International Journal of Security and Its Applications
Vol. 9, No. 6 (2015), pp. 53-60
http://dx.doi.org/10.14257/ijsia.2015.9.6.06

Fast Authentication Method for Wireless Local Area Network

Guo Hong-tao

North China University of Water Resources and Electric Power,
Zhengzhou 450045, Henan, China
htguo2000@163.com

Abstract

WLAN (wireless local area network) connect the users and the network by using radio frequency signals. It reduces network cabling between the terminals and the network equipment. Thus WLAN has the following benefits: giving end users a great deal of mobility, convenience, saving network cabling project costs. WLAN can share the wireless traffic of 2G or 3G network. But WLAN authentication from the safety and convenience of comprehensive consideration has not been a fine solution. This paper analyzes the various existing problems of authentication used in the field of WLAN. A fast authentication method is proposed in this article considering the character of the terminal user. Compared with existing authentication methods, this method is fast, it improves the system applicability under the comprehensive consideration of accessibility and safety. This method is validated by experiments, so that users can easily access secure WLAN systems.

Keywords: *WLAN; Fast authentication; safety method; convenient method*

1. Introduction

Wired LAN is a local area network, which using the twisted-pair network to connect the network devices. Wired LAN is also called LAN. The LAN access to the local network with larger bandwidth and higher access control. But its wiring work is more cumbersome, and not flexible enough. With the rapid development of mobile Internet technology, WLAN (Wireless Local Area Network) gradually developed in recent years and become more and more popular. WLAN is utilized in a certain local area network with radio communication technology [1, 2]. WLAN can reduce a lot of network cabling and other tedious work used between the network access layer and the terminal user, so it can reduce network time cost and economic cost of the project. WLAN can support many kinds of terminals including desktops, laptops, cell phones, PDA and other handheld devices. So a user with a cellphone supporting WLAN can access to the network anytime and anywhere. The WLAN service providers provide users with wireless signal and convert it to a fixed wired signal. In this way we can use fixed wired bandwidth to make up for the bandwidth deficiency of 2G (second generation, second-generation mobile communication technology) and 3G (3rd-generation, third generation mobile communication technology) network.

In order to provide better service, the network service provided by SP (service provider) must have user authentication mechanism. The existing authentication mechanism of WLAN cannot meet the requirements of convenience and safety comparing with 2G/3G networks' authentication mechanism.

2. Research Background

Currently, WLAN authentication process is relatively complex. In general portal Web page mechanism will be used for authentication, as shown in Figure 1. Figure 1 is a

ISSN: 1738-9976 IJSIA

schematic flow diagram of an existing WLAN authentication. User terminals STA (station) connect to the Central AAA (Authentication, Authorization, and Account) server through the Access Controller AC (access controller) to finish the Portal authentication. In which STA connect to AC through AP (Access Provider). STA is connected with AP by wireless connection, and AC is connected with AP by wired connection AC [3, 4].

Figure 1. WLAN Traditional Authentication Framework

Specific procedures are as follows:

1. The STA (user terminal station) will find a number of SSIDs (Service Set Identifier), STA will choose one to associate, and obtain an IP address after the process of network attachment;

2. AC has an authenticated user information table in which every authenticated STA has a data item. The information in the table can be modified according to the commands sent by the radius server.

3. If STA requests to surf on the Internet, AC will be notified the operation and determine whether the STA has the authentication to access to the Internet. Central portal server is part of the central AAA. If the STA does not have the authentication, the request will be redirected to the central AAA, and an authentication page from central portal server will pop up on the STA. Then the STA user can perform normal login with the account and password, and the login information will be submitted to the central portal. Central portal server will request an authentication to the central radius server according to the login information, and then return the authentication result to the AC and STA. AC will add an item to the authenticated user table, and let go the STA's original request to surf on the Internet.

4. If the STA has the authentication to access to the Internet, AC can find will let go the request to surf on the Internet, and no more redirection will be done.

5. When the STA user logs off, the central radius server will send a command to AC ask AC to delete the authenticated STA.

6. Next time when the STA accesses to the Internet, steps 1 through 5 will be repeated.

The existing Mobile WLAN Internet gives huge user experience gap with the GPRS (General Packet Radio Service). Following are their main aspects:

Because phone screen is small, so it is not very convenient to type words on the portal web page; WLAN mobile client software is required to installed by the user and needs to fit a variety of phone models, development investment is huge, usability is low ; SIM (Subscriber Identity Module, SIM cards) authentication is limited to the terminal and the network, so it cannot reach large scale quantity in short term [5-7]; other existing network using only MAC address to authenticate has security deficiencies [8, 9].

3. Fast Authentication Method

The main purpose of this study is to provide a fast wireless LAN authentication method which is designed to achieve rapid network access by the mobile phone user and improve the user experience.

UA (user agent) is a protocol used between terminal browser and server for user to use Internet. Different terminal hardware and software uses different UA information. In

order to provide differentiated services to different user, server can determine the type of user from different UA information provided by the terminal user.

MAC (Media Access Control) address is the hardware physical address. To access the Internet, every network device must have a globally unique 48 binary number as its MAC address.

In this paper, we use STA stand for the terminal user, UA for the UA information of the STA, MAC for the MAC address of the STA.

WLAN network authentication system includes AC, BOSS (Business Operation Support System) and the Central AAA. In a WLAN network, BOSS provides creating and maintaining service of user data and SMS (short message service) support simultaneously. AAA is a centralized-control system including radius server and portal server.

The fast WLAN authentication method proposed in this paper is depicted in Figure 2.

The fast authentication method proposed in this paper will only apply to mobile phone user. AC can determine a mobile phone user from its UA. Step S101: after the terminal connects to the network, AC can get the MAC and UA of the STA. If a STA is a mobile phone user, AC requests local AAA for the register information of the STA according to its MAC and UA. Step 102: AC handle the portal authentication process to the central AAA for the STA with the registered MAC and UA of the STA obtained in step S101.

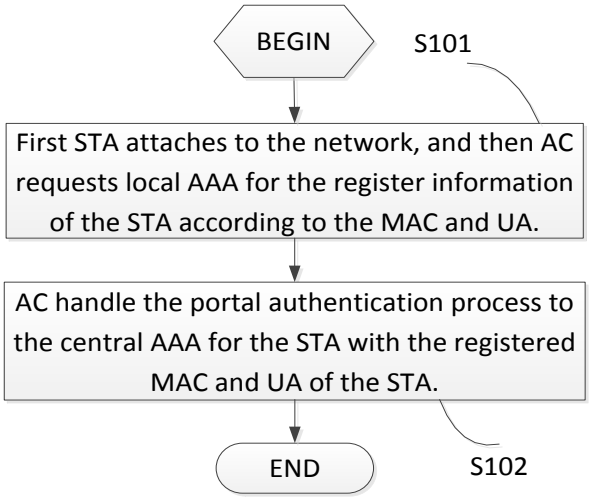

Figure 2. Process of Fast Authentication

Compared with the traditional portal authentication, the fast authentication method proposed in this paper adds local AAA to the system, and the authentication is more convenient and safe. The local AAA includes local radius server AAA and portal server. Network architecture of the fast authentication is shown in Figure 3.

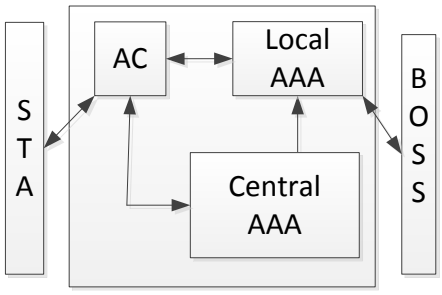

Figure 3. Network Architecture of Fast Authentication

Central AAA stores all the WLAN users' account information for authentication. For each user the information should include user name and password. Local AAA stores local user's registration information including account information, MAC and UA of the STA. The local AAA can send messages to the STA through BOSS, and support the operation of create delete and modify for STA user according to the commands from BOSS.

Step S101: AC can get the MAC and UA of STA when STA connects to the network. And then AC requests local AAA for the register information of the STA according to the MAC and UA. This process is detailed depicted in Figure 4.

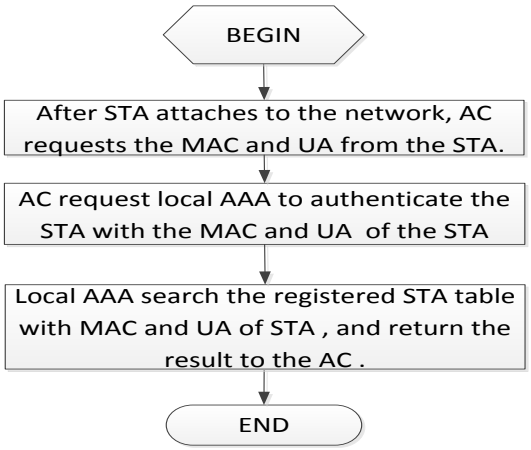

Figure 4. AC Check Local AAA Registration Information

In WLAN system, an AP will broadcast a certain SSID (service set identifier) to uniquely identify its service. A STA should associate to a SSID before it can access the Internet. If the STA is a mobile phone user and the uplink network traffic of STA during a period of time exceeds the threshold, fast authentication process will be activated.

The authentication process of the STA is depicted in Figure 5.

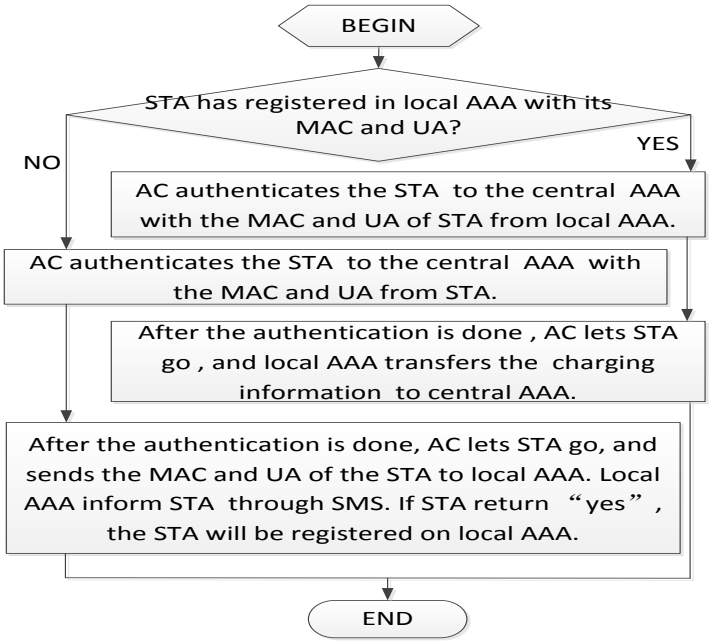

Figure 5. STA Authentication of the Fast Authentication Method

If the terminal is a mobile phone user, AC will request local AAA to check whether the user is a registered user. The registration information includes MAC address and UA and account information. If all three information are matched with the information from STA, the system identifies the STA as registered STA and let go the STA's request to Internet. If the local AAA does not have the STA's registration information, the system can conclude this is the first time the STA use fast authentication and traditional portal authentication should be performed which means the request for Internet will be redirect to the central portal. If the local AAA has the STA's registration information, AC will handle the authentication process to central AAA instead of STA with the MAC and UA information got from local AAA. And on the STA side, no more portal authentications are needed. The fast authentication method improves the efficiency of the authentication significantly. The fast authentication method verifies the MAC, UA and the account information of STA. When there is a counterfeit user to imitate one characteristic of the STA, the system is able to identify and inform the legitimate STA user proactively via SMS. To enhance the security of the system, when user changes SIM card or mobile phone, one of the STA's account information will be changed, and the system will notice the change and delete the rapid authentication registration information stored in local AAA. A new traditional portal authentication should be performed when the STA access the Internet.

If the STA's information is not registered on the local AAA, the authentication process is depicted in Figure 6. AC handles the traditional portal authentication process with central AAA with the UA and MAC information from STA. After the successful portal authentication, a successful authentication web prompt will be brought to the STA user, and AC will let go the STA's request for Internet. Then AC will record related STA status information, and request the local AAA to add a register record about the STA in the registration STA table. After the local AAA identifies the STA as a mobile phone user with its UA, STA will receive a SMS request for start its fast authentication service from local AAA through BOSS. If the STA reply the SMS message with "YES", its fast authentication service will be started and the local AAA will add the STA's information to the registered STA table.

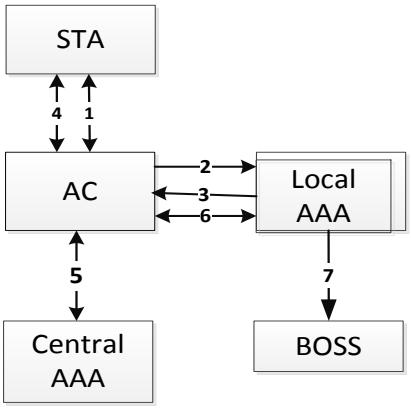

Figure 6. Authentication Process of Unregistered STA

Fast authentication process when STA information has been registered in local AAA is depicted in Figure 7. If the MAC address and UA of STA and STA account information have been registered on the local AAA, the local AAA will inform the AC of STA account information. Then AC will handle the portal authentication process to the central AAA instead of STA. After successful authentication, AC will update STA status information saved in AC according to central AAA's command and let go the STA's request for Internet. And on the STA side, no more portal web pages will be popped up. The STA information for fast authentication in local AAA will be updated after central

AAA authentication is successful done. The updated information including the last time fast authentication used by the STA and routing information can be a basis for further network optimization. At the end of the fast authentication, STA will be informed the use of the fast authentication through BOSS system by local AAA for safety reason. And if for safety reason the STA wants to stop the service, STA can shut down its fast authentication service temporarily or permanently by BOSS system.

Fast authentication process when STA information has been registered in local AAA is depicted in Figure 7. If the MAC address and UA of STA and STA account information have been registered on the local AAA, the local AAA will inform the AC of STA account information. Then AC will handle the portal authentication process to the central AAA instead of STA. After successful authentication, AC will update STA status information saved in AC according to central AAA's command and let go the STA's request for Internet. And on the STA side, no more portal web pages will be popped up. The STA information for fast authentication in local AAA will be updated after central AAA authentication is successful done. The updated information including the last time fast authentication used by the STA and routing information can be a basis for further network optimization. At the end of the fast authentication, STA will be informed the use of the fast authentication through BOSS system by local AAA for safety reason. And if for safety reason the STA wants to stop the service, STA can shut down its fast authentication service temporarily or permanently by BOSS system.

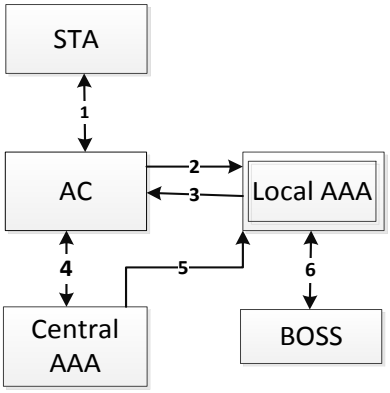

Figure 7. Authentication Process of Registered STA

The practical commercial application of this method has shown that this method is more convenient than the traditional portal authentication, and need fewer changes to the existing network than the client software authentication and the SIM authentication. The combination of MAC address and UA in this method can effectively prevent potential MAC address or the UA been counterfeited, and improve the safety of the system.

4. Summary and Conclusions

Compare with traditional portal authentication of WLAN, fast authentication method described in this paper is more convenient for STA users and practical for WLAN service providers. This paper retains the existing Portal certification process to the central AAA certification and increases the local AAA server to support fast authentication. Local AAA can save STA user account information and the STA's UA, MAC and STA registration information. The system using this fast authentication is called fast authentication system. When the STA first use fast authentication system, operation on the STA side is same as the operation in the traditional portal authentication; but on the system side fast authentication system will save the STA user accounts and STA's MAC, UA and registration information in the local AAA. When all these information are saved

in local AAA, we can say the STA is registered or the STA is authenticated. When a registered STA use the fast authentication system, from the STA's point of view no more authentications are needed, and AC of the fast authentication system will do the authentication job for the STA. Quick authentication system using STA user account information, UA and MAC of STA can improve the safety of the system and reduce the garbage data to the central AAA and improve the performance of central AAA. This method can be compatible with existing authentication, and fewer changes should be made to apply this method to existing network. This method can be supported by all WLAN terminals. So the practical application of this method has promising prospects.

Acknowledgements

This work was supported by the National High-Tech Research and Development Program of China (863 Program) under grant No 2011AA01A104 and Key Science and Technology Program of He'nan Province of China under grant No 132102210044. It was also supported by Foundation of He'nan Educational Committee under grant No 14A520010.

References

[1] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std. 802.11 2007, **(2007)**.
[2] A. Tudzarov and T. Janevski, "Functional Architecture for 5G Mobile Networks", International Journal of Advanced Science and Technology, vol. 32, **(2011)**, pp. 65-78.
[3] IEEE Std. 802.11i-2004, **(2004)**.
[4] Q. Ni, L. Romdhani and T. Turletti, "A survey of QoS enhancements for IEEE 802.11 wireless LAN", Wiley Journal of Wireless Communication and Mobile Computing (JWCMC), vol. 4, no. 5, **(2004)**, pp. 547-566.
[5] J. Arkko and H. Haverinen, "Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA)", Internet Draft. draft-arkko-pppext-eap-aka-15.txt, **(2004)**.
[6] J. Lei, X. M. Fu and D. Hogrefe, "Comparative studies on authentication and key exchange methods for IEEE 802.11 wireless LAN Computers and Security", vol. 26, **(2007)**, pp. 401-409.
[7] L. Zhangzhe and S. Huaying, "Research of WLAN authentication in roaming environment with the trend of network integration", Journal on Communications, vol. 33, no. S1, **(2012)**, pp. 233-238.
[8] L. MeiChang, W. Meng and Y. Haitao, "Discussion on Guangdong Unicom WLAN authentication without perception application deployment", Designing Techniques of Posts and Telecommunications, vol. 2, **(2014)**, pp. 52-57.
[9] Q. Jin'guang, L. Xiangqian and W. Xinzhong, "Research on security of WLAN authentication system", Telecom Engineering Technics and Standardization, vol. 12, **(2013)**, pp. 24-27.
[10] W. JiYi, L. WenJuan, H. JianPing, Z. JianLin and C. DeRen, "Key techniques for Mobile Internet: a survey", SCIENTIA SINICA Informationis, vol. 45, no. 1, **(2015)**, pp. 45-69.
[11] Z. Jun and W. Ji-yi, "Provable Secure Efficient Arbitrated Quantum Signature Scheme", Journal of Beijing University of Posts and Telecommunications, vol. 36, no. 2, **(2013)**, pp. 113-116.

Author

Guo Hong-tao, received his MS degree in computer science from HUST (huazhong university of science and technology), Wuhan, China in 2005. He is currently a lecturer in the software institute at North China University of Water Resources and Electric Power. He has more than 10 technical publications as well as about 3 patents. His current research interests include wireless communication system.

