

Acknowledgment. "13th Five-Year Plan" for national social sciences education program-Education MinistryKey Subject in 2017. Research on the innovation ability of application-oriented talents training under the background of education supply-side reform: a case study of "The Internet of things".

References

1. Kim, D.Y., Kim, S., Park, J.H.: Remote software update in trusted connection of long range IoT networking integrated with mobile edge cloud. IEEE Access, PP(99), 1–1 (2017)
2. Bin, Y., Jarod, W., Surya, N., et al.: IoTChain: establishing trust in the Internet of Things ecosystem using blockchain. IEEE Cloud Comput. **5**(4), 12–23 (2018)
3. Gong, B., Wang, Y., Liu, X., et al.: A trusted attestation mechanism for the sensing nodes of Internet of Things based on dynamic trusted measurement. China Commun. **15**(2), 100–121 (2018)
4. Yuli, Y., Rui, L., Yongle, C., et al.: Normal cloud model-based algorithm for multi-attribute trusted cloud service selection. IEEE Access, 1–1 (2018)
5. Xu, D., Fu, C., Li, G., et al.: Virtualization of the encryption card for trust access in cloud computing. IEEE Access, PP(99), 1–1 (2017)
6. Lu, M., Liu, S.: Nucleosome positioning based on generalized relative entropy. Soft. Comput. **23**(19), 9175–9188 (2018). https://doi.org/10.1007/s00500-018-3602-2
7. Pawlick, J., Chen, J., Zhu, Q.: ISTRICT: an interdependent strategic trust mechanism for the cloud-enabled internet of controlled things. IEEE Trans. Inf. Forensics Secur. **14**(6), 1654–1669 (2018)
8. Tsai, J.L., Lo, N.W.: A privacy-aware authentication scheme for distributed mobile cloud computing services. IEEE Syst. J. **9**(3), 805–815 (2015)
9. He, D., Kumar, N., Khan, M.K., et al.: Efficient privacy-aware authentication scheme for mobile cloud computing services. IEEE Syst. J. 1–11 (2017)
10. Liu, S., Liu, D., Srivastava, G., et al.: Overview and methods of correlation filter algorithms in object tracking. Complex Intell. Syst. (2020). doi:10.1007/s40747-020-00161-4
11. Zhu, C., Rodrigues, J.J.P.C., Leung, V.C.M., et al.: Trust-based communication for the industrial Internet of Things. IEEE Commun. Mag. **56**(2), 16–22 (2018)
12. Yu, B., Wright, J., Nepal, S., et al.: Iotchain: establishing trust in the internet of things ecosystem using blockchain. IEEE Cloud Comput. **5**(4), 12–23 (2018)
13. Chen, J., Tian, Z., Cui, X., et al.: Trust architecture and reputation evaluation for Internet of Things. J. Ambient Intell. Humanized Comput. **10**(8), 3099–3107 (2019)
14. Fu, W., Liu, S., Srivastava, G.: Optimization of big data scheduling in social networks. Entropy **21**(9), 902 (2019)
15. Porambage, P., Okwuibe, J., Liyanage, M., et al.: Survey on multi-access edge computing for internet of things realization. IEEE Commun. Surv. Tutorials **20**(4), 2961–2991 (2018)