Advances in Computer Science Research, volume 44
3rd International Conference on Wireless Communication and Sensor Network (WCSN 2016)

The Remote Wifi Investigation of Network and Forensics System for Police Based on Raspberry Pi

Yang Liu, Dian-Jie Lu, Xing-Yue Li
School of Information Science and Engineering, Shandong Normal University, Jinan 250014, China
E-mail: oraaly@aliyun.com, ludianjie@sina.com, 17862954076@163.com

***Abstract*-This project brings forward the design of the remote WiFi investigation of network and forensics system for police based on Raspberry Pi. It can realize remote control in a few hundred meters away, and aim at the traffic data in the suspects' WiFi networks to gather the evidence. The contents of the evidence are specific and comprehensive. This system uses Raspberry Pi as the core device, and uses the XBee module to realize the function of controlling the forensics system remotely and efficiently. It can also sense the surrounding information by the photosensitive sensor. When it gets damaged, it will erase the key documents automatically. This system will ensure the safety of the detectives and fight diverse crimes efficiently.**

Keywords-raspberry pi; xbee module; WiFi forensics; investigation

I. INTRODUCTION

With the rapid development of the WiFi technology and the wide application of mobile devices, mobile social networks are developing rapidly [1-4]. The measures of cyber crimes such as network attacks and telecommunications frauds are not restricted to the implementation of wired networks, instead it is done by wireless networks. Data separating means that while the offenders are committing crimes, the detectives intercept the evidence by some technologies at the same time [5]. Therefore, it has the function of realizing monitoring and getting the intranet data packets in the suspects' WiFi networks. It is of great meaning to the investigation of many criminal cases. But it also increases the difficulty of collecting criminal evidence for its small coverage of WiFi networks and high degree of encryption.

II. INNOVATION

In the information age, the process of law enforcement and evidence collection is very difficult for a lot of relevant departments. Because once there is any error, it will not only get no essential evidence, but also cause immeasurable casualties and the loss of properties. For the law enforcement officers, especially those in the field of digital forensics, it seems even more important to get some possible factors by analyzing the wireless data captured near the suspects' residences [5].

However, the existing forensics of wireless detection equipment makes the law enforcement officers take great risks so that it cannot guarantee the safety of the law enforcement officers. The forensics system based on assev wireless network [6] producted by AnXinWei Technology Co., Ltd. in 2012 demands that the detectives must gather the evidence within the WiFi coverage of the suspects. It cannot realize remote control and effective concealment, which brings great risks to the detectives.

The low-power communication module XBee-PRO HP900 based on the ZigBee protocol and the mini-computer Raspberry Pi offers hardware basis for the design of remote WiFi environment forensics system. The greatest advantage is that there are a lot of measures to crack the WiFi passwords in this remote forensics system. It can come into the WiFi intranet of the suspects in a few hundred meters away with the remote control equipment, then monitor the data packets and deliver them out. It can also work as springboard to intrude the other intelligent devices of the suspects, so that they can gather more criminal evidence. When the system reacts the damage, it will erase the key documents automatically to ensure the confidentiality of the technology and forensics.

III. DESIGN SCHEME

Raspberry Pi works as the control commands receiver of the system and the hardware carriers for specific forensics. It is connected with the control terminal of the detectives by XBee module, then it accepts the control commands and executes the task of cracking the WiFi passwords. Therefore, it can pass the evidence back timely. The power bank supplies electricity for Raspberry Pi. It can be equipped with solar panel alternatively for different forensics environments to increase the endurance of the system. The detectives can let Raspberry Pi carried through Oray Internet/Intranet Dynamic Mapping Service [7] to access the intranet networks of suspects by their external networks. They can see Raspberry Pi as the springboard. Here is the architecture diagram of the system in Fig. 1.

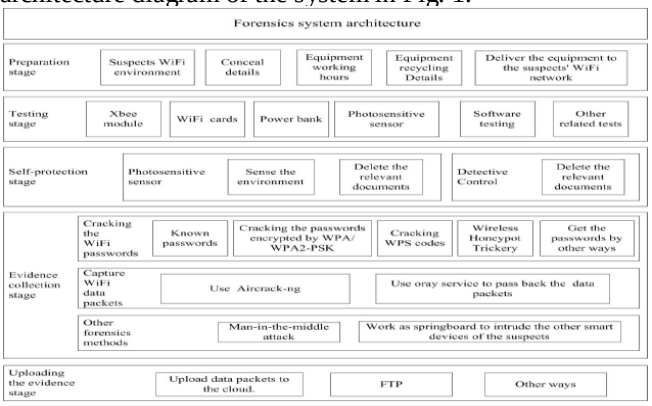

Figure 1. Forensics system architecture.

A. *Hardware Design*

The hardware design of this system has three main parts. They are remote communication modules, hazard sensing circuits and wireless network adapters. Here is the architecture diagram of hardware circuit in Fig. 2.

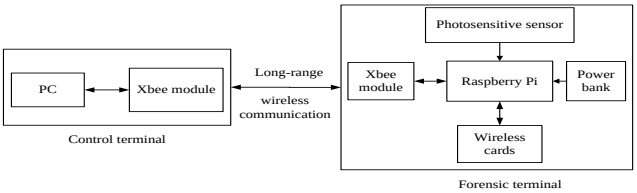

Figure 2. Hardware architecture.

In the remote WiFi forensics system, the core device of serial control and processing instruction is Raspberry Pi [8]. The core module to realize remote communication in this system is XBee-Pro HP900. XBee Adapter Board for Raspberry Pi [9] in this system is produced from Waveshare Electronics. After the actual test, using this adapter board can avoid the connection problems between Dupont Lines and Bread Bands, it can also avoid the interface of the intertwined Dupont Line so that it is able to enhance the robustness of the system.

The wireless adapter used by Raspberry Pi should be able to open monitor mode and achieve driving without installation. By analysing RPi_USB_Wi-Fi_Adapters, it will choose Tenda wireless network card, whose model is W311M(drive：Ralink Technology, Corp. RT5370 Wireless Adapter), install Aircrack-ng,crack WiFi passwords and capture data packets, etc. The system chooses EDU wireless network card, whose model is EP-N8508(drive：Realtek Semiconductor Corp. RTL8188CUS 802.11n WLAN Adapter), to connect WiFi networks and build Wireless Honeypot Trickery.

The system chooses normal photosensitive sensor module,whose working voltage is 3.3V-5V. The photosensitive sensor uses LM393 Wide-Range Voltage Comparator and digital switching outputting(signal 0 and 1)with continuously variable potentiometers, which can adjust and check the threshold of the light.

B. *Remote Forensic Terminal Controlled by Xbee Module*

There is the USB serial console in Raspberry Pi, which uses the USB-to-ttl serial line to connect the GPIO pin of Raspberry Pi to a USB interface of a computer [8]. The principles of the USB serial console controlled by XBee wireless module and the console used by the USB-to-ttl serial line are essentially the same. XBee module is connected with the TXD port of Raspberry Pi(BCM pin 14(P1-08)), RXD port(BCM pin 15（P1-10）) and GND pin (P1-06) by the XBee Adapter Board.It uses the software X-CTU instrument to configure its data rate(Baud rate) of XBee module, which is 115200bps. After finishing the connection of all the hardwares, the detectives open the serial control software in the computer then they will get the Raspberry Pi USB serial console. Compared with the USB-to-ttl serial line, this console has the strength that can realize the remote control of Raspberry Pi by XBee module.

But the method mentioned above will limit the function of data transmission of XBee module. And the data rate(Baud rate) of XBee module can only be 115200bps, which has a certain limitation. To get rid of the limitation, it can use instruction processing module, program startup module and force-completed module to realize the remote forensic terminal controlled by XBee module.

There runs an instruction processing module in Raspberry Pi, which is used to control the XBee module with antenna in XBee Adapter Board for Raspberry Pi. And it is used for receiving the instructions from the control terminal of the detectives. Then it will run the instruction in the terminal and pass the execution results back to the detectives' computer. Here is the specific process of controlling instructions by the module:

The instruction processing module initializes the Raspberry Pi serial port, and it calls the forensic terminal XBee module to pass the successful results of the initialization back to the control terminal. The instruction processing module keeps processing the instruction from the control terminal and executes the instruction in the console, then judges whether it echoes the results back to the control terminal. While the ith unappropriated instruction processing module receives the terminated instruction, it will come to an end by itself. The flow diagram of the algorithm is shown in Fig. 3.

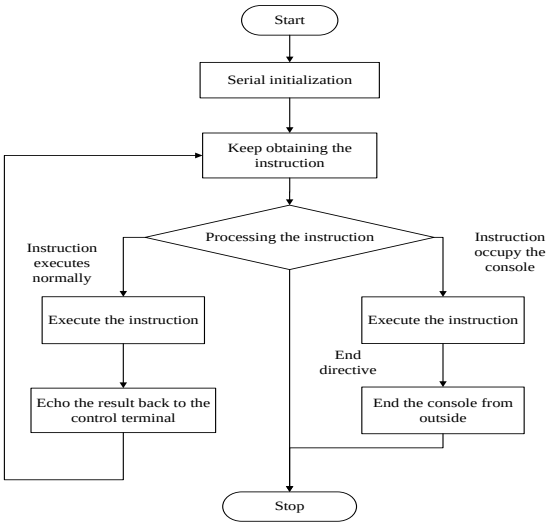

Figure 3. The flow chart of instruction processing module algorithm

Program startup module and force-completed module can resolve the problem that the instructions transmitted from the detectives occupy the instruction processing module.

The program startup module opens an instruction processing module every period of time. Here is the specific process of this step: the program startup module opens the ith instruction processing module(i is a positive integer that is greater than 1), the users set reasonable interval, then the module opens the (i+1)th instruction processing module at regular time.

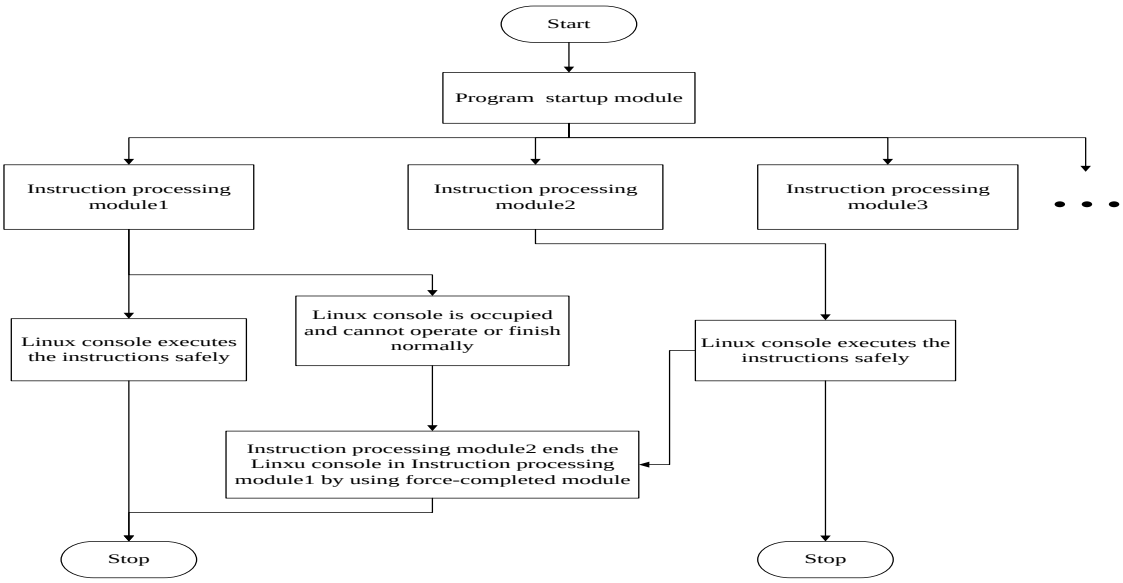

Figure 4. The algorithm to solve the problem of instructions' occupying Linux console.

The force-completed module will end the process of the occupation. After that, the instruction processing module will be ended at the same time. Here is the working flow chart of algorithm in Fig. 4.

C. *Cracking the Wifi Passwords by Remote Forensic Terminal*

This forensics system is installed with Aircrack-ng and Reaver. Aircrack-ng is a professional software to check the safety of the wireless networks, and it can scan the details of WiFi networks, crack WPS codes and the passwords encrypted by WPA/WPA2-PSK. Reaver is a special software to crack the wireless passwords encrypted by WPS.

Almost the whole WiFi networks constructed by household routers are encrypted by WPA2, and many of them are encrypted by WPS at the same time. For the WiFi networks encrypted by WPA/WPA2-PSK, the forensics system can realize the real-time capture of the handshake packets in the coverage area of the wireless router when the suspects connect the WiFi network. The forensic terminal calls the program to return the handshake packets to the detective control terminal and crack them. The success of cracking the handshake packets is due to the performance of the detectives' computers and the size of the password dictionary package. If the suspects' WiFi is also encrypted by WPS at the same time, the detectives can use Reaver to brute force PIN codes and crack the suspects' WiFi passwords in a short time. But there are some new versions of wireless routers that can avoid brute forcing PIN codes, which influences the success rate. The detectives will combine the early methods of investigation and the above two methods to crack the WiFi passwords efficiently.

D. *Use Oray Internet/Intranet Dynamic Mapping Service to Control the Forensic Terminal*

When the forensic terminal is connected with the WiFi networks of the suspects, in order to control the forensic terminal conveniently and efficiently, the detectives can control the Raspberry Pi forensic terminal in the suspects' WiFi network online by using Oray Internet/Intranet Dynamic.

There is Oray Service client in the Raspberry Pi system, the detectives execute these commands in the console "./oraynewph start", if it prompts "Oraynewph start success", and it means the Oray Service runs successfully. When the forensic terminal works under the WiFi network of the suspects, it will run the commands of "ifconfig" in the console and get the intranet IP address of the wireless adapter. The detectives will log on b.oray.com according to the SN code of Raspberry Pi Oray Service in the control terminal, and they configure the IP address and ports.

By the above steps, the investigators can be connected with Raspberry Pi forensic terminal by entering the domain address of Oray Service in SSH or VNC, and realize the direct remote control of the forensic terminal in the suspects' WiFi network instead of controlling Raspberry Pi by using XBee module remotely, and it would not be limited to the communication distance of XBee module. So the forensic terminal can work as springboard to intrude the suspects' intranet further to get more evidence that the detectives need.

E. *Capture and Pass Back the Suspects' Wifi Network Data Packets*

After the forensics system cracked the wireless passwords, it will capture the data packets in the suspects' WiFi networks by using Aircrack-ng, then it decrypts the

data packets by using Wirshark. By analysing the wireless data packets or man-in-the-middle attack, it can get the sensitive data, such as the forums and mailbox account details, server account passwords and mail attachments [5,10]. Here are the specific steps to capture data packets.

The detectives will send the capturing traffic data commands to the Raspberry Pi forensic terminal by the using control terminal, and keep the data packets in the Raspberry Pi forensic terminal. The detectives use Oray Service to connect with the Raspberry Pi forensic terminal, and pass back the wireless data packets in the suspects' WiFi networks.

When the detectives decrypt the wireless data packets, they must import the wireless data packets with handshake packets to Wireshark, and find Edit->Preferences->IEEE 802.11 in turns, click "Edit…" and edit the WiFi SSID and passwords of the suspects. After decrypting the wireless data packets, other data packets without handshake packets can all be decrypted directly. If it cannot capture the wireless data packets with handshake packets, it cannot decrypt all data packets. The detectives can use "Aireplay-ng" in Aircrack-ng to make the suspects connect the WiFi network again and capture the handshake packets. The theory of forensics system is shown in Fig. 5.

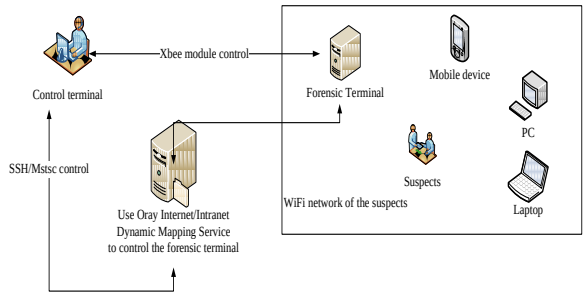

Figure 5. The theory of forensics system.

F. *Program of Deleting the Key Codes*

There is a hazard elements sensing circuit in this system, which puts the whole hardware to a box without light. Raspberry Pi work as serial control device to connect with the photosensitive sensor. Raspberry Pi handles the data collected by the photosensitive sensor every 3 minutes. When it senses the light exceeds the threshold, it means that the Raspberry Pi forensic terminal is being destroyed. The forensic terminal has the protection of the username and passwords. But to reach the secrecy requirement of the forensic contents and technology. It should delete the relevant documents completely and avoid the situation that it is restored. The program uses the Shred command to delete the key documents, such as forensic contents and controlling terminal. Shred command will cover the nodes and data blocks that contain the original documents by using random data five times. Finally the forensic terminal will pass the self-destruction event back to the control terminal by XBee module. Here is the algorithm of deleting the key codes in Fig. 6.

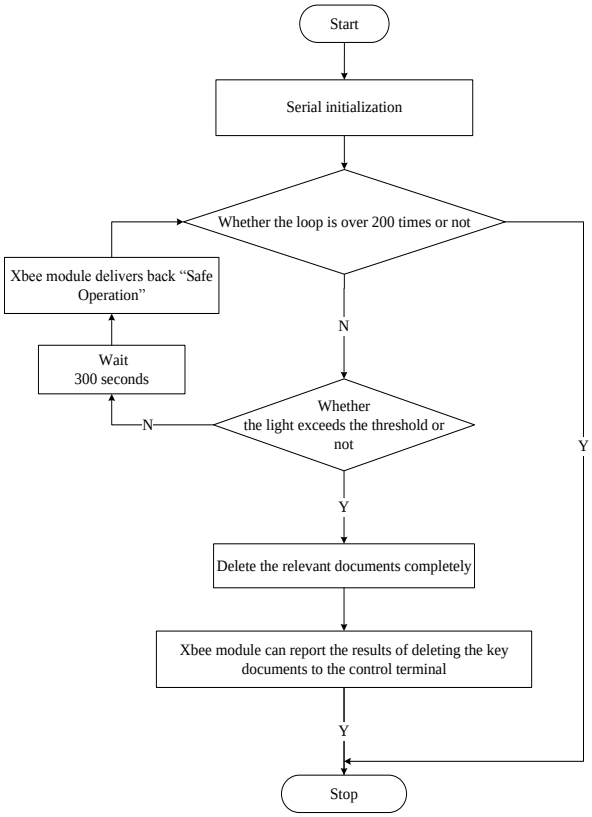

Figure 6. The flow chart of deleting the key codes algorithm.

IV. USABILITY TESTING

It will simulate the reality of operations when it is tested. The suspect's wireless routers is in the interior of a building, the forensics system is put within the scope of coverage of the suspect's WiFi networks,there are some barriers such as buildings or trees between the detectives and the forensic terminal. By testing the RSSI(Received Signal Strength Indicator) of XBee module in different distances and the changes of packet loss rate, the detectives can judge the efficient distance of the remote control. The line chart of the specific test data is shown in Fig. 7.

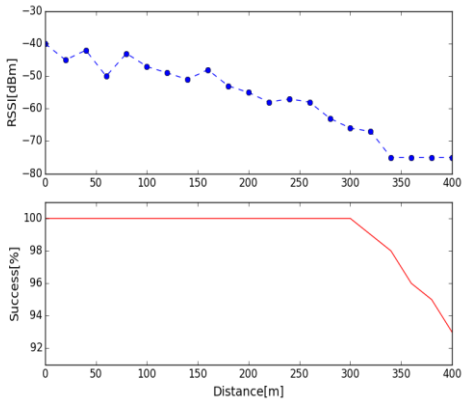

Figure 7. RSSI and packet loss rate changes over distance.

After the actual test, XBee-Pro HP900 module can control the forensics system efficiently and realize the evidence collection in the range of 300 meters surround the building.

The power test uses TECMAN power monitor, whose model is TM6 micropower precision model, it is specialized in monitoring the micro power under 1A. The data of power consumption is listed in Table 1.

TABLE I. The Power Consumption Data Of Forensic Terminal

Number	Power [W]	Current [mA]	Power factor	Devices
1	1.70	17	0.443	Raspberry Pi+XBee module
2	1.74	17	0.445	Raspberry Pi+XBee module+Photosensitive sensor
3	2.60	23	0.486	Raspberry Pi+XBee module+Photosensitive sensor +EP-N8508 cards(Disconnect state)+Tenda W311M cards(Monitor mode)
4	3.15	26	0.526	Raspberry Pi+XBee module+Photosensitive sensor +EP-N8508 cards(Disconnect state)+Tenda W311M cards(Capture handshake packets)
5	3.24	27	0.535	Raspberry Pi+XBee module+Photosensitive sensor +EP-N8508 cards(Disconnect state)+Tenda W311M cards(Capture data packets)
6	2.21	22	0.483	Raspberry Pi+XBee module+Photosensitive sensor +EP-N8508 cards(Connect to suspect's WiFi network)+Tenda W311M cards（Disconnect state)

According to the table, a normal 10400mAh power bank can keep the system working for more than 10 days theoretically. In the practical forensic work, it will be equipped with the power bank that can store more power in order to ensure it can keep working in the suspect's WiFi network.

V. SUMMARY

In recent years, network forensics is the hotspot in the research on the forensic technology. But the network traffic is evanescent and modifiable which can be dumped. The detectives will take great risks to get the evidence. This paper presents the remote WiFi investigation of network and forensics system for police based on Raspberry Pi. It has functions of XBee remote control, cracking the WiFi passwords and getting the inside data packets of the suspects' WiFi networks under remote control. It can also work as springboard to intrude the other smart devices of the suspects. The contents of the evidence are so comprehensive that it can ensure the detectives' safety efficiently. This system is used in investigating the telecom fraud gangs, financial fraud groups, pyramid schemes and espionage remotely, then get the criminal evidence or transfer records of the suspects and record their individual behaviors and habits in order to offer strong supports to the arrest.

ACKNOWLEDGEMENTS

This work is supported by National Natural Science Foundation of P. R. China under Grant Nos. 61272094, 61472232, 61373149, 61572299, 61402269, 61402270, Shandong Provincial Natural Science Foundation of China under Grant No. ZR2014FQ009 and Shandong Normal University 2015 Practice and Exploration of the Undergraduate Innovation and Entrepreneurship Training Program under Grant No. 201510445184.

REFERENCES

[1] D. Lu, G. Zhang, X. Zheng, H. Liu, B. Hu, Secure connectivity analysis of mobile Ad Hoc social networks, SCIENTIA SINICA Informationis, 2015, 45(1):97-110.

[2] C. Zhang, Y. Song, Y. Fang, et al. On the price of security in large-scale wireless ad hoc networks. IEEE/ACM Trans Network, 2011, 19: 319–331.

[3] P. Li, C. Zhang, Y. Fang. Asymptotic connectivity in wireless ad hoc networks using directional antennas. IEEE/ACM Trans Network, 2009, 17: 1106–1110.

[4] Yavuz, J. Zhao, O. Yagan, et al. On secure and reliable communications in wireless sensor networks: towards k-connectivity under a random pairwise key predistribution scheme. In: Proceedings of the IEEE International Symposium on Information Theory, Piscataway, 2014. 2371–2375.

[5] Z. Yang, Advanced Wireless Network Offensive & Defensive Techniques, Publishing house of electronics industry, Beijing, 2011.

[6] The forensics system based on assev wireless network producted by AnXinWei Technology Co. , Ltd. in 2012 on http://www.god-eyes.cn/product.asp?sid=85&bid=61

[7] Oray Internet/Intranet Dynamic Mapping Service on http://hsk.oray.com/

[8] Girling, Rasperry Pi Manual, Posts & telecom press, Beijing, 2014.

[9] ARPI600-Waveshare Wiki on http://www.waveshare.net/wiki/ARPI600

[10] W. Zhang, Research and Implementation of WLAN Sniffer System, Northwestern Polytechnical University. (2007)