Intelligent support and command system based on WAPI terminal equipment

Yu Wang 1*, Zongchun Wei 1, Haibo Bao 1, Gaofeng Deng 2, Jiangwei Li 1, Pei Li 1, Leigang Nie 1, and Hua Fu 1

1 Nanning power supply bureau of Guangxi Power Grid Co. Ltd
2 Guangxi Power Grid Co. Ltd

*Corresponding author’s e-mail: wangy0515@nng.gx.csg.cn

Abstract: In order to solve the problem that the process of WAPI terminal connection is troublesome, this paper proposes an intelligent support and command system of WAPI terminal equipment based on centralized control AC + AP architecture. The system stores WAPI certificate on AC (centralized controller), WAPI terminal equipment is associated with AP (wireless access point), and AP equipment notifies AC of the associated events of the terminal, AC equipment and terminal equipment enter authentication and complete certificate authentication. Complete access authentication through AC and terminal equipment, and store the unicast and multicast keys generated by authentication negotiation on AC. This method is more convenient to maintain the certificate. At the same time, on the premise of ensuring the security of the certificate, it also improves the encryption and decryption efficiency and improves the user's business experience.

1. Introduction

WAPI wireless LAN Authentication and privacy infrastructure is a secure transmission protocol for IEEE802.11 protocol [2]. In the gb15629.11 [3] standard of wireless local area network in China, there is a clear security solution for WLAN (wireless LAN), which adopts the certificate mechanism of public key cryptosystem and realizes the two-way authentication between mobile terminal (MT) and wireless access point (AP) in a real sense, making the information transmission between both ends more secure.

However, when all terminals supporting WLAN function need to support WAPI security protocol, the problem of secure storage of WAPI certificate also arises. At present, many WAPI certificates are directly stored on terminals, WAPI security modules or intermediate wireless access points. This method of saving WAPI certificates has great security risks. WAPI certificates are easy to be illegally copied or stolen by others, which leads to the threat of network security. Similarly, the data security of the business between AP equipment and AC equipment also depends on the tunnel defined by each manufacturer, which can not ensure sufficient security and privacy. For a lightweight AP, the performance of the device is limited. When maintaining the corresponding certificate, when multiple terminals are associated at the same time, the performance of the AP device will be seriously affected, resulting in packet loss or fragmentation during data transmission. Daily maintenance and management are also difficult, and ultimately affect the user experience.

By studying an intelligent support and command system based on WAPI terminal equipment, this paper proposes a WAPI technology system based on centralized control AC + AP architecture. In this
system, the equipment certificate is installed on AC, which has high security, convenient maintenance and effectively improves the user experience.

2. Composition and implementation method of intelligent support and command system based on WAPI terminal equipment

2.1. System architecture composition and function

The intelligent support and command system based on WAPI terminal equipment is a system of WAPI technology based on centralized control AC + AP architecture. The system includes AS server (WAPI authentication server), AC (access controller), AP (wireless access point) and WAPI terminal. The system architecture is shown in Figure 1:

![Figure 1 system architecture](image)

AC (access controller) is mainly responsible for configuration management of all downstream AP devices, authentication, management, security, storage and installation of wireless users, generation and issuance of WAPI certificates from AS servers and other control functions. After the AC establishes a CAPWAP tunnel with the lightweight access point AP equipment, the AC equipment performs online centralized management of the AP and centralized management of the terminal services, but does not directly issue relevant WAPI certificates to the AP equipment. The WAPI terminal notifies the AC of related events through the AP, the AC and the terminal enter the authentication process, and the AC equipment and the AS server complete the authentication of the certificate.

AP (wireless access point) is mainly responsible for providing wireless access for the terminal and forwarding the encryption and decryption service data based on CAPWAP tunnel. It mainly plays the role of seamless integration and bridging of wired and wireless management frames and service frames.

AS server (WAPI authentication server) is the core equipment in the system architecture based on WAPI protocol. It is mainly responsible for providing WAPI identity certificate management and authentication services. AS authentication server is divided into CISU (certificate issuing function of AS) and ASU (identity authentication function of AS). Among them, CISU supports WAPI certificate issuance service, forces the use of digital identity certificate as identity certificate, and can issue digital
identity certificate for the accessed AP and STA. The system adopts SM4 symmetric cryptographic algorithm approved by the State Password Administration to encrypt and decrypt the transmitted data, which fully ensures the security of data transmission and the integrity of user information. ASU (authentication service unit) is mainly used to manage the certificates required in the information interaction of each network element, such as certificate generation, issuance, revocation and update [4] [5]. A certificate contains the public key and signature of the issuer and holder of the certificate. In addition, ECC based algorithm is adopted in the whole certificate authentication process, which can make the secure message hash algorithm more ensure the integrity of the message, and make it difficult for those who deliberately attack the system to modify and forge the authenticated information, so as to improve the security.

WAPI terminal is a WAPI module with encryption chip, including the main control chip, the encryption chip and RF chip, the connection management and configuration of the main control chip to the whole WAPI module, and the WAPI protocol stack. The most important is that the encryption chip can verify the WAPI certificate used for WAPI authentication, key negotiation, key decryption and so on.

2.2. Implementation method of intelligent support and command system based on WAPI terminal equipment

Store the AP's WAPI certificate on the AC device. After the AP and AC establish a capwap tunnel, and the terminal is associated with the AP and registered online on the AC, the terminal completes the authentication of WAPI certificate through AC and AS. WAPI protocol adopts the public key cryptography mechanism to authenticate and authenticate the terminal and AP in the system by using the issued certificate. Figure 2 shows the flow chart of the working process:

![Flow chart](image_url)

The terminal is associated with the AP device through SSID, and then the AP device sends the terminal associated event notification message to the AC device to inform the AC device. After the terminal is associated with the AP, the AP notifies the AC of the associated event, and the terminal and AC start mutual identity authentication. During this period, the terminal must send its own certificate and current time to the AP, and the AP forwards the relevant information to the AC.

The AC device accesses the WAPI certificate sent by the AP device, initiates the access
authentication process, and the intermediate interactive authentication message is forwarded by the AP device. The AC signs the message sent by the AP, and sends the terminal certificate, submission time and the private key of the AP device to the AS server.

The authentication of WAPI certificate is carried out interactively in AC and AS [6] [7]. The AS server completes the authentication of relevant certificates. After receiving the authentication request message sent by the AC equipment, the AS will first verify the signature of the AP in the request message and the integrity and validity of the AP certificate. The second is to verify the certificate information of the terminal [8]. Finally, the AS authentication server will sign the authentication results of the AP and the terminal with its own key, and send the signature to the AC together with the previous two authentication results. AC signs and further verifies according to the message authentication result sent by AS, and obtains a corresponding final authentication result, so as to decide whether to allow the terminal to access. The AC forwards the authentication result to the terminal through the AP device, and then the terminal device identifies and verifies the signature result of the as, so as to determine whether it can access the AP.

2.3. Specific implementation of intelligent support and command system based on WAPI terminal equipment

The system involved here adopts capwap tunnel (a special tunnel in WLAN system) on the wired link to enhance the security of data. WAPI technology is adopted in the aspect of air interface. It adopts ternary symmetric security architecture. The trusted third-party authentication server as will conduct two-way authentication between the terminal and AP, which can effectively ensure the security of air interface data transmission. The message interaction process [9] is shown in Figure 3:

---

Figure 3 message interaction process
Install the WAPI certificate issued from the as authentication server on the AC, and configure the association relationship between the AC and the AP's WAPI certificate, so that the configuration capability of the AC can be connected to the AP.

The AP sends beacon / probe request to the terminal Frame message, which includes SSID and WAPI capability set information. After receiving the Becon broadcast frame message sent by the AP, the terminal will send the Authentication message frame. After receiving the Authentication message sent by the terminal, the AP sends an Association message to the terminal, which includes its associated SSID, WAPI capability set and other information. After the terminal successfully associates with the AP, the AC device sends an authentication activation instruction to the terminal, which is forwarded to the terminal through the AP. After receiving the authentication activation instruction, the terminal immediately sends an access authentication request to the AC device, and the same request is forwarded to the AC device through the AP. After receiving the corresponding request message, the AC equipment will send the certificate authentication request message to the AS and wait for the as equipment to analyze and respond to the message. After receiving the authentication request message sent by the AC, the AS performs parsing processing. If the certificate is authentic, it sends the response message of the certificate authentication result to the AC equipment. After receiving the response authentication message from the AS, the AC sends back the access authentication response message to the terminal [10] [11]. The response message is finally forwarded to the terminal through the AP equipment.

After the previous access authentication operation is completed, the subsequent key negotiation is carried out. The AC device sends a unicast key agreement request message to the terminal device, which is forwarded to the terminal through the AP device. Then, the terminal sends a unicast key agreement response message to the AC device, which is forwarded through the AP device. After receiving the key negotiation response message from the terminal, the AC device continues to send unicast key negotiation confirmation to the terminal [12].

Finally, after the terminal matches the AS key, the AC device starts to send multicast key notification to the terminal. The terminal sends the corresponding multicast key agreement response message to the AC equipment, and finally completes the whole WAPI protocol operation process.

In general, the first is the link negotiation process, the second is the unicast key negotiation process, the third is the multicast key negotiation process, and the last is the WAPI access control process.

The intelligent support and command system based on WAPI terminal equipment shares a WAPI certificate for multiple AP devices without spending too much resources. It manages multiple WAPI certificates for centralized management and maintenance. According to different services among all AP devices under the same AC, multiple WAPI certificates can be used at the same time. For example, one AP uses one WAPI certificate and multiple AP devices share one WAPI certificate.

The AP equipment mentioned in this paper has two logical ports: controlled port and uncontrolled port. Before the terminal passes the authentication, all interactive messages are transmitted through the uncontrolled port. Once the terminal passes the authentication, the service data of the terminal is transmitted through the controlled port.

3. System verification

3.1. Experimental resources

In order to show the advantages of the command system, the required software and hardware are shown in the table below:
Table 1 list of experimental resources

| resources                        | quantity | explain                                                                 |
|----------------------------------|----------|-------------------------------------------------------------------------|
| As server                        | 1        | Provide WAPI identity certificate management and authentication services |
|                                  |          | It is used for centralized management of WAPI certificates. It is also convenient for centralized management of AP, and then centralized management of all details |
| Ac server                        | 1        | It is used for centralized management of WAPI certificates. It is also convenient for centralized management of AP, and then centralized management of all details |
| AP                               | 3        | It is used for terminal equipment access management and forwarding interactive messages between terminal and AC. |
| Wireless terminal                | some     | For access and service test                                             |
| Switch                           | 2        | The wired link communication network element between AC and AP has the function of mirror port |
| Wire shake                       | 1        | It is used to capture the interactive message of wired link for analysis |
| Omni Peek                        | 1        | It is used to grab the wireless link interaction message for analysis   |
| WAPI negative tester (xwn1000t)  | 1        | The abnormal message is constructed to test the judgment and processing ability of the mobile terminal to the abnormal message |
| WAPI protocol analysis tool      | 1        | Capture WAPI protocol related messages, comprehensively and carefully analyze the message content, and give accurate prompts for possible error fields and locations |

The AC server here can be any one of 512, 1024, 2048 and 4096, and the number in the model represents the maximum number of APS it supports.

3.2. Verification process
The test networking is shown in Figure 4. WAPI negative tester and WAPI protocol analysis tool are used in the test environment. WAPI negative tester can construct abnormal message to test the judgment and processing ability of mobile terminal to abnormal message. WAPI protocol analysis tool can efficiently capture WAPI protocol related messages, comprehensively and carefully analyze the message content, and give accurate prompts for possible error fields and locations.

Figure 4 test networking diagram
Take the protocol integrity test sample of AE signature attribute type field in the access authentication response message as an example, analyze it, and analyze its message packet by using capture tools such as WAPI protocol analysis tool.

AE signature attribute type value should be '1'. When the AE signature attribute type is given an exception value. At this time, the tested mobile user terminal does not respond to the abnormal message, does not continue the subsequent key negotiation steps, and continues to wait for the retransmission message.

The negative tester first sends two abnormal multicast key announcement packet messages, with an interval of 100 ms. Mobile user terminals do not respond to abnormal multicast key announcement packet packets. Finally, the negative tester sends a normal multicast key announcement packet message (AE signature attribute type field value is "1"), and the interval between normal message and abnormal message is 100 ms. Then the mobile user terminal can respond to the normal multicast key announcement packet message, complete the whole process of subsequent key negotiation, and finally establish the connection.

After receiving the abnormal specified field message for the first two times, the terminal still does not disconnect, but continues to make the third attempt. When the message of normal Wai header field is received for the third time, normal processing is carried out and the connection is finally established.

4. Conclusion
In this paper, by installing the WAPI certificate on the AC device instead of sending it to the AP device, the keys generated after subsequent terminal negotiation are stored on the AC, which makes the certificate maintenance convenient and more secure. The user's air interface message encryption and decryption is carried out on the AC equipment, which improves the efficiency of encryption and decryption and the user's business experience. At the same time, it also improves the security and robustness of the business data of the whole system.

Reference
[1] SUN Hao. Design and implementation of WLAN network monitoring system [J], communication and information system, 2014.
[2] Yang Kunyuan. Planning and implementation of wireless campus network in University Park [J], computer technology, 2014.
[3] Zhu Weiwei. Research on WLAN construction and application [J], wireless interconnection technology, 2013.
[4] Chen Jigang. Security Protocol Improvement of WLAN based on management frame [b], 2008.
[5] Zhao Yujuan. Research on security mechanism of WLAN [J], computer software and theory, 2006.
[6] Deng Guoqiang, ye Zhao, Lu Yiqin. Wireless roaming between colleges and universities using WAPI [J], China education network, 2015.
[7] Nie Ming, Liu Changrui. Some problems to be solved in the application of WAPI to operator networks [J], Internet world, 2013.
[8] Hou Liqun, Mao Yuming. Comparative analysis of WLAN user security access solutions [J], national network and information security technology seminar, 2004.
[9] Cai Kai. WLAN security protocol testing technology research and system implementation [J], computer system architecture, 2011.
[10] Shi Yunzhi. Research on WLAN security mechanism and implementation of wireless access point WAPI protocol [J], communication and information system, 2010.
[11] Sun Xuan. Analysis of WAPI protocol and its implementation in WLAN integrated authentication platform [J], computer system architecture, 2006.
[12] Zhang Hao. Network security integration of WLAN and 3G based on WAPI [J], electronic and communication engineering, 2012.