A hardware solution to overcome the bandwidth limitation of drone jamming platforms

Mohammed RABIAI
High School Ali Chabati,
Algiers, Algeria
mohammed.rabiai2013@gmail.com

Mohammed Raouf SENOUCI
University of Electronic Science and Technology of China,
Chengdu, China
senoucimedraouf@std.uestc.edu.cn

Abdelkader SENOUCI
Northumbria University,
Newcastle, United Kingdom
abdelkader.senouci@northumbria.ac.uk

Krishna BUSAWON
Northumbria University,
Newcastle, United Kingdom
krishna.busawon@northumbria.ac.uk

Laurent DALA
Northumbria University,
Newcastle, United Kingdom
laurent.dala@northumbria.ac.uk

***Abstract*—Drone jamming platforms are faced with a significant constraint on bandwidth limitation compared to the broadband spectrum used by remote control radio links in view of implementing the advanced techniques of spread spectrum on these devices. In this work, we propose a hardware solution to overcome the bandwidth limitation of drone jamming platforms by using the dual AD9361 transceiver integrated on the AD-FMCOMMS5-EBZ radio prototyping platform. The hyperchaotic generator of random digital signals and the custom control architecture have been implemented on the ZC706 FPGA development board. A versatile real time chaotic signals generation IP have been developed and integrated on the FMCOMMS5-EBZ HDL reference design considering timing constraints related to the AD9361 data exchange and the AXI-LITE bus interface. The experimental results showed a coverage capacity of more than 100 MHz of bandwidth, which made it possible to guarantee an integral coverage of the WIFI band and consequently to neutralize consequently any potential threat evolving on this band.**

***Index Terms*—jamming, chaotic system, hardware design, SoC, AD9361, high performance FPGA embedded platform, wideband wireless signal, software defined radio.**

I. Introduction

Currently, the communication between drone and its remote-control system is established using high-performance techniques that allow them to operate in an environment characterized by a high rate of interference, [1]. These interferences result from the coexistence of multiple users sharing the same communication medium, and, the sources of intentional interferences such as jammers. In fact, the WI-FI band is an open access wireless support for any kind of low power, non-licensed transmitters. Spread spectrum techniques are often the most used technique by drone communication systems, [2].These techniques extend the spectral band occupied by the control signals, by the application of a pseudo random bit sequence on the data in the case of "Direct Sequence Spreading Spectrum, DSSS" or by the use of a pseudo random carrier frequency set in the case of "Frequency Hopping Spreading Spectrum, FHSS", [2]. Consequently, the RF link between the drone and its remote control-system strengthens its immunity against intentional and unintentional interferences by reducing the signal-to-noise ratio needed to establish the communication while maintaining a minimum of performance and increasing the margin jamming, [1]. The purpose of this paper is to counter the potential threat posed by drones by neutralizing the radio link between the targeted drone and its remote control-system.The principle consists in the formation a more powerful jamming signal, along the occupied band, to deteriorate the performance of the drone receiver by increasing the bit error rate. Statistically, this jamming signal must ideally approach a white noise with a constant spectral density. This feature makes it possible to interfere with all spectral components of the target signal with the same probability. In addition, it is noted that remote control systems are the main axis of attack against drones. In fact, the communication between drone and its control system do not respect any common standard and each designer uses its own private parameters. Therefore, using a barrage jamming type is the appropriate choice in this context, [3]. Indeed, jammers are categorized into four main classes, namely: barrage, tone, sweep and protocol-aware jamming, [4]. The performance of drone receivers under different types of jammers has been the subject of several studies in the literature. In [3], the author showed that barrage jamming is the best technique when there is no prior information on the parameters of the targeted system. With respect to monotone jammers, it has been shown in [2] that it is ineffective against FHSS systems; unlike a well-distributed multitone jammer, which has been remarkably effective for DSSS systems. In [5], it has been shown that the performances of the WLANs based on 802.11 standard degrade significantly under the effect of sweeping jamming using particular jump periods. In [6], [7], it has been shown that protocol-aware jamming can achieve effective jamming with very low energy requirements and low probability of detection of the jamming signal. In this work, we have designed a jammer device based on the statistical properties of chaotic systems which are widely used in cryptography and data security. We propose an appropriate model, whose jamming signals are obtained by quadrature amplitude modulation scheme. We customize the HDL reference design of the rapid prototyping SDR system AD-FMCOMMS5-EBZ to integrate the real time jamming signal generator based on hyperchaotic system. The characteristics of this SDR platform, particularly: the integration of two transceivers with 56 MHz bandwidth, allow us to target separately and in the same time the two sub-bands of WIFI support: (2.4 to 2.45 GHz) and (2.45 to 2.5 GHz). We implement the entire architecture, which include

the developed HC generator IP and the dual AD9361 transceiver control system, on the Zynq ZC706 evaluation board, , ensuring full coverage of the operating target band.

This paper is organized as follows: In the next section, we recall some general concepts on the jamming of the communication systems. Then, in Section III, we present the architecture of the proposed jamming device as well as the specification of the different modules allowing the realization of this device. In Section IV, we present the integration of the designed HC generator on the dual transceiver control architecture AD9361. We demonstrate the laboratory performed device and experimental results in Section V. Finally, some conclusions are drawn in Section VI as well as some scope for future works on this topic.

II. Jamming Requirements and Principles

Before presenting the model of our jammer, we describe, in this subsection, the main principles of the chosen jamming technique employed in this work as well as the barrage jamming in its simplest form as is thoroughly detailed in [2]. The metric expressing the jamming efficiency is the bit error rate (BER), which is a function of the SNR at the RF terminal of the drone receiver [2]. A successful jam requires a BER of 0.1 or higher, [2]. Our goal is then to decrease the signal to noise ratio by increasing the jamming to signal ratio JSR. The equations (1 and 2) give the expression of these parameters:

$$SNR_{dB} = 10 * log_{10}(\frac{P_{signal}}{P_{noise}}) \quad (1)$$

$$JSR_{dB} = 10 * log_{10}(\frac{P_{jamming} + P_{noise}}{P_{signal}}) \quad (2)$$

The Barrage jamming affects essentially the channel capacity of a communication system across the entire portion of spectrum occupied by the target with full duty cycle, both in the case of DSSS or FHSS communication technique. Therefore, this way is the best solution is to jam a remote-control system with unknown parameters.

III. The Proposed Jamming Model and Problem Formulation

We propose a jamming model that is based on a typical transmission chain using the Quadrature Amplitude Modulation scheme. The Fig.1 illustrates the different modules composing the jamming device.

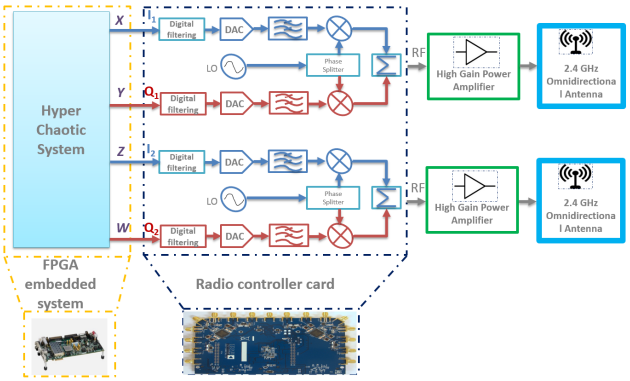

Fig. 1. Jamming model diagram.

the critical parameters of this architecture are the choice of the random digital signals generator, the bandwidth which is defined by The cutoff frequency f_{cuttof} and the carrier frequency. Given these parameters, the band occupied by each transmission chain is expressed by the following equation.

$$B_{jamming} = [f_{lo} - f_{cuttof}, f_{lo} + f_{cuttof}] \quad (3)$$

The Fig.2 shows the set channels used by WIFI LANs with reference to the standard IEEE 802.11, [8]. By projection on

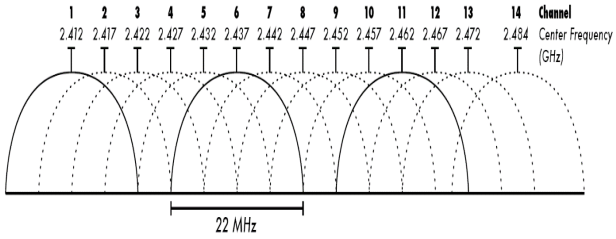

Fig. 2. Graphical representation of Wi-Fi channels in the 2.4 GHz band.

the parameters of the system to be attacked and to ensure a full coverage of the target band, we find two main technical requirements, namely: a suitable choice of carrier frequencies and a bandwidth parameter which enables to cover the full range of the WIFI band. For this purpose, it is proposed to subdivide the target band into two sub-bands. The first varies from 2400 MHz to 2450 MHz and the second from 2450 to 2500 MHz. Therefore, by choosing a 2425 MHz carrier frequency of the first transciever and a 2475 MHz as a carrier frequency of the second transciever, we hope to cover the integrity of the channels used for the instantaneous communication of radio controls between the drone and its remote control system.

To perform the architecture given by the model, we propose to implement the jamming signal generator on a digital platform. It is a hyperchaotic generator based on the resolution of a four-dimensional nonlinear differential Lorenz system. We make this choice in relation to the quality of its statistical properties. Then, the first and the second determined solutions are matched to the two components in phase quadrature necessary for the first modulator. Similarly, the third and the forth modulator are matched to the second modulator. Regarding the signal conditioning, modulation and RF conversion part, we go through a radio frequency controller with good performance in terms of robustness and reconfiguration. This is the FMCOMMS5-EBZ radio prototyping platform based on the built-in transceiver system AD9361. This transceiver is characterized by a wide operating bandwidth (70MHz-6000 MHz) with a channel width ranging from 200 kHz to 56 MHz. Therefore, it is fully compatible with the working band of remote controller communication systems. The ZC706 evaluation board will serve as a development platform for the implementation of the Pseudo Random Sequence Generator as well as the control architecture of the radio frequency converter.

IV. The Control Architecture

In our design flow, we base on the ”design reuse” approach by modifying the original HDL reference design given by Analog

Device. This approach allows saving the development time while providing a great effort of the architecture decortication. Indeed, the package relating to the FMCOMMS5-EBZ card includes an editable block design as well as software APIs allowing the configuration of the different architecture IP cores. Therefore, the object is to customize the transmission chain of the AD9361 transceiver by interfacing the data generator according to the technical specifications defined in the jammer model. The Fig.3 illustrates the main features of this architecture. It is implemented on a ZC706 evaluation board. The hardware design contains on a Programming Logic PL part including cores such as AD9361 core, FIFOs, communication bridges and as well as the developed HC generator. The zynq Processing System PS, based on dual ARM Cortex-A9, represent the part who supports the communication with the peripherals such as UART, Ethernet and interactions with the integrated cores using AXI protocol through High Performance HP ports. Therefore, NO Operating System software ensure the control of this architecture. The chip receives control signals produced by the dual ad9631 cores through the HPC and LPC-FMC connectors.

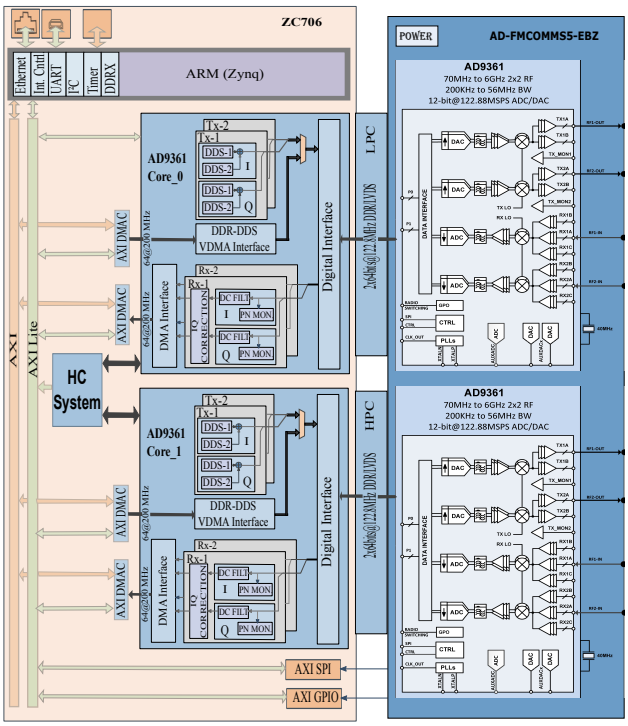

Fig. 3. Hardware design of the control architecture.

A. The HC generator formatting and packaging

We package the Lorenz resolution entity to design an IP core with a custom interface performing, simultaneously, the data exchange with the dual AD9361 cores and interactions with the ARM processor to take advantage of its versatility as shown in the Fig.4.

First, the synthesized resolution circuit is instantiated in the data-formatting unit that is on a higher hierarchy. This entity processes the contents of the buses (X, Y, Z and W) at the output of the Lorenz system's resolution circuit according to the state expressed by the signals (valid and enable) coming from the dual AD9361 cores shown in the Fig.4. It is important to note that the design of the resolution entity is adapted to the data exchange protocol while ensuring the synchronization between the cores by producing a new sample every each request transmitted by the AD9361 core. Each AD9361 core has four data inputs representing (I1, Q1, I2 and Q2). In our case, we use the first transmit channel of the first transceiver by connecting the X output to the first data input of the DAC core, the Y output to the second DAC data input. For the second transceiver, we use the Z and W outputs connected to the 5th and the 6th DAC data input. The size of the bus is 16 bits for each component and therefore corresponds to the fractional part of each dimension of the hyperchaotic generator system. The two AD9361 cores are in master position with respect to the HC generator, which is in slave position. Before packaging the entity thus obtained by the Vivado tool, we design a slave AXI_LITE port with four registers. These registers are accessible for reading and writing by the ARM processor. Thus, we bring controllability to the generator by matching the reset and start signals on one of these registers. In parallel, we develop software commands to write and read on these registers where each value of these registers gives a specific behavior of the HC generator. The

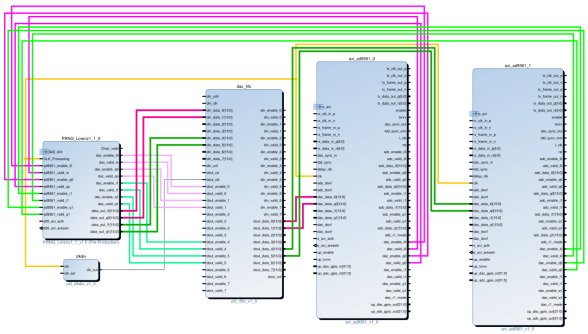

Fig. 4. The modified reference design.

integration of the HC generator in the reference design is shown in the Fig.4. It is equivalent to a FIFO write interface, which is connected with the read side of the DAC FIFO from which the first and the second AD9361 core read the data and transmits it to the dual AD9361 CHIP. Note that the integration of the new IP involve automatically a slight modification on the HDL design AXI_CPU_INTERCONNECT by adding a new port on the bridge, which is completely normal to support the new AXI_LITE connectivity. In addition, according to the HDL design clock routing, we use the mother clock signal of the AD9361 core to clock the resolution sub-circuit given that this clock goes four time faster than the effective data rate. Thus, we guarantee the synchronization between the HC generator core and the dual AD9361 core.

V. THE EXPERIMENTAL RESULTS

In this section, we present at first the specifications of a 4 channels WIFI targeted commercial drone remote control system. Fig.5 shows a visualization of remote control signals on a spectrum analyzer with cumulating mode. We can easily conclude that the radio link use frequency hopping between 4

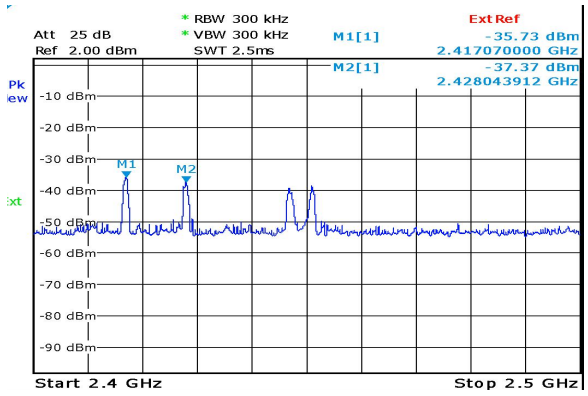

Fig. 5. Drone RF link specifications.

identified channels, as well as 2417, 2427, 2447 and 2452 MHz. The jamming barrage must be able to block the whole of this spreading band that is the perfect case of the ad-fmcomms5-ebz system performance.

Running the elf file, result of Software Defined Radio application compilation with the specified parameters, on the PS part of the zc706 card and visualization of the RF terminal in the spectrum analyzer gives us the evolution represented in Fig.6 and the Fig.7.

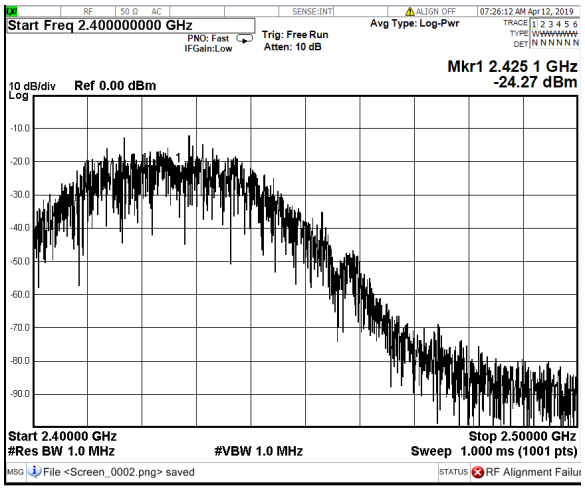

Fig. 6. Firt Tx channel spectrum output.

Analyzing these figures, we can note that the whole spectrum band was efficiently occupied, covering the different frequencies used by the remote controllers. Furthermore, the quality spectral density of the generated signal is uniform along the jammed band allowing a jamming effect with the same probability. This effect returns to the statistical parameters of the jamming sequence obtained by the chaotic generator. In addition, the fact of bypassing the analog filter in the transmission chain gives rise to a spectral window that is not perfect on the edges, which makes it possible to involve the neighboring components in the barrage jamming attack with enough amplification.

VI. Conclusion

In this paper, we have shown the utility of the Lorenz chaotic generator in terms of jamming remote control system of drones.

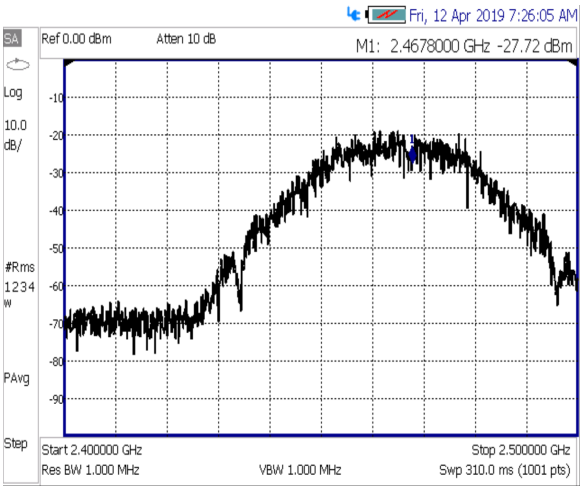

Fig. 7. Second Tx channel spectrum output.

Spectral coverage efficiency has been shown through experimental measurements to counter all kinds of spread spectrum techniques. The main contributions of this work is the hardware design of chaos signals generator with taking into account the timing requirement to make a real time interfacing with principal IP AD9361 controller. Thus, this customized IP will give another fields of applications such as securing streaming data. As future works, one can study the robustness and the agility of the rapid prototyping platform in addition to the reconfigurability of the control design will allow us to develop other techniques of jammers in order to make our embedded system to consume less energy and with a low probability detection. For example, the 4 by 4 receive chain can be exploited to develop a reactive jammer by making characterisation of the targeted communication drone system parameters and adequate the transmit chain to these estimated parameters.

References

[1] P. Hell, M. Mezei, and P. J. Varga, "Drone communications analysis," IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI), Herl'any, 2017, pp. 213-216.

[2] Richard A. Poisel, "Modern Communications Jamming Principles and Techniques," Artech House, 2011.

[3] T. Basar, "The Gaussian test channel with an intelligent jammer," in IEEE Transactions on Information Theory, vol. 29, no. 1, pp. 152-157, January 1983.

[4] P. L. Lineswala, S. N. Shah and R. Shah, "Different categorization for jammer: The enemy of satellite navigation," 2017 2nd International Conference for Convergence in Technology (I2CT), Mumbai, 2017, pp. 282-287.

[5] I. Harjula, J. Pinola and J. Prokkola, "Performance of IEEE 802.11 based WLAN devices under various jamming signals," 2011 - MILCOM 2011 Military Communications Conference, Baltimore, MD, 2011, pp. 2129-2135.

[6] A. Hussain, N. A. Saqib, U. Qamar, M. Zia and H. Mahmood, "Protocol-aware radio frequency jamming in Wi-Fi and commercial wireless networks'," in Journal of Communications and Networks, vol. 16, no. 4, pp. 397-406, Aug. 2014.

[7] D. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11b and other networks," in Proc. MILCOM 06, 2006, pp. 1075-1081.

[8] "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz Band - Corrigendum 1," in IEEE Std 802.11b-1999/Cor 1-2001, vol., no., pp.1-24, 7 Nov. 2001.