Wi-Fi Devices Individual Identification based on Envelope Front Characteristic

Dongze Lv, Junlin Chen, Yanting Che
Science and Technology on Electronic Information Control Laboratory, Chengdu, SiChuan Province, 61000, China
e-mail: cheyanting@hrbeu.edu.cn

Abstract. There are some characteristics are used for traditional Wi-Fi devices individual identification methods, such as: amplitude and phase characteristics during the period that Wi-Fi devices are turned-on or turned-off, MAC address, and IP address. In fact, on one hand, MAC address and IP address are easily to be changed. Traditional methods can‘t identify individual Wi-Fi devices if MAC address or IP address changed. On the other hand, the amplitude and phase characteristics of Wi-Fi devices can only be identified during the short period of turned-on or turned-off. The traditional methods have application limitations. Therefore, the Wi-Fi devices individual identification based on envelope front characteristic is proposed in this paper. Firstly, envelopes of Wi-Fi signals are extracted. Secondly, front characteristics of Wi-Fi envelope are extracted. Then envelope front characteristics are used to compare and match with models saved in the library to realize Wi-Fi devices individual identification. By using the method proposed in this paper, Wi-Fi devices individual identification can be realized whether MAC address or IP address changed. Scope of identification application can be effectively expanded into the whole time when Wi-Fi devices transmit signals by using this method. Since envelope front characteristics have the advantages of non-changing and non-copying, accuracy of Wi-Fi individual identification is also improved by using this method.

1. Introduction
With the development of Wi-Fi technology, wireless networks play an increasing important role in daily lives. Compare with wired transmission, the openness of Wi-Fi provides more intrusion possibilities for unauthenticated devices. Therefore, the security of Wi-Fi is particular important [1].

The traditional identification method is to use MAC address or IP address to identify Wi-Fi devices. However, the traditional method is invalid if MAC address or IP address is changed which is easily realized. Amplitude and phase characteristics are used to individual identify Wi-Fi devices when they are turned-on or turned-off. But this method has application limitation, because it only works in the very short period when Wi-Fi devices are turned-on or turned-off [2]. Fingerprint features of wireless device refer to the unintentional modulation feature attached to the signal. Fingerprint features are different with each other due to the different hardware of different devices. They are as unique as human fingerprints. And they are stable, unique and measurable [3-10].

Therefore, envelope front characteristics are used to identify Wi-Fi devices as one of fingerprint features. This method can be used for Wi-Fi access control in future. Envelope front characteristic has the advantages of non-changing and non-copying. This method is valid all the time when Wi-Fi is transmitting signals, and still valid after MAC address or IP address is changed. Compared with
traditional methods, this method can expand the scope of application, and solve the problem that can’t identify Wi-Fi devices in some cases.

2. Wi-Fi individual identification

Wi-Fi devices individual identification based on envelope front characteristic is proposed in this paper. Firstly, signal envelopes of Wi-Fi signals are extracted and separated into pulse envelopes. And the valid of pulse envelopes is judged. Secondly, pulse envelope front characteristics are extracted when pulse envelopes are valid. Compare the pulse envelope front characteristics with models in library. Finally, Wi-Fi devices individual identification results are given. Individual identification flow figure is shown as:

![Individual Identification Flow](image)

**Figure 1. Individual Identification Flow**

### 2.1 Envelope Extraction

Due to the short duration of the pulse envelope front characteristic of Wi-Fi signal, a higher sampling rate $f_s$ is necessary in order to ensure sufficient sample points. The real and imaginary parts of Wi-Fi signal after complex sampled are shown as:

$$
\text{Re}[s(n)] = \text{real}[s(n)] \\
\text{Im}[s(n)] = \text{imag}[s(n)]
$$

Where, $s(n)$ represents the Wi-Fi signal. $n = 1, 2, 3, \ldots$ represents the sampled number.

According to the real and imaginary parts of signal, the signal envelope of Wi-Fi signal is shown as:

$$
\text{Envelope}(n) = \sqrt{\text{Re}[s(n)]^2 + \text{Im}[s(n)]^2}
$$

Normalize the Wi-Fi signal envelope. The normalized signal envelope is shown as:

$$
\text{Envelope}_{\text{norm}}(n) = \frac{\text{Envelope}(n)}{\max(\text{Envelope}(n))}
$$

Set the starting threshold $Th_L$ for the normalized signal envelope. The signal envelope is separated into each pulse envelope by using starting threshold. The sampling point $n_1$ can be regarded as the starting point of the pulse envelope front characteristic when signal envelope satisfies the following conditions:

$$
\begin{cases}
\text{Envelope}_{\text{norm}}(n_1 - 1) < Th_L \\
\text{Envelope}_{\text{norm}}(n_1) \geq Th_L
\end{cases}
$$

The sampling point $n_2$ can be regarded as the ending point of the pulse envelope front characteristic when signal envelope satisfies the following conditions:
A pulse envelope of Wi-Fi signal is separated from the sampling points between \( n_t \leq n \leq n_2 \) of normalized signal envelope \( \text{Envelope}_{\text{norm}} \).

\[
(6) \quad \begin{cases}
\text{Envelope}_{\text{norm}}(n_2) \geq \text{Th}_l \\
\text{Envelope}_{\text{norm}}(n_2 + 1) < \text{Th}_l
\end{cases}
\]

Repeat the envelope separation process for saved Wi-Fi signal until the entire signal envelope is completely separated into each pulse envelope:

\[
(7) \quad \{\text{Envelope}_{\text{pulse}_1}, \ldots, \text{Envelope}_{\text{pulse}_N}\}
\]

Where, \( N \) represents the total number of pulse envelopes.

Set the pulse duration threshold as \( \text{Th}_{\text{dur}} \). Compare the duration of each pulse envelope with the pulse duration threshold. If the duration of the pulse envelope is less than the pulse duration threshold, the pulse envelope is determined to be invalid and discarded. Otherwise, the envelope is determined to be valid and saved. The total number of valid pulse envelopes is \( N \).

### 2.2 Envelope Front Characteristics Extraction

Extract pulse envelope front characteristics from valid pulse envelopes. Set the envelope front characteristic ending threshold as \( \text{Th}_{\text{f}} \). Set \( n_3 \) as the ending sampling point of pulse envelope front characteristic, when the following conditions are met:

\[
(9) \quad \begin{cases}
\text{Envelope}_{\text{pulse}}(n_3) < \text{Th}_{\text{f}} \\
\text{Envelope}_{\text{pulse}}(n_3 + 1) \geq \text{Th}_{\text{f}}
\end{cases}
\]

Set the starting point of pulse envelope as the starting point of pulse envelope front characteristic. The pulse envelope front characteristics are shown as:

\[
(10) \quad \text{Rising}_\text{edge}_i = \text{Envelope}_{\text{pulse}}(1:n_3)
\]

According to the above method, extract pulse envelope front characteristics from all the pulse envelopes, are shown as:

\[
(11) \quad \{\text{Rising}_\text{edge}_1, \ldots, \text{Rising}_\text{edge}_N\}
\]

Pulse envelope front characteristic models in library are shown as:

\[
(12) \quad \{\text{Model}_1, \ldots, \text{Model}_M\}
\]

Where, \( M \) represents the total number of pulse envelope front characteristic models in library.

The difference square between all the pulse envelope front characteristics of Wi-Fi signals and models from library is shown as:

\[
(13) \quad \sigma^2 = \text{mean} \left[ (\text{Rising}_\text{edge}_i - \text{Model}_j)^2 \right]
\]

where, \( i = 1,2,\ldots, N \), \( j = 1,2,\ldots, M \).

Set the difference square threshold to \( \text{Th}_{\text{var}} \). The pulse envelope front characteristic is considered to match the \( \text{Model}_j \), if the following condition is met:

\[
(14) \quad \sigma^2 < \text{Th}_{\text{var}}
\]
According to the above condition, the number of pulse envelope front characteristics which matching models in library can be calculated, which are $N_{\text{mod,ef1}}$, $N_{\text{mod,ef2}}$, ..., $N_{\text{mod,efM}}$.

2.3 Individual Identification

Define the similarity of $N$ pulse envelope front characteristics of Wi-Fi signals to each model in library as:

$$N_{\text{mod,ef1}} / N, \ldots, N_{\text{mod,efM}} / N$$ (15)

Set the similarity threshold to $Th_{\text{sum}}$.

$$\left( N_{\text{mod,ef}} / N \right) \geq Th_{\text{sum}}$$ (16)

The Wi-Fi signal is considered to match Model$^j$ in library, if above condition is met. Otherwise, the Wi-Fi signal does not match Model$^j$.

The model with greatest similarity is selected if the Wi-Fi signal matches multiple models in library. And the individual identification result is: the Wi-Fi device is identified as the device saved by model selected. If the Wi-Fi signal matches only one model in library, the individual identification result is: the Wi-Fi device is identified as the device saved by the matched model. If the Wi-Fi signal does not match any models in library, the individual identification result is: the Wi-Fi device is considered as an unknown device.

3. Simulation

Wi-Fi devices individual identification method proposed in this paper is simulated and verified by using Matlab. Receive signals from 8 Wi-Fi devices. Select 2 of 8 Wi-Fi devices, extract both pulse envelope front characteristics and store the characteristics into library. Then, change MAC address and IP address of 8 Wi-Fi devices. Individual identify all the Wi-Fi devices by using the method proposed in this paper. The simulation parameters are shown as: sampling rate is $f_s = 250\text{MHz}$, the normalized signal envelope starting threshold is $Th_L = 0.1$, pulse duration threshold is $Th_{\text{len}} = 150\text{ns}$, the pulse envelope front characteristic ending threshold is $Th_{\text{H}} = 0.8$, the difference square threshold is $Th_{\text{var}} = 0.01$, the similarity threshold is $Th_{\text{sum}} = 0.9$.

All the Wi-Fi signals are complex sampled by using sample rate $f_s = 250\text{MHz}$. Signal envelopes are extracted and normalized, shown as:

![Figure 2. Envelopes of 8 Wi-Fi devices](image)

Extract pulse envelopes of all the Wi-Fi signals according to $Th_L = 0.1, Th_{\text{len}} = 150\text{ns}, Th_{\text{H}} = 0.8$. Then extract all the pulse envelope front characteristics according to $Th_{\text{H}} = 0.8$. Pulse envelope front
The characteristics of all Wi-Fi signals are shown as:

As shown in the above figure, each pulse envelope front characteristics of different Wi-Fi devices is different. The pulse envelope front characteristic is unique, and can’t be copied or changed. Save the pulse envelope front characteristics of Wi-Fi devices No.1 and No.2 as models into library.

Calculate the difference square between all the Wi-Fi pulse envelope front characteristics and all the models in library. Results are shown as following table:

**Table 1. Difference square between 8 Wi-Fi devices and 2 models**

| Wi-Fi Devices | N0.1 | N0.2 | N0.3 | N0.4 | N0.5 | N0.6 | N0.7 | N0.8 |
|---------------|------|------|------|------|------|------|------|------|
| Model N0.1    | 0    | 0.1167 | 0.0992 | 0.1119 | 0.077 | 0.077 | 0.1301 | 0.1254 |
| Model N0.2    | 0.1167 | 0 | 0.0906 | 0.0953 | 0.1275 | 0.1251 | 0.089 | 0.1 |

Individual identify all the Wi-Fi devices by using $T_{\text{var}} = 0.01$ and $T_{\text{sum}} = 0.9$. The result is: Wi-Fi device No.1 is identified as model1 in library and Wi-Fi device No.2 is identified as model2 in library. The Wi-Fi individual identification result is correct by using the method proposed in this paper.

Perform 100 Monte-Carlo tests under the simulation conditions. Save pulse envelope front characteristics of 8 Wi-Fi devices as models in library. Respectively perform individual identification for each Wi-Fi device by using the method. The identification accuracy rate is shown as:

**Table 2. Wi-Fi devices individual identification accuracy rate**

| Wi-Fi Devices | N0.1 | N0.2 | N0.3 | N0.4 | N0.5 | N0.6 | N0.7 | N0.8 |
|---------------|------|------|------|------|------|------|------|------|
| Identification accuracy rate | 0.985 | 0.976 | 0.981 | 0.97 | 0.981 | 0.982 | 0.971 | 0.986 |

In summary, the method proposed in this paper can effectively identify individual Wi-Fi devices. The Wi-Fi device can be correctly identified by using this method even after MAC address and IP address are changed.
4. Conclusion
A method of Wi-Fi devices individual identification based on envelope front characteristic is proposed in this paper. The individual Wi-Fi device can be correctly identified by this method even after MAC address and IP address are changed. Simulation results show the effectiveness of the method. Compared with traditional Wi-Fi devices individual identification methods, on one hand the method is effective regardless of whether MAC address and IP address are changed. On the other hand, the method is not limited to the short period of Wi-Fi devices power-on and power-off. The method is effective during the whole working time of Wi-Fi devices. The adaptation range of Wi-Fi devices individual identification is improved by using this method. And it can provide support for Wi-Fi devices access control in future.

References
[1] Huang, S.C., Zhu, X.L. (2018) A communication individual recognition method based on radio frequency fingerprint. J. Aerospace Electronic Warfare, 1: 31-34.
[2] Yuan, H.L., Hu, A.Q. (2010) Preamble-based detection of Wi-Fi Transmitter RF fingerprints. J. Electronics Letters, 46.
[3] Zhang, G.Z. (2005) Research on Emitter Identification. National University of Defense Technology, Changsha.
[4] Chen, J. (2013) Features Selection and Specific Emitter Identification of Radar. Xidian University, Xian.
[5] Chaudhary, A., Raheja, J.L., Das, K. (2011) Intelligent approaches to interact with machines using hand gesture recognition in natural way: a survey. J. International Journal of Computer Science and Engineering Survey, 2: 122-133.
[6] Shen, J.H., Huang, J.C., Zhu, Y.C. (2017) Overview of Radar Signal Fast Recognition. J. Electronic Information Warfare Technology, 32: 5-10.
[7] Xu, H.L., Wang, J., Zhou, S.L. (2008) Design and Realization of Specific Radar Emitter Fingerprint Identification Equipment. J. Aerospace Electronic Warfare, 24: 43-58.
[8] Leng, P.F., Xu, C.Y. (2018) Specific Emitter Identification based on Deep Reinforcement Learning. J. Acta Armamentarii, 39: 2420-2426.
[9] Zhou, Z.W., Huang, G.M., Chen, H.Y. (2017) A Review of Radar Emitter Recognition Algorithm. J. Telecommunication Engineering, 57: 973-980.
[10] Qin, C.H., Xue, J. (2009) A Method for Specific Emitter Identification of Radar based on the Rising Edge of Pulse. J. Shipboard Electronic Countermeasure, 32: 27-30.