Research on the Universal Access Security Authentication Technology of Multi-source Heterogeneous Terminal Communication Module

Bao-ren Chen[1(✉)], Dan-ke Hong[1], Li Wang[1], Yong-tong Ou[2], and Xin-hui Zhong[2]

[1] Communication Office of China Southern Power Grid, Guangzhou 510670, China
cbr4256l@163.com

[2] Digital Power Grid Branch of China Southern Power Grid Digital Power Grid Research Institute, Guangzhou 510670, China

Abstract. Access interference and security authentication of multi-source and heterogeneous terminals are always important factors that affect the successful communication of wireless networks. Because of the contradiction between the authentication efficiency of handoff and the access security, the security of the traditional multi-source heterogeneous terminal communication module cannot meet the application requirements. Aiming at this problem, this paper puts forward the research on the security authentication of multi-source heterogeneous terminal communication module. Using the uniform data communication protocol, we collect and process the data of multi-source heterogeneous terminal, and design the access security authentication protocol based on random number. Experimental results show that the authentication technology of multi-source heterogeneous terminal communication module has low authentication delay and good stability, and its overall security is improved.

Keywords: Multi-source heterogeneous terminal · Communication module · Pan-access · Security authentication technology

1 Introduction

With the rapid development of information science and technology and the popularization of network applications, especially the development of mobile networks, intelligent mobile terminals, mobile applications and other technologies, mobile office and remote operation tend to mature, making remote office more convenient and effective, and greatly improving the efficiency and efficiency of work [1]. At present, wireless network connection is not only a simple way of network access, but also a lot of important applications such as language service, video service and location-based service. Users pay more attention to the fluency of browsing after network connection, but with the rapid development of network multimedia application market, the number of various network applications increases rapidly, and the wireless interference

S. Wang et al. (Eds.): IoTCare 2021, LNICST 414, pp. 3–14, 2022.
https://doi.org/10.1007/978-3-030-94185-7_1

problems encountered by dynamic users in the process of network connection increase accordingly, which leads to the poor quality of network service and difficult to achieve the expected experience of users. In addition, due to the characteristics of mobile networks and terminals, information security problems caused by network viruses and hackers are becoming more and more important [2]. Especially in the field of healthcare settings authentication, network virus not only interferes with the communication process of medical information, but also causes the loss of patients' privacy information [3]. Therefore, it is urgent to study the secure access scheme based on mobile environment. The importance of information security is self-evident, especially for banks, State Grid, public security organs and other government agencies and national enterprises, information security is particularly important [4]. Therefore, how to ensure that confidential data will not be leaked, and to achieve the authentication of mobile access objects is also the most important security access scheme.

In reference [5], a security protection method of user login information authentication based on qos-afd was proposed. By analyzing the failure frequency and dispersion degree of user information in the Internet of things, possible attacks are detected. Firstly, the average value of the historical user information interval is calculated by power-law weighting method, and the delay interval of the next user information is calculated by exponential distribution function, In reference [6], a new two-way authentication security enhancement protocol was proposed. Different from the traditional RFID authentication protocol, the proposed protocol uses a zero knowledge proof based authentication method to authenticate the membership, The zero knowledge proof is achieved by the real-time information interaction between the prover and the verifier, and the identity security of the participants is defined to the security of their own identity key. In the practical application of traditional access security authentication methods, there is a conflict between the authentication efficiency of handoff between heterogeneous networks and access security, which leads to the security vulnerability of security authentication methods.

Therefore, the multi-source heterogeneous terminal communication module panaccess security authentication technology is proposed to solve the problems mentioned above.

2 Design of Universal Access Security Authentication Technology for Multisource Heterogeneous Terminal Communication Module

2.1 Multisource Heterogeneous Data Collection Processing

In order to process the dynamic flow data collected by multi-source heterogeneous data and be used by other services efficiently, it is necessary to collect multi-source data, which plays an important role in the analysis and decision-making of subsequent services [7]. The collection of heterogeneous data refers to the integration of interconnected distributed heterogeneous data sources to form a "global view" of the underlying data sources, as shown in Fig. 1.

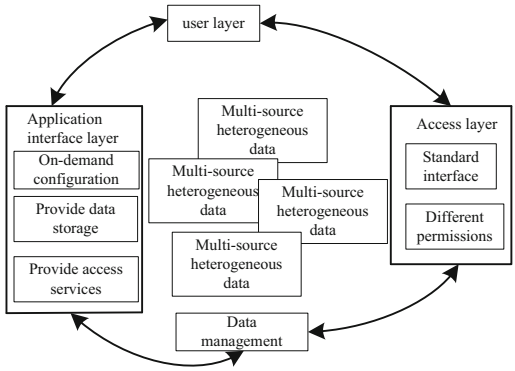


Fig. 1. Global view of multi-source heterogeneous data

So that users can easily and transparently access the required data. The process of determining data collection points is as follows:

A circle with radius r is known, and the following conditions are satisfied:

$$\begin{cases} x_{\max} - r \le x_s \le x_{\min} + r \\ y_{\max} - r \le y_s \le y_{\min} + r \end{cases} \tag{1}$$

This means that the position of coordinate (x_s, y_s) will not exceed the square shown in the figure below. If the sides of the square are represented by l_1 and l_2 respectively, the formula is as follows:

$$\begin{cases} l_1 = x_{\min} + r - (x_{\max} - r) = 2r - (x_{\max} - x_{\min}) \\ l_2 = y_{\min} + r - (y_{\max} - r) = 2r - (y_{\max} - y_{\min}) \end{cases} \tag{2}$$

According to the above equation, if the nodes in the circle are more clustered, the length of l_1 and l_2 will increase relatively, and the square area will also increase. On the contrary, if the nodes are more dispersed, the length of l_1 and l_2 and the area of the square will decrease. As can be seen from this, if the range of the square region is large and meets the above conditions, then the mean value of coordinates of all nodes can be used as the coordinates of the collection point. However, if the square range is relatively small, approximate processing should be performed. The square range is divided evenly by using l root line along the horizontal and vertical directions. By testing each intersecting point, coordinate data satisfying the minimum sum of distance can be obtained, which can be used as the collection point.

In view of the specific situation of heterogeneous data sources and the actual needs of data integration, the data integration solutions are also different. The following is a comparative analysis of the heterogeneous data integration methods commonly used at present [8].

Off-line data integration, off-line data integration The integration of heterogeneous data is achieved by importing and exporting intermediate data files. [9] Its intermediate

files are usually in XML, Excel, Access, JSON and other formats, which are relatively simple to implement. However, due to the use of intermediate files, there are obvious deficiencies in data format conversion and data security, and its synchronization performance is not good [10–13].

Database Provider Integration. Database Provider Integration utilizes a mature data provider to access data directly by establishing a connection between heterogeneous data sources. In order to ensure the security of the target system, it is necessary to set up a corresponding view for the required data, and then set up a specific access account to ensure the security of data access.

Data warehouse integration, Data warehouse integration through the form of data snapshots to heterogeneous data sources copied to the designated data warehouse, so as to achieve effective data integration. This method is usually used by ETL tools to filter the data from the data source periodically, and then load it into the data warehouse for the user to read. During the implementation, the target data can be directly copied to the local database, or copied to the third party temporary table, and then accessed by data interface. The latter is more open and can provide data sources for other systems. Data warehouse integration has both advantages and disadvantages. It has the obvious advantages of fast query and high performance.

Middleware integration, Middleware integration is the use of Web services or grid as a building platform tools, and then through XML heterogeneous data conversion and transmission. Web Services are self-describing, self-contained, network-enabled modules that use open XML standards to describe, publish, discover, coordinate, and configure these applications to develop distributed, interoperable applications. Grid is a kind of mechanism that uses the Internet to link all kinds of resources in geography into an organic whole, and can cooperate to accomplish difficult tasks, and provide users with integrated services such as storage and computation. The shared geographical resources include computer system, storage system, communication system, file, database and program, etc. Middleware integration allows consistent access to heterogeneous resources across heterogeneous platforms, providing platform support for large-scale, distributed, heterogeneous data resource access and integration.

In the multi-source and heterogeneous communication module access security authentication, the application scenario is to ensure the access and processing of large-scale heterogeneous data, which is different from the traditional data aggregation, and does not need to access data in the database or other heterogeneous resources, so a unified data communication protocol is adopted to solve the problem of heterogeneous data aggregation.

2.2 Design Two Way Authentication Architecture

Considering that both sides of the terminal communication module access security authentication in heterogeneous networks are not trusted, there are serious security risks, so a two-way authentication structure is designed. The specific flow of the two-way authentication architecture is shown in Fig. 2.

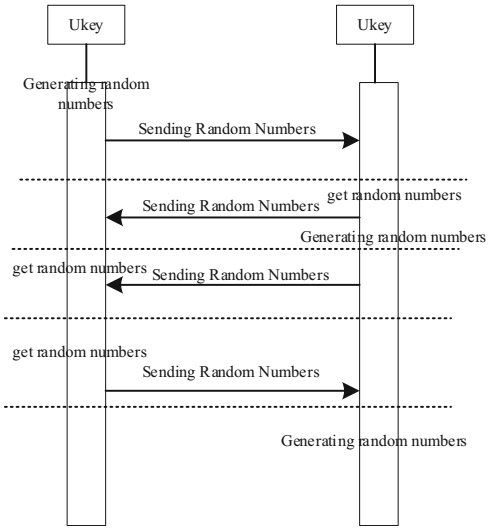


Fig. 2. Flow chart of two way authentication architecture

When the user requests access to the terminal communication module, two-way identity authentication shall be conducted between the two parties. The hardware security authentication module (Ukey) can be inserted on the authentication party and the authentication party. Ukey is a portable plug-in hardware device with the only hardware serial number in the world, as shown in Fig. 3.

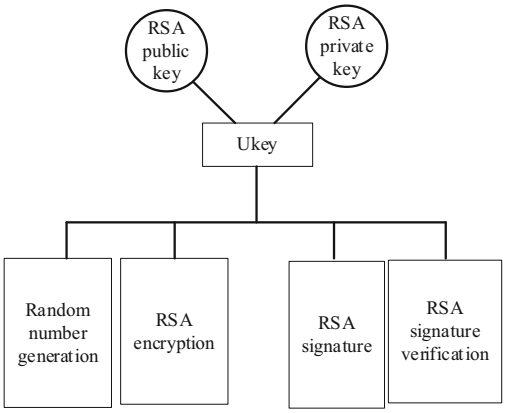


Fig. 3. Composition of ukey software

Random number generator, RSA encryptor, RSA decryption program, RSA signature program and RSA verification signature program are securely encapsulated, and RSA public and private keys for RSA operation are stored. Ukey also has two types of PIN, the user PIN and the developer PIN. The average user only needs to know the user

PIN, so the user only needs to know the user PIN; as a developer, the developer PIN has more privileges to develop more user-friendly features.

Two-way authentication method is based on RSA encryption and decryption, which needs to use RSA public and private keys. RSA related programs and RSA public and private keys have been securely encapsulated in Ukey, and all of them have been burned and written when Ukey is published to the user. The RSA public and private keys in the same Ukey are not a pair. The certification procedures are as follows:

The user inserts Ukey 1 on the party to be authenticated and confirms that Ukey2 is also inserted on the terminal communication module; the access point establishes a connection application for the access terminal communication module and enters the PIN code to start the two-way authentication. The user PIN with the above PIN of Ukey 1 is designated by the terminal at the time of publishing the Ukey, and the right to modify the user PIN after publishing is reserved to the user; if the user forgets the user PIN, the right to reset the user PIN is reserved to the terminal. The party to be authenticated generates a set of random numbers through the random number generator in Ukey 1. The random numbers are sent to the terminal after being RSA encrypted by the party to be authenticated through Ukeyl. After receiving the ciphertext, the terminal decrypts RSA by Ukey2 to get the random number. The terminal signs the random number with RSA through Ukey2 and sends it to the party to be authenticated. After receiving the signature, the terminal verifies the RSA signature through Ukeyl. If the verification result is identical to the random number, the authentication is successful and the next step is performed; otherwise, the authentication fails and access is denied.

After successful authentication, the terminal generates a group of random numbers through the random number generating program in Ukey2. The terminal encrypts the random numbers through Ukey2 and sends them to the party to be authenticated after RSA encryption. After the party to be authenticated receives the cipher text, the random numbers are decrypted through Ukey2, and the random numbers are obtained. The party to be authenticated sends the random numbers through Ukey 1 to the terminal after RSA signature, and the party to be authenticated receives the signature and then carries out RSA signature verification through Ukey2. If the verification result is completely consistent with the random number (02), the terminal succeeds in authenticating VD and has access permission. Otherwise, access is denied. The above process needs to be implemented under the support of security authentication protocol.

2.3 Determine Access Security Authentication Protocol

When the access party makes an access request, the multi-source heterogeneous terminal communication module initiates e_0 session, generates a random number, and sends authentication requests *query* and e_0. At the same time, a random number e_1 is generated by the party to be authenticated. After determining the random number, the size of the first eight binary digits of e_1 is calculated, and the authentication threshold χ_1 is calculated according to $q(K, e_1)$. The calculation formula is as follows:

$$\chi_1 = X(q(K, e_1) \oplus e_1 \oplus e_0) \tag{3}$$

The formula above, K said the identity information in the database, authentication information $X(K)$ that contains the target object, after the calculation, χ_1, e_1 and $X(K)$ is sent to the back-end database, the backend database lookup to see if there is meet $X(K') = X(K)$, if found no response to record the judge to stop illegal information communication, to find records using the corresponding K'.

Formula 1 calculates χ'. If χ' is not equal to χ_1, the authentication information is considered to be illegal information and the communication is ended. If it is equal, random number e_2 is generated by the back-end database and χ_2 is calculated.

$$\chi_2 = X(q(K', e_2) \oplus e_2 \oplus e_0) \tag{4}$$

The result is then sent to the authenticator, and then the data is updated. If $K' = K$, then K_1 and $X(K_1)$ are updated:

$$K_1 = K_1 \oplus e_1 \tag{5}$$

$$X(K_1) = X(K_1 \oplus e_1) \tag{6}$$

If $K' = K_1$, we update K. After receiving the data, χ_2 is calculated according to Formula 2. By comparing whether χ_2' is equal to χ_2, if not, the access is judged to be illegal. If equal, K is updated. The authentication of both parties can be realized through this authentication protocol, and the access security can be further guaranteed.

3 Experimental Study on Universal Access Security Authentication of Multisource Heterogeneous Terminal Communication Module

3.1 Experimental Preparation and Design

The experiment is based on the platform system which is based on streaming data communication server. The system can monitor the sensor device 24 h, receive a lot of data and view the data in real time. The experimental environment is to deploy web servers, communication servers, message servers, and data storage servers on four servers. The experimental flow is to use Loadrunner to simulate a large number of concurrent scenarios, while simulating heterogeneous multi-source terminal data. After the whole platform system is started up, Loadrunner sends the data to the streaming data communication server, which parses the access data and distributes it to the message server. The message server forwards the message and persists it to the data, where different access security authentication techniques are applied, and the data is finally presented in a web-based application. After the above preparation is completed, the security authentication technology is evaluated from the authentication delay experiment and stability test. Details of the hardware required for the experiment are

shown below, with Table 1 showing the machine configuration. Tools Options Options Options Page.

Table 1. Hardware configuration required for experiment

Machine name	Machine configuration	Purpose
m_loadrunner1	Winxp, 4G, Binuclear 15	Data acquisition front end of analog multi-source heterogeneous terminal
m_loadrunner2	Winxp, 4G, Binuclear 15	Analog multi-source heterogeneous terminal information sending front end
m_ccs	Centos6.6, 4G, Binuclear 15	Used as a streaming data communication server
m_activeMQ	Centos6.6, 4G, Binuclear 15	Use as a message server
m_web	Win7, 4G, Binuclear 15	Use as a web server

The experimental environment topology is shown in Fig. 4.

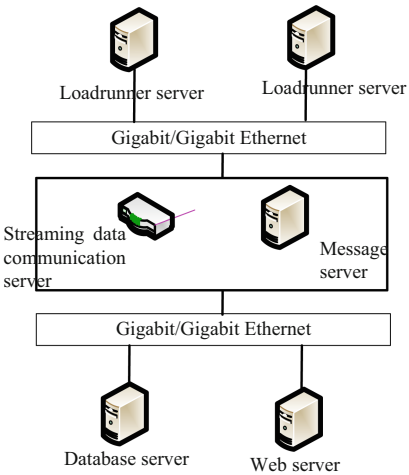
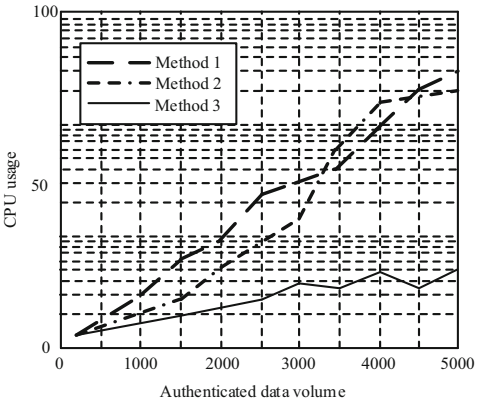


Fig. 4. Experimental environment topology

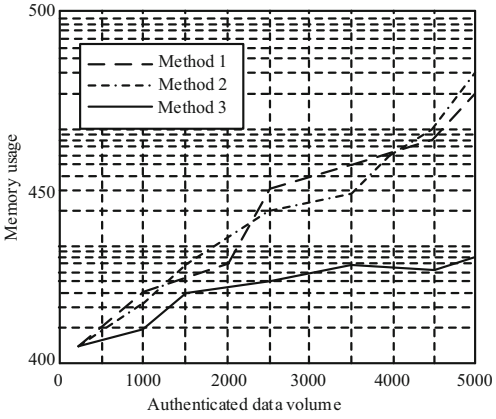
After the preparation of the experiment, the stability and authentication delay of different security authentication technologies are tested.

3.2 Security Certification Performance Test

Use LoadRunner to simulate a large number of concurrency and test the stability of security authentication technology. The main observation indexes in the experiment are the data receiving and sending of LoadRunner console, the CPU occupancy rate and memory occupancy rate of streaming data communication server. The experimental results are shown in Fig. 5.



(a) Application of different methods in each security authentication



(b) Memory usage of different methods in each security authentication

Fig. 5. Stability test results of the same security authentication technology

In the figure, method 1 represents traditional security authentication technology 1, method 2 represents traditional security authentication method 2, and method 3 represents the proposed security authentication method. In Figure a, it is clear that the CPU

utilization of security authentication technology is increasing with the increase of the amount of authentication data. In contrast, the CPU utilization rate of security authentication technology is always 50%, which shows that the technology runs stably. As can be seen from Figure b, memory usage is also increasing as authentication data increases, and the proposed security authentication technique has lower memory usage compared to the three sets of results, indicating that its support for high concurrency does not depend on memory and does not consume large amounts of memory.

3.3 Experimental Results and Analysis of Authentication Delay

In the experiment, different security authentication technologies are used to act on heterogeneous terminals. While data communication is conducted, the authentication delay of different security authentication technologies is monitored. The experimental results are shown in Table 2.

Table 2. Test results of authentication delay of different security authentication technologies

Experimental parameters	Traditional security authentication technology 1		Traditional security authentication technology 2		Proposed security authentication technology	
Operation mode	Non roaming	Roaming	Non roaming	Roaming	Non roaming	Roaming
Certification time	96	638	177	831	86	167
Configure time	15	17	16	17	15	16
Association and handshake time	16	17	15	17	18	19
Switching delay	16	17	15	17	15	14

The unit of data in the table is Ms. the authentication time represents the execution time of the security authentication technology, the configuration time represents the time spent in the pre configuration phase, the association and handshake time represents the time spent in the security association and four handshakes, and the handover delay represents the whole handover time. From the data in the overall observation table, we can see that the time gap between the three security authentication technologies is relatively small in the case of non roaming, and the time difference between the first two security authentication methods is not big in the case of roaming, but it is obvious that the time of the proposed security authentication technology is much less than them. Combined with the stability experiment results of security authentication technology, it can be concluded that the design of multi-source heterogeneous terminal communication module pan access security authentication technology can well overcome the problem of large authentication delay between heterogeneous networks, and ensure the transparency of real-time services and higher security. In practical application, the proposed security authentication technology has more advantages than the other two security authentication technologies.

4 Conclusion

With the trend of heterogeneous wireless network convergence becoming more and more obvious, the demand for access security in heterogeneous wireless network is becoming higher and higher. At present, the research on access authentication technology of heterogeneous wireless fusion network is still in the stage of theoretical exploration. The research in this paper can provide unified access authentication technology for heterogeneous wireless fusion network and provide theoretical support for future engineering implementation.

In this paper, multi-source heterogeneous terminal communication module access security authentication is the focus of this research. Based on a large number of research materials and literature, a new authentication method is designed. After the completion of the design, a large number of comparative experiments show that the security authentication technology has better stability and feasibility, and provides better guarantee for multi-source heterogeneous terminal communication security. There are still some difficulties in the design and research. Although some problems in the traditional security authentication technology have been solved, there are still some details, such as access status monitoring, etc. In the future research, this aspect will be studied to further improve the security authentication technology for communication access of multi-source heterogeneous terminals and improve the security of data and access.

References

1. He, X.: Simulation research on multi source heterogeneous large data cross source scheduling method. Comput. Simul. **36**(03), 339–342 (2019)
2. Zheng, X., Ying, Z., Wang, Q., et al.: Research on wireless communication access technology for ubiquitous power Internet of Things. Electr. Power Constr. **40**(11), 16–23 (2019)
3. Chen, X., Hu, X., Shen, C., et al.: Research on access authentication technology of power IoT based on Blockchain. Appl. Electron. Tech. **45**(11), 77–81 (2019)
4. Yang, C., Jian, Y., Ren, S., et al.: Power LTE network security access technology based on improved authentication protocol. Electr. Meas. Instrum. **56**(03), 91–96+102 (2019)
5. Yan, S., Wang, C.: Simulation research on user information authentication security protection of Internet of Things. Comput. Simul. **5**, 329–332 (2019)
6. Tan, F.: An improved RFID mutual authentication security hardening protocol. Control Eng. China **26**(4), 783–789 (2019)
7. Lu, Y., Zhao, Y., Jiang, L., et al.: Certificateless authentication protocol based on EAP-IBTLS in IoT. J. Nanjing Univ. Posts Telecommun. (Nat. Sci.) **39**(01), 62–67 (2019)
8. Tong, S.: Design and verification of security of mobile terminal access workshop information system based on SM4 algorithm. Mach. Tool Hydraul. **47**(07), 105–109 (2019)
9. Liu, S., He, T., Dai, J.: A survey of CRF algorithm based knowledge extraction of elementary mathematics in Chinese. Mobile Netw. Appl. **26**(5), 1891–1903 (2021). https://doi.org/10.1007/s11036-020-01725-x

10. Liu, S., Fu, W., He, L., Zhou, J., Ma, M.: Distribution of primary additional errors in fractal encoding method. Multimedia Tools Appl. **76**(4), 5787–5802 (2014). https://doi.org/10.1007/s11042-014-2408-1
11. Liu, S., Liu, G., Zhou, H.: A robust parallel object tracking method for illumination variations. Mob. Netw. Appl. **24**(1), 5–17 (2018). https://doi.org/10.1007/s11036-018-1134-8
12. Ma, Y., Liu, Z., Wang, Z.: Research on heterogeneous terminal security access technology in edge computing scenario. Comput. Eng. Appl. **56**(17), 115–120 (2020)
13. Lin, N., Chen, Z., Zuo, L., et al.: Security analysis and improvement of access protocol for voltage monitoring device in power network. Comput. Eng. Des. **40**(11), 3085–3089 (2019)