Power Ramped-up Preamble RF Fingerprints of Wireless Transmitters

Honglin YUAN[1,2], *Zhihua BAO*[1], *Aiqun HU*[2]

[1] School of Electronics and Information, Nantong University, Road Seyuan 9, 226019 City Nantong, Province Jiangsu, P. R. China
[2] School of Information Science and Engineering, Southeast University, Sipailou 2, 210096 City Nanjing, Province Jiangsu, P. R. China

ntusignal@gmail.com, bao.zh@ntu.edu.cn, aqhu@seu.edu.cn

Abstract. *In this paper, we propose a novel kind of RF fingerprints (RFF) with better discriminability than typical RFF for identifying preamble-based wireless transmitters. First, the equivalent model of RFF identification system is built. Then, the typical RFF are analyzed with the built model and the novel RFF, which is transformed from preamble signal when its power is ramped up, is presented. Finally, the discriminability of the proposed RFF and typical RFF is experimentally evaluated with Wi-Fi 802.11b devices. The proposed RFF can be integrated into fusion identification of preamble-based wireless devices with multiple RFF.*

Keywords

Non-cryptographic authentication, hardware security, device identification, RF fingerprints, power ramped-up, fusion identification, RF fingerprinting, transmitter identification.

1. Introduction

Non-cryptographic authentication and identification are attracting more attention owing to the more security threats in wireless networks [1]. Identifying wireless devices according to their RF fingerprints (RFF) to control their access, which is a method of non-cryptographic authentication, had been proposed for enhancing the physical layer security of wireless networks [2]. Although it was reported that RFF is vulnerable to impersonation attacks when the attacker is equipped with high-end instruments [3], this situation is not common as the attack cost is very high; RFF has also been presented to be used for building cross layer signatures of wireless networks [1].

RFF is the transformation of a received radio signal that carries the hardware information of the transmitter part of the radio to be identified [4], which embodies the hardware characteristics of the transmitter part and is comparable. Turn-on RFF and steady-state RFF are two kinds of typical RFF. Turn-on RFF is transformed from the transient of the received signal when the transmitter is powered-up in step mode [5]. As the transient of the received signal is generally extremely short, the demanded sampling rate is normally very high. It was pointed out that the application of turn-on RFF is limited because its demanding sampling rate is usually several giga samples per second (GSps) [6].

Steady-state RFF which is transformed from the received steady-state wireless signal was proposed recently with hardware experiments [6] - [8], such as the spectrum of the UMTS and Wi-Fi 802.11a OFDM preamble, the frequency offset, and the modulation domain parameters of the modulated signal etc. Although the experiments had presented that good identification rates were achieved with normal sampling rate, adverse factors such as the time-variant wireless channel and the orientation of antenna etc. had not been thoroughly investigated.

In addition, it is common that abundant wireless devices with same manufacturer/same model exist in one network, which makes their RFF's discriminability that can be measured by the inter-class distance of RFF bad. So, identifying wireless devices with RFF remains an arduous task. And more kinds of RFF that carry more hardware information of the transmitter to be identified are needed for fusion identification [9] of the wireless transmitter, a possible structure of fusion identification of wireless transmitter with multiple RFF is shown in Fig. 1.

We present a new kind of RFF with good discriminability in this paper. The rest of this paper is organized as follows: Section 2 builds an equivalent model of RFF identification system, the foundation and discriminability of RFF are then explained with the built model. In Section 3, we firstly analyze the typical RFF, turn-on RFF and steady-state RFF, with the built model. A novel RFF called ramped-up preamble RFF is then proposed. And their discriminability is compared with the built model. Section 4 presents the experiments with a few wireless network interface cards (NIC) which verified the analysis results on the discriminability of RFF with the built model. The last section is the conclusion of this paper.

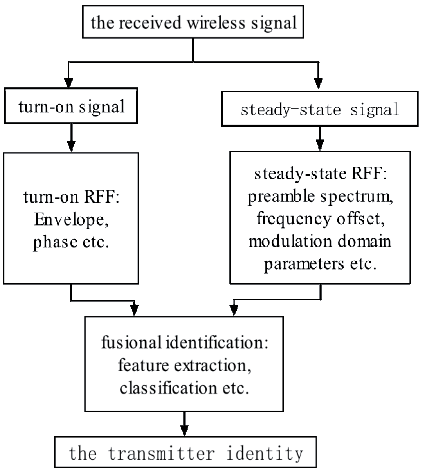
the received wireless signal
turn-on signal
steady-state signal
turn-on RFF: Envelope, phase etc.
steady-state RFF: preamble spectrum, frequency offset, modulation domain parameters etc.
fusional identification: feature extraction, classification etc.
the transmitter identity

Fig. 1. A kind of possible structure of fusion identification of wireless transmitter with multiple RFF.

2. Equivalent Model of RFF Identification System

The equivalent model of RFF identification system is illustrated in Fig. 2, where $m(t)$ is the equivalence of the baseband signal of the transmitter to be identified; $h_{tx}(t)$ and $h_{rcv}(t)$ are equivalent linear impulse responses of the transmitter to be identified and the receiver of RFF identification system respectively, and the $h_{tx}(t)$ is determined by the structure of the linear-part of the transmitter and the actual values of its internal components V_i, $i = 1, 2, 3...$; $g[\bullet]$ is the equivalent input-output relationship of the nonlinear-part of the transmitter, which is determined by its structure and the actual values of its components V_j, $j = 1, 2, 3...$; $s(t)$ is the transmitted signal; $h_{ch}(t)$ is the equivalent impulse response of wireless channel; $n(t)$ is the equivalent AWGN of RFF identification system which is mainly caused by low noise amplifier [10]; $r(t)$ is the received signal; and $T\{r(t)\}$ is the transform of the received signal $r(t)$.

Then, the transmitted signal

$$s(t) = g[m(t) * h_{tx}(t)] \tag{1}$$

where * denotes convolution operation; the received signal

$$r(t) = [s(t) * h_{ch}(t) + n(t)] * h_{rcv}(t) \tag{2}$$

and the transform of *r(t)* can be expressed as

$$\begin{aligned} T\{r(t)\} &= F_1\{m(t), h_{tx}(t), g[\bullet], h_{ch}(t), n(t), h_{rcv}(t)\} \\ &= F_2\{m(t), V_i, V_j, h_{ch}(t), n(t), h_{rcv}(t)\} \end{aligned} \tag{3}$$

where F_1, F_2, and F_k, $k = 3,4,5,6,7$ in the following denote definite functions respectively.

When the ideal transform $T\{\bullet\}$ makes the $T\{r(t)\}$ a function only of V_i, $i = 1, 2, 3...$ and V_j, $j = 1, 2, 3...$, and the $T\{r(t)\}$of different wireless transmitters are comparable, the $T\{r(t)\}$ can serve as RFF for identification of the wireless transmitters. The existence of component tolerances makes the V_i and V_j of different wireless transmitters unique, the RFF of the wireless transmitters are consequently unique. And it is not difficult to understand that the discriminability of RFF, which is generally in digital domain, is determined by the component tolerances property of the transmitter to be identified, the discrete samples of the received wireless signal used for transform of RFF etc., where the more discrete samples of the signal used for transform of RFF, the more hardware information may be transferred to the transformed RFF.

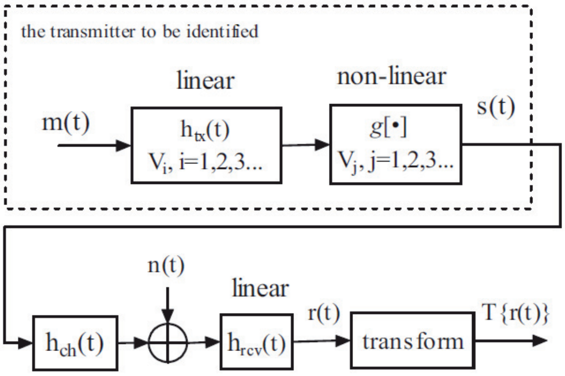

Fig. 2. Equivalent model of RFF identification system.

3. Analyses of RFF

Suppose that the ideal RFF transform removes the impacts of the $h_{ch}(t)$, $n(t)$, and $h_{rcv}(t)$ in equation (3), then the $T\{r(t)\}$ is a function only of $m(t)$, V_i and V_j which can be written as

$$T\{r(t)\} = F_3\{m(t), V_i, V_j\} . \tag{4}$$

3.1 Typical Turn-on and Steady-state RFF

Typical turn-on RFF can be written as the transforms of the transient of the received signal $r(t)$, where the $m(t)$ is equivalent to unit step excitation $u(t)$ or the wireless transmitter reaches its rating power in step mode, which can be written as

$$T\{r(t)\} = F_4\{u(t), V_i, V_j\} . \tag{5}$$

As $u(t)$ in (5) of different transmitters are comparable and the V_i and V_j are uniquely determined by the structure and actual component values of the transmitter, the equations (5) of different transmitters embody their hardware property and are comparable, which can serve as one kind of RFF, called turn-on RFF, for identification of the transmitters.

In a similar way, typical steady-state RFF can be written as the transforms of the received signal $r(t)$, where the exciting $m(t)$ in (4) is the transmitted preamble signal $p(t)$ that are comparable, which can be written as

$$T\{r(t)\} = F_5\{p(t), V_i, V_j\} \, . \tag{6}$$

Comparing equations (6) and (5), it can be seen that the influencing factors of steady-state RFF are not more than that of turn-on RFF. However, the signal duration of steady-state RFF can be significantly longer than that of turn-on RFF; Under the circumstance that the sampling rates are the same, the hardware information carried by steady-state RFF can be significantly more than that carried by turn-on RFF with more discrete samples of the received wireless signal used for RFF transform.

Thus, the discriminability of steady-state RFF outperforms that of turn-on RFF, which conforms to the experimental results in literature [6], [7], [8].

3.2 The Proposed Ramped-up Preamble RFF

The power ramp-up control of wireless transmitters can ensure that power is not spread to adjacent frequency channels [11], and preamble is usually used for synchronization in modern wireless communications. When the power control mode of wireless transmitters is ramp-up and the transmission of preamble is initiated immediately when the power amplifier is ramped on, suppose that the $m(t)$ in equation (4) when its power is ramped up is equivalent to

$$m(t) = ramp(t) \bullet p_1(t) \tag{7}$$

where the $ramp(t)$ in (7) is the equivalent amplitude ramp-up function and the $p_1(t)$ is the preamble head when its power is ramped up, as the $ramp(t)$ in (7) is deter-mined by the structure of the ramp-up control hardware and the actual values of its internal components V_k, $k = 1, 2, 3 \ldots$, (4) can be written as

$$\begin{aligned} T\{r(t)\} &= F_6\{ramp(t), p_1(t), V_i, V_j\} \\ &= F_7\{V_k, p_1(t), V_i, V_j\} . \end{aligned} \tag{8}$$

As the preamble head $p_1(t)$ in (8) is comparable, and the V_k, V_i, and V_j in (8) are determined by the hardware property of the transmitter, (8) can serve as a novel kind of RFF, called ramped-up preamble RFF, for identification of preamble-based wireless transmitters. With the above analyses, it can be seen that the ramped-up preamble RFF is substantially a hybrid turn-on RFF.

Comparing (8) and (5), we can see that the influencing factors of ramped-up preamble RFF are more than that of turn-on RFF at power ramp-up control parameters V_k in RF band, while a slight difference of actual component values in RF band caused by component tolerances has a big impact on the transmitted signal. And the signal duration of ramped-up preamble RFF is longer than the transient of turn-on RFF, under the circumstance that the sampling rates are the same, the hardware information carried by ramped-up preamble RFF can be greatly more than that carried by turn-on RFF with more discrete samples of the received wireless signal used for RFF transform. So, the discriminability of ramped-up preamble RFF outperforms that of turn-on RFF.

Comparing Equation (8) and (6), we can see that the influencing factors of ramped-up preamble RFF are more than that of steady-state RFF at power ramp-up control parameters V_k in RF band. So, in the case that the duration of $p_1(t)$ in (8) is equal to that of $p(t)$ in (6) and the sampling rates are the same, the discriminability of ramped-up preamble RFF is better than that of typical steady-state RFF.

4. Experiments and Results

An RF signal collection and process system, shown in Fig. 3, was designed to analysis the preamble signal of Wi-Fi 802.11b USB NIC.

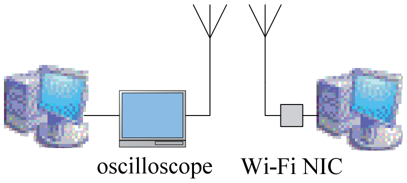

Fig. 3. Wi-Fi 802.11b RF signal collection and process system.

The NIC in Fig. 3 was installed in computer and set to ad-hoc networking mode on radio channel at 2.412 GHz. The NIC transmitted packets at regular intervals to announce its presence, and its power control mode was set as continuous access and its preamble type was set as short. An Agilent RF oscilloscope 91304A, whose sampling rate was set to 10 GSps and was connected with a high-gain antenna, was used to acquire the transmitted RF packets. The distance between the transmitting and the receiving antennas was about 10 cm long. The indoor temperature and humidity were kept constant, and electromagnetic shielding was provided.

The RF packets of each NIC were acquired and processed with MATLAB (normalized, down-converted, band-pass filter) and Simulink (Costas PLL demodulation) to obtain their preamble baseband signals $r_i(n)$ and $r_q(n)$.

The envelope of the received preamble signal, which is not related to PLL transients, was used as an instance of these RFF whose transform is given by

$$e(n) = \sqrt{r_i(n)^2 + r_q(n)^2} \, . \tag{9}$$

As the DSSS-preamble of Wi-Fi 802.11b/g is specified to use the 1-Mbit/s Barker Code (10110111000) spreading with DBPSK modulation [12], the envelope $e(n)$ is periodic with 1 μsec period and the shape of its fundamental period is unaltered and identical. The reference instant of $e(n)$, used for RFF alignment and denoted as P_{ref}, was obtained according to literature [4], which is the starting instant of the first complete Barker code envelope of $e(n)$.

Each NIC is a class. The mean of one kind of RFF from each NIC is denoted as column vector $\mathbf{u}_i$ where $i = 1, 2, 3 \ldots$ denotes different NIC. Then the global mean vector of the RFF from m NIC is given by

$$\mathbf{u}_0 = \sum_{i=1}^{m} P_i \bullet \mathbf{u}_i \tag{10}$$

where P_i is the a priori probability of NIC i. That is, $Pi \cong n_i / N$, where n_i is the number of the RFF in NIC i, out of a total of N RFF [13]. Then the between-class scatter matrix of the RFF from all NIC is given by

$$\mathbf{S}_b = \sum_{i=1}^{m} P_i \bullet (\mathbf{u}_i - \mathbf{u}_0) \bullet (\mathbf{u}_i - \mathbf{u}_0)^T \tag{11}$$

where T in equation (11) denotes transpose operation. Then the discriminability of the RFF can be measured by the trace of $\mathbf{S}_b$, denoted as $tr\{\mathbf{S}_b\}$, which is a measure of the average (over all classes) distance of the mean of each individual class from the respective global value [13]. Thus, the bigger the $tr\{\mathbf{S}_b\}$, the better the discriminability of the RFF.

Although it is easy to compare the discriminability of ramped-up preamble RFF with that of turn-on RFF using the built model, the corresponding experiences is difficult. Because an actual specific transmitter has only one specific power up mode, and the component tolerance properties of transmitters with different power up modes are generally different, which does not make the discriminability comparison between ramped-up preamble RFF and turn-on RFF meaningful strictly. So, experiments in this paper compare the discriminability of these RFF using Wi-Fi 802.11b NIC with different power up modes in a strict and a rough fashion respectively.

4.1 The Discriminability Comparison of the Proposed RFF with Steady-state RFF

Eighteen D-Link AirPlus USB Wi-Fi 802.11b NIC with continuous series numbers, which transmit their preamble immediately when their power amplifier is ramped on, were used for comparison of the discriminability between the proposed ramped-up preamble RFF and the typical steady-state RFF.

As shown in sub-graph NIC-A of Fig. 4, the received preamble signal envelopes *e(n)* were aligned with the detected reference instants P_{ref}, and the *e(n)* truncated from P_{ref} backward for the duration of 1 µs serves as the envelope ramped-up preamble RFF, called ERUP-RFF for short, and the *e(n)* truncated from P_{ref} forward for the same length duration serves as the envelope steady-state RFF, called ESS-RFF for short, in this experiments.

Decoding analysis of the received preamble baseband signal according to the IEEE 802.11b standard showed that: Firstly, two or three complete symbols on the head of the preamble signal are “eaten” during the power is ramped up and, secondly, the following decoded preamble codes conform to the IEEE standard. Hence, the ERUP-RFF is the envelope of the residual Barker code when the preamble signal power is ramped-up.

With manual observation, some big differences are found existing among the ERUP-RFF of different cards and the ERUP-RFF of the 18 cards can be classified into 5 sub-classes denoted to as A, B, C, D, E respectively. The card numbers of each ERUP-RFF subclass are illustrated in Tab. 1.

ERUP-RFF subclass	A	B	C	D	E
number of cards	3	5	4	2	4

Tab. 1. Card numbers of each ERUP-RFF subclass.

Five cards, denoted to as NIC-A, NIC-B, NIC-C, NIC-D, and NIC-E respectively, were chosen from the 5 ERUP-RFF subclass cards, each from one subclass, for further experiments. Fifty preamble head envelopes $e(n)$ from each card were acquired during 5 months span, 10 $e(n)$ each month, for investigating their stability. The 250 ERUP-RFF and 50 ESS-RFF of the 5 cards truncated from the obtained $e(n)$ are shown in Fig. 4.

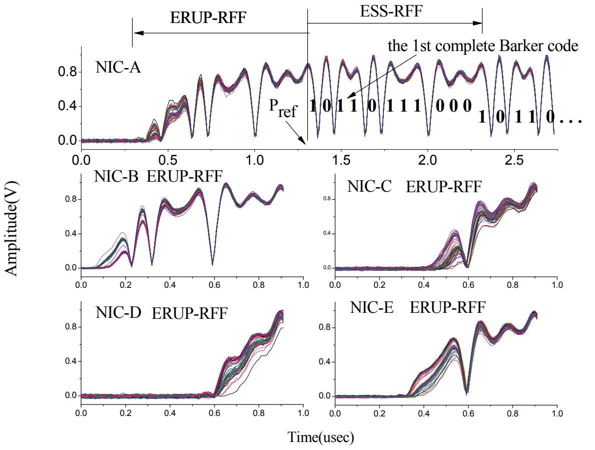

Fig. 4. Aligned ERUP-RFF and ESS-RFF from 5 cards.

As shown in Fig. 4, sub-graph NIC-A illustrates 50 $e(n)$ from NIC-A card aligned with their reference instants P_{ref}, which included the ERUP-RFF and the ESS-RFF. The other 4 sub-graphs, denoted as NIC-B, NIC-C, NIC-D and NIC-E, illustrated 200 ERUP-RFF from the other 4 cards, 50 ERUP-RFF from each card, respectively.

The ERUP-RFF and ESS-RFF of the 5 cards were down-sampled and their discriminability were calculated as $20 \log[tr\{\mathbf{S}_b\}]$, which were shown in Fig. 5 where $m = 5$, $n_i = 50$ and $N = 250$.

It can be observed from Fig. 5 that the discriminability of the two RFF becomes better when the sampling rate becomes higher; for a specific sampling rate, the discriminability of the envelope ramped-up preamble RFF (ERUP-RFF) outperforms that of the envelope steady-state RFF (ESS-RFF) where their signal durations are equal, which conforms to the analysis results based on the built model.

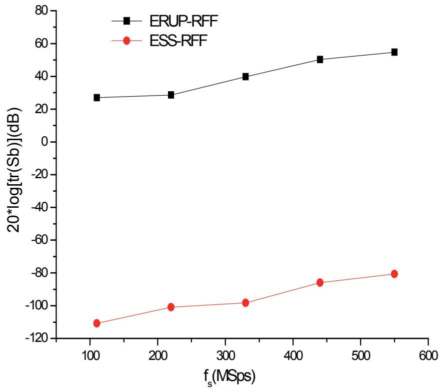

Fig. 5. The discriminability measure 20*log[$tr\{\mathbf{S}_b\}$] versus sampling rate f_s for the two kinds of RFF.

The classification experiments of the two RFF were carried out. The RFF with a sampling rate of 110 MSps were obtained and added with AWGN noise to make their SNR 20 dB, which were denoted as *erff*(n). The resemblance coefficient feature vector [C_{r1}, C_{r2}] [14] was extracted from *erff*(n) as

$$C_{r1}=\frac{\sum U(n)\bullet erff(n)}{\sqrt{\sum U^2(n)}\bullet\sqrt{\sum erff^2(n)}} \qquad (12)$$

and

$$C_{r2}=\frac{\sum T(n)\bullet erff(n)}{\sqrt{\sum T^2(n)}\bullet\sqrt{\sum erff^2(n)}} \qquad (13)$$

where $U(n)$ in (12) and $T(n)$ in (13) are the rectangular and the triangular signal respectively with the same length as *erff*(n). The resemblance coefficient feature vector [C_{r1}, C_{r2}] was then fed into the k-nearest neighbor (k-NN) classifier with no rejection option. The k feature vectors were selected randomly from the 50 feature vectors of each NIC as the training database, 10-k feature vectors were selected randomly from the remaining 50-k feature vectors of the NIC as the testing database, and the identification rate of the 5 NIC with the EURP-RFF and ESS-RFF was illustrated in Tab. 2 where k is 1, 2, 3 and 4 respectively.

k-NN RFF	1-NN(%)	2-NN(%)	3-NN(%)	4-NN(%)
EURP-RFF	97.78	100.00	100.00	100.00
ESS-RFF	17.78	27.50	28.57	23.33

Tab. 2. Results of the k-NN classifier when the sampling rate is 110 MSps.

It can be seen from Tab. 2, with conventional sampling rate, that excellent identification performance can be achieved with the envelope ramped-up RFF (ERUP-RFF) while the identification performance with the envelope steady-state RFF (ESS-RFF) whose signal duration is same as that of ERUP-RFF is not practical.

4.2 The Discriminability Comparison of Steady-state RFF with Turn-on RFF

Five Segment USB Wi-Fi 802.11b NIC with continuous series numbers, which reach their rating power in step mode – do not agree with the standard, were used for comparison of the discriminability between typical turn-on RFF and steady-state RFF.

The preamble signal of the 5 NIC were acquired with the Wi-Fi 802.11b RF signal collection and processed by a system shown as Fig. 3. The envelope of the preamble signal from the 5 NIC were then obtained and aligned with the detected reference instances P_{ref}. The 50 aligned preamble head envelopes from each card were shown in Fig. 6 as NIC-1, NIC-2, NIC-3, NIC-4, and NIC-5 respectively.

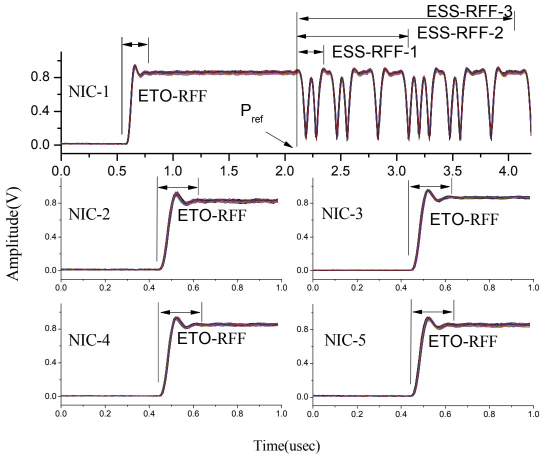

Fig. 6. The aligned preamble head envelopes from 5 NIC.

As illustrated in Fig. 6, the envelope truncated from P_{ref} forward for the durations of 0.2 μs, 1 μs and 2 μs long serves as envelope steady-state RFF which are denoted to and called as ESS-RFF-1, ESS-RFF-2, and ESS-RFF-3 for short respectively. The envelope turn-on RFF, called ETO-RFF for short, shown in Fig. 6, are truncated from the aligned envelopes for duration of 0.2 with manual observation.

The ESS-RFF-i ($i = 1, 2, 3$) and ETO-RFF of the 5 NIC were down-sampled and their discriminability were calculated as 20 log[$tr\{\mathbf{S}_b\}$], which were shown in Fig. 7 where m = 5, n_i = 50 and N = 250.

It can be seen from Fig. 7 that the discriminability of envelop steady-state RFF (ESS-RFF-1) is unexpectedly slightly poorer than that of envelop turn-on RFF (ETO-RFF). The reason is probably that their time intervals are too short. However, as the signal duration gets longer, the discriminability of ESS-RFF (ESS-RFF-2,3) gets a little better than that of ETO-RFF.

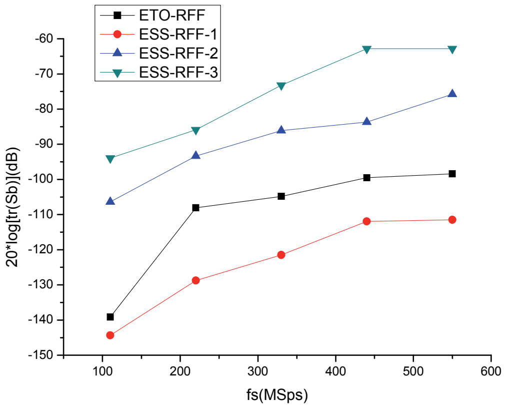

Fig. 7. The discriminability measure 20*log[$tr\{\mathbf{S}_b\}$] versus sampling rate f_s for the 4 RFF.

Furthermore, when Fig. 7 was compared to Fig. 5, it can be deduced in a rough fashion that the discriminability of the envelope ramped-up preamble RFF (ERUP-RFF) significantly outperforms that of the other RFF as the component tolerances properties of different Wi-Fi 802.11b NIC are similar.

5. Conclusions

In this study, we have proposed a novel type of RFF called ramped-up preamble RFF which is a hybrid turn-on RFF in nature. Analyses based on the built RFF identification system model demonstrated that the discriminability of the proposed RFF outperforms that of the typical turn-on RFF and steady-state RFF, and experiments with several Wi-Fi 802.11b NIC verified the analysis results based on the built model.

Although it is impossible to obtain the excellent identification performance when identifying any wireless transmitters with the proposed ramped-up preamble RFF, the excellent discriminability of the proposed RFF make it a good potential RFF for fusion identification of preamble-based wireless transmitters with multiple RFF.

The generating technique of the proposed ramped-up preamble RFF, which is initiating transmission of preamble immediately when the power amplifier is ramped-on, can be applied to the design and manufacturing of wireless devices, and can be recommended into the standards of the related wireless devices.

Acknowledgements

This work was supported by the project of National Natural Science Foundation of China “Energy detection algorithm of cognitive radio based on relay cooperation (61071086)”.

Also thanks the reviewers for their labors on this paper and the K2009001 Nantong Foundation of China.

References

[1] KAI ZENG, GOVINDAN, K., MOHAPATRA, P. Non-cryptographic authentication and identification in wireless networks. *IEEE Wireless Communications*, 2010, vol. 17, no. 5, p. 56 - 62.

[2] KLEIN, R. W., TEMPLE, M. A., MENDENHALL, M. J. Application of wavelet denoising to improve OFDM-based signal detection and classification. *Security and Communication Networks*, 2010, vol. 3, no. 1, p. 71 - 82.

[3] DANEV, B., LUECKEN, H., CAPKUN, S., EL DEFRAWY, K. Attacks on physical-layer identification. In *Proceedings on the Third ACM Conference on Wireless Network Security*. Hoboken (USA), 2010, p. 89 - 98.

[4] YUAN, H. L., HU, A. Q. Preamble-based detection of Wi-Fi transmitter RF fingerprints. *Electronics Letters*, 2010, vol. 46, no. 16, p. 1165 - 1167.

[5] DANEV, B., CAPKUN, S. Transient-based Identification of Wireless Sensor Nodes. In *International Conference on Information Processing in Sensor Networks*. San Francisco (California, USA), 2009, p. 25 - 36.

[6] KENNEDY, I. O., SCANLON, P., BUDDHIKOT, M. M. Passive steady state RF fingerprinting: A cognitive technique for scalable deployment of co-channel femto cell underlays. In *3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*. Chicago (USA), 2008, p. 1 - 12.

[7] BRIK, V., BANERJEE, S., GRUTESER, M., OH, S. Wireless device identification with radiometric signatures. In *14th ACM International Conference on Mobile Computing and Networking*. San Francisco (USA), 2008, p. 116 - 127.

[8] CANDORE, A., KOCABAS, O., KOUSHANFAR, F. Robust stable radiometric fingerprinting for wireless devices. In *IEEE International Workshop on Hardware-Oriented Security and Trust*. San Fran-cisco (USA), 2009, p. 43 - 49.

[9] TALBOT, K. I., DULEY, P. R., HYATT, M. H. Specific emitter identification and verification. *Technology Review Journal*, 2003, p.113-133.

[10] BARAN, O., KASAL, M., Modeling of the phase noise in space communication systems. *Radioengineering*, 2010, vol. 19, no. 1, p. 141 - 148.

[11] URETEN, O., SERINKEN, N. Wireless security through RF fingerprinting. *Canadian Journal of Electrical and Computer Engineering*, 2007, vol. 32, no. 1, p. 27 - 33.

[12] *IEEE Std. 802.11-2007 (Revision of IEEE Std 802.11-1999)*. IEEE, 2007, p. C1-1184.

[13] THEODORIDIS, S., KOUTROUMBAS, K. *Pattern Recognition*. 4th ed. Academic Press, 2008.

[14] ZHANG, G., JIN, W., HU, L. Resemblance coefficient based intrapulse feature extraction approach for radar emitter signals. *Chinese Journal of Electronics*, 2005, vol. 14, p. 337 - 340.

About Authors ...

Honglin YUAN received the Master degree in 2003 from the Guilin Electronic Technology University, Department of Electronic Engineering, Guilin, Guangxi Autonomous Region, China. In 2011, he finished the study for a Ph.D. degree at the School of Information Science and Engineering, Southeast University, China. His research interests are signal processing and pattern classification.

Zhihua BAO was born in Nantong City, Jiangsu Province, China, in 1955. He received the Master degree from the

Nanjing University of Posts and Telecommunications, Jiangsu Province, China. He is Professor at the School of Electronics and Information, Nantong University, China. His research is concentrated on cognitive radio, radio circuit design and radio transmitter identification.

Aiqun HU is Professor at the School of Information Science and Engineering, Southeast University, China. He received the Ph.D. degree from Southeast University, China, in 1993. His research area includes wireless communication and information security.