Master thesis : Study and Design of UAS Jamming Systems

Auteur : Heuchamps, Alexandre
Promoteur(s) : Redouté, Jean-Michel; 12799
Faculté : Faculté des Sciences appliquées
Diplôme : Master : ingénieur civil électricien, à finalité spécialisée en "electronic systems and devices"
Année académique : 2021-2022
URI/URL : http://hdl.handle.net/2268.2/14454

University of Liège - School of Engineering and Computer Science

Study and Design of UAS Jamming Systems

Author:
Alexandre Heuchamps

Supervisors:
Pr. J.-M. Redouté (ULiège)
Ir. C. Greffe (GeneriX)

Reading committee:
Pr. J.-M. Redouté (ULiège)
Ir. C. Greffe (GeneriX)
Pr. A. Papy (RMA)
Dr. Ir. M. Spirlet (ULiège)

Master's thesis carried out to obtain the degree of Master of Science in Electrical Engineering by Heuchamps Alexandre.
Academic year 2021-2022.

Acknowledgement

It is (very) seldom that the writing of a Master thesis is done alone. This work not being an exception, several people to whom I own acknowledgment have to be thanked.

First, and appropriately, I would like to thank my supervisors, Pr. J.-M. Redouté and Ir. C. Greffe, for various reasons, the first one being their great (infinite ?) patience to me during this whole year, the second for the subject of this thesis in itself, both extremely interesting and up-to-date, as the topics of drone and their non-destructive neutralisation seems to become a concern worldwide. I would also like to thank them for their guidance throughout the development of this thesis.

Next, I would like to thank some of the Microsys research lab from the university of Liège, with a particular focus on M. Diepart, H. Pierre, G. Digregorio, and F. Piron, as much for their constant good mood as for their wise advice and lunch times spent together. I would also like to express my gratitude to A. Calderon Jimenez whom, by its periodic appearances at Microsys, allowed to blow some steam off by cracking jokes and telling anecdotes.

Drones being a convergence point of various technical domains, several Master students were writing their theses in parallel of mine on more or less connected topics. In particular, A. Shehabi, F. Harmel, T. Pirottin, and L. Delfino, whose works consisted in RADAR drone detection, construction, and control of drones, respectively. The more or less narrow link between their works and mine allowed me to gain a broader vision on drone world, for which I thank them.

My next acknowledgment goes, of course, to my family, friends, and relatives, whom encouraged and bear with me throughout those two Master years. Without all these people, the result of this work would surely have been different to what it is today.

Also, to anyone who looks at this work: thank you for taking an interest in this thesis.

I would like to conclude this round of thanks by expressing once again my gratitude to all those who have followed and supported me throughout these two years of the Master. Thank you very much, and may these few lines make you happy/smile. Enjoy your reading.

A. Heuchamps,
June 2022.

Remerciements

La rédaction d'un travail de fin d'études est un processus qui s'effectue (très) rarement seul. Ce travail n'étant pas une exception, plusieurs personnes à qui je dois des remerciements me viennent en tête.

Tout d'abord, j'aimerais remercier mes promoteurs, Pr. J.-M. Redouté et Ir. C. Greffe, et ce pour diverses raisons, la première étant leur grande (infinie ?) patience envers moi au cours de cette année, la seconde étant pour le sujet de ce travail, à la fois intéressant et très actuel, puisqu'ayant attrait aux drones et à de possibles mesures de neutralisation non destructives. J'aimerais aussi les remercier pour leur aiguillage tout au long de la réalisation de ce mémoire.

Les prochains remerciements que j'aimerais exprimer vont à certains membres du laboratoire de recherche Microsys, et plus particulièrement à M. Diepart, H. Pierre, G. Digregorio, ainsi qu'à F. Piron, tant pour leur constante bonne humeur que pour leurs conseils avisés et temps de midi passés ensemble. J'aimerais également remercier A. Calderon Jimenez qui, par ses passages réguliers chez Microsys, m'a permis de souvent rire grâce aux diverses anecdotes qu'il racontait.

Les drones se trouvant à la confluence de différentes composantes techniques, plusieurs étudiants réalisant leur travail de fin d'études en parallèle au mien travaillaient sur des sujets plus ou moins connexes. Je pense entr'autre à A. Shehabi, F. Harmel, T. Pirottin, et L. Delfino, dont les travaux consistaient en la détection RADAR, la construction, et le contrôle de drones, respectivement. Le lien plus ou moins grand entre leurs travaux et le mien m'a permis d'avoir une vision plus large du monde des drones, ce pour quoi je leurs suis reconnaissant.

Mes prochains remerciements vont, bien évidemment, à ma famille, mes amis et, plus largement, mon entourage, qui m'ont encouragés et soutenus tout au long de ces deux années de Master. Sans leur soutient, le résultat aurait très probablement été différent de ce qu'il est aujourd'hui.

De plus, à toute personne posant les yeux sur ce travail : merci de porter un intérêt à ce mémoire.

J'aimerais conclure cette ronde de remerciements en exprimant une fois de plus ma gratitude à toutes celles et ceux qui m'ont suivi et soutenu tout au long de ces deux années de Master. Merci de tout coeur, et puisse ces quelques lignes vous faire plaisir/sourire. Bonne lecture.

A. Heuchamps,
Juin 2022.

Contents

List of Figures

Acronyms

ADC analogue-to-digital converter. 17, 22
ASK amplitude shift keying. 9
AWGN additive white Gaussian noise. 11, 12, 31, 36–38

BER bit error rate. 4, 11, 12, 14, 16
BIPT Belgian institute for postal services and telecommunications. 29

DAC digital-to-analogue converter. 17, 21
DSP digital signal processing. 19, 20, 38
DSSS direct sequence spread spectrum. 12, 13, 15

EASA European union aviation safety agency. 2
EIRP effective isotropic radiated power. 30
ESC electronic speed controller. 6, 7

FAA federal aviation administration. 2
FEC forward error correction. 19
FFHSS fast frequency hopping spread spectrum. 12
FHSS frequency hopping spread spectrum. 12–15, 17, 28, 39
FPGA field programmable gate array. 17, 21, 34
FSK frequency shift keying. 9, 24, 25, 28

GLONASS global navigation satellite system. 4
GNSS global navigation satellite systems. 2, 4, 40
GPS global positioning system. 4

IC integrated circuit. 21, 24
ISI intersymbol interference. 9
ISM industrial, scientific, and medical. 3, 7, 21, 28, 29

LNA low-noise amplifier. 21

MIMO multiple input multiple output. 21, 24

NCO numerically controlled oscillator. 12, 13
NDO nonlinear disturbance observer. 7
NN neural network. 7

OSI open systems interconnection. 12

PCM pulse-coded modulation. 7, 10
PID proportional, integral, and derivative. 7
PLL phase-locked loop. 21
PSK phase shift keying. 9

RF radio frequency. 2, 3, 9, 14, 21, 24
RSSI return signal strength information. 28
Rx receiver. 3, 4, 13, 17, 22, 27, 29, 32

SDR software defined radio. 4, 17, 19–22, 24, 28, 31, 33, 39
SFHSS slow frequency hopping spread spectrum. 12
SMC sliding mode control. 7
SNR signal-to-noise ratio. 11, 30
SPI serial peripheral interface. 21
SS spread spectrum. 4, 7, 12, 20, 39

TSP transceiver signal processor. 21, 22
Tx transmitter. 3, 4, 13, 17, 22, 27, 29, 33

UAS unmanned aerial system. 1–4, 39
UAV unmanned aerial vehicle. 1, 2, 4–6

VNA vector network analyzer. 28

1 Introduction[1]

Unmanned aerial systems (UASs) and unmanned aerial vehicles (UAVs), the latter being commonly known as drones, are today's main disruptive technology, and will continue to dominate the future of flight. With their wide span of sizes and shapes, drones are extremely versatile, offering a large variety of functions, in different areas, ranging from State and Public applications, to Industrial ones, through Commercial, and even recreational ones, some of which shown in figure 1.1.

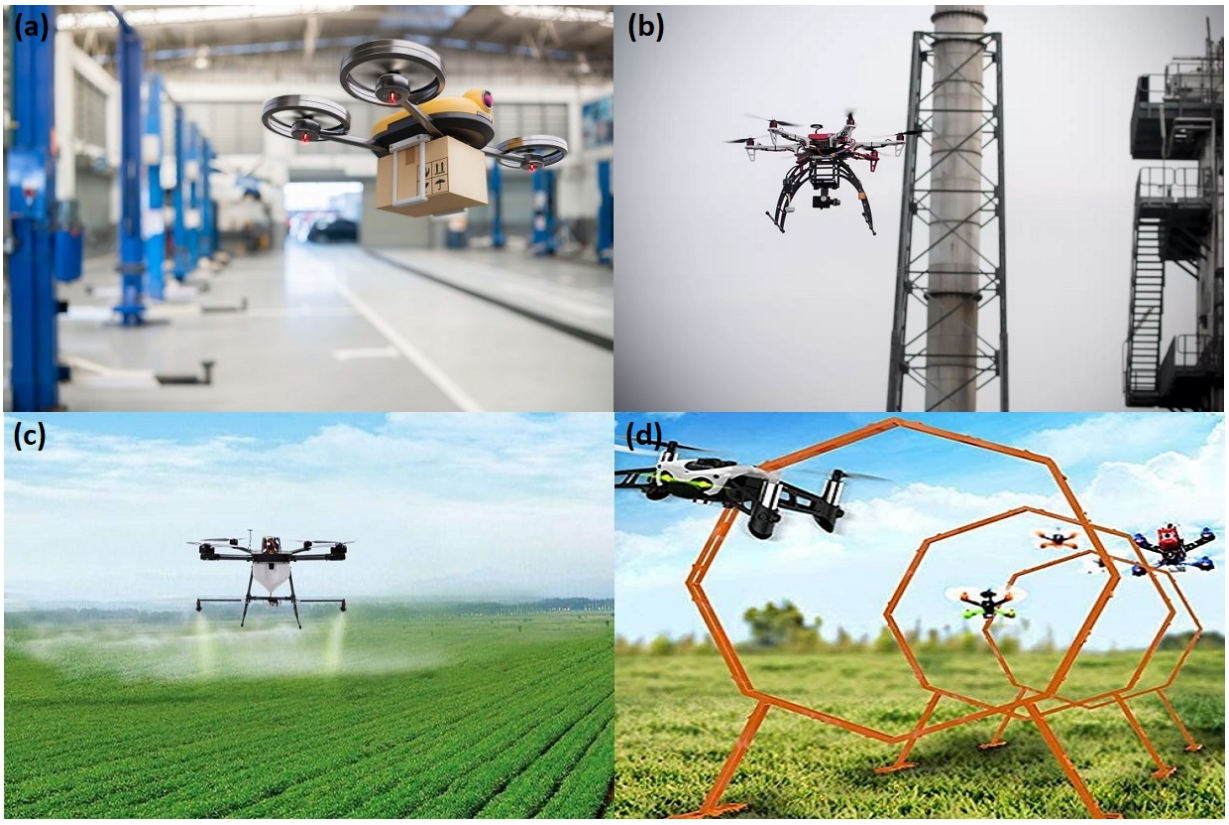


Figure 1.1: Illustration of some of civil drone applications, with emphasis on **(a)** commercial (Shutter2U/iStock), **(b)** industrial (Protek-Labo), **(c)** agronomic (Guide Drone), and **(d)** recreational usages (Amazon). Sources last accessed on 27th May 2022.

Those drones offer various advantages, such as (i) a relative low cost, (ii) an arguably long operating range, (iii) an increase in work productivity, and (iv) a reduced risk to human life in

[1]In the following, all images are used under the "fair use" licence.

some situations, which led to their mass production and integration into military planning [1], [2].

Despite their significant functional, technological, and economical benefits, UAVs pose regulation and oversight challenges, primarily due to their dual-use: drones' cheapness and user-friendliness led that technology to nefarious usages. Indeed, terrorists have been dabbling with drones for various purposes and with varying degrees of success for more than two decades now: in 1994, a civilian minicopter initially intended for crop spraying was used in an attempt to disperse sarin gas on Tokyo. Another, more recent, example involves the use of drones to attempt murder on Venezuelan president Maduro in 2018. Even today, in the Russian-Ukraine war, drones are being used extensively [3].

Other examples, presumably not terroristic, include several nuclear power plants overflights in France [4] and Belgium [5], airport traffic disruption, privacy intrusion, and much more, (non-exhaustive lists of such happenings can be found in [6] and [7], for example). All these examples tend to converge to the same conclusion: States need regulations and means to enforce them.

To mitigate, or even prevent, the possible risks posed by rogue drones, some regularisations have been put into place by States [8]–[10], as well as regulation bodies, such as the European union aviation safety agency (EASA) in Europe and the federal aviation administration (FAA) in the United States of America. However, even with these regulation bodies, the enforcement of these laws and regulations remains a challenge, hence the need for effective and efficient UASs detection and neutralisation techniques, as the European research call ISFP-2020-AG-CUAS "UAS Countermeasures" highlights.

Fortunately, with time, more and more solutions have been deployed to either detect, track, and/or neutralise rogue flying systems. Some of those detection and tracking technology rely on (i) acoustic [11]–[13], (ii) imaging [14]–[17], (iii) radio frequency (RF) [18]–[20], or (iv) hybrid [21], [22] technologies, some of which are shown in figure 1.2. Regarding neutralisation, a

Figure 1.2: Different UAV monitoring techniques. Image from [23].

plethora of means and techniques exist, such as (i) electromagnetic pulses [24], [25], aimed at damaging/destroying internal electronics of the targeted drone (ii) RF jamming and spoofing, aimed at communication link disruption, (iii) projectiles and missiles, either guided or not, to completely destroy the drone, and even (iv) prey birds [26], specially trained to attack enemy drones. Some of these neutralisation techniques are shown in figure 1.3. Recently, the French MC2-technologies company even developed FlyJam, a flying jamming platform claimed to be efficient against 95% of commercial drones.

Scope

This master thesis is aimed at implementing a countermeasure to neutralise rogue UASs. Drones usually have a preprogrammed flight route and use global navigation satellite systems (GNSS)

Figure 1.3: Some of the possible neutralisation techniques, with emphasis on **(a)** electromagnetic pulse (image from Epirus Systems), **(b)** RF jamming (image showing the DroneGun Tactical™ from DroneShield), **(c)** missile (image showing the Red Sky 2 Drone Defender System by IMI Systems), and **(d)** eagle (as used by the French French Air Force) techniques. Sources last accessed on 27th May 2022.

signals to follow that path, or are being manually piloted using a remote controller. In the case of a preprogrammed flight trajectory without any feedback signal, the various detection techniques cited previously can be used (excepted for passive RF spectrum analysis). On the other hand, in case of a remotely-controlled drone, or if it transmits a video and/or positional feedback, such signal can be spotted in the RF spectrum, and be acted upon.

This work focuses on the jamming, and subsequent disruption, of a communication link between a drone and its remote controller, in a typical situation represented in figure 1.4. In that figure, an external jammer disrupts the communication link between a transmitter (Tx) (a remote controller in this case) and a receiver (Rx) (a drone in this work).

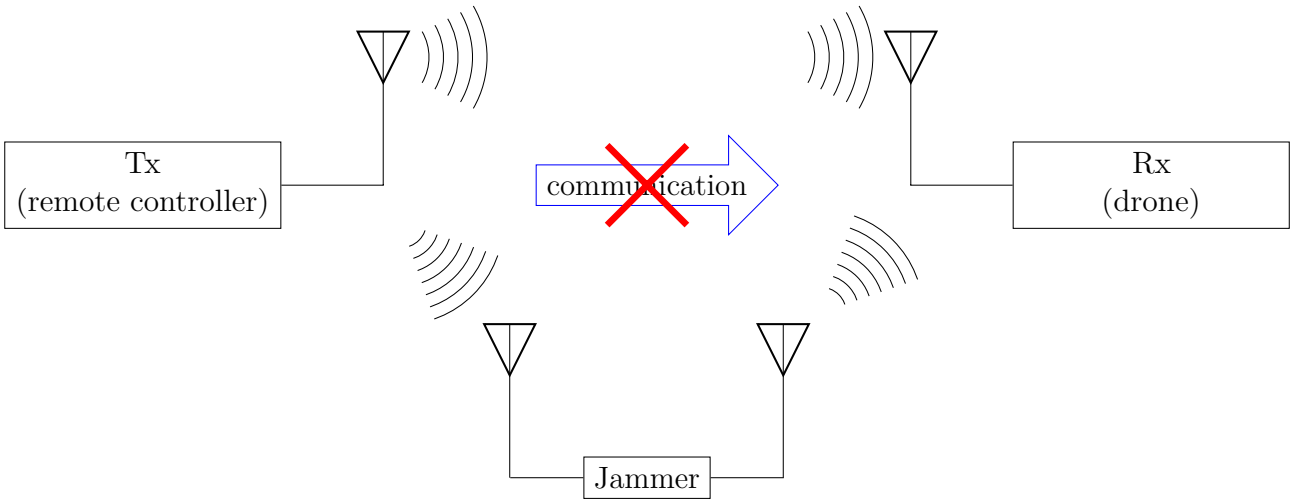


Figure 1.4: Graphical representation of the communication link jamming between a Tx and a Rx by means of a third party jammer.

Problem statement

As already stated, the aim of this thesis is to implement a UAS neutraliser by disrupting the communication link existing between a rogue drone and its remote controller. This is achieved by inspecting the RF spectrum. In this work, the targets communicate in the 2.4 GHz industrial, scientific, and medical (ISM) band, chosen due to its widespread use amongst commercially available and hobbyist UASs [27].

Considering the wide range of applications using the considered frequency band, the developed jamming technique should minimise its impact on non-targeted devices. This limits the employable jamming techniques not only on an efficiency criterion, but also on its impact to other applications. For example, so-called barrage and sweep jammers have less specificity than protocol-aware jamming, hence are more prone to interact with untargeted devices.

Figure 1.4 shows a graphical representation of a protocol-aware jamming strategy, where the jammer synchronises on the frequencies used for the communication between the Tx and Rx, and emits enough energy at the desired moment so as to increase sufficiently the bit error rate (BER), ultimately resulting in the UAV neutralisation. More precisely, considering the widespread use of spread spectrum (SS) methods in controller-drone communications [28], [29], focus on such method is placed.

Some drones use preprogrammed flight routes using GNSS, under which global positioning system (GPS), global navigation satellite system (GLONASS), Galileo, or Beidou[2], for which there exist an extensive literature on jamming/anti-jamming [30]–[32]. The jamming and/or takeover of such signals is out of scope for this work, as are the detection and neutralization of possible video and telemetry information, which are all left as future prospective works.

Thesis overview

As Sun Tzu taught in his *The Art of War*: ‘ If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle. ’ [33], which, once transposed to this work, could be translated to something like ‘ All drones can be defeated if their strengths, weaknesses, and operating modes are known. Not understanding UASs will lead to unsuccessful countermeasures ’. By following this principle, theoretical reminders are given in chapter 2. More specifically, some generalities about drones are presented in section 2.1, with emphasis on their classification and on their onboard hardware. The discussion is then extended to general telecommunication principles in section 2.2, where all the necessary material and vocabulary is introduced to gain further insight into the jammed link. Further exploring the communication link of interest, SS techniques are exposed in section 2.3. Finally, section 2.4 discusses some of the existing jamming techniques.

The discussion continues in chapter 3, where both hardware and software platforms are presented in section 3.1 and section 3.2, respectively. More specifically, generalities regarding software defined radios (SDRs) are discussed in section 3.1.1, which are then transposed to the device used in this work in section 3.1.2. In section 3.2, the software platform used to interface the hardware is briefly presented.

Building upon the previous theoretical reminders, results for software implementation of various jamming techniques presented in section 2.4 are presented in chapter 4. More precisely, the experimental setup and signal characterisation are first presented in section 4.1. From there, the implementation results for barrage, sweep, and reactive jammers are given in sections 4.2.1 to 4.2.3, respectively. Building upon the results, a conclusion with several possible prospective works is given in chapter 5.

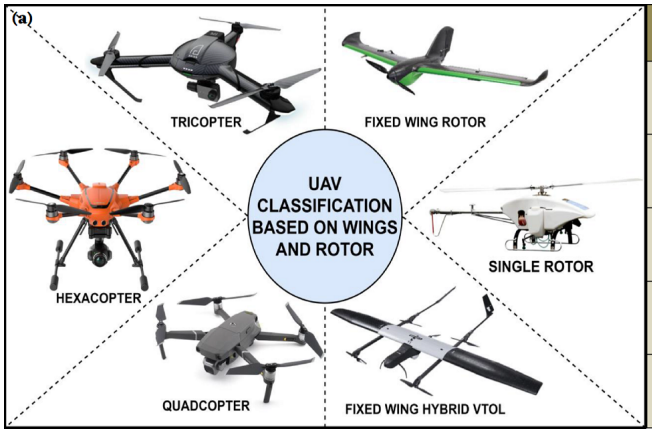
[2]Beidou is a Chinese GNSS consisting in a satellite constellation, initially functional for most part of the Asia-Pacific region in December 2012.

2 Background

2.1 Drone rudiments

2.1.1 General classification

UAVs can be operated remotely by a pilot, or autonomously, through different onboard computers and navigation systems, to accomplish scores of missions. This wide variety of drone usages implies a multiplicity of classification criteria: Defense and security UAV operators classification (a NATO UAVs classification can be found in [34]) differs from ever-evolving civilian ones. Despite the differences, drones can be classified based either on their size, range, type, number of propellers, endurance, etc. An extensive classification review can be found in [35], while a graphical representation of some of the possible classification criteria is shown in figure 2.1.



(b)

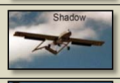
UAS Groups	Maximum Weight (lbs) (MGTOW)	Normal Operating Altitude (ft)	Speed (kts)	Representative UAS	
Group 1	0 – 20	<1200 AGL	100	Raven (RQ-11), WASP	
Group 2	21 – 55	<3500 AGL	< 250	ScanEagle	
Group 3	< 1320	< FL 180		Shadow (RQ-7B), Tier II / STUAS	
Group 4	>1320		Any Airspeed	Fire Scout (MQ-8B, RQ-8B), Predator (MQ-1A/B), Sky Warrior ERMP (MQ-1C)	
Group 5		> FL 180		Reaper (MQ-9A), Global Hawk (RQ-4), BAMS (RQ-4N)	

Figure 2.1: Some UAVs classification criteria, based either on **(a)** wings and rotors [23], or **(b)** various other criteria [36] ("AGL" = Above Ground Level, "FL" = Flight Level).

The goal of this thesis not being to give an extensive overview of the various possible drone classifications, no further discussion on that subject will be made.

2.1.2 Drone hardware and software rapid analysis

A drone can be seen as the interconnection of different interacting modules, such as (i) power modules, responsible for power distribution to targeted devices, (ii) sensor module(s), responsible for feedback provision on various drone parameters and further consequently acting, (iii) a communication module, responsible for the interaction between the drone itself and external devices (ground and/or navigation stations), and (iv) one or several control unit(s), used to

link all the other modules together and ensure correct drone behaviour in various conditions. A graphical, high-level, representation of those modules and their interconnection is shown in figure 2.2. The aim of this work lying in the communication link disruption between a drone and its controller, no extensive discussion on various modules will be given, although a concise summary overview on some typical drone modules is given in the remainder of this section.

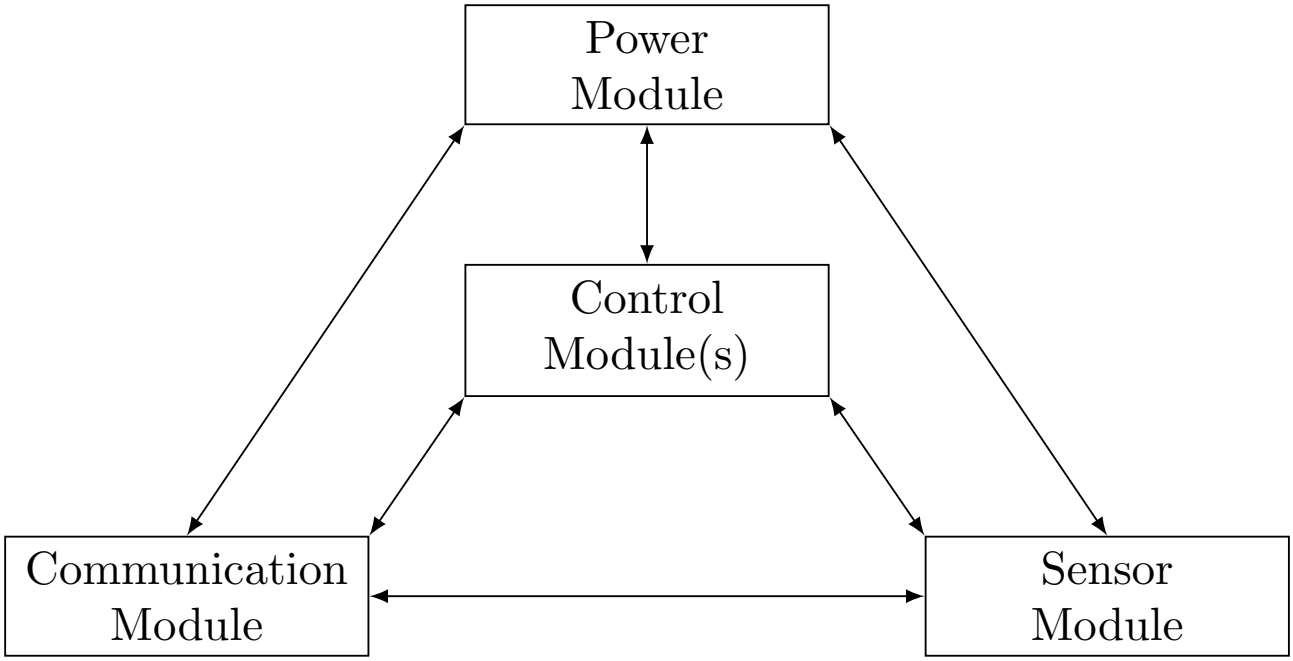


Figure 2.2: Graphical, high-level, representation of a typical UAV module interconnection.

Power module

The (analogue) power module is meant to provide regulated power, usually from a lithium-polymer (LiPo) battery due to their high energy density for a given weight, as well as current and battery status monitoring, to the flight controller. Those information sent to the controller will in turn allow for triggering failsafe warning and other actions in case of a low battery level.

Power modules usually include a backup battery system for increased UAV reliability and (potentially) autonomy. Some drones with advanced power systems implement a power distribution system, allowing to modulate the power withdrawal per the motor and payload requirements [37].

Sensor module

As already stated, drone application span is very large, hence a possibly large set of embedded sensors. Whereas some are mission-specific, others are mandatory for good drone behaviour, such as (i) electronic speed controllers (ESCs), aimed at regulating the propellers rotation speed, (ii) gyroscopes, used to acquire information about the drone orientation, (iii) accelerometers, serving various purposes such as drone orientation evaluation, and feedback provision on environmental factors (such as wind, for example), (iv) a combination of accelerometers and gyroscopes (with magnetometers) into a single device known as an inertial measurement unit (IMU) (the two previous sensors are combined into a new one to correct their weaknesses, i.e. short-term noise for accelerometers and long-time drift of gyroscopes), and (v) a compass, used by the drone to know its trajectory and orientation.

Control module

The control module can be seen as the brain of the drone, serving a plethora of different functionalities, from which the most fundamental is, unsurprisingly, to control the drone behaviour. By acquiring and fusing information returned by various onboard sensors, the controller is able to calculate the desired rotation speed for the propeller(s), send it to the ESCs, which translates that request into a motor-friendly format.

All the computations, information acquiring and fusing, and drone safety and durability evaluation, are made in software. Various controller types, linear or not depending on the drone type, can be used, such as proportional, integral, and derivative (PID), neural network (NN), sliding mode control (SMC), nonlinear disturbance observer (NDO), amongst others [38].

Communication module

Whether the drone operates autonomously or not, a certain communication with a remote station is required. The communication usually take place in free ISM bands, such as those at 2.4 and 5.7 GHz [39], through the use of antennas of various types and geometries.

The goal of the communication module is precisely to ensure that communication is effective and efficient, and implements various ways to achieve its goal. One of these methods consists in "hiding" narrowband information in a much wider bandwidth, known as SS technique, discussed more thoughtfully in section 2.3.

2.2 Telecommunication rudiments

The goal of this thesis being to disrupt a communication link, an introduction to digital telecommunication seems appropriate. A communication chain from information source to information sink is shown in figure 2.3, where a distinction between optional and essential blocks is made. Some of those blocks will now be presented and briefly discussed.

Formatting and baseband modulation

First, a source produces information which is formatted into a format suitable for digital treatment, assuring compatibility between the information and the signal processing steps within the communication system. Depending on the nature of the information produced by the source, different steps have to be undertaken, as shown in figure 2.4: digital information bypasses the formatting block, while textual information has to first be encoded before transmission, and analogue signals first have to be sampled and quantized, prior to any encoding.

The information is conveyed as a bit stream through the other blocks, up to the modulation part, where the message symbols (or channel symbols if channel coding is used) are converted to channel-compatible waveforms, i.e. waveforms compatible with constraints imposed by the channel. Depending on whether the modulation is applied to binary or non-binary symbols, the resulting waveform is called either pulse-coded modulation (PCM) (various possibilities being shown in figure 2.5) or M-ary pulse-modulation waveform, respectively. It should be noted that PCM waveforms requiring only two levels are particular cases of M-ary pulse-modulation waveforms (with $M = 2$).

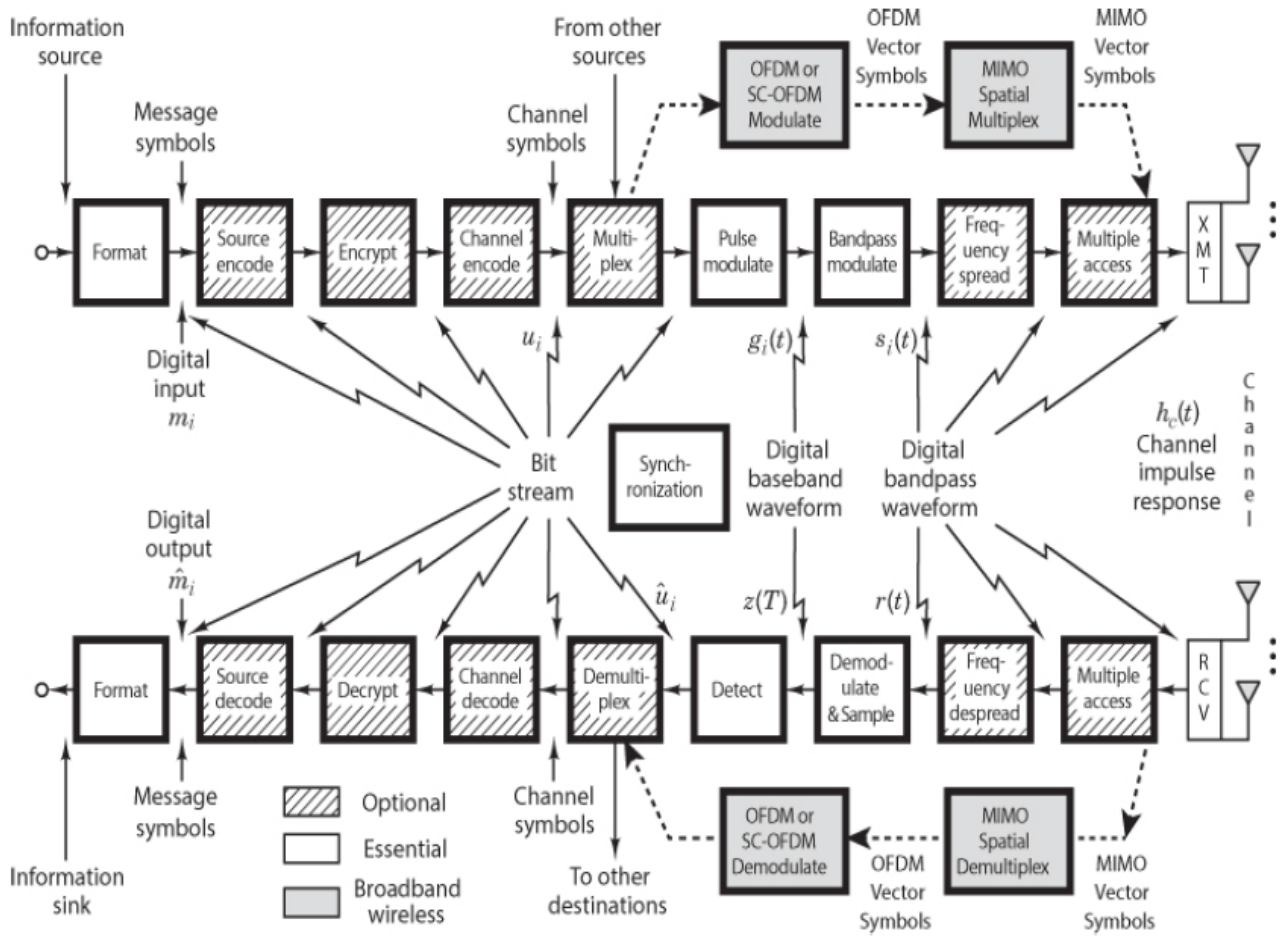


Figure 2.3: Block diagram view of signal flow between an information source and sink, through transmitter and receiver (with intermediate signal processing steps), of a typical digital communication system. Image from [40].

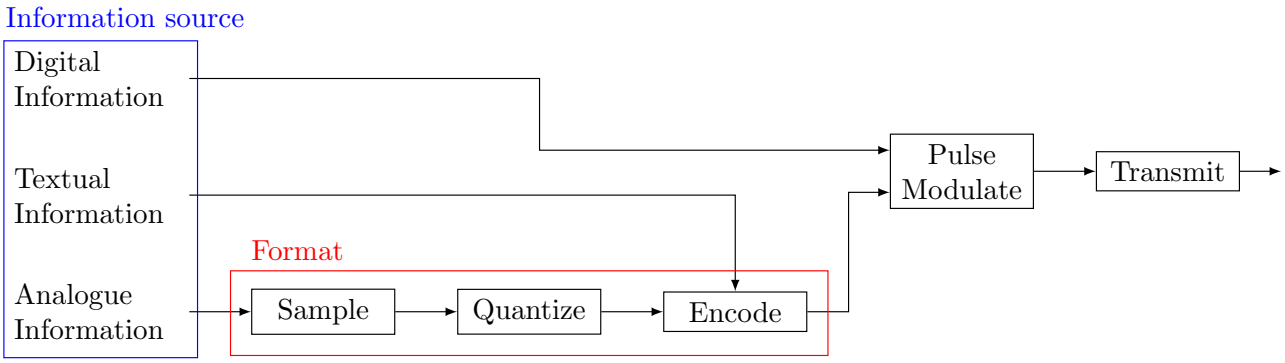


Figure 2.4: Formatting and transmitting of baseband signals. Image adapted from [40].

Bandpass modulation

After pulse modulation, each message or channel symbol is represented by a baseband waveform $g_i(t)\,(i = 1, \ldots, M)$, which then goes through a bandpass modulation block, transforming the pulse-like waveforms into medium-friendly signals, i.e. baseband pulse-like waveforms are converted into bandpass waveforms $s_i(t)\,(i = 1, \ldots, M)$, obtained by modulating a carrier wave by the shaped pulses.

In RF communications, the bandpass waveform $s_i(t)$ can be written as a sinusoid, i.e. under the form $s_i(t) = A(t)\sin\left[2\pi f(t)t + \theta(t)\right]$, where $A(t)$, $f(t)$, and $\theta(t)$ represent the instantaneous amplitude, frequency, and phase, respectively, hence three different physical characteristics of the wave can be altered to convey information. Depending whether the information is placed on the amplitude, frequency, or phase, the bandpass modulation format is known as amplitude shift keying (ASK), frequency shift keying (FSK), or phase shift keying (PSK), respectively, and are shown in figure 2.6 for the bitstream `10110`. More formally, a bandpass waveform $s(t)$ can be written under the form

$$s(t) = \mathrm{Re}\left\{\psi[m(t)]e^{j(2\pi f_c t + \varphi_c)}\right\}, \tag{2.1}$$

where f_c and φ_c are carrier parameters, j is the complex number such that $j^2 = -1$, and where $\mathrm{Re}\,\{\cdot\}$ represents the real-part operator. The form of the complex function $\psi[m(t)]$, related to the modulating signal $m(t)$ (i.e. the information-bearing signal), defines the type of modulation: in the case where $\psi[m(t)]$ is a linear function of $m(t)$, the modulation is called linear, whereas if $\psi[m(t)]$ takes the form $e^{j\varphi[m(t)]}$, with $\varphi[m(t)]$ being a linear function of $m(t)$, the modulation is of angular type. The expression appearing in (2.1) can be further decomposed into a real an an imaginary part, i.e.

$$\begin{aligned} s(t) &= \mathrm{Re}\left\{\psi[m(t)]e^{j(2\pi f_c t + \varphi_c)}\right\} \\ &= \psi_I[m(t)]\cos\left(2\pi f_c t + \varphi_c\right) - \psi_Q[m(t)]\sin\left(2\pi f_c t + \varphi_c\right), \end{aligned}$$

known as IQ, or quadrature, decomposition. Before the signal is send in the channel, it has to be filtered so as to (i) exhibit a finite duration, commensurate with the symbol duration T_s, and (ii) reduce intersymbol interference (ISI), possibly resulting in a signal corruption. In the case of a binary FSK signal, the information is encoded onto the frequency of the signal, and can be written under the form $m(t) = \sum_{k\in\mathbb{Z}} a_k g_k(t - kT_s)$, where a_k are the bits representation, and where the shapefunctions $g_k(\cdot)$ are usually the same for all symbols, i.e. $g_k(\cdot) \to g(\cdot)$.

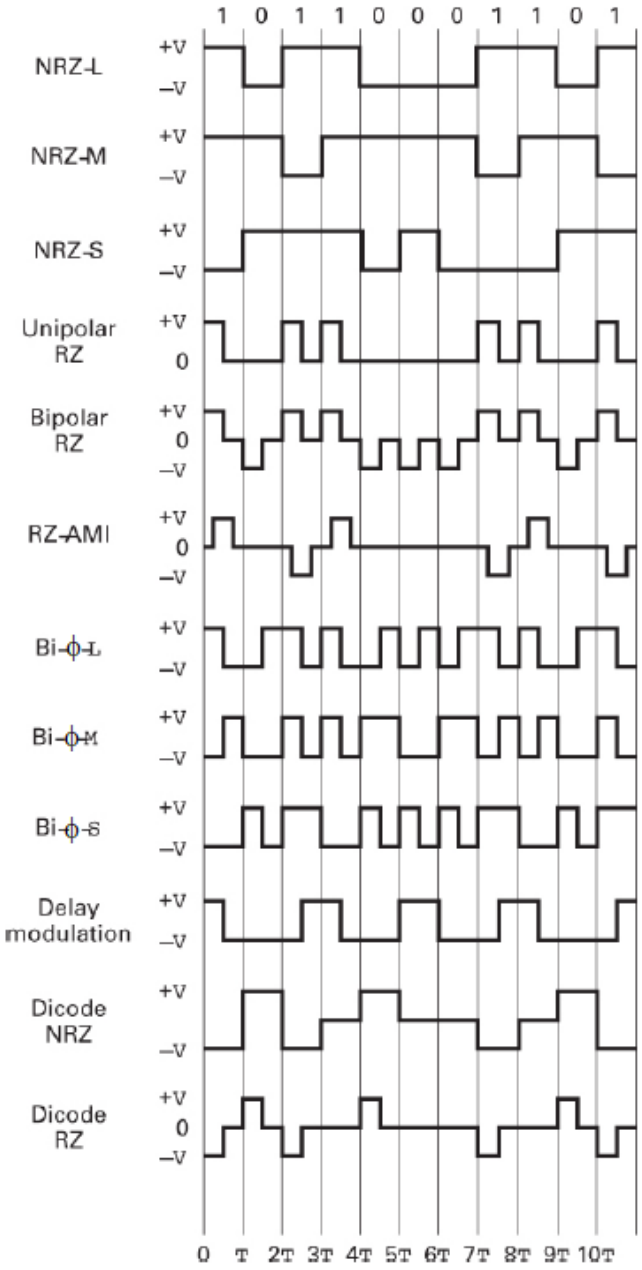


Figure 2.5: Various PCM possible waveforms, for binary symbols having period T. Image from [40].

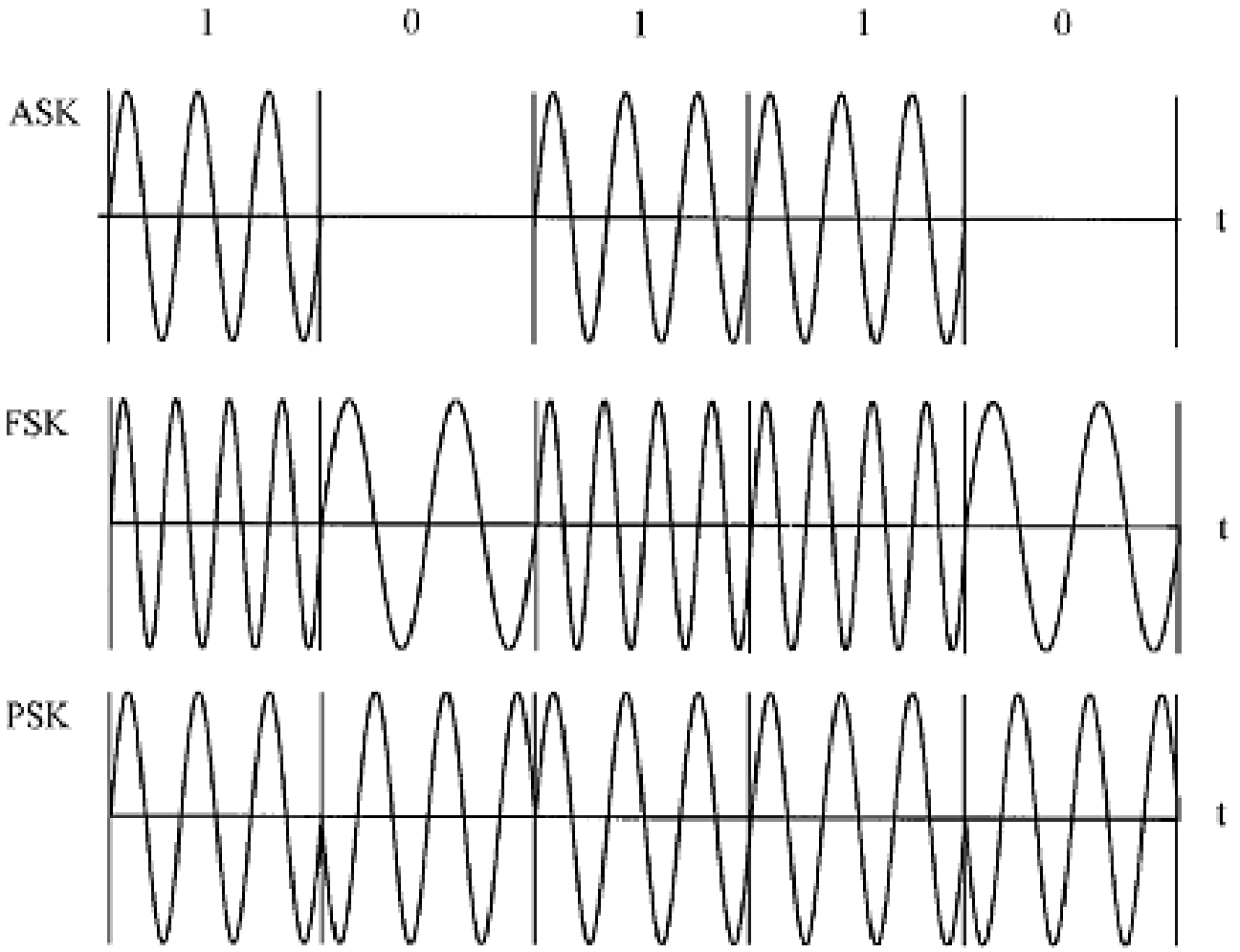


Figure 2.6: Time representation of amplitude, frequency, and phase shift keying for the `10110` bitstream. Image from [41].

Channel transmission and demodulator input

As the signal $s_i(t)$ propagates from the transmitter, through the channel, up to the receiver, it undergoes a series of perturbations, so that the received signal $r_i(t)$ reads

$$r_i(t) = s_i(t) \otimes h(t) + n(t) \quad (i = 1, \ldots, M),$$

where $h(t) = h_t(t) \otimes h_c(t) \otimes h_r(t)$ is the complete system's impulse response, consisting of the combination of the transmitter's filter impulse response $h_t(t)$, the channel's impulse response $h_c(t)$, and the demodulator's impulse response $h_r(t)$, $n(t)$ is noise (usually additive white Gaussian noise (AWGN)), and $\otimes$ is the convolution operator. The principal idea of a jammer is to increase the noise $n(t)$, so that the received waveform is too different from the sent one, leading to an incorrect communication between transmitter and receiver or, stated otherwise, increase the BER above the understanding threshold. This idea comes from the discovery by Claude Shannon in 1948 that the maximum capacity C of a channel, in terms of information bits per second, was linked to the signal-to-noise ratio (SNR) through the relation [42]

$$C = B \log_2 \left(1 + \frac{P_S}{P_N}\right) = B \log_2 \left(1 + \frac{E_b R_b}{N_0 B}\right), \tag{2.2}$$

where B represents the channel's bandwidth, P_S and P_N the signal and noise powers, respectively, E_b and R_b the energy per bit and the bitrate, respectively, and N_0 the power spectral density of

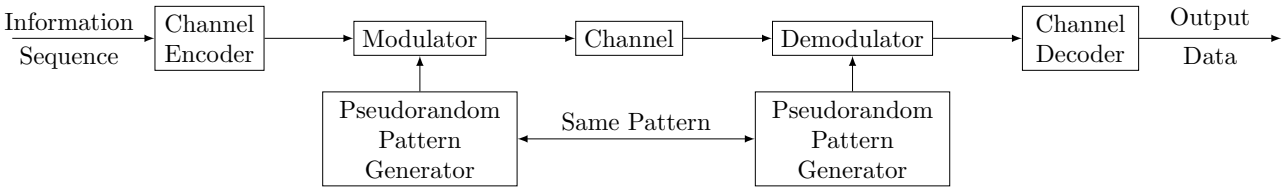


Figure 2.7: Model of a spread spectrum digital communication system, where the pseudorandom pattern generator has to generate the same values at the emitter and receiver, at the right time. Image adapted from [48].

the AWGN. Per (2.2), irrespective of system's nature (be it analogue or digital), increasing the noise level (or, equivalently, the noise power P_N) reduces the channel capacity, meaning that all excess information with respect to C is lost for the receiver, hence a bigger BER.

2.3 Spread spectrum

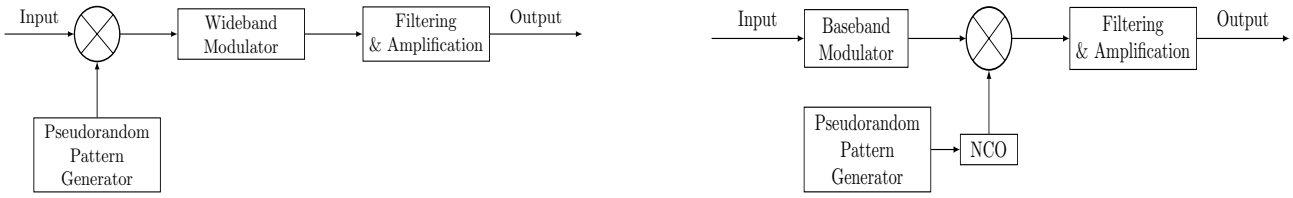
Originally developed in 1941 to remotely control dirigible crafts, such as torpedoes [43], spread spectrum techniques are now ubiquitous in communication systems [44]–[46]. Such techniques can be decomposed in two main families, namely direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS), the last one being subdivided into slow frequency hopping spread spectrum (SFHSS) and fast frequency hopping spread spectrum (FFHSS). No matter the technique used, the general idea is to spread the message to be sent over a bandwidth much bigger than the information rate, expressed in $\mathrm{bit\,s^{-1}}$.

The goal of such spectrum spreading techniques is manyfold, and consists in (i) combating detrimental effects of interference due to jamming, channel sharing, and multipath fading, (ii) hiding the signal by transmitting it at low power, making it difficult for an external listener to discriminate between the message and the background noise (in case of DSSS), or rapidly switching the carrier frequency, swiftly avoiding detrimental spectral bands (in case of FHSS), and (iii) achieving message privacy in the presence of other listeners. Consequently, in a seven-layer open systems interconnection (OSI) model, SS techniques can be seen as a layer 0 (PHY layer) encryption method [47].

The last point, message secrecy, is obtained by introducing unpredictability or (pseudo)-randomness in each of the transmitted coded signal waveforms known to, and hopefully only to, the intended receiver. A general, high-level, view of such spread spectrum digital communication system is shown in figure 2.7, where the pseudorandom pattern generator at the modulator and demodulator sides must generate the same pattern, at the right time [1]. The pseudorandom sequence is usually generated by the output of a feedback shift register, or by combining the outputs of feedback shift registers.

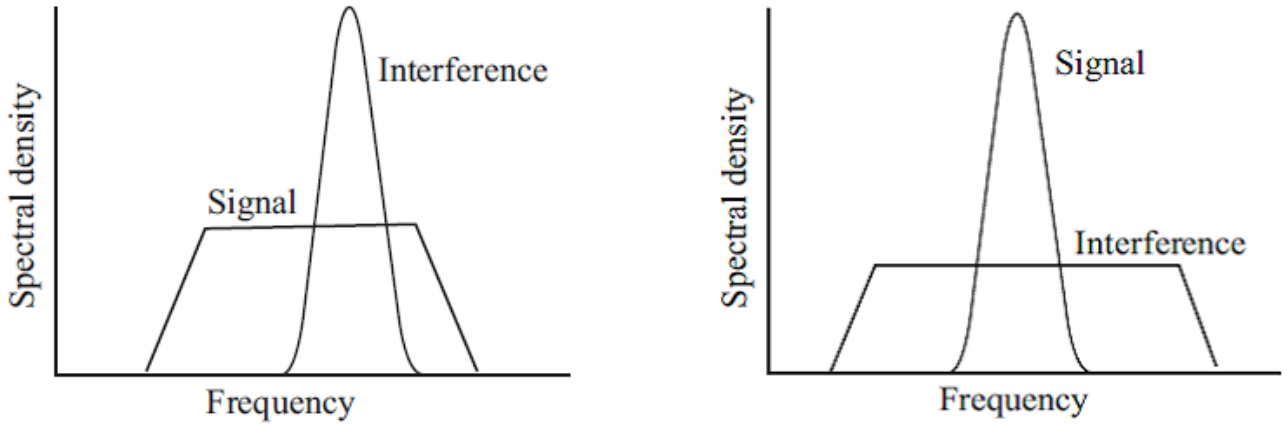
The working principle between DSSS and FHSS being different, the hardware underlying these principles must also be, at least partially, different. These differences are schematically shown in figure 2.8, where it is seen that for DSSS the pseudorandom pattern is directly applied onto the message before further treatment, while for FHSS it is fed to a numerically controlled oscillator (NCO), generating a pseudorandom carrier frequency. From that figure, it is now

[1]Here, "at the right time" means that the receiver must implement some code synchronisation mechanism, usually split into code acquisition and tracking operations, to precisely or nearly coincide with the instant where the signal was emitted by the emitter. If the signal at the receiver does not coincide more or less precisely with what was emitted by the emitter, the resulting misalignment would result in a decreased receiver-signal amplitude, the amount of which would correspond to the autocorrelation function of the signal.



(a) DSSS **(b)** FHSS

Figure 2.8: Main principle behind **(a)** DSSS, and **(b)** FHSS communication-enabling hardware. Images adapted from [49].



(a) Tx **(b)** Rx

Figure 2.9: Graphical representation of the desired signal and interference spectra of a DSSS transmission method at **(a)** the output of the wideband modulator on the transmitter side, and **(b)** the demodulator input on the receiver side. Images from [50].

clear that the concept behind DSSS is spectral spreading, as the input and random pattern multiplication yields a much broader spectrum than that of the sole input, while the working principle behind FHSS is avoidance, as the result of the random number application on the NCO results in a carrier change, allowing the signal to quickly change from an unfavourable frequency band to a better one. In the following, some more precise discussion about direct sequence spreading and frequency hopping is given.

2.3.1 Direct sequence spread spectrum

The general principle of a DSSS transmitter was shown in figure 2.8a, which highlights the mixing principle between a high-rate pseudorandom spreading sequence and a lower-rate code symbol sequence, resulting in a higher-bandwidth transmitted signal (compared to that of the sole code symbol sequence). At the receiver, mixing the received signal (useful signal + noise) allows to retrieve the narrowband sent message, as well as decrease the noise importance. The spreading and despreading operations are both shown in figure 2.9, form which it is clear that the noise effect is limited by the spreading. By further implementing some sort of envelope or energy detection mechanism, the noise can be separated from the message, which can then be further interpreted by the receiver and perform the corresponding action.

2.3.2 Frequency hopping spread spectrum

The general principle of a FHSS transmitter was shown in figure 2.8b, which highlight the fact that a pseudorandom number is fed to a controlled oscillator, producing a certain carrier frequency.

The sequence of carrier frequencies produced by such a system is known as the frequency-hopping pattern, and if M different carrier frequencies are possible, the set $\{f_1, \ldots, f_M\}$ is known as the hopset. The rate at which the carrier frequency is changed is the hop rate, and the frequency band over which the hopping is possible is the hopping band, which includes M frequency channels (or simply channels). A graphical representation of those concepts is shown in figure 2.10, for a system in which the hopping band and each channel have a bandwidth of W

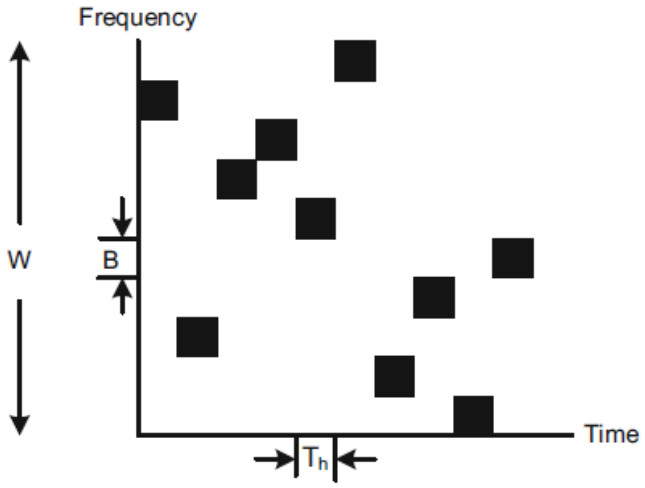


Figure 2.10: Graphical representation of a typical FHSS spectrograph, where the hopping band and each channel have a bandwidth represented by W and B, respectively, and where the carrier changes every T_h second, the hopping time. Image from [50].

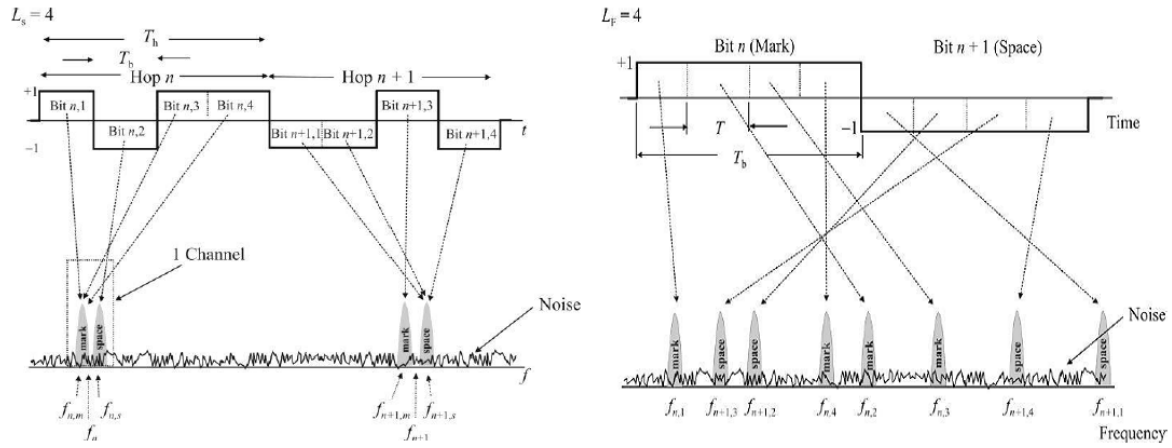
and B, respectively, and where the hopping time (i.e. the elapsed time before carrier switching) is T_h. Once again, implementing some sort of energy detector, together with all the required decoding and demodulation, at the receiver allows to retrieve the message given that the right carrier frequency is known.

Frequency hopping techniques may be classified as either fast or slow. In the case of fast hopping, each information symbol is transmitted by multiple frequency hops, while slow hopping ensues if one or more information symbols are transmitted between each hop. Slow and fast hopping are schematically represented in figure 2.11 (with data encoded as a binary NRZ signal), where a symbol is constituted by four bits in the case of slow hopping, and where four hops per bit are used in the case of fast hopping.

2.4 Jamming techniques

Adversarial parties in a secure telecommunication problem can be split in two different groups, namely passive or active. The former, called eavesdroppers (or wiretappers), intercept and overhear the communication, while the later, called jammers, manipulate the message and/or transmission medium, with the objective of denying communication over a RF link. By emitting enough power, the jammer ensures the intended message receiver cannot understand requests, leaving it unable to operate properly. In this work, only jammers will be considered, with focus on barrage, tone, sweep, and reactive jammers, shown in figure 2.12.

Jamming approximately 30% or more of a voice communication results in a significant intelligibility degradation, ultimately leading to communication disruption [52]. In case of coded or uncoded digital communication, jamming substantially less than 30% of the signals delivers quite satisfactory results in terms of BER, and serves as a reasonable threshold.



(a) Slow FHSS **(b)** Fast FHSS

Figure 2.11: Channel structure of **(a)** slow, and **(b)** fast frequency hopping systems, where each bit lasts for a time T_b, and a hop occurs every T_h. Images from [51].

2.4.1 Barrage jamming

The principle of barrage jammers is to place noise energy across a given bandwidth of the frequency spectrum used by the targeted communication system, with a 100% duty cycle, as shown in figure 2.12a.

Barrage jamming was shown game and information-theoretically to deliver the best jamming performance in the absence of prior knowledge on the targeted signal (hence theoretically effective against all transmission means) [53], the downside being that non-targeted devices are also affected. Moreover, the method suffers from high energy requirement, and high detection probability (detrimental in most cases, as its detection could result in countermeasures such as communication adaptation, or even jammer integrity menacing manoeuvres). Spread spectrum techniques, discussed previously in section 2.3, were designed to increase jamming resistance, making barrage jamming inefficient against such information transmission means until jamming margin is overcome.

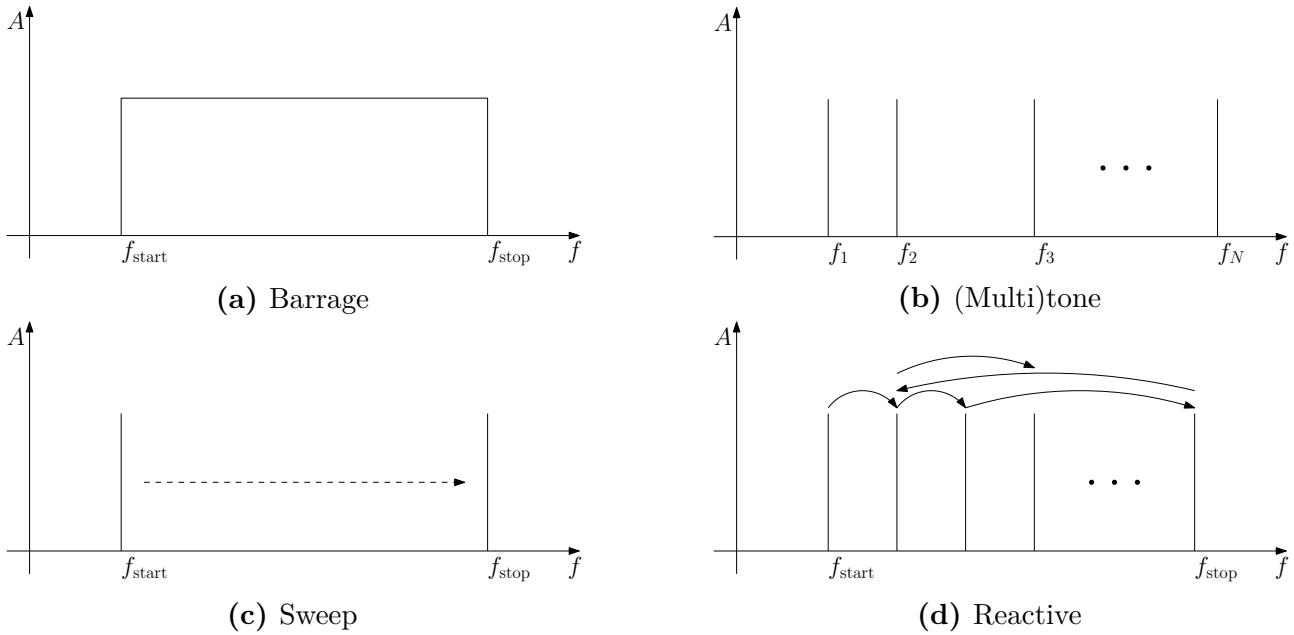
2.4.2 (Multi)tone jamming

A (multi)tone jammer uses one or more strategically placed tones, the number and placement of which affect jammer performances. A typical configuration of a N-tone jammer is shown in figure 2.12b, for which the tone signal takes the form [54]

$$J(t) = \sqrt{\frac{2P_J}{N}} \sum_{i=1}^{N} \cos\left(2\pi f_i t + \phi_i\right),$$

where P_J is the jammer power, f_i the frequency of the i-th jamming tone, and ϕ_i the phase difference between the i-th jamming tone and the carrier of the hopping frequency slot.

As shown in [51], monotone jamming is ineffective against FHSS systems, be it slow or fast. The case of multitone is more involved and depends on the number and placement of tones, as well as type of FHSS. In case of DSSS communication, (multi)tone jamming could be efficient, under the condition that the processing margin at the receiver (defined as the ratio between the modulated and original data signal bandwidths) is overcome, in combination with judicious choice of tone(s) placement.



(a) Barrage **(b)** (Multi)tone **(c)** Sweep **(d)** Reactive

Figure 2.12: Different jamming strategies, with **(a)** barrage, **(b)** (multi)tone, **(c)** sweep, and **(d)** reactive jammers.

2.4.3 Sweep jamming

Sweep jamming, schematically shown in figure 2.12c, consists in a combination of barrage and tone jamming, as a relatively narrowband signal is swept periodically across a targeted frequency band. At any time, the jammer is centred on a specific frequency, and only a narrow spectral region around that frequency is perturbed. The signal being swept, a broad range of frequencies can be covered in a short amount of time.

The net effect of the sweep is similar to that of a barrage jammer, except that the full jammer power can be concentrated in a narrowband channel. It is also possible to split the jamming strategy and avoid certain bands that might be used by other devices, but such an approach necessitate a certain level of intelligence on the receiver, as the timing should be tailored to ensure the right receiver's dwell time.

The jamming signal can be written under the form

$$J(t) = P_J \cos\left[2\pi f(t)t + \phi\right],$$

where the instantaneous frequency can be written under the form $f(t) = f_{\text{start}} + \frac{f_{\text{stop}} - f_{\text{start}}}{T_{\text{sweep}}}$, where T_{sweep} is the period of the sweep, and f_{start} and f_{stop} are the two extremal frequencies of the sweep set.

2.4.4 Reactive jamming

Reactive jamming, known under various other names such as protocol-aware jamming, follower jammer, or correlated jammer, is schematically shown in figure 2.12d. Multiple implementations exist, allowing to synchronise the jammer on the targeted signal, hence achieving efficient jamming, both in terms of achievable BER and power consumption.

Real-world realisations of protocol-aware jammers have been greatly facilitated by the evolution towards SDR systems (further discussed in section 3.1.1), driven by the demand for more flexible and reconfigurable radio systems, as well as the evolution of the enabling technologies, such as analogue-to-digital converters (ADCs), digital-to-analogue converters (DACs), and field programmable gate arrays (FPGAs) [55]. The flexibility and reconfiguration opportunities of SDRs allowed the development of cognitive radios, i.e. environment-aware systems able to adapt to their surroundings, in which spectrum sensing is crucial.

Despite its supposedly advantages on many aspects with respect to other types of jammers, some limitations still exist. Considering a FHSS signal to be jammed, physics limit the operating range of the jammer: the additional required time for the signal to reach the jammer, be processed and re-emitted, compared to the time needed for the signal to transit directly from transmitter to the intended receiver, imposes the the jammer to be inside an ellipse (with the Tx and Rx at its loci) to be effective [56].

3 Hardware and software platforms

The implementation of the jammers presented in section 2.4, together with the ability to configure an arbitrarily high number of times their parameters, requires both flexibility and robustness. Fortunately, SDR systems offers the perfect combination of both requirements with cost, making them ideal platforms to implement and test jammers in real-world applications. In the following, the enabling hardware and software platform allowing jammer realisation are presented.

3.1 Hardware platform

3.1.1 Software Defined Radio

Radios have considerably evolved over time, from the early designs consisting of a tuned antenna and a diode detector (used for Morse code transmission), to the most up-to-date configurations where most of the processing is done digitally through digital signal processing (DSP) techniques. The transition from analogue information treatment, through hardware, to mostly digital treatment, through software, allowed improvements regarding flexibility, cost effectiveness, hence powerfulness, of SDRs systems [57].

Basics of telecommunication were exposed in section 2.2, where the transmitter and receiver have to deal with well-known signals qua bandwidth, modulation, and carrier frequency. Removing those constraints would allow for universal adaptive platforms, in which a single transmitter would be able to deal with all type of signals, irrespective of their bandwidth, modulation and carrier frequency, without changing its hardware composition. This objective can be realised by moving the digitalization as close to the antenna as possible, as shown in figure 3.1 for a typical radio receiver (the transmitter being the exact dual).

Today, modern SDRs implement any necessary cryptography, forward error correction (FEC) coding, as well as source coding, along with various other DSP functionnalities. A more detailled block-diagram vue of a basic SDR hardware platfom than that presented in figure 3.1 is shown in figure 3.2, where all the necessary components to define carrier frequency, bandwidth, modulation, and possibly coding in software is displayed. The figure also highlights the point that a SDR consists of two main “blocks”, namely an analogue front end, dealing with all signal acquisition steps, and a digital back end, performing all signal processing steps.

Depending on its operating mode, the modem (modulation/demodulation) block in the device receives signals, synthesizes them, or do both for a full duplex radio. In receiver mode, the

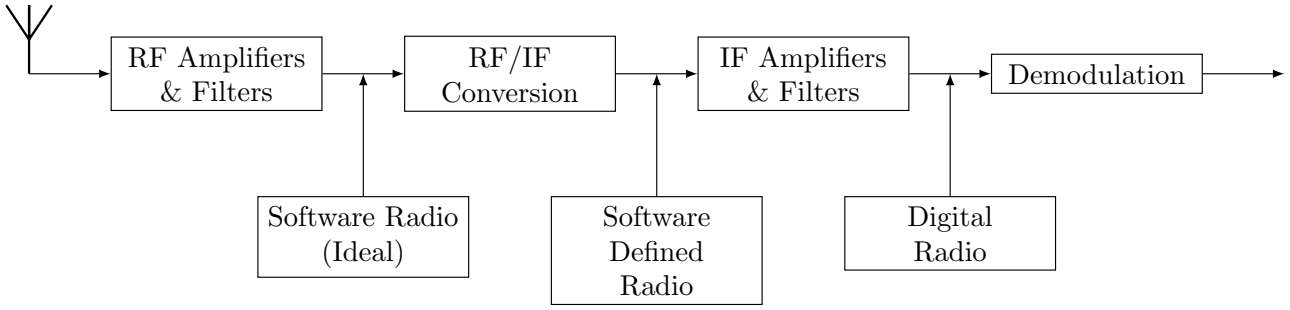


Figure 3.1: High-level block diagram representation of the possible places where digitalization can occur in a typical radio receiver. Image adapted from [58].

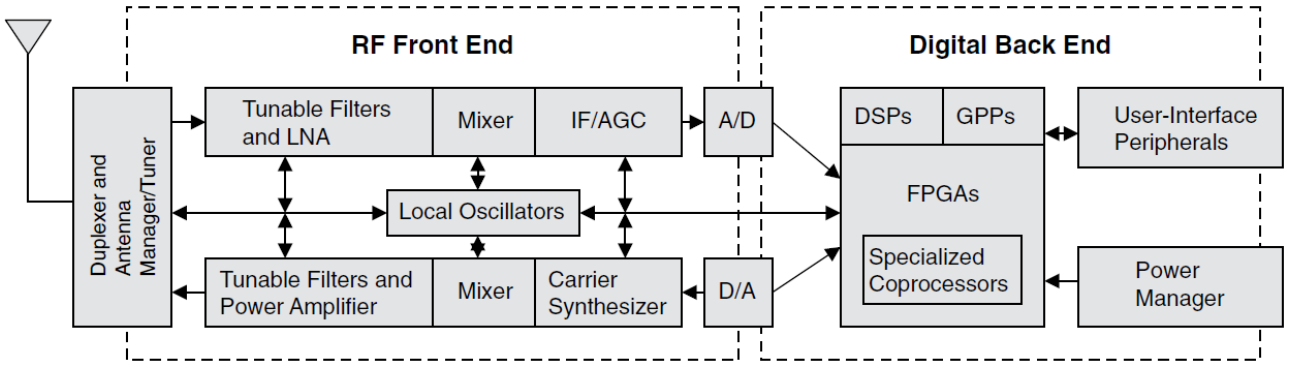


Figure 3.2: Basic SDR hardware platform, with enough components to define carrier frequency, bandwidth, modulation, and possible coding in software. Image from [59].

modem heterodynes the carrier frequency of the desired signal to a specific frequency, and filters it, allowing spurious signals removal. From there, the signal is (possibly) despread, refiltered so as to ensure commensuration with the information bandwidth, and time-aligned to the desired baud rate, ensuring feasible successfull demodulation. A generalized radio receiver designed for digital system is shown in figure 3.3, where the sampling process for DSP can be placed at several location, as shown previously in figure 3.1, without dramatic performance degradation.

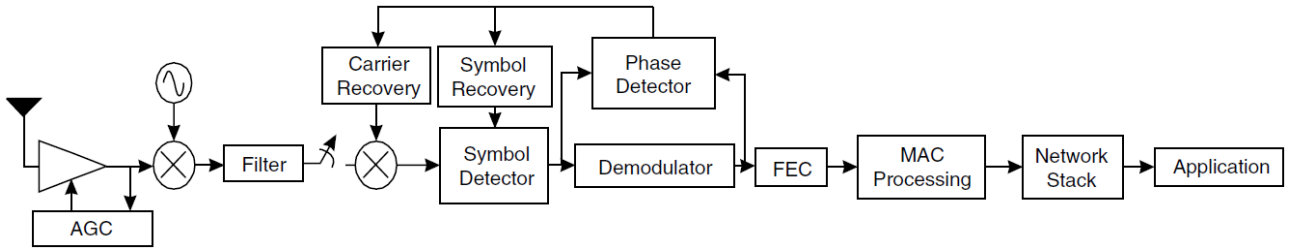


Figure 3.3: Bloc diagram representation of a generalized radio receiver designed for digital systems. Image from [59].

The transmitter mode is receiver's mode dual, and was illustrated in figure 2.3: information bitstreams are grouped into packets, to which redunduncy is often added (for error correction purposes), generates symbols, to which waveforms are associated and synthetized, filters it so as to fit the transmission channel, and possibly spreads it (typically through SS methods, as exposed in sections 2.3.1 and 2.3.2).

3.1.2 LimeSDR

In this work, the LimeSDR, a low-cost and open-source SDR platform, is used as target architecture. Developed by Lime Microsystems, it features a `LMS7002SM` MIMO RF transceiver chip, an Altera Cyclone IV `EP4CE40F23` FPGA, a Cypress USB 3.0 `CYUSB3014-BZXC` controller, 10 U.FL connectors, an a lot more, as shown in figure 3.4. The continuous coverage of the 100

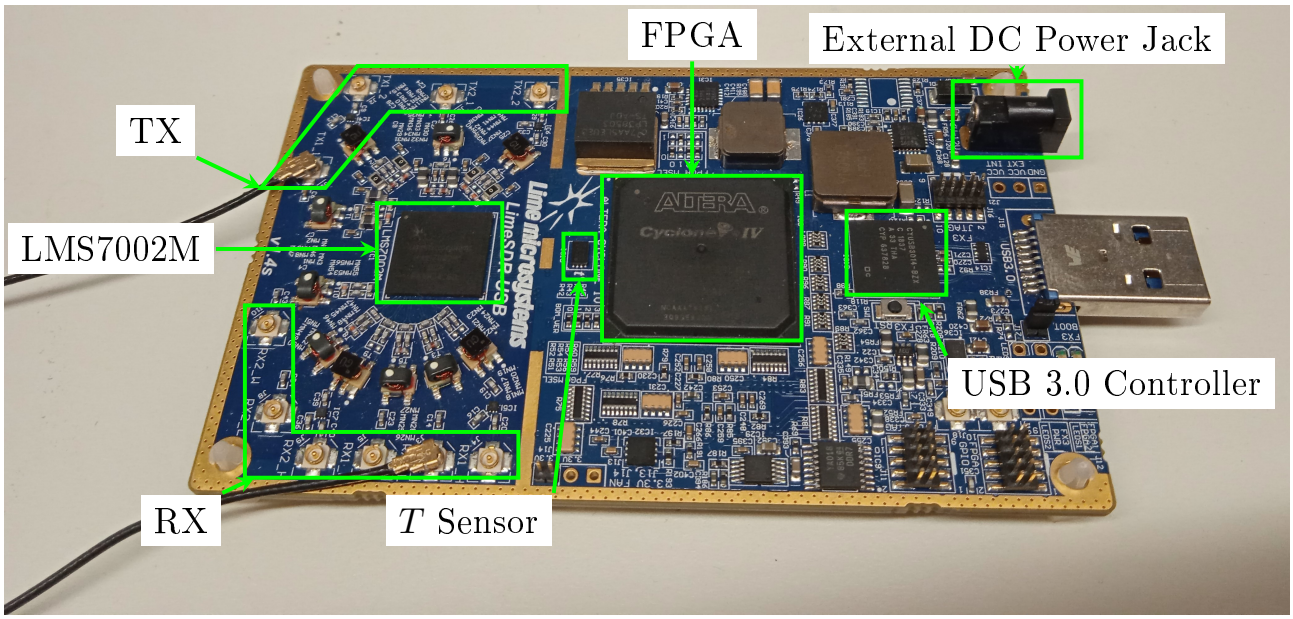


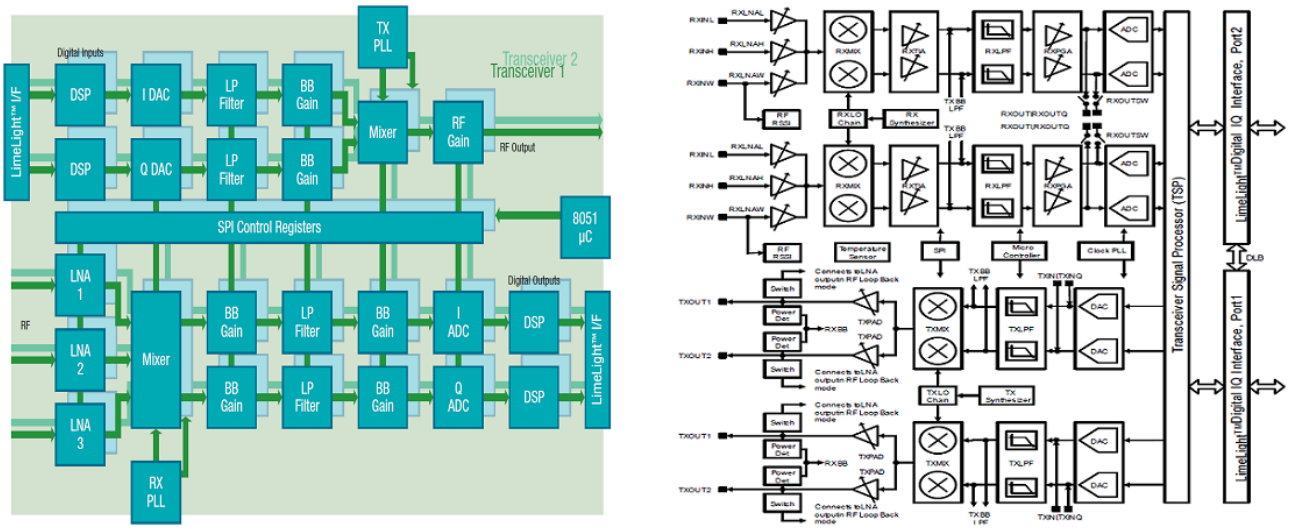
Figure 3.4: The LimeSDR platform, with some of its components highlighted.

kHz - 3.8 GHz RF frequency range, combined with its 61.44 MHz bandwidth, makes it a good candidate for 2.4 GHz ISM band jamming, even though a full 83.5 MHz bandwidth coverage would have been mandatory to ensure full band coverage.

The internal structure of the FPRF `LMS7002SM` multiple input multiple output (MIMO) transceiver integrated circuit (IC) is shown in figure 3.5a, where its dual topology is highlighted, together with the transmission and reception parts, on top and bottom half of the figure, respectively, and serial peripheral interface (SPI) data exchange between the microcontroller and various peripherals. The transmission chain first gets samples from the FPGA, processes them, converts them to the analogue domain, before filtering, amplifying, and mixing them with a carrier frequency. The reception chain mainly performs the same operations in reverse order, with the notable exception that the input signal undergoes a preselection, based on its frequency span, with three possible outcomes: depending whether the bandwidth is low, high, or wideband, the analogue paths are different.

A more formal description of the different transmit/receive stages can be described based on figure 3.5b. In transmission, IQ DAC data samples are passed from the baseband processor to the transceiver, via the `LimeLight`™ digital IQ interface. Samples are then preprocessed in the digital transceiver signal processor (TSP) to reduce distorsion, and further applied to the on-chip transmit DACs, generating analog IQ signals, which are then filtered by transmit low-pass filters and mixed with phase-locked loops (PLLs) outputs, yielding modulated RF signals, which are then amplified, and finally sent into the communication channel.

In reception, three possible inputs, each provided with their own low-noise amplifiers (LNAs), optimised for narrow or wideband operation, are heterodyned to baseband thanks to PLLs. From there, signals are possible re-amplified and low-pass filtered to remove possible aliases. IQ



(a) High-level (from [60])

(b) Lower-level (from [61])

Figure 3.5: Block diagram representation of the FPRF `LMS7002SM` MIMO transceiver, highlighting its dual topology.

input samples are further passed through another amplifying stage, and DC-filtered to avoid saturation and preserve receiver ADCs dynamic range. The analog signals are then passed on to on-chip ADCs, and further transferred to the TSP„ from which the resulting signals are passed to the baseband processor via the `LimeLight`™ interface. Zoomed-in views of the TSP internal functionning for both receive and transmit operating modes are shown in figure 3.6, where the upper rectangle corresponds to a reception (`RXTSP`) and the lower to a reception (`TXTSP`) mode, and which shows that both modes are similar.

From figure 3.6, it appears that the Rx and Tx parts of the transceiver feature a decimation and interpolation block, respectively. Those rate-modifying blocks are crucial parts of SDRs, as they allow for multiple signals with arbitrary bandwidths and center frequencies to be correctly processed inside the radio device [58]. In addition to decimation and interpolation, some coefficient-programmable general purpose finite impulse response filters are present in the Rx and Tx parts, serving various purposes: for transmission, one filter could be used as a phase equalizer, one to flatten the amplitude response of the low-pass filter, and the last one to further enhance channel filtering[1]. Possible applications of reception filters are similar to transmission ones.

3.2 Software platform

Based on the general concepts introduced in section 3.1.1, as well as the acronym “SDR” meaning, the behaviour of a SDR can be software-parametrized. Different software radio development kit exist, such as (i) LabView, a licensed program developed by National Instrument, widely used with USRPs, (ii) Matlab and Simulink, for which some free packages can be downloaded, and used in combination with (paying) other packages, (iii) GNU Radio, a free and open-source software development toolkit that can be used both with or without external hardware, and (iv) many others. In addition to those toolkits, some SDR manufacturers propose their own packages, as is the case for Lime Microsystems: with the free and open-source Lime Suite, users have access to a collection of software supporting several hardware platforms, including

[1] If phase equalization is not required, only one filter could be used, reducing delays introduced by the filters.

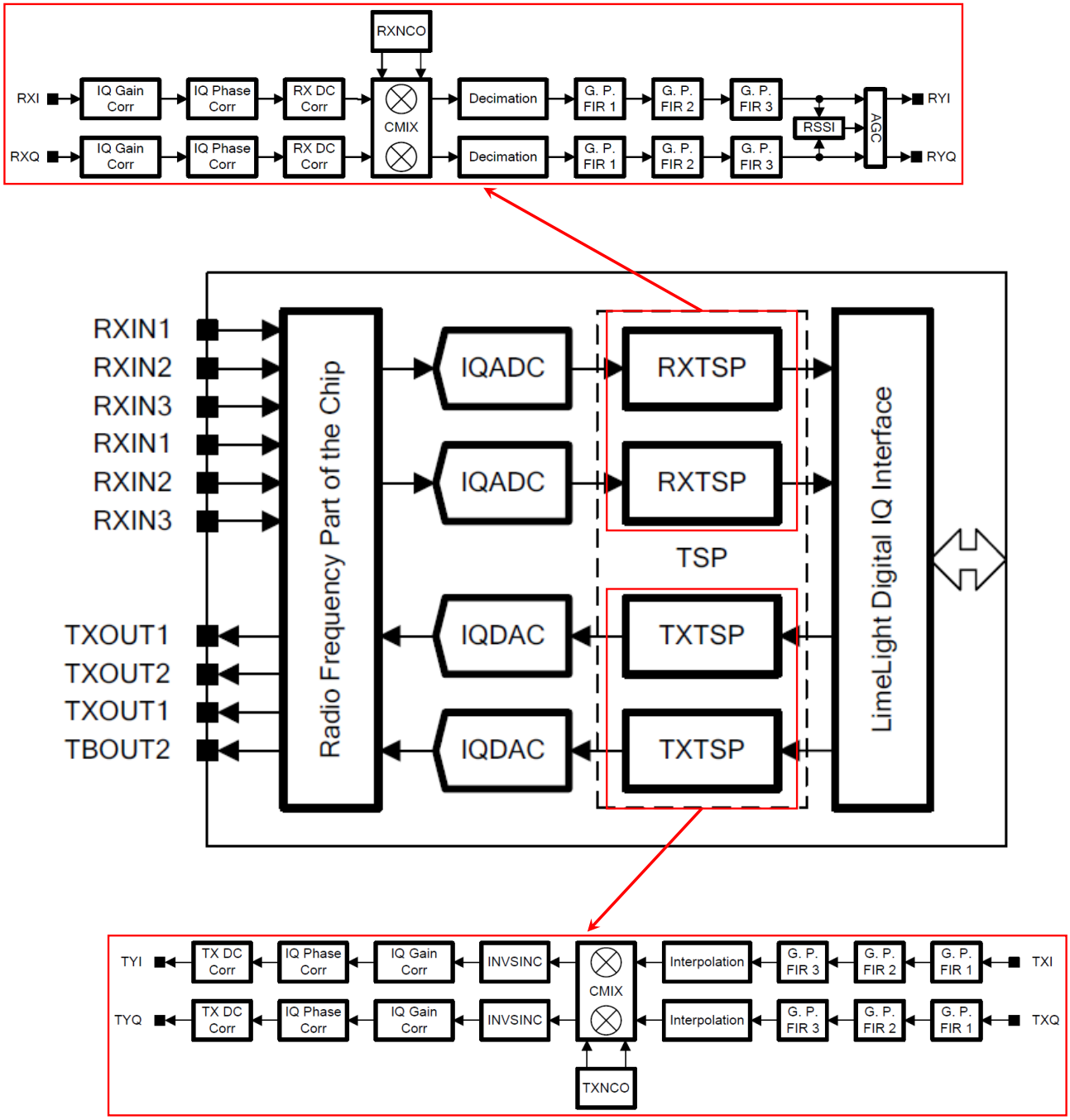


Figure 3.6: Zoomed-in view of the `LMS7002M` transceiver signal processor, for both receive and transmit modes. Image adapted from [61].

the LimeSDR, drivers for the `LMS7002M` RF MIMO transceiver IC, as well as other tools for developing with `LMS7`-based harware. In the following, only the GNU Radio software development toolkit will be considered.

3.2.1 Introduction to GNU Radio

GNU Radio is an open-source software toolkit founded in 1998 by Eric Blossom. The combination of signal processing blocks with external RF hardware allows for the complete development of SDR applications ,explaining its popularity amongst researchers, industry, hobbyists, etc. Per its documentation, last accessed on 11th May 2022, GNU Radio is cross-platform, but running it on a Linux distribution is advised.

GNU Radio consists of two principal entities, namely blocks and flowgraphs, the latter being the result of the former interconnection. Blocks are structured to have a certain number of input, output, and possible message ports, and perform signal processing functions. They can be categorised as either source, sink, or filter, depending on their behaviour: sources do not have input ports, sinks do not have output ports, and filters are all the possible in-between components.

Some existing blocks, such as modulation/demodulation techniques, filters, signal sources, etc. are integrated within GNU Radio, but the user is free to implement and add new components inside its application.

To maximise code modularity, flowgraphs are created either as hierarchical or top blocks: hierarchical blocks contain a certain number of input/output ports, can take parameters, and their behaviour is forwarded to their parent class through an *init()* method. Top blocks, on the other hand, are top-level graphs containing all the other flowgraphs, and have no input/output ports. Based on that terminology, all signal processing blocks are connected within hierarchical blocks, themselves embedded in a top block.

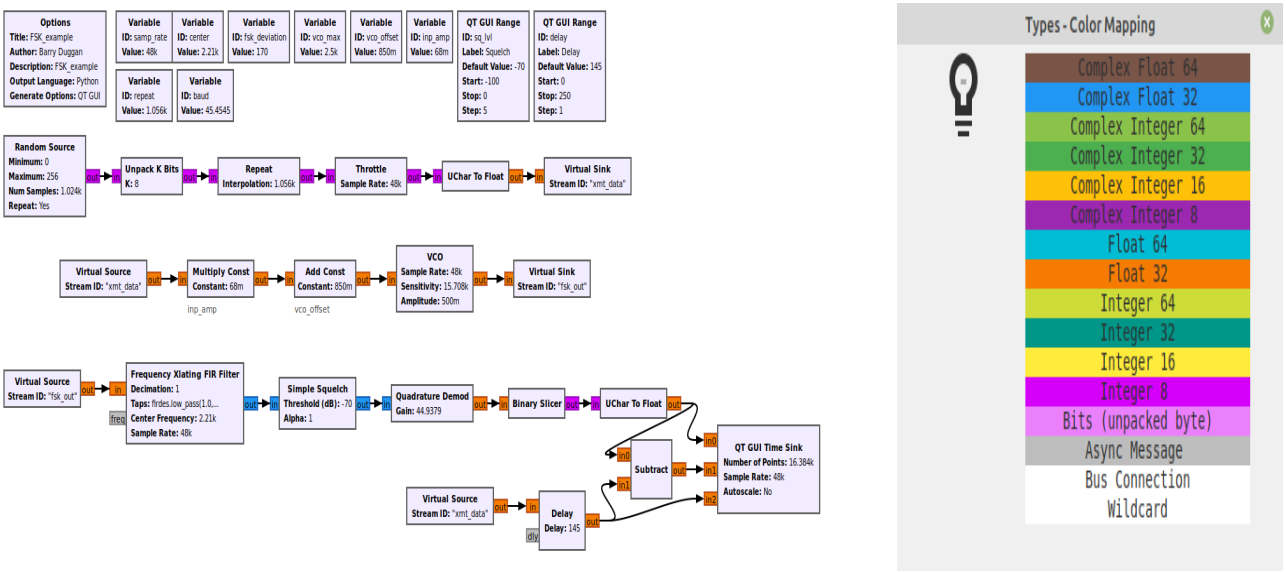
Blocks communicate with each other by exchanging data streams, where each stream having its own type. To ensure block compatibility, the data types for the output of one block connected to the input of an other one must match, and be either of type (i) bits, (ii) integer, (iii) float, or (iv) complex.

3.2.2 Introduction to GNU Radio Companion

In order to avoid to have to dive constantly in potentially long code, GNU Radio comes with a graphical user interface known as GNU Radio Companion (GRC). At flowgraph creation, the *Options* window and *samp_rate* variable are automatically added. The variable *samp_rate* is initialised at 32000, and the *Options* windows features various fields, such as *Title*, *Output Language*, *Generate Options*, etc. Once the flowgraph is run inside GRC, a file with the extension corresponding to the selected *Output Language* is created, the name of which is given by the *Id* field inside the *Options* window.

A typical flowgraph created inside GRC is shown in figure 3.7a, where a FSK emitter and receiver are illustrated. As can be seen, interconnected blocks have matching colours regarding inputs and outputs, in good agreement with the explanation provided in section 3.2.1. Fortunately, the matching is eased in GRC through the use of a colour code, illustrated in figure 3.7b.

From figure 3.7a, it appears a typical flowgraph can implement different functionalities in the same file, one bloc output can be connected to several blocks input, and *Async Message* ports can be left empty without compilation error. It should however be noted that a given input port cannot accept several connections.



(a) FSK emitter and receiver **(b)** GRC coulour code

Figure 3.7: GNU Radio Companion flowgraph example with matching colour code.

4 Results

This section is concerned with practical jammers implementation on the hardware platform presented in section 3.1.2, through the use of GNU Radio, presented in section 3.2.2. First, experimental setup and system characterization are presented in section 4.1, on the basis of which a discussion on jammers implementation is given in section 4.2. In that part, a brute force barrage jammers is first considered, with some theoretical considerations regarding the required power to reach effective jamming. The discussion is then extended to a sweep jammer, and a reactive jammer, for which the various constituting building blocks are presented and briefly described.

4.1 Experimental conditions

The experimental conditions in which the various jammers were tested in shown in figure 4.1, from which it appears that the Tx is a Taranis X9D Plus 2019, the Rx is a FrSky X8R telemetry

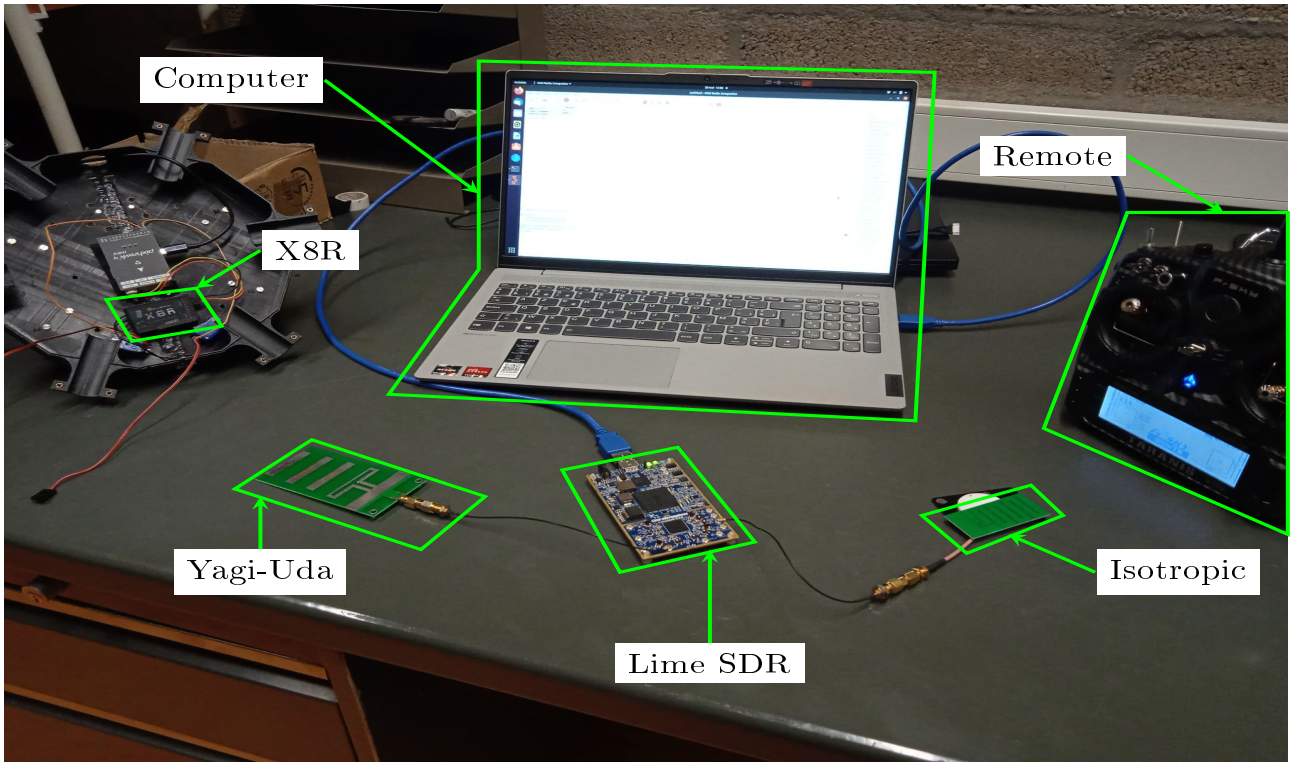


Figure 4.1: Experimental setup, showing the computer, the Lime SDR, and the antennas configuration to test various jammers.

receiver, and that two different antennas are used: one isotropic for signal reception, and one directional, directed towards the receiver. A preliminary spectrum analysis shown in figure 4.2 performed thanks to a ZNL3 vector network analyzer (VNA) from Rohde & Schwarz, allows

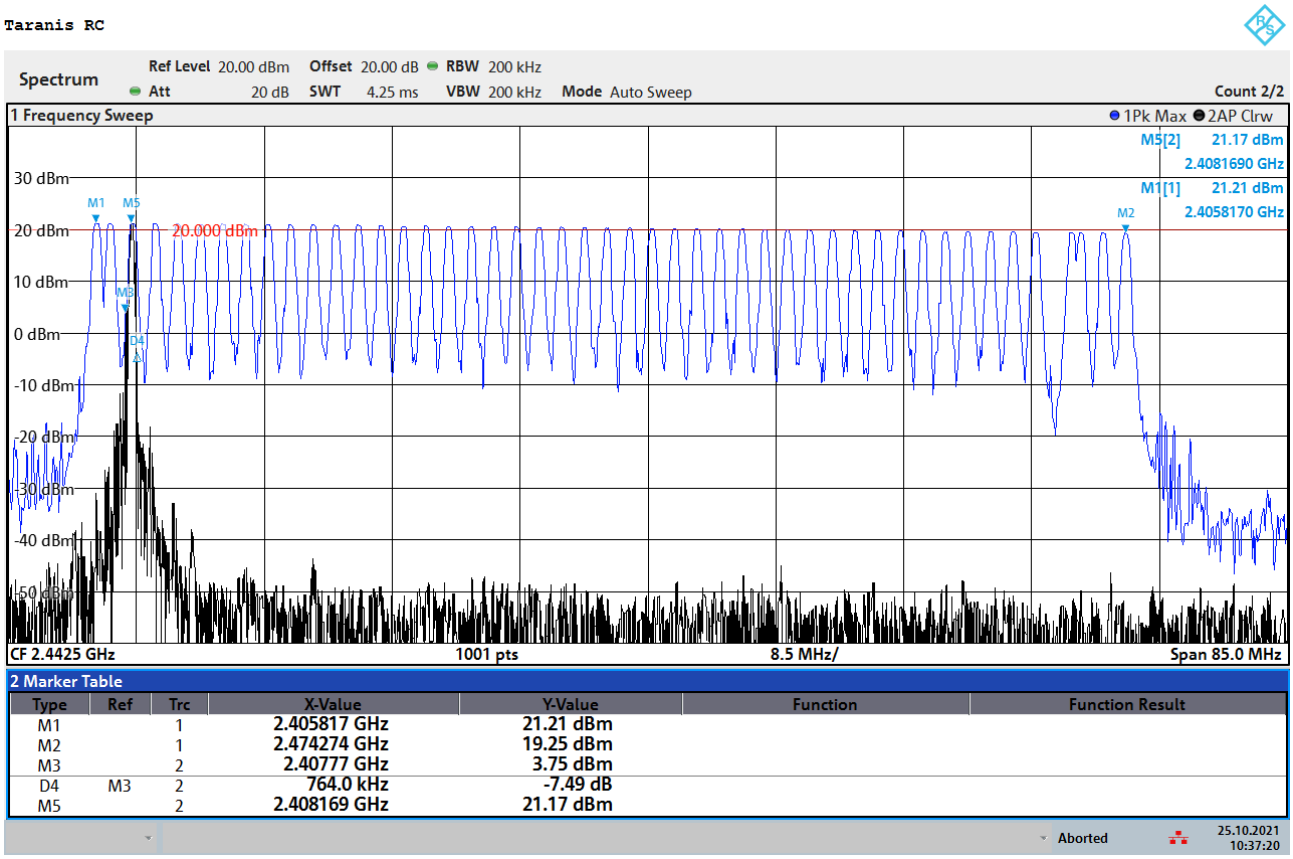
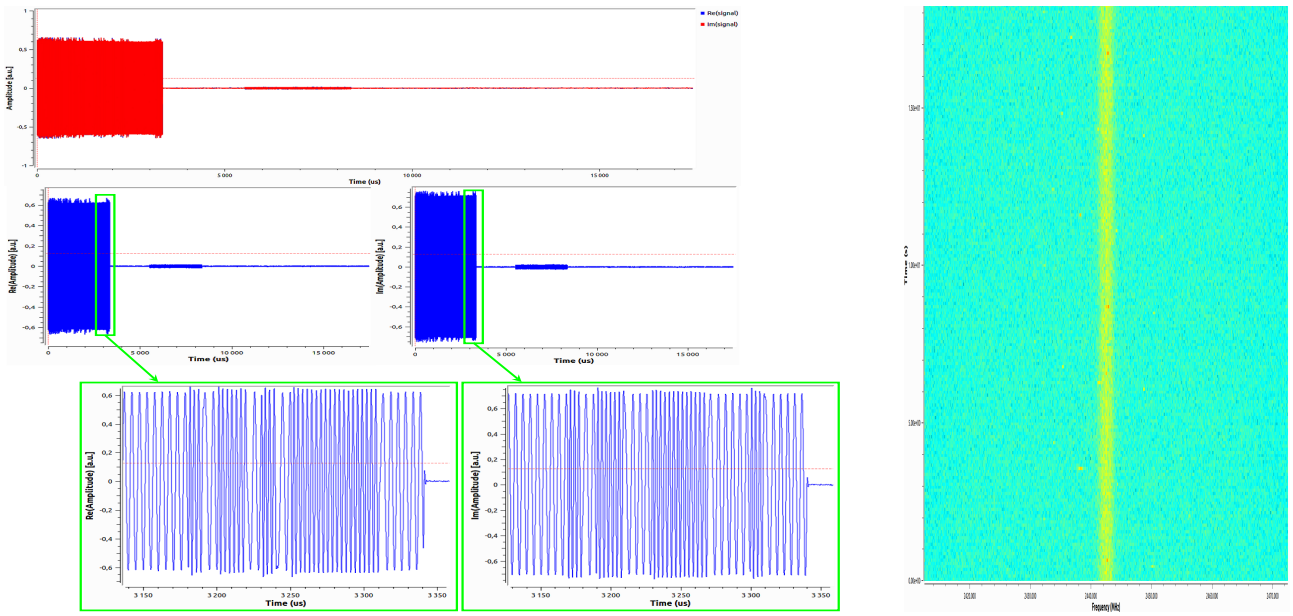


Figure 4.2: Frequency representation of the communication between the Taranis X9D Plus 2019 remote controller and the FrSky X8R receiver, highlighting a FHSS-like information transmission.

to see that the communication between the remote controller and the receiver lies in the 2.4 GHz ISM band, with a FHSS transmission for which the hopset consists of approximately 50 channels, some of which not used (probably reserved for various purposes, such as firmware updates and return signal strength information (RSSI)-sending operations). To further get information on the signal's modulation, the Lime SDR presented in section 3.1.2 can be used. Fixing its sample sample rate to 60 Msample s^{-1}, time and frequency representations of the signals are shown in figures 4.3a and 4.3b, respectively. From figure 4.3a, it appears that the signals follow an IQ 2-FSK modulation. The spectrogram shown in figure 4.3b further confirms the use of FHSS to transmit the modulated signals. The maximum bandwidth of the Lime SDR being 61.44 MHz, the full 83.5 MHz-wide band of interest could not be covered in its entirety, hence the hopping time could not be determined. Moreover, to discriminate between slow and fast frequency hopping, a packet analyser should have been used.

4.2 Jammers implementation

The results obtained by a GNU Radio implementation of the techniques exposed in sections 2.4.1, 2.4.3 and 2.4.4 are now presented. For the barrage jammer, a feasibility analysis, based on simple arguments, is performed prior to software implementation. Regarding the sweep jammer, only a brief discussion is made, given its ineffectiveness against FHSS systems. For the reactive



(a) time representation **(b)** spectrogram

Figure 4.3: Time and frequency representations of the signals send from the remote controller to the drone receiver.

jammer, the various blocks are presented, with a discussion of the implementation and results of the various blocks taken independently from one another, when appropriated.

4.2.1 Barrage jammer

The power factor being critical for a jammer implementation (a forciori for a drone-mounted one) points towards the realisation of a feasibility analysis study prior to any practical elaboration. Such a study can be made through the Friis equation, relating received power to other quantities. More precisely, the power received at Rx, denoted $\mathcal{P}_{\mathrm{RX}}$, as a function of its antenna gain G_{RX}, its distance to a Tx, denoted $r_{\mathrm{TX,RX}}$, emitting a power $\mathcal{P}_{\mathrm{TX}}$, thanks to an antenna presenting a gain G_{TX}, is given by [62]

$$\mathcal{P}_{\mathrm{RX}} = \mathrm{G}_{\mathrm{RX}}\mathrm{G}_{\mathrm{TX}}\mathcal{P}_{\mathrm{TX}}\frac{1}{\mathcal{L}_{\mathrm{FS}}^{(\mathrm{TX,RX})}\mathcal{L}_{\mathrm{M}}^{(\mathrm{TX,RX})}}\left(\frac{\lambda}{4\pi r_{\mathrm{TX,RX}}}\right)^2, \tag{4.1}$$

where λ represents the wavelength of the emitted signal, and where $\mathcal{L}_{\mathrm{FS}}^{(\mathrm{TX,RX})}$ and $\mathcal{L}_{\mathrm{M}}^{(\mathrm{TX,RX})}$ are path and other miscellaneous losses (including fading, polarisation mismatch, body losses, etc.) between Rx and Tx. Focusing on the real power a system must emit to reach a radiated power $\mathcal{P}_{\mathrm{TX}}$, denoted $\mathcal{W}_{\mathrm{TX}}$, the budget link takes the form

$$\eta_{\mathrm{RX}}\mathcal{W}_{\mathrm{RX}} = \mathrm{G}_{\mathrm{RX}}\mathrm{G}_{\mathrm{TX}}\eta_{\mathrm{TX}}\mathcal{W}_{\mathrm{TX}}\frac{1}{\mathcal{L}_{\mathrm{FS}}^{(\mathrm{TX,RX})}\mathcal{L}_{\mathrm{M}}^{(\mathrm{TX,RX})}}\left(\frac{\lambda}{4\pi r_{\mathrm{TX,RX}}}\right)^2,$$

where emission and reception circuit efficiencies are represented by η_{TX} and η_{RX}, respectively.

The studied configuration is schematically shown in figure 4.4, where the receiver is the drone, and the two transmitters TX_1 and TX_2 are the drone's controller and the jammer, respectively. Knowing that TX_1 emits in the 2.4 GHz ISM band, the Belgian institute for postal services and telecommunications (BIPT), i.e. the regulating body in Belgium for matters linked to

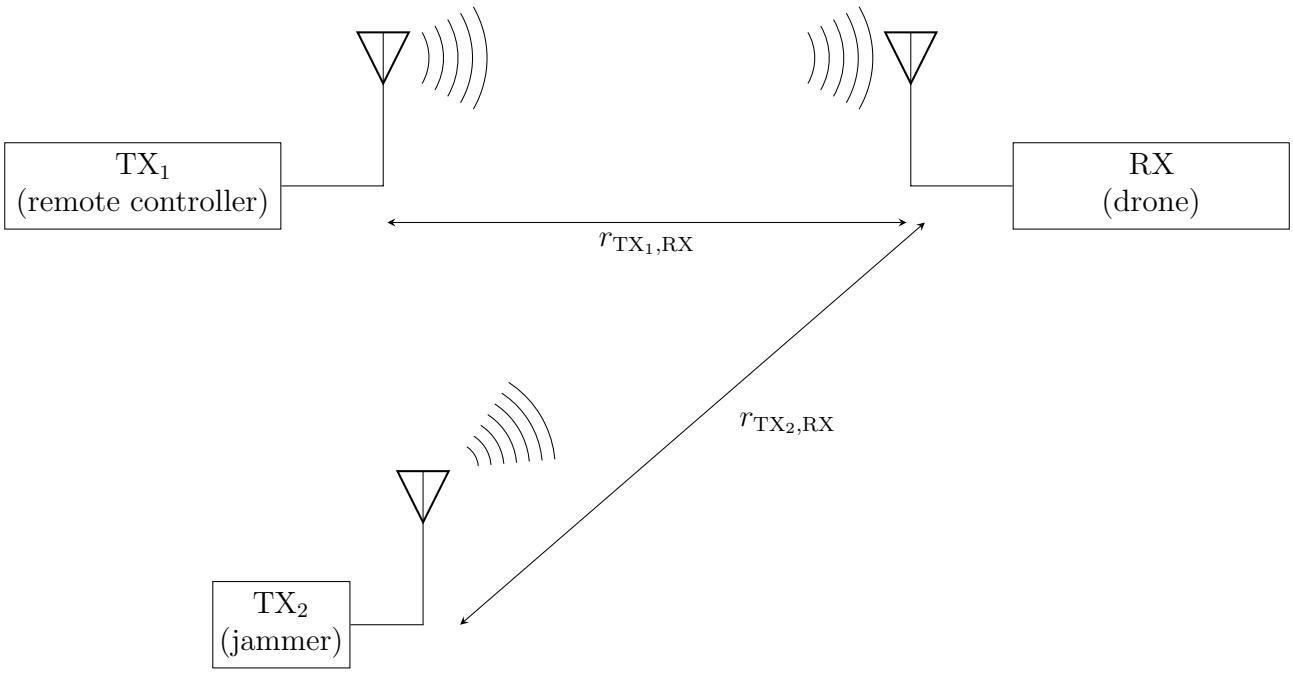


Figure 4.4: Schematic representation of the studied configuration, in which a jammer TX_2 has to perturb the communication link between a remote controller TX_1 and a drone RX. The distance between objects a and b is denoted by $r_{a,b}$.

telecommunications, imposes a maximum mean effective isotropic radiated power (EIRP) of 20 dBm, meaning that $\mathcal{P}_{\mathrm{TX}_1} = 20\,\mathrm{dBm}$ is considered in the following. Reexpressing the received power in dBm yields

$$\begin{aligned}\mathcal{P}_{\mathrm{RX}}\,[\mathrm{dBm}] &= \mathrm{G}_{\mathrm{RX}}\,[\mathrm{dBi}] + \mathrm{G}_{\mathrm{TX}_1}\,[\mathrm{dBi}] + \mathcal{P}_{\mathrm{TX}_1}\,[\mathrm{dBm}] - \mathcal{L}_{\mathrm{FS}}^{(\mathrm{TX}_1,\mathrm{RX})}\,[\mathrm{dB}] - \mathcal{L}_{\mathrm{M}}^{(\mathrm{TX}_1,\mathrm{RX})}\,[\mathrm{dB}] \\ &\qquad + 20\log_{10}\left(\frac{\lambda}{4\pi r_{\mathrm{TX}_1,\mathrm{RX}}}\right), \\ &= \mathrm{G}_{\mathrm{RX}}\,[\mathrm{dBi}] + \mathrm{G}_{\mathrm{TX}_1}\,[\mathrm{dBi}] + 20\,[\mathrm{dBm}] - \mathcal{L}_{\mathrm{FS}}^{(\mathrm{TX}_1,\mathrm{RX})}\,[\mathrm{dB}] - \mathcal{L}_{\mathrm{M}}^{(\mathrm{TX}_1,\mathrm{RX})}\,[\mathrm{dB}] \\ &\qquad + 20\log_{10}\left(\frac{\lambda}{4\pi r_{\mathrm{TX}_1,\mathrm{RX}}}\right).\end{aligned} \tag{4.2}$$

To reach the same (or greater) amount of power, considering that the communication between the remote and the drone is effective under a SNR of $\mathrm{SNR}\,[\mathrm{dB}]$, the jammer TX_2 will have to radiate a power $\mathcal{P}_{\mathrm{TX}_2}\,[\mathrm{dBm}] \geq \mathcal{P}_{\mathrm{RX}}\,[\mathrm{dBm}] - \mathrm{SNR}\,[\mathrm{dB}]$. Combining that constraint with (4.2) yields

$$\begin{aligned}\mathcal{P}_{\mathrm{TX}_2}\,[\mathrm{dBm}] \geq \mathrm{G}_{\mathrm{RX}}\,[\mathrm{dBi}] + \mathrm{G}_{\mathrm{TX}_1}\,[\mathrm{dBi}] + 20\,[\mathrm{dBm}] - \mathcal{L}_{\mathrm{FS}}^{(\mathrm{TX}_1,\mathrm{RX})}\,[\mathrm{dB}] - \mathcal{L}_{\mathrm{M}}^{(\mathrm{TX}_1,\mathrm{RX})}\,[\mathrm{dB}] \\ + 20\log_{10}\left(\frac{\lambda}{4\pi r_{\mathrm{TX}_1,\mathrm{RX}}}\right) - \mathrm{SNR}\,[\mathrm{dB}].\end{aligned} \tag{4.3}$$

Since the losses $\mathcal{L}_{\mathrm{FS}}^{(\mathrm{TX}_2,\mathrm{RX})}$ and $\mathcal{L}_{\mathrm{M}}^{(\mathrm{TX}_2,\mathrm{RX})}$ can be different from those between TX_1 and RX, the combination of (4.3) with (4.1) allows for the determination of a proportional distance relation reading

$$\left(\frac{r_{\mathrm{TX}_1,\mathrm{RX}}}{r_{\mathrm{TX}_2,\mathrm{RX}}}\right)^2 \geq \frac{\mathrm{G}_{\mathrm{TX}_1}}{\mathrm{G}_{\mathrm{TX}_2}}\frac{100\mathcal{L}_{\mathrm{FS}}^{(\mathrm{TX}_2,\mathrm{RX})}\mathcal{L}_{\mathrm{M}}^{(\mathrm{TX}_2,\mathrm{RX})}}{\mathrm{SNR}\mathcal{L}_{\mathrm{FS}}^{(\mathrm{TX}_1,\mathrm{RX})}\mathcal{L}_{\mathrm{M}}^{(\mathrm{TX}_1,\mathrm{RX})}}.$$

For a system in which losses can reasonably be considered equal, i.e. $\mathcal{L}_{\mathrm{FS}}^{(\mathrm{TX}_1,\mathrm{RX})} \approx \mathcal{L}_{\mathrm{FS}}^{(\mathrm{TX}_2,\mathrm{RX})}$ and $\mathcal{L}_{\mathrm{M}}^{(\mathrm{TX}_1,\mathrm{RX})} \approx \mathcal{L}_{\mathrm{M}}^{(\mathrm{TX}_2,\mathrm{RX})}$, where $\mathrm{G}_{\mathrm{TX}_1} = 1\,[\mathrm{dBi}]$ and $\mathrm{G}_{\mathrm{TX}_2} = 3\,[\mathrm{dBi}]$, and where the SNR is

SNR $= -6\,[\text{dB}] \approx 0.25$, the relative distance between the jammer to the drone, compared to that between the drone and its remote controller, should approximately be $\frac{r_{\text{TX}_2,\text{RX}}}{r_{\text{TX}_1,\text{RX}}} \lesssim 0.06$, highlighting the impracticalness of using a (drone-mounted) barrage jammer to disrupt the communication between a drone and its controller.

The ineffectiveness of the method was experimentally verified through a GNU Radio implementation, in which a AWGN was emitted over the full Lime SDR bandwidth, as shown in figure 4.5. It was experimentally determined that the jammer had to be approximately one hun-

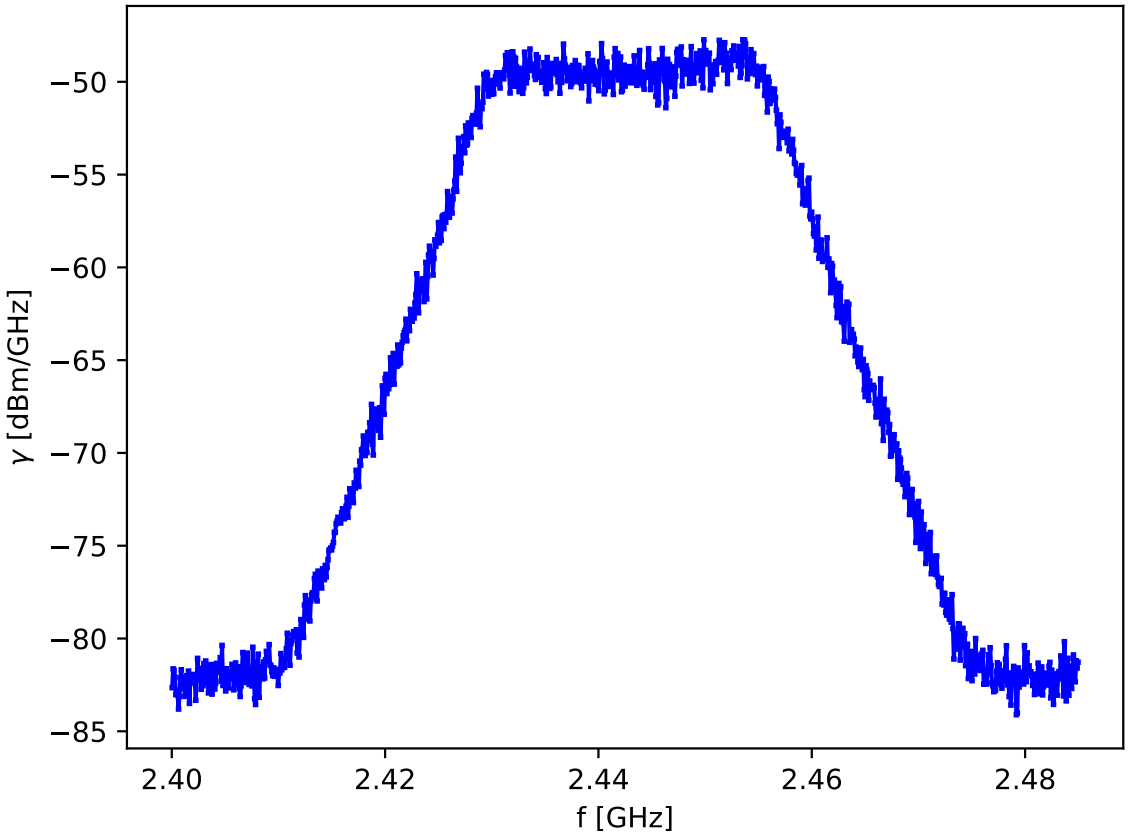


Figure 4.5: Power spectral density of the noise emitted by the barrage jammer.

dred times closer to the receiver than the remote, i.e. $r_{\text{TX}_2,\text{RX}} \approx 0.1\,[\text{m}]$ while $r_{\text{TX}_1,\text{RX}} \approx 10\,[\text{m}]$. This discrepancy between the predicted and measured values could be explained by several factors, such as the violation of the same-loss hypothesis, "inefficient" electrical circuits, or the fact that $\mathcal{P}_{\text{TX}_1}$ is less than the expected 20 dBm, due to its unknown antenna gain.

4.2.2 Sweep jammer

The ineffectiveness of the barrage jammer, demonstrated both analytically and experimentally in section 4.2.1, leads to the conclusion that a more involved configuration is required. A direct improvement of the barrage jammer could consists in sweeping periodically a signal across a given bandwidth, known as a sweep jammer, in agreement with the preliminary discussion given in section 2.4.3. As for the barrage jammer, the results of a GNU Radio implementation are

given in figure 4.6, in which a sine is swept across a 16 kHz-wide[1] bandwidth, for illustrative purposes, with a real-time configurable sweep rate. The ineffectiveness of the method suggests a

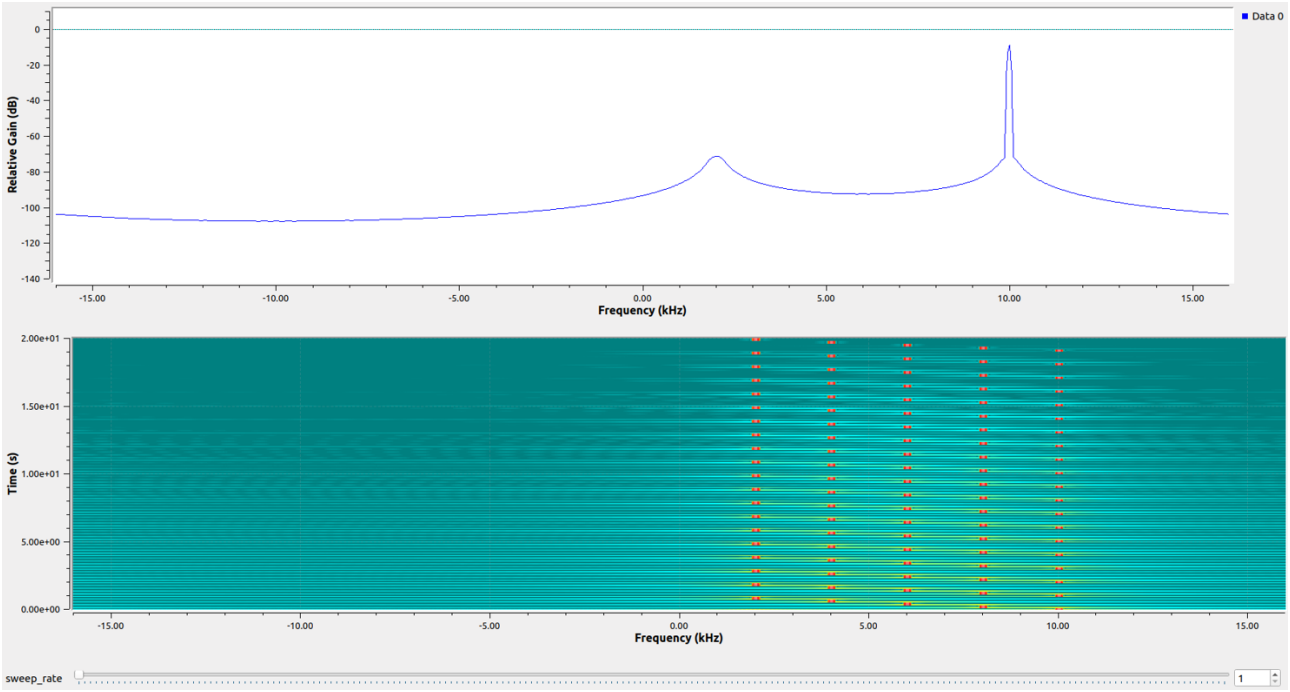


Figure 4.6: Frequency representation and spectrogram of the implemented sweep jammer.

yet more complex jamming strategy is required, which is discussed next.

4.2.3 Reactive jammer

The jammer implementations of sections 4.2.1 and 4.2.2 not delivering satisfactory results, a more involved method is required, which idea is schematically shown in figure 4.7. The signals

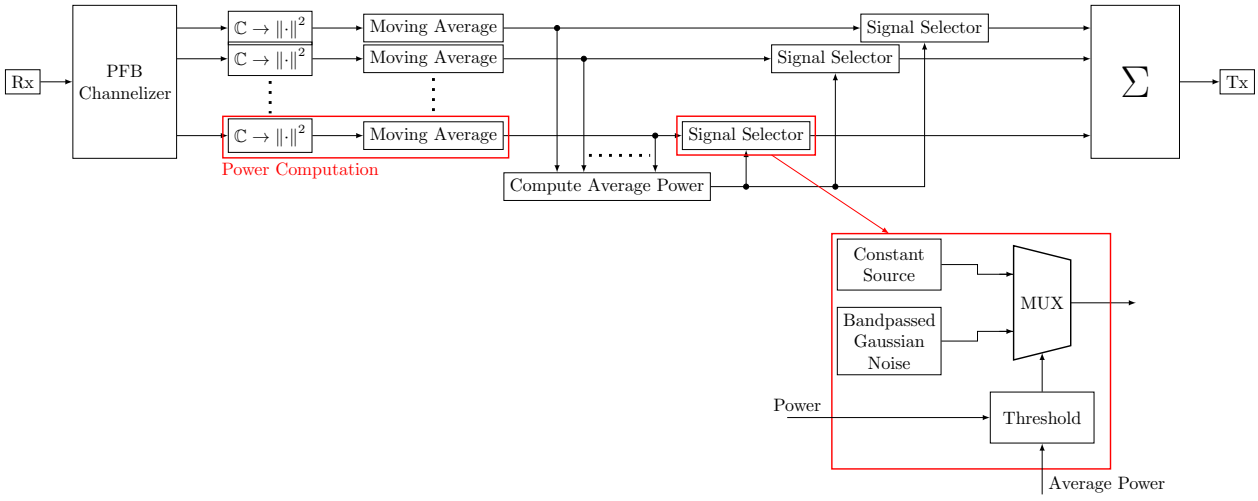


Figure 4.7: Graphical representation of a reactive jammer, highlighting its spectral occupancy analysis triggering (or not) the emission of a jamming signal.

present in the band of interest are first acquired through a Rx block, and are then separated into

[1]Sweeping across the band of interest, 83.5 MHz wide, would require too much computations for a classical computer CPU.

subbands through a polyphase filter bank channelizer. The energy contained in each subband is computed by averaging of the samples modulus, in agreement with Parseval's identity, which is then forwarded to a dynamic threshold-computing block in parallel to signal-selecting blocks where, depending on the input relative to the fed threshold, emits either a constant (null) signal or a jamming signal. The results for each individual subband are then summed, the result of which is then emitted through a Tx block. In the following, the various blocks are presented and discussed.

Polyphase channelizer

As stated in section 3.1.1, one the biggest advantages of SDRs is their ability to deal with varying signal parameters. In practice, the variation of, say, signal bandwidth, can be realised through the use of a polyphase channelizer, for which two operating modes exist: in analysis mode, a wideband input signal is decomposed into a subset of smaller bandwidth signals, easier to analyse. Such a segmentation is realised by implementing a prototype filter, which is then split among M channels. In synthesis mode, several narrowband signals are assembled together, yielding a wideband signal. Only the analysis mode is considered here, with a subsequent synthesis serving as filter parameters confirmation. The reader interested in the working principles behind channelisation are redirected to dedicated literature, such as [63]–[68].

In the case of interest here, considering the maximum 60 MHz bandwidth of the Lime SDR, together with the 50-channel hopset, the number of channels in the channelizer is put to $M = 50$. The chosen filter is lowpass, designed at the maximum sample rate, with a cutoff frequency $f_{\text{cutoff}} = \frac{60\,\text{MHz}}{50} = 1.2\,\text{MHz}$, a transition bandwidth $W_{\text{trans}} = 0.01 f_{\text{cutoff}}$, and an attenuation of 80 dB, split amongst the 50 channels, and is shown in figure 4.8. The signals resulting from such

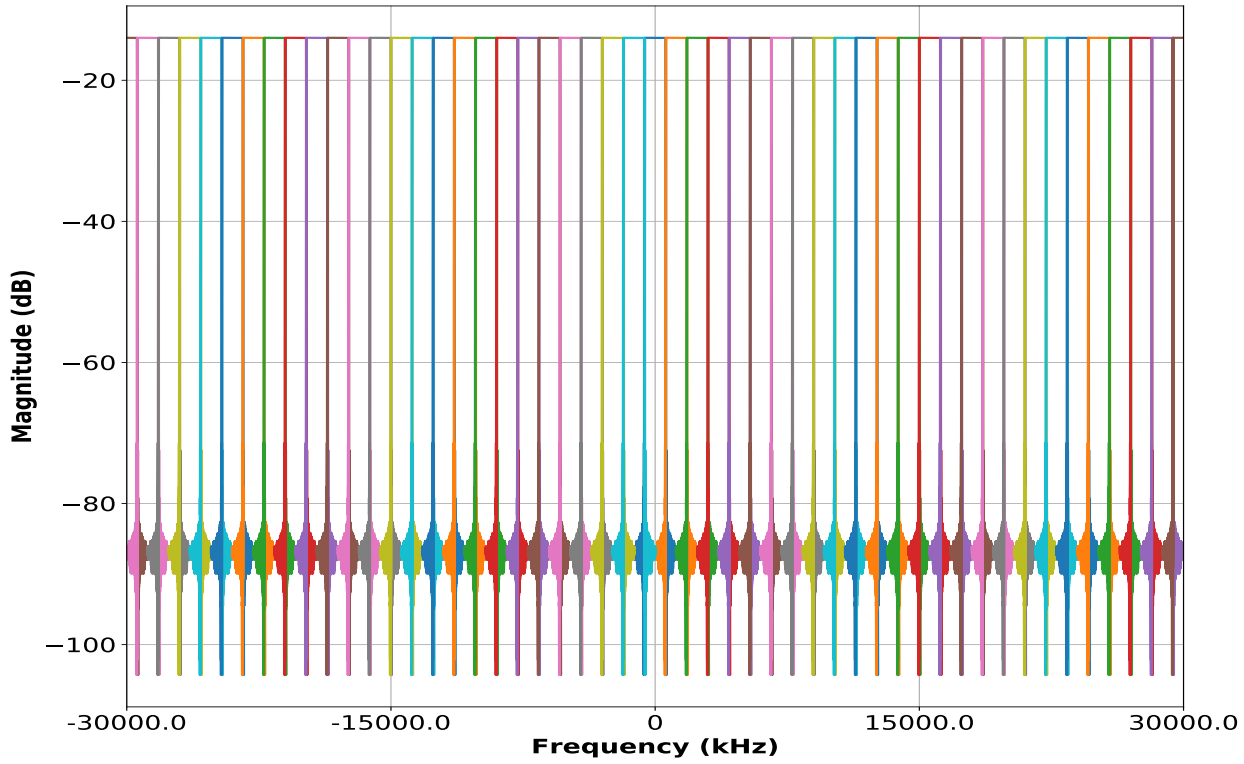


Figure 4.8: Prototype lowpass filter used in the 50-channel polyphase channelizer, with a cutoff frequency $f_{\text{cutoff}} = 1.2\,\text{MHz}$, a transition bandwidth $W_{\text{trans}} = 0.01 f_{\text{cutoff}}$, and an attenuation of 80 dB.

a splitting would have a much lower bandwidth, allowing to drastically decrease the required sample rate to analyse them. To validate the filter design parameters, a synthesising operation could be performed, consisting in bringing the various channels together: if no attenuation is present, the signal integrity is guaranteed. The result of such a synthesising operation is shown in figure 4.9, showing virtually no attenuation over the 60 MHz bandwidth. The seemingly

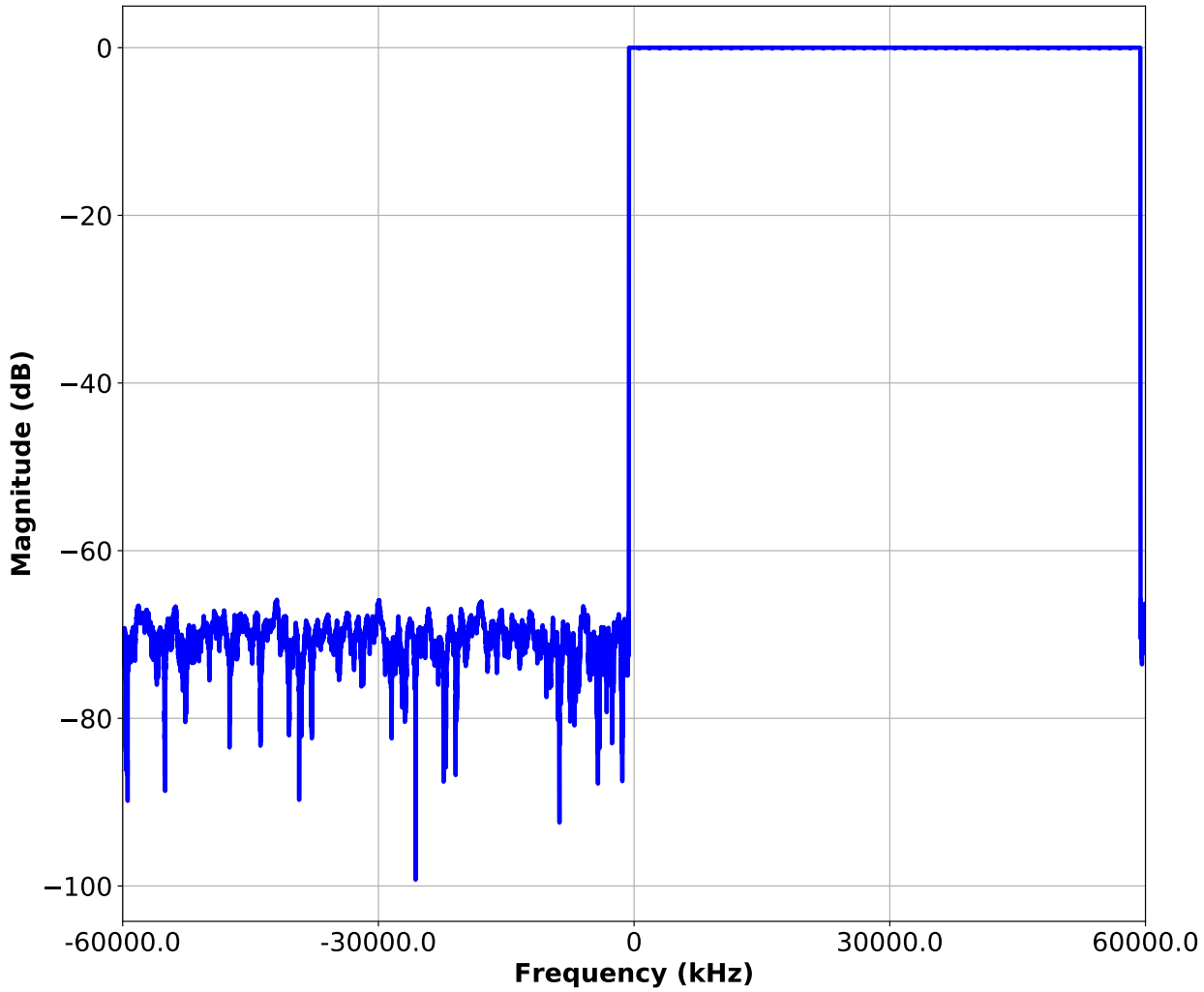


Figure 4.9: Signal synthesis from channelized spectrum.

very good filter comes with a catch, namely its high number of taps: given the requirements, it was found numerically that the filter features 36363 taps which, once split among the $M = 50$ channels, leads to a 728-taps-long filter for each channelizer arm. Let alone the high resources required to acquire and deal with the full 60 MHz, the lengthy filters hints that a traditional computer implementation is not enough, and that a FPGA-based solution is required.

Power and dynamic threshold computations

Once the wideband signal has been split into many narrowband components, the power contained in each of those bands can be computed. In this work, using Parseval's identity, an estimate of the power is computed by taking the average of the modulus of the signal coefficients, i.e. the power contained in band Q is computed as $\mathcal{P}_Q \approx \frac{1}{N}\sum_{n=1}^{N} |x[n]|^2$, where the average is taken over N samples. Taking the average of those averages gives an estimate of the total power, which can serve as a (dynamic) threshold. Such an approach allows, in principle, to discriminate

between the presence of mere noise and signal plus noise combination. This distinction amounts to a binary hypothesis test problem, and can be written under the form

$$\begin{aligned} H_0 &: r(t) = n(t) && \text{(noise only)} \\ H_1 &: r(t) = n(t) + s(t) && \text{(signal and noise),} \end{aligned}$$

and consists in maximizing the correct guess, i.e. maximize the likelihood of not emitting a jamming signal when there is nothing but noise or, on the contrary, jam a signal only when it is present. A graphical representation of the threshold placement, and its influence on the decision making, is shown in figure 4.10, where the false alarm and miss probability are highlighted. The case where the noise only probability density function is above the threshold corresponds

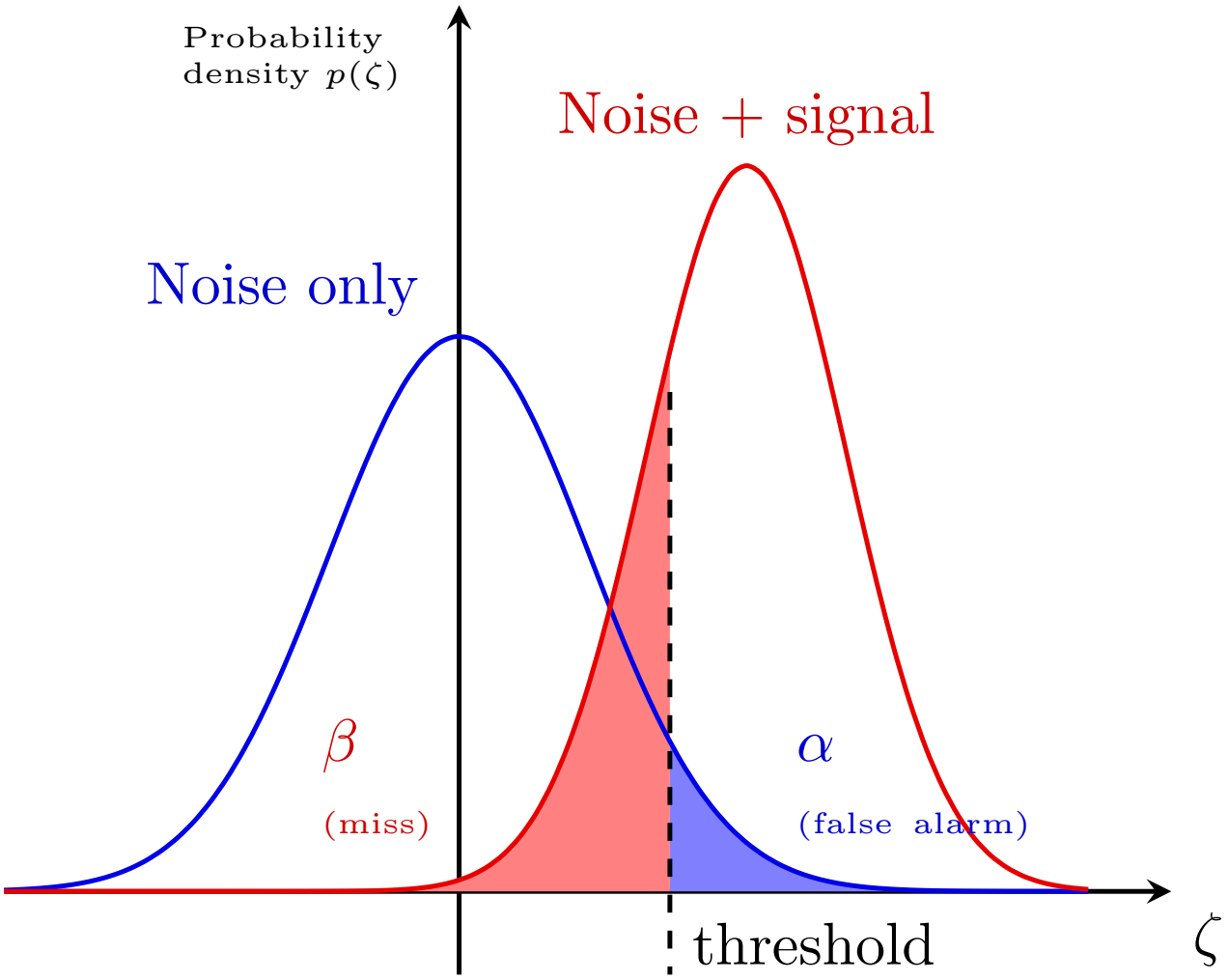


Figure 4.10: Graphical representation of the threshold placement and how it influences the false alarm and miss probabilities. Image adapted from [51].

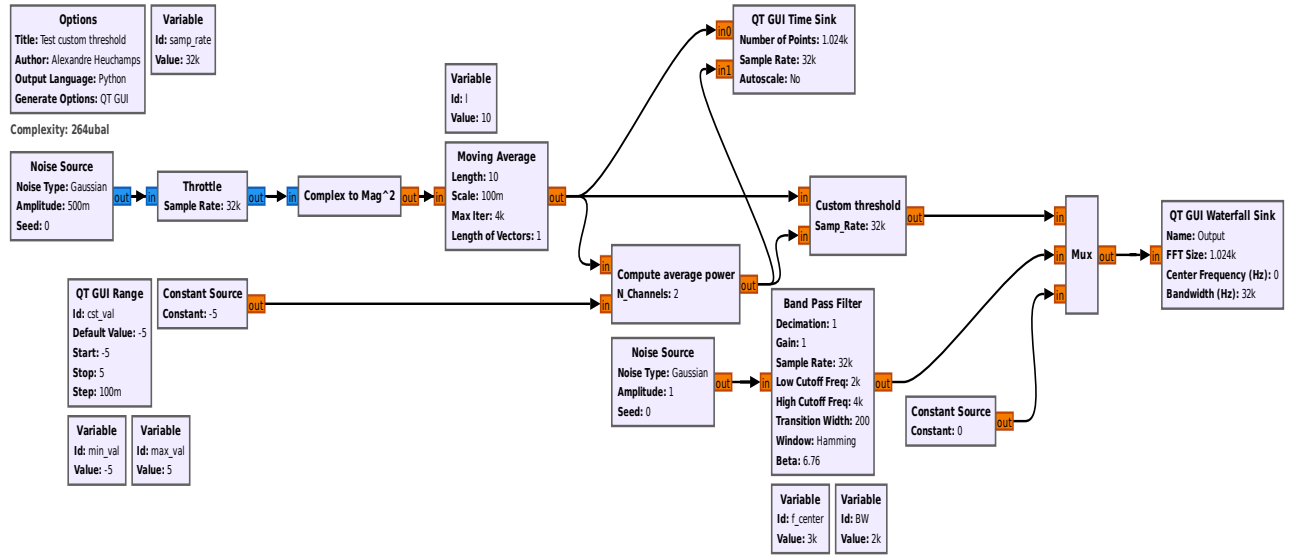
to a false alarm, as there is only noise present but the signal level is above the threshold. On the other hand, the case where the noise + signal probability density function lies below the threshold corresponds to a miss, as no signal is declared present, even if the is one. The detection probability is given by the area under the red curve up to the threshold.

Signal selection

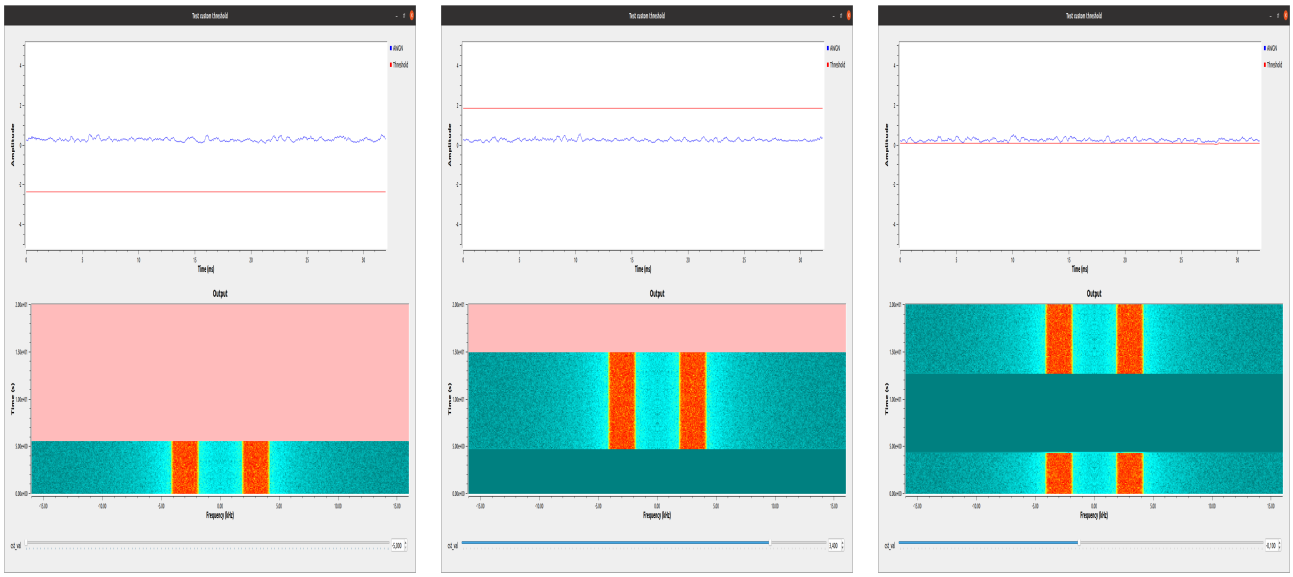
The average power contained in the signal serves as a dynamic threshold, and is fed into a custom GNU Radio block, in which either nothing or a bandpassed white Gaussian noise is

emitted. Noise bandwidth is the same as that of the different channels of the channelizer, with a centre frequency centred around that of the considered channel (known in virtue of frequency wrapping inside the channelizer).

A graphical representation of typical GNU Radio flowchart for a signal selector is shown in figure 4.11a, with typical outputs shown in figures 4.11b to 4.11d. When the input has a



(a) Signal selector



(b) Above threshold **(c)** Under threshold **(d)** Above threshold (again)

Figure 4.11: GNU Radio flowchart and output for the signal selector.

power greater than a threshold (represented by a constant source in the above illustration), a bandpassed AWGN is emitted. When the power is below the threshold, nothing is emitted. For the sake of illustration, the Gaussian noise is centred around a frequency $f_{\text{centre}} = 3\,\text{kHz}$ with an arbitrarily chosen bandwidth of 2 kHz. As stated previously, those parameters should be chosen such as to respect the constraints of the studied situation (a bandwidth of 1.2 MHz, centred around the the frequency of the channel containing the biggest power).

Everything together

Putting all the blocks together would lead to a scheme analogous to that shown in figure 4.7. Due to the high bandwidth to acquire (and subsequent computational load for a computer CPU), no practical implementation of the complete jammer could be realised in software. The interaction of the different blocks can nevertheless be simulated with parameters making the computations bearable for a computer. The flowgraph used to test the various blocks interconnections is shown in figure 4.12. It consists in a signal switching periodically between a single sinusoid at

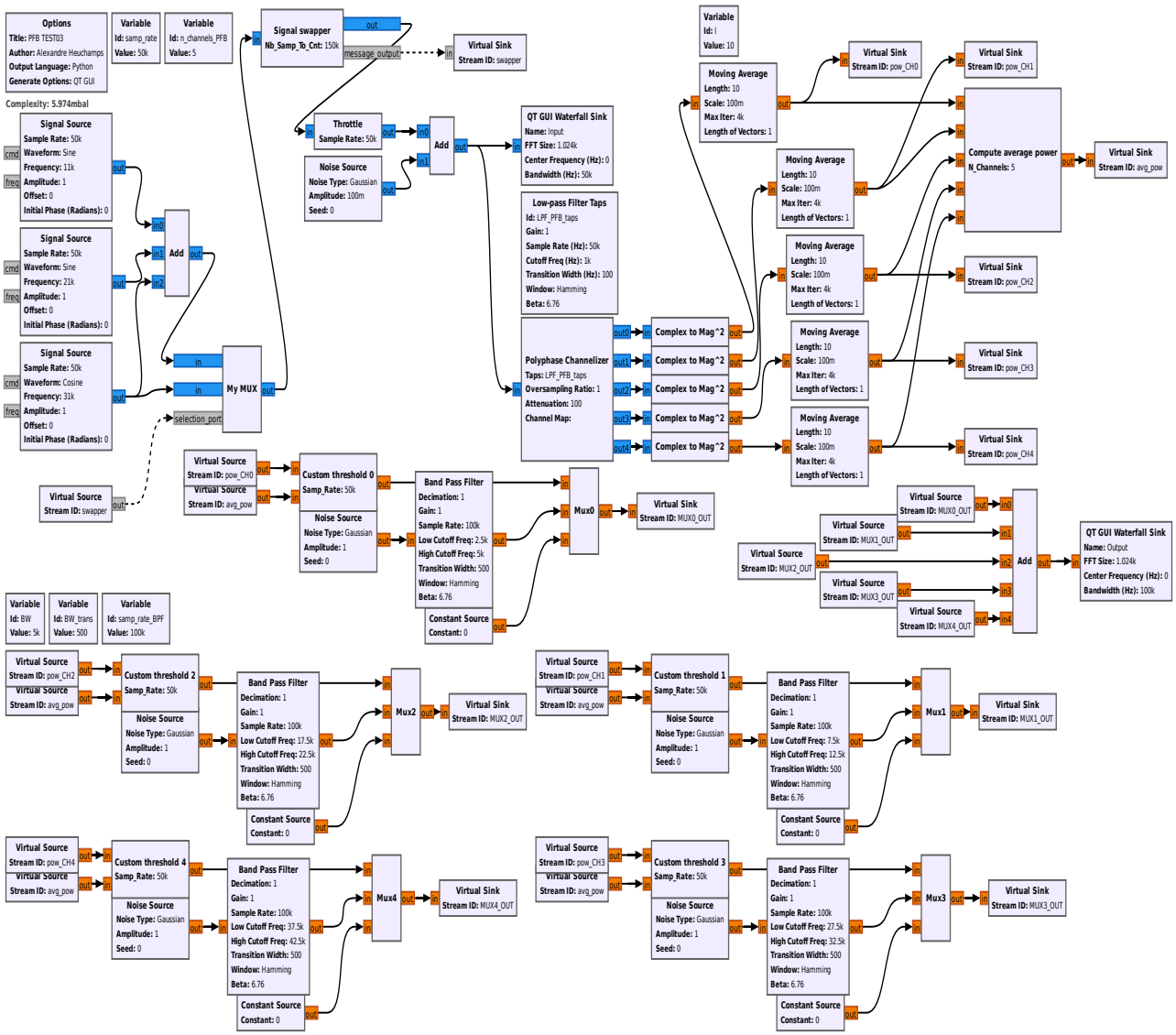


Figure 4.12: GNU Radio flowchart of the complete reactive jammer.

31 kHz or a sum of three sinusoid at frequencies of 11 kHz, 21 kHz, and 31 kHz, to which an AWGN is added. The resulting signal is then fed to a 5-arm polyphase filter bank, and for which the prototype filter is a lowpass filter, with a cutoff frequency of $f_{\text{cutoff}} = 1\,\text{kHz}$ and a transition bandwidth ten times smaller, i.e. $W_{\text{trans}} = 100\,\text{Hz}$. The power contained in each channel is then computed, and sent to signal selectors, which outputs were schematically represented in figure 4.11. The average power contained in all the channels is also computed, the result of which is fed as dynamic threshold for the signal selectors, in agreement with the discussion given in section 4.2.3. The circuit presented in figure 4.12 could be refined, by including the various signal selector blocks into a so-called hierarchical GNU Radio block, for example. Unfortunately, for reasons unknown to the author, this solution proved ineffective, as no filtering of the AWGN

inside those blocks could be achieved.

Figure 4.13 shows the relation between the input and output signals (both software simulated rather than experimentally acquired). It appears from the figure that when a signal with a given

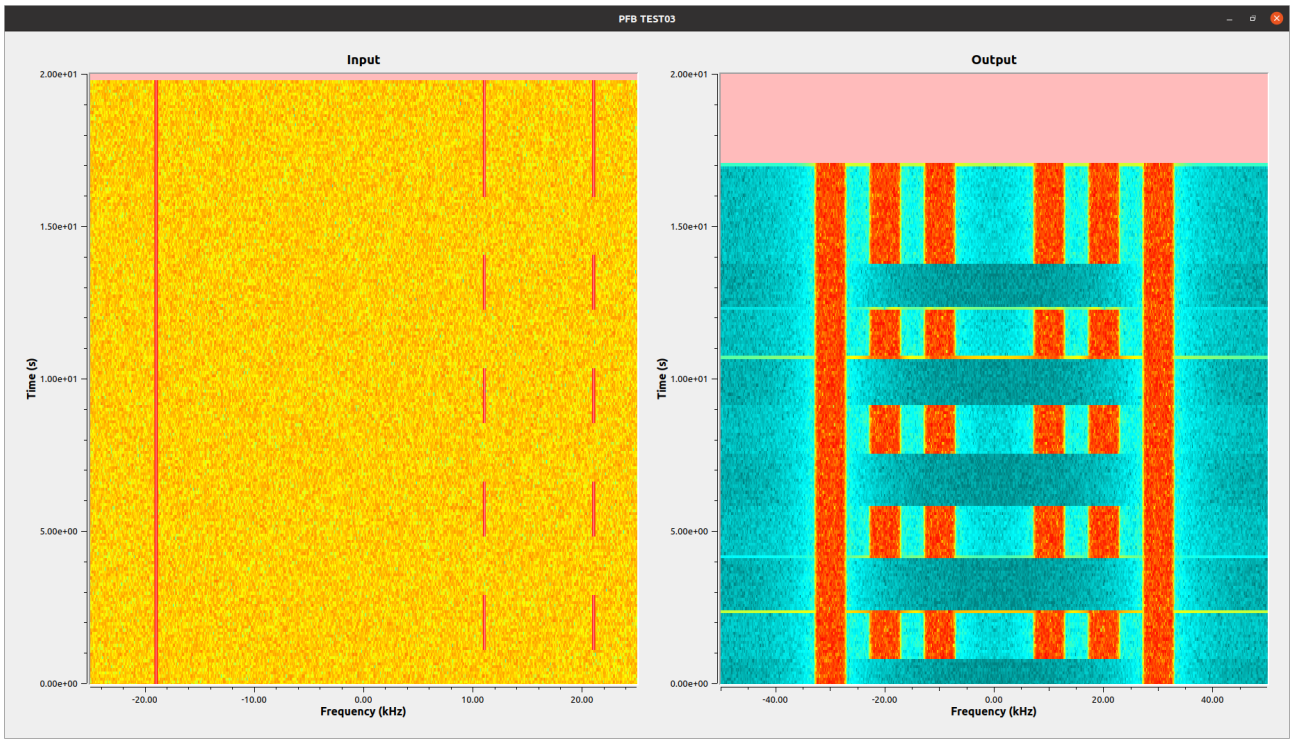


Figure 4.13: Graphical representation showing the (simulated) received signal on the input, and the corresponding (simulated) signal emitted at the output of the jammer.

centre frequency is detected with a power above the average power contained in all the channels, a bandpassed AWGN is emitted, centred around the centre frequency of that channel (i.e. centred around a frequency $f_{\text{centre}} = k\frac{samp\_rate}{M}$ for the k^{th} channel in a M-channel channelizer). It should be noted that the sine with frequency 31 kHz appear at -19 kHz in the left-pannel of figure 4.13, due to spectral folding inherent to DSP techniques, which does not preclude the technique to detect several occupied bands simultaneously. From the same figure, it also appears that some delay between the input and output exists, due to computations required for the AWGN filtering.

5 Conclusion

The combination of today's UASs pervasiveness, coupled with lack of clear regulating laws, leads to increasing fears regarding various aspects of life, ranging from mere privacy issues, to State safety integrity. In those regards, the scope of this work was to investigate the feasibility of a (drone-mounted) telecommunication jammer, to respond to those potential threats.

The investigation was initiated with some theoretical reminders in chapter 2, mainly aimed at introducing fundamental concepts and vocabulary used throughout the remainder of the text. More specifically, a rapid overview of drones was given in section 2.1, with a brief discussion on their classification, as well as some of their embedded hardware. The discussion was then extended in section 2.2, where some (digital) telecommunication principles ware presented and reviewed. Building upon those telecommunication aspects, some technicalities about SS techniques were presented in section 2.3, with focus on both direct-sequence and frequency-hopping, in sections 2.3.1 and 2.3.2, respectively, due to their well-studied characteristics and intensive use in drone remote controller communications. A final touch of reminders was provided in section 2.4, where various jamming techniques were presented and briefly discussed, with emphasis on barrage, (multi)tone, sweep, and reactive jammers in sections 2.4.1 to 2.4.4.

Building upon the theoretical reminders, a presentation of both hardware and software platforms used in this work were presented in chapter 3. The discussion in section 3.1 concerns hardware considerations, with first general principles of SDRs presented in section 3.1.1, and concrete considerations regarding the Lime SDR in section 3.1.2. The GNU Radio software platform was then presented and discussed in section 3.2.

Experimental implementations and results were then presented in chapter 4 for some of the jammers discussed previously. The discussion, initiated with a presentation of the experimental setup and signal characterisation in section 4.1, from which it was observed that the communication between a drone and its remote controller used a FHSS transmission technique, was then extended to results from some of the previously-presented jammer implementations in section 4.2. More specifically, the results of the ineffective barrage jammer implementation are first given in section 4.2.1, in which a preliminary mathematical model backs up the experimental conclusion that such a technique is ineffective against frequency hopping systems. The subsequent jammer configurations are then presented in sections 4.2.2 and 4.2.3, where no "real" application could be tested, due to high computational requirements (no better explanation to that fact can be given than the quote from [69]: "At high sample rates, even the simplest digital filtering task may saturate the hardware processing limit. This is because the hardware operation speed is limited by its clock rate, and the number of operations required per clock interval is directly

related to signal's sampling rate or bandwidth."). Despite not being able to confirm/infirm the proposed methods, simulations for a reactive jammer highlight its potential to detect and jam dynamically the occupied channel(s) only when a signal is detected.

Despite not being able to clearly answer the question to know whether a (drone-mounted) jammer is practically realisable or not, this work lays the foundations to further subsequent works. More precisely, as shown in section 4.2.3, the proposed scheme seems to bear interesting results. Consequently, a direct extension of this work, consisting in translating the GNU Radio codes into a hardware description language such as VHDL or Verilog, could allow to test in real-world conditions the feasibility of the project. A lot of other works can also be thought of, such as implementing a packet analyser, allowing to focus on a specific drone in a swarm configuration or, as stated in the introduction, additional frequency ranges to the 2.4 GHz could be targeted, allowing to disable potential video and/or GNSS links.

Bibliography

[1] J. Dorsey and N. Amaral, *Military drones in Europe, Ensuring transparency and accountability*, C. house, Ed. April 2021, ISBN: 9781784134556. [Online]. Available: https://www.chathamhouse.org/sites/default/files/2021-04/2021-04-30-military-drones-europe-dorsey-amaral.pdf (visited on 22nd April 2022).

[2] T. Laţici, 'Civil and military drones, Navigating a disruptive and dynamic technological ecosystem,' *EPRS: European Parliamentary Research Service*, October 2019. [Online]. Available: https://policycommons.net/artifacts/1337677/civil-and-military-drones/1945645/ (visited on 22nd April 2022).

[3] V. Mittal, 'Puzzling out the drone war over ukraine,' *IEEE Spectrum*, March 2022. [Online]. Available: https://spectrum.ieee.org/ukraine-drone-war (visited on 22nd April 2022).

[4] Belga, *France: Un drone de greenpeace survole une centrale nucléaire*, Jul. 2018. [Online]. Available: https://www.rtbf.be/article/france-un-drone-de-greenpeace-survole-une-centrale-nucleaire-9962974 (visited on 22nd April 2022).

[5] L'Express, *Un drone survole une centrale nucléaire en belgique*, December 2014. [Online]. Available: https://www.lexpress.fr/actualite/monde/un-drone-survole-une-centrale-nucleaire-en-belgique_1634743.html (visited on 22nd April 2022).

[6] K. Chávez and O. Swed, 'The proliferation of drones to violent nonstate actors,' *Defence Studies*, vol. 21, no. 1, pp. 1–24, 2021. DOI: 10.1080/14702436.2020.1848426. [Online]. Available: https://doi.org/10.1080/14702436.2020.1848426.

[7] F.-L. Chiper, A. Martian, C. Vladeanu, I. Marghescu, R. Craciunescu and O. Fratu, 'Drone detection and defense systems: Survey and a software-defined radio-based solution,' *Sensors*, vol. 22, no. 4, 2022, ISSN: 1424-8220. DOI: 10.3390/s22041453. [Online]. Available: https://www.mdpi.com/1424-8220/22/4/1453.

[8] C. Stöcker, R. Bennett, F. Nex, M. Gerke and J. Zevenbergen, 'Review of the current state of uav regulations,' *Remote Sensing*, vol. 9, no. 5, 2017, ISSN: 2072-4292. DOI: 10.3390/rs9050459. [Online]. Available: https://www.mdpi.com/2072-4292/9/5/459.

[9] H. Nakamura and Y. Kajikawa, 'Regulation and innovation: How should small unmanned aerial vehicles be regulated ?' *Technological Forecasting and Social Change*, vol. 128, pp. 262–274, 2018, ISSN: 0040-1625. DOI: 10.1016/j.techfore.2017.06.015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0040162517307977.

[10] T. M. Jones, *International Commercial Drone Regulation and Drone Delivery Services*. Santa Monica, CA: RAND Corporation, 2017. DOI: 10.7249/RR1718.3.

[11] J. Busset, F. Perrodin, P. Wellig *et al.*, 'Detection and tracking of drones using advanced acoustic cameras,' in *Unmanned/Unattended Sensors and Sensor Networks XI; and Advanced Free-Space Optical Communication Techniques and Applications*, E. M. Carapezza, P. G. Datskos, C. Tsamis, L. Laycock and H. J. White, Eds., International Society for Optics and Photonics, vol. 9647, SPIE, 2015, pp. 53–60. DOI: 10.1117/12.2194309. [Online]. Available: https://doi.org/10.1117/12.2194309.

[12] A. Bernardini, F. Mangiatordi, E. Pallotti and L. Capodiferro, 'Drone detection by acoustic signature identification,' *Electronic Imaging*, vol. 2017, no. 10, pp. 60–64, 2017.

[13] Z. Shi, X. Chang, C. Yang, Z. Wu and J. Wu, 'An acoustic-based surveillance system for amateur drones detection and localization,' *IEEE Transactions on Vehicular Technology*, vol. 69, no. 3, pp. 2731–2739, 2020. DOI: 10.1109/TVT.2020.2964110.

[14] A. Rozantsev, V. Lepetit and P. Fua, 'Detecting flying objects using a single moving camera,' *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 39, no. 5, pp. 879–892, 2017. DOI: 10.1109/TPAMI.2016.2564408.

[15] R. Opromolla, G. Fasano and D. Accardo, 'A vision-based approach to uav detection and tracking in cooperative applications,' *Sensors*, vol. 18, no. 10, 2018, ISSN: 1424-8220. DOI: 10.3390/s18103391. [Online]. Available: https://www.mdpi.com/1424-8220/18/10/3391.

[16] C. J. Li and H. Ling, 'An investigation on the radar signatures of small consumer drones,' *IEEE Antennas and Wireless Propagation Letters*, vol. 16, pp. 649–652, 2017. DOI: 10.1109/LAWP.2016.2594766.

[17] P. Wellig, P. Speirs, C. Schuepbach *et al.*, 'Radar systems and challenges for c-uav,' in *2018 19th International Radar Symposium (IRS)*, 2018, pp. 1–8. DOI: 10.23919/IRS.2018.8448071.

[18] P. Nguyen, M. Ravindranatha, A. Nguyen, R. Han and T. Vu, 'Investigating cost-effective rf-based detection of drones,' in *Proceedings of the 2nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use*, ser. DroNet '16, Singapore, Singapore: Association for Computing Machinery, 2016, pp. 17–22, ISBN: 9781450344050. DOI: 10.1145/2935620.2935632. [Online]. Available: https://doi.org/10.1145/2935620.2935632.

[19] P. Nguyen, H. Truong, M. Ravindranathan, A. Nguyen, R. Han and T. Vu, 'Matthan: Drone presence detection by identifying physical signatures in the drone's rf communication,' in *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services*, ser. MobiSys '17, New York, NY, USA: Association for Computing Machinery, 2017, pp. 211–224, ISBN: 9781450349284. DOI: 10.1145/3081333.3081354. [Online]. Available: https://doi.org/10.1145/3081333.3081354.

[20] S. Basak, S. Rajendran, S. Pollin and B. Scheers, 'Combined rf-based drone detection and classification,' *IEEE Transactions on Cognitive Communications and Networking*, vol. 8, no. 1, pp. 111–120, 2022. DOI: 10.1109/TCCN.2021.3099114.

[21] X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi and J. Chen, 'Anti-drone system with multiple surveillance technologies: Architecture, implementation, and challenges,' *IEEE Communications Magazine*, vol. 56, no. 4, pp. 68–74, 2018. DOI: 10.1109/MCOM.2018.1700430.

[22] F. Svanström, C. Englund and F. Alonso-Fernandez, 'Real-time drone detection and tracking with visible, thermal and acoustic sensors,' in *2020 25th International Conference on Pattern Recognition (ICPR)*, 2021, pp. 7265–7272. DOI: 10.1109/ICPR48806.2021.9413241.

[23] V. Chamola, P. Kotesh, A. Agarwal, Naren, N. Gupta and M. Guizani, 'A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques,' *Ad Hoc Networks*, vol. 111, p. 102 324, 2021, ISSN: 1570-8705. DOI: 10.1016/j.adhoc.2020.102324. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870520306788.

[24] W. A. Radasky, C. E. Baum and M. W. Wik, 'Introduction to the special issue on high-power electromagnetics (hpem) and intentional electromagnetic interference (iemi),' *IEEE Transactions on Electromagnetic Compatibility*, vol. 46, no. 3, pp. 314–321, 2004. DOI: 10.1109/TEMC.2004.831899.

[25] B. Zohuri, 'Retracted chapter: High-power microwave energy as weapon,' in *RETRACTED BOOK: Directed-Energy Beam Weapons*. Cham: Springer International Publishing, 2019, pp. 269–308, ISBN: 9783030207946. DOI: 10.1007/978-3-030-20794-6_4.

[26] E. Darack, 'Attack of the drone-snatching eagles, A natural solution to a growing threat,' *Smithonian Magazine*, March 2017.

[27] 'Protecting the sky: Signal monitoring of radio controlled civilian unmanned aerial vehicles and possible countermeasures,' Ptolemaeuslaan 900, 3528 BV Utrecht, Nederland, Tech. Rep.

[28] D. Mototolea, 'A study on the actual and upcoming drone communication systems,' in *2019 International Symposium on Signals, Circuits and Systems (ISSCS)*, ser. 2019 International Symposium on Signals, Circuits and Systems (ISSCS), 2019, pp. 1–4. DOI: 10.1109/ISSCS.2019.8801800. [Online]. Available: https://doi.org/10.1109/ISSCS.2019.8801800.

[29] R. Prasad, P. Popovski and H. Yomo, 'Strategies for adaptive frequency hopping in the unlicensed bands,' *IEEE Wireless Communications*, vol. 13, no. 6, pp. 60–67, 2006, ISSN: 1558-0687. DOI: 10.1109/MWC.2006.275200. [Online]. Available: https://doi.org/10.1109/MWC.2006.275200.

[30] G. X. Gao, M. Sgammini, M. Lu and N. Kubo, 'Protecting gnss receivers from jamming and interference,' *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1327–1338, 2016, ISSN: 1558-2256. DOI: 10.1109/JPROC.2016.2525938. [Online]. Available: https://doi.org/10.1109/JPROC.2016.2525938.

[31] S. Zahran, A. Moussa and N. El-Sheimy, 'Enhanced drone navigation in gnss denied environment using vdm and hall effect sensor,' *ISPRS International Journal of Geo-Information*, vol. 8, no. 4, 2019, ISSN: 2220-9964. DOI: 10.3390/ijgi8040169. [Online]. Available: https://www.mdpi.com/2220-9964/8/4/169.

[32] M. Ceccato, F. Formaggio and S. Tomasin, 'Spatial gnss spoofing against drone swarms with multiple antennas and wiener filter,' *IEEE Transactions on Signal Processing*, vol. 68, pp. 5782–5794, 2020, ISSN: 1941-0476. DOI: 10.1109/TSP.2020.3028752. [Online]. Available: https://doi.org/10.1109/TSP.2020.3028752.

[33] S. Tzu, *The Art of War*, 1st ed. Filiquarian, November 2007, p. 68, ISBN: 9781599869773.

[34] N. S. O. (NSO), *Nato standard ajp-3.3. allied joint doctrine for air and space operations.* Version 1, April 2016. [Online]. Available: https://www.japcc.org/wp-content/uploads/AJP-3.3-EDB-V1-E.pdf (visited on 24th April 2022).

[35] M. Hassanalian and A. Abdelkefi, 'Classifications, applications, and design challenges of drones: A review,' *Progress in Aerospace Sciences*, vol. 91, pp. 99–131, 2017, ISSN: 0376-0421. DOI: 10.1016/j.paerosci.2017.04.003. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0376042116301348 (visited on 24th April 2022).

[36] D. of Defense, *Unmanned aircraft system airspace integration plan*, version 2, March 2011. [Online]. Available: https://info.publicintelligence.net/DoD-UAS-AirspaceIntegration.pdf (visited on 24th April 2022).

[37] G. Markarian and A. Staniforth, *Countermeasures for Aerial Drones*, 2nd ed., N. A. House, Ed. 2021, p. 350, ISBN: 9781630818012.

[38] V. Kangunde, R. S. Jamisola and E. K. Theophilus, 'A review on drones controlled in real-time,' *International Journal of Dynamics and Control*, vol. 9, no. 4, pp. 1832–1846, December 2021, ISSN: 2195-2698. DOI: 10.1007/s40435-020-00737-5. [Online]. Available: https://doi.org/10.1007/s40435-020-00737-5.

[39] B. Vergouw, H. Nagel, G. Bondt and B. Custers, 'Drone technology: Types, payloads, applications, frequency spectrum issues and future developments,' in *The Future of Drone Use: Opportunities and Threats from Ethical and Legal Perspectives*, B. Custers, Ed. The Hague: T.M.C. Asser Press, 2016, pp. 21–45, ISBN: 978-94-6265-132-6. DOI: 10.1007/978-94-6265-132-6_2. [Online]. Available: https://doi.org/10.1007/978-94-6265-132-6_2 (visited on 18th May 2022).

[40] B. Sklar and fred j. harris, *Digital Communications, Fundamentals and Applications*, eng, 3rd ed. New York: Pearson, 2020, ISBN: 9780134588568.

[41] F. Xiong, *Digital modulation techniques*, 2nd ed., A. H. Publishers, Ed. 2006, p. 1046, ISBN: 9781580538633.

[42] C. E. Shannon, 'A mathematical theory of communication,' *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, Jul. 1948. DOI: 10.1002/j.1538-7305.1948.tb01338.x. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/j.1538-7305.1948.tb01338.x.

[43] M. H. Kiesler and A. George, 'Secret commuincation system,' 2292387A, Jun. 1941. [Online]. Available: https://patents.google.com/patent/US2292387A/en (visited on 12th March 2022).

[44] P. M. C. Lal, V. S. Palsule and K. V. Ravi, 'Applications of frequency hopping spread spectrum techniques: An overview,' *IETE Technical Review*, vol. 3, no. 5, pp. 210–220, 1986. DOI: 10.1080/02564602.1986.11437952.

[45] R. Jordan and C. T. Abdallah, 'Wireless communications and networking: An overview,' *IEEE Antennas and Propagation Magazine*, vol. 44, no. 1, pp. 185–193, 2002, ISSN: 1558-4143. DOI: 10.1109/74.997963. [Online]. Available: https://doi.org/10.1109/74.997963 (visited on 12th March 2022).

[46] E. Lopelli, J. van der Tang and A. van Roermund, 'Fhss systems: State-of-the-art and power trade-offs,' in *Architectures and Synthesizers for Ultra-low Power Fast Frequency-Hopping WSN Radios*. Dordrecht: Springer Netherlands, 2011, pp. 45–91, ISBN: 978-94-007-0183-0. DOI: 10.1007/978-94-007-0183-0_3. [Online]. Available: https://doi.org/10.1007/978-94-007-0183-0_3 (visited on 12th March 2022).

[47] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang and H.-H. Chen, 'Physical layer security in wireless networks: A tutorial,' *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66–74, 2011. DOI: 10.1109/MWC.2011.5751298.

[48] J. G. Proakis and M. Salehi, *Digital Communications*, eng, 5th ed. McGraw Hill, 2007, ISBN: 9780072957167.

[49] K. Pärlin, 'Jamming of spread spectrum commuincations used in uav remote control systems,' M.S. thesis, School of Information Technologies Thomas Johann Seebeck Department of Electronics, Tallinn, Estonia, 2017.

[50] D. Torrieri, *Principles of Spread-Spectrum Communication Systems*, 5th ed. Springer International Publishing, 2022, ISBN: 978-3-030-75342-9. DOI: 10.1007/978-3-030-75343-6.

[51] R. Poisel, *Modern Communications Jamming Principles and Techniques*, 2nd ed., A. H. Publishers, Ed. February 2011, ISBN: 9781608071654.

[52] R. Poisel, *Introduction to Communication Electronic Warfare Systems*, 2nd ed., A. H. Publishers, Ed. February 2008, ISBN: 9781596934528.

[53] T. Basar, 'The gaussian test channel with an intelligent jammer,' *IEEE Transactions on Information Theory*, vol. 29, no. 1, pp. 152–157, 1983. DOI: 10.1109/TIT.1983.1056602.

[54] J. H. Lee, B. S. Yu and S.-C. Lee, 'Probability of error for a hybrid ds/sfh spread-spectrum system under tone jamming,' in *IEEE Conference on Military Communications*, vol. 1, 1990, pp. 410–414. DOI: 10.1109/MILCOM.1990.117452.

[55] T. Ulversoy, 'Software defined radio: Challenges and opportunities,' *IEEE Communications Surveys Tutorials*, vol. 12, no. 4, pp. 531–550, 2010. DOI: 10.1109/SURV.2010.032910.00019.

[56] D. Torrieri, 'Fundamental limitations on repeater jamming of frequency-hopping communications,' *IEEE Journal on Selected Areas in Communications*, vol. 7, no. 4, pp. 569–575, 1989. DOI: 10.1109/49.17721.

[57] J. Mitola, 'The software radio architecture,' *IEEE Communications Magazine*, vol. 33, no. 5, pp. 26–38, 1995. DOI: 10.1109/35.393001.

[58] E. Venosa, frederic j. harris and F. A. N. Palmieri, *Software Radio, Sampling Rate Selection, Design and Synchronisation* (Analog Circuits and Signal Processing), 1st ed. Springer, New York, NY, ISBN: 9781461401124. DOI: 10.1007/978-1-4614-0113-1.

[59] B. Fette, *Cognitive Radio Technology*, 2nd ed. Academic Press, March 2009, ISBN: 9780123745354. DOI: 10.1016/B978-0-12-374535-4.X0001-X.

[60] L. Microsystems, 'Lms7002m product brief, Second generation field programmable radio frequency mimo transceiver,' Guildford, UK, White Paper, February 2015, p. 2. [Online]. Available: https://github.com/myriadrf/LMS7002M-docs/blob/master/LMS7002M_Product_Brief.pdf (visited on 4th May 2022).

[61] L. Microsystems, 'Lms7002m, Fprf mimi transceiver ic with integrated microcontroller,' English, Tech. Rep., version 3.2r00, Jul. 2019. [Online]. Available: https://github.com/myriadrf/LMS7002M-docs/blob/master/LMS7002M_Data_Sheet_v3.2r00.pdf (visited on 5th May 2022).

[62] C. A. Balanis, *Antenna Theory, Analysis and Design*, 4th ed. John Wiley & Sons, Inc., Hoboken, New Jersey, February 2016, p. 1104, ISBN: 9781118642061.

[63] M. G. Bellanger and J. L. Daguet, 'Tdm-fdm transmultiplexer: Digital polyphase and fft,' *IEEE Transactions on Communications*, vol. 22, no. 9, pp. 1199–1205, 1974. DOI: 10.1109/TCOM.1974.1092391.

[64] fredric j. harris, C. Dick and M. Rice, 'Digital receivers and transmitters using polyphase filter banks for wireless communications,' *IEEE Transactions on Microwave Theory and Techniques*, vol. 51, no. 4, pp. 1395–1412, 2003. DOI: 10.1109/TMTT.2003.809176.

[65] R. Mahesh, A. P. Vinod, E. M.-K. Lai and A. Omondi, 'Filter bank channelizers for multi-standard software defined radio receivers,' *Journal of Signal Processing Systems*, vol. 62, no. 2, pp. 157–171, February 2011, ISSN: 1939-8115. DOI: 10.1007/s11265-008-0327-y. [Online]. Available: https://doi.org/10.1007/s11265-008-0327-y (visited on 27th May 2022).

[66] fredric j. harris, E. Venosa, X. Chen and B. D. Rao, 'Polyphase analysis filter bank down-converts unequal channel bandwidths with arbitrary center frequencies,' *Analog Integrated Circuits and Signal Processing*, vol. 71, no. 3, pp. 481–494, Jun. 2012, ISSN: 1573-1979. DOI: 10.1007/s10470-011-9746-y. [Online]. Available: https://doi.org/10.1007/s10470-011-9746-y (visited on 4th Jun. 2022).

[67] P. M. Krishna and T. S. Babu, 'Polyphase channelizer demystified [lecture notes],' *IEEE Signal Processing Magazine*, vol. 33, no. 1, pp. 144–150, 2016. DOI: 10.1109/MSP.2015.2477423.

[68] fredric j. harris, *Multirate Signal Processing for Communication systems*, 2nd ed. River Publishers, March 2021, p. 618, ISBN: 9788770222105.

[69] X. Chen, F. J. Harris, E. Venosa and B. D. Rao, 'Non-maximally decimated analysis/synthesis filter banks: Applications in wideband digital filtering,' *IEEE Transactions on Signal Processing*, vol. 62, no. 4, pp. 852–867, 2014. DOI: 10.1109/TSP.2013.2295549.