An Authentication Method for Ubiquitous Electric Internet of Things Communication Terminal Based on Coordinated Filtering

Xinhui Zhong

1 Digital Grid Research Institute, China Southern Power Grid.

*Corresponding author’s e-mail: zhongxh@csg.cn

Abstract. The current terminal authentication is mainly based on the identification of user markers, which can not be accurately judged according to the user behavior. It is not only complex to calculate the hardware requirements, but also inefficient when processing a large number of requests. In order to optimize the above defects, an identity authentication method for ubiquitous power Internet of Things communication terminals based on coordination filtering is proposed. After establishing the user identity characteristic information matrix of the communication terminal, the identity authentication protocol is designed by using the public key. Trust degree is introduced to improve coordination filtering, and the improved algorithm is used to process user identity information, so as to realize identity authentication. The design of comparative experiment verifies that the average certification time of the research method is less than 6ms, which can effectively carry out safety protection and is feasible.

1. Introduction

Ubiquitous power IOT is a special IOT after introducing IOT technology into the current operating power grid to realize extensive connection and sharing of various infrastructure equipment, management and maintenance personnel, power environment, and power grid operation information in the power grid. Ubiquitous power IOT is the technical integration of communication technology and artificial intelligence technology in the power industry. Ubiquitous power IOT is built to realize comprehensive energy efficiency services in distributed grid power generation, grid electrical equipment access, industrial integration of multiple new energy utilization and financial integration of related industries, and grid operation data processing [1]. At present, the basic technology and external environment in the development of the ubiquitous electric Internet of Things have basically developed and matured. The implementation of ubiquitous electric Internet of Things brings about not only the speed and convenience, but also the problem of information security protection. In the construction of the data access system of the ubiquitous electric Internet of Things, it is necessary to overcome the defects of the traditional terminal security access technology, that is, the identity of the end user should be authenticated before the communication terminal is connected to the ubiquitous power Internet of Things. If the measurements meet in electric power network access security policy, allows access to the terminal in the power of things, or be disconnected terminal or to connect to the specified isolation area, thus to boycott before most of the potential attacks in occur, will flood in the power of the Internet of things trust chain extension from the terminal to the network, to ensure the security and credibility of the connection of each node in the ubiquitous electric Internet of Things, and to realize
the trusted access and transmission of data in the Internet of Things [2]. The identity authentication in the traditional network is mainly realized by the authentication password or the configured smart card. This authentication method is simple and efficient, but it has the defects and limitations that are easy to be cracked, so it is no longer used for the identity authentication alone [3]. With the increasingly extensive application of biometric technology, it is more and more common to use the unique voice print, fingerprint, pupil and other information on the human body as authentication markers for identity verification [4]. Such as the current most common fingerprint access control and punch in; the combination of voice print recognition and communication technology to realize remote authentication has been widely used [5]. However, the above method of using biometrics to authenticate the identity has some defects when it is applied to the authentication of passing terminal. In addition, the use of user name/password, dynamic password card, block chain, quantum and other authentication markers for identity authentication is vulnerable to theft [6].

Now the two-factor authentication mode which is widely used at home and abroad is based on these authentication modes. However, the above authentication methods are mainly based on the basic principle of changing the identity identification. The authentication and identification process is relatively complex, and the efficiency of authentication processing is difficult to meet the communication authentication needs of the ubiquitous power Internet of Things. According to the above analysis content, this paper will study the identity authentication method of ubiquitous power Internet of Things communication terminal based on coordinated filtering by referring to the existing authentication technology of Internet of Things communication terminal at home and abroad.

2. An Authentication Method for Ubiquitous Electric Internet of Things Communication Terminal Based on Coordinated Filtering

2.1. The identity characteristic information matrix of end users of ubiquitous electric Internet of Things communication is established

This study adopts coordinated filtering algorithm to filter the user identity authentication credential information of ubiquitous power IOT communication terminal. According to the principle of coordinated filtering algorithm, the corresponding information matrix should be established based on the identity characteristics of ubiquitous power IOT communication terminal users first. In this paper, based on the two-dimensional user characteristics information matrix, we introduce the user usage items of communication terminal to establish the three-dimensional model of ubiquitous power IOT communication terminal user identity characteristics \( U \times C \times I \), where \( U \) is the communication terminal user, \( C \) is the user usage context information of the communication terminal, \( I \) is the communication terminal user item [7]. In filtering the ubiquitous power IOT communication terminal user identity, this study selects the established communication terminal user characteristic information matrix to replace the above three-dimensional model of \( C \), so as to achieve the initial classification of the end-user identity. Let \( C = \{c_1, c_2, \ldots, c_m\} \), where \( c_i \) denotes the information attributes of the communication terminal to identify the user identity. For n ubiquitous power IOT communication end-users, the \( n \times m \) matrix of their identity feature information is established as follows[8].

\[
\begin{bmatrix}
  x_{11} & x_{12} & \cdots & x_{1m} \\
  x_{21} & x_{22} & \cdots & x_{2m} \\
  \vdots & \vdots & \ddots & \vdots \\
  x_{n1} & x_{n2} & \cdots & x_{nm}
\end{bmatrix}
\] (1)

Each row vector consisting of elements in the above matrix represents a user's authentication feature information, and each authentication information feature is described by multiple attributes.
\( x_j \) denotes the \( j \)th attribute value of the user's \( i \)th identity feature information [9]. In this paper, the four identity feature attributes of department, level, name, and management authorization level, which are the most important for communication terminal user identification, are selected for initial identity classification [10]. The above identity feature attributes are mainly binary variables and nominal variables. For binary variables whose attributes take values as two mutually independent values, the dissimilarity between attribute vectors can be calculated based on the number of different state variables of the vectors corresponding to the actual attributes [11]. The weights represented by the attribute taking values of two mutually independent values of nominal type variables are not necessarily equal, and if the two state attributes take the same weight, the formula for calculating the phase dissimilarity of the variables is as follows [12].

\[
d(i,j) = \frac{a+b}{n} \tag{2}
\]

In the above formula, \( a \) is the number of attribute states with the same values of object \( i \) and object \( j \) in the attribute of binary variables. \( b \) is the number of attribute states with different values of object \( i \) and object \( j \) in the binary variable attribute; \( n \) is the number of all value attribute states of object \( i \) and object \( j \). The corresponding state attributes of nominal variables are independent of each other [13]. Therefore, for nominal variables with \( n \) state numbers, the formula for calculating the difference is as follows:

\[
d(i,j) = \frac{m-n}{n} \tag{3}
\]

In the above formula, \( m \) is the same number of attributes whose attribute states of the two variables match each other. After calculating the differences of the corresponding variables of the communication end-user authentication attribute, the k-means clustering algorithm is used to cluster the user identity information [14]. After user authentication information is preliminarily classified by K-means clustering algorithm, user identity attribute features are extracted according to the similarity of corresponding identity attributes, and the identity characteristic information matrix of end users of ubiquitous electric Internet of Things communication is established [15].

2.2. Communication terminal authentication protocol design

Since the ubiquitous power IOT communication network needs to access new end users at any time, this study will design the terminal authentication protocol under the public key mechanism [16]. The schematic diagram of two-way authentication between the ubiquitous power IOT communication network and the communication terminal using public key is shown in Fig.1 below:
The detailed public key-based two-way authentication process is as follows:

1. The ubiquitous power IOT communication terminal generates a random number r1, multiplies and encrypts the random number r1 with the ID marked by the communication terminal in the ubiquitous power IOT according to the RSA encryption algorithm, and sends the encrypted information to the server of the communication network via the communication port.

2. The server of the communication network decrypts the received encrypted information in accordance with the decryption process of RSA encryption algorithm, obtains the random number r1, generates the random number r2 and the corresponding symmetric key ECB_KEY, and sends the random numbers r1, r2 and the symmetric key ECB_KEY encrypted to the communication terminal [17].

3. The communication terminal decrypts random numbers r1 and r2 and the symmetric key ECB_KEY, and determines the identity of the communication network server of the transmission object based on the random number r1 in the decryption result. The symmetric key ECB_KEY is used to encrypt the received decrypted r2 in accordance with the ECB encryption algorithm and send it to the communication network server whose identity has been determined. The communication network server receives the encrypted information and decrypts it, and compares the random number obtained from the decryption with the originally generated random number r2 to complete the authentication of the communication terminal.

Based on the above-designed authentication protocol for communication terminal user access, an authentication password is introduced for security enhancement. Before authentication, the communication terminal performs hashing operations on the user input authentication ID information and the user password respectively, and sends the result of the hashing operations to the server. The server searches and matches the hash information of the user ID and continues to connect to the communication terminal if the user ID information is matched; if the corresponding hash information of the user ID cannot be found, the server directly disconnects from the communication terminal. After confirming the connection to the communication terminal, the server looks for the hash information of the user password based on the hash information of the user ID. If the user password hash information can be found, the user authentication connection request is passed, otherwise the connection is disconnected. After that, the authentication is performed according to the public key-based two-way authentication process mentioned above. The communication terminal will communicate using the determined communication key based on the received two-way authentication result. After designing
the communication terminal authentication protocol, the coordinated filtering algorithm for filtering user identity information is improved.

2.3. Coordinated filtering improvements based on trust

The classical coordinated filtering algorithm has some problems such as rough computing granularity and low recommendation coverage. In order to improve the accuracy of filtering for different user identities, this study introduced trust to improve the coordinated filtering algorithm. The direct trust degree of the user identity is calculated according to the corresponding behavior of the login ID of the communication end user. If in the communication process of ubiquitous power Internet of Things, there are more communications between two user IDs using fixed communication terminals, it indicates that the trust degree of the two user IDs is high. Similarly, if the user ID communicates with the server with higher management level in the ubiquitous power Internet of Things communication server more times, the trust of this user ID will be improved accordingly. Based on the interaction information between the communication end user and the server, this study calculates the user's trust degree. The formula is described as follows [18]:

$$IT(u, v) = \frac{|I_u \cap I_v|}{|I_u|}$$ (4)

In the above formula, $I_u \cap I_v$ is the interactive information set of communication end user $u$ and communication server $v$; $I_u$ represents the set of all communication information of communication end user $u$ in the past; $I_v$ is the set of all the past interaction information of the communication server; $| |$ represents the amount of interactive information. In the process of ubiquitous power Internet of Things communication, if the authentication is successful, the server will enhance the trust of the identity of the end user. Otherwise, it will reduce the user's trust degree to the greatest extent, thus affecting the identity authentication of the terminal. In order to avoid the security problems caused by the theft of the authentication credentials of the end users, the indirect trust formula is also introduced to evaluate the trustworthiness of the end users [19]. The formula of indirect trust is described as follows:

$$INT(u, v) = \frac{\sum_{p \in U_{(w,t)}} DT(w, p) DT(p, t)}{\sum_{p \in I_{(w,t)}} DT(w, p)}$$ (5)

In the above formula, $U_{(w,t)}$ is the set of users of other communication terminals trusted by server $w$ and $t$; $p$ is a trust communication terminal trusted by both server $w$ and $t$; $DT$ is the level of trust between servers. Therefore, the final calculation formula of the trust degree of end users of electric Internet of Things communication is as follows:

$$DNT(u, v) = \lambda IT(u, v) + (1 - \lambda) INT(u, v)$$ (6)

In the above formula, $\lambda$ is the adjustable parameter in the interval [0,1], and its calculation formula is as follows:

$$\lambda = \frac{DT^2}{DT^2 + INT^2}$$ (7)

After introducing the trust degree of the communication terminal calculated in the above formula to the user, the processing effect of the coordinated filtering algorithm is enhanced. The improved
coordination filtering algorithm is used to realize the identity authentication of the ubiquitous power Internet of Things communication terminal.

2.4. Realize the identity authentication of communication terminal

The communication terminal downloads the updated authentication information from the server of the communication network regularly when the communication terminal uses the improved trust filtering algorithm to authenticate the identity of the communication terminal. When a user requests communication with the communication terminal, the communication server issues the corresponding response. Users input their own authentication information, and the communication terminal calculates the current user's trustworthiness according to the above formula. The user information is processed according to the following coordinated filtering process to improve the efficiency of identity authentication [20].

1) First calculate the direct trust, indirect trust and final trust of users. The first k users with the highest trust degree were selected to form the trust neighbor set.

2) According to the principle of coordinated filtering algorithm, the similarity between users is calculated to screen users in the trusted neighbor set. The calculation formula is as follows:

\[
P_{u,v} = \bar{r}_u + \alpha \sum_{q \in U_T} \left[ \alpha U_s(u,q) + (1 - \alpha) DNT(u,q) \right] (r_{q,i} - \bar{r}_q) \sum_{q \in U_T} \left[ \alpha U_s(u,q) + (1 - \alpha) DNT(u,q) \right]
\]

In the above formula, \( \alpha \) is the adjustable parameter; \( U_s(u,v) \) is the similarity between user \( u \) and user \( q \); \( \bar{r}_u \) and \( \bar{r}_q \) are ratings of the degree of trust to user \( u \) and user \( q \) respectively; \( U_T \) is the trusted neighbor set; \( r_{q,i} \) is an element in the user trust rating matrix. After selecting the users in the trusted neighbor set, the trust degree of the new server corresponding to the new users is evaluated, and the trust level of the server to the users is determined. According to the trust level, the user's trust level is transmitted to the communication response node of the Internet of Things according to the communication transmission protocol of the ubiquitous power Internet of Things. After receiving the communication request, the communication response node issues the authentication message. The user's identity is authenticated according to the identity authentication protocol of the communication terminal designed above, and the Reply message received by the communication node after authentication is forwarded to the Internet of Things gateway to confirm the trust status of the authentication certificate of the communication terminal and complete the identity authentication of the communication terminal. According to the above process, the research on the identity authentication method of ubiquitous power Internet of Things communication terminal based on coordinated filtering is completed.

3. Experimental study

3.1. Experimental purpose and setup

Purpose: In this section, the feasibility and effectiveness of the coordination filtering-based authentication method for ubiquitous power IOT communication terminals proposed above will be investigated through experiments.

Content setting: The ubiquitous power IOT in a large smart grid is selected as the background environment for this experiment, and there are 500 communication terminals in this ubiquitous power IOT, and these communication terminals are taken as the research object of this experiment. The authentication method proposed in this paper is used as the experimental group, and the authentication method based on password identification is selected as the comparison group. With the objective of
testing the authentication performance and security of communication terminals after applying the two
groups of methods, the experimental data are counted and the experimental verification is completed.

3.2. Experimental results
The experiments test the efficiency of authentication processing of the ubiquitous power IOT
communication terminal authentication service, and test the load on the terminal network computing
server by running a large number of authentication requests for a long time. Each group is tested 20
times, and the duration of each test is 100 min. In each group, the authentication processing time is
recorded and averaged to obtain the average authentication processing time of the communication
terminal in each group. In addition, by recording the number of server responses to authentication
requests during the test, the average number of transactions per second processed by the server is
obtained.

| Test group | Maximum number of concurrency | Min/max time/ms | Average time/ms | Number of authentication transactions processed by the server per unit time |
|------------|-------------------------------|-----------------|----------------|---------------------------------------------------------------|
| 1          | 100                           | 1.1/7.9         | 4.2            | 196.1                                                         |
| 2          | 200                           | 1.4/8.7         | 4.8            | 185.4                                                         |
| 3          | 300                           | 1.7/9.2         | 5.3            | 180.7                                                         |

Analyzing the data in Table 1 above, it can be seen that the maximum number of concurrent
authentication requests that the terminal can accept when using the experimental group method to
authenticate the access user is significantly larger than that of the communication terminal applying
the comparison group method, and the maximum and minimum time range and upper and lower limits
for authentication of the communication terminal applying the experimental group method are smaller
than those of the communication terminal applying the comparison group method. From the viewpoint
of the average processing time of authentication of communication terminals, the average
authentication time of communication terminals applying the experimental group method is less than
6ms, while the minimum average processing of communication terminals applying the comparison
group method is greater than 9ms. Meanwhile, the number of authentication transactions per unit time
of terminals applying the experimental group method is much larger than that of the comparison group
method. The above analysis shows that the authentication performance of the communication terminal
applying the experimental group method is better.

Figure 2 below shows the danger index (the proportion of communication content cracking to the
full content of communication) of the IOT terminal after applying the two methods of authentication
during the above test, when the simulated checkout authentication identity attacked the network.
Figure 2 Comparison of communication terminal security

Analysis of the curves in the above figure shows that the application of the two authentication methods effectively reduces the hazard index of the IOT communication terminal. In comparison, the hazard index of the communication terminal applying the experimental group method is lower, and the hazard index of the terminal applying the experimental group method changes less and is more stable during the overall experiment. It shows that the experimental group method is more reliable for protecting the terminal security when applied.

The above experimental data analysis shows that the ubiquitous power IOT communication terminal authentication method based on coordinated filtering proposed in this paper can support more authentication services per unit time, and the authentication of communication terminals applying the method is more efficient, i.e., the authentication method studied in this paper is more effective.

4. Conclusion
At present, the information construction of the power grid has achieved more significant results, the introduction of the Internet of Things technology to improve the efficiency of the power system. However, the characteristics of ubiquitous power IOT terminal distribution, complex deployment environment and flexible access methods may cause the sensitive information contained in the network to be maliciously tampered and leaked when the network is attacked, and at the same time, due to the special node structure of IOT, the communication terminal connected to the IOT node may be illegally stolen or used to reverse control the power grid, thus endangering the stable operation of the power grid. To this end, this paper investigates the authentication method of ubiquitous power IOT communication terminals based on coordinated filtering, and verifies the feasibility of the method through experiments.

References
[1] Zhu JiaDong, JiaDong Zhu. Research on the Key Technologies of the Ubiquitous Electric Internet of Things. Journal of Physics: Conference Series,2020,1682(1): 012045.
[2] CHEN Xuefeng. Simulation of Visual Apparent Evaluation Method for Multimedia Human–Computer Interaction. Computer Simulation,2018,35(06):172-175+179.
[3] Abir Mhenni, Estelle Cherrier, Christophe Rosenberger, Najoua Essoukri Ben Amara. Double serial adaptation mechanism for keystroke dynamics authentication based on a single password. Computers & Security,2019,83(1):151-166.
[4] Joseph Teena, Kalaiselvan S. A., Aswathy S. U., Radhakrishnan R., Shamna A. R.. A multimodal biometric authentication scheme based on feature fusion for improving
security in cloud environment. Journal of Ambient Intelligence and Humanized Computing, 2020, 12(6): 6141-6149.

[5] J Paul Rajasingh, D Sai Yaswanth. Fingerprint Authentication. International Journal of Engineering and Advanced Technology (IJEAT), 2021, 10(5): 87-89.

[6] Elshamy Elsayed M., Hussein Aziza I., Hamed Hesham F. A., Abdelghany M. A., Kelash Hamdy M.. Voice over internet protocol voicemail security system using two factor authentication and biometric prints with new efficient hybrid cryptosystem. Multimedia Tools and Applications, 2020, 80(7): 9877-9893.

[7] Piotr Zawadzki. Quantum identity authentication without entanglement. Quantum Information Processing, 2019, 18(1): 1-12.

[8] Jui-Chan Huang, Ming-Hung Shu, Bi-Min Hsu, Chien-Ming Hu. (2020). Service architecture of IoT terminal connection based on blockchain identity authentication system. Computer Communications, 160(2):411-422.

[9] Quan Liu, Bei Gong, Zhenhu Ning. (2020). Research on CLPKC-IDPKC cross-domain identity authentication for IOT environment. Computer Communications, 157(5):410-416.

[10] Shivendu Mishra, Ritika Yaduvanshi, Kumkum Dubey, Prince Rajpoot. (2021). ESS-IBAA: Efficient, short, and secure ID-based authentication algorithm for wireless sensor network. International Journal of Communication Systems, 34(8): e4764.

[11] Kumari Saru, Renuka Km.. (2019). Design of a Password Authentication and Key Agreement Scheme to Access e-Healthcare Services. Wireless Personal Communications, 117(1): 27-45.

[12] Ali Qazi Ejaz, Ahmad Naveed, Malik Abdul Haseeb, Rehman Waheed Ur, Din Aziz Ud, Ali Gauhar. (2019). ASPA: Advanced Strong Pseudonym based Authentication in Intelligent Transport System. PLoS one, 14(8): e0221213.

[13] Koumpis N. P., Panagiotou P. A., Arvanitakis I.. (2021). A critical comparison on attitude estimation: From gaussian approximate filters to coordinate-free dual optimal control. IET Control Theory & Applications, 15(10): 1297-1313.

[14] Evangelina Lara, Leocundo Aguilar, Mauricio A. Sanchez, Jesús A. García. (2020). Lightweight Authentication Protocol for M2M Communications of Resource-Constrained Devices in Industrial Internet of Things. Sensors, 20(2):501.

[15] Kyoungsoo Bok, Geonsik Ko, Jongtae Lim, Jaesoo Yoo. (2020). Personalized content recommendation scheme based on trust in online social networks. Concurrency and Computation: Practice and Experience, 32(18):e5572.

[16] Armieille Noulapeu Ngaffo, Walid El Ayeb, Zied Choukair. (2020). A time-aware service recommendation based on implicit trust relationships and enhanced user similarities. Journal of Ambient Intelligence and Humanized Computing, 12(2): 3017-3035.

[17] Gong Liangqin, Alghazzawi Daniyal M., Cheng Li. (2021). BCoT Sentry: A Blockchain-Based Identity Authentication Framework for IoT Devices. Information, 12(5):203-203.

[18] González Guílñen Carlos E., González Vasco María Isabel, Johnson Floyd, Pérez del Pozo Ángel L.. (2021). An Attack on Zawadzki’s Quantum Authentication Scheme. Entropy, 23(4):389-389.

[19] Mahesh Kumar Morampudi, Sowmya Veldandi, Munaga V. N. K. Prasad, U. S. N. Raju. (2020). Multi-instance iris remote authentication using private multi-class perceptron on malicious cloud server. Applied Intelligence, 50(1):1-19.

[20] Izwa Altaf, Muhammad Arslan Akram, Khalid Mahmood, Saru Kumari, Hu Xiong, Muhammad Khurram Khan. (2020). A novel authentication and key-agreement scheme for satellite communication network. Transactions on Emerging Telecommunications Technologies, 32(7):e3894.