Fingerprint Extraction Based On Frame Interval For Wireless Network Devices

Zhibin Yu, Shuangqiu Li and Ruilun Zong

October 16, 2019

Fingerprint Extraction Based On Frame Interval For Wireless Network Devices

Zhibin YU
Southwest Jiaotong University
Chengdu,Sichuan
China
+86-18224075056
zbyu@swjtu.edu.cn

Shuangqiu LI
Southwest Jiaotong University
Chengdu,Sichuan
China
+86-17361061979
lsq19950222@163.com

Ruilun ZONG
Southwest Jiaotong University
Chengdu,Sichuan
China
+86-17358653392
zongruilun@foxmail.com

ABSTRACT

Traditional communication encryption methods can effectively protect our communication security in some extent, but in practical use, the vulnerabilities of the traditional methods can be cracked , thus results in information leakages. So it is necessary to deeply research the individual characteristics of wireless network devices. This paper proposes a method which takes frame interval as a fingerprint feature to represent different wireless devices. The experimental results show that the proposed method is effective for the identification of IEEE802.11 wireless network devices, and the average recognition rate reaches 95%.

CCS Concepts

Networks → Network protocols → Link-layer protocols

Networks → Network components → End nodes → Network adapters

Computing methodologies → Machine learning

Keywords

IEEE802.11; CSMA/CA; Frame Interval;

1. INTRODUCTION

Wireless networks are becoming increasingly widespread in both public and individual environment. The wireless device recognition is a hot issue. Spectrum [1], signal envelope [2], and other modulation features [3] from the transient part and the steady-state part of the wireless signals are extracted to distinguish different wireless network devices.

The traditional methods above have been well validated, but it can be not widely applied due to the requirements of experimental facilities. In recent years, researchers have found new ways to achieve the purpose of identifying wireless network devices, they focus on wireless protocols. In 2006, B. Sieka [4] proposes a method for IEEE802.11 device fingerprinting. The researchers extract the frame interval between AUTH frame and ACK frame during authentication procedure. Five devices are tested in the experiment, four of the devices are the same model of the same brand and one device comes from different brand. In 2012, C. Neumann [5] proposes a method using IAT(Inter-Arrive-Time) and TT(Transmission Time) as features to distinguish different IEEE802.11 devices. In 2017, J. Liang [6] proposes the method that using probability density curve of IAT to distinguish different Cisco routers.

However, the collection of wireless frames of AUTH and ACK in [4] is very time-consuming, it needs to connect to the wireless network and then disconnect the wireless network continuously, which is relatively inefficient. The work in [5] relies on high precision experimental equipment, in addition, it has extremely strict requirements for the experimental environment, which has to avoid external electromagnetic interference. Although the probability density curves adopted in [6], its scope of application is very limited, the research object of it is a private protocol issued by Cisco company, therefore, it can not be applied in IEEE802.11 wireless network devices identification.

Based on the existed wireless transmission mechanism, in this paper, we extract different types of frame interval during data exchange via wireless packet sniffing software. It's of high efficiency and no requirements for the surrounding environment. The feasibility of the method is verified by identification experiments. Probability density curve are used to represent the signature.

The rest of the paper is organized as follows. The second part describes the working mechanism of IEEE802.11, the third part contains the calculation formulas and description of the experiments. Classification results presented in the forth part. Conclusions are found in the fifth part. Acknowledgment and references are shown in the last two parts.

2. MECHANISM

To minimize frame collisions, IEEE 802.11 standard has designed a special MAC sub-layer, which including Distributed Coordination Function (DCF) and Point Coordination Function (PCF). DCF is the most basic media access method of the IEEE802.11 MAC protocol. It mainly adopts the method of CSMA/CA to access wireless medium. Stations compete to obtain the right of utilizing wireless channel. In WLAN, not all the stations could communicate with each other directly, therefore IEEE802.11 uses the Network Allocation Vector (NAV) to indicate the remaining busy time of the medium, having passed the time, stations can compete again to obtain the access to the channel. Each station updates its latest value of NAV with the Duration field of the frame transmitted over the medium.

2.1. RTS/CTS handshake mechanism

RTS/CTS is the protocol that mainly used to solve the hidden terminal problem, it defines the response interval of subsequent frames. As the following figure shows, station A emits an RTS frame, the Duration filed of it has already calculated all the time that required for the whole transmission process. Station B receives the RTS frame, waiting for SIFS time, and then responds with CTS frame. Other stations use the Duration filed of the CTS frame to update their NAV values. Having received the CTS frame, station A then sends DATA frame after waiting for SIFS time. Station B waiting for another SIFS time to respond with

ACK frame .The transmission process ends till station A received ACK frame.

In IEEE802.11 wireless protocols, SIFS is a fixed value, which implies the minimum interframe space. As a consequence, stations using SIFS have the highest priority to access the wireless medium. In different standards, SIFS has different value. The relationship of DIFS, SIFS, and Slot can be formulated as follows, the specific value are displayed in table 1.

In IEEE802.11 wireless protocols, SIFS is a fixed value, which implies the minimum interframe space. As a consequence, stations using SIFS have the highest priority to access the wireless medium. In different standards, SIFS has different value. The relationship of DIFS, SIFS, and Slot can be formulated as follows, the specific value are displayed in table 1.

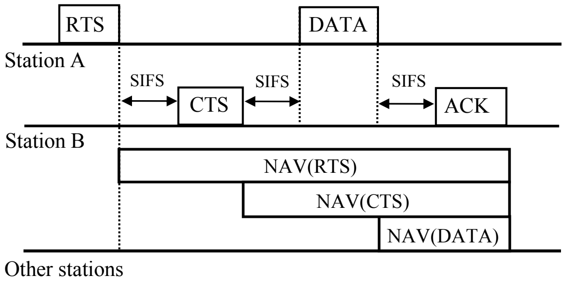

Fig.1. RTS/CTS mechanism

$$DIFS = SIFS + 2Slot \tag{1}$$

Table 1. Basic Interframe Space

Standard	SIFS (μs)	Slot (μs)	DIFS (μs)
IEEE802.11n	10	9 or 20	28 or 50
IEEE802.11b	10	20	50
IEEE802.11g	10	9 or 20	28 or 50

2.2. Random backoff mechanism

When a station is to emit frames, it must sense whether the wireless medium is idle:

1) If the station detects that the medium is idle and the time reached DCF Interframe Space (DIFS), it is then start to backoff. In the backoff phase, when there is no other stations to compete with, the station will occupy the wireless channel once the station ends up the backoff procedure, otherwise the station has to compete with other stations. The one which has less backoff time will utilize the wireless channel.

2) If the station detects that the medium is busy, it has to postpone transmitting frames until it meets one of the following condition:

a) The last frame of the transmission over the current channel received correctly, and the idle time of the current channel reaches to DIFS.

b) The last frame of the transmission over the current channel received incorrectly, and the idle time reached to EIFS. EIFS is another kind of interframe space, its value equals to the DIFS plus SIFS and the transmission time of ACK frame with the lowest rate.

The backoff time is determined by the backoff counter.The backoff counter is a decreasing counter, the value of the it ranges from 0 to CW, CW means contention window, it is a integer which randomly choose from CWmin to CWmax, the initial specific value is related to the physical layer. Once collision occurs, the value of CW changes. In the beginning, CW value is CWmin. The relation between CW and CWmin is shown in the formula below, n represents the collision times. The stations which participated in the competition but can not occupy the channel remains in the backoff status until the next backoff occurs. When subsequent backoff occurs, stations compete again, and the remaining backoff time of last defer will be used as the newly backoff time.

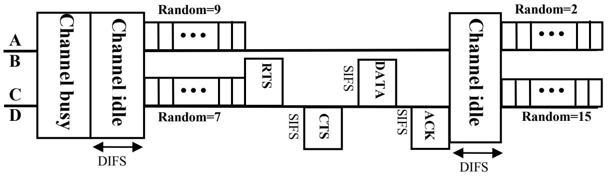

Fig.2. When there has other stations to compete the channel

$$CW = 2^{n} CW_{min} - 1 \tag{2}$$

As the figure 2 shows, station A and station C switch to backoff at the same time. To station A, the value of the backoff counter of is 9, as for station C, the value is 7. The value of station A turn to 2 when value in station C decreased to 0. Then station C occupies the channel. During the occupation, station A keeps silent, its backoff counter stops working. In the consequence backoff , station C has to choose a new integer to compete according to the formula (2).

3. MATHODOLOGY AND EXPERIMENT

This section explains how we extract the features considered in the previous sections.

3.1. Frame interval

3.1.1. The interval between RTS and its previous frame

T0 is used to represent the interval between RTS and its previous frame, and the formation of T0 is given by

$$T0 = DIFS + T_{backoff} + T_{RTS} \qquad (3)$$

3.1.2. The interval between RTS and CTS

The interval between RTS and the corresponding CTS is defined as T1. Its formula is given by

$$T1 = SIFS + T_{CTS} \qquad (4)$$

3.2. Probability density curve

IEEE802.11 wireless frames are obtained by wireless capture tools. The values of the T0 and T1 of the tested wireless device are calculated by the formula above. Then we draw their histogram figures.

In figure 3 and figure 4, RTS frames of two different wireless devices are collected, for each device we collect once, 10000 RTS frames are sampled each time. The corresponding T0 are calculated, and histograms are plotted. We compare their distributions based on the histograms.

To ensure the stability of the features, for different device, we perform data collection multiple times in the following experiments. On this basis, the corresponding interval of T0 and T1 are calculated. The wireless devices used in the experiment are displayed in Table 2. The working mode of three wireless network devices are set to IEEE802.11n, and the channel number fixed to 13, channel bandwidth is 20MHZ.

Table 2. Wireless Devices Used in The Experiment

No.	Type	Serial Number
A	TL-WR842N	1143246077664
B	Tenda-AC9	180269710140000866
C	MW305R	1177604009999

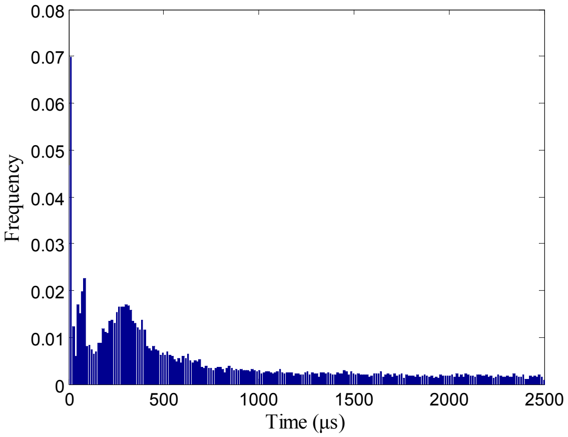

Fig 3. The histogram of interval T0 of wireless device 1

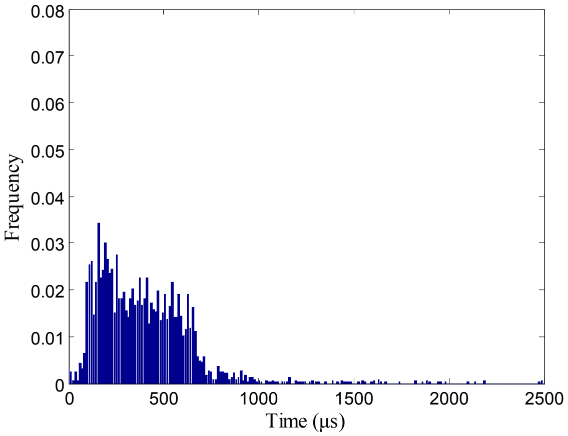

Fig 4. The histogram of interval T0 of wireless device 2

Then, we extract probability density curve from the histograms.

3.2.1. Extraction of probability density curve of interval T0

When RTS frames of the wireless devices are captured, we draw their probability density curves respectively. To drop the unqualified curves, we did some preparing works that described as follows: first, for each wireless device, mean curve are calculated, we observing the similarity between each curve and the mean curve, and drop the curves with low matching result. Then, we calculate a new mean curve from the remaining curves, observing the similarity between each curve and the mean curve, and drop the curves with low matching result. Repeat the steps above, until the matching result meet the requirements.

As the formula shown below, we use cosine similarity to indicate the related coefficient between two curves. In the formula, *br* represents the mean curve, *bc* denotes the curve tested, *n* stands for the vector length of *br*.

$$sim_{\cos}(b_c, b_r) = 1 - \frac{\sum_{j=1}^{n}(b_{c,j}b_{r,j})}{\sqrt{\sum_{j=1}^{n} b_{r,j}^{2}}\sqrt{\sum_{j=1}^{n} b_{c,j}^{2}}} \qquad (5)$$

After the processes above, the corresponding mean curves of the three wireless devices is shown in figure 6.

3.2.2. Extraction of probability density curve of interval T1

The interval T1 from three wireless devices are extracted, the corresponding curves are also drawn. As the figure 7 shows, the mean curves of the devices are exactly overlapped, which means their distributions have little difference in interval T1. According to formula (4), in the IEEE802.11 protocols, the SIFS is a fixed value of 10 μs, and the specific value of T_{CTS} is shown in Table 3.

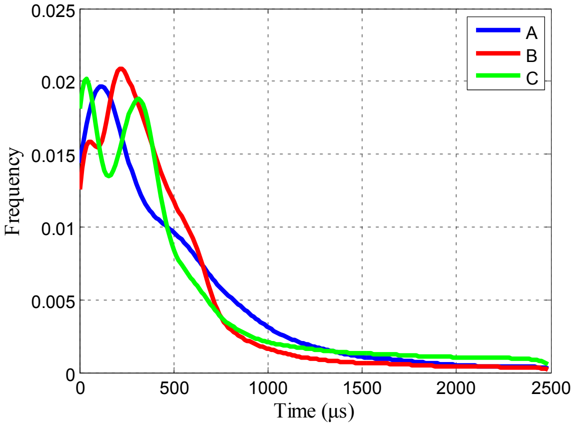

Fig. 6. The mean curve of interval T0 of three wireless devices

In Table 3, for the T_{CTS} of these devices, the values are the same, 1.3μs. That is to say, it is no distinction in T_{CTS}. This has explained why the probability density curves of interval T1 have little differences.

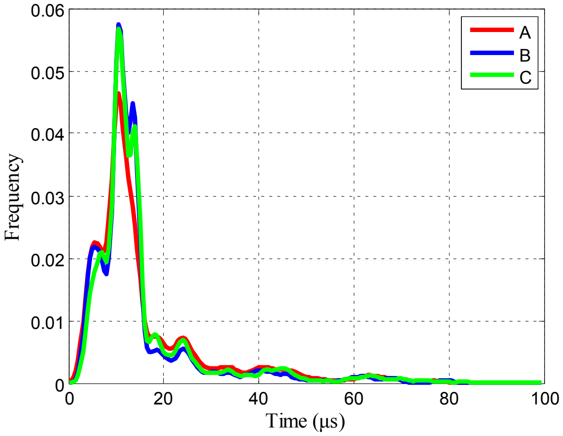

Fig. 7. The mean curve of interval T1 of 3 wireless devices

Table 3. The value of T_{CTS}

No.	T_{CTS}(μs)
A	1.3μs
B	1.3μs
C	1.3μs

4. CLASSIFICATION

After the analyses above, the following experiments abandon the parameter T1, we only concerned the interval T0. From figure 6, the probability density mean curve of the three wireless devices of interval T0 in range 200 μs ~ 1000 μs decrease monotonically, and the difference is obvious. Thus we conduct our following research of interval T0 in range 200 μs ~ 1000 μs.

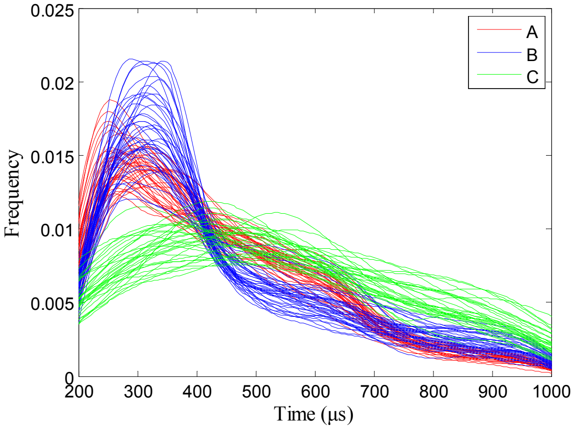

Fig.8. The curves of three wireless devices in 200-1000μs

The classification result are shown in Table 4 .

Table 4. Wireless Devices Used In The Experiment

No.	Training times	Test times	ratio

A	100	50	90%
B	100	50	95%
C	100	50	100%

5. CONCLUSION

Wireless network devices recognition is closely related to information security. Similar to human fingerprints, different wireless device has their own fingerprint, thus can be distinguished from each other. The fingerprints we obtained by timing analysis is influenced by physical layer characteristics, which shows hardware features. In this paper, we proposed a method using frame interval as the feature to differentiate wireless network devices. Parameter T0 and T1 are used to indicate the device fingerprint, especially T0, which is far more expressive. In the following works, we will investigate the intrinsic features based on this method and conduct experiments on more devices.

6. ACKNOWLEDGMENT

This work is supported by the Equipment Development Department Funds grant 61403120304<JZX7Y20190252032701>) and the Fundamental Research Funds for the Central Universities grant (2019XJ04).

7. REFERENCES

[1] Zhang, Y. Li and C. Wang, "*Research on Individual Identification of Wireless Devices Based on Signal's Energy Distribution*," 2018 IEEE 23rd International Conference on Digital Signal Processing (DSP), Shanghai, China, 2018, pp. 1-5.

[2] Z. Shi, M. Liu and L. Huang, "*Transient-based identification of 802.11b wireless device*," 2011 International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, 2011, pp. 1-5.

[3] Y. Ren, L. Peng, W. Bai and J. Yu, "*A Practical Study Of Channel Influence On Radio Frequency Fingerprint Feature*s," 2018 IEEE International Conference on Electronics and Communication Engineering (ICECE), Xi'an, China, 2018, pp. 1-7.

[4] B. Sieka, "*Active fingerprinting of 802.11 devices by timing analysis*," CCNC 2006. 2006 3rd IEEE Consumer Communications and Networking Conference, 2006., Las Vegas, NV, USA, 2006, pp. 15-19.

[5] C. Neumann, O. Heen and S. Onno, "*An Empirical Study of Passive 802.11 Device Fingerprinting*," 2012 32nd International Conference on Distributed Computing Systems Workshops, Macau, 2012, pp. 593-602.

[6] J. Liang, J. Han and G. Xiong, "*A passive fingerprint feature for the recognition of Cisco routers*," 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, 2017, pp. 1021-1025.