Honglin YUAN, Zhihua BAO, Chen XU*, Guoan ZHANG

University of Nantong

Robust Cepstrum Radio Frequency Fingerprint Transformed from BPSK Signal

Abstract. *Identifying wireless devices based on Radio Frequency fingerprint* (*RFF*) *is a promising physical layer security methodology. One practical issue is the robustness of RFF affected by wireless multi-path channels, etc. Proposed is a kind of RFF with robustness for identifying digital BPSK transmitters. The cepstrum of the received BPSK signal is obtained and then low-pass filtered, the result signal is mainly determined by device impulse response, and thus is robust. The proposed fingerprint can be used in the fusion identification of BPSK wireless transmitters.*

Streszczenie. *W artykule opisano sposób radiowej identyfikacji urządzeń bezprzewodowych, o bezpiecznej identyfikacji cyfrowych nadajników BPSK. Uzyskane cepstrum odebranego sygnału BPSK, poddawane jest filtracji dolno-przepustowej, co w efekcie daje sygnał wyznaczony przez odpowiedź impulsową urządzenia. Opracowany algorytm można wykorzystać w rozpoznaniu łączenia się nadajników BPSK. (**Transformacja sygnału BPSK do fingerprintu w cepstrum częstotliwości radiowej o zwiększonej odporności**).*

Keywords: physical layer authentication, cepstrum analysis, Radio Frequency fingerprints
Słowa kluczowe: uwierzytelnienie warstwy fizycznej. Analiza cepstrum, RFF.

1. Introduction

With the rapid development of wireless networks and the increasing security threats, wireless network security is developing toward physical layer [1]. Identifying wireless transmitters according to their radio frequency (RF) fingerprints (RFFs) is a potential physical layer authentication methodology in wireless networks [2].

RF Fingerprint (RFF) is caused by the component tolerances of wireless transmitters, consisting of manufacturing tolerance which is brought in during the manufacturing and assembly process, and drift tolerance which is brought in during the transmitter's life cycle. Component tolerances result in the nature of wireless transmitters, even if their structures and component nominal values are the same, are not exactly the same. Furthermore, even a slight difference of hardware in RF band has a big impact on the received signal and its transformation —— RFF.

RFF can be summarized as the transformation of a received signal from a wireless device, which carries the hardware information of the transmitter of the device to be identified and is comparable [3-11]. The existence of component tolerances of the devices to be identified causes their transmitter fingerprints unique and unclonable ideally [12]. However, since abundant devices with the same manufacturer/model commonly exist in one network, the discriminability of transmitter fingerprints is generally bad. So, identifying transmitters with their fingerprints remains an arduous task. However, fusion identification of a transmitter with multiple fingerprints is regarded as one feasible methodology [13], where the received signal from the device to be identified is transformed as linear, nonlinear and mixed transmitter fingerprints which embody diverse hardware information of the device. Features are extracted from the fingerprints and the device is then identified with the features [14].

The robustness of RFF, which refers to the consistency of different RFF samples transformed from signals emitted by a wireless transmitter, is a necessary condition for the identification of a wireless transmitter according to its RFF [15]. Time-varying wireless multi-path channel is the dominant factor affecting the robustness of RFFs in a wireless network.

BPSK modulation which has large inter-symbol distance is often used in generating the preamble of the wireless network physical layer frame, such as in IEEE 802.11b/g. This article proposes a kind of novel RFF transformed from BPSK signal, called cepstrum-RFF, which is a low-pass filtered cepstrum of the received BPSK baseband analog signal. Theoretical analysis shows that the proposed cepstrum-RFF is mainly constituted by the cepstrum components of device impulse response where the impacts of wireless multi-path channel and baseband digital signal are eliminated, and thus is stable. The proposed technique is verified with 2.4GHz BPSK RF signals collected from Vector Signal Generator. Experimental results demonstrate that the proposed cepstrum-RFF is more robust than classical turn-on RFF and can be used in fusion identification of BPSK wireless devices with multiple RFFs.

2. System Model

Modern communication transmitters, whose power is low or whose transmitted signals are pre-processed to eliminate nonlinear components, can be approximated to linear systems. Relative to processing time of RFF identification algorithm, the variation of component drift tolerances is extremely slow, so the actual value of the components can be modeled as linear time invariant in short term. Suppose the wireless multi-path channel remains unchanged during one physical layer frame, then the equivalent low-pass system, which includes the BPSK transmitter to be identified, the wireless multi-path channel, additive white Gaussian noise (AWGN), and the BPSK baseband signal receiver, can be modeled as a linear time-invariant system. Then the received BPSK baseband signal is:

$$r(t) = [m(t) \star h_{tx}(t) \star h_i(t) + n_i(t)] \star h_{rcv}(t) \tag{1}$$

where ★ denotes convolution.

In equation (1), $m(t)$ is the baseband transmitted BPSK signal which can be expressed as:

$$m(t) = \sum_k b(k)\delta(t - kT) \tag{2}$$

where $b(t)$ is the binary data sequence of {±1} transmitted at a rate of 1/T bits/s; $h_{tx}(t)$ is the impulse response of equivalent low-pass system of BPSK transmitter; $h_i(t)$ is the in-phase component of equivalent low-pass multi-path channel [16] :

$$h_i(t) = \sum_k \alpha_k \cos(2\pi f_c \tau_k)\delta(t - \tau_k) \tag{3}$$

where α_k is the attenuation factor for the signal received on the kth path, τ_k is the propagation delay for the kth path, and f_c is the carrier frequency of BPSK RF signal; $n_i(t)$ is the in-phase component of equivalent low-pass AWGN; and

$h_{rcv}(t)$ is the impulse response of equivalent low-pass system of BPSK baseband signal receiver.

$h_{tx}(t)$ in Equation (1) is determined by the structure and components' actual parameter values of the BPSK transmitter. As with the existing component tolerances, $h_{tx}(t)$ of different transmitters, even with the same structure and components with the same nominal value, are different.

For different transmitters, even if functions in Equation (1) besides $h_{tx}(t)$ are all the same, $r(t)$ are different as different $h_{tx}(t)$. When $m(t)$ is the unit step excitation, the envelope of $r(t)$ is one kind of classical turn-on RFF [12, 15].

By equation (1), we can see that $h_i(t)$ may be different with different frames emitted by the transmitter to be identified, which affects the robustness of $r(t)$ and its RFF.

3. The Proposed Cepstrum RF Fingerprint of BPSK signal

3.1 Transform Technique

Discrete time Fourier transform (DTFT) version of equation (1) is:

$$R(e^{jw}) = M(e^{jw}) \bullet H_{tx}(e^{jw}) \bullet H_i(e^{jw}) \bullet H_{rcv}(e^{jw})[1 + \frac{N_i(e^{jw})}{M(e^{jw}) \bullet H_{tx}(e^{jw}) \bullet H_i(e^{jw})}] \quad (4)$$

where $R(e^{jw})$, $M(e^{jw})$, $H_{tx}(e^{jw})$, $H_i(e^{jw})$, $H_{rcv}(e^{jw})$ and N_i (e^{jw}) are DTFT of $r(t)$, $m(t)$, $h_{tx}(t)$, $h_i(t)$, $h_{rcv}(t)$ and $n_i(t)$, respectively.

Then the cepstrum version, the inverse DTFT of logarithm of amplitude of equation (4), is:

$$\hat{r}(n) = \hat{m}(n) + \hat{h}_{tx}(n) + \hat{h}_i(n) + \hat{h}_{rcv}(n) + \hat{n}_i(n) \quad (5)$$

where $\hat{r}(n)$, $\hat{m}(n)$, $\hat{h}_{tx}(n)$, $\hat{h}_i(n)$ and $\hat{h}_{rcv}(n)$ are the cepstra of $r(n)$, $m(n)$, $h_{tx}(n)$, $h_i(n)$ and $h_{rcv}(n)$, respectively; and $\hat{n}_i(n)$ arises from the presence of noise $n_i(n)$ and vanishes in its absence.

From equation (2) and (3), we can see that $m(n)$ and $h_i(n)$ are impulse trains, so their cepstra $\hat{m}(n)$ and $\hat{h}_i(n)$ are impulse trains that vary rapidly [17]; By contrast, $\hat{h}_{tx}(t)$ and $\hat{h}_{rcv}(t)$ concentrate near time original point and vary slowly based on communication system and cepstrum theories. Therefore, the low-pass filtered $\hat{r}(n)$ in cepstrum domain:

$$LPF\{\hat{r}(n)\} = \hat{h}_{tx}(n) + \hat{h}_{rcv}(n) + LPF\{\hat{m}(n) + \hat{h}_i(n) + \hat{n}_i(n)\} \quad (6)$$

would remove $\hat{m}(n)$, $\hat{h}_i(n)$ and varying-rapidly components of $\hat{n}_i(n)$. So, $LPF\{\hat{r}(n)\}$ is robust as $\hat{h}_{tx}(n)$ and $\hat{h}_{rcv}(n)$ are uniquely determined by the hardware property of the BPSK transmitter and the baseband signal receiver, respectively.

3.2 Experiment Study

The experimental setup consists of a vector signal generator (VSG), RF oscillograph, antennas and computers, etc. Agilent's E4438C VSG connected with an antenna is used to generate random BPSK RF signal frames, the carrier frequency is 2.412GHz, power is maximum 20dBm, binary data rate is 11Mbps, and a frame is 80usec long. The Agilent RF oscilloscope 54854A connected with a high-gain antenna is used to acquire the transmitted RF signal frame, the sampling rate is 10GSps, data memory is 1025000 samples, and indoor wireless channel is changed man-made when acquiring the RF signal frames, with indoor temperature and humidity are kept constant.

One hundred BPSK RF frames are acquired and processed with Matlab (normalize, down-convert, low-pass filter) and Simulink (costas PLL) in Pentium 4 computer to obtain baseband signal $r_i(n)$ and its quadrature component $r_q(n)$ ($r_q(n)$ is not all zero during the phase-locked loop transitional period).

The cepstrum (cepstra) of $r_i(n)$, or $\hat{r}_i(n)$ is obtained, and the superposed graph of heads of 100 $\hat{r}_i(n)$ samples is illustrated as Fig. 1. We can see from Fig. 1 that $\hat{r}_i(n)$ is mainly composed of low-time component, random vary-quickly component, and periodic-component. The fact that the period of the periodic-component is coincident with the period of $m(n)$ and that the signal-to-noise ratio of the received $r_i(n)$ and $r_q(n)$ is high ensures that the periodic-component of $\hat{r}_i(n)$ is mainly constituted by $\hat{m}(n)$, the low-time component of $\hat{r}_i(n)$ is mainly constituted by $\hat{h}_{tx}(n)$ and $\hat{h}_{rcv}(n)$, and the random vary-rapidly component of $\hat{r}_i(n)$ is mainly constituted by $\hat{h}_i(n)$.

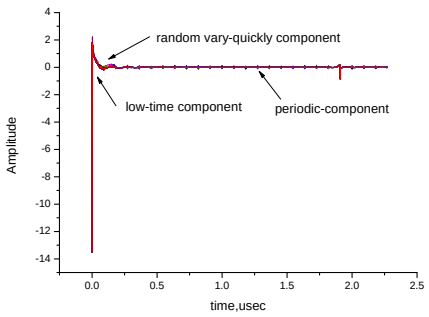

Fig.1. Superposed graph of heads of 100 $\hat{r}_i(n)$ samples

The 100 $\hat{r}_i(n)$ samples are then low-pass filtered with an easy finite impulse response low pass filter. The truncated head signals are the cepstrum-RFF denoted as $LPF\{\hat{r}_i(n)\}$. One hundred samples of $LPF\{\hat{r}_i(n)\}$ are illustrated as Fig. 2.

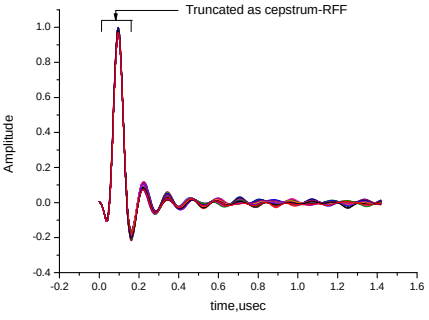

Fig.2. Superposed graph of 100 $LPF\{\hat{r}_i(n)\}$ samples

We can see from Fig. 2 that almost all vary-quickly components of $\hat{r}_i(n)$ including $\hat{m}(n)$ and $\hat{h}_i(n)$, etc., in Fig. 1 have been removed, and the 100 $LPF\{\hat{r}_i(n)\}$ samples demonstrate robustness under time-varying wireless multi-path channel.

To compare the robustness of cepstrum-RFF with turn-

on RFF, the corresponding classical turn-on RFF samples are obtained based on $r_i(n)$ and $r_q(n)$, and the superposed graph of the 100 corresponding turn-on RFF samples is illustrated as Fig. 3.

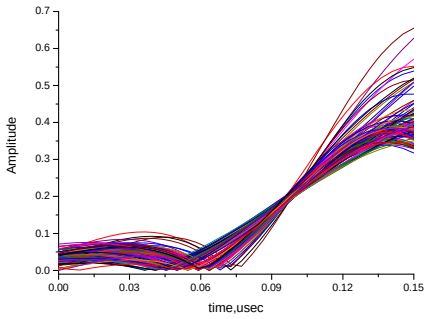

Fig.3. Superposed graph of the 100 corresponding classical turn-on RFF samples

The average interclass Euclidean distance per sample point of RFF D is calculated for measuring its robustness: D of cepstrum-RFF is 9.5479e-004 while D of turn-on RFF is 1.01e-2. We can see that the robustness of cepstrum-RFF is better than that of classical turn-on RFF. This result is determined by their transform techniques; turn-on RFF is the square root of sum of squares of $r_i(n)$ and $r_q(n)$ [12, 15], which cannot remove the impact of wireless channel, while the transform of cepstrum-RFF removes it.

4. Conclusion

In this article, the transform technique of cepstrum-RFF for the identification of BPSK wireless transmitters is proposed where cepstrum of the received BPSK baseband analogue signal is obtained and then low-pass filtered. Theoretical analysis and experience demonstrate that the proposed cepstrum-RFF is more robust than the corresponding turn-on RFF as it is mainly determined by device hardware property.

On the other hand, it is proved that the discriminability of one kind of RFF is mainly determined by the comparing relationship between the resolution of the RFF identification system versus the construction and component tolerances property of the transmitter to be identified. The smaller the resolution of the RFF identification system, the better the discriminability of this kind of RFF. Therefore, the discriminability of the proposed cepstrum-RFF is not studied in this paper.

The identification of transmitters with the same manufacture/model, which is realistic in the physical-layer security of communication network, is quite hard, fusion identification with multiple RFFs is a feasible methodology, and more kinds of independent RFFs are beneficial to the identification of the transmitter. BPSK modulation, which has large inter-symbol distance, is often used in generating the preamble of the wireless network physical layer frame, such as in IEEE 802.11b/g. As the proposed fingerprint can supply new dimensional hardware information for the fusion identification of BPSK transmitters, the proposed cepstrum-RFF is consequently valuable to relevant applications such as access control of wireless network on physical layer.

Acknowledgments: This research was supported by the National Natural Science Foundation of China under Grant 61071086, the Ministry of Transport of China under Grant 2010-353-332-110 and 2012-319-813-270.

REFERENCES

[1] W. Trappe, V. Poor, H. Iwai, A. Yener, P. Prucnal, and J. Barros, Special Issue on Using the Physical Layer for Securing the Next Generation of Communication Systems. *IEEE Trans. Inf. Forensic Secur.*, 6 (2011), 521-522.

[2] K. Zeng, K. Govindan, and P. Mohapatra, Non-Cryptographic Authentication and Identification in Wireless Networks. *IEEE Wirel. Commun.*, 17 (2010), 56-62.

[3] R. M. Gerdes, T. E. Daniels, M. Mina, and S. F. Russell, Device Identification via Analog Signal Fingerprinting : A Matched Filter Approach. *Annual Symposium on Network and Distributed System Security*, San Diego (USA), 2006.

[4] D. G. Lee, J. W. Han, D. S. Park, and I. Y. Lee, Intelligent Pervasive Network Authentication : S/Key Based Device Authentication. *IEEE Consumer Communications and Networking Conference*, Las Vegas (USA), 2009, pp. 1-5.

[5] R. W. Klein, M. A. Temple, and M. J. Mendenhall, Application of Wavelet-Based RF Fingerprinting to Enhance wireless Network Security. *Journal of Communications and Networks*, 11 (2009), 544-555.

[6] M. Hamdi, A. Meddeb-Makhlouf, and N. Boudriga, Multilayer Statistical Intrusion Detection in Wireless Networks. *Eurasip Journal on Advances in Signal Processing*, (2009), 1-13.

[7] C. Andrea, K. Ovunc, and K. Farinaz, Robust stable radiometric fingerprinting for wireless devices. *IEEE International Workshop on Hardware-Oriented Security and Trust*, San Francisco (USA), 2009, pp. 43-49.

[8] L. Li, H. B. Ji, and L. Jiang, Quadratic time-frequency analysis and sequential recognition for specific emitter identification. *IET Signal Processing*, 5 (2011), 568-574.

[9] M. W. Liu and J. F. Doherty, Nonlinearity Estimation for Specific Emitter Identification in Multipath Channels. IEEE Transactions on Information Forensics and Security, 6 (2011), 1076-1085.

[10] A. C. Polak, S. Dolatshahi, and D. L. Goeckel, Identifying Wireless Users via Transmitter Imperfections. IEEE Journal on Selected Areas in Communications, 29 (2011), 1469-1479.

[11] Y. Shi and M. A. Jensen, Improved Radiometric Identification of Wireless Devices Using MIMO Transmission. *IEEE Trans. Inf. Forensic Secur.*, 6 (2011), 1346-1354.

[12] H. L. Yuan and Z. H. Bao, Power ramped-up preamble RF fingerprints of wireless transmitters. *Radioengineering*, 20 (2011), 703-709.

[13] I. Kenneth, R. Paul and H. Martin, Specific emitter identification and verification. *Technology Review Journal*, (2003), 113-133.

[14] H. L. Yuan and A. Q. Hu, Preamble-based detection of Wi-Fi transmitter RF fingerprints. *Electronics Letters*, 46 (2010), 1165-1167.

[15] K. J. Ellis and N. Serinken, Characteristics of radio transmitter fingerprints. *Radio Science*, 36 (2001), 585-597.

[16] J. G. Proakis, Digital communication. New York: McGrawHill, 1995.

[17] R. W. Schafer, Echo removal by discrete generalized linear filtering. Massachusetts institute of technology, 1969.

***Authors**: dr. Honglin Yuan, prof. Zhihua Bao, prof. Chen Xu (corresponding author) and prof. Guoan Zhang, School of Electronics and Information, Nantong University, No. 9, Seyuan Road, 226019 Nantong, P.R.China, E-mail: ntusignals@gmail.com.*