Robust cepstrum device fingerprint of proximity coupling RFID tags

Honglin Yuan
School of Electronics and Information
Nantong University
Nantong, Jiangsu, P.R.China
ntusignal@gmail.com

Guoan Zhang
School of Electronics and Information
Nantong University
Nantong, Jiangsu, P.R.China
gzhang@ntu.edu.cn

***Abstract*—A novel device fingerprint (DF) based on the hardware property of RFID tags is proposed to enhance the privacy protection and information security of RFID system. The received signal of proximate tag is processed with quadrature down-conversion, cepstrum analysis, etc., the result is called cepstrum DF of tags. Modeling analyses, numerical simulation and experiments demonstrate that the impact of digital information have been eliminated from the proposed cepstrum DF which is mainly determined by the physical property of the hardware of tags. The proposed DF can be used for the physical identification and verification of the identity of proximate RFID tags.**

Keywords-hardware security; RFID; device fingerprint; cepstrum transformation

I. INTRODUCTION

Due to low cost and convenience in identifying an object without physical contact, Radio frequency identification (RFID) has been extensively explored in many creative applications. Generally speaking, an RFID system consists of one server, one or many readers, and hundreds or thousands of tags. The readers and tags of one RFID system communicate with electromagnetic wave. The broadcast nature of the medium facilitates many security attacks, such as eavesdropping, impersonation, tag cloning, counterfeiting, denial of service, de-synchronization, and retransmission. Conventional security protocols based on cryptographic mechanisms have been widely used to realize secure communications of RFID system. However, the digital information within RFID systems is ease to be replicated illegally; with the illegal digital information, the authentication protocols of RFID system are prone to be compromised. Consequently, new mechanisms are needed to enhance the information security and privacy protection of RFID systems.

Authentication of communication entities is the key to and foundation of the information security and privacy protection of RFID systems. Recently, many non-cryptographic authentication methods are proposed to enhance the security of RFID and other wireless systems [1-4]. In literature [4], device fingerprints or electronic fingerprints of RFID tags are combined with authentication protocol to raise the security level of RFID system, which is one kind of technologies of non-cryptographic authentication. However, the success run of DF-based authentication protocol as proposed in [4] relies on the accurate identification of the DF of RFID tags. As RFID tags with the same manufacturer/model are abundant, identifying RFID tags with DF remains an arduous task; and more kinds of DF that carry more hardware information of one tag are beneficial to the fusion identification of the tag.

In this paper, we present a new kind of DF transformed from the signal of proximity coupling RFID tags, which can be used in the fusion identification of tags. The rest of this paper is organized as follows: Section 2 builds an equivalent model of RFID DF identification system; the novel DF of the tags and its numerical simulation are introduced in Section 3; section 4 is the experiments with ISO 14443A RFID tags, which demonstrates the performance of the proposed DF transformation method. The last section is the conclusion of this paper.

II. EQUIVALENT MODEL OF RFID DF IDENTIFICATION SYSTEM

A. Signal of proximity coupling RFID tags

Proximity coupling RFID systems are widely used for tracking pets, shopping payment and identification confirmation etc, and one prevalent standard of proximity coupling RFID system is ISO 14443. With ISO standard 14443, the power supply of tags is provided by the magnetic alternating field of a reader at a transmission frequency of 13.56MHz. A load modulation procedure with sub-carrier is used for data transfer from the tag to the reader. The sub-carrier frequency is 847.5KHz (13.56MHz/16). The modulation of the sub-carrier is performed by on/off keying of the sub-carrier using a Manchester coded data stream when the mode is Type A; the sub-carrier is modulated by 180 degree phase shift keying (BPSK) of the sub-carrier using the NRZ coded data stream when the mode is Type B. The spectrum of load modulated signal regulated by ISO standard 14443A is shown in Fig.1.

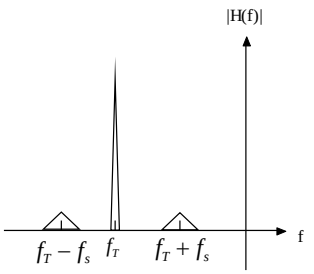

Fig. 1 The spectrum of load modulated ISO 14443A signal

f_T in Fig. 1 is 13.56MHz which is the frequency of the carrier; f_s in Fig. 1 is 847.5KHz which is the frequency of sub-carrier that carries the digital information of tags. One actual RF signal sample of ISO 14443A and the zoom view of the corresponding delay-demodulated result are shown in Fig. 2.

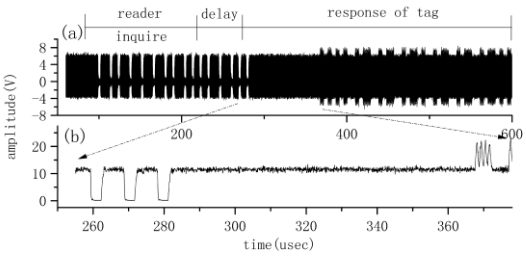

Fig. 2 One actual ISO 14443A RF signal sample and the zoom view of the corresponding delay-demodulated result

Sub-graph (a) of Fig. 2 is one actual RF signal sample acquired near the antenna of one 14443 reader. The start signal is initiated by the reader which inquires the near tags, then is the delay RF signal which is necessary to keep the power supply of the near tags, the end signal is the response of the inquired tag. The RF signal in sub-graph (a) is delay-demodulated, and the zoom view of the local demodulated result is shown in sub-graph (b).

With ISO standard 14443 and Fig. 2, it can be concluded that the response signal of 14443 RFID tag can be modeled as quasi-BPSK signal.

B. Equivalent Model of RFID DF Identification System

The equivalent model of RFID DF identification system based on quadrature downconverter is illustrated in Fig. 3.

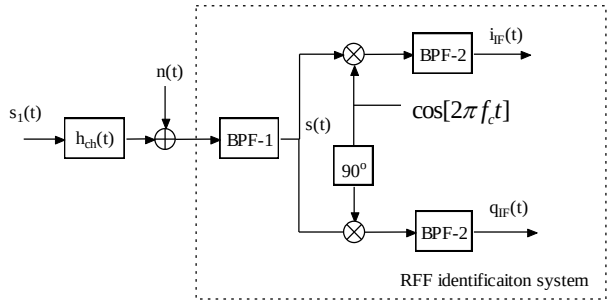

Fig. 3 The equivalent model of RFID DF identification system

In Fig. 3, $s_1(t)$ is the signal transmitted by the proximity coupling RFID tag to be identified; $h_{ch}(t)$ is the impulse response of wireless channel; $n(t)$ is the AWGN noise; band-pass filter BPF-1 is used to obtain the upper or lower sideband of the input signal, and the output signal of BPF-1 is noted as $s(t)$; $\cos(2\pi f_c t)$ is the signal of oscillator; BPF-2 are the band-pass filters whose output signals are noted as $i_{IF}(t)$ and $q_{IF}(t)$, respectively.

As the distance between the proximity coupling RFID reader and the corresponding tag is within 7-15cm approximately, the impulse response of wireless channel $h_{ch}(t)$ in Fig. 3 can be regarded as $\delta(t)$.

$n(t)$ in Fig. 3 is the AWGN noise of the RFID DF identification system, which can be written as follows:

$$n(t) = \mathrm{Re}\{n_l(t)e^{j2\pi f_c t}\} \tag{1}$$

$n_l(t)$ in Equation (1) is the equivalent low-pass signal which can be written as follows:

$$n_l(t) = n_x(t) + jn_y(t) \tag{2}$$

$n_x(t)$ and $n_y(t)$ in Equation (2) are the equivalent low-pass signal of I and Q channel AWGN noise, respectively.

$s(t)$ is Fig. 3 can be described as follows:

$$s(t) = \mathrm{Re}\{s_l(t)e^{j2\pi(f_c+\Delta f)t}\} \tag{3}$$

where $s_l(t) = x(t) + jy(t)$ is the equivalent low-pass signal of $s(t)$, f_c is the corresponding standard-defined carrier frequency which is $f_T - f_s$ (upper sideband) or $f_T + f_s$ (lower sideband), Δf is the actual difference of frequency between that of the tag to be identified and the corresponding standard. $x(t)$ and $y(t)$ of $s_l(t)$ are the baseband transmitted signal of I and Q channel respectively, which can be written as follows:

$$x(t) = m_x(t) * h_x(t) \tag{4}$$

and

$$y(t) = m_y(t) * h_y(t) \tag{5}$$

$m_x(t)$ and $m_y(t)$ in Equation (4) and (5) are the baseband transmitted digital signal of I and Q channel, respectively; $h_x(t)$ and $h_y(t)$ are the impulse response of I and Q channel equivalence respectively, which are determined by their hardware property of the tag to be identified.

Suppose the band-pass filters BPF-2 are ideal, and the theoretical derivation is done with low-pass equivalences domain, then the received low-pass equivalent signal of the RFID DF identification system is given by

$$r_l(t) = s_l(t) * c_l(t) + n_l(t) \tag{6}$$

And the received IF signals are given by

$$i_{IF}(t) = \mathrm{Re}\{r_l(t)\square e^{j2\pi\Delta ft}\} \tag{7}$$

and

$$q_{IF}(t) = \mathrm{Im}\{r_l(t)\square e^{j2\pi\Delta ft}\} \tag{8}$$

III. THE PROPOSED DF TRANSFORMED FROM PROXIMITY COUPLING RFID TAG SIGNALS

A. Theoretical derivation

The received IF signals are firstly denoising processed, and as the SNR of the transmitted signal from the proximate coupling RFID tag is not low, the noise terms $n_x(t)$ and $n_y(t)$ in Equation (7) and (8) can be neglected. Consequently, Equation (7) becomes

$$i'_{IF}(t) = [x(t) + y(t)] \cdot \cos(2\pi\Delta f t) - [y(t) - x(t)] \cdot \sin(2\pi\Delta f t)\} \quad (9)$$

and Equation (8) becomes

$$q'_{IF}(t) = [y(t) - x(t)] \cdot \cos(2\pi\Delta f t) + [x(t) + y(t)] \cdot \sin(2\pi\Delta f t) \quad (10)$$

As the signal of 14443 RFID tag can be modeled as quasi-BPSK signal, $y(t)$ in Equation (9) and (10) are supposed as zero. Suppose the Fourier Transform of $i'_{IF}(t)$ and $q'_{IF}(t)$ are $I_{IF}(f)$ and $Q_{IF}(f)$, respectively. Then, the Fourier Transform of the composed complex IF signal $g(t) = i_{IF}(t) + j \cdot q_{IF}(t)$ can be written as:

$$G(f) = I_{IF}(f) + j \cdot Q_{IF}(f) = M_x(f) \cdot H_x(f + \Delta f) \quad (11)$$

where $M_x(f)$ is the Fourier Transform of the baseband transmitted signal $m_x(t)$, and $m_x(t)$ can be expressed as the binary data sequence; $H_x(f)$ is the Fourier Transform of the impulse response of the transmitting hardware equivalence $h_x(t)$. The inverse FT of logarithm of amplitude, or cepstrum, of Equation (11) can be written as:

$$\hat{g}(t) = \hat{m}_x(t) + \hat{h}_x(t) \quad (12)$$

$m_x(t)$ is impulse trains, so its cepstrum $\hat{m}_x(t)$ is impulse trains that vary rapidly. By contrast, $\hat{h}_x(t)$ in Equation (12) varies slowly whose power concentrated at the IF according to the basic property of communication system. Therefore, low-pass filter the Equation (12), and suppose the varying quickly component of Equation (12) is removed, Equation (12) consequently becomes

$$LPF\{\hat{g}(t)\} = LPF\{\hat{h}_x(t)\} \quad (13)$$

Equation (13) is mainly determined by the frequency difference Δf and the equivalent impulse response of the transmitter of the tag $h_x(t)$.

The frequency of RFID DF identification system f_c is predefined based on the proximate coupling RFID standard and fixed for all tags to be identified; however, Δf is the actual frequency difference between the tag to be identified and f_c, which is unique for each tag. The equivalent impulse response of the tag to be identified $h_x(t)$ is also unique as it is determined by the hardware of the transmitter of the tag. Therefore, Equation (13) can be used as a kind of DF, called cepstrum DF, for the identification of proximity coupling RFID tags. With above analyses, the impacts of the transmitted digital baseband signal is eliminated from cepstrum DF which is consequently mainly determined by the hardware property of the transmitter part of tag to be identified, so cepstrum DF is time invariant and robust theoretically.

B. Numerical simulation

With a RF oscillograph, a vector signal generator, an antennas and computers, etc., the numerical simulations are done. Agilent's E4438C VSG connected with an antenna is used to generate random frames of BPSK RF signal, the carrier frequency is set to 2.412GHz, power is set to the maximum 20dBm, and the binary data rate is 11Mbps. The RF oscilloscope 54854A connected with a antenna is used to acquire the transmitted RF signals, and the sampling rate is set to 10GSps[5].

One hundred of BPSK RF signals are acquired and processed with Matlab to normalize, down-convert, low-pass filter, and with Simulink to obtain the baseband signal $r_i(n)$ and $r_q(n)$.

The cepstrum of $r_i(n)$, or $\hat{r}_i(n)$, is then obtained, and the superposed graph of the heads of 100 $\hat{r}_i(n)$ samples is illustrated as Fig. 4. With Fig. 4, it can be seen that $\hat{r}_i(n)$ is mainly composed of the low-time components, the random vary-quickly components, and the periodic components; and the period of the periodic components is coincident with that of the baseband signal.

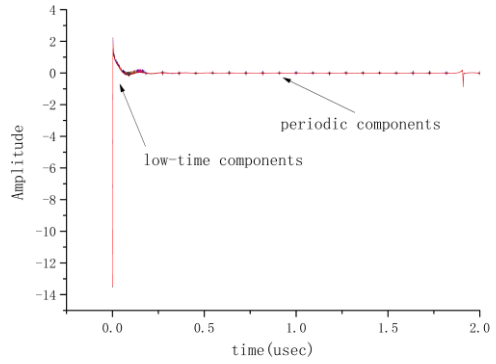

Fig. 4 Superposed graph of the heads of 100 $\hat{r}_i(n)$ samples

The 100 $\hat{r}_i(n)$ samples are then low pass filtered with a easy FIR low pass filter. The truncated head signals are the cepstrum DF, which are denoted as $LPF\{\hat{r}_i(n)\}$. One hundred samples of $LPF\{\hat{r}_i(n)\}$ are illustrated in Fig. 5.

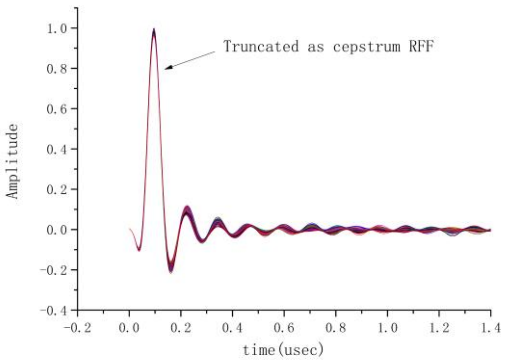

Fig. 5 Superposed graph of the 100 $LPF\{\hat{r}_i(n)\}$ samples

With Fig.5 it can be seen that almost all vary-quickly components of $\hat{r}_i(n)$ have been removed from the cepstrum DF, and the 100 $LPF\{\hat{r}_i(n)\}$ samples demonstrate good robustness.

IV. EXPERIMENTAL RESULTS

A RFID DF identification system used for the acquisition of ISO standard 14443A RFID tag signals and the corresponding DF transformation was constructed. A RFID reader was installed in a computer. The reader transmitted packets at regular intervals. An Agilent DSO91304A oscilloscope connected to a high gain 13.56MHz antenna was used to acquire the signals responded from the RFID tag. The distance between the tag and the reader was kept constant. The sample rate of DSO91304A was 500MSps, and the acquired signal was then processed with Matlab and a computer.

Process the acquired RFID tag signals according to the proposed transform method of cepstrum DF, A RF signal sample of the tag to be identified and the according middle results were illustrated in Fig. 6.

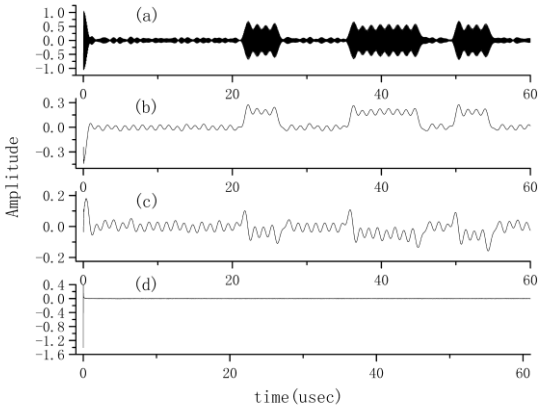

Fig. 6 One RF signal sample of ISO 14443A tag and its intermediate results

Sub-graph (a) was the obtained lower-sideband signal $s(t)$, sub-graph (b) and (c) were the obtained signal $i_{IF}(t)$ and $q_{IF}(t)$ respectively, sub-graph (d) was the signal $\hat{g}(t)$, and the signal $LPF\{\hat{g}(t)\}$ was omitted, truncate the start part of $LPF\{\hat{g}(t)\}$ as the proposed cepstrum DF.

Three tags, denoted as PICC-1, PICC-2, and PICC-3 respectively, were chosen for experiments. One hundred of Cepstrum DF from each tag were obtained during 3 months span. The 300 Cepstrum DF of the 3 tags were then processed to obtain features according to the proposed transform method of cepstrum DF.

The resemblance coefficient feature vector [C_{r1}, C_{r2}] were then extracted from cepstrum DF as

$$C_{r1} = \frac{\sum U(n) \cdot LPF\{\hat{h}_x(n)\}}{\sqrt{\sum U^2(n)} \cdot \sqrt{\sum LPF^2\{\hat{h}_x(t)\}}} \tag{14}$$

and

$$C_{r2} = \frac{\sum T(n) \cdot LPF\{\hat{h}_x(t)\}}{\sqrt{\sum T^2(n)} \cdot \sqrt{\sum LPF^2\{\hat{h}_x(t)\}}} \tag{15}$$

where $U(n)$ in equation (14) and $T(n)$ in equation (15) were rectangular and triangular base signal, respectively. The resemblance coefficient feature vector [C_{r1}, C_{r2}] were then fed into the k-nearest neighbor (k-NN) classifier with no rejection option. The k feature vectors were selected randomly from the 100 feature vectors of each cepstrum DF as the training database, and 10-k feature vectors were selected randomly from the remaining 100-k feature vectors of the cepstrum DF as the testing database, the identification rate of the 3 tags were 74.07% (k =1), 83.33% (k =2), 95.20% (k =3) and 100.00% (k =4) respectively.

It can be seen that excellent identification performance can be achieved with the proposed cepstrum DF.

V. CONCLUSIONS

In this study, a novel type of DF called Cepstrum DF for the identification of proximity coupling RFID tags is proposed. Analyses and simulation based on the built RFID DF identification system model reveal that the propose DF is mainly determined by the hardware property of the tag to be identified, and experiments with three ISO 14443 RFID tags demonstrate the good uniqueness and stability of the proposed DF.

Although the tags used in experiments are chosen, and the discriminability and stability of the other tags may not good. The proposed DF is still a potential DF for the fusion identification of proximity coupling RFID tags with multiple kinds of DF.

ACKNOWLEDGMENT

The Science and Technology Project of Ministry of Transport of China under Grant 2012-319-813-270; the Jiangsu Provincial Government Overseas Scholarship (2012); the Nantong University Doctor Foundation (2013).

REFERENCES

[1] C. Bertoncini, K. Rudd, B. Nousain, and M. Hinders, "Wavelet Fingerprinting of Radio-Frequency Identification (RFID) Tags[J]," IEEE Transactions on Industrial Electronics, vol. 59, pp. 4843-4850, 2012.

[2] YUAN Hong-lin, and HU Ai-qun, "Preamble-based detection of Wi-Fi transmitter RF fingerprints," Electronics Letters, vol. 46, pp. 1165-1167, 2010.

[3] Bayat, S., Louie, R.H.Y., Zhu Han, Vucetic, B., and Yonghui Li, "Physical-Layer Security in Distributed Wireless Networks Using Matching Theory," IEEE Transactions on Information Forensics and Security, vol. 8, pp. 717-732, 2013.

[4] Khor J. H, Ismail W, Younis M. I, et al., "Security Problems in an RFID System," Wireless Personal Communication, vol. 59, pp.17-26, 2011.

[5] H.L Yuan, etc., "Robust Cepstrum RF Fingerprint Transformed from BPSK Signal," Przeglad E, vol. 20131b, pp. 193-195, 2013.