Wireless Network Security Detection System Design Based on Client

Li Baiping,Yu Huawei,Tan Fengfen

Xi'an University of Science & Technology, Xian 710000, China
569285117@qq.com

***Abstract*—Paper first discusses the development and security safeguard mechanism of WLAN(Wireless Local Area Network).Then it introduces the technical standards of several types of security protocols in the development of WLAN,analyzes the security problems of several standards in application,and finally proposes a Phishing Wi-Fi detection scheme.**

Keywords-WLAN; Security Protocols; Phishing Wi-Fi

I. INTRODUCTION

WLAN layout is relatively flexible,which brings a lot of potential threats to itself. It is easy to be eavesdropped, because the data in the network is transmitted over the air through radio waves.In the wireless network environment,it is difficult to apply the physical access control method to the wired network.So it faces more security problems than wired networks.

In terms of WLAN security mechanisms,the earliest IEEE802.11 standard which was released in 1997,did not define a security scheme.The first WEP（Wired Equivalent Privacy)aiming at WLAN security didn't appear until the release of the IEEE802.11b protocol in 1999.Later,it was discovered that there was a major security flaw in WEP.Along with the IEEE802.11i standard appeared in June 2004,the security performances in WLAN protocol were greatly improved and developed.In September 2009,the IEEE802.11w standard was released as an extension to the 802.11i standard,mainly regulating the registration and management of frame encryption and making up the existing vulnerabilities in the 802.11i standard.

WLAN security safeguard mechanism generally consists of three parts:access control and authentication,encryption algorithms and key management,data integrity testing. In order to avoid any user free access to the network, access control and authentication through user's identity and authorization status to verify.Encryption algorithms and key management are designed to prevent unauthorized users from extracting information from them.The data integrity check is used to verify whether the data has been tampered. Because of the broadcast nature of radio waves,WLAN face more security issues than wired networks,typically including:

1)Unauthorized access to data: an intruder can use a wireless network card to tap the user data, signaling data and control data on the wireless link,then analysis the traffic flow to obtain user data.

2) Denial of service attack: to achieve radio link denial of service attacks,the intruder interfering the correct transmission of user data, signaling data and control data on the radio link,.

3) Pseudo-AP interference: An attacker can set up a high-power AP to cover the real AP so that the wireless terminal is connected to the pseudo-AP.

4) Threat to Integrity: An attacker could modify, insert, replay and delete legitimate users' signaling data on the radio link throw sending data to the network.

II. PROJECT DESING

There are already a lot of detection tools against network malicious attacks in the market,which are implemented in hardware and require higher cost.Generally, they are adopted in large scale enterprises.However,the detection system on client has been barely developed in recent researches.A detection software based on client is presented in this paper.

SYSTEM SCHEME: ensure the terminal is connected to wireless network,then determine the type of the network according to the network attribute information,finally, send the network verification data packet to the network. According to the data returned from the packet, the terminal will estimate whether the wireless network is a phishing one. If so, prompt user to disconnect from the wireless network. The scheme can accurately detect the wisely camouflaging phishing wireless network and also protect the user information security.

A network type determination unit,a phishing network determination unit,and a user prompt unit are concluded in the phishing network detection system includes,as shown in Figure 1.

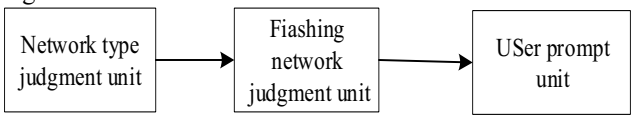

Figure 1. phishing network detection system diagram

The specific realization of the flowchart shown in Figure 2.

A. Judgment unit of network type

T1, terminal connect to the wireless network;

The information of SSID,RSSI, BSSID,channel, maximum data transfer rate and encryption type will be collected in this step.

T2,determine whether the wireless network is a encrypted one;if not,remind the user that it is a non-encrypted wireless network,and skip to step T3;otherwise, prompt the wireless network to be a non-encrypted network, and skip to step T3;

0-7695-6368-6/18/$31.00 ©2018 IEEE
DOI 10.1109/ICITBS.2018.00066

T3,judging whether the wireless network is a carrier network,if yes and it is non-encrypted network,switching to F1 in the phishing network determination unit; if yes and being encrypted,skip to R2 in the prompt unit of the user; Otherwise,if this is not the case,go to step T4;

When the user asks for a connection request, the carrier's network will ask the portal server for identification through the AC,then the portal server will push the unified authentication page to user.

T4,determining that the wireless network is a home network,and turn to F5 in the phishing network determining unit;

B. Judgment unit of phishing network

F1,sending the first level authentication data packet to the wireless network;

To detect the network's connectivity we need to send the first level authentication data packet to the wireless network.When the client receives feedback data from the packet,it means that the network is connectable.

F2,judging whether the received F1 feedback data is correct,if yes,turn to step F3;otherwise,turn to R2 in the user prompt unit;

F3,sending second level authentication data packet to the wireless network;

F4,verify the correctness of the data returned by F3,and if it is right,turn to the user prompt unit R1;otherwise,turn to the user prompt unit R2;

F5,sending a verification data packet to T4 in the network type determining unit;

F6,judging whether the received data of F5 is correct,if yes,turn to R1 in the user prompt unit;otherwise,turn to R2 in the user prompt unit;

C. User prompt unit

R1,determine the wireless network a secure network;

R2,determine the wireless network a phishing network and prompting the user.

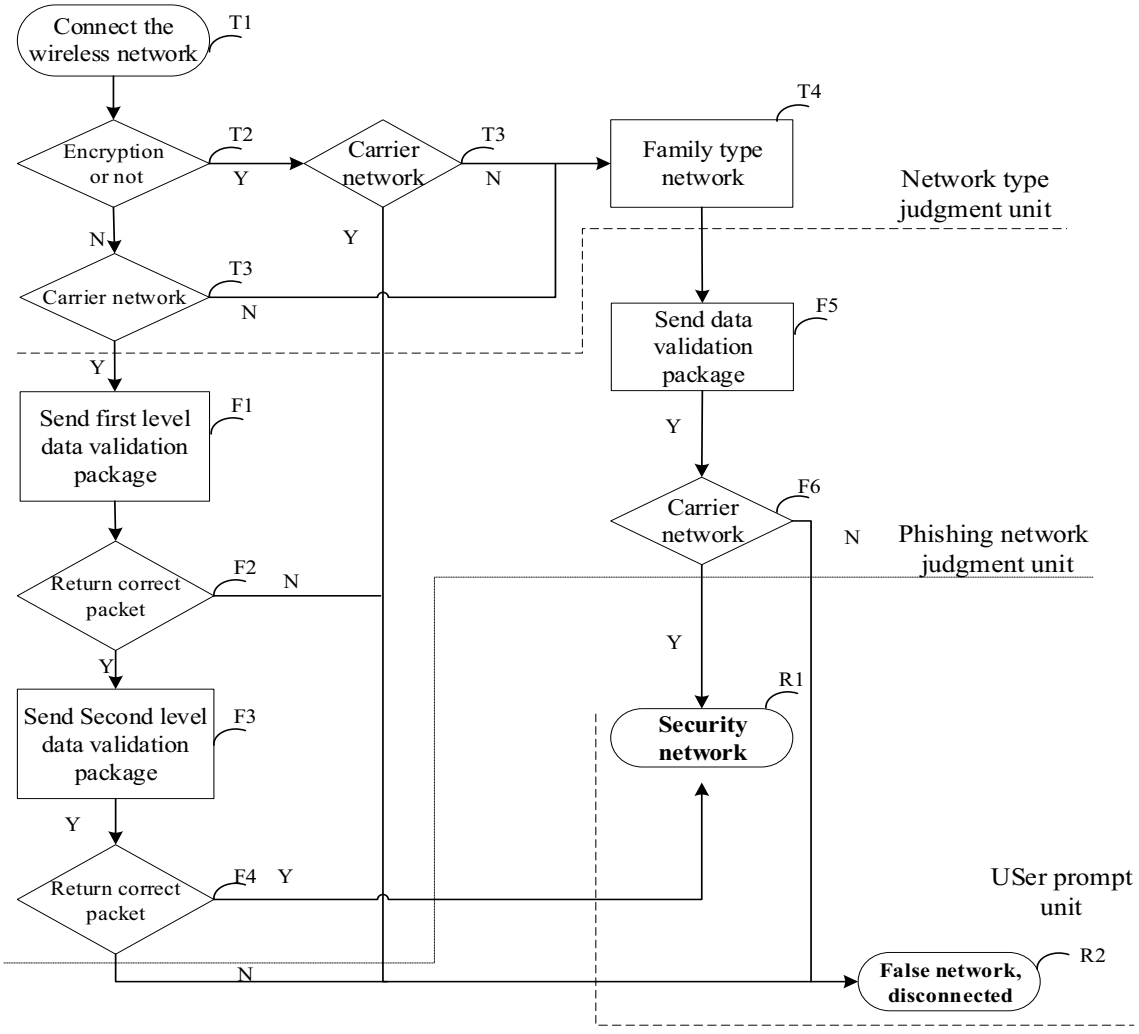

Figure 2. holistic system design flowcha

III. EXPERIMENT VERIFICATION

The main purpose of the system is detecting phishing Wi-Fi through the client,and alarming the user about it.We implement the experiment through two scenarios:

Scene one,establish a normal home wireless network whose SSID is "206" ,and test its legitimacy;

Scene two,use a wireless LAN card attack the network with the SSID of "206"that we have just established in scene one, and another wireless LAN card establish a virtual network with the same SSID of "206" at the same time.

Experiment equipment:a laptop (Ubuntu operating system),two wireless LAN cards,one is used to attack the normal network and the other to create a fake network;a Android phone, used to connect and detect Wi-Fi. The overall experiment environment is shown in Figure 3.

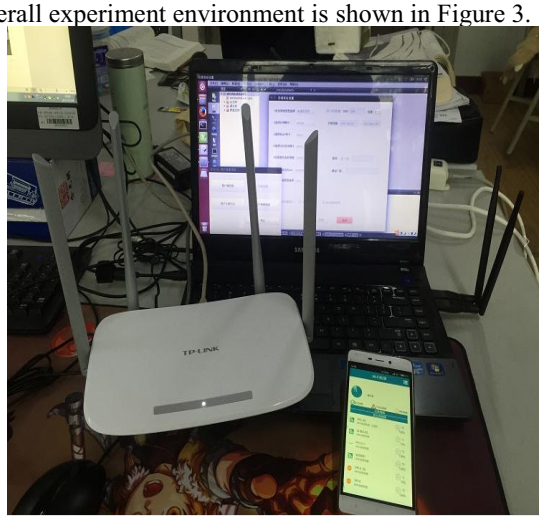

Figure 3. Experiment environment

As it is shown in the figures presented below,a network that has been connected and needs to be detected.Figure 5 shows a detect-result about a valid Wi-Fi,and Figure 6 shows a detect-result about a phishing Wi-Fi.

IV. CONCLUSION

This paper presents a lightweight phishing Wi-Fi detection scheme based on client,verifies its feasibility through experiments,and achieves the detection of phishing Wi-Fi on the client.In view of the potential security risks of WLAN,to protect the enterprises from being attacked,here gives some ways to strengthen the WLAN security:

1) Adopt WPA-AES authentication method,use high-strength password(character,letter and number mixed),and change the password frequently.

2) Turn off the DHCP service,disable dynamic IP allocation,assign static IP to each computer,and implement bidirectional binding between IP and MAC to prevent unauthorized users from connecting to WLAN.

3) Changing the service set identifier and prohibiting SSID broadcast to prevent strangers illegally access to the wireless network.

4) Deploy wireless intrusion detection system to detect illegal network behavior,alarm abnormal network traffic and MAC address spoofing,and prevent large-scale network attacks.

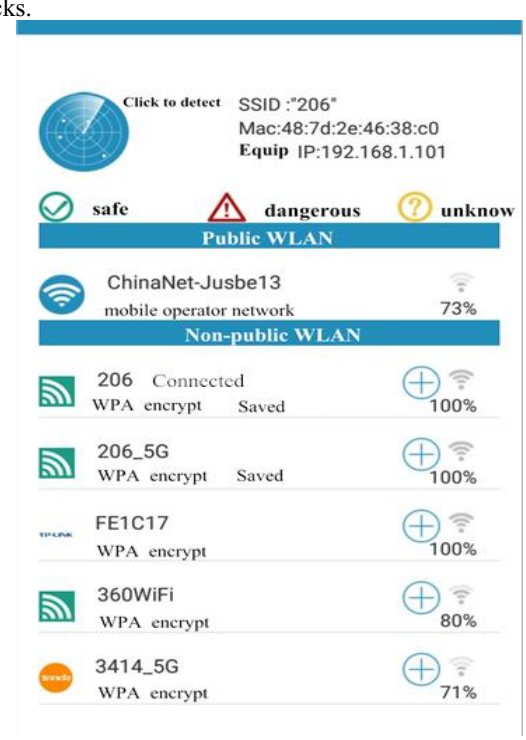

Figure 4. test interface

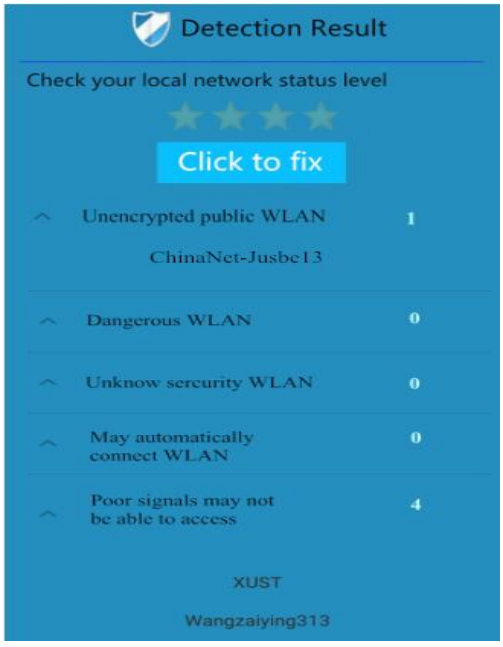

Figure 5. legitimate Wi-Fi detect result

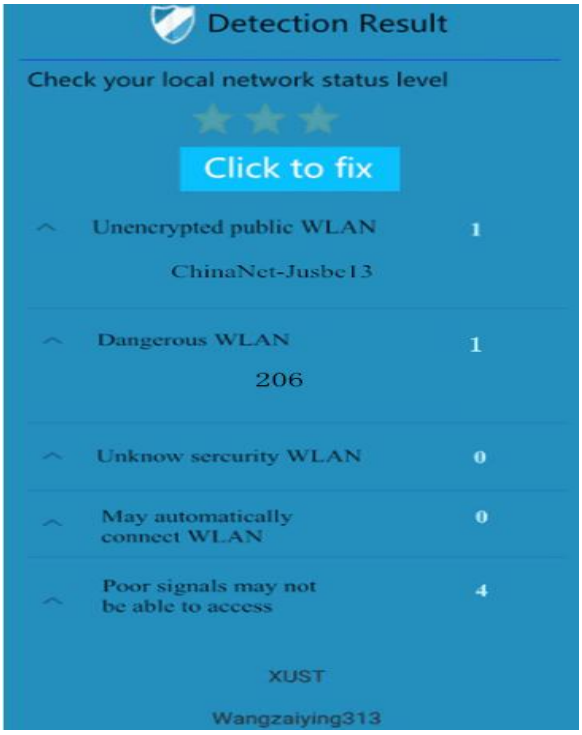

Figure 6. phishing Wi-Fi detect result

REFERENCE:

[1] Zhang lei,Zheng fei,Analysis and research of wireless LAN security protocol.Shanghai:2004,09:132-137.

[2] Mishra A,Nadkami K,Patcha A.Intrusion Detection in Wireless Ad-Hoc Network.IEEE Wireless Communications,2004,11(1):48-60.

[3] Snort-Wiress[EB/OL],http://www.snort-wireless.org.

[4] Y.Zhang,W.Lee,Y.Huang,Intrusion detection detection techniques for mobile wireless networks[J],Wireless Network,Vol.23,2003.04,pp:63-69.

[5] Y.Huang,W.Fan,W.Lee,P.S.Yu,Cross-feature analysis for detecting ad-hoc routing anomalies[A],In Proceedings of ICDCS[C],Vol.27,2003.06, pp:478-485.

[6] Nam SY,Kim D,Kim J.Enhanced ARP:preventing ARP poisoning-based man-in-the-middle attacks[J].Communications Letters IEEE,2010,14(2);187-189.

[7] Foh CH, Tantra JW.Comments on IEEE 802.11 saturation throughput analysis with freezing of backoff counters[J].IEEE Communications Letters.2005,9.

[8] Jang B,Sichitiu ML.IEEE 802.11 Saturation Throughput Analysis in the Presence of Hidden Terminals[J].IEEE/ACM Trans Netw.2012,20.

[9] Wiedmann U, Lillie T L,Sneiderman R P, et al. Methods and systems for automated configuration of 802.1 x clients:U.S. Patent 8,019,082[P]. 2011-9-13.