FPGA-BASED ARCHITECTURE FOR BASEBAND SIGNALS GENERATION APPLIED TO MOBILE PHONE JAMMING

Isabela Trindade
LASSE - 5G & IoT Research Group
Rua Augusto Corrêa, 1 - Guamá
Belém, Para 66075-110
isabela.trindade@itec.ufpa.br

Patricio Cordeiro
LASSE - 5G & IoT Research Group
Rua Augusto Corrêa, 1 - Guamá
Belém, Para 66075-110
patricio@ufpa.br

Leonardo Ramalho
LASSE - 5G & IoT Research Group
Rua Augusto Corrêa, 1 - Guamá
Belém, Para 66075-110
leonardolr@ufpa.br

Adalbery Castro
LASSE - 5G & IoT Research Group
Rua Augusto Corrêa, 1 - Guamá
Belém, Para 66075-110
adalbery@ufpa.br

Aldebaro Klautau
LASSE - 5G & IoT Research Group
Rua Augusto Corrêa, 1 - Guamá
Belém, Para 66075-110
aldebaro@ufpa.br

ABSTRACT

Mobile phone jamming has gained popularity as a tool for combating the use of mobile phones in areas where their use is prohibited and, e. g., to prevent detonation of radio-controlled explosives. Recent technological advances in digital signal processing techniques using field programmable gate array (FPGA) and the availability of advanced and efficient IP cores makes possible to flexibly synthesize high sampling rate waveforms in a cost-effective way. This paper presents an approach for the generation of baseband signals for mobile phone jammer using FPGA and digital to analog converters (DACs). Benefiting from these advances, the proposed architecture uses a programmable direct digital synthesizer (DDS) to generate a multitone baseband signal, which can adapt to the characteristics of the radio frequency (RF) signal of target mobile radio access technologies (RATs). From the proposed architecture we derive a complete jamming system and an algorithm for the calculation of the main parameters of the baseband signal. A prototype was built using the Altera Cyclone III (EPC3C120) FPGA chip, adopting GSM as a case study. The results show that the presented system is very efficient with respect to hardware resources usage while achieving good performance in terms of the generated signal spectra.

CCS CONCEPTS

•Hardware → Communication hardware, interfaces and storage; *Signal processing systems;* Digital signal processing;

KEYWORDS

Jammer; DDS; NCO; FPGA; GSM.

ACM Reference format:
Isabela Trindade, Patricio Cordeiro, Leonardo Ramalho, Adalbery Castro, and Aldebaro Klautau. 2016. FPGA-BASED ARCHITECTURE FOR BASEBAND SIGNALS
GENERATION APPLIED TO MOBILE PHONE JAMMING. In *Proceedings of SForum 2017, Fortaleza, Ceará, Brazil, August 28–September 1,* 4 pages.
DOI: 10.1145/nnnnnnn.nnnnnnn

SForum 2017, Fortaleza, Ceará, Brazil

1 INTRODUCTION

Recently, cell phones have gone from simple voice communication devices to so called "smart devices" that allow, among numerous actions, the transmission of text messages and images, Internet access, video streaming, etc. Widely used for simple conversations to business transactions, the importance of their jamming in specific situations increases, whether for ensuring a certain level of silence and privacy, such as in classrooms, churches, libraries, cinema, theater, etc.; or for safety reasons, such as in prisons or to prevent detonation of radio-controlled explosive devices. Mobile phones jammer (MPJ) [1], which aim to disrupt the communication between a mobile device (MD) and its base stations (BS), is a important tool for combating the use of mobile phones or other wireless devices where their use is prohibited.

There are several types of MPJs and five categories - "A" to "E" - [2]. This work focuses on type "A" MPJs due to their relative low cost and simplicity. For type "A" MPJs, the existence of multiplexing strategies, such as OFDMA (orthogonal frequency-division multiple access) or TDMA (time division multiple access) is irrelevant. For instance, even if the communication is taking place in a specific time slot, the MPJ generates a radio frequency disturbing signal (RF-DS), uninterruptedly.

The frequency range covered by the RF-DS of the MPJ-A can be applied only to control channels (e. g., a 200 kHz TP0 beacon channel in GSM [3]) or to the full band (e. g., over 25 MHz bandwidth for a GSM deployment using 124 channels). Thus, the MPJ-A can be subdivided in two subtypes: "Ac" or MPJ-Ac and "Af" or MPJ-Af, for the signals that cover only control channel frequencies or the full band, respectively. The former can be more energy-efficient due to the lower bandwidth, but it depends on the radio access technology (RAT) that is used on the communication.

MPJs-Ac were previously described in a GSM scenario, with the RF-DS applied to selected control channels [1, 4, 5]. The jamming system monitors the power received in a closed area, corresponding to carriers emitted by nearby BSs, and emits the RF-DS on these channels [1]. Similarly, in other setup, the RF-DS is generated only when the power of control channels exceeds some predefined value [4]. On the other hand, MPJ-Af was investigated in [6–8]. In one of them, jamming is achieved by distorting the spectrum [8].

Most of the previous works on type MPJs-A adopts analog processing to generate the RF-DS signal [4, 6, 7]. This is typically done using a system based on a voltage controlled oscillator (VCO) or analog synthesizers. However, issues such as components aging and temperature drift can change dramatically the output signal frequency, which may accidentally interfere in nearby RF transmitter systems. Such problems can be minimized or avoided by using an hybrid system that uses a direct digital synthesizer (DDS) to generate the baseband signal and a heterodyne transmitter to translate the signal to RF frequencies. Digital processing has strong advantages over analog such as increased flexibility, which is specially important due to the fast pace of RAT technologies.

In this work we propose a FPGA based architecture that implements a multitone DDS to generate the baseband signal for a MPJ-A (MPJ-Ac or MPJ-Af) system. A complete MPJ-A system is also implemented to validate the proposed architecture. The remaining of the paper is organized as follows. In Section 2, we introduce the novel MPJ-A that uses digital signal processing to generate the baseband signal. In Section 3 we present and discuss the system model. Section 4 and 5 presents the results and the conclusions, respectively.

2 BASEBAND DIGITAL SIGNAL GENERATION FOR MPJ-A JAMMERS

Analog type MPJ-A are generally composed of the following main blocks: a signal generator, a heterodyne transmitter, a power stage and one or more antennas. The signal generator creates the analog baseband jamming signal. The heterodyne transmitter is composed of mixers and filters to properly move the baseband signal to a radio frequency given by a local oscillator (LO). Finally, the power stage amplifies the signal for proper wireless transmissions.

The proposed MPJ-A system uses digital signal processing techniques to efficiently generate the baseband signal. More specifically, a multitone signal is used as jamming signal which can comply with the spectrum regulation and effectively jams the target RAT without disturbing others communication systems.

The process of modeling the digital signal for the proposed MPJ-A system requires specific knowledge about the characteristics of the target RATs signals, such as subcarriers spacing Δ_f, carrier frequency f_c and total system bandwidth BW. Other parameters of the signal model for the proposed system will be discussed with the help of the block diagram shown in Fig. 1, where a digital logic unit (DLU) is used to generate the baseband signal and can be implemented, e. g., using a FPGA.

If the MPJ must operate in contiguous frequency bands, it may be beneficial to use a single $x[n]$. In other situations, such as when jamming multiple RATs, it may be beneficial to use M distinct DACs and upconversion stages, as indicated in Fig. 1. Thus, the DLU generates a digital signal $x_i[n]$ for every single channel $i = 1, 2 \ldots M$, where M is the total number of MPJ-A channels. Then, each $x_i[n]$ is then converted to its analog counterpart $x_i^{\mathrm{BB}}(t)$ by the DAC, low-pass filtered and then up-converted to the desired radio frequency (RF) by the heterodyne-transmitter to produce $x_i^{\mathrm{RF}}(t)$, which, in turn, is amplified and transmitted via an antenna.

This work focuses solely on the baseband signals $x[n]$ and $x^{\mathrm{BB}}(t)$, which inherit specifications from $x^{\mathrm{RF}}(t)$. In the proposed approach

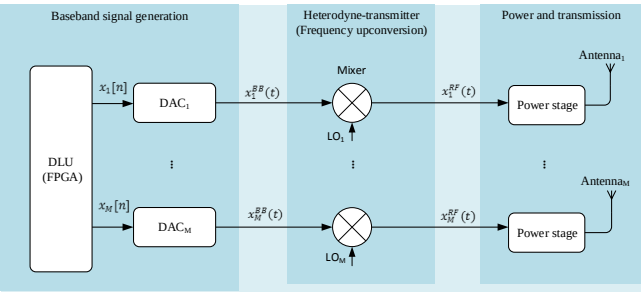

Figure 1: Block diagram for the proposed jammer signal generation.

the jamming signal is a multitone signal composed of several sinusoids with different frequencies f_c^{RF} and phases θ. To model this multitone signal, a set $\mathcal{K}$ of sinusoids with frequencies multiples of Δ_ω is selected. Then, all the sinusoids are combined to create the multitone signal:

$$y[n] = \sum_{k \in \mathcal{K}} a \cos(k\Delta_\omega n + \theta_k), \tag{1}$$

where a is the amplitude, $n = [0 \ldots N-1]$ is the number of samples, k is the frequency index and θ_k is the phase in radians. Thus, the signal $x[n]$ in Fig. 1 is obtained by periodically repeating $y[n]$ with period N. Assuming the DAC operates at F_s samples per second (SPS), Δ_ω in radians corresponds to a frequency resolution $\Delta_f = F_s\Delta_\omega/(2\pi) = F_s/N$ Hz, such that a component of $x[n]$ with frequency $k\Delta_\omega$ corresponds to $k\Delta_f$ in $x^{\mathrm{BB}}(t)$.

3 PROPOSED FPGA ARCHITECTURE

In this section we propose an architecture to implement the DLU in Fig. 1 with FPGA. The computation and generation of $x[n]$ can benefit from parallelism and high sampling rates offered by FPGAs. Yet, the possibility of reconfiguring provides flexibility to change in real time the location of the carriers and the bandwidth covered by the signal $x[n]$.

A simple but effective way to generate a sine wave digitally is to use direct digital synthesizer (DDS), which are generally implemented with numerically controlled oscillator (NCO). The NCO output waveform is given by [9]:

$$s(nT) = B \sin\left[2\pi(f_o nT + \phi_p)\right], \tag{2}$$

where f_o is the output frequency, T is the operation clock period, ϕ_p is the phase of the sinusoid, $B = 2^{R_M-1}$ is the magnitude of the sinusoid and R_M is the magnitude precision. The output frequency is given by the following expression:

$$f_o = \frac{\phi_i f_{clk}}{2^{R_i}}\mathrm{Hz}, \tag{3}$$

where $1 \leq \phi_i \leq 2^{R_i}$ is the phase increment, $f_{clk} = \frac{1}{T}$ is the system clock frequency and R_i is the phase increment precision. The frequency resolution of the NCO, f_{res}(Hz), is obtained when $\phi_i = 1$ and is given by:

$$f_{res} = \frac{f_{clk}}{2^{R_i}}, \tag{4}$$

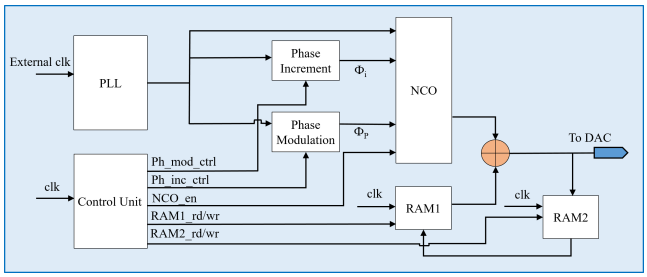

Figure 2: FPGA Top Level DDS design for baseband signal generation.

which determines the minimum f_o that can be achieved for a given f_{clk} and R_i.

From Eq. (3), if f_{clk} and R_i are fixed then f_o is determined by the ϕ_i value. Thus, after a cycle, f_o can be changed instantaneously by simply changing the value of ϕ_i. This gives the possibility to calculate several sinusoids with distinct frequencies using distinct ϕ_i values and then combine them to form a multitone signal. In this section, we present an architecture that takes advantage of this NCO characteristic to generate a baseband multitone signals that can be applied by MPJ-A for mobile phone jamming.

The top level schematic representation of the FPGA design is shown in Fig. 2. The design consists basically by: a PLL, a phase increment, a phase modulator, a control unit, a NCO, two RAMs and an adder block. The PLL generates the system f_{clk}, which is used by all blocks. The phase increment and the phase modulation blocks are used to store a set of pre-calculated $\boldsymbol{\phi_i} = [\phi_{i0}, \phi_{i1} \ldots \phi_{iS}]$ and $\boldsymbol{\phi_P} = [\phi_{p0}, \phi_{p1}\phi_{pS}]$ values, respectively, where S is the number of subcarriers (i.e., the size of the set $\mathcal{K}$). Note that the vectors $\boldsymbol{\phi_i}$ and $\boldsymbol{\phi_P}$ store the phase increment (i.e., the frequency) and phase of each sinusoid, respectively.

In Fig. 2, the NCO receives the clock from PLL and the elements of $\boldsymbol{\phi_i}$ and $\boldsymbol{\phi_P}$ to calculate the samples of the desired signal, as stated in Eq. (2). The adder adds the NCO signal with the RAM1 signal and stores the results on RAM2, which, at the end of the process, sends the stored content to DAC. The operations of the proposed method can be divided in three stages:

STAGE 1 In this stage the NCO is *ON* and $\phi_i = \phi_{i_0}$ and $\phi_p = \phi_{p_0}$. The NCO samples are subsequently summed with the content of the RAM1, which, in this case, is 0 for all n, and the resulted samples are then stored in the RAM2. This process continues until all N samples are stored.

STAGE 2 In this stage the NCO is *OFF* and the samples previously stored in the RAM2 are sent and stored in the RAM1. After that we go back to STAGE 1. This process is repeated until all S-sinusoids are summed and then we go to STAGE 3.

STAGE 3 This is the last stage, all the S-sinusoids are already summed and stored in RAM2. From this point the NCO and RAM1 are turned *OFF* and the content of RAM2 is continuously repeated and sent to the DAC.

4 RESULTS

In this section we present results of experiments in generation of the jamming signal and its application on blocking mobile phone signals. The experiments were divided in simulations and real world implementations of the proposed DLU. The simulations were performed in Modelsim software and the real world implementation was performed in a custom FPGA board developed by the authors.

Table 1: Physical channel parameters of the subband A and B of GSM in Brazil [10].

Parameter	GSM900
Δ_f(kHz)	200
f_c^{RF} (MHz)	869:Δ_f:894
DL central frequency (MHz)	881.5
BW_{DL} (MHz)	25
Total number of channels	126

4.1 Scenario definition

In our experiments we targeted a GSM900 system where our goal was to operate as a MPJ-A and transmit a jamming signal in all down-link channels, since disruption in the downlink, typically, requires less energy than in uplink. We set the total number of channels to 126 (BW = 25 MHz), which corresponds to the same BW of the targeted GSM system, as shown in Table 1.

4.2 Baseband signal parameters calculation

We start our calculations by first determining the minimum and maximum frequencies (f_{min} and (f_{max})) of the baseband signal $x^{BB}(t)$, taking into account the trade-off of using low cost DACs and analog filters. The value of F_s impacts on the choice of the DAC and the difference between F_s and f_{max} determines the order of the anti-image filters. Hence, we set f_{min} = 10 MHz, which results in f_{max} = 35 MHz and a central frequency of 22.5 MHz. This signal can be translated to RF using a mixer with a LO frequency of 859 or 904 MHz, and filtering (removing) the lower side band or the upper side band at RF-port of the mixer, respectively.

Afterwards, we choose F_s = 150 MSPS to ease the signal reconstruction process and decrease the quantization noise PSD level, while obeying $F_s > 2 \times 35$ MHz. This results in a spacing of 80 MHz ($150 - 2 \times 35$) between the baseband jamming signal and its image at DAC output. The images should be removed to properly create a signal with frequencies between f_{min} and f_{max}, only. Furthermore, after setting F_s, the number of samples of the multicarrier discrete signal $y[n]$ is $N = F_s/\Delta_f = 750$. Recall that digital jamming signal $x[n]$ is constructed by periodically transmitting $y[n]$.

4.3 FPGA implementation

The FPGA design was implemented and simulated in the Altera Quartus II, where we target a Cyclone III EP3C120F780C7 device in a custom board developed by the authors. The control unit was split in three sub-blocks: the NCO control and the RAM1 and RAM2 control. The sync delays are used to synchronize data between blocks and the output registers are used to register the output signal.

The design parameters and corresponding configured values are summarized in Table 2. For $f_{clk} = F_s$ = 150 MHz and phase increment precision of R_i = 32 bits, the frequency resolution is

Table 2: Parameters values in the FPGA implementation.

Parameter	Value
Phase increment precision (R_i)	32 bits
Magnitude precision (R_M)	12 bits
System clock (f_{clk})	150 MHz

$f_{res} \approx 34.9$ mHz. For such values, $\phi i_0 = 286331153$ corresponds to $f_0 \approx 10$ MHz and is subsequently increased in steps of $\Delta_{\phi i} = 5726623$ or $\Delta_f = 200$ kHz until the maximum frequency, $f_{\max} = 35$ MHz is reached. The phase modulation input values $\boldsymbol{\phi_p}$ were pre-calculated in Matlab, stored in a RAM and fed to the corresponding NCO input.

In this implementation of the proposed scheme shown in Fig 2, the blocks RAM1, RAM2 and adder have a precision of 14-bits, which is the same precision of the DAC used in the project (DAC5672 from Texas Instruments). In order to decrease the probability of overflow, we set the width of the NCO output to $R_M = 12$ bits. Then, we concatenate two new bits at the NCO output to match the width of the adder input (14 bits). These two bits are equals to the sign bit of the NCO output.

4.4 Real world results

The proposed architecture was validated with a prototype based on the architecture presented in Section 3, was obtained with the DLU implemented in a custom board. The board consisted of the Altera's FPGA EP3C120F780C7 connected to the 14-bits DAC (DAC5672). Furthermore, the same project described above was also used in another FPGA that has fewer resources, the Altera's FPGA EP1C3T100C6. Table 3 summarizes the usage of the resources in both platforms, in terms of logic elements and memory.

Table 3: MPJ hardware consumption with DLU implemented in FPGA.

Type of resource	Used	Percentage of used resources	
		EP3C120F780C7	EP1C3T100C6
Logic elem. (LEs)	14	1 %	1 %
Memory bits	16,000	1 %	26 %

In terms of the signal, Fig. 3 shows the PSD of the generated jamming signals for the target GSM900 band. It was as captured with a spectrum analyzer and also shows four subcarriers of the multitone signal. The measured out-of-the emissions are 50 dB lower than than the desired jamming signal power. In this case, the out-of-band emissions are highly dominated by the quantization noise of the DAC. Indeed, the jamming signal has a flat PSD in the band of interest. The proposed method is able to generate a power uniformly over the desired band and maintain low out-of-band emissions. Thus, the proposed architecture can be efficiently used to generate jamming signals to the target RAT with low impacts on RATs that operates in others frequencies.

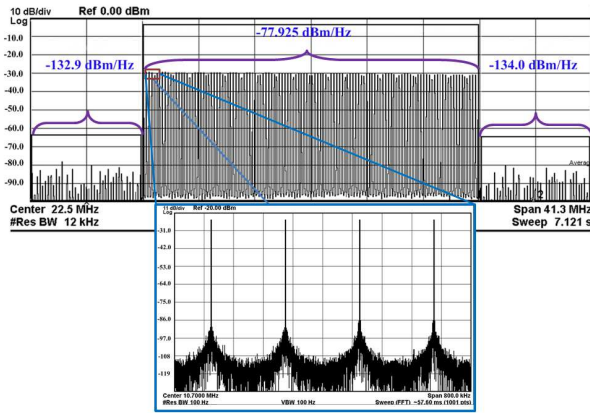

Figure 3: PSD of the jamming signal generated by the proposed system.

5 CONCLUSIONS

This paper proposed a digital system for generating a RF-DS. A design methodology was detailed and evaluated with GSM as a case study. Results showed that the presented system is efficient and consumes only a relatively small amount of hardware resources to generate the baseband signal. Furthermore, the proposed digital system has many advantages over the analog ones. For example, the baseband frequencies are configurable and can be changed by simply updating the RAM contents. Besides, the hardware usage does not increase with the number of channels to be jammed, since each new sinusoid is created iteratively. Lastly, the system can also be used as part of many types of jammer, including, e. g., the ones that are more sophisticated and activate the RF-DS only when detect some signal of the target RAT.

REFERENCES

[1] J.M. Pousada-Carballo, F.J. Gonzblez-Castaiio, F.I. de Vicente, and M.J. Fernbndez-Iglesias. Jamming System For Mobile communications. *Electronics Letters*, 34(22):2166–2167, 1998.
[2] RABC M&PC Committee. Use of jammer and disabler devices for blocking PCS, cellular & related services. Technical report, Mobile & Personal Communications Committee of the Radio Advisory Board of Canada, 2001. http://www.meshcode.ca/PROJECTS/telefire/MK_jamming_laws_canada_01pub3.pdf.
[3] M. Sauter. *From GSM to LTE: An Introduction to Mobile Networks and Mobile Broadband.* Wiley, 2010.
[4] E. Divya and R. Aswin. Design of User Specific Intelligent Cell Phone Jammer . In *Recent Advances in Information Technology (RAIT), 2012 1st International Conference on*, pages 312–316, 2012.
[5] I. Patel, R. Kulkarni, and J.A. Khan. Intelligent FM Signal Jamming System. In *Computing Communication Networking Technologies (ICCCNT), 2012 Third International Conference on*, pages 1–6, 2012.
[6] N.K. Mishra. Development of GSM900 Mobile Jammer: An approach to overcome existing limitation of jammer. In *Wireless Communication and Sensor Networks (WCSN), 2009 Fifth IEEE Conference on*, pages 1–4, 2009.
[7] V.K. Sambhe, D.S. Kale, A. Wasule, and N. Shikha. Antenna for mobile phone jammer. In *Emerging Trends in Engineering and Technology, 2008. ICETET '08. First International Conference on*, pages 856–859, 2008.
[8] S.W. Shah, M.I. Babar, M. N. Arbab, K. M. Yahya, G. Ahmad, T. Adnan, and A. Masood. Cell Phone Jammer. In *Multitopic Conference, 2008. INMIC 2008. IEEE International*, pages 579–580, 2008.
[9] Altera. NCO megacore function, 2014. https://www.altera.com/en_US/pdfs/literature/ug/ug_nco.pdf.
[10] National Telecommunications Agency in Brazil. Resolution no. 454, of december 11, 2006, 2006. http://www.anatel.gov.br/legislacao/resolucoes/2006/89-resolucao-454.