

Specific Emitter Identification based on the Energy Envelope of Transient Signal

Fei Zhuo^a, Yuanling Huang, Jian Chen

Science and Technology on Blind Signal Processing Laboratory, Chengdou, China

^afeiz_24@163.com

Keywords: specific emitter identification, radio frequency fingerprint, energy envelope, iterative least squares.

Abstract. Specific Emitter Identification (SEI) is the method to identify the individual radio emitter using the transmitted signals' characteristic called Radio Frequency Fingerprint (RFF), which are originated from transmitter imperfections. A novel SEI approach to extract transient fingerprint features of energy envelope of transient signals is proposed in this paper. The origin of energy envelope is explored, and a nonlinear system model is utilized to explain how the features of energy envelope produce. An iterative least squares identification algorithm is proposed to extract the parameters of model, which can be constructed the fingerprint features. Experimental results demonstrate that the method is effective, and the method can be applicable any signal of TDMA system.

1. Introduction

Radio Frequency Fingerprint (RFF) that results from the unintentional and unavoidable physical layer imperfections provides a physical layer approach for device identification. SEI is often used for the device identity management and intrusion detection to improve the security of Wi-Fi networks, cellular networks, cognitive radios and so on [1].

There are two main types of radio SEI method: SEI based on transient signal and based on steady state signal. Transient based identification is the most popular solution. When an emitter is turned on, the signal goes through a transient state which is caused by a combination of effects, such as the characteristics of the frequency synthesizer and the power amplifier. The transient signals of different emitters usually have unique RFF for SEI [2]. The RFF of transient signal is mainly extracted from the instantaneous amplitude, phase, time frequency energy distribution (TFED) and bispectrum of transient signals. Hall et al. explored a combination of features such as amplitude, phase and frequency for identifying Bluetooth emitter and wireless networks [3,4]. Many features were extracted from TFED of signal, which can represent the characteristics of signal in both time and frequency domains. Thirteen features of four types were extracted from TFED of transient signals to classify different kind of mobile phones [5]. Shuhua Xu et al extracted features using integral bispectrum of signals [6,7]. Fisher's Linear Discriminant Analysis (LDA) was used to extract features directly [8]. These methods above all maybe have good identification performance; however, there are several challenges. Firstly, transient starting point and endpoint are necessary, but it is difficult to estimate accurately the starting point and endpoint in non-cooperative application. Secondly, the duration of the transient may be too short to contain enough information to discriminate between similar devices.

In this paper, a new transient based SEI method based on energy envelope is proposed. We make the effort to utilize a system to explore the source of energy envelope, and propose an amended least squares algorithm to estimate parameters of model. The signals from five radio emitter in TDMA system are used to evaluate the performance, and the experimental results demonstrate that the method is effective.

The rest of the paper is organized as follows. Section II details the source model of transient energy envelope. In Section III, the algorithm to extract features is explained. Experimental results and conclusion are discussed in Sections IV and Sections V, respectively.

2. Nonlinear system

When an emitter is turned on, the signal goes through a transient state. Due to the inductors and capacitors, the power level of signal is ramped up smoothly in the transient state, as shown in Fig.1. As we can see, the power level of signal does not perform sudden change, but gradually increases. IEEE 802.11 standard specifies that the power level increase gradually to avoid the interface between adjacent frequency channels [9].

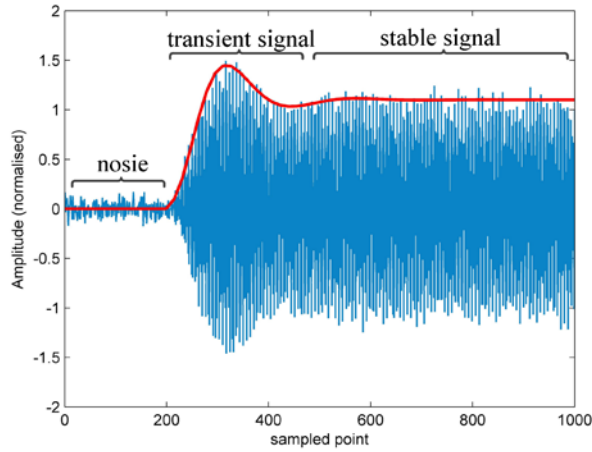


Figure 1 Typical data from TDMA

We assume the transient energy envelope is the output of a system, which contain a linear subsystem and a nonlinear subsystem, and the input is a step function. We use a linear subsystem explain the effect of inductors and capacitors, and the nonlinear subsystem is explained the effect of electronic component, such as power amplifiers.

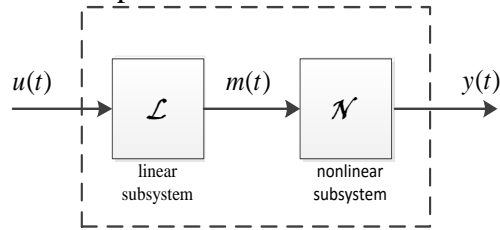


Figure 2 Source of transient energy envelope

The linear subsystem can be given as

$$m(t) = \frac{B(z)}{A(z)} u(t) \quad (1)$$

where $u(t)$ is the input, $A(z)$ and $B(z)$ are polynomials in z^{-1} , and defined as

$$A(z) := 1 + a_1 z^{-1} + a_2 z^{-2} + \dots + a_{n_a} z^{-n_a}$$

$$B(z) := b_1 z^{-1} + b_2 z^{-2} + \dots + b_{n_b} z^{-n_b}$$

The nonlinear subsystem is expressed as a polynomial

$$\mathcal{N}(m(t)) = \gamma_1 m(t) + \gamma_2 m^2(t) + \dots + \gamma_{n_\gamma} m^{n_\gamma}(t) \quad (2)$$

Without loss of generality, let $\gamma_1 = 1$, then can get the system output

$$y(t) = [1 - A(z)]m(t) + B(z)u(t) + \sum_{i=2}^{n_\gamma} \gamma_i m^i(t) \quad (3)$$

3. Feature extraction

The discrepancies between transmitters generate different parameters of the model, which can be constructed the fingerprint features. Least-squares based and gradient based iterative identification algorithm is proposed to extract the parameters. We introduce a stochastic white noise $v(t)$ with zero mean and variance σ^2 to signals, so the sampled energy envelope is expressed

$$y(n) = [1 - A(z)]m(n) + B(z)u(n) + \sum_{i=2}^{n_\gamma} \gamma_i m^i(n) + v(n) \quad (4)$$

Define the parameter vectors and information vectors

$$\begin{aligned} \mathbf{x}_L(n) &= [-m(n-1), \dots, -m(n-n_a)], \\ & \quad u(n-1), \dots, u(n-n_b)]^T \in \mathbb{R}^{n_a+n_b} \\ \mathbf{x}_N(n) &= [m^2(n), \dots, m^{n_\gamma}(n)]^T \in \mathbb{R}^{n_\gamma-1} \\ \mathbf{x}(n) &= \begin{bmatrix} \mathbf{x}_L(n) \\ \mathbf{x}_N(n) \end{bmatrix} \in \mathbb{R}^{n_a+n_b+n_\gamma-1} \\ \boldsymbol{\theta}_L &= [a_1, \dots, a_{n_a}, b_1, \dots, b_{n_b}]^T \in \mathbb{R}^{n_a+n_b} \\ \boldsymbol{\theta}_N &= [\gamma_2, \dots, \gamma_{n_\gamma}]^T \in \mathbb{R}^{n_\gamma-1} \\ \boldsymbol{\theta} &= \begin{bmatrix} \boldsymbol{\theta}_L \\ \boldsymbol{\theta}_N \end{bmatrix} \in \mathbb{R}^{n_a+n_b+n_\gamma-1} \end{aligned}$$

Thus, (4) can be written in a vector form

$$y(n) = \mathbf{x}^T(n)\boldsymbol{\theta} + v(n) \quad (5)$$

The auxiliary model identification method is applied, i.e. replacing the unknown $m(n)$ with the last estimate of $\hat{m}(n)$. Let $k=1,2,3,\dots,N$ be an iteration variable, and $\hat{\boldsymbol{\theta}}_k$ be the iterative estimate of $\boldsymbol{\theta}$. We derive an iterative least-squares algorithm in the following.

Table 1 algorithm of least-squares

Step1: To initialize, $\hat{m}_0(n)=\mathbf{0}$, $\hat{\boldsymbol{\theta}}_0=\mathbf{0}$, $\mathbf{P}_0=\mathbf{I}$
Step2: Collect the input data $u(n)$ and energy envelope $y(n)$
Step3: Estimate $\boldsymbol{\theta}$
for $k=1:N$
$\hat{\boldsymbol{\theta}}_k = \hat{\boldsymbol{\theta}}_{k-1} + \Omega_k (y(k) - \mathbf{x}_k^T \hat{\boldsymbol{\theta}}_{k-1})$
$\Omega_k = \frac{\mathbf{P}_{k-1} \mathbf{x}_k^T}{\mathbf{x}_k \mathbf{P}_{k-1} \mathbf{x}_k^T + 1}$
$\mathbf{P}_k = (\mathbf{I} - \Omega_k \mathbf{x}_k^T) \mathbf{P}_{k-1}$
$\mathbf{x}_k = \begin{bmatrix} \mathbf{x}_{L,k}(k) \\ \mathbf{x}_{N,k}(k) \end{bmatrix}$
$\mathbf{x}_{L,k}(n) = [-\hat{m}_{k-1}(n-1), \dots, -\hat{m}_{k-1}(n-n_a), u(n-1), \dots, u(n-n_b)]^T$
$\mathbf{x}_{N,k}(n) = [\hat{m}_{k-1}^2(n), \dots, \hat{m}_{k-1}^{n_\gamma}(n)]^T$
$\hat{m}_k(n) = \mathbf{x}_{L,k}^T(n) \hat{\boldsymbol{\theta}}_{L,k}$, $n=1,2,3\dots N$
end

The estimate $\hat{\boldsymbol{\theta}}$ is constructed the fingerprint features. In our experiment, $n_a=n_b=3$, $n_\gamma=5$.

4. Experimental results

In this experiment, signals of five terminals from Automatic Identification System (AIS) were captured to investigate performance of our method. The signals of AIS are typical burst signals, in which transient signals can be capture easily. Fig.3 shows the energy envelope of transient signals of five emitters. As we can see, the discrepancies among different transient signals are subtle. Each burst has 440 sampled points, and five terminals have 188, 690, 706, 150, 78 bursts respectively. Half of the bursts construct the train data set, and the rest of burst construct the test data set.

MATLAB and its associated toolboxes are used for signal processing and performance evaluation, and Support Vector Machine (SVM) classifier which was is used [10]. To investigate the performance, we take the proposed approach to compare with the bispectrum based method, the method of TFED and the method of LDA. The identification accuracy is showed in Fig.4.

When the sampled points are not enough, the TFED of signals obtained by Hilbert-Huang transform may be incorrect. The End Effects of EMD and Hilbert-Huang transform are severely. The method of LDA is affected by noise easily, and signals are polluted severely when the SNR (Signal to Noise Ratio) is low, so the identification accuracy is low. Otherwise, our method utilize the coefficients of a model that describe the origin of energy envelop as radio frequency fingerprint, and the noise only influences the accuracy of the estimated coefficients.

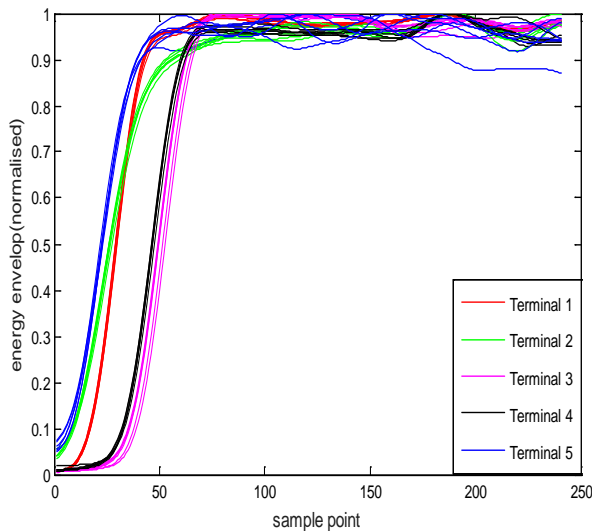


Figure 3 the energy envelope of signals

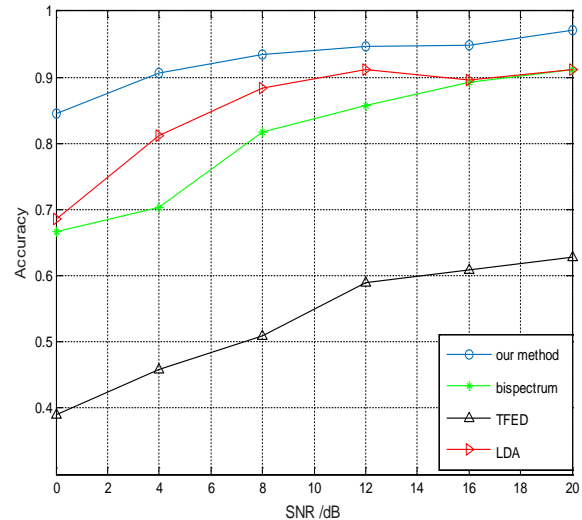


Figure 4 Accuracy of methods in the experiment

5. Conclusion

An SEI method based on energy envelope features is proposed in this paper. A model is utilized to explain that how the energy envelope features of transient signals generate. An iterative least-squares algorithm is proposed to extract the parameters of model. Transient signals are used to test the validity of fingerprint features and the experiment results demonstrate that the proposed method is effective. Compared with three previous techniques, the features extracted with the proposed method are affected rarely by noise. The accurate starting point and endpoint of transient signals and many sampled points are not needed. The proposed approach can be applicable any signals with transient signals.

References

- [1] .Ureten and N. Serinken. Wireless security through RF Fingerprint [J]. Can. J. Elect. Comput. Eng., February 2007, 32(1), pp. 27-33.
- [2] Danev, B., Luecken, H., Capkun, S., et al. Attacks on physical-layer identification [J]. WiSec'10:

Proc. Third ACM Conf. on Wireless Network Security, New York, NY, USA, 2010, pp. 89–98.

- [3] J. Hall, M. Barbeau, and E. Kranakis. Radio frequency fingerprinting for intrusion detection in wireless networks [J]. IEEE Transactions on Dependable and Secure Computing, pp. 1-35, 2005.
- [4] Hall J, Barbeau M, Kranakis E. Detecting rogue devices in bluetooth networks using radio frequency fingerprinting[C]. Iasted International Conference on Communications & Computer Networks. 2006:108-113.
- [5] Yingjun Yuan, Zhitao Huang, Hao Wu. Specific emitter identification on Hibert-Huang transform-based time-frequency-energy distribution features [J]. The Institution of Engineering and Technology, 2014, 8(13):2404-2412.
- [6] Shuhua Xu, Benxiong Huang, Yuchun Huang, Zhengguang Xu. Identification of Individual Radio Transmitter Based on Selected Surrounding-line Integral Bispectra [C]. IEEE International Conference on Advanced Communication Technology (ICACT), 2007,2:1147-1150.
- [7] TAO Wanglin, LU Xuanmin, LIU Lijian. Transmitter individual identification baded on local surrounding-line integeal bispectrum[J]. Computer Engineering and Application. 2013, 49(1):131-133.
- [8] Yuanling Huang, Hui Zheng. Radio frequency fingerprinting based on the constellation errors[C]. 18th Asia-Pacific Communications Conference(APCC), 2012:900-905.
- [9] Caidan Zhao, Lianfen Huang, Liting Hu, et al. Transient fingerprint feature extract for WLAN cards based on polynomial fitting [C], The 6th International Conference on Computer Science & Education(ICCSE 2011).
- [10] Chih-Chung Chang and Chih-Jen Lin, LIBSVM : a library for support vector machines, 2001. Software available at <http://www.csie.ntu.edu.tw/~cjlin/libsvm>.