Research and Analysis of Library Access Control Authentication Scheme Based on IPv6 and Location Technology

Panfeng Li¹2, Jiangshu Wei¹2*, Di Zhang³, Lin Hu¹2, Qiyao Hu¹2

¹College of Information Engineering, Sichuan Agricultural University, Ya'an, Sichuan, 625014, China
²Key Laboratory of Agricultural Information Engineering of Sichuan Higher Education Institutions, Sichuan Agricultural University, Ya'an, Sichuan, 625014, China
³Information and Educational Technology Center, Sichuan Agricultural University, Ya'an, Sichuan, 625014, China
*Corresponding author’s e-mail: weijiangshu66@163.com

Abstract. With the maturity of IPv6 technology, smart campus has become a trend, and the management of libraries will inevitably become intelligent. Nowadays, libraries in many colleges and universities use the method of swiping for identity authentication, which has great drawbacks. In order to solve the defects of traditional access control technology, this paper proposes a library access control authentication scheme based on IPv6 and location technology: this scheme realizes identity authentication through IPv6 wireless local area network and WIFI positioning technology, effectively avoiding a series of authentication problems.

1. Introduction

As we all know, the access control system is an extremely important part of the security system, which is also an important part of the libraries of many universities[1]. For schools, the role of the library access control system is not only to authenticate students' information, but also to collect data from students entering and leaving the library to assess the school's learning style. Unfortunately, the access control system used by most libraries today is still the traditional campus card model, and only authenticates when entering the library, leaving the library to not record. This is obviously unreasonable, because only the number of students entering the library can be counted, and the time, behavior, etc. of entering the library cannot be directly reflected. In addition, this authentication method based on "user owned" is very insecure. In order to improve the performance of the library access control authentication system and enhance the practicability of the data collected by the access control system, An access control authentication scheme based on IPv6 wireless local area network and WIFI positioning technology is proposed. This method uses mobile phones for access control authentication, makes full use of existing hardware resources, improves library access control authentication strategies, and helps the smart campus to further develop[2]. At the same time, this method uses WIFI positioning technology to record and analyze the behavior of library users, and provides data sources for library operation and school style construction[3].
2. IPv6 network security
The traditional IPv4 network itself does not have security. In order to make up for this defect and ensure the security of network layer data packets, the next generation Internet technology IPv6 introduces a new IPSec (IP Security) mechanism[4].

IPsec is a three-layer tunnel encryption protocol. And it is a mechanism to ensure network security. It uses cryptography to provide reliability for data transmitted over the Internet. Through IPSec, the following security guarantees are provided between the two parties at the IP layer by means of encryption and data source authentication:

- Data integrity: After receiving the data packet, the IPsec receiver authenticates the data packet using the IPsec authentication protocol, and checks the data content through the message digest to ensure that the data has not been tampered with during transmission.
- Data confidentiality: The sender of IPsec encrypts the data packet before transmitting the data packet through the network. The encrypted data packet can be guaranteed not to be stolen, or the real content of the data cannot be known even after being stolen by an illegal user.
- Data source authentication: The recipient of IPsec can determine whether the sender is a legitimate user, and can determine whether the other party is a real interlocutor, effectively avoiding man-in-the-middle attacks.
- Anti-replay: The receiver of IPsec can detect and refuse to receive outdated or repeated packets through the protocol mechanism, and effectively avoid replay attacks.

In view of the characteristics of the IPv6 protocol in network security, identity authentication on this basis is a good choice.

3. Identity authentication technology
Identity authentication refers to the process of confirming the identity of a user on the network by means of an existing computer system and a network system. The technology derived on the basis of this is also called identity authentication technology. Computer systems and computer networks are virtual digital worlds in which information is represented by a specific bit stream. Since computers can only recognize digital information, only digital information can be used for identity authentication in the computer field. The real world we live in is an objective physical world, and everyone has a unique physical identity. In order to match the identity information of the user in the virtual world of the network with the physical information in the real world, the identity authentication technique is generated: the user is authenticated by means of the user's own unique identification information.

There are three types of common authentication technologies: based on the user's knowledge, based on what the user has, based on biometrics. In the library access control system, the most traditional way to brush the card is based on what the user has. But the drawbacks of this approach are obvious: whoever has a card is a legitimate user, which has great obstacles to traceability and data analysis.

In the era of intelligence, the mobile phone has become a person's "identity mark". Entering the key through the mobile phone for identity authentication can solve the above problem to a large extent[5]. The reasons are as follows:
- Using the sensor that comes with the mobile phone, positioning, fingerprint verification, and behavior recording can be easily realized[6-7].
- Many schools have developed relatively complete library APPs, and integrating identity authentication into existing APPs is a good trend.
- The key authentication method based on mobile phone is no longer restricted by the physical card, and the identity verification is more flexible.

4. WIFI positioning technology
In the case of access control authentication, it is inevitable that the determination of the user's location is involved. In the traditional card swiping mode, the user's geographic location is defined by default, but based on the IPv6 network authentication method, the user's location needs to be judged through the wireless local area network. For indoor positioning, WIFI positioning is a good choice[8].
Nowadays, WIFI has become a universally applied technical means, and the indoor coverage of its infrastructure is also very good. Many public places that need to be located are covered, and almost full coverage of the area is achieved. Therefore, the use of WIFI for indoor positioning is very reasonable. In addition, the current university campus network has basically achieved full coverage of WIFI, which is also the premise of smart campus operation. So WIFI resources can be made full use of to achieve precise positioning.

There are three main types of positioning technologies based on WIFI:

The first is the trilateration positioning method based on received signal strength, which is currently the most widely used technology. By detecting the WIFI signal strength, the obtained data is compared with the known signal weakening model, the distance between the reference point and the point to be measured is calculated, and a circle is drawn by using the distance as a radius, and three circles are drawn in this way. The overlapping part of the three circles is the position of the target to be tested. However, in the actual situation, the situation where three circles are at one point is difficult to exist, and the positioning accuracy obtained by this method is very low, and there is about 10 m error, so this method is not suitable for precise positioning.

The second type is fingerprint positioning, which is based on the received signal strength. The premise of this technology is that it needs to collect fingerprint information of the area and construct a fingerprint information base. During positioning, the measured signal strength is compared with the signal strength of each reference point measured in the previous stage, and the position with the best matching is selected as the position of the measurement target. Many of the current positioning technologies are based on this method. Its advantage is that it has high positioning accuracy and can achieve an accuracy of 3–5m. The disadvantage is that the cost of layout and maintenance is expensive, and the system relies on the fingerprint database of RF signal strength. If it is used in a large-scale scenario, it will lead to a large database, relatively high maintenance costs, and also a poor degree of portability. Considering the nature of the library's geographic location, it is more reasonable to use this method for indoor positioning in the library[9].

The third measurement method is based on the time of flight of the signal, by measuring the time of the round trip between the two nodes of the WIFI signal, and then using this time to calculate the distance between the nodes, and a circle is drawn by using the distance as a radius, and many circles are drawn in this way. The resulting overlap is the location of the target to be tested. This method is similar to the trilateration positioning method, but it is based on signal flight time and is more reliable than what method based on signal strength. It has the advantage of high precision and can reach an accuracy of 1 meter. But unfortunately, this method is too expensive for the router's resources, and it is too burdensome for multi-user use.

5. Access control certification model

Aiming at the particularity of campus library and the completeness of campus infrastructure, with the security features of IPv6 network, the library access control system and WIFI location technology are combined to authenticate the library users, making the access control system more intelligent and convenient.
In a local area network with multiple locating APs, the fingerprint information of each location is collected in the early stage to form a fingerprint information database. When the user enters the library, the mobile phone is in the range of the local area network, and the positioning information is formed after comprehensive analysis by information exchange between multiple APs close to the mobile phone. When the phone is in a specific location, the access authentication operation is performed. The system checks the MAC information and user information of the mobile phone through the IPv6 wireless network to complete the identity authentication. When the user leaves the library, the system then unregisters the user's information. The specific flow chart is as follows:

Figure 1. WIFI positioning diagram.
Identity authentication in this way can make the campus library access control system more intelligent. At the same time, by using the accuracy of indoor positioning, it is also possible to analyze the behavior of students in the library, and draw a library study report, which is of great significance to the school's academic assessment. Of course, after the user connects to WIFI, it is not analyzed for traffic, because it is unreasonable to steal user information. On the contrary, it is only using WIFI positioning to record the user's location information, so as to know whether the user is focused on learning.

Due to the uniqueness of the MAC address of the user's mobile phone and the hugeness of the IPv6 address space, the user's mobile phone MAC address information can be bound to the private IPv6 address in the process of authentication, making the authentication faster, safer and more reliable.

To simulate the connection of the phone to the AP, a network simulation tool was used: Cisco Packet Tracer. Cisco Packet Tracer is a network simulation tool developed by Cisco. It is a CCNA-level visual learning platform designed for network learners to design, configure and solve complex problems. But unfortunately, most wireless devices, including Cisco analog devices, do not yet support IPv6 networks, but using IPv4 network configurations here does not affect the experimental situation. However, under the IPv6 network, all aspects of performance will be better, and users can also have a separate IP address.

In the Cisco simulation environment, AP1 is set as the primary route, and AP2 and AP3 are set as the secondary routes to implement the bridging function of the wireless router to simulate the real situation of the campus wireless network. When the user enters the library, the mobile phone connects to any AP after positioning, and assigns a corresponding IP address according to its MAC address to communicate, uses the mobile phone to send the user's information to the server, and authenticates and registers the user on the server side. The identity is now complete. When the user leaves the library, the mobile phone connects to the AP and performs positioning, sends the user's information to the server, retrieves the registered user's information on the server side, and logs out.

Of course, there are many options for how the user's information is entered during the entire verification process. Among them, it is a relatively simple method to input the account password by using Web technology. In the campus environment, information such as the student number is used as the authentication condition, and personal information is transmitted through the Web for authentication. In addition, it is safer and more accurate to use fingerprints from the phone's own fingerprint sensor. Under the current mature fingerprint technology, the recognition speed can reach milliseconds.

Simulate the LAN with Cisco Packet Tracer as follows:

![Figure 2. Library access control certification flow chart.](image)
Figure 3. Simulation of information transmission in a LAN environment.

In the LAN environment, it is very convenient for the mobile terminal to connect to the AP, and the user access speed to the database is also good. As long as the AP's constituent topology is reasonably planned, the multi-user service on the campus will not cause congestion problems. On this basis, identity authentication is also considerable.

6. Conclusion
In the IPv6 environment, the WIFI indoor positioning technology is used to detect the location of the library users, and further authenticate the identity through the IPv6 network, thereby replacing the traditional card swiping mode. This strategy can make full use of existing hardware resources to ensure the security and convenience of access control authentication. At the same time, it is also possible to grasp the behavior of library users by means of WIFI positioning technology, and use the big data to analyze the learning atmosphere, which is of great significance to the construction of colleges and universities.

Acknowledgments
This work is supported by the CERNET Innovation Project (No. NGII20170605).

References
[1] Zhan, X. (2014) The Impact of “Access Control System” on Library Service and Management. Lantai World, 14: 104-105.
[2] Xu, J.C., Hu, S.J. (2005) To apply intelligent gateway control system to raise the efficiency of library management. RESEARCHES IN LIBRARY SCIENCE, 5: 29-30, 13.
[3] Zhang, Z.Z. (2018) The Design of Library Entrance Guard and Reader Analysis System based on Fingerprint Identification. Journal of Mianyang Teachers' College, 2: 102-106, 113.
[4] Shi, C., Shen, P.B., Yang, W. (2010) Research on IPSec VPN Security Based on IPv6 Campus Network. COMPUTER TECHNOLOGY AND DEVELOPMENT, 10:167-170, 175.
[5] Xu, G.Y., Miao, X.N., Zhang, J.F. (2018) Review of implicit authentication for mobile devices. Computer Engineering and Applications, 6:19-25.
[6] Wei, Y.N. (2014) Research on Technology of Unlocking Mobile Terminals Based on Identity Authentication. Information Technology & Informatization, 6: 155-156.

[7] Liang, W., Wang, Z.M., Fan, L. (2014) Investigation and study on terminal users behavior of mobile search. Journal of Xi’an University of Post and Telecom, 2: 108-112.

[8] Liu, Y.H. (2018) Research on WiFi indoor location algorithm based on location fingerprint. Science & Technology Information, 2: 44-45.

[9] Qin, G.W., Sun, X.Z., Chen, M.Y. (2018) Bio-inspired SLAM fingerprint location based on WIFI. CAAI Transactions on Intelligent Systems, 3: 407-413.