Design of Low-Cost Modular RF Front End for RF Fingerprinting of Bluetooth Signals

Emre UZUNDURUKAN, Aysha M. ALI, Ali KARA
Department of Electrical and Electronics Engineering
Atilim University
Ankara, Turkey
uzundurukanemre@gmail.com, ali.kara@atilim.edu.tr

***Abstract*—For RF fingerprinting of wireless devices, data acquisition has a critical role. Because of this, highly sophisticated devices are used for data capturing or acquisition. In this paper, design of a RF receiver front end with modular components is presented. This design contains filtering and down conversion processing of Bluetooth signals for cellular phones. Moreover, AWR VSS and MATLAB have been used for simulating the down converter circuit. With this simulation, effects of components that used in the design on recorded signal have been observed. In this work in progress paper, only high SNR conditions are considered.**

Keywords—Wireless networks; RF fingerprinting; RF front end design.

I. Introduction

In recent years, usage of wireless communication systems has increased dramatically. With this popularity, security of these systems became more important day by day. Because of this situation, wireless communication security needs to be improved. There are many software developments in the industry, but these developments are not enough to have completely secured systems. In order to assure complete security of the systems, physical layer precautions have been developing.

Hardware of the transceivers has imperfections due to the manufacturing processes. Radio Frequency (RF) Fingerprinting is a technique that identifies distinctive characteristics (manufacturing imperfections) of transceivers. In the literature, there are two main techniques for RF fingerprinting which are transient based and modulation based RF fingerprinting. Transient based technique tries to extract features from transient signals that occur at the beginning of the transmission. On the other hand, modulation based techniques focus on modulator imperfections of the transceiver [1].

Previous research have shown that RF fingerprinting can be done for ZigBee networks [2] and Wi-Fi networks [3]. In the light of these researches, it can therefore be said that frequency, amplitude and phase are the key elements for RF fingerprinting process. In addition, statistical features such as variance, kurtosis and skewness are the features that can be extracted from these three key elements of transient signal. In addition, burst detection can also be used as a feature for this kind of detection systems.

For Bluetooth networks, energy envelope [4] has been used in order to generate features such as area under the normalized energy curve, duration of the transient, maximum slope of the transient energy curve, kurtosis of the transient curve, skewness of the transient curve and the variance of the transient envelope. With this feature set high classification rate has been achieved.

Data acquisition has important role for RF fingerprinting processing because performance of the RF fingerprinting depends on features that generated from received signal. It can be seen that most of the RF fingerprinting works have been done with highly sophisticated receivers such as PSA E4448A Spectrum analyzer and oscilloscope [4], PXIe-1085, 5791 RF Transceiver and USRP 2921 [5] and also E3238S [2]. Due to their high precision, these devices are very expensive. Instead of using expensive devices, receiver part can be designed with inexpensive modular components.

In this paper, design of a RF receiver front end with modular components for Bluetooth signals is presented and analysis of effects of designed modular RF front end on data acquisition is presented. In section II, experimental data acquisition, understanding of sampling frequency and signal to noise ratio (SNR) are presented. In section III, understanding of filtering techniques, important parameters of filter that is used in this work are presented. In section IV, theory of down conversion, construction of down converter circuit and AWR VSS simulation are given. In section V, simulation results are summarized. Finally, conclusion and future work are discussed in section VI.

II. Data Acquisition

As observed in the literature, highly sophisticated devices [2], [4], [5] have been used for data acquisitions. Without using these devices, data acquisition can be done with low-cost modular components. In order to feed such a system with real data, test data were captured by high end instrument (TDS7404 DSO Oscilloscope) with unity gain antenna. It is known that the Bluetooth signal has a carrier frequency between 2400 MHz and 2483.5 MHz. In order to digitize captured signal, ADC

978-1-5090-6494-6/17/$31.00 ©2017 IEEE

(analog to digital converter) should have at least 4.8 GHz sampling frequency by Nyquist Theorem as given as follows: [6].

$$f_s \geq 2f_c \tag{1}$$

Sampling frequency (f_s) was set to 20 Gsps because higher sampling rate means that more realistic signal is captured in this study. However, there is a tradeoff between (f_s) and undesired frequency components, and sampling frequency is directly proportional to Bandwidth (BW) of the signal. When the BW is increased, both desired and undesired frequency components, and high frequency noise, are sampled together. Signal to noise ratio (SNR) is critical for signal analysis. SNR can be described as the ratio of the signal power and the environmental noise power as given as follows:

$$SNR = \frac{P_S}{P_N} \tag{2}$$

For the data recording/capturing process, edge detection mode of the oscilloscope was used. By this way, the device automatically detects the turn on transient of the Bluetooth signal. By using oscilloscope's cursors, the region of interest was selected and exported as a text file. In order to reduce undesired signals and noise, every cellular phone was set to flight mode. After that, only Bluetooth was activated, in this way, the phone can only emit Bluetooth signal. Every record includes noise due to receiver, environmental effects, transient signal and steady state signal. It has been observed that a typical Bluetooth transient has approximately 10 μs duration. In this preliminary test, there were only five cellular phone models in data capturing. However, more than 100 cellular phones will be used for complete data set, and 10 records will be taken from each phone for realistic classifications.

III. Filtering

After the recording process, it was observed that recorded signals have undesired frequency components. In order to eliminate these unwanted frequencies, a filter is needed to be implemented on recorded signals. Filters help reduce amplitudes of various frequency components including noise without adding any new frequency component. Transfer function of a filter is simply is given as follows:

$$|H(f)| = \frac{|V_o(f)|}{|V_i(f)|} \tag{3}$$

where $V_o(f)$ is the filter's output signal spectrum while $V_i(f)$ is the input signal's spectrum. Fig.1 shows sample signal spectra for illustration [8].

For Bluetooth signals, band-pass filter is required to eliminate most of the unwanted frequency components. In this paper, Finite Impulse Response (FIR) filter was used to eliminate the unwanted signals, and especially, noise of the recorded Bluetooth signal. It has been chosen as it has the following advantages:

- Easy to build and use
- Stable
- Better performance of quantization effects than IIR filters
- Easy to design specific magnitude responses [9].

In order to design a FIR band-pass filter, however, several parameters need to be determined. One of them is cut-off frequency. To achieve desired filter, response of the filter should be given as follows [10]:

$$H_d(f) = \begin{cases} 0, & 0 \leq f \leq f_L \\ 1, & f_L \leq f \leq f_U \\ 0, & f_U \leq f \end{cases} \tag{4}$$

By using MATLAB filter design toolbox, a FIR band-pass filter was designed. Frequency range of the filter is between 2400 MHz and 2483.5 MHz. It is the range of Bluetooth signals. Moreover, the ripple of the filter is set to 1dB. By using designed filter, signal SNR was dramatically improved, approximately 38.5 dB. The filter was designed in MATLAB environment. In order to simulate the downconverter design, oscilloscope was used to record test data. It was observed that oscilloscope generates unwanted frequency components. This filter is designed to eliminate these unwanted frequency components. According to this, this filter will not be used in the real implementation as the data will be recorded directly after the downconverter circuit. Fig. 2 shows the response of the designed BPF. Fig. 3 & 4 represent sample input and output signals of the filter.

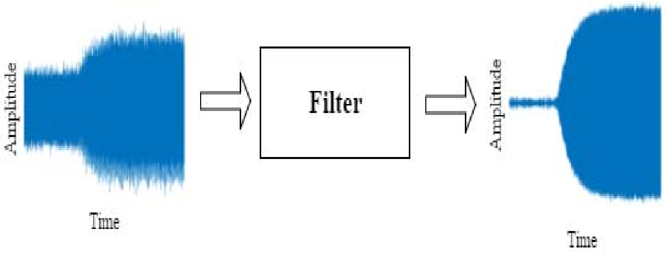

Fig. 1. Illustration of input and output signals for band pass filtering.

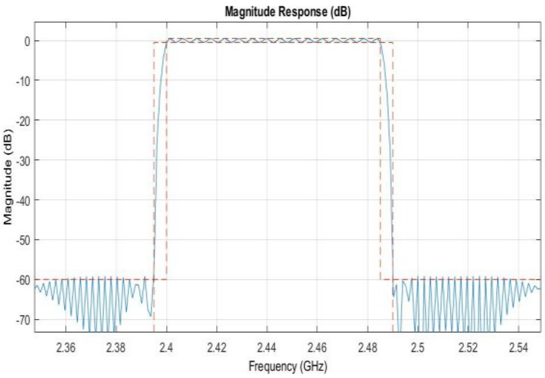

Fig. 2. Magnitude response of the BPF

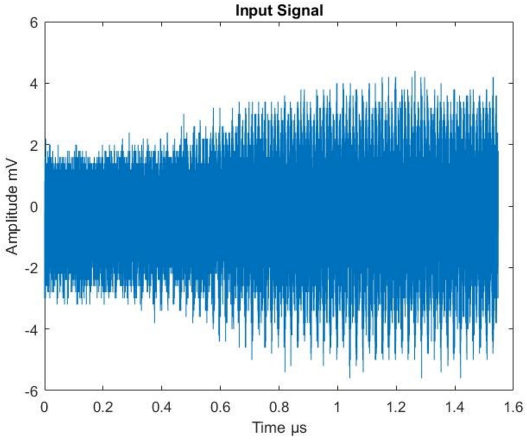

Fig. 3. Noisy input signal (captured in the lab.).

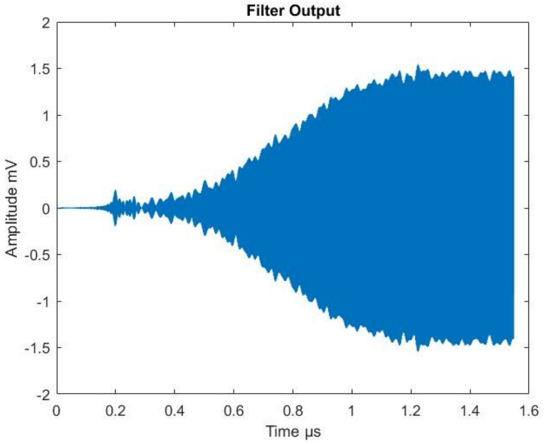

Fig. 4. Filtered signal given in Fig. 3.

IV. Down Conversion

Down conversion is an important part of communication systems. Radio receivers have a high speed ADC that digitize the incoming RF signal and generating a high rate digital data. However, the frequency content of Bluetooth signals is beyond the range of commercially available ADCs. A down converter moves the band of interest by shifting the carrier frequency to a lower band. By this way, the sampling rate can be reduced in ADC and further processing can be done easily. Down conversion can be implemented easily by using RF mixers. After the mixer, a low pass filter should be connected to the output of the mixer in order to shift the input frequency to an Intermediate Frequency (IF) which is given as follows:

$$f_{IF} = \begin{cases} f_{LO} + f_{RF} \\ f_{LO} - f_{RF} \end{cases} \tag{5}$$

Down conversion was implemented in AWR VSS environment. In this process, down conversion blocks were designed by using equivalent models of commercial components. For this purpose, commercially available LNA (ZQL-2700MLNW+), Mixer (ZX05-63LH+) and Low Pass Filter (VLFX-105) were selected. Then, with the 2.5 GHz local oscillator frequency, recorded signals were shifted between DC and 100 MHz. In this process, gain of LNA and the power of LO were selected according to mixer's isolation thresholds. Because if the input of the mixer exceeds the threshold level, output will be invisible. For the mixer that used in this simulation has 30 dB typical isolation. According to this power threshold, input power of the mixer tuned carefully. In Fig. 5, the downconverter schematic is presented. Moreover, input and output signal spectra of the down converter is presented in Fig. 6 & 7. Output power can be derived as follows:

$$P_O = P_I + G_{LNA} - L_{mixer} - L_{filter} \tag{6}$$

where P_O is the output power and P_I is the input power. In the simulation, the gain of LNA was considered as 18.3 dB and the total loss of the mixer and the LPF was considered as 15.1 dB. Then, the total gain was approximately 3.2 dB.

V. Results

By using the proposed system discussed in previous section, it can be seen that Bluetooth signals can be down converted with modular components. An illustration of low-cost modular receiver design is provided in Fig. 8. Some simulation results for five cellular phones are listed in table 1. It should be noted that the durations of transients are not equal for each device. This may be used as a feature alone for RF fingerprinting process.

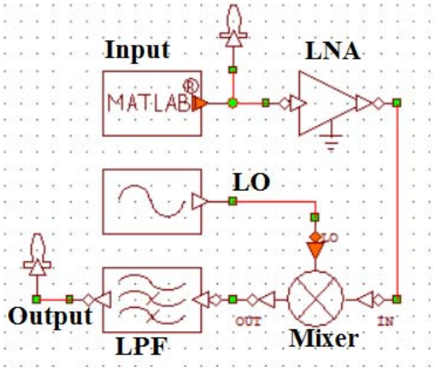

Fig. 5. AWR VSS down converter system diagram

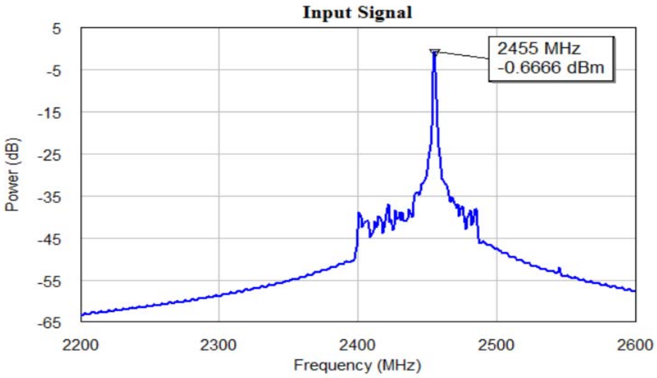

Fig. 6. RF input of the down converter at 2455 MHz

978-1-5090-6494-6/17/$31.00 ©2017 IEEE

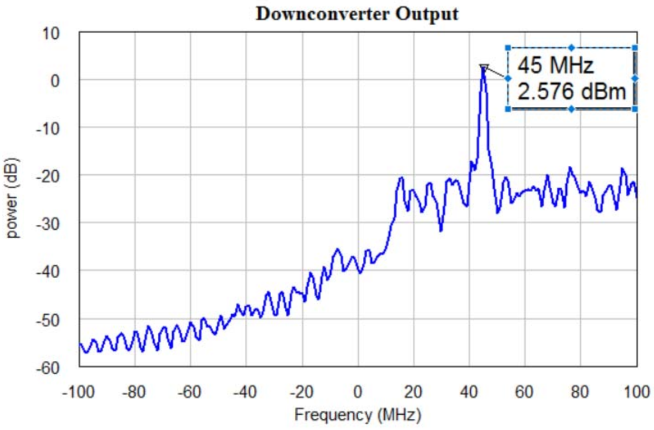

Fig. 7. IF output of the downconverter at 45 MHz

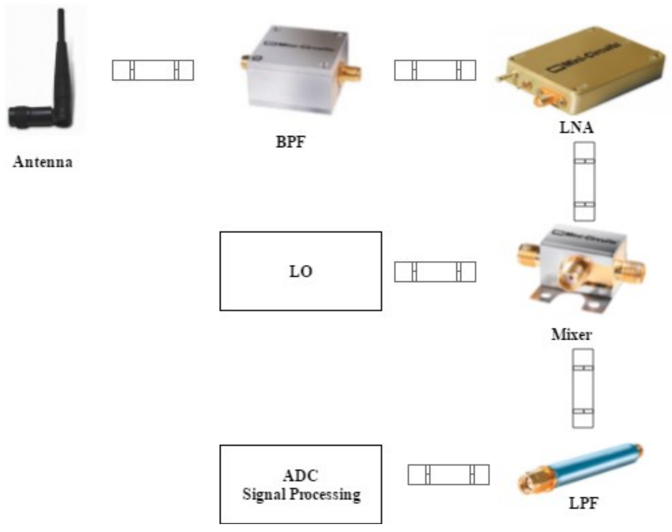

Fig. 8. Designed low-cost modular reveiver.

Moreover, the SNR of the records was improved dramatically but this is just a simulation, and needs to demonstrate in the laboratory. When the hardware implementation is completed, the level of the SNR improvement may not be satisfactory.

VI. Conclusion and Future Work

In this paper, an experimental down conversion system design for capturing Bluetooth signal has been presented. According to simulation results, instead of using high-end expensive devices, data acquisition can be achieved with low cost modular designs.

In this way, Bluetooth signals can be captured with 200 MHz sampling frequency instead of using 5 Gsps sampling rate imposed by Nyquist theorem. Five different cellular phones were used as a test subject to demonstrate this. Effects of sampling rate and filtering have been discussed by using these recorded data.

TABLE I. Simulation Results

Device ID	1	2	3	4	5
Transient Duration (µs)	1.332	0.872	0.810	0.851	0.911
SNR before Filtering (dB)	38	36,79	33	39,5	37
SNR after Filtering (dB)	75,27	74,94	75,4	76,61	74,38
Center Frequency after mixer (MHz)	45	49	21	29	45

In future work, there will be implementation of a working prototype of the proposed system. After finishing the hardware implementation, there will be extensive data capturing phase of RF fingerprinting system for Bluetooth signals. Moreover, there will be tests on the capturing performance and analyze its effects on the recorded data.

Acknowledgment

This work was supported by Atilim University under the grant number LAP-C-1617-18.

References

[1] B. Daney, H. Luecken, S. Capkun, K. El Defrawy, “Attacks on physical-layer identification,” 2010.

[2] C. K. Dubendorfer, B. W. Ramsey, M. A. Temple, “An RF-DNA verification process for ZigBee networks,” 2013.

[3] D. R. Reising, M. A. Temple, J. A. Jackson, “Authorized and rogue device discrimination using dimensionally reduced RF-DNA fingerprints,” IEEE Transactions on Information Forensics and Security, vol. 10, No. 6, June 2015.

[4] S. U. Rehman, K. Swerby, C. Coghill, “RF fingerprint extraction from the energy envelope of an instantaneous transient signal,” Australian Communications Theory Workshop, 2012.

[5] B. W. Ramsey, T. D. Stubbs, B. E. Mullins, M. A. Temple, M. A. Buckner, “Wireless infrastructure protection using low-cost radio frequency fingerprinting receivers,” International Journal of critical infrastructure protection 8, 2015, pp. 27-39.

[6] S. J. Orfanidis, “Introduction to signal processing,” Rytgers University, 2010, pp. 6-7.

[7] K. Lacanette, “A basic introduction to filters-active, passive and switched-capacitor,” National Semiconductor Application Note 779, April 1991.

[8] R. A. Losada, “Digital filters with MATLAB,” The MathWorks Inc., 2008.

[9] A. V. Oppenheim, R. W. Scafer, “Discrete-time signal processing,” 2nd ed., Prentice Hall, 1999, pp. 507-510.

[10] T. Schilcher, “RF applications in digital signal processing,” Paul Scherrer Institut, Switzerland.

978-1-5090-6494-6/17/$31.00 ©2017 IEEE