

Design and implementation of wireless network security
detection system based on Raspberry Pi

filling explanation

1. All the entries must be a basically complete design. The purpose of the work report is to clearly and accurately describe (or illustrate) the entries (or plans) of the team.

2. The work report is written on A4 paper. Except for the title, all content must be song, 5,1.5 times the line spacing.

3. The template text of each project in the work report is for reference only. After the work report is written, please delete all the template text. (This page is not deleted)

4. The content already listed in the work report template is for reference only. On this basis, the author can add more content or fine-tune the structure of the document.

5. The online evaluation adopts double-blind evaluation, so do not have any information about schools, teams, and individuals in this document, otherwise it will be regarded as cheating.

catalogue

catalogue.....	2
abstract.....	3
Chapter I: Background and Key Technologies.....	5
1.1 Research Background and Significance.....	5
1.2 Introduction to wireless LAN communication.....	6
1.3 802.11 Agreement security issues.....	8
1.3.1 WEP encryption method.....	8
1.3.2 WPA encryption method.....	9
1.3.3 Analysis of WEP security problems.....	11
1.3.4 Analysis of WPA safety problems.....	12
Chapter II: System Design and Implementation.....	13
2.1 System design and composition.....	13
2.1.1 System structure framework.....	13
2.1.2 System function design.....	14
2.1.3 System composition.....	15
2.3 Online detection system.....	16
2.3.1 Hardware composition of the online system.....	16
2.3.2 Online system program section.....	18
2.4 Offline analysis system.....	20
2.4.1 System overview.....	20
2.4.2 Specific implementation.....	20
Chapter 3: Evaluation of Works.....	22
3.1 Detection and capture of the data.....	22
3.2 Data analysis and presentation.....	24
Summary and outlook.....	29
reference documentation.....	30

abstract

Wireless network communication is deeply applied to every aspect of the society, and its security issues are also becoming more and more widely concerned. At present, various wireless network communication protocols are quite different, there are a variety of different encryption authentication methods, it is difficult to authenticate and communicate with each other, and the application scenarios are also very different, it is difficult to use one device or software to detect the security problems of different wireless networks. In order to solve such problems, this project designs a system framework to detect the security problems of wireless network communication. The embedded system carries out different wireless communication protocol modules and listening programs to implement online wireless signal acquisition. Through the development and integration of various software and program modules, the analysis of different protocols and data, security issues are realized offline. Based on this framework, we realize a system of detection and analysis for the weak password security problem of Wi-Fi network. The system is based on Raspberry Pi, which integrates wireless network card, GPS positioning, aircrack-ng series tools, and also includes self-developed analysis software. The system can realize automatic detection of wireless LAN AP access points based on 802.11a/b/g/n/ AC protocol, packet capture and storage, detection of weak password of WEP / WPA / WPA 2 encryption mode, and display the data analysis results in a graphical way. The experimental results show that the system works well for signal detection and safety analysis of WLAN.

Key words: wireless network security; network vulnerability detection; Wifi password cracking; Raspberry Pi;

Chapter I: Background and Key Technologies

1.1 Research Background and Significance

With the rapid development of communication technology, wireless network communication technology is more and more deep into all aspects of the society, in personal communication, smart home, Internet of vehicles, industrial Internet and other aspects have been widely used, greatly facilitating people's life and work. The Wi-fi communication network enables the terminal devices to get rid of the shackles of the network cable, and realizes a certain number of terminal devices to access to and access the Internet network in a large range. Cellular communication network enables people to access the voice and data communication network anytime and anywhere, enabling the Internet to be continuously associated with individuals. Zigbee, Bluetooth and other networking modes make smart home and other devices can be easily connected and controlled.

However, while fully enjoying the convenience brought by wireless communication, the loopholes of various wireless network protocols also make there are many security risks in the application of these communication systems. For example, common Wi-fi networks may be set to a weak password, which will be monitored by attackers and grabbed for analysis by packets, and then invade the target network. Zigbee Many devices in the network use the symmetric encryption mode, using the plaintext transmission key, and many keys are set to the default "ZigBeeAlliance09", which is easy to be guessed and hacked into the target network by attackers. The security risks of these protocols and the hardware and software systems of the operating protocols may affect the application of the upper operating system, and then bring inconvenience and even a serious security threat to people's lives. Moreover, due to the great differences in the system structure, communication

protocols and application scenarios of different network applications, it is difficult to use a specific device or software to complete the security detection of various different network systems.

In view of the above problems, the goal of this topic is to design and implement a security detection tool for various wireless network systems. Through the Raspberry PI carries different communication modules, it can realize the detection and analysis of different types of networks, and can realize the detection and collection of different network signals in different scenarios. The collected wireless network data is downloaded to the local reuse software for analysis to detect possible vulnerabilities in the system. Due to the limitation of funds, time and other factors, this topic only takes the 802.11 protocol in the wireless communication network as the specific detection and analysis object, mainly targeting the weak password security problem of Wi-Fi network. AP hotspot scanning through the combination of hardware and software, handshake packet capture, data analysis and statistics.

1.2 Introduction to wireless LAN communication

Wireless LAN Wireless Local Area Network (WLAN) is a wireless communication network built within a radius of about 100 meters by using a wireless communication protocol. WLAN has several different protocols, the most common communication protocol is the IEEE 802.11 series standard. Since the 802.11 series standard is promoted by the Wi-Fi (Wireless Fidelity) alliance, the wireless LAN based on the 802.11 protocol is sometimes called the Wi-Fi network. Because Wi-fi networks are easily deployed, have good communication quality, have large throughput, and are easy to expand, they have a large number of applications in various scenarios. Our mobile phones, tablets, laptops, desktops, smart wearable devices, smart home appliances and other terminals, can be extremely convenient to access to the Wi-fi network. Wireless LAN has become one of the most important networks in the world.

Wi-Fi networks usually contain infrastructure and related devices [1], which

are generally known as different components of the network. The typical Wi-Fi network components mainly include sites, access points, basic service set, distributed systems, and extended service set:

(1) Site refers to the terminal devices with Wi-Fi communication function that can access to the wireless network, such as mobile phones, laptops and other devices.

(2) Access point refers to a device that can provide wireless to wired bridging function. In terms of basic functions, the wireless router can be considered to be an access point, and the access point is also a site.

(3) Basic service Set (Basic Service Set, BSS), generally composed of sites in the same basic service area, can be divided into independent networks and basic structural networks, as shown in Figure 1. The independent network consists of multiple sites, with at least two sites, which are reciprocal and can communicate directly. The independent network includes an access point and multiple sites that transfer all the communication traffic within the network, including the communication between the various stations within the network.

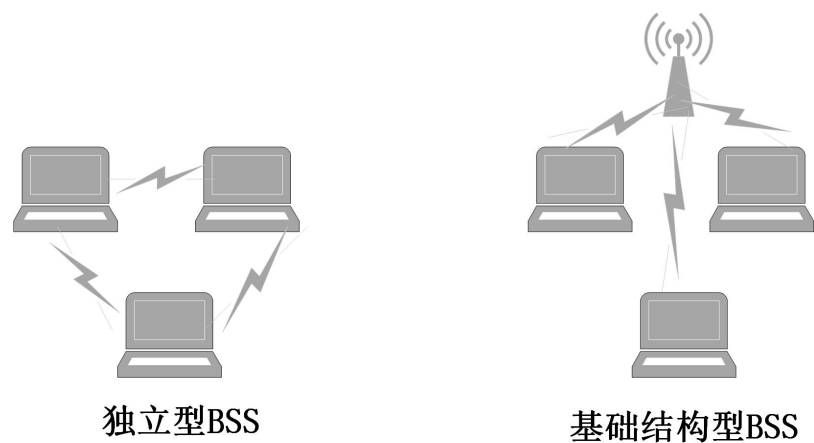


Figure 1.1 Classification of basic service sets

(4) Distributed system, also known as transmission system, is responsible for transmitting frames between base stations and forwarding them to the destination terminal.

(5) Extended Service Set (Extended Service Set, ESS), In order to solve the problem of limited coverage of a single basic service set, multiple basic service

sets can be combined together to expand the coverage area of the wireless network.

1.3 802.11 Agreement security issues

The common encryption methods of wireless LAN are WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) and WPA 2.

1.3.1 WEP encryption method

WEP, the RC4 password used belongs to the symmetric password, that is, encryption and decryption use the same key flow [2]. WEP provides weak authentication between client to access points, but not between access point to client. To enable the receiver to verify that the data received has not been tampered with during transmission, the frame generates an integrity check value through the integrity check algorithm, which is also encrypted during the encryption process. Then, the frame encryption key is assembled, which is composed of the WEP key and the initial vector. The key is the key of RC4, which is the seed of the random number generator. RC4 generates the key flow according to the key, in which the selection of the initial vector has important security significance. Next up is the encryption process, which is usually done by a dedicated circuit on the network card. When encryption is complete, the workstation begins to assemble the frame to be transferred and inserted into the WEP header. Finally, the check code is calculated for the entire MAC frame. When decrypt frame, first check to ensure that the frame is not tampered with during transmission, decryption, the receiver using the same method to calculate the key flow, the text or decryption, and then calculate integrity check value, compared with the check value in the frame, if the same, verify success, the packet to the upper protocol. The WEP symmetric key consists of two parts: a variable 24-bit initialization vector IV, and a fixed 40-bit or 104-bit key. The key plus vector IV constitutes a 64-bit or 128-bit WEP encryption.

The WEP sharing key recognition step is as follows: [3] to realize the secure

authentication of the access point to the client:

- (1) The client sends the authentication request.
- (2) The access point returns the challenge string in plain text.
- (3) The client selects an IV.
- (4) The client uses IV and the basic key to encrypt the challenge string.
- (5) The client sends the IV and the encrypted challenge string to the access point.
- (6) The access point also uses IV and the same base key to encrypt the challenge string.
- (7) There is an association if the encrypted challenge string of the access point agrees with the encrypted challenge string sent by the client.

1.3.2 WPA encryption method

WPA (WiFi Protected Access) — Wi-Fi network security access, is an encryption method designed to improve the lack of WEP, and is a supplement to WEP. WPA addresses these issues with a new protocol for the Temporary Key Integrity Protocol (Temporal Key Integrity Protocol, TKIP), combining a larger initialization vector with the physical MAC address of each device on the network to ensure that each node uses a different key stream to encrypt its data. TKIP then uses the RC4 encryption algorithm to encrypt the data, but unlike WEP, TKIP changes the common keys to make the entire network more secure and less vulnerable to damage.

WPA adopts RADIUS and pre-shared key (PSK) authentication methods. The WPA includes integrity checks to be sure that the key has not been attacked, strengthens the virtual user authentication function provided by WEP, and includes support for 802.1X and Extensible Certification Protocol (EAP), so that the WPA can authenticate wireless users through external remote authentication to RADIUS, or use the RADIUS protocol to automatically change and assign the key.

WPA uses dynamic key encryption, whose keys are constantly changing, making it more difficult to invade wireless networks than WEP. In the small wireless LAN and home network, the PSK mode is adopted, which requires only one key input in advance

in each WLAN node. The customer get access to a WLAN. The longer the pre-shared key password, the more complex, the more difficult it is for hackers to crack, and the longer the crack time, the higher the security of the wireless network. WPA uses TKIP to establish dynamic key encryption and mutual verification mechanisms, and the TKIP security function makes up for the lack of WEP and provides a high level of security for small wireless LAN and home users. In commercial and enterprise level of wireless LAN, using the RADIUS server authentication, extensible authentication protocol (EAP) for verification in the process of message exchange, its bearing is the user to provide authentication required credentials, such as user name password, it through the RADIUS server using 802.1x to verify the identity of the user, provide enterprise security authentication for wireless LAN network.

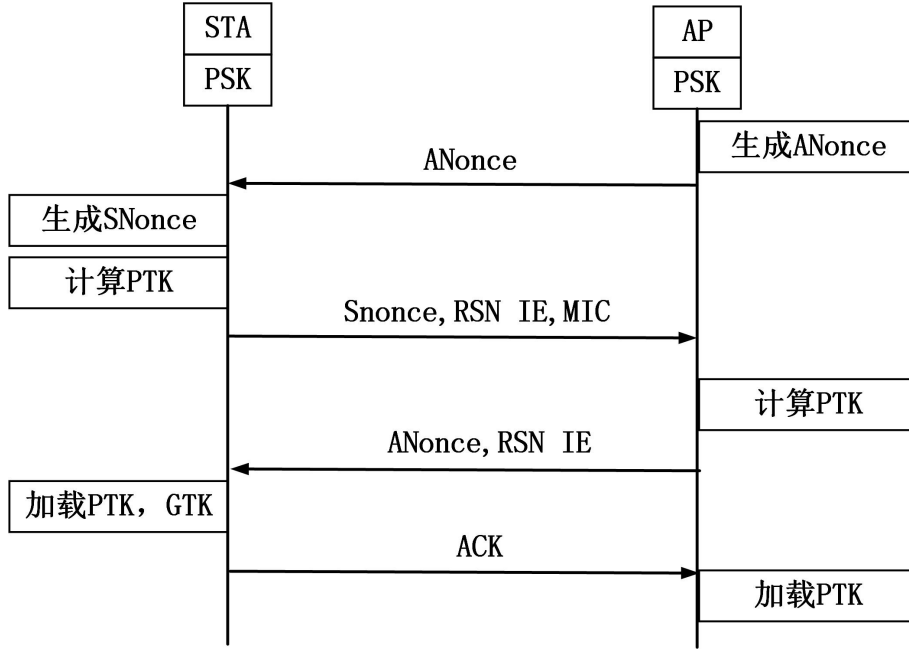


Figure 1.2 Four times handshake process of WPA

$$PMK = PSK = PBKDF2_SHA\ 1\ (passphrase, SSID\ SSID\ Length, 4096) \quad (Formula\ 1.1)$$

$$PTK = SHA\ 1_PRF\ (PMK, len\ (PMK), "pairwise\ key\ expansion", MIN\ (AP_MAC, STA_MAC) \parallel MAX\ (AP_MAC, STA_MAC) \parallel MIN\ (Anonce, SNonce) \parallel MAX\ (Anonce, SNonce)) \quad (Formula\ 1.2)$$

$$MIC = HMAC_MD5\ (MIC_KEY, 16, 802.11x\ data) \quad (Formula\ 1.3)$$

WPA 2 The process of four handshake is as follows:

(1) The authenticator (AP) sends a random number ANonce to the applicant (site Station), using this random number to prevent a replay attack, the message is in the form of broadcast, the message also contains the authenticator's MAC, service set identification (Service Set Identifier, SSID) information.

(2) The applicant sends its own generated random number SNonce and the message integrity verification code to the authenticator, and the whole message is verified by the integrity.

The applicant receives the random number ANonce sent by the access point, and then generates a random number SNonce by himself. According to the algorithm in formula 1.2, calculate the value of PTK. 2, and then the applicant sends MIC, SNIE, SNonce and PTK to the access point AP.

(3) The authenticator sends the serial number of the paired key and the current group temporary key to the applicant. The group temporary key is encrypted with the extended authentication protocol key based on the LAN.

(4) The applicant sends a confirmation message to the authenticator, indicating that the pair of transmission key has been installed and can be used for communication encryption.

1.3.3 Analysis of WEP security problems

The WEP key used for the WEP frame is calculated by using some information known in the data load of the WEP frame. Because the WEP encryption algorithm actually uses the RC4 flow cryptographic algorithm as a pseudo-random number generator, the initial vector IV and WEP key combination to generate the WEP secret key flow, and then the key flow and the WEP frame data load to complete the encryption operation. The RC4 flow cryptography algorithm is the input seed key for some kind of displacement and combination operation to generate the WEP key flow. Since the first byte of the data load in the WEP frame is the 802.2 header information controlled by the logical link, the header information is the same for each WEP frame, it is easy for the attacker to guess that the first plaintext byte and the WEP frame data

load dense text can get the first byte of the key stream generated by PRNG through XOR operation.

In addition, the 24-bit initial vector in the seed key is transmitted in plain text, which the attacker can intercept and save it to the initial vector. S. Fluhrer , I. Martin and A. Shamir Prove: using the known initial vector IV and the first byte key flow output, and combined with the characteristics of the RC4 key scheme, the attacker can determine the WEP key through calculation.

1.3.4 Analysis of WPA safety problems

The key to WPA-PSK cracking lies in the verification of MIC. MIC is generated by formula 1.3, and the important element is MIC KEY, which is composed of the first 16 bytes of PTK. Therefore, then the calculation of MIC must get PTK. According to formula 1.2, PTK is calculated by ANonce, SNonce, MAC, PMK of client and access point. Formula 1.1 can also see that PMK needs to calculate the key (passphrase) of SSID and WPA, so the value of MIC only needs to intercept the data of the first and second handshake packets. The principle of dictionary cracking is to constantly take out a password information passphrase from the dictionary, according to formula 1.1, calculate the PMK, and then calculate the MIC according to other parameter information, and compare the MIC value in the intercepted data package, if the same, is this password, otherwise take out the next password in turn and repeat the above steps.

There are usually two ways for password cracking of Wi-Fi routers using WPA-PSK / WPA 2-PSK encryption, one violent cracking and one dictionary cracking. In fact, the two solutions of the same principle, both are constantly tried to calculate the value of the MIC, and compared with the captured MIC value, the same is the result. The difference is that the violent cracking is to try all the possible situations in order, and the dictionary cracking is based on the dictionary file prepared by the attacker.

Chapter II: System Design and Implementation

2.1 System design and composition

2.1.1 System structure framework

In order to realize the detection and analysis of wireless signals for different types of models, this project designs the vulnerability detection system into two parts: online part and offline part. The online part uses the relevant software and hardware to realize the detection and collection of the communication signals of the target network, and the offline part analyzes the collected data to find out the possible vulnerabilities. The structural framework design of the system is shown in Figure Figure 2.1.

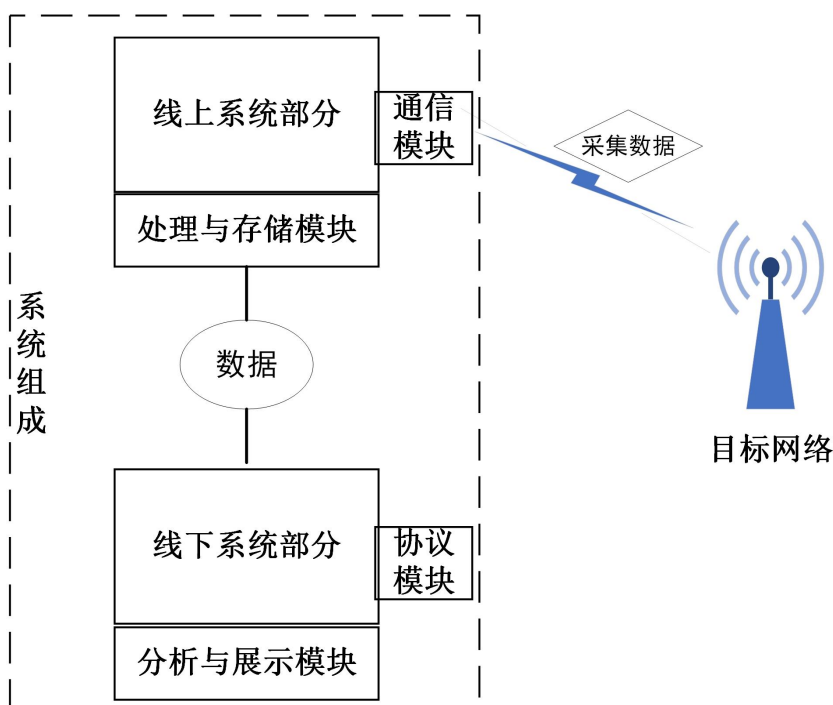


Figure 2.1 Design

The main components of the online system include the basic support platform, processing and storage module, and communication module. Through the support

platform, the online target signal detection and data collection system is built. According to the different communication protocol of the target network, different communication modules are selected to detect and collect the target network signals. At the same time, the corresponding storage module is configured to store the collected data, and the corresponding program is written to complete the functions of detection, collection, storage and processing. Considering that the goal of this topic is to detect and analyze security vulnerabilities, rather than invading the target network, the data analysis is placed in the offline part.

The main components of the offline system part include related support components, analysis and display modules, and protocol modules. The offline system partially receives the collected data, and deploys the relevant protocol modules on the corresponding supporting platform to analyze the communication data and analyze the possible security problems.

2.1.2 System function design

The main function of the system is to collect data, store data, analyze statistics and security detection. The basic functional flow and data flow are shown in Figure 2.2.

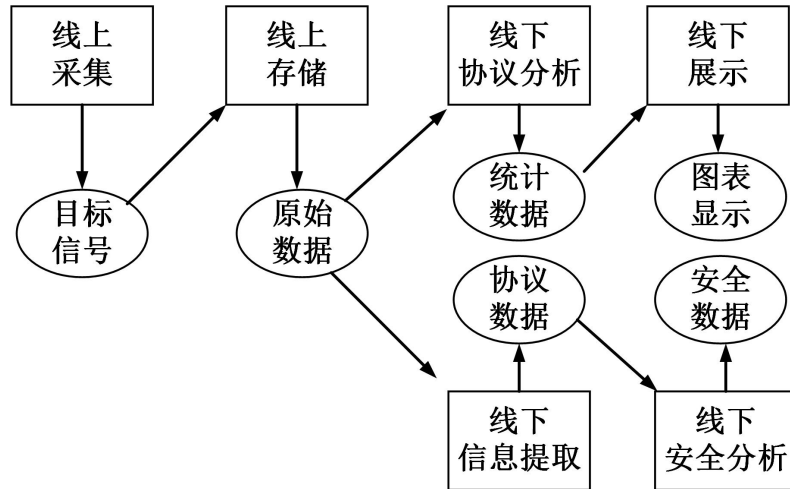


Figure 2.2 A schematic diagram of the system function and data flow

(1) Online collection

The online acquisition module includes the embedded system, wireless network card / antenna, etc., which is mainly based on the embedded development board such

as Raspberry Pi. The existing Raspberry Pi system has certain data processing capability, but the performance cannot meet the requirements, so the existing development board needs to be transformed to integrate the antenna, power supply and other components. On the basis of the Linux system installed on the Raspberry Pi, the grab package tool is integrated to detect the signal.

(2) Online system storage

Online collection uses the packet capture tool to intercept data packets, saved as a file, and stored in the storage space of the system.

(3) Offline protocol analysis and display

In order to analyze the data in more detail, the offline system needs to write programs according to the protocol, extract the frame data from the communication signal file, analyze the data package types, analyze and count the other information, and display it in a chart way.

(4) Offline information extraction and security analysis

Conduct security detection and analysis of the data, extract the relevant information of identity authentication in the data, combine with the existing key cracking tools, and build an effective key dictionary, to realize the key analysis and cracking of offline data packets, and detect whether there are weak password vulnerabilities and other problems.

2.1.3 System composition

Based on the above structure design and function description of the system, the system composition is further refined, and the hardware and software systems such as Raspberry Pi and aircrack-ng are used, combined with the self-developed program, to complete the wireless network security detection system for the weak password cracking of Wi-Fi LAN. The specific composition of the system is shown in Figure Figure 2-3.

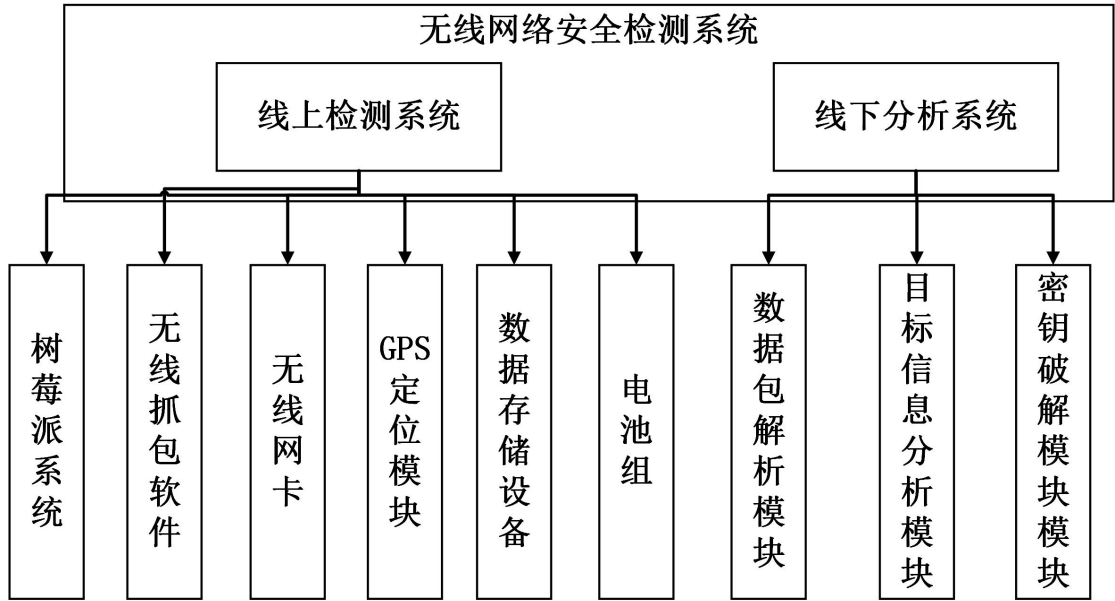


Figure 2.3, the system composition

The whole system is divided into two subsystems: the online detection system and the offline analysis system. The online detection system is mainly developed based on the Raspberry Pi system, including the Raspberry Pi system, wireless network card, GPS positioning module, data memory card, battery pack, and the corresponding wireless grab packet grabbing tool and execution script program group. The offline analysis system mainly consists of data packet parsing program, information analysis program and key cracking program.

2.3 Online detection system

2.3.1 Hardware composition of the online system

This paper develops and realizes a set of online detection system based on Raspberry PI 4, which can realize the detection of target network signals, data packet capture and storage. The hardware composition of the system is shown in Figure 2.4. The system in the figure includes Raspberry Pi, battery pack, GPS module, wireless network card and TTL-USB conversion interface.

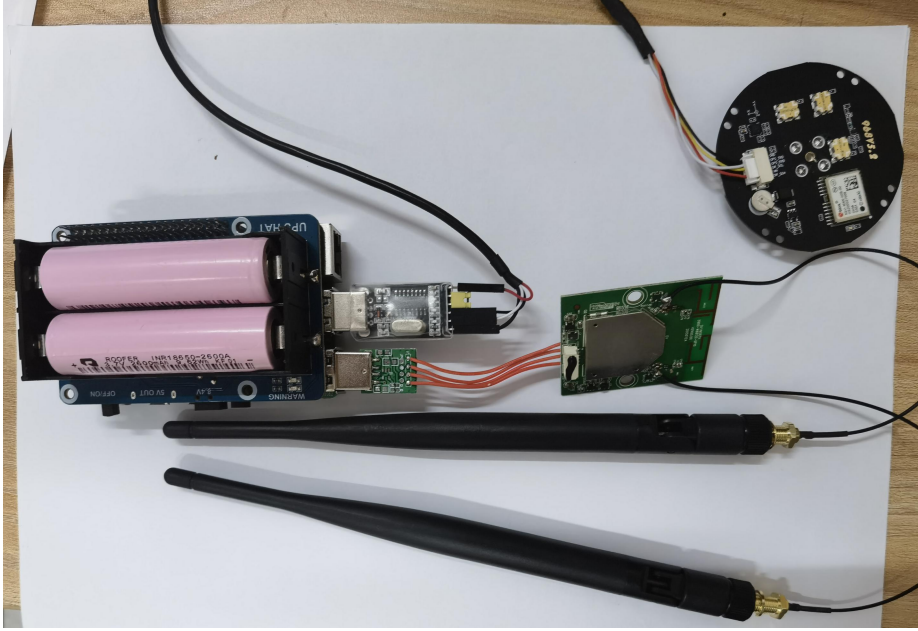


Figure 2.4 Hardware composition of the online detection system

Due to the low power consumption of the wireless network card of raspberry PI and the signal it can receive is weak, the online detection system uses the external wireless network card to detect the Wi-Fi network hotspots based on the 802.11 protocol. When the system runs to the conditions set by the program (for example, when entering a specific coordinate position, or being in a certain static state), the online detection system will open the wireless network card to scan the target area, capture its data packets for the specific target AP, and store them in the external SD memory card of Raspberry PI.

The wireless network card adopted in the system is the RealTek RTL8812AU chip series wireless network card, as shown in Figure 2.5. The operating frequency is 2.4G/5G/5.8G, which can cover the operating frequency range of 802.11a/b/g/n/ac.

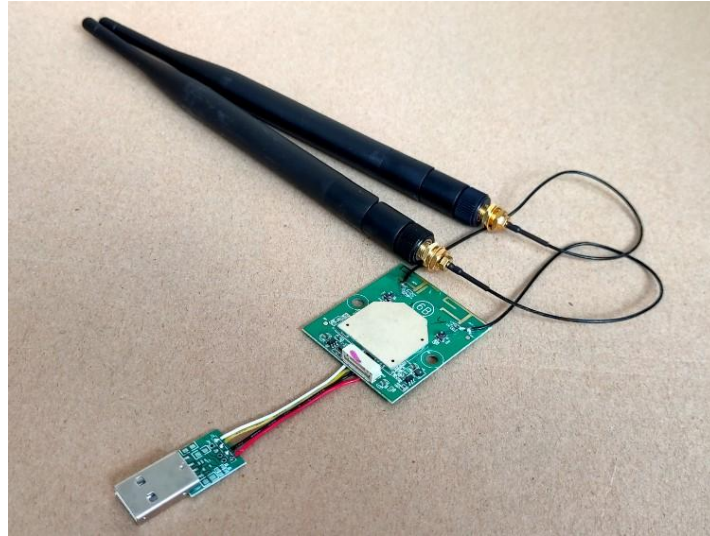


Figure 2.5 RTL8812AU wireless network card

The GPS module adopts the MXT906AM enhanced single-frequency RTK high-precision module, which can achieve the submeter-level GNSS 4-star positioning capability, as shown in Figure 2.6.



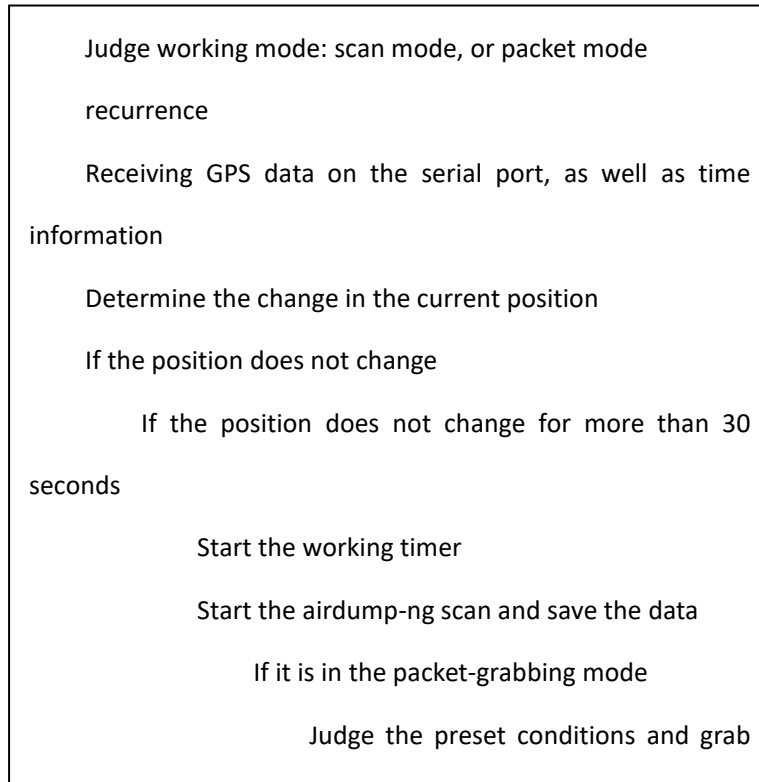
Figure 2.6 The MXT906AM GPS module

2.3.2 Online system program section

The online system program includes two parts. One is the control program based on the python script, which is used to judge the running state of the system in real time according to the user setting, and run the signal detection and package grasping

tool. The second is the signal detection and capture tool, which mainly uses airdump-ng and airoplay-ng tools to scan the target network signal and capture the data package.

The control program pseudocode is shown below.



After running the scanning and packet grabbing, the data was saved as cap format data files, as well as xml and csv format files, as shown in Figure 2.7. The cap file record all target AP communication data of scanning and grasping package, and netxml and csv files record the basic information of AP and listening equipment, including BSSID, ESSID, signal strength, channel and listening time, etc.

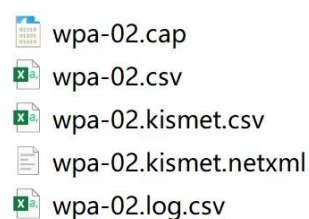


Figure 2.7 List of the saved files

2.4 Offline analysis system

2.4.1 System overview

The offline analysis system includes the protocol data resolution module, the statistical display module and the key cracking module, and the program interface is shown in Figure 2.8. The data resolution module and statistical display module are written based on C++ and used to read the required frame data from cap files and conduct basic statistic analysis of external features, including frame type, length distribution, time period distribution, etc. The key cracking module uses the aircrack-ng tool, which calculates the handshake package in the data based on the dictionary to determine whether there is a weak password vulnerability.



Figure 2.8 Offline analysis system interface

2.4.2 Specific implementation

The procedure is adopted.netframework4.7 Do the interface design, loaded with ws2_32.lib, wpcap. The lib library reads the package, the following is the function of the program:

- Read of the data packets:

```
⊕typedef struct wlan_header { ... } wlan_header;
```

```
⊕int readFrames(vector<Frame>& fvec, char* filepath) { ... }
```

- Package resolution processing:

```
⊕void ConvStat::BasicCharacters() { ... }
```

```
⊕void ConvStat::setLenVal(int num_val) { ... }
```

```
⊕void ConvStat::updateTime() { ... }
```

```
⊕void ConvStat::setTimeval(int num_val) { ... }
```

```
⊕bool ConvStat::ReadParaXml(string m_strXmlPath, BasicInfo& basicinfo) { ... }
```

```
⊕void ConvStat::reset() { ... }
```

- Gps data processing:

```
⊕gps_t* gps_open(const char* path) { ... }
```

```
⊕int gps_next_ex(gps_t* fp, int* type, gps_data* data) { ... }
```

```
⊕int gps_close(gps_t* fp) { ... }
```

```
⊕int parseGPRMC(gps_data* data, GPRMC* ent) { ... }
```

```
⊕int parseGPGGA(gps_data* data, GPGGA* ent) { ... }
```

```
⊕void format_gps(std::ifstream& fin, std::ofstream& fout) { ... }
```

```
⊕int findCharCount(std::string str) { ... }
```

- User implements interaction with the program using the button:

```
private: System::Void button_open_Click(System::Object^ sender, System::EventArgs^ e) { ... }  
private: System::Void button_analysis_Click(System::Object^ sender, System::EventArgs^ e) { ... }  
private: System::Void button_key_Click(System::Object^ sender, System::EventArgs^ e) { ... }  
:
```

The key cracking part of the system calls the aircrack component, loads the program given the dictionary, and breaks the password of the weak password handshake package by violence.

Chapter 3: Evaluation of Works

In order to display the working mechanism of the system, the working process of the system is displayed in detail from two aspects: detection and capture of data and analysis and display of data.

3.1 Detection and capture of the data

The wireless network vulnerability detection system will run automatically after starting from Raspberry Pi. In order to better display its working process, this paper uses the host to remotely access Raspberry Pi, read the running state of its program, and display its working process. When the system raspberry PI moves, the system records its location and time information. When the system stops at a certain point, the program thinks that the system is ready to start detecting the network signal in a certain area, and the start time is 30 seconds. If the system has not moved during this period, the system will automatically start the program to detect the signal and scan the packet.

Figure 3.1 shows a list of the wireless LAN AP information in the target area when the system starts to run the scanning function. The mac address is locally coded to implement anonymization processing.

CH 2][Elapsed: 10 mins][2021-09-30 07:07

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
9C:9D:7E:EF:AA:77	-28	406	2085	0	8	54	WPA2	CCMP	PSK Xia
64:64:4A:2B:2C:2D	-68	342	1	0	4	360	WPA2	CCMP	PSK Red
6A:64:4A:2B:2C:2D	-69	384	0	0	4	360	OPN		<le
8C:21:0A:2B:2C:2D	-71	228	0	0	1	54	WPA2	CCMP	PSK pri
F0:B4:29:2B:2C:2D	-73	318	146	0	11	54	WPA2	CCMP	PSK yan
28:D1:27:2B:2C:2D	-76	303	0	0	11	54	WPA2	CCMP	PSK Mag
D0:05:E4:2B:2C:2D	-77	240	0	0	11	360	OPN		EDL
74:C3:30:2B:2C:2D	-79	189	45	0	13	54	WPA2	CCMP	PSK FAS
D0:05:E4:2B:2C:2D	-79	203	5	0	11	360	WPA2	CCMP	PSK EDL
1A:47:3D:2B:2C:2D	-81	58	0	0	6	54	WPA2	CCMP	PSK DIR
80:EA:07:2B:2C:2D	-84	200	5	0	1	54	WPA2	CCMP	PSK TP-
00:16:78:2B:2C:2D	-85	233	0	0	3	54	WPA2	CCMP	PSK GAO
64:64:4A:2B:2C:2D	-85	61	0	0	40	1733	WPA2	CCMP	PSK Red
34:96:72:2B:2C:2D	-89	96	0	0	1	54	WPA2	CCMP	PSK TP-
FC:D7:33:2B:2C:2D	-93	50	0	0	1	54	WPA2	CCMP	PSK TP-
9C:A6:15:2B:2C:2D	-93	28	19	0	6	54	WPA2	CCMP	PSK TP-
8C:A6:DF:2B:2C:2D	-93	15	0	0	1	54	WPA2	CCMP	PSK TP-
64:6E:97:2B:2C:2D	-93	4	5	0	6	720	WPA2	CCMP	PSK TP-
8E:C8:4B:2B:2C:2D	-93	0	0	0	1	54	WPA2	CCMP	PSK DIR

Figure 3.1 The system scans the wireless local area network in the target area

According to the result of the scan, the program selects a specific BSSID or ESSID, or selects a specific AP according to the signal intensity to carry out the Deauthenticate attack. Through the attack, a connected customer site is forced to disconnect from the AP and has to re-authenticate the connection. During the reconnection process, the system obtains the authentication packet containing the encrypted information. The program running interface is shown in Figure Figure 3.2.

CH 8][Elapsed: 24 s][2021-09-30 07:36

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
9C:9D:7E:EF:AA:77	-47	0	20	54	0	8	54	WPA2	CCMP	PSK Xia

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	F0:B4:29:2B:2C:2D	-79	0 - 1	220	133	magicmusic
(not associated)	DA:A1:2B:2C:2D:2E	-87	0 - 1	0	2	
(not associated)	34:F6:2B:2C:2D:2E	-93	0 - 1	0	2	
9C:9D:7E:EF:AA:77	E4:5F:2B:2C:2D:2E	-27	0e- 0e	176	30	
9C:9D:7E:EF:AA:77	98:8D:2B:2C:2D:2E	-34	0e- 0e	0	158	Xia

Figure 3.2 The system attacks a client under the AP to grab the handshake packet

After the attack and packet capture are completed, the system saves the above data as a working directory, including data packet, AP basic information, etc. The probe program is closed automatically after the system moves. If the system stops many times, the program will run many times to detect the target network in different

regions. The results of each probe scratch packet are saved to a working directory.

3.2 Data analysis and presentation

The data packets detected by the online system can be downloaded locally. The cap file is a general network packet file and can be opened using any third-party analysis software. Figure 3.3 shows the data file to open the system grab package using wireshark.

52	2.636234	f6:d1	6...	XiaomiCo	...	802.11	16 Request-to-send, Flags=
53	2.765331	f6:d1		XiaomiCo	...	802.11	33 Action, SN=925, FN=0, F
54	2.765825	Xiaom		f6:d1:08	...	802.11	33 Action, SN=1097, FN=0,
55	2.795455	f6:d1		XiaomiCo	...	802.11	28 802.11 Block Ack, Flags
56	2.938661			NewH3CTe	...	802.11	10 Acknowledgement, Flags=
57	2.939627			NewH3CTe	...	802.11	10 Acknowledgement, Flags=
58	2.940570			NewH3CTe	...	802.11	10 Acknowledgement, Flags=
59	2.941964			NewH3CTe	...	802.11	10 Acknowledgement, Flags=
60	2.944633			NewH3CTe	...	802.11	10 Acknowledgement, Flags=
61	2.958151			NewH3CTe	...	802.11	10 Acknowledgement, Flags=
62	3.095478		XiaomiCo	...	802.11	10 Acknowledgement, Flags=	
63	3.119309	Xiaom	f6:d1:08	...	802.11	26 QoS Null function (No d	
64	3.149492		BeijingX	...	802.11	10 Acknowledgement, Flags=	
65	3.261319	Xiaom	f6:d1:08	...	802.11	26 QoS Null function (No d	
66	3.261325		XiaomiCo	...	802.11	10 Acknowledgement, Flags=	
67	3.289898	Xiaom	f6:d1:08	...	802.11	26 QoS Null function (No d	
68	3.460833		NewH3CTe	...	802.11	10 Acknowledgement, Flags=	
69	3.461470		NewH3CTe	...	802.11	10 Acknowledgement, Flags=	
70	3.585670		NewH3CTe	...	802.11	10 Acknowledgement, Flags=	
71	3.758699	Xiaom	f6:d1:08	...	802.11	26 QoS Null function (No d	
72	3.887930		NewH3CTe	...	802.11	10 Acknowledgement, Flags=	
73	3.937628		BeijingX	...	802.11	10 Acknowledgement, Flags=	
74	3.957668	Xiaom	f6:d1:08	...	802.11	26 QoS Null function (No d	
75	3.960546	Xiaom	f6:d1:08	...	802.11	26 QoS Null function (No d	
76	3.960832		XiaomiCo	...	802.11	10 Acknowledgement, Flags=	
77	4.079915	Xiaom	f6:d1:08	...	802.11	26 QoS Null function (No d	
78	4.127645		NewH3CTe	...	802.11	10 Acknowledgement, Flags=	

Figure 3.3 Data files for the system probe

Using software analysis, we can analyze the frames in the data, calculate the distribution of different types of frames, frame length distribution, frame number distribution in different time periods, and AP BS SID, ESSID, signal intensity of these basic information. Figure 3.4 shows the proportion of 802.11 different type frames in a probe file.

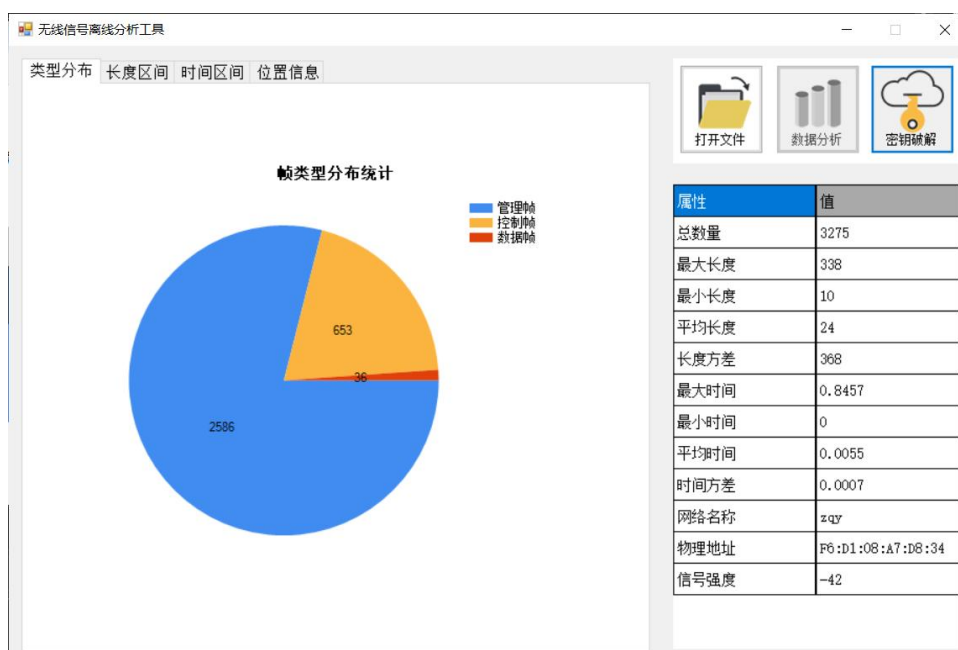


Figure 3.4 Frame proportional distribution

Figure 3.5 shows the different frame length distribution in the data analyzed using the software.

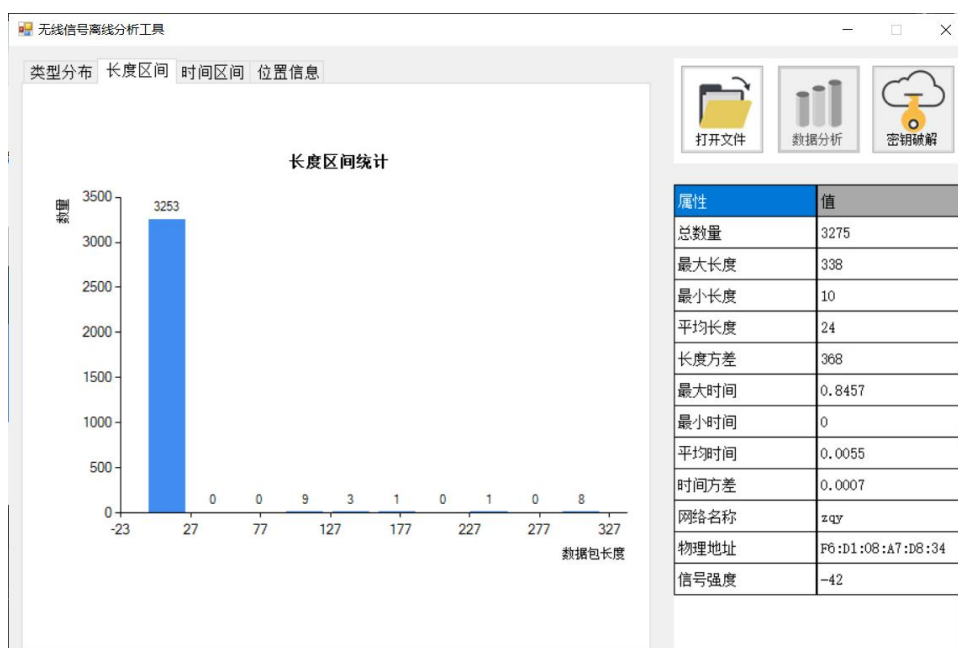


Figure 3.5 Frame-length distribution

Figure 3.6 is the distribution of the amount of data in different time periods in the data using the software.

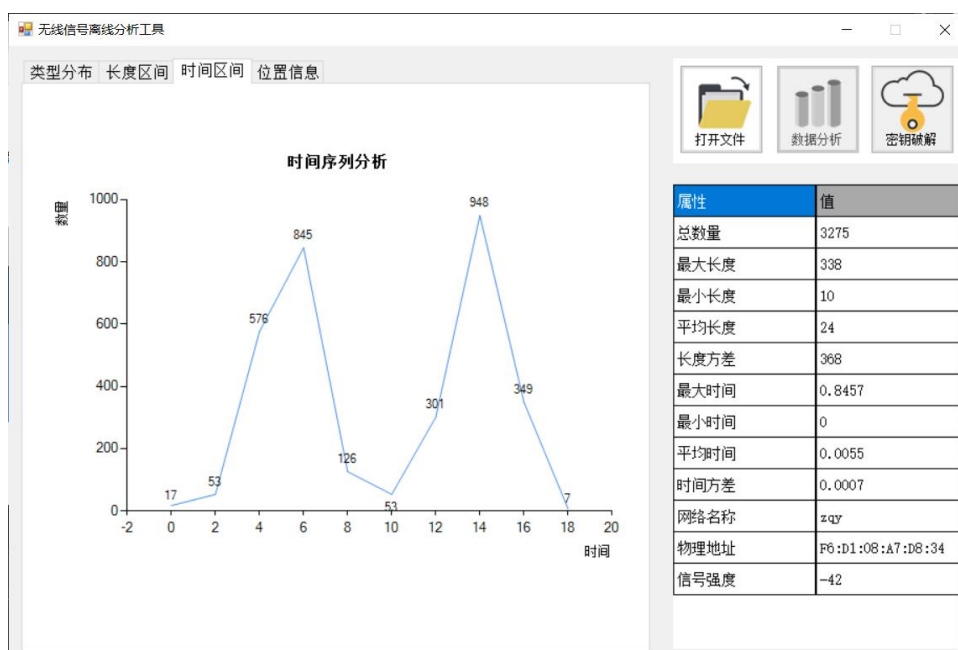


Figure 3.6 Distribution of frames in different periods

Parameters such as frame length, arrival time, and type scale can be used for anonymous traffic analysis.

The position information data during the operation of the system is shown in Figure 3.7, and Figure 3.8 shows the movement trajectory of the system drawn by the GPS data.

```

1 45,23,,46,24,,35*7B
2 $GPGSV,2,2,07,25,,35,31,,24,32,,35*7C
3 $GPGLL,,,,,105130.00,V,N*4C
4 $GPRMC,105131.00,V,,,,,310821,,N*73
5 $GPVTG,,,,,,N*30
6 $GPGGA,105131.00,,,,,0,00,99.99,,,,,*61
7 $GPGSA,A,1,,,,,,,99.99,99.99,99.99*30
8 $GPGSV,2,1,07,10,,40,12,,45,23,,46,24,,31*
9 $GPGSV,2,2,07,25,,32,31,,31,32,,34*7E
10 $GPGLL,,,,,105131.00,V,N*4D
11 $GPRMC,105132.00,V,,,,,310821,,N*70
12 $GPVTG,,,,,,N*30
13 $GPGGA,105132.00,,,,,0,00,99.99,,,,,*62
14 $GPGSA,A,1,,,,,,,99.99,99.99,99.99*30
15 $GPGSV,2,1,07,10,,36,12,,41,23,,42,24,,36*
16 $GPGSV,2,2,07,25,,31,31,,21,32,,24*7D
17 $GPGLL,,,,,105132.00,V,N*4E
18 $GPRMC,105133.00,V,,,,,310821,,N*71
19 $GPVTG,,,,,,N*30

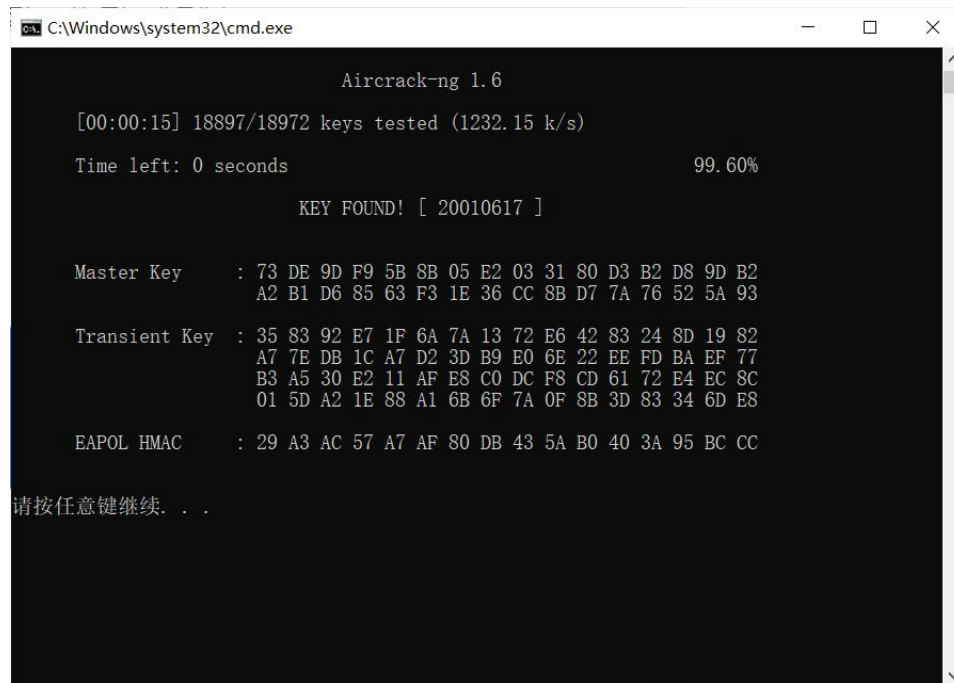
```

Figure 3.7 for GPS data



Figure 3.8, the movement trajectory

In addition to external feature statistical analysis, data can be cracked using aircrack-ng, as shown in Figure 3.9. The results show that the target AP uses a weak password and its key is calculated through a common dictionary violent attack.



```
C:\Windows\system32\cmd.exe

Aircrack-ng 1.6

[00:00:15] 18897/18972 keys tested (1232.15 k/s)

Time left: 0 seconds                                99.60%

KEY FOUND! [ 20010617 ]

Master Key      : 73 DE 9D F9 5B 8B 05 E2 03 31 80 D3 B2 D8 9D B2
                  A2 B1 D6 85 63 F3 1E 36 CC 8B D7 7A 76 52 5A 93

Transient Key   : 35 83 92 E7 1F 6A 7A 13 72 E6 42 83 24 8D 19 82
                  A7 7E DB 1C A7 D2 3D B9 E0 6E 22 EE FD BA EF 77
                  B3 A5 30 E2 11 AF E8 C0 DC F8 CD 61 72 E4 EC 8C
                  01 5D A2 1E 88 A1 6B 6F 7A 0F 8B 3D 83 34 6D E8

EAPOL HMAC     : 29 A3 AC 57 A7 AF 80 DB 43 5A B0 40 3A 95 BC CC

请按任意键继续...
```

Figure 3.9 Connection key crack for the target network AP

Summary and outlook

This project implements a general system framework for wireless network communication protocol security problem detection, and according to the design framework, based on the raspberry pie system, integrated GPS, wireless network card, and aircrack-ng tools, self-developed program to realize the security detection system for 802.11 protocol wireless LAN, and verify the feasibility of the design framework and the availability of the equipment through experiments.

Due to the limited cost and time limit, the system only realizes the security detection for Wi-Fi networks, and fails to realize the detection and analysis of other wireless communication protocols. The next step is to improve the system as follows

(1) For the WLAN network, the directional gain antenna is integrated in the system to improve the sensitivity of the system to Wi-Fi network signals, and the electronic compass is integrated to further accurately locate the area of the target network and realize the accurate capture and detection of AP signals at specific locations.

(2) Increase the support for other wireless network communication protocols, such as Zigbee / Bluetooth, including the communication signal transceiver module, protocol support, protocol resolution program, etc. Different protocol functions are realized in the way of modules, so as to make plug and play.

(3) Add the function of anonymous traffic analysis in the offline system, introduce artificial intelligence algorithm, continue to analyze the external characteristics of anonymous traffic, and further analyze the types of traffic and other information.

reference documentation

- [1]. Crow B P , Widjaja I .IEEE 802.11 Wireless Local Area Networks[J]. IEEE Communications Magazine, 1997, 35(9):116-126.
- [2]. Lu ping. The Design and Implementation of a Wireless Network Attack Detection System Based on WiFi Technology [D]. Beijing University of Posts and Telecommunications, 2020.
- [3]. Gao Gu jun. Wireless LAN security analysis and WEP key improvement [D]. Shanghai Jiao Tong University, 2014.