Effect of Sampling Rate on Transient Based RF Fingerprinting

Selçuk Taşcıoğlu[1], Memduh Köse[2], and Ziya Telatar[1]

[1]Department of Electrical and Electronics Engineering
Ankara University
selcuk.tascioglu@eng.ankara.edu.tr, ziya.telatar@ankara.edu.tr

[2]Computer Sciences Research and Application Center
Ahi Evran University
memduh.kose@ahievran.edu.tr

Abstract

In this paper, effect of sampling rate on the performance of transmitter identification system using transient-based RF fingerprints is considered. Two different existing RF fingerprinting techniques have been employed to investigate the performance of a transmitter identification system by using experimental data collected at a high sampling rate. Decimation was carried out to analyze the effect of lower sampling rates. It has been shown that transient-based RF fingerprinting methods can be effectively used for identification of wireless transmitters at low sampling rates.

1. Introduction

RF fingerprints are defined as the unique characteristics of transmitters caused by their radio circuitry. These unique characteristics can be employed for the identification of wireless devices. RF fingerprinting methods have been employed for identification of several wireless devices, e.g. VHF transmitters [1]-[3], WiFi [4]-[8] and UMTS [9], [10] transceivers. An overview of transmitter identification systems based on RF fingerprinting is presented in [11].

The main stages of an identification system based on RF fingerprinting are defined as signal detection, feature extraction, and classification. After detecting identification signals, such as transients and preambles, from the transmitted signals, distinctive features are extracted from the detected signals and employed to classify transmitters. The identification systems using steady state characteristics such as preambles can exploit the prior information about the known signals. On the other hand, the identification systems using transient characteristics have the advantage that the unintended transients are transmitted before settling down to a steady state condition for all types of wireless devices. In [9], transient-based RF fingerprinting methods are claimed to require extremely high sampling rates to extract features from transient signals without providing experimental or simulation results. This has been regarded as a major disadvantage of the transient based RF fingerprinting methods in [10], [12], [13]. In [12], transient detection stage, as well as feature extraction stage, is claimed to require high sampling rate due to its relatively small duration compared to steady state signal regions. However, none of these works deals with verifying the claim about the high sampling rate requirement of transient based RF fingerprinting methods.

In this paper, effect of sampling rate on the classification performance of a transient-based transmitter identification system is investigated. For this purpose, two different existing RF fingerprinting methods, which are based on instantaneous amplitude responses of turn-on transient signals [4], have been employed. It has been shown through experimental data that, contrary to the claim in the literature, high sampling rate is not a requirement to identify wireless transmitters through transient-based RF fingerprinting.

The organization of the paper is as follows: In Section 2, a brief description of transmitter identification system using transient based RF fingerprints is presented. In Section 3, decimation process applied to experimental data is explained. Performance evaluation results of the transient based RF fingerprinting method at low sampling rates is presented in Section 4. Our comments on the effect of sampling rate on transient based RF fingerprinting are given in Section 5. Finally, section 6 concludes the paper.

2. Transmitter Identification Through Transient Based RF Fingerprinting

The transmitter identification procedure using transient based RF fingerprints is depicted in Fig.1. Sampled baseband signals including transients following channel noise are applied to a detector to find the transient signals. In this study, we used a Bayesian ramp detector [14], to obtain transient signals. This algorithm estimates the transient starting points based on a likelihood function constructed under Gaussian noise assumption. In [15], transient detection performance using this detector was evaluated at different SNR levels and it was demonstrated that the Bayesian ramp detector can be used with a high accuracy for the SNR levels above 10 dB. In the same study, the authors also investigated the effect of detection errors on overall identification system performance for varying SNRs, where SNR levels of transient signals were calculated using the approximation in [16].

In feature extraction stage, we used instantaneous amplitude responses (Amplitude features) [4] and their dimensionally reduced forms obtained by using principal component analysis (PCA features) [4]. At the last stage, a probabilistic neural network (PNN) classifier was used to classify the transmitters by using the extracted features. PNN classifiers have been widely used for classification of transmitters [2], [4], [7], [15]. In [7], the performance of the PNN classifier was compared to a k-nearest neighbor (kNN) classifier in a transmitter classification problem and observed that the PNN classifier outperforms the kNN classifier for varying SNR levels and training sample sizes.

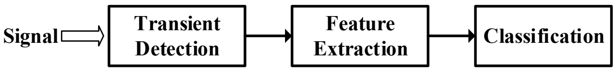


Fig. 1. The procedure for transmitter identification through transient based RF fingerprinting.

3. Decimation Process

Since the main objective of this work is to evaluate the impact of sampling rate on classification performance, sampling rates of data sequences were reduced in the identification process. Decimation is generally defined as the process of low-pass filtering followed by downsampling [17], as depicted in Fig. 2.

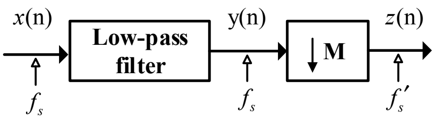


Fig. 2. Block diagram of the decimation process.

Sampling rate of the filtered signal can be reduced as [18]

$$z(n) = y(nM) \tag{1}$$

for an integer downsampling factor M. $z(n)$ represents the signal at the reduced sampling rate, which consists of every Mth samples of the filtered signal. After decimation, sampling rate is given by

$$f_s' = \frac{f_s}{M} \tag{2}$$

where f_s and f_s' denote sampling rates before and after downsampling, respectively.

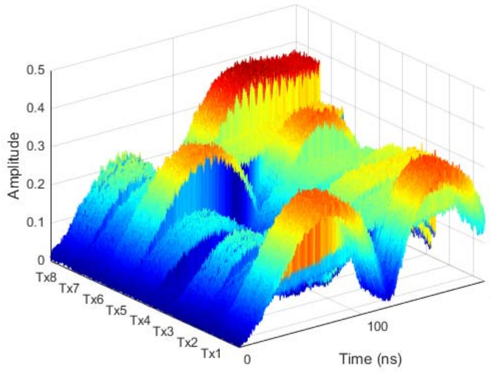
A sixth-order low-pass Butterworth filter with a cutoff frequency of $f_s'/2$ was employed to avoid aliasing. For the sampling rates higher than the Nyquist, this selection of cut off frequency also provides preservation of out-of-band frequency components, i.e. spectral components outside the transmission band, if exist.

The experimental data consist of 100 transmissions from eight different IEEE 802.11b WiFi transmitters. The initial sampling rate of the experimental data is 5 GSamples/s. The downsampling factors and corresponding sampling rates tested in this work is given in Table 1.

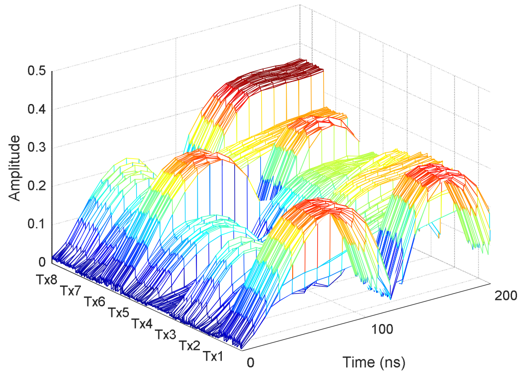
In this study, transient duration is taken as approximately 200ns since this value was found experimentally for WiFi signals in [4]. Therefore, transients are taken as the signal parts of this length following the estimated transients starting points

Table 1. Downsampling factors and corresponding sampling rates

Downsampling factor (M)	2	5	10	25	50	100	180
f_s'	2.5GS/s	1GS/s	500MS/s	200MS/s	100MS/s	50MS/s	28MS/s



(a)



(b)

Fig. 3. Instantaneous amplitudes of transients at sampling rates of (a) 5 GSamples/s and (b) 100MSamples/s from 8 transmitters. 100 transients are shown for each transmitter.

by using the Bayesian ramp detector. Transient signals at sampling rate of 5 GSamples/s are demonstrated in Fig. 3(a). There are 100 transients for each of eight transmitters. In Fig. 3(b), the same transients are shown after decimation process in which downsampling factor was taken as 50, i.e. sampling rate was reduced to 100 MSamples/s. As seen from this figure the impact of the decimation process on instantaneous amplitude responses is not substantial. Therefore, the performance of the classifier based on these responses can be expected to be approximately constant.

The bandwidth of the baseband data from 802.11.b WiFi transmitters is 22 MHz in the range of [-11MHz, 11MHz]. Minimum sampling rate was set to be about 28MS/s as seen in Table 1. This value was chosen to provide the minimum practical sampling rate, which is 2.5 times the maximum frequency component of 11 MHZ in the signal.

4. Performance Evaluation

In order to evaluate the classification performance of the transient-based RF fingerprinting method at low sampling rates, two test scenarios were considered. In the first test scenario, sampling rate reduction was carried out after detecting transient signals at the initial high sampling rate. In the second test scenario, whole identification process was performed at the reduced sampling rates.

In each test scenario, 500 trials were performed to evaluate the classification performance for each sampling rate. Training and test vectors were picked up randomly in each trial to eliminate any selection bias. In each trial, 20 of 100 transients were used as training set. This selection was used since, for a transmitter classification problem in [7], it was demonstrated that increasing the training sample size over 20% of total sample size does not improve the classification performance.

4.1. Test Scenario 1: Decimating Transient Signals

In Test Scenario 1, the main objective is to evaluate the effect of sampling rate on features extracted from the transmitter turn-on transient signals. Therefore, transient detection was performed at the initial high sampling rate and then sampling rate of the detected transient signals was reduced prior to feature extraction. This test scenario is shown in the block diagram in Fig. 4.

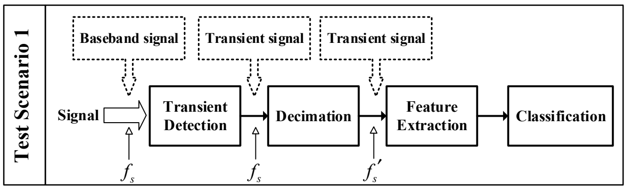


Fig. 4. Test Scenario 1: Decimating transient signals.

4.2. Test Scenario 2: Decimating Baseband Signals

Contrary to Test Scenario 1, overall performance of the transmitter identification system using transient based RF fingerprints was tested for low sampling rates in Test Scenario 2. As shown in the block diagram in Fig. 5, whole identification process, including the transient detection, was performed at the reduced sampling rates.

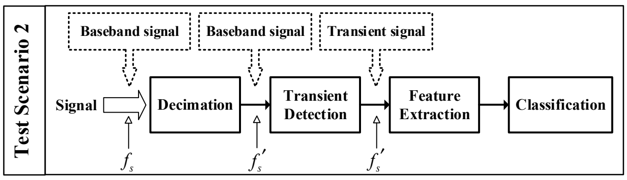


Fig. 5. Test Scenario 2: Decimating baseband signals.

4.3. Classification Test Results

Fig. 6 and Fig. 7 show classification performance evaluation test results over 500 Monte Carlo trials for Amplitude and PCA features, respectively, obtained at different sampling rates.

For Test Scenario 1, average classification accuracies for Amplitude and PCA features are represented by dashed lines with circle markers in Fig. 6(a) and Fig. 7(a), respectively. As seen from these figures, classification accuracy of each feature set remains almost constant at about 98% at the tested sampling rates between 28 MSamples/s and 5 GSamples/s. Correct classification rates of Amplitude and PCA features in Test Scenario 1 are also summarized by boxplot in Fig. 6(b) and Fig. 7(b), respectively. The notches of the boxes in these figure indicate the median values whereas the lower and upper edges of the boxes show the 25th and 75th percentiles, respectively. The dashed lines extend to the most extreme values of correct classification rates. As seen from these figures, variations in median, minimum, 25th and 75th percentiles values of classification results are also small. Test Scenario 1 results show that sampling rate almost does not affect the discrimination capability of the tested transient-based features.

For Test Scenario 2, average classification accuracies are shown by solid lines in Fig. 6(a) and Fig. 7(a). Classification performances of the features in Test Scenario 2 are also demonstrated by boxplot in Fig. 6(c) and Fig. 7(c). Compared to Test Scenario 1 results, the variations in descriptive statistics, such as mean, median, and percentiles, of classification accuracy increase slightly as the sampling rate changes. This is caused by the effect of sampling rate on transient detection algorithm. Note that maximum variation in average classification accuracy of each feature is less than 1% when the sampling rate changes. Besides, when comparing the classification results at the same sampling rate in each test scenario, it is observed that maximum performance loss caused by the effect of sampling rate on transient detection is below 1% for both features. Test Scenario 2 results demonstrate that the Bayesian ramp detector performs well at low sampling rates.

From Fig. 6(a) and Fig. 7(a), the average classification accuracies of Amplitude and PCA features at all sampling rates were obtained over 97.7% and 97.5% in Test Scenario 1 and Test Scenario 2, respectively. Overall, the results in both cases indicate that the transient-based RF fingerprinting method considered in this work can be effectively used for identification of WiFi transmitters at low sampling rates.

In addition, when comparing the results in Fig. 6 and Fig. 7, it is clear that dimension reduction for Amplitude features using PCA does not cause any performance loss. Actually, this result was obtained in [4] at a high sampling rate. In this study, we showed that the result is also valid for lower sampling rates.

5. Comments

The required bandwidth to capture a radio transient signal does not need to be larger than the transmission bandwidth of the radio, therefore there is no need to sample at rates higher than the Nyquist. The reason for this is that all practical radios are implemented using output filters with high roll-off to avoid interference into adjacent channels to comply with regulatory bodies' emission requirements. These filters have high rejection (>40dB) outside the transmission band, i.e. any spectral component outside the band will be highly attenuated, therefore will eliminate the need for unnecessarily high sampling rates and sampling rates of about 2.5 times the channel bandwidth will suffice in practice. This claim was supported by the test results obtained in this paper. We believe that high sampling rates used in transient based techniques reported in the existing literature are not a requirement but it is simply due to the convenience of the use of sampling scopes in these works. Sampling scopes are commonly available in every electronics labs nowadays and they are used for various data acquisition projects. However, oscilloscopes, by their nature, do not include a down conversion stage as in radio receivers or spectrum analyzers and they directly sample at carrier frequencies, so the sampling rates are higher than the required rates. However, this is not a limitation of the transient based techniques; it is just an artifact of the measurement setup.

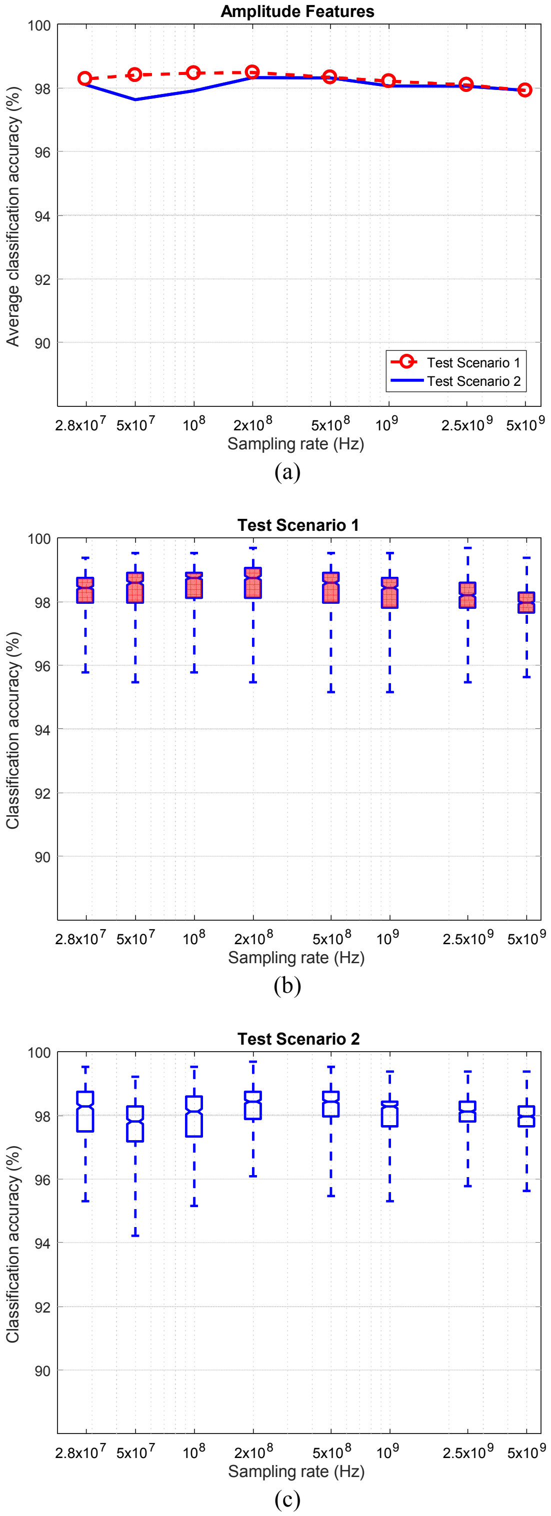


Fig. 6. Performance evaluation test results for Amplitude features at different sampling rates given in logarithmic scale: (a) Average classification accuracies for Test Scenario 1 (dashed lines with circle markers) and Test Scenario 2 (solid lines). Boxplot of the classification results for (b) Test Scenario 1 and (c) Test Scenario 2.

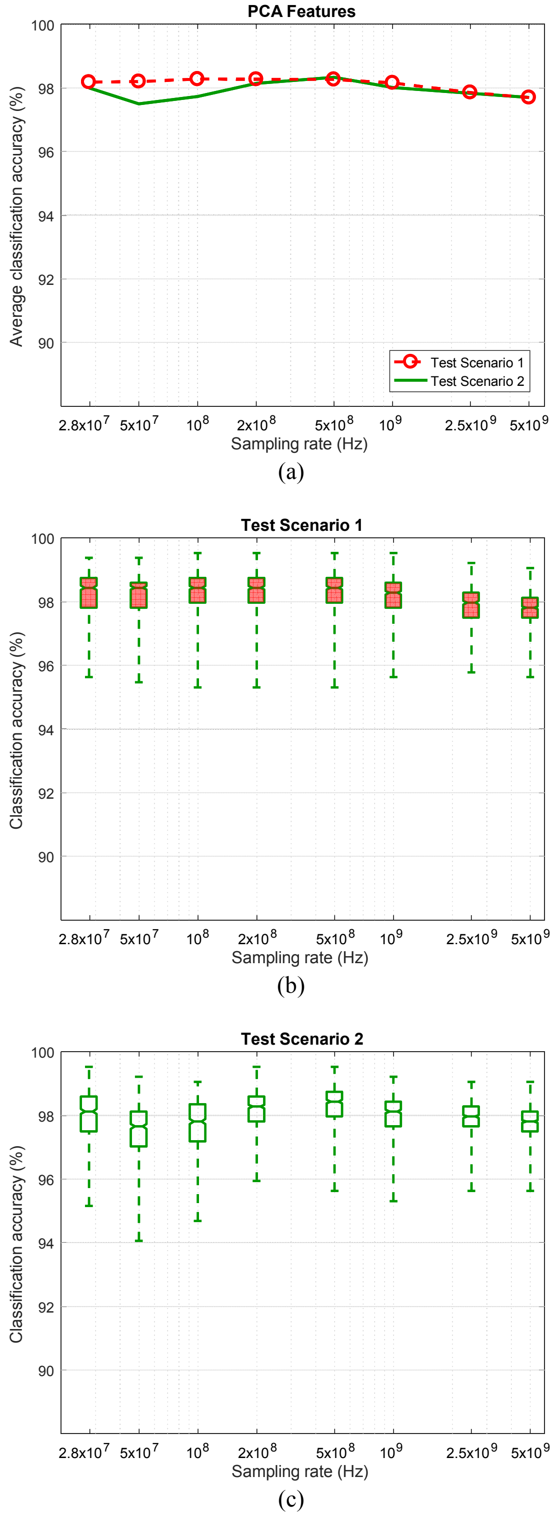


Fig. 7. Performance evaluation test results for PCA features at different sampling rates given in logarithmic scale: (a) Average classification accuracies for Test Scenario 1 (dashed lines with circle markers) and Test Scenario 2 (solid lines). Boxplot of the classification results for (b) Test Scenario 1 and (c) Test Scenario 2.

6. Conclusions

In this work, it has been shown through experimental data that, contrary to the claim in the literature, high sampling rate is not a requirement to detect transmitter turn-on transient signals and extract discriminative features from these signals for the purpose of transmitter identification. This result is important in terms of practical implementation of these methods, since today's low cost receivers operate at low sampling rates. In a future work, the transient based RF fingerprinting approach will be tested with experimental data collected directly from low cost receivers at low sampling rates and potential distorting effects of these receivers on RF fingerprinting performance will be considered.

7. References

[1] O. Ureten and N. Serinken, "Detection of radio transmitter turn-on transients", *Electron. Lett.*, vol. *35*, no. *23*, pp. *1996-1997*, Nov. 1999.

[2] N. Serinken and O. Ureten, "Generalised dimension characterisation of radio transmitter turn-on transients", *Electron. Lett.*, vol. *36*, no. *12*, pp.*1064-1066*, Jun. 2000.

[3] K. J. Ellis and N. Serinken, "Characteristics of radio transmitter fingerprints", *Radio Sci.*, vol. *36*, no. *4*, pp. *585-597*, 2001.

[4] O. Ureten and N. Serinken, "Wireless security through RF fingerprinting", *Can. J. Elect. Comput. Eng.*, vol. *32*, no. *1*, pp. *27-33*, 2007.

[5] W. C. Suski II, M. A. Temple, M. J. Mendenhall, and R. F. Mills,"Using spectral fingerprints to improve wireless network security", in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, 2008, pp. 1–5.

[6] D. R. Reising, M. A. Temple, and J. A. Jackson, "Authorized and rogue device discrimination using dimensionally reduced RF-DNA fingerprints", *IEEE Trans. Inf. Forensics Security*., vol. 10, no. 6, pp. 1180-1192, Jun. 2015.

[7] M. Kose and Z. Telatar, "An approach on identification of 802.11b devices by RF signature in wireless local area networks", in *Proc. IEEE 18th Signal Process. and Commun. Appl. Conf. (SIU)*, 2010, pp. *800-803*.

[8] M. Kose, S. Tascioglu, and Z. Telatar, "Wireless device identification using descriptive statistics", *Communications Fac. Sci. Univ. of Ankara Series A2-A3*, vol. *57*, no. *1*, pp. *1-10*, 2015.

[9] I. O. Kennedy, P. Scanlon, F. J. Mullany, M. M. Buddhikot, K. E. Nolan, and T. W. Rondeau, "Radio transmitter fingerprinting: A steady state frequency domain approach", in *Proc. Vehicular Technology Conference*, 2008. VTC 2008-Fall. IEEE 68th, 2008, pp. *1-5*.

[10] I. O. Kennedy, P. Scanlon, and M. M. Buddhikot, "Passive steady state RF fingerprinting: A cognitive technique for scalable deployment of co-channel femto cell underlays", in *2008 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, 2008, pp. *1-12*.

[11] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices", *ACM Comput. Surveys*., vol. 45, no. 1, pp. 1-29, Nov. 2012.

[12] S. U. Rehman, K. Sowerby, and C. Coghill, "Analysis of receiver front end on the performance of RF fingerprinting", in *Proc. IEEE 23rd Int. Symp. on Personal, Indoor and Mobile Radio Commun. (PIMRC)*, 2012, pp. *2494-2499*.

[13] S. U. Rehman, K. Sowerby, and C. Coghill, "Radio-frequency fingerprinting for mitigating primary user emulation attack in low-end cognitive radios", *IET Communications*, vol. *8*, no. *8*, pp. *1274-1284*, 2014.

[14] O. Ureten and N. Serinken, "Bayesian detection of Wi-Fi transmitter RF fingerprints", *Electron. Lett.*, vol. *41*, no. *6*, pp. *373-374*, Mar. 2005.

[15] M. Kose, S. Tascioglu, and Z. Telatar, "The effect of transient detection errors on RF fingerprint classification performance", in *Proc. 14th Int. Conf. on Circuits, Syst., Electron., Control & Signal Process. (CSECS'15)*, 2015, pp. *89-93*.

[16] M. Kose, S. Tascioglu, and Z. Telatar, "Signal-to-noise ratio estimation of noisy transient signals", *Communications Fac. Sci. Univ. of Ankara Series A2-A3*, vol. *57*, no. *1*, pp. *11-19*, 2015.

[17] R. G. Lyons, "Understanding Digital Signal Processing", Prentice-Hall, Upper Saddle River, NJ, USA, 2004.

[18] L. Tan and J. Jiang, "Digital signal processing fundamentals and applications", Elsevier Inc., Waltham, MA, USA, 2013.