Advances in Engineering Research, volume 141
5th International Conference on Mechatronics, Materials, Chemistry and Computer Engineering (ICMMCCE 2017)

Research on Wi-Fi Probe Technology Based on ESP8266

Xiaodong Zhou[1, a]

School of Electrical and Electronic Engineering North China Electric Power University, Beijing, China, 102206

E-mail: zhou_xd2015@163.com

Keywords: Wi-Fi, Probe, ESP8266

Abstract. Wi-Fi probe is a kind of wireless terminal detection technique. It captures transmitted packets in the air to gain numerous information, which is potential in commercial value and social value. A solution of Wi-Fi probe with low cost based on ESP8266 chip and a system of probe data gathering is proposed in this article. Finally, two types of application are mentioned to show that Wi-Fi probe has a positive effect on commercial and social development in the big data era.

Introduction

In recent years, smartphones have become more and more popular in people's daily life. In 2016, the shipment of China's smartphones accounted for 95.7% of China's mobile phone shipment in the same period. Also, as the most convenient and commonest way for information acquisition in the world, the network service has permeated into everyone's life. With development of mobile devices such as smartphones, people's life and production have taken on a more flexible way. Wi-Fi is a reliable bridge for people to get access to the network communication with higher speed but lower cost. Mobile phone manufacturers have equipped all their smartphones with it and thus, Wi-Fi has been widely promoted.

Wi-Fi probe technique is a kind of technology that is used to monitor surrounding wireless terminals turning up with popularization of Wi-Fi. It utilizes the interaction handshake protocol between wireless terminals and wireless access points of 802.11 protocol, monitors handshake packet in the air and analyzes its contents to detect wireless devices around the probe. As smartphones with Wi-Fi function are widely used, by analyzing these equipment, the technique can be applied to many aspects such as detection of passenger flow, precise marketing and public security, and besides, it can be one of reliable data sources in the big data era.

Wi-Fi Probe Principles

Wi-Fi Connecting Process. IEEE 802.11 is a universal WLAN standard being widely used at present. It's permitted by the Institute of Electrical and Electronics Engineers. The norm defines MAC layer and PHY layer, and divides all passing through transmitted data into three types:

Table 1. Transmitted data types defined by IEEE

Type Description	Type Value	Usage
Data	10	Carry data for higher layer
Control	01	Control access to physical media
Management	00	Manage and maintain wireless connection

Thereinto, management-type data packet establishes and maintains the entire Wi-Fi connection between Access Point (AP) and Wireless Station (STA). While setting up connection, the following subtypes complete interaction through this type of data packet:

(1) Beacon: AP broadcast this packet outwards on a regular basis for STAs to search.

(2) Probe request: STA broadcast this packet on each channel when launching inquiry request to APs.

(3) Probe response: APs return the response packet carrying its information after STA probe request received.

(4) Authentication: Using to establish some kind of encrypting mechanism.

(5) Associate request: STA sends this request to AP to establish the connection.

(6) Associate response: AP responds to STA to complete the connection after receiving associate request from STA.

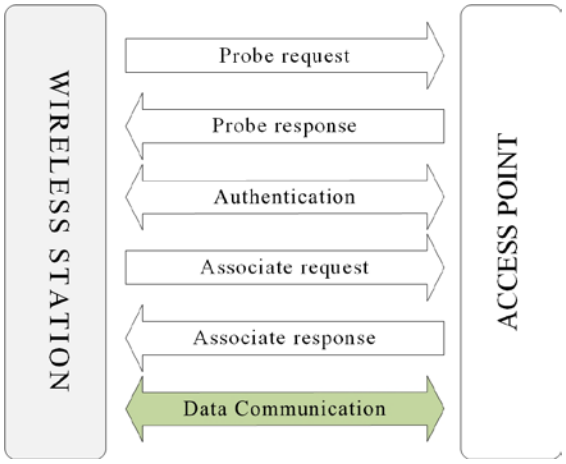

Fig. 1. Wi-Fi connection setup process

Principles of Wi-Fi Probe. Wi-Fi station usually adopts two approaches while scanning access points:

(1) Passive scanning:

STA passively monitors beacon frames which are regularly sent by APs so as to gain information of access points

(2) Active scanning:

STA proactively sends probe request frames on each channels; AP returns probe response that contains its information to STA after receiving the packet.

When the station scans access points only in the first method, the device is completely anonymous because there's no outward data transmission. However, the default beacon sending interval of access points is quite long (about 100μs by default). If all channels are needed to be scanned, suppose 13 channels, it takes about 2.5 seconds to complete the search, which is unfavorable to reducing power consumption of the device. Hence at present, STA usually utilizes passive and active scanning at the same time.

As Wi-Fi signal is transmitted in the open air, suppose that MAC address of each device is unique in the world, we can use sniffers to capture probe frames (request and response) sent by devices nearby, and parse the MAC address of communication parties, or even calculate devices' position using RSSI, thus realizing the Wi-Fi probe function.

Building Wi-Fi Probe Experimental Environment with ESP8266

This experimental environment selects ESP8266 Wi-Fi chips of Espressif Company. The design is a set of highly integrated SoC solutions which are characterized by low cost, low power consumption, small volume and high stability. It's applicable to layout with intensive end products so as to make up for shortcomings of a single module in coverage ability. ESP8266 integrates a 32-bit ARM processor on the inside and secondary development can be conducted through SDK. The designed experimental environment is built as shown in Fig.2 and Fig.3.

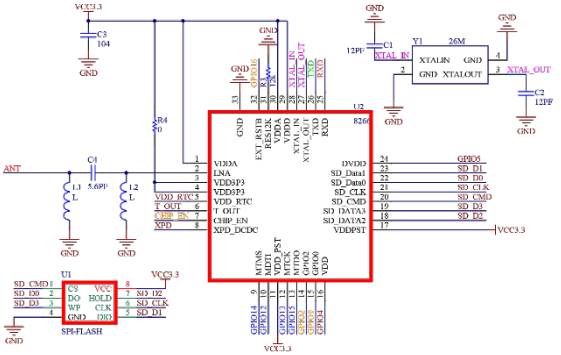

Fig. 2. Schematic diagram of ESP8266 probe

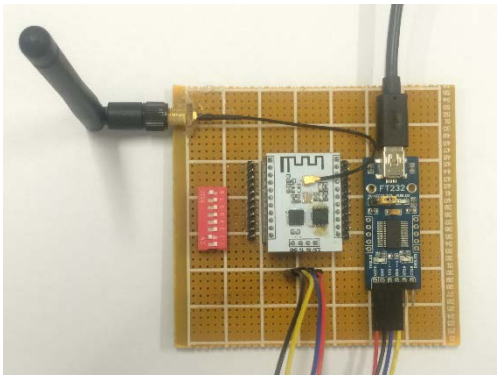

Fig. 3. Experiment environment

In the experiment, the sniffer API in SDK is used. After the SoC is electrified and initialized, the "wifi_promiscuous_enable" function is called to place the wireless network adapter in a promiscuous mode. Under this mode, ESP8266Ex can capture all data packets that are transmitting in the air. Parameters such as MAC address and RSSI of the communication parties are extracted from the packets captured, as shown in Fig.4. This module transmits the data to the server and so that analysts can easily manage them.

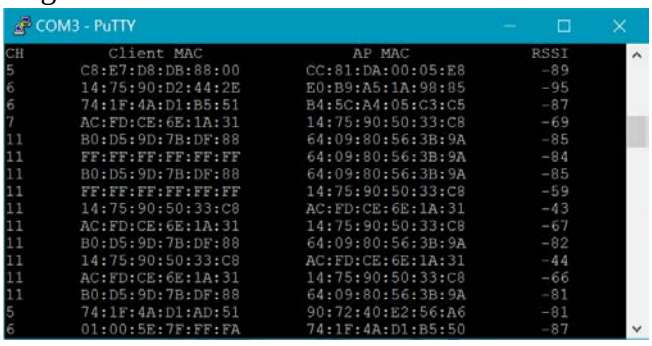

Fig. 4 Wi-Fi probe capture list

The solution adopts the approach of probe frame capture. Even if users are not connected with any wireless network, as long as the wireless module is enabled, the device is sending probe frames on a regular basis to inquire available access. Therefore, the technology expands the searching scope of devices. In the sniffing process, ESP8266 can only capture packet header that did not contain any other personal information, the communication between STAs and APs is still secured and safe.

In practical application, the monitoring scope of a single module is limited. For large-scale public areas such as supermarkets, usually multiple modules are needed to build a network for a full coverage. Ad hoc network solution is employed in this paper. When the passenger flow increases dramatically, data flow in the sensor network will be accordingly amplified. Besides, multiple hop

transmission is needed as the coverage area is enlarged. The traffic rate of 250kbps of ZigBee appears to be in a stretched circumstance. The ad hoc solution supports multiple hop transmission which is much faster and more reliable than the transmission speed of ZigBee. In addition, the ad hoc solution can be realized through ESP8266, and the cost is superior to the ZigBee solution as well.

In terms of data collection, we divide the area into lots of small regions. All sensors in the region are connected to one host computer of the region. Sensors directly send updates to the host at a fixed interval after collecting data. The host will summarize all data and transfer them to the cloud server. And at the end of the link, the cloud server provides a uniform data interface for secondary use.

Application of Wi-Fi Probe

Passenger Flow Statistics. Wi-Fi probe technology can be used to detect passenger flow in public areas. Comparing with those traditional method of passenger flow statistics, it has following advantages:

(1) Visual count by human: The method has greater error, less efficiency. The data is hard to synchronize in real time.

(2) Counting by gate: This counting is accurate and with lower cost, but contains less information except numbers.

(3) Counting by camera: Using facial recognition, higher accuracy but with higher operational and maintenance cost.

(4) Using Wi-Fi probe: Detect wireless terminals around the probes. Although this counting method have lower accuracy (some people will not enable the Wi-Fi switch in their phones, the situation will be improved as the number of smartphones usage is growing), it has advantages as extremely low cost, much information with higher value in it. More importantly, the data can be synchronize in real time.

Precise Marketing. With the advent of Wi-Fi probes, the technique will have a great impact on the offline business. Information will gradually become the most significant component for commercial decision making, of which is originally by experience. Consider that the Wi-Fi probe can identify the customer by detecting his / hers smartphones' MAC address. As the customer is strolling in the supermarket, the supermarket system using Wi-Fi probe notices someone has stayed at the fruit market for a long time, so the supermarket decide to push fruit sales information to his smartphone in the next few days. The Wi-Fi probe makes business targeted.

Conclusions

As the most reliable and convenient way of networking, Wi-Fi is used extensively. By using Wi-Fi probe technology, we can establish strong correspondence between information and individuals. The ESP8266 Wi-Fi probe solution giving by this article has low cost and power consumption , and it has operated for more than ten days before this article finally submitted. So it is a fine solution for Wi-Fi probe that can be used in passenger flow statistic area.

References

[1] Dickson. Will "Probe" be a rigid demand for a wireless city?[EB/OL]. http://mt.sohu.com/20170216/n480886820.shtml, 2017-02-16/2017-05-29.

[2] "IEEE Standard for Information technology - Telecommunications and information exchange between systems Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007), pp. 1–2793, March 2012.

[3] CHEN Jiangang, CHEN Wei, CAI Hongxin, TAN Guolong, LIN Jiaqun. Using open source router to achieve multi - functional intelligent monitoring alarm system[J]. Computer Knowledge and Technology,2016,(26):221-223.