Radio Frequency Fingerprint Identification Method in Wireless Communication

Zhe Li(✉), Yanxin Yin, and Lili Wu

Research and Development Center,
China Academy of Launch Vehicle Technology, Beijing, China
zheli@163.com, xinye624@163.com, shsqulili@163.com

Abstract. The Radio frequency fingerprinting (RFF) generation mechanism is analyzed in this paper. It is proved to be a secure means for network security access. At the same time, the method of RFF extraction is also given. The characteristics of RFF are analyzed theoretically. Then, a high-precision fingerprint feature identification method based on Kalman filter is proposed. The results of the experiments show that the proposed system can work effectively in the environment where the signal-to-noise ratio (SNR) is higher than 10 dB, and the achieved identification rate is higher than 90%.

Keywords: Radio frequency fingerprinting · Identification method
Identity authentication

1 Introduction

With the constantly emerging information countermeasure in the complex electromagnetic environment, soft attack can be achieved to deceive, disruption, and even control the enemy's information space by using open air interface. Accordingly, the advanced information security technology has become increasingly prominent in wireless communications. At present, there is still flaw in the security protocol. It is very important to study the new physical layer security technology on the theoretical basis of security, which is of urgent military demand and military application value.

Radio frequency fingerprinting (RFF) is derived from the inconsistency in the production process of the components in wireless transmitters, which is reflected by a subtle feature in the launch signal. This subtle difference identifies the different characteristics of the transmitters, similar to human fingerprints, with the uniqueness. RFF can be used for physical layer authentication to protect against replicating, tampering, forgery and other attacks. It can support large-scale concurrent security access authentication and seamless security switch. It can guarantee that the node identity is maintained credibly and the service is maintained continuously.

2 Uniqueness of RFF

The tolerance in the production of the components of radio transmitters is the main cause of RFF. The possible sources of the tolerance include internal electrical components, printed circuit boards, power amplifiers, antennas and other transmitter components.

X. Gu et al. (Eds.): MLICOM 2017, Part I, LNICST 226, pp. 195–202, 2018.
https://doi.org/10.1007/978-3-319-73564-1_19

Even the components with the same standard values have different actual values. The actual value is generally distributed within the tolerance range centered on the standard value and subjects to a certain probability distribution. Due to the presence of component tolerances, the transmitter output signal is different even with the same input excitation. Thus the RFF is formed.

Since the tolerance is slow time-varying, the actual value can be modeled as a random variable, with a mean value of the standard value and subjecting to a certain probability distribution within the tolerance, expressed as m_i, $i = 1, 2, 3, \cdots$.

The baseband signal is translated into an intermediate frequency (IF) signal by quadrature modulation. Then it is converted to an radio frequency (RF) signal via the up-conversion module and the power amplifier. Finally it is eradiated into the radio environment through the antenna. The RFF identification system receives the RF signal from the radio channel, and then is transformed into two baseband signals, namely the in-phase (I) and the quadrature (Q) components, through filtering, amplification and demodulation processing. Then the recognition algorithm will deal with the I and Q components.

The part between the transmitted signal $f(t)$ and the received signal $y(t)$ can be modeled as a constant invariant continuous system with an impulse response of $h(t)$. Since $h(t)$ is determined by the internal electronic components, it is equivalent to RFF [1].

The transmitter element m_i is a random variable, and the recognition system is the same for different transmitters. So the recognition system component value is modeled as a constant invariant quantity. At any time t, $h(t)$ is a definite function of the random variable m_i, expressed as $h(m_i|t)$, which subjects to the determined probability distribution, whose probability density function is $pdf(h(m_i|t))$

The uniqueness of the RFF is equivalent to the uniqueness of $h(t)$, that is, the probability of $\Delta h(m_i|t) = 0$.

$$\begin{aligned} P &= p\{\Delta h(m_i|t) = 0\} \\ &= \int\limits_{\Delta h(m_i|t)=0} pdf(h(m_i|t))dh(m_i|t) = 0 \end{aligned} \tag{1}$$

That is, at any time, the RFF of arbitrary wireless transmitter is unique.

3 Extraction Method and Feature of RFF

3.1 Extraction Method

The procedure of RFF extraction is as follows: Firstly, the demodulated baseband signal is preprocessed and the signal is processed by the coarse synchronization module to obtain the frequency offset of the received signal roughly. Then the frequency offset of the received baseband signal is corrected coarsely. Afterwards, the frequency offset of the received baseband signal is corrected accurately through the precise synchronization module. Finally, the baseband signal is compensated by the sampling rate offset estimation module.

The signal is then compensated with the estimated phase shift by carrier phase synchronization module after the synchronization of the frequency offset and the sampling rate. After a series of synchronization and compensation operations described above, a stable baseband signal is obtained. The constellation trajectory feature, time domain feature and frequency domain feature are obtained from the constellation trajectory, the time-domain waveform and the frequency-domain of the baseband signal. The wireless target identification is carried out in multiple dimensions and multiple time resolutions [2, 3] (Fig. 1).

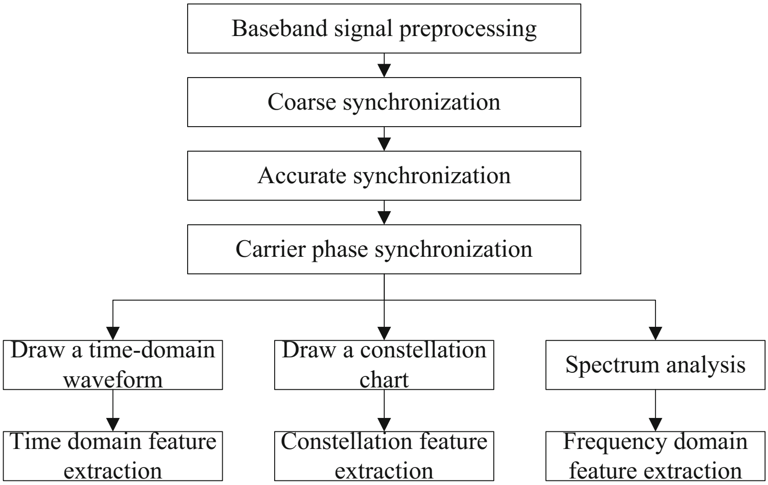

Baseband signal preprocessing
Coarse synchronization
Accurate synchronization
Carrier phase synchronization
Draw a time-domain waveform
Draw a constellation chart
Spectrum analysis
Time domain feature extraction
Constellation feature extraction
Frequency domain feature extraction

Fig. 1. RFF extraction workflow

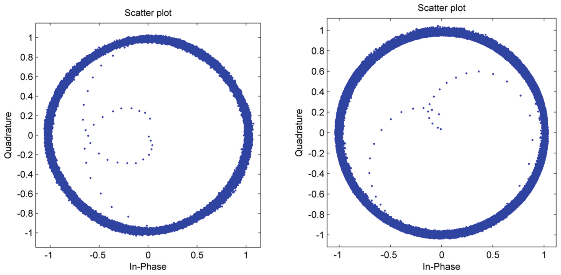
3.2 Fingerprint Features

Offset Quadrature Phase Shift Keying (OQPSK) is a kind of high efficiency constant envelope digital modulation technique which is suitable for band-limited nonlinear channels. It is widely used in wireless communication systems. In this paper, OQPSK is used to analyze the characteristics of RFF.

After preprocessing and frequency/phase offset correction, the constellation trajectory is shown in Fig. 2.

It can be seen from Fig. 2 that although the frequency offset has been estimated and compensated, there is still residual frequency offsets. Accordingly, the directly received constellation is blurred. But we can take a split circle to extract the coordinates of the circle in the trajectory of the constellation. Using this method, the results are shown in Fig. 3.

As can be seen from Fig. 3, we can identify two devices very well through the analysis of the constellation. At the same time, the device has been repeatedly measured with the results of a high degree of consistency. The time domain waveform contains three dimensional information, the time axis, I axis and Q axis, as shown in Fig. 4.



a) OQPSK device 1 b) OQPSK device 2

Fig. 2. Collected OQPSK constellation trajectory map

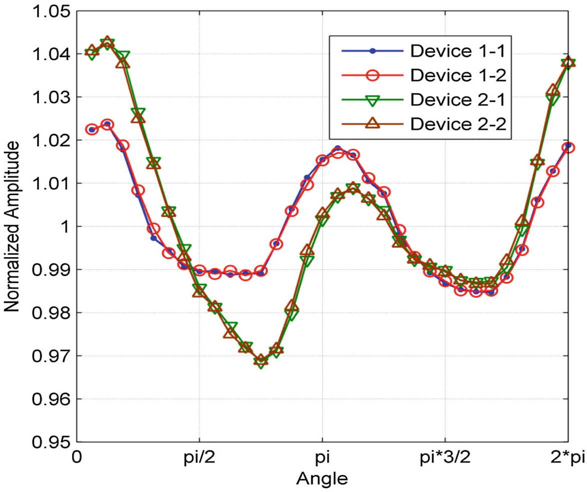


Fig. 3. Analysis of distortion degree of circular for two devices

The time domain feature can also be used to construct a feature extraction method for wireless objects with multiple temporal resolution to accommodate different symbol rates and different channels.

The frequency domain power spectrum is drawn by segmenting the received signal according to a certain length and then the Fourier transform. The spectrum can be analyzed after the Fourier transform, to extract the feature in the frequency domain (Fig. 5).

The spectrum feature is mainly to collect the characteristics of the received signal inside the signal bandwidth and outside the signal bandwidth, so as to obtain the auxiliary wireless target identifying feature.

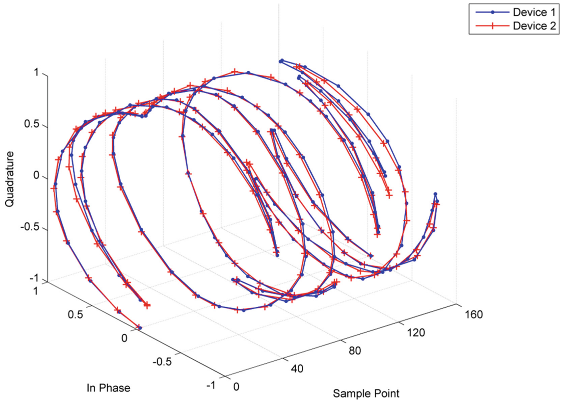


Fig. 4. Time-domain waveform which contains three dimensional information

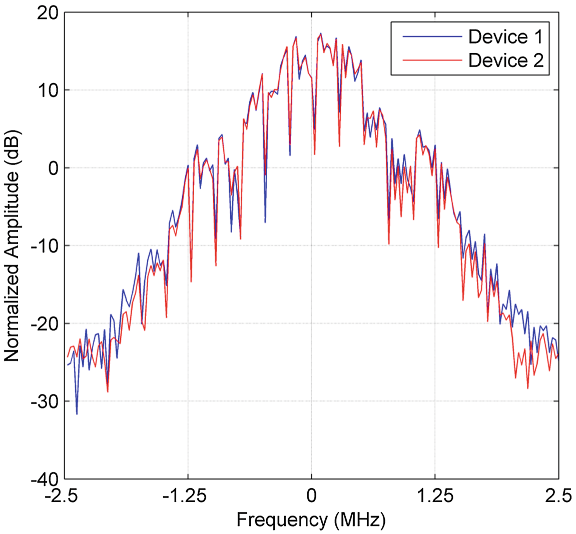


Fig. 5. Frequency-domain spectrum of the two devices

4 High Precision Identification Method for RFF

In the second section, the extraction method of the RFF is given. The next step is to select the appropriate identification algorithm to realize the correct identification of the RFF for different devices. Since the RF characteristics collected in practice are affected by the distortion of the amplifier and the distortion of the channel multipath effect, it is necessary to establish an easily recognizable identification model, to estimate the non-linear characteristics of the amplifier and the channel transmission characteristics, and select the appropriate identification vector, in order to achieve a higher identification rate.

According to the definition of RFF in [4, 5], the identification vector of RFF features is modeled as follows.

$$RFF = \left(\left| \frac{h_b^2}{h_b^1} \right|, \left| \frac{h_b^3}{h_b^1} \right|, \cdots, \left| \frac{h_b^M}{h_b^1} \right| \right)^T \tag{2}$$

Since the extended channel is time invariant, that is

$$\mathbf{h}_{bn} = \mathbf{h}_{b(n-1)} \tag{3}$$

Kalman filter is designed to calculate $\mathbf{h}_b$, and then we can obtain RFF.

The state equation and the measurement equation are as follows.

$$\begin{cases} \mathbf{h}_{bn} = \mathbf{h}_{b(n-1)} \\ y_n = \mathbf{\Phi}_n \mathbf{h}_b + v_n \end{cases} \tag{4}$$

The Kalman filter algorithm can be decomposed. The decomposition formula of optimal predictive value is as follows.

$$\hat{\mathbf{h}}_{b(n/n-1)} = \hat{\mathbf{h}}_{b(n-1)} \tag{5}$$

The decomposition formula of the predictive error covariance is:

$$\mathbf{P}_{n/n-1} = \mathbf{P}_{n-1} \tag{6}$$

The decomposition formula of the filter gain is:

$$\mathbf{K}_n = \mathbf{P}_{n/n-1} \mathbf{\Phi}_n^H (\mathbf{\Phi}_n \mathbf{P}_{n/n-1} \mathbf{\Phi}_n^H + \mathbf{R})^{-1} \tag{7}$$

The decomposition formula of the estimated error covariance is:

$$\mathbf{P}_n = (1 - \mathbf{K}_n (\mathbf{\Phi}_n \mathbf{P}_{n/n-1} \mathbf{\Phi}_n^H + \mathbf{R})) \mathbf{P}_{n/n-1} \tag{8}$$

The decomposition formula of the optimal filter value is:

$$\hat{\mathbf{h}}_{bn} = \hat{\mathbf{h}}_{b(n/n-1)} + \mathbf{K}_n \cdot \left(y_n - \mathbf{\Phi}_n \cdot \hat{\mathbf{h}}_{b(n/n-1)} \right) \tag{9}$$

where $\mathbf{\Phi}_n$ is the measurement matrix and $\mathbf{R}$ is the correlation matrix of measurement noise. According to the observed value y_n obtained at the n$^{\text{th}}$ time, the n$^{\text{th}}$ state estimation $\hat{\mathbf{h}}_{bn}$ can be estimated. When the extended channel $\mathbf{h}_b$ is estimated, the RFF can be calculated and classified.

A software radio platform is used to establish the experiment system. The Zigbee wireless modules are used as target to be identified. In this experiment, different CC2530 Zigbee templates were used to simulate different wireless targets. The software radio platform receives the modulation signals transmitted by different CC2530 modules and identifies the different CC2530 modules.

A channel simulator is used for the simulation of the wireless channel. The recommended parameters of ITU-R M.1225 are used. The equivalent multipath delay parameter is: [0, 50, 110, 170, 290, 310] (ns). The amplitude parameter is: [0, −3, −10, −18, −26, −32] (ns).

Using the identification vector given by Eq. (2), $\mathbf{h}_b$ can be recursively calculated with the Kalman filter method. Then the identification vectors of different CC2530 devices can be calculated.

By adding different sizes of white noise, the performance of the algorithm can be evaluated. The results of the measurement are shown in Fig. 6.

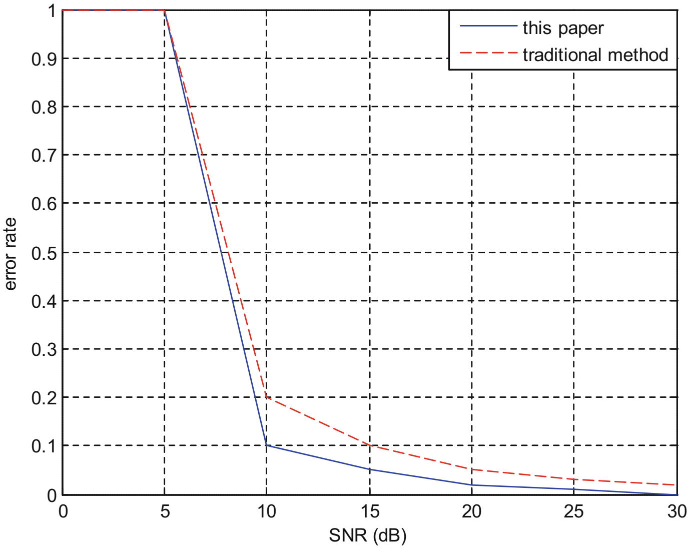


Fig. 6. Error recognition rate with the changes of the signal to noise ratio

As can be seen, the system can work effectively in the environment where the signal-to-noise ratio (SNR) is higher than 10 dB. And the identification rate is higher than 90%. The identification rate approaches 100% when the SNR reaches 28 dB. The traditional method is to draw the constellation map with the normalization process, and look for the appropriate threshold for device identification. When the SNR is higher than 15 dB, the identification rate of the system is up to 90%.

5 Conclusion

In this paper, the RFF extraction method is given, and the uniqueness of the fingerprint feature is verified from the results of the experiments. A high precision identification method of RFF is proposed and verified by experiments. RFF identification technology in military communications has broad application prospects, and can be combined with protocol layer security mechanism to greatly improve the wireless communication network security performance. Besides, fingerprint features of wireless transmitter can be used to distinguish between different transmitters, which can also be used to determine the equipment production process consistency.

References

1. Yuan, L.: Mathematical model of RF fingerprint recognition system. J. Commun. Technol. **42**, 113–117 (2009)
2. Xu, D.: Radiation source fingerprint mechanism and identification method. Ph.D. National University of Defense Technology. Changsha, China (2008)
3. Padilla, P., Padilla, J.L., Valenzuela-Valdes, J.F.: Radio frequency identification of wireless devices based on RF fingerprinting. Electron. Lett. **49**, 1409–1410 (2013)
4. Tang, Z.L., Yang, X.N., Li, J.D.: Fingerprint feature extraction method for narrowband communication radiation source based on sequential statistics. J. Electron. Inf. Technol. **33**, 1224–1228 (2011)
5. Liu, M.W., Doherty, J.F.: Nonlinearity estimation for specific emitter identification in multipath channels. IEEE Trans. Inf. Forensics Secur. **6**, 1076–1085 (2011)