TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies
Thomas Johann Seebeck Department of Electronics

Karel Pärlin, IVEM153252

JAMMING OF SPREAD SPECTRUM COMMUNICATIONS USED IN UAV REMOTE CONTROL SYSTEMS

Master's Thesis

Supervisors:
Muhammad Mahtab Alam
PhD

Yannick Le Moullec
PhD

Tallinn 2017

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond
Thomas Johann Seebecki elektroonikainstituut

Karel Pärlin, IVEM153252

MEHITAMATA ÕHUSÕIDUKITE JUHTIMISEKS KASUTATAVATE HAJASPEKTER SIDESÜSTEEMIDE SEGAMINE

Magistritöö

Juhendajad:
Muhammad Mahtab Alam
PhD

Yannick Le Moullec
PhD

Tallinn 2017

Author's declaration of originality

I hereby certify that I am the sole author of this thesis and this thesis has not been presented for examination or submitted for defence anywhere else. All used materials, references to the literature and work of others have been cited.

Author: Karel Pärlin
May 17, 2017

Abstract

Jamming of Spread Spectrum Communications Used in UAV Remote Control Systems

Unmanned aerial vehicles (UAV) have become widely available and their usage introduces new security risks. In particular, their reckless usage can lead to accidents and they can be intentionally used to carry out attacks or illegal surveillance from a distance. It has therefore become highly desirable to restrict UAV usage in areas such as airports, nuclear power plants, prisons, national borders and military controlled areas. Detection and neutralization of UAVs has consequently become an important research issue.

Most commercially available UAVs use spread spectrum techniques, such as direct sequencing and frequency hopping, in the remote control systems to reduce the impact of interference from other communication systems or remotely controlled UAVs on the system itself. As a result, the UAV remote control systems are also more difficult to neutralize.

In this thesis, an UAV neutralization system is proposed. Different jamming techniques are simulated against a hybrid spread spectrum system model which combines direct sequencing and frequency hopping. Based on the simulation results and similar research found in literature, protocol-aware jamming technique is chosen and implemented on a software defined radio platform. The developed UAV neutralization system is shown to work successfully against two widely used UAV remote control systems. Using the protocol-aware jamming technique, the developed system is capable of jamming the considered remote control systems when the jamming signal at the receiver is only couple decibels higher than the targeted signal.

The thesis is in English and contains 38 pages of text, 5 chapters, 33 figures.

Annotatsioon

Mehitamata õhusõidukite juhtimiseks kasutatavate hajaspekter sidesüsteemide segamine

Mehitamata õhusõidukitest on saanud laiatarbekaup ja nendega kaasnevad uued turvaohud. Mehitamata õhusõidukite reeglitevastane kasutamine võib põhjustada õnnetusi, ühtlasi võimaldavad need eemalt korraldada pahatahtlikke rünnakuid või jälgida piiratud juurdepääsuga alasid. Sellest tulenevalt on soovitav tundmatute mehitamata õhusõidukite kasutamist piirata näiteks lennujaamades, tuumeelektrijaamades, vanglates, riigipiiridel ja kaitseväe julgeolekualadel. Mehitamata õhusõidukite tuvastamisest ja kasutamise takistamisest on seega saanud aktuaalsed probleemid.

Enamikus kaubanduslikult kättesaadavate mehitamata õhusõidukite kaugjuhtimissüsteemides on kasutusel hajutatud spektriga signaalid, et vähendada teiste raadiosageduslike süsteemide (sh teiste mehitamata õhusõidukite kaugjuhtimissüsteemide) segavat mõju kaugjuhtimissüsteemile. Selle tagajärjel on aga keerukam ka nende kaugjuhtimissüsteemide tuvastamine ja kasutamise takistamine ehk segamine.

Käesolevas lõputöös kirjeldatakse kaugjuhitavate mehitamata õhusõidukite tuvastamiseks ja segamiseks loodud süsteemi ning antud lõputöö raames tehtud panust selle süsteemi loomisel. Lõputöö keskendub nimetatud süsteemi ühele alamosale, mille ülesandeks on kaugjuhtimissignaalide segamine. Erinevate segamistehnikate mõju hajaspekter signaale kasutavate süsteemide tööle on hinnatud käesolevas töös simulatsioonide abil. Simulatsioonide ja kirjanduse põhjal välja valitud protokolliteadlikku segamistehnikat kasutav segaja on implementeeritud tarkvaralise raadio platvormil.

Loodud protokolliteadliku segaja ja kahe teistsuguse segamistehnikaga süsteemi efektiivsust on käesolevas töös uuritud laialtlevinud mehitamata õhusõidukite kaugjuhtimissüsteemide vastu. Kuigi protokolliteadliku segaja rakendamine on keerulisem kui võrreldud segajate puhul, sarnanevad mõõdetud segajate efektiivsused simulatsioonide tulemustega ning kinnitavad loodud protokolliteadliku segaja paremust.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 38 leheküljel, 5 peatükki, 33 joonist.

Acknowledgements

I would like to use the chance to express my gratitude to those who have contributed to this research project.

First of all, I want to thank my supervisors, Muhammad Mahtab Alam and Yannick Le Moullec, from the Thomas Johann Seebeck Department of Electronics at the Tallinn University of Technology for their patient guidance and useful critiques of my work.

This project has been carried out in cooperation with Rantelon and I am thankful to them for providing the necessary equipment together with the jammer platform used for comparison in this thesis. Also their assistance throughout this project is much appreciated. Special thanks is addressed to Gaspar Karm who developed the detection subsystem and assisted me with several aspects of my work.

My studies have been supported by the Vladimir Heinrichsen's scholarship of which I am very grateful. It has allowed me to focus on my studies and on writing this thesis.

Acronyms

ACCST Advanced Continuous Channel Shifting Technology. 41, 42, 44–46

ADC analog-to-digital converter. 33, 53, 54

AJ antijam. 19, 26, 29

ASK amplitude-shift keying. 38, 39

AWGN additive white Gaussian noise. 21, 26

BER bit error rate. 19, 26, 27, 29, 30, 42, 43

BPSK binary phase-shift keying. 19, 22

CORDIC Coordinate Rotation Digital Computer. 38–41, 56, 57

DAC digital-to-analog converter. 33, 53, 54

DSP digital signal processing. 15, 33

DSSS direct-sequence spread spectrum. 16, 18, 19, 22, 23

FASST Futaba Advanced Spread Spectrum Technology. 41–43, 45, 46

FHSS frequency-hopping spread spectrum. 16, 18, 21–23, 29

FIFO first in, first out. 35, 38

FPGA field-programmable gate array. 15, 32–36, 38, 41, 47, 53, 56

FSK frequency-shift keying. 24, 38, 39

GLONASS Global Navigation Satellite System. 13

GNSS global navigation satellite system. 11, 13–15, 47, 48

GPIO general-purpose input/output. 35

GPS Global Positioning System. 13, 17, 32

GSM Global System for Mobile Communications. 32

IF intermediate frequency. 32, 33, 54

ISM industrial, scientific, and medical radio. 12, 14, 23

JSR jam-to-signal ratio. 19, 20, 26, 27, 30, 42–45

JTAG Joint Test Action Group. 33

PLL phase-locked loop. 37

PN pseudo noise. 16, 19, 23, 26, 38

PSK phase-shift keying. 38, 39

RF radio frequency. 11–15, 19, 21, 23, 24, 30, 33, 36, 41, 46, 48, 53, 54

RTL register-transfer level. 34, 39

SDR software defined radio. 12, 14, 15, 32, 53, 54, 56

SNR signal-to-noise ratio. 17, 19, 21, 26

SPI Serial Peripheral Interface bus. 33

UART universal asynchronous receiver/transmitter. 33

UAV unmanned aerial vehicle. 11–16, 21–24, 31, 32, 34, 36, 37, 41–48

VCO voltage controlled oscillator. 37

VHDL VHSIC Hardware Description Language. 34

Contents

List of Figures

1 Introduction

Unmanned aerial vehicles (UAVs) have made the leap from military to consumer grade with UAVs being widely used for personal interest and in industries ranging from cinematography to construction and law enforcement. Goldman Sachs aerospace and defense research analysts forecast UAVs becoming a $100 billion market by 2020 [1]. This increase in the availability of consumer grade UAVs has lead to new challenges in security and surveillance. Specifically, there is a need for restricting the usage of UAVs in areas such as airports, nuclear power plants, prisons, national borders and military controlled areas where UAVs might cause accidents or be used for illegal purposes.

To prevent the possible risks involved with non-regulated UAV flights, methods for detection and neutralization of UAVs are essential. Detecting and neutralizing UAVs has been recognized as an important issue by various authorities, such as in the European research call H2020-SEC-2016-2017 with topic "Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism" and sub-topic "Detection and neutralization of rogue/suspicious light drone/UAV flying over restricted areas."

This thesis is part of a project to design and implement a portable cognitive system for detecting and neutralizing rogue UAVs. UAVs generally have either a flight route preprogrammed and use global navigation satellite system (GNSS) signals to follow the preprogrammed path, or they are being manually controlled using a remote control. If the UAV has a flight route preprogrammed and it is not itself transmitting any signals, then it can be detected for example by visual or radar based methods but not by passively analyzing the radio frequency (RF) spectrum. If the UAV is being remotely controlled, or it is transmitting for example a video feedback or positional information, then the transmitted signals can be distinguished in the RF spectrum. Based on the way the UAV is operated, either some RF signal is transmitted by the UAV or its remote control or not; the detection and jamming methods which can be applied are therefore quite different. The system, which this thesis is a part of, focuses on detecting and neutralizing the RF signals from the remote control to the UAV.

This thesis focuses on the neutralization, that is jamming and takeover, of the UAVs remote control signals. The goal of UAV jamming is to introduce a high enough error rate in the RF receiver of the UAV so that it would not be able to react to the commands from the remote control. Several different jamming techniques exist, for example barrage, tone, sweep and protocol-aware jamming are considered in this thesis and a detailed overview of these techniques is given in Subsection 2.2. Similar research into the performance of

different jamming techniques against other RF communication systems suggests that to efficiently jam the remote control link of an UAV, it is desirable to use the protocol-aware jamming technique [2]. This technique takes into account the characteristics of the RF signal transmitted by the remote control and uses a jamming signal similar to the signal transmitted by the remote control. In comparison, barrage, tone and sweep jamming techniques are less sophisticated and do not take all of the targeted signal characteristics into consideration.

Different UAV systems use different frequencies, modulations and spread spectrum techniques, which requires the jammer to be able to alternate between frequencies, modulations and spread spectrum techniques in order to apply protocol-aware jamming. This kind of adaptable radio can be implemented using software defined radio (SDR) with the benefit of using a single RF front end for all different configurations that are required for jamming the different UAV systems.

This thesis is organized as follows. Chapter 1 states the problem studied in this thesis and highlights related works. In Chapter 2 the spread spectrum concepts and the considered jamming techniques are introduced. Simulations to analyze efficiencies of different jamming techniques are covered in Chapter 3. Chapter 4 describes the developed jamming subsystem and presents the measured efficiencies of different jammers (including the developed subsystem) against several UAV remote control systems. Finally conclusions are provided in Chapter 5.

1.1 Problem Statement

As stated in the introduction, this thesis is part of a project which aims to create a portable cognitive radio system for detecting and neutralizing rogue UAVs. The detection and the neutralization are based on inspecting and manipulating the RF spectrum. The system targets UAVs which are operating in the 2.4 GHz industrial, scientific, and medical radio (ISM) band because of the wide usage of this band by commercially available and hobbyist UAVs [3]. When the system is functional at the 2.4 GHz ISM band then it can be extended to work in other bands, but that is out of the scope of this project.

The 2.4 GHz ISM band is not only popular in UAV remote control systems, but it is also used for Bluetooth, wireless local area networks, ZigBee, audio and video broadcasts and other remote controls. Thus, it would be beneficial for the system proposed in this thesis to minimize the impact on the performance of other communication systems or regulated UAVs operating in this band. This limits the set of jamming techniques which can be used for jamming UAVs not only based on efficiency but also taking into account how much the jamming technique affects other communication systems. Barrage and sweep jamming

techniques for example have less selectivity than protocol-aware jamming. That means that the barrage and sweep jamming techniques compared to the protocol-aware jamming technique are more likely to affect other than the targeted communication systems.

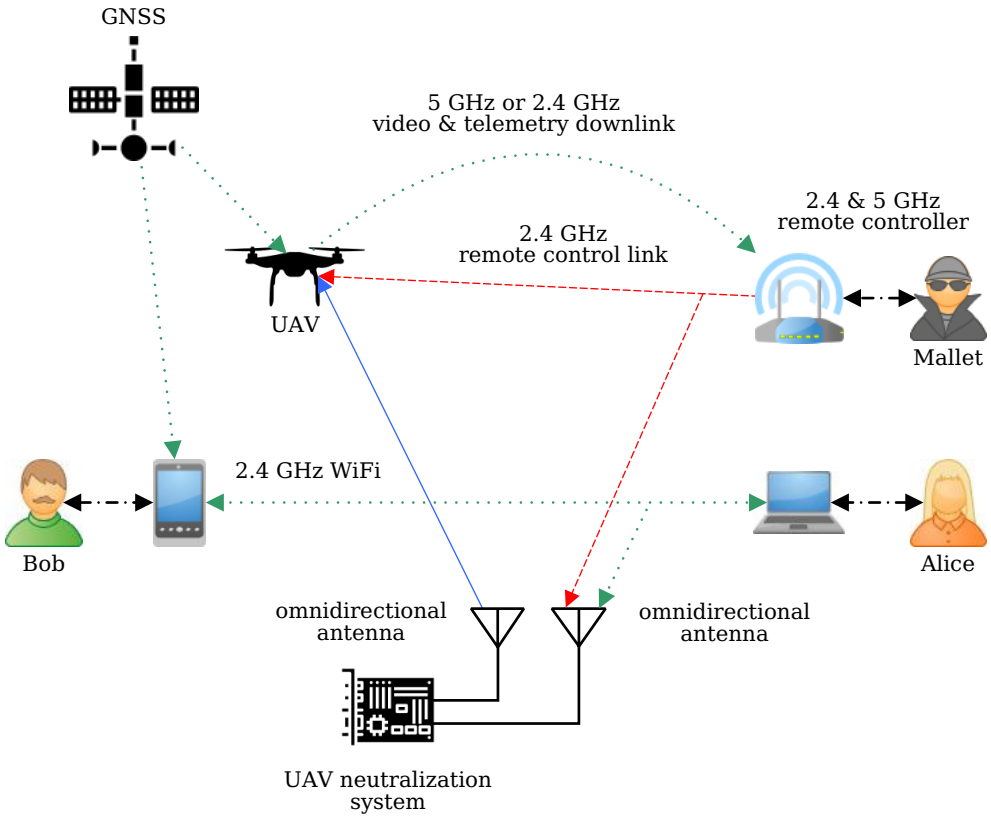

Figure 1. Scope of the project for detecting and neutralizing UAVs. The UAV remote control signal targeted for detection is shown with a dashed line. The jamming signal used for neutralizing the UAV is shown with a solid line. The signals which are not considered or should not be disturbed are shown with dotted lines.

Figure 1 illustrates the usage scenario of the detection and neutralization system. The targeted signal (the UAV remote control signal) is shown with a dashed line in red, the jamming signal is shown with a solid line in blue and the signals which are not considered or should not be disturbed are shown with dotted lines in green. The proposed system is protocol-aware in the sense that it will not be affected by signals other than the remote control signals of UAVs and reactive in the sense that the jamming will start only when the malicious remote control signal is detected. The protocol-aware detection is achieved by searching for known UAV remote control signals in the RF spectrum.

As mentioned in the introduction, some UAVs can fly a preprogrammed route using GNSS signals such as the Global Positioning System (GPS), Global Navigation Satellite System (GLONASS), Galileo or BeiDou. GNSS jamming and anti-jamming have been widely researched (a good overview is presented by G. Gao et al. in [4]) and integrating these jamming capabilities into this system is left as future work. Furthermore, the system

proposed in this thesis does not try to detect or neutralize the video feedback or telemetry info which can be possibly transmitted from the UAV. Detecting or interfering with the signals transmitted from the UAV would be useful in some cases, for example to determine the direction of the UAV or stop the UAV operator from receiving the video feedback. These are also prospective future additions to the system, but the initial goal is to restrict remote controlling of the UAV.

This project has been divided into two parts, separating it into detection and neutralization subsystems and it is the aim of this thesis to deal with the neutralization part by means of designing and implementing an universal jammer targeting UAV remote control signals. Protocol-aware jamming technique is chosen based on its efficiency, low detection probability and low interference caused to other communication systems. In order to apply protocol-aware jamming against different UAV remote control systems the underlying jammer architecture needs to be configurable, this is achieved by implementing the jammer on an SDR platform. Furthermore, the protocol-aware jammer is implemented in a way which allows it to be used for remote control takeover.

1.2 Related Works

Multiple commercial systems exist for detecting and jamming UAVs and several different approaches have been used for UAV detection. However, the literature discussing the neutralization of the remote control links of UAVs is not very vast. One of the possibilities for detection of UAVs is to use active radars and then analyze some parameters, for example the micro-Doppler feedback from the flying objects. The micro-Doppler effect is the result of radar signals being affected in special manner by micro-motion dynamics, such as the UAVs rotating propellers [5]. In this way the small rotors of an UAV can be detected, indicating that the flying object is an UAV and not something else [6, 7]. Instead of active radars, RF spectrum analyzers can also be used for detection [3, 8]. Usage of SDR for detecting UAVs which use frequency hopping has been researched and a general scheme to extract the hopping sequences of UAV communication systems has been proposed in [9] without considering the neutralization of UAVs.

The jamming effectiveness of commercially available low-cost jammers against UAVs has been studied in [10]. Due to the lack of specifically UAV targeted low-cost jammers, the effectiveness of generic jammers working in the 2.4 GHz ISM band was studied. It is concluded that jamming of the GNSS signal can be achieved from sufficient distance (couple hundred meters from the UAV). In comparison, jamming of the remote control signals with the studied jammers is not even effective when the jammer is much more closer to the UAV than the remote control. This study only reflects the performance of low-cost generic jammers against UAVs, but it emphasizes that the simplest jamming

techniques are not so effective in jamming UAVs and motivates the implementation of a specifically UAV targeted jammer that can apply protocol-aware jamming.

In [11] a reactive detection and jamming framework built on an SDR platform is introduced for detecting and jamming WiFi and WiMAX networks. In this framework, the RF spectrum is scanned for the targeted signals and jamming is done reactively. The framework can separate the WiFi and the WiMAX signals and only jam the targeted network. All of the digital signal processing (DSP) components of this system are implemented in a field-programmable gate array (FPGA) which resides on the SDR platform. The system presented in this thesis is similar to the framework presented in [11]. Both systems are developed on an SDR platform and the DSP components are implemented in a FPGA. However, the system presented in this thesis is aimed at detecting UAVs instead of WiFi or WiMAX networks. Furthermore, it features a flexible protocol-aware jammer which can be used to transmit arbitrary data with different modulation types and use direct-sequencing and frequency-hopping spread spectrum techniques.

Another approach to neutralizing UAVs is by taking over the remote control of the UAV. Taking over an UAV can help avoid unpredictable behavior by the UAV as compared to jamming the UAV. These kinds of works have been presented at recent security conferences in 2016. At Positive Hacking Days conference, a drone takeover competition was held [12] and at PacSec conference a system capable of taking over the remote control of drones which use the DSMx remote control protocol was presented [13]. In either case, a ready-made transceiver very much similar to the UAV's transceiver was used. The transceiver's capabilities in this approach limit the range of different UAVs which can be targeted. The subsystem proposed in this thesis is similar to the works in [12, 13], but it aims to be more versatile and capable of jamming or taking over different UAVs. The versatility is achieved by implementing the system on an SDR platform instead of using a particular transceiver. Flexibility provided by the SDR implementation allows it to use different modulation types, data rates and spread spectrum techniques.

Taking over an UAV that is using a preprogrammed flight route has been demonstrated in [14]. UAVs with preprogrammed flight routes rely on the GNSS for positional information and by spoofing the GNSS signals the UAV can be misdirected. This approach is less dependent on the type of the targeted UAV since all UAVs are restricted to the few available GNSS systems. Spoofing or jamming the GNSS signals still allows the UAV to be remotely controlled and the system introduced in this thesis focuses on limiting the ability to remotely control UAVs.

2 Background

This section gives an overview of the concepts and techniques which are used and targeted in this thesis. Firstly, spread spectrum techniques are introduced and their antijam capabilities explained. Follows an overview of jamming techniques which can be used when targeting spread spectrum systems and specifically UAVs.

2.1 Spread Spectrum

Commercially available UAVs use spread spectrum techniques to reduce interference from noise, jamming and other UAVs operating in the vicinity. Development of spread spectrum techniques started in the 1940's during the race for secure communications to increase resistance to jamming and prevent detection [15]. The increase in resistance to jamming and detection prevention is achieved by transmitting a signal which occupies bandwidth in excess of the minimum bandwidth necessary to send the data [16] (as illustrated in Figure 2). Spreading of the bandwidth is accomplished by means of a pseudo noise (PN) code which is independent of the data and can be replicated at the receiver for despreading and subsequent data recovery. The spread spectrum techniques considered here are frequency-hopping spread spectrum (FHSS) and direct-sequence spread spectrum (DSSS).

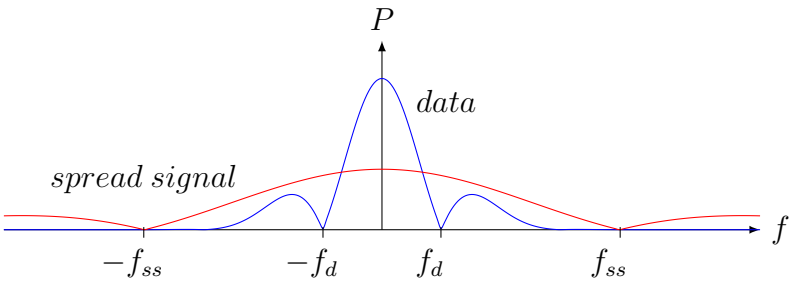

Figure 2. Power spectrum of data and of spread signal.

2.1.1 Processing Gain

Spread spectrum communication systems benefit from the wider bandwidth occupied by the modulated signal compared to the data signal. This bandwidth expansion, which characterizes the communication system's resistance to interference, is usually referred to as processing gain [2]. The processing gain (G_p) of a spread spectrum communication system is defined by the ratio of the bandwidth of the modulated signal to the bandwidth

of the data signal (Equation 1). The underlying principle of the processing gain is that by distributing a relatively narrowband data signal in a wider band forces a jammer with a fixed amount of total power to either spread that fixed power over all of the wide band, thereby inducing just a little interference in each subsection, or else place all of the power into a small subsection, leaving the remainder of the band interference free [16].

$$G_p = \frac{B_{ss}}{B_d} \tag{1}$$

For example the GPS, which encodes signals using unique code division multiple access technique, has data bandwidth of 50 Hz and modulated signal bandwidth of 1.023 MHz [17]. Therefore yielding a processing gain of 1.023 * 10^6 / 50 = 20460, or in decibels 10*$\log_{10}$(20460) = 43 dB.

It could be expected that the interference which can be successfully rejected is equal to the processing gain, but that is not entirely so. The level of interference that a system is able to accept and still maintain a specified level of performance is called jamming margin, and for direct-sequence and frequency-hopping spread spectrum systems with identical processing gain the jamming margins are quite different. The processing gain of a system will always be greater than its jamming margin.

The jamming margin is defined as in Equation 2, where G_p is the processing gain (dB), L_{system} is the system implementation loss (dB) and SNR_{min} (dB) is the minimum required output signal-to-noise ratio (SNR). The system implementation loss is a consequence of imperfect synchronization at the receiver, imperfect correlation of the received waveform and the spreading sequence and so on. All modulated signals require a minimum output SNR in order to perform to a certain level [18].

$$M_j = G_p - [L_{system} + SNR_{min}] \tag{2}$$

For example, a spread spectrum system with a 43 dB processing gain, a minimum required output SNR of 14 dB and system implementation loss of 4 dB would have a jamming margin of 43 - (4+14) = 25 dB. This system could not be expected to perform in an environment with interference more than 25 dB above the desired signal.

2.1.2 Frequency-Hopping Spread Spectrum

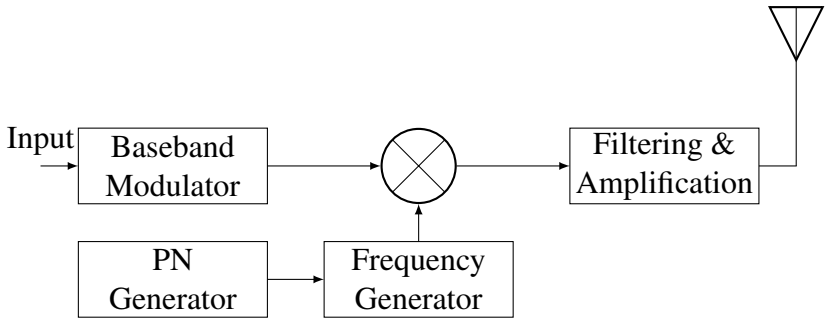

Figure 3. Generic frequency-hopping spread spectrum transmitter.

In FHSS communication systems the data signal is modulated onto a carrier signal and the frequency of the carrier signal is changed periodically (Figure 3), which helps the system avoid narrowband interference [19]. FHSS is divided into fast frequency hopping and slow frequency hopping based on the amount of data bits sent per frequency hop. For both types of FHSS communication systems the processing gain is defined by the ratio of the total bandwidth of all the channels to the bandwidth of a single channel [18], that is by the number of channels N_c with width B_d in B_{ss} (Equation 3).

$$G_p = \frac{B_{ss}}{B_d} = N_c \tag{3}$$

Jamming margin for FHSS systems is not clearly defined, because for FHSS systems interference with demodulation occurs only when the interferer is within the current channel. Interference in one channel though has no effect on the other channels as long as channel filters have sufficient selectivity. The throughput of an FHSS system goes to zero only when the jamming signal is present on all channels. This differs from DSSS, where a single interferer with enough power can reduce the throughput to zero [20].

2.1.3 Direct-Sequence Spread Spectrum

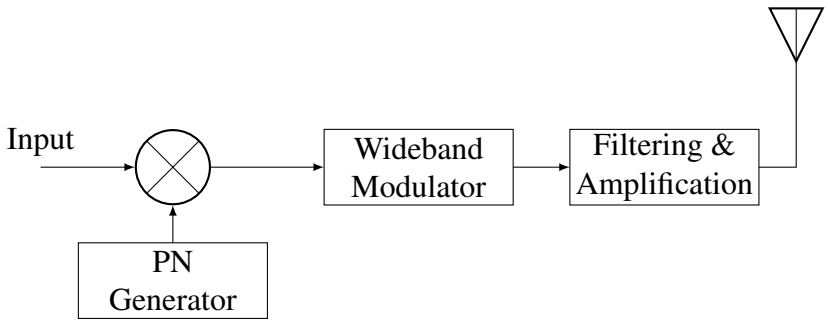

Figure 4. Generic direct-sequence spread spectrum transmitter.

In DSSS communication systems the data signal is multiplied with a PN code (Figure 4), which has a higher rate than the data signal. A faster signal results in greater spectrum width and the multiplied signal has the same bandwidth as the PN signal used for coding [2]. For DSSS communication systems the processing gain is defined by the ratio of the bandwidth of the PN signal to the bandwidth of the data signal [18], that is by the number of PN bits to data bits (Equation 4).

$$G_p = \frac{B_{ss}}{B_d} = \frac{T_b}{T_c} = N_c \tag{4}$$

The jamming margin of a DSSS system is at least the difference between the processing gain and the the minimum SNR at the information output and further decreased by the possible implementation losses in the DSSS system. For example, in a DSSS system using binary phase-shift keying (BPSK) modulation and Barker 11 spreading code [21] the processing gain is $10*\log_{10}(11)$ = 10.4 dB. With required probability of error of at least 10^{-3}, the minimum SNR at the information output is 4 dB [18]. Assuming no implementation loss, the jamming margin is 10.4 - 4 = 6.4 dB.

2.2 Jamming Techniques

This subsection gives an overview of jamming techniques that could be used against antijam (AJ) targets which have been developed to facilitate communications in presence of intentional jamming. The coverage is not all-inclusive, but the most common approaches are introduced. Classification of the jamming techniques is based on the works of Poisel [2], Lichtman et al. [22] and Grover et al. [23]. Each of the presented techniques has its own advantages and disadvantages which requires the particular targets to be considered when choosing the optimal method.

Performance of communication systems needs to be measured to compare efficiencies of different jamming techniques against these systems. In this thesis the bit error rate (BER), sometimes referred to as the probability of an error occurring in a bit (P_e), is used to characterize the performance of digital communication systems. Jammers attempt to raise the BER to 10^{-1} or higher to successfully jam AJ targets [2]. BER is a function of the SNR at the receiver RF input. SNR itself is defined as a function of signal and noise power (Equation 5). The goal of a jammer is to increase the noise level at the target receiver, therefore decreasing the SNR. Jammer's performance is determined by the jam-to-signal ratio (JSR) at the receiver, that is by the power of the jamming signal compared to the power of the signal which is jammed at the receiver. JSR can be viewed as reciprocal of SNR with the addition of jamming signal to the existing noise, as shown in Equation 6.

$$SNR_{dB} = 10 * log_{10}\left(\frac{P_{signal}}{P_{noise}}\right) \tag{5}$$

$$JSR_{dB} = 10 * log_{10}\left(\frac{P_{jammer} + P_{noise}}{P_{signal}}\right) \tag{6}$$

JSR in this thesis implicitly refers to the signal levels at the target receiver while the effective radiated power is not considered. That is to say that we are not analyzing the effects that the channel can have on the signals and we are working with a simplified model in which all signals reach the target receiver unchanged. Digital communication system jamming is simulated in Chapter 3 to compare the performance of different jamming techniques. Figure 5 illustrates a channelized spectrum such as the spectrum of a frequency-hopping system. Four commonly used jamming techniques, which are considered in this thesis, are illustrated in Figure 6 and further described in the next paragraphs.

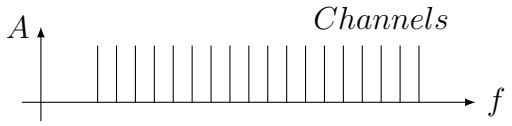

Figure 5. Channelized spectrum.

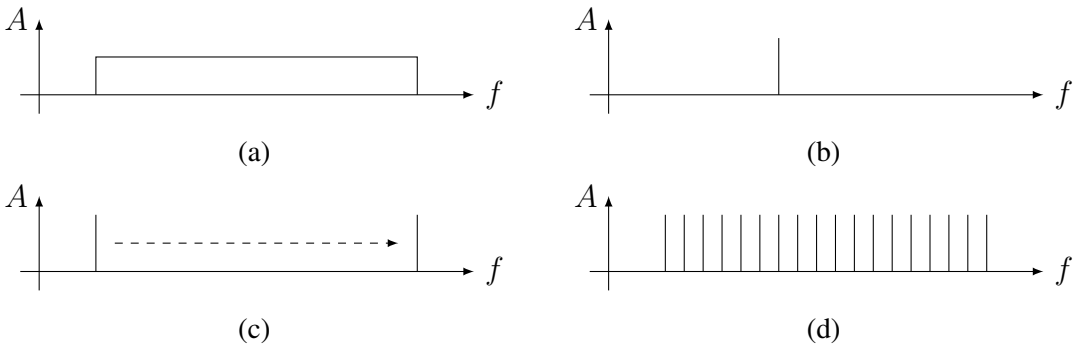

Figure 6. Four jamming techniques considered in this thesis based on a channelized spectrum are (a) barrage jamming, (b) tone jamming, (c) sweep jamming and (d) protocol-aware jamming.

2.2.1 Barrage Jamming

Barrage jamming is the simplest form of jamming and is usually defined as a jammer which transmits noise-like energy across the entire portion of spectrum occupied by the target with 100% duty cycle in time (shown in Figure 6a). It essentially raises the noise level at the receiver, making it more difficult for the communication system to operate. Barrage jamming directly affects the channel capacity of a communication system. The

channel capacity was first studied by Shannon in 1948 with regard to Gaussian noise [24]. Shannon derived the maximum data rate for a channel so that the error rate will be infinitesimal. If for the given channel a higher data rate is used then errors are assured to be present in the received signal. The capacity of a channel which is subject to additive white Gaussian noise (AWGN) is given by

$$C = B * log_2\left(1 + \frac{S}{N}\right) \tag{7}$$

where B is the bandwidth of the channel, S is the average power of the signal and N is the total average of noise present in the system. Incidentally, as the AWGN level is intentionally raised in the channel the SNR decreases altogether with the channel capacity.

Barrage jamming has been shown game-theoretically and information-theoretically to be the best a jammer can do in the absence of any knowledge of the target signal [25]. It is recognized that complete jamming of wireless networks can be realized by generating a continuous noise with sufficient power. On the downside, this approach has high energy requirements, high probability of detection and no way of selecting which signals to jam in the used RF band. Resistance to barrage jamming is further improved by spread spectrum techniques, against which barrage jamming is relatively inefficient until the jamming margin is overcome as will be shown in Subsection 3.2.

2.2.2 Tone Jamming

A tone jammer uses one or more strategically placed jammer tones. Tone placement and the number of tones affects the performance of the jammer. Monotone jamming is illustrated in Figure 6b. For multitone jamming, the jammer power is distributed among several tones. The tone jamming signal is given by

$$J(t) = \sqrt{\frac{2P_J}{N_J}} \sum_{i=1}^{N_j} \cos(2\pi f_i t + \phi_i) \tag{8}$$

where P_J is the jamming power, N_J is the number of jamming tones, f_i is the frequency of the i-th jamming tone, ϕ_i is the phase difference between the i-th jamming tone and the carrier of the hopping frequency slot [26].

Monotone jamming has been shown to be unsuccessful in jamming FHSS systems [2]. This is also the case in jamming UAVs, which typically have quite a lot of redundancy in the sense that the state of the remote control is constantly transmitted over different

channels much faster than humans can react to visual stimulus. Therefore, if one of the channels is unavailable then the responsiveness of the UAV will not degrade noticeably. However, it can be useful, for example against communication systems using DSSS by overcoming the processing gain of such systems at the receiver. Multitone jamming technique is not effective against FHSS systems either unless enough channels are successfully jammed. But multitone jamming could also be used against DSSS communication systems, in which case the jammer tone placements are very important [2].

Tone jamming exhibits similar disadvantages compared to barrage jamming when targeting spread spectrum systems. For tone jamming to work against spread spectrum systems it needs to overcome the jamming margin and therefore has high energy requirements and a high probability of detection.

2.2.3 Sweep Jamming

Sweep jamming is a combination of barrage and tone jamming. With sweep jamming, a relatively narrowband signal is swept in time across the targeted frequency band (shown in Figure 6c). The sweeping signal is usually referred to as chirp signal. Similarly to tone jamming, only a portion of the spectrum is being jammed at any instant in time. However, since the signal is swept, a broad range of frequencies can be jammed in a time period. The chirp signal used for sweep jamming is given by

$$\begin{aligned} J(t) &= P_J \cos(2\pi f(t)t + \phi) \\ f(t) &= f_0 + kt,\ k = \frac{f_1 - f_0}{T_{sweep}} \end{aligned} \tag{9}$$

where P_J is the jamming power, $f(t)$ is the instantaneous frequency, f_0 is the initial frequency of the cirp signal, f_1 is the stop frequency of the cirp signal, T_{sweep} is the time period with which the frequency range is covered.

The net effect of such a jamming strategy viewed over a time period is similar to a barrage jammer. It is also possible to sectorize the jamming strategy and avoid jamming certain bands which might be necessary from the jammer's point of view. This is true only when the timing is tailored to the target receivers so that the jamming signal is present at the receiver for an adequate time. It has been shown that BPSK modulation has the best performance compared to other modulation types when jammed with a sweeping signal [27]. In Chapter 3 the performance of spread spectrum systems when jammed with a sweeping signal will be simulated and shown that the characteristics of the spread spectrum system must be taken into consideration for sweep jamming to be effective.

Performance of IEEE 802.11 based wireless local area network devices has been studied under various jamming signals in [28] and rather surprisingly the sweeping jammer at certain sweeping rates is quite effective. That would be a downside considering that the UAV jammer proposed in this thesis should not disturb other communication systems and that the IEEE 802.11 based wireless local area network typically uses the 2.4 GHz ISM band.

2.2.4 Protocol-Aware Jamming

The last jamming technique presented is protocol-aware jamming, with which the parameters of the targeted signal are taken into consideration while constructing the jamming signal (as illustrated in Figure 6d). The parameters which are considered include the modulation type, the data rate and the channel bandwidth. Furthermore, if FHSS is used then the channel frequencies, hopping patterns and hopping rate must be known. If DSSS is used then the PN code used for spreading and the spreading rate must be known. The ability to synchronize the jamming waveform with the target signal is also required in protocol-aware jamming. This problem is exacerbated by the flight time of the target and jamming signals, which is difficult to predict.

The feasibility of using protocol-aware jamming has been so far mostly studied on IEEE 802.11 based wireless local area network communication systems and it has been concluded that protocol-aware jamming can achieve effective jamming with very low energy requirements and low probability of detection of the jamming signal [29, 30]. Protocol-aware jamming also possibly prevents jamming of other communication systems operating in the same RF band because the protocol-aware jamming signal is only in the portions of the band which are used by the targeted signal.

2.2.5 Observations

The above jamming techniques were presented in order of implementation difficulty. Barrage, tone and sweep jamming techniques are considerably easier to apply than the protocol-aware jamming technique which requires more knowledge about the targeted signal. On the other hand, the protocol-aware jamming approach offers better efficiency, less interference to other communication systems and lower probability of detection than the other considered techniques.

3 Simulations of Jamming Techniques

In this section the efficiency of barrage, tone, sweep and protocol-aware jamming on a hybrid spread spectrum communication system is evaluated by means of simulations. The hybrid spread spectrum system is a combination of frequency-hopping and direct-sequence spreading. It has been shown, as discussed in previous sections, that the protocol-aware jamming technique which is the most difficult to implement, is the most efficient jamming technique against spread spectrum communication systems. It is the aim of this section to study the feasibility and expected efficiency of using protocol-aware jamming when targeting spread spectrum systems which are used by UAVs. Comparison with other jamming techniques is done to find the anticipated increase in efficiency.

3.1 Hybrid Spread Spectrum System Model

The hybrid spread spectrum communication system model which is simulated in this section is based on the typical characteristics and specifications of UAVs available on the market today as reported in [3] and verified by inspecting the RF characteristics of several UAV platforms. The hybrid model uses 40 channels with 2 MHz channel spacing and hop rate of 375 hops per second. The channel usage is uniformly distributed and no effort is made to avoid the channels with higher interference. Data rate is 150 kbps and the data is spread with an 11 element long code resulting in signal with 1.65 Mbps rate. The resulting signal is modulated using continuous phase binary frequency-shift keying (FSK) with 500 kHz deviation from the carrier frequency.

The described hybrid spread spectrum system model has considerable processing gain. From the direct-sequence aspect, with every bit being spread by an 11 element code, the processing gain is $10*\log_{10}(11) = 10.4$ dB. Furthermore, frequency-hopping spreads the signal between 40 channels which could be expected to result in processing gain of $10*\log_{10}(40) = 16$ dB. The hybrid processing gain is therefore $10*\log_{10}(11*40) = 26$ dB.

A Simulink model of the described hybrid spread spectrum communication system was developed as shown in Figure 7. The methods described in [31] were followed to construct the Simulink model. The model is divided into five subsystems: the transmitter, the channel, the receiver, the spread spectrum code generator and the error rate calculator. In each of the following subsections a jamming subsystem will be added into the signal path to study its effect on the receiver.

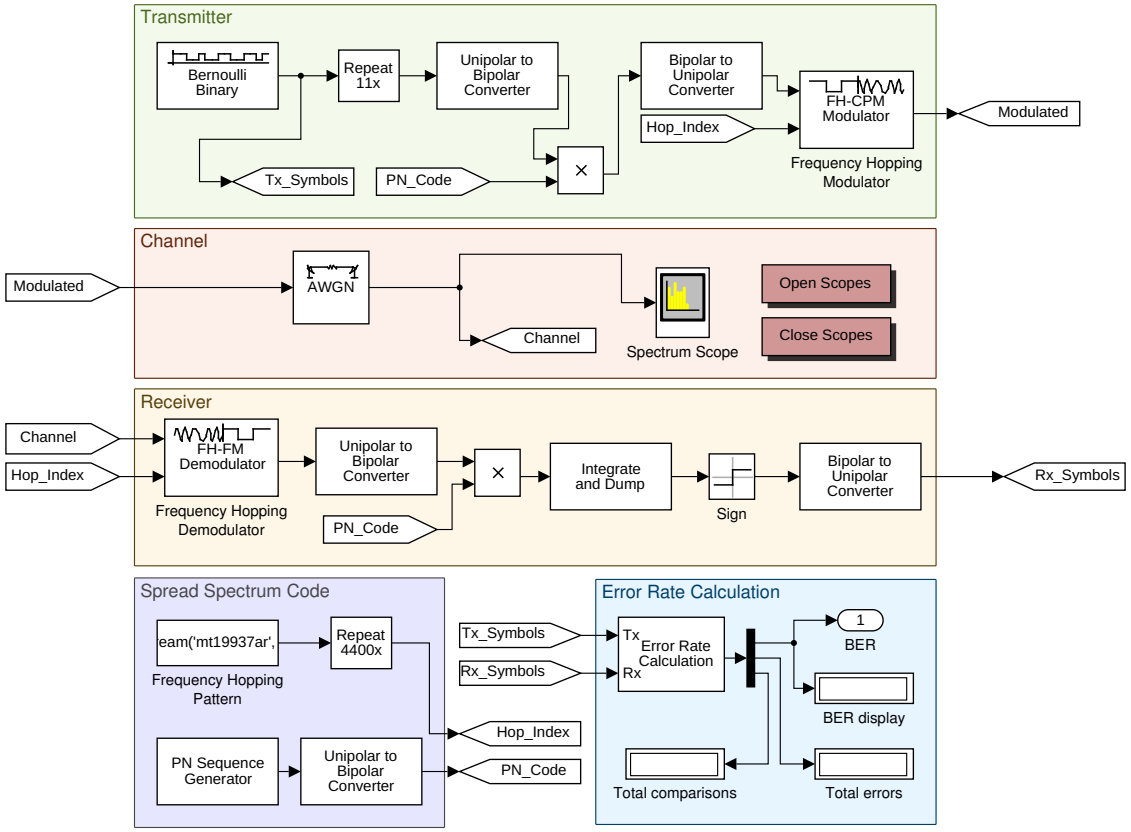

Figure 7. Developed hybrid spread spectrum digital communication system model in Simulink.

In the transmitter subsystem the data to be transmitted is randomly generated using a Bernoulli Binary generator block. The data is uniformly distributed and its sample rate is increased to match the sample rate of the spreading code. Conversion between unipolar and bipolar signal types is used to avoid multiplying with zero since the unipolar signal type stores values 0 and 1, the bipolar signal type however stores values -1 and 1. The spread signal is modulated using a frequency hopping modulator. The internal architecture of the frequency hopping modulator is shown in Figure 8. The data to be transmitted is first modulated and then the baseband signal is multiplied with a carrier signal to use the specified channel.

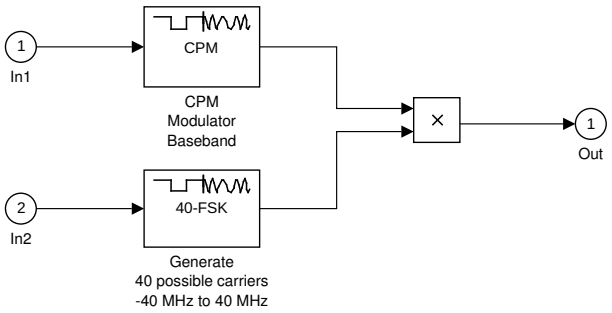

Figure 8. Developed frequency hopping FSK modulator model in Simulink.

The Simulink model of the demodulator block, which is used in the receiver subsystem, is shown in Figure 9. The received signal is downconverted to baseband from the used channel, then the baseband signal is filtered to reduce interference. Finally the downconverted and filtered baseband signal is demodulated.

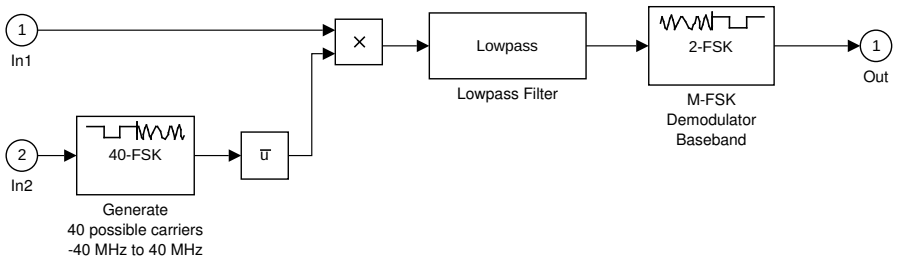

Figure 9. Developed frequency hopping FSK demodulator model in Simulink.

The channel subsystem adds white Gaussian noise to the modulated signal. The variance of the noise generated by the AWGN channel block is specified in SNR calculation. That is, it calculates the variance from SNR and input signal power quantities which are defined as *MATLAB* variables in the model workspace. At the receiver subsystem, the received signal is demodulated and the spreading is removed using the known hopping pattern and PN code. Both, the hopping pattern and the PN code, are generated in the spread spectrum subsystem. The last subsystem is the error rate calculation part, which calculates the error rate as a running statistic by dividing the total number of unequal pairs of transmitted and received data bits by the total number of transmitted data bits.

3.2 Barrage Jamming

As described previously in Subsection 2.2.1, barrage jamming directly affects the channel capacity of a communication system. Barrage jamming is effectively decreasing the SNR of the system and with that the channel capacity is decreasing. Barrage jamming simulations against the hybrid spread spectrum model described in Subsection 3.1 were done with two different direct-sequencing code lengths used by the model to illustrate the effect that the length of the code has on the processing gain. The simulation results are plotted in Figure 10. Increasing the jam-to-signal ratio (JSR) at the receiver subsystem results in higher BER and it is evident that the longer direct-sequencing code provides better processing gain. This gives some insight to the antijam (AJ) characteristics of the hybrid spread spectrum system.

It is worth reiterating that complete jamming of wireless networks can be realized using barrage jammer with sufficient power, but its energy requirements are quite high and this technique has no mechanism for selecting which signals to jam. For spread spectrum

systems the jamming margin must be overcome, which in this case is below the processing gain of 26 dB. Exact jamming margin depends on the system implementation loss and as can be seen from the results the system is fully jammed at JSRs approaching the processing gain.

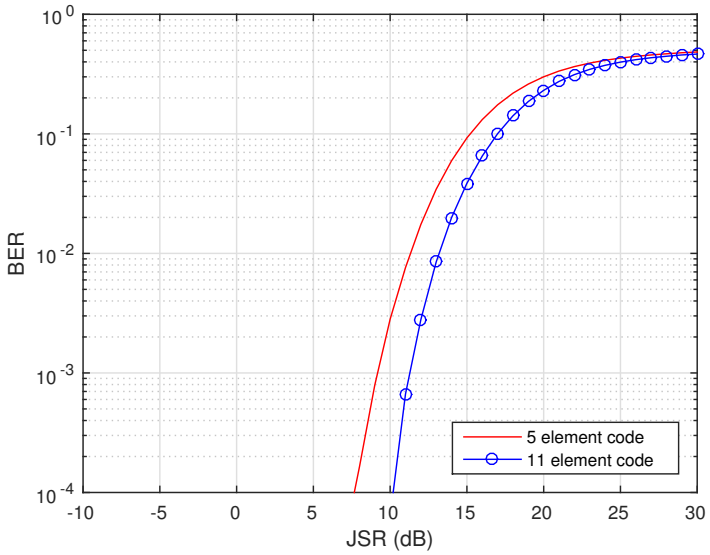

Figure 10. Barrage jammer performance against hybrid spread spectrum digital communication system for the model described in Subsection 3.1.

3.3 Tone Jamming

The developed tone jammer Simulink model is shown in Figure 11. It generates a single tone in one of the channels used by the hybrid spread spectrum system. Power of the jamming tone signal is set in the Signal Generator block. The jamming signal is added to the modulated signal from the transmitter subsystem and their combination is received at the receiver subsystem.

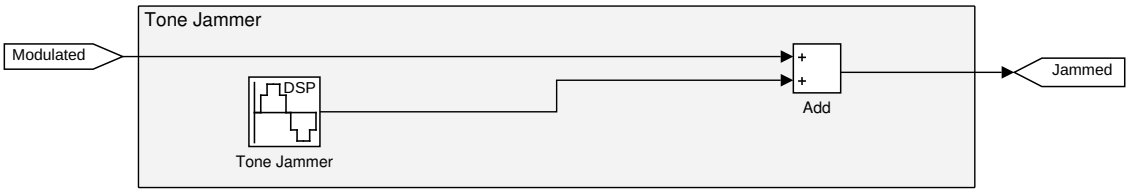

Figure 11. Developed tone jammer model in Simulink.

The simulation results of tone jamming the hybrid spread spectrum system are shown in Figure 12. The results indicate that while the tone is efficient in jamming a channel from certain JSR then the other channels remain free from the interference and the BER stays well below 10^{-1}.

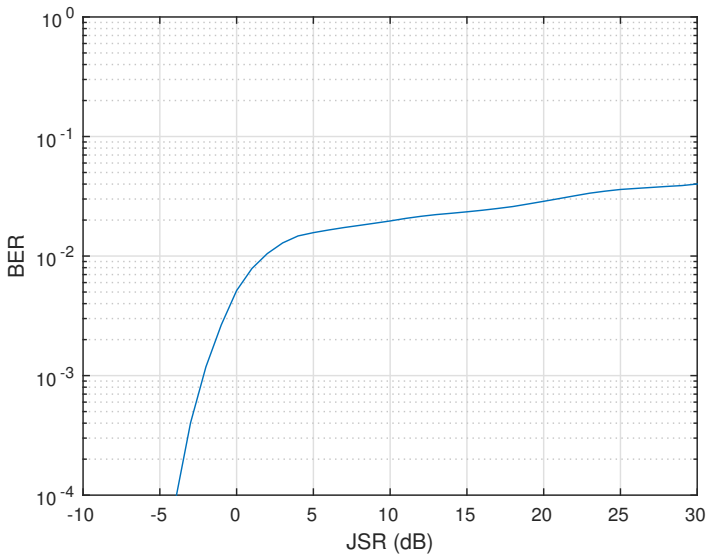

Figure 12. Tone jammer performance against hybrid spread spectrum digital communication system for the model described in Subsection 3.1.

3.4 Sweep Jamming

When considering sweep jamming, timing is one of the most important aspects. The jamming signal must be swept fast enough while covering the whole band, otherwise hops in the target signal will occur for which the jamming signal is not present. Then again, the jamming signal should not move too fast or insufficient portion of the hop will be jammed.

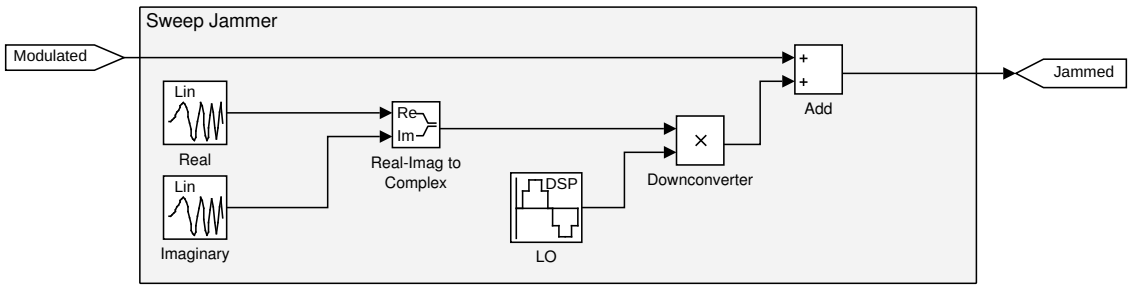

Figure 13. Developed sweep jammer model in Simulink.

The Simulink model used for generating the sweeping jamming signal is shown in Figure 13. Chirp blocks are used to generate a linearly sweeping signal. Because the Chirp block does not output complex values, only real values, two otherwise identical signals with a phase offset of $\pi/2$ are generated and input to the Real-Imag to Complex block to create a complex signal. This eliminates the negative frequencies. Sine Wave generator and multiplication are used to downconvert the sweeping signal to cover all the channels.

Given that the hybrid spread spectrum communication system described in Subsection 3.1 is sending data at 150 kpbs, 15000 bits must be jammed to produce a BER of 10^{-1} (aimed BER for successfully jamming AJ targets). With the hybrid communication system using 375 hops per second, each hop contains 400 bits. Therefore, at least 37.5 hops in every second must be jammed. Since these hops can be anywhere in the spectrum from the jammer's point of view, at least 37.5 sweeps per second are required.

Figure 14 shows the performance of the sweeping jammer deployed with different sweeping rates. Simulating with different sweeping rates revealed that the sweeping rate of 10 times the hopping rate was the most efficient. For comparison sweeping jammer's efficiency with sweeping rate of 1000 times the hopping rate is plotted. In either case the jammer sweeps in the full bandwidth used by the communication system. These results further emphasize that timing is important when sweep jamming a communication system that uses FHSS.

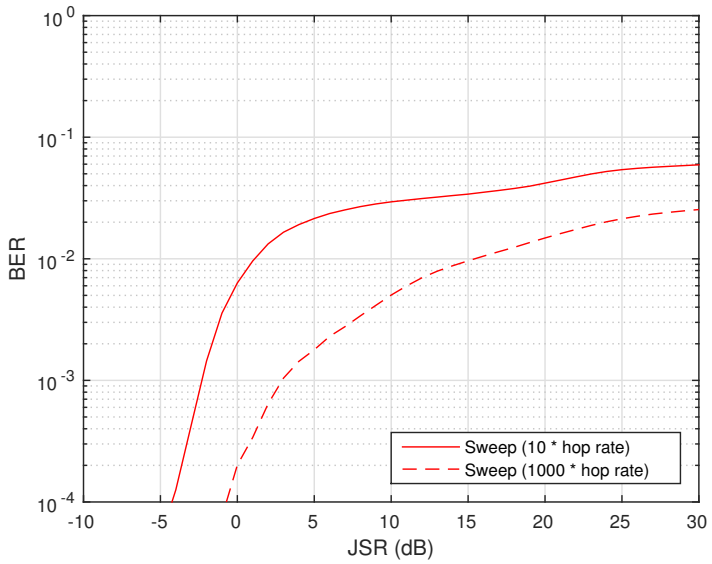

Figure 14. Sweep jammer performance against hybrid spread spectrum digital communication system for the model described in Subsection 3.1.

3.5 Protocol-Aware Jamming

For protocol-aware jamming simulations, a jamming signal similar to the targeted signal is generated. The jamming signal uses the same modulation type, the same data rate, the same direct-sequencing rate and the same frequency hopping pattern as the targeted signal. Simulink model of the jammer is shown in Figure 15. Similarly to the transmitter subsystem, a Bernoulli binary generator block is used to generate random data to be sent. Different seed is used for the pseudo random generator in this block to not use the same data as the transmitter does. Other than that, construction of the jamming signal is very

much similar to the construction of the transmitted signal. Amplification of the jamming signal is used to vary the JSR, the power is given in dBm.

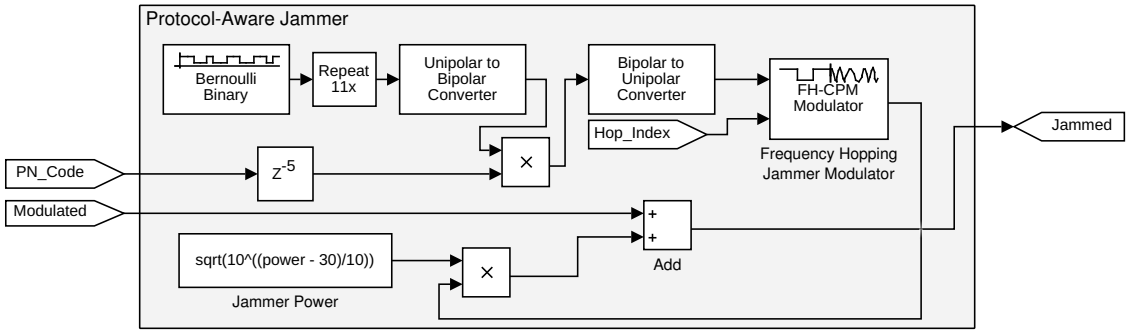

Figure 15. Developed protocol-aware jammer model in Simulink.

Results of the protocol-aware jammer against the hybrid spread spectrum communication system are shown in Figure 16. It can be seen that the protocol-aware jammer does not require high JSR to cause interference and can successfully jam all of the used channels.

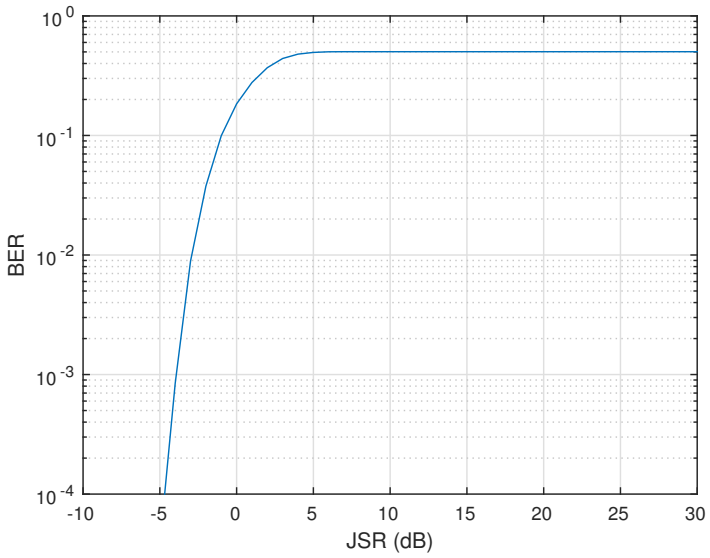

Figure 16. Protocol-aware jammer performance against hybrid spread spectrum digital communication system for the model described in Subsection 3.1.

3.6 Performance Comparison

The simulated efficiencies for the discussed jamming techniques against the hybrid spread spectrum system are plotted in Figure 17. Barrage jammer can achieve very high BERs with sufficient JSR, but it is not so useful when considering JSRs closer to zero. Also, barrage jammer lacks the ability to target specific communication systems in a RF band and can result in jamming other systems than the intended one.

Tone jammer can be very successful in jamming a single channel in a system which uses frequency-hopping. If the channel filters have poor selectivity, then also adjacent channels of the targeted channel can be interfered. It depends on the upper layers of the communication protocol how much the interference in one or a couple of channels affects the whole communication system. As discussed previously, the remote control systems for UAVs use the channels to continuously transmit the remote control state and depending on the channel count and hop rate, losing a single channel to interference might not cause problems in controlling the UAV.

Sweep jammer performance relies on its sweeping frequency and the width of the covered band. In the comparative plot, sweep jammer with sweeping rate 10 times the hopping rate of the hybrid spread spectrum system is used as this was found to be one of the most effective configurations (see Subsection 3.4). As can be seen from the comparative plot in Figure 17, sweep jammer achieves similar performance to the tone jammer in terms of the bit error rate. But, the sweep jammer is able to spread the errors among all of the channels, which can be much more desirable from the jammer point of view as this can make all of the channels unusable.

Protocol-aware jammer has the advantage of being able to jam all of the channels exactly at the time they are being used. That makes it efficient against frequency-hopping. Furthermore, using direct-sequence spreading similarly to the system which is jammed can result in higher efficiency compared to for example a single tone jammer. It can be concluded that protocol-aware jamming is the most efficient jamming technique of the simulated techniques against the hybrid spread spectrum system.

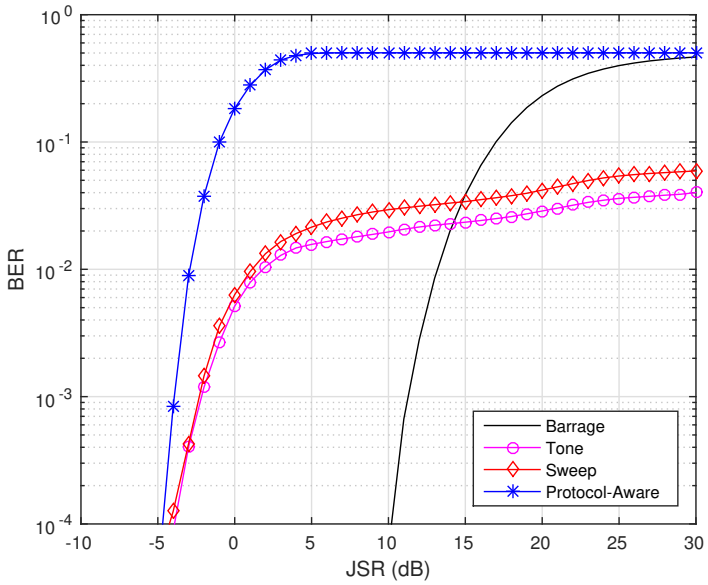

Figure 17. Comparison of the performances of different jamming techniques against the hybrid spread spectrum communication system model described in Subsection 3.1.

4 Protocol-Aware Jammer

In order to implement a protocol-aware jammer with the ability of configuring the different parameters of the jamming signal, SDR approach is used. BladeRF, an open source SDR platform, is used as the target architecture. Digital signal processing is implemented inside the FPGA to reduce system component requirements (that is a host computer) and allow for efficient, real-time processing of signals. Furthermore, controlling of the work flow and operation of the signal processing blocks is handled inside the soft core processor which runs in the FPGA concurrently to the signal processing algorithms. In this chapter, architecture of the BladeRF is described, followed by the protocol-aware jammer implementation description and experimental results.

4.1 Hardware

The UAV detection and jamming system is implemented using BladeRF, an SDR platform developed by Nuand. BladeRF with its main components highlighted is shown in Figure 18. It is based on the zero intermediate frequency (IF) architecture which is described in Appendix A. It can be used for creating Global System for Mobile Communications (GSM) access points with Yate Base Transceiver Station [32], spoofing GPS signals [33] and tracking aircrafts by decoding the ADS-B signals [34].

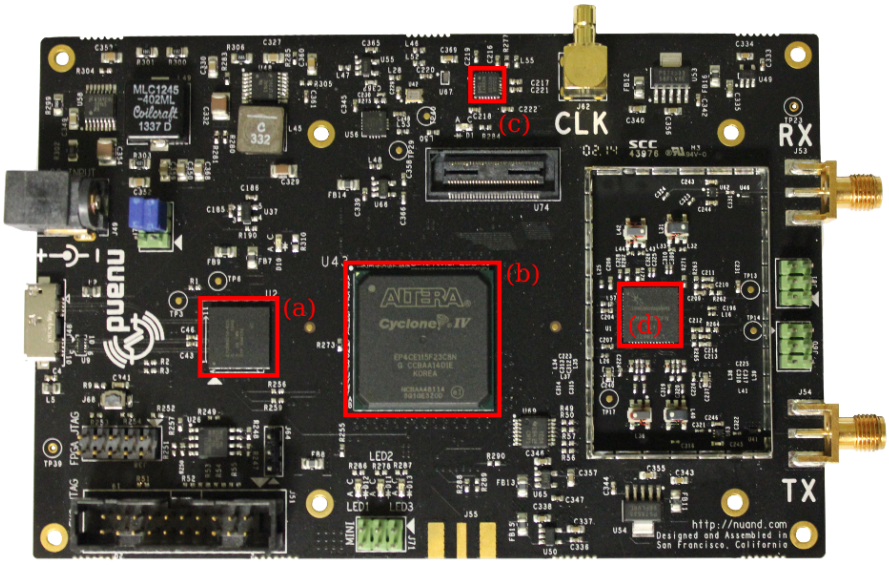

Figure 18. BladeRF with the main components highlighted (a): Cypress FX3 USB 3.0 Superspeed microcontroller; (b): Altera Cyclone IV E FPGA; (c): Si5338 programmable clock generator; (d): Lime Microsystems LMS6002D transceiver.

A more detailed description of the BladeRF hardware architecture is shown in Figure 19. BladeRF has separate paths for receiving and transmitting RF signals and can do so in full-duplex mode. Both analog to digital conversion and digital to analog conversion is carried out by the LMS6002D chip. It is a single chip RF transceiver based on zero IF architecture, covering 0.3 to 3.8 GHz frequency range and has up to 28 MHz instantaneous bandwidth [35].

The LMS6002D has 12 bit analog-to-digital converters (ADCs) and digital-to-analog converters (DACs), which are interfaced to Intel's Cyclone IV FPGA. Configuration of the LMS6002D is done from the FPGA via Serial Peripheral Interface bus (SPI). Optionally some DSP algorithms can be performed inside the FPGA, assuming they can fit in the remaining resources, otherwise the received IQ samples can be simply passed through it to the Cypress FX3 USB 3.0 microcontroller or the other way around for transmitted samples. Both the Cypress FX3 microcontroller and the Cyclone IV FPGA feature Joint Test Action Group (JTAG) debugging capabilities. Control data between the Cypress FX3 microcontroller and the Cyclone IV FPGA is exchanged via universal asynchronous receiver/transmitter (UART) interface.

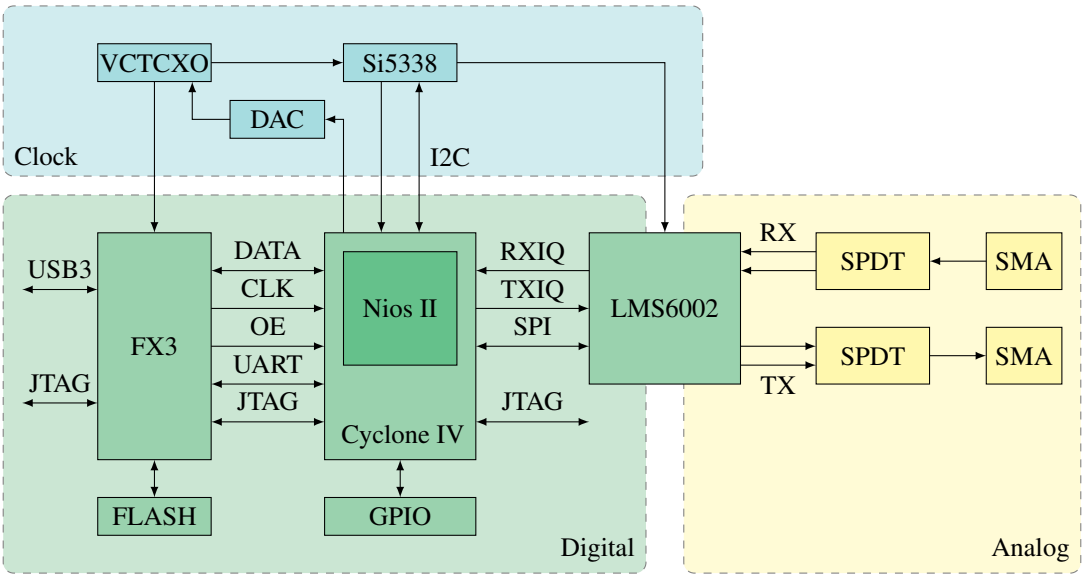

Figure 19. Block diagram of the BladeRF board.

Inside the FPGA is a synthesized Nios II soft core processor, which is essentially equivalent to a microcontroller [36]. It has a processing unit, memory and can have several different peripherals. The amount of memory and the exact peripherals can be configured. This flexibility is one of Nios II's main benefits which is exploited in this work. In BladeRF, the peripheral functionality (for example SPI and UART) inside the FPGA is provided by the Nios II. These peripherals have been configured for usage by Nuand and the configurations can be downloaded from the BladeRF source code repository.

4.2 Implementation

The detection and jamming subsystems are implemented entirely inside the FPGA and the Nios II soft core processor. Therefore the system does not require a connection to a host device (such as a computer or a mobile device) for IQ sample processing. In this system, the open source FPGA and Nios II configurations provided for BladeRF by Nuand have been taken as basis and improved on. The jamming subsystem's digital signal processing algorithms, encoding and baseband modulation, are implemented in hardware using VHSIC Hardware Description Language (VHDL). Control of the digital signal processing, sample rate and frequency hopping is implemented in the Nios II soft core processor using the C programming language. Block diagram of the architecture of the jamming subsystem is shown in Figure 20.

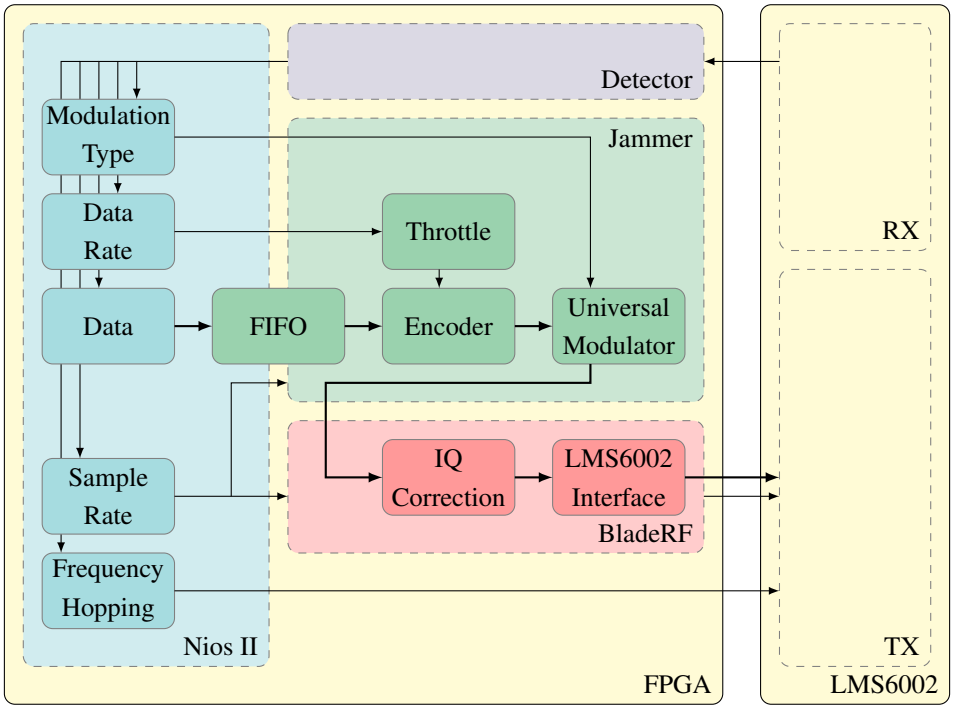

Figure 20. Architecture of the SDR based UAV jamming subsystem.

In general, the data flow moves from the receiving analog front end to the transmitting analog front end. When an UAV signal is detected the transmitter path is configured and then a signal is transmitted to disturb the reception of the detected signal at the UAV. Signal detection is done by the detector block in the FPGA and the jammer is notified via the Nios II processor. This allows the soft core processor to set the required modulation type, data to be sent, sample rate and the frequency hopping pattern. Figures 21 and 22 show the register-transfer level (RTL) view of the developed architecture described in Figure 20. In Figure 21 the connections between the Nios II and the jammer module are shown and in Figure 22 the signal path from the jammer to the LMS6002D is shown.

The data to be transmitted by the jammer module is sent from the control logic in Nios II using a first in, first out (FIFO) buffer. Intel provides FIFO functions through parameterizable single-clock FIFO and dual-clock FIFO intellectual property cores. A dual-clock FIFO intellectual property core was added to the Nios II processor and configured for usage with the jammer subsystem. The usage of a dual clock FIFO is required to provide safe clock domain crossing because the processor and the jammer FPGA implementation operate at different clock frequencies.

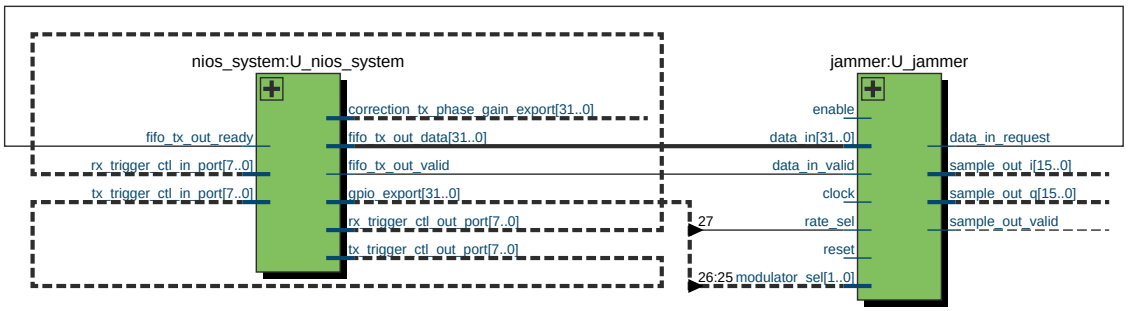

Figure 21. RTL view of the Nios II, the jammer and their connections.

The modulation type and data rate selections are done through the general-purpose input/output (GPIO) interface, which was configured for usage in the Nios II by the BladeRF developers. It is a 32-bit wide interface, which by default is used for enabling and resetting hardware modules. As it is not fully utilized in the default BladeRF configuration some of its outputs were used for configuring the jammer module. These outputs can be written to in the Nios II very similarly to how GPIO pins are written to in regular microcontrollers.

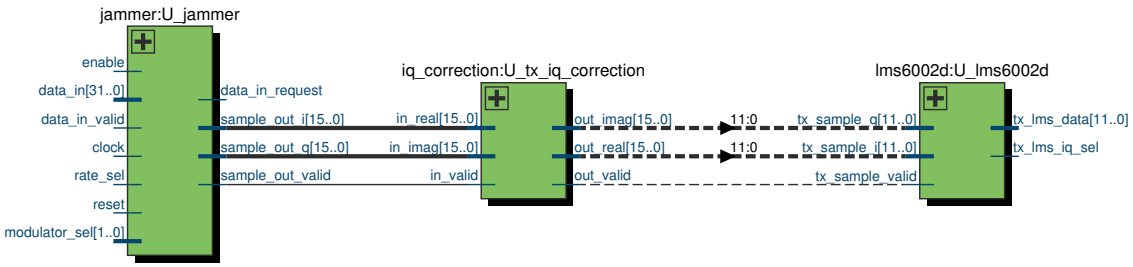

Figure 22. RTL view of the signal path from the jammer to the LMS6002D interface.

The jammer module generates IQ samples based on the input data and the jammer configuration and forwards the samples to the IQ correction block which was developed for the BladeRF by Nuand. The IQ correction block can be used for DC offset correction and IQ imbalance correction if necessary, but for the corrections to work the BladeRF requires calibration. A table-based automatic DC calibration is in the BladeRF codebase. However, the IQ imbalance needs to be done manually by adjusting IQ balance parameters.

From the IQ correction block the samples are output to the LMS6002D interface, which transmits the samples to the LMS6002D chip.

4.2.1 Control Logic

Figure 23 displays the flow of the control logic implemented in the Nios II soft core processor. After the RF front end is initialized, the jamming subsystem waits for the detection notification from the detection subsystem. Depending on the type of UAV which is detected, the parameters are loaded and the transmission with frequency hopping is started. A timeout is set for the transmission to allow the jamming subsystem to resynchronize to the targeted signal or stop jamming when the signal is lost.

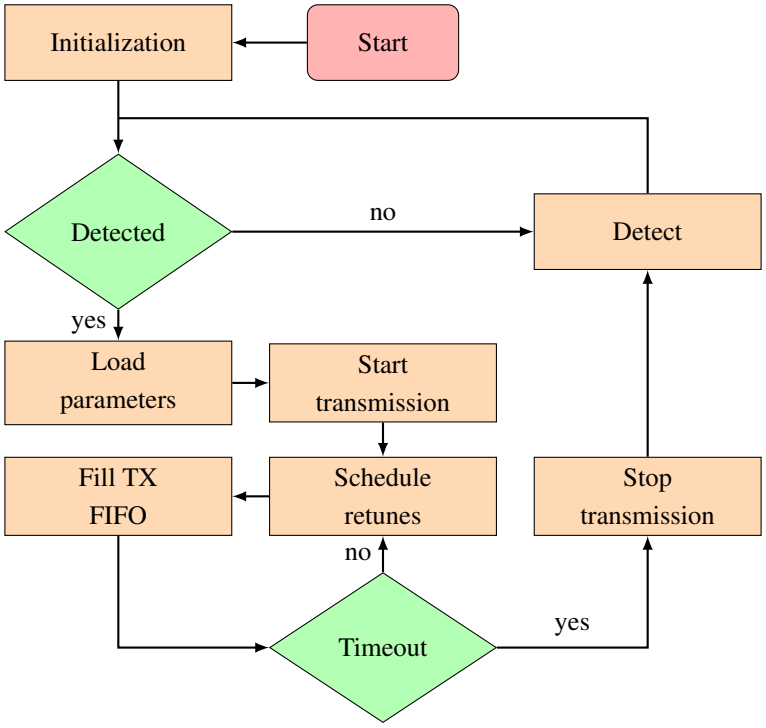

Figure 23. Flowchart of the control logic implemented in Nios II.

Frequency hopping is done by retuning the LMS6002D from the Nios II processor at every hop. To provide timing for frequency hopping, a timestamp counter module in the FPGA is used. This module increments at every clock cycle, with the cycle length dependent on the sample rate. In Nios II, a programmable interrupt is used to trigger a callback when the timestamp counter has reached the hop time. The code in Nios II allows multiple retune requests to be queued up, currently up to 32 requests. This allows the control logic to schedule multiple frequency hops in advance and does not require the frequency retune requests to be submitted shortly before the retune needs to take place.

Tuning the LMS6002D to a new frequency involves configuring a number of registers in the LMS6002D regarding its phase-locked loop (PLL). The variables corresponding to these registers are the frequency range selection, the integer and the fractional part of the PLL divider and the voltage controlled oscillator (VCO) capacitor selection. Based on the targeted frequency the frequency range can be easily selected and the integer and the fractional part of the PLL divider can be calculated. For the VCO capacitor selection however, a flexible algorithm is given in the LMS6002D programming and calibration guide [37]. The algorithm has been implemented by Nuand for BladeRF and it is partially limiting the maximum achievable frequency hopping rate.

Tuning to a random frequency using the aforementioned algorithm takes about $700\,\mu s$ [38]. This time can be shortened at each successive tuning to the same frequency if the previously described LMS6002D registers have been saved. By writing previously identified tuning parameters, including the VCO capacitor selection, directly to the LMS6002D registers the tuning can be achieved in under $250\,\mu s$ [38]. Listing 1 shows the developed code which runs in Nios II and retrieves the LMS6002D registers for all defined frequencies. This is done in the parameters loading step of the control logic after a certain UAV is detected and the used frequencies are known. There is a trade-off for this quicker tuning since the PLL and tuning parameters are sensitive to changes in the environment and therefore this can result in increased phase noise over time. This can be aided by occasionally refreshing the parameters and rerunning the VCO capacitor selection algorithm.

```
int hop_set_load_quick_tunes(bladerf_module m,
                struct hop_set *h)
{
    int status;
    size_t i;

    for (i = 0; i < h->count; i++) {
        status = lms_set_frequency(0, m, h->params[i].f);
        if (status != 0)
            return 1;

        status = lms_get_quick_tune(0, m, &h->params[i].qt);
        if (status != 0)
            return 2;
    }
    return 0;
}
```

Listing 1. Functionality for saving the LMS6002D register states for a set of frequencies in order to use quick tuning when changing back to those frequencies.

4.2.2 Digital Signal Processing

The digital signal processing blocks of the jammer are shown in Figure 24. The main blocks of the jammer are encoder, throttle, demultiplexer, clock divider and universal modulator blocks. The data to be transmitted is pulled from the dual clock FIFO buffer by the encoder block. The encoder block applies the PN code multiplication and acts as a parallel input serial output FIFO. It has an input width of 32 bits, therefore acquiring four bytes of data at each request, and an output width of 1 bit, outputting the remaining least significant bit of the encoded data at every request. The throttle block is used to control the data rate. It is essentially a configurable clock divider which controls the data flow from the encoder to the modulator. The demultiplexer directs the encoded bits to the appropriate input of the universal modulator based on the modulation type selection done in the Nios II processor. The clock divider is used to lower the sample rate by half. The *LMS6002D* component runs at half the sample rate of the jammer subsystem itself and the IQ samples are produced at a lower rate so the *LMS6002D* can process all of the samples.

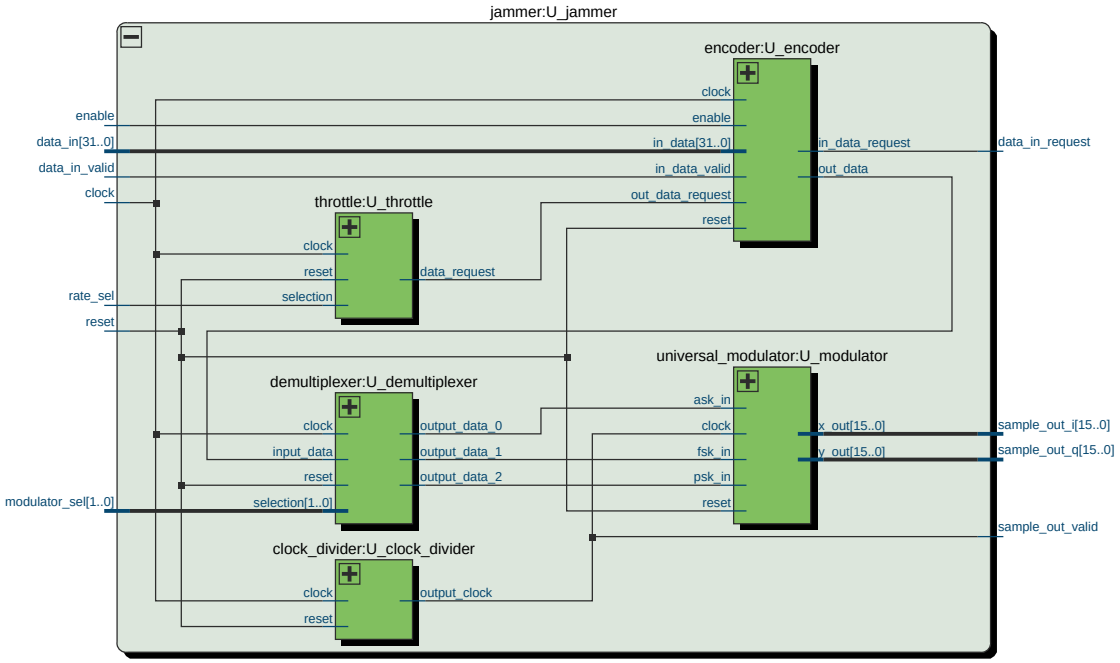

Figure 24. RTL view of the jammer module.

The encoded data is processed by the universal modulator. The universal modulator is capable of amplitude-shift keying (ASK), FSK and phase-shift keying (PSK) modulations and uses the Coordinate Rotation Digital Computer (CORDIC) algorithm as underlying mechanism for calculating the IQ samples. Modulator implementations in FPGA with and without using the CORDIC algorithm have been compared in [39]. Modulators implemented using the CORDIC algorithm require more hardware resources than the approaches without it but provide an easily configurable way of computing the IQ samples.

The block diagram of the developed universal modulator is shown in Figure 25 and the RTL view of the universal modulator is shown in Figure 26. The modulator acts as a numerically controlled oscillator with a simple modification. Numerically controlled oscillators generally only consist of a phase accumulator and a phase-to-amplitude converter. The modulator in addition has a phase adder in-between the phase accumulator and phase-to-amplitude converter to provide a way for not only accumulating but also modulating the phase. The modulation type, which is used, depends on which of the three inputs (ASK, FSK or PSK) is changed according to the data bits.

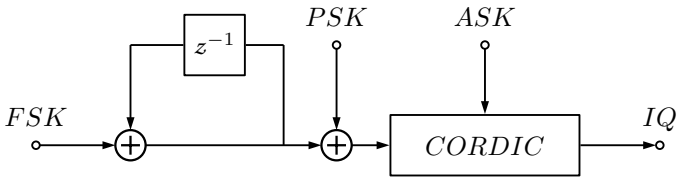

Figure 25. Block diagram of the universal modulator.

The phase accumulator consists of a 12-bit input, a 12-bit adder and a register. At each clock cycle a new 12-bit output is produced by summing the input and the register value. The new output value is written to the register and the resulting output is a staircase waveform with step size controlled by the frequency modulation input. The phase adder is used to change the accumulated phase, thus providing a simple way of modulating the phase.

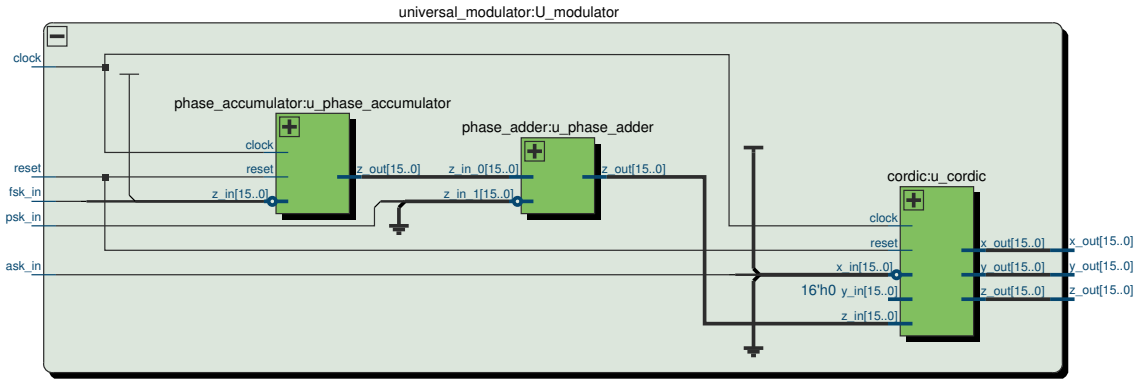

Figure 26. RTL view of the universal modulator.

The phase-to-amplitude converter, CORDIC kernel in this case, calculates sine and cosine values based on the accumulated phase at each clock cycle as described in Appendix B. In time, this results in the phase, sine and cosine waveforms as illustrated in Figure 27.

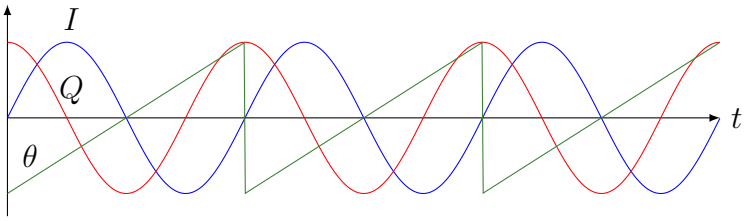

Figure 27. Modulator outputs corresponding to the accumulated phase.

The amplitude of the output signal is modulated by changing the amplitude input of the CORDIC kernel. The phase of the signal in case of amplitude modulation changes constantly and only the amplitude of the output signal is affected. This is illustrated in Figure 28a with the data, the accumulated phase, and the output signals plotted. The data, in case of amplitude modulation, is fed to the CORDIC kernel's amplitude input as mentioned.

Frequency-shift keying is achieved by accumulating the phase at different rates. Since all of the digital signal processing is done at baseband frequencies, accumulating the phase at a negative rate results in a negative frequency. This is illustrated in Figure 28b. When up-converted to the carrier frequency in the LMS6002D, as described in Appendix A, the negative and positive frequencies will be equally shifted sidebands from the carrier frequency. Phase of the output signal is modulated by shifting the phase in the phase adder by either 180° or 0° as illustrated in Figure 28c.

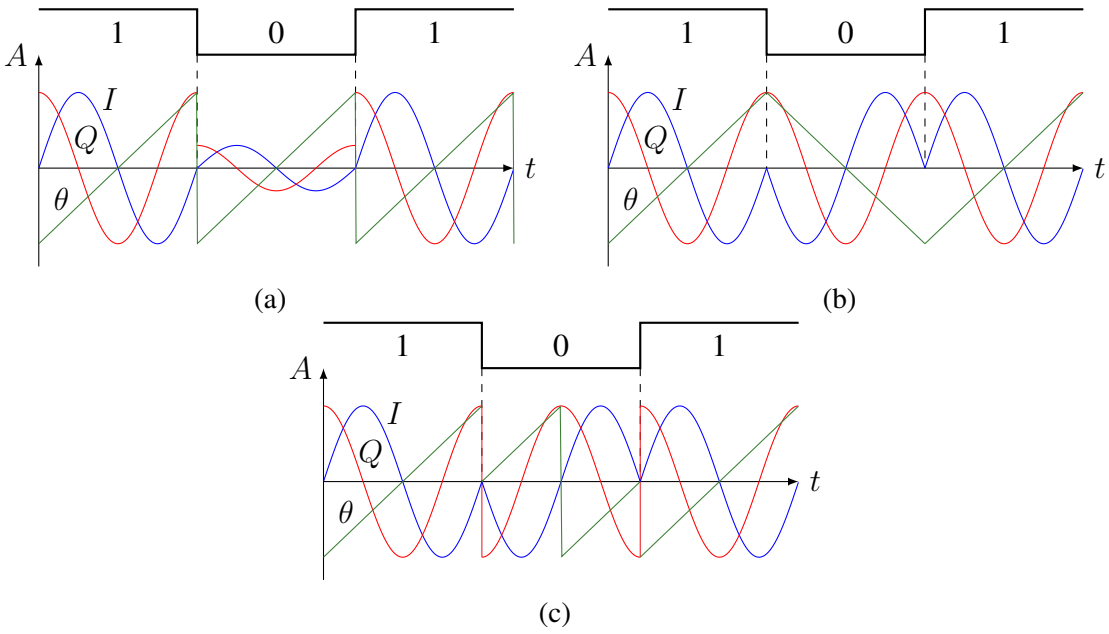

Figure 28. Three modulation types provided by the universal modulator are (a) amplitude-shift keying, (b) frequency-shift keying and (c) phase-shift keying.

The synthesized jammer entity which includes the universal modulator takes up 909 logic cells and 597 dedicated logic registers in the FPGA. No digital signal processing elements such as multipliers are used and most of the logic elements are used by the CORDIC kernel. This is a rather small amount of the total 114480 available logic elements and the implementation is not in this case restricted by the available resources.

4.3 Testing of UAV Remote Control Jamming

Testing of the developed UAV jamming subsystem was done against two widespread UAV remote control systems, the Futaba Advanced Spread Spectrum Technology (FASST) and the Advanced Continuous Channel Shifting Technology (ACCST) systems. Both of these systems were studied and their RF parameters were determined in order to use protocol-aware jamming technique against them. The FASST remote control communication system uses hybrid spread spectrum consisting of frequency-hopping and direct-sequencing. In contrast, the ACCST remote control system uses only frequency-hopping. In addition to testing the developed jamming subsystem, measurements with a jammer platform capable of generating sweeping and tone signals were performed. The following subsections describe the setup which was used for measuring the efficiency of different jammers against the remote control systems and give an overview of the experimental results.

4.3.1 Experimental Setup

The experimental setup shown in Figure 29 was used to find the jammer-to-signal ratios required to successfully jam the remote control links of the FASST and ACCST systems. Several remote controllers and receivers which use these systems have been developed. In these experiments the DJI Phantom 2 UAV, which is compatible with the FASST technology, was used. In case of ACCST, the FrSky Taranis X9D remote controller and FrSky X8R receiver were used. In order to reduce interference from the channel and to be able to measure the output powers, the RF connectors of the remote control, the UAV receiver and the jammer were directly connected using coaxial cables, attenuators, a splitter and a combiner. Both the output of the remote control and the output of the jammer were attenuated to bring the signal levels down to the linear working region of the UAV receiver (that is about -40 dBm). Otherwise signals from the jammer and the remote controller could have harmed the receiver input which has maximum input power specified less than the maximum output powers of the transmitters.

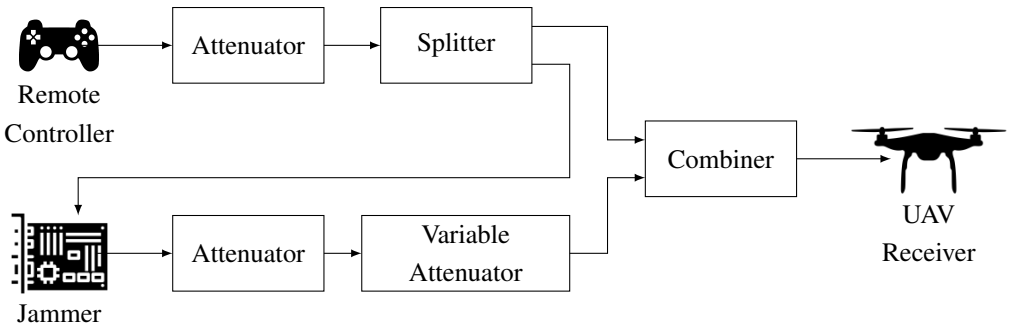

Figure 29. Setup for measuring the efficiencies of different jamming techniques against the FASST and the ACCST UAV remote control systems.

The remote controller signal was split and input to both the UAV receiver path and the jammer. This allowed the detection subsystem to detect the remote controller signal and notify the neutralization subsystem of it. A digital variable attenuator with 31 dB attenuation range and 0.25 attenuation step was put into the signal path of the jammer to change the JSR in the range of -11 dB to +20 dB. Remote controller and jammer signals were combined and then directed to the receiver of the UAV.

The measurements were limited by the fact that neither of the UAV remote control systems outputs a BER. To evaluate the performance of the FASST system a logic analyzer was inserted after the direct-sequence spreader and before the frequency hopping modulator in the remote controller. The logic analyzer was also attached to the receiver in the respective place, that is after the frequency-hopping demodulator and before the direct-sequence despreader. This allowed to compare the transmitted and received spread data and give an estimate of the actual BER caused by different JSRs. For the ACCST system the logic analyzer was connected to the receiver chip which only outputs packets with a matching cyclic redundancy check. Hence, for the ACCST system the packet error rate can be measured by comparing the number of received packets to the number of transmitted packets over a period of time. Furthermore, both systems indicate total remote control link loss visually and this was used to determine the threshold for successful jamming.

4.3.2 Experimental Results

FASST Against the FASST system the efficiencies of tone, sweep and protocol-aware jamming were measured. In addition to jamming, the developed UAV neutralization system was also used to take over the FASST remote control and the necessary JSR for a successful takeover was measured. The measurement results are plotted in Figure 30 together with the simulation results from Chapter 3. It can be seen that in case of jamming, the measurement results differ slightly from the simulation results, but in general the performance of the three jamming techniques is as expected based on the simulations.

The tone jammer was incapable of successfully jamming the remote control link as expected based on the simulation results from Subsection 3.3. The optimal sweeping rate for the sweeping jammer was found to be 1.5 kHz (in range of 0.5 kHz to 200 kHz). The sweeping jammer does not achieve BERs above 10^{-1} in the measured JSR range, but it affects enough bits in different packets to successfully jam the remote control link at 10 dB JSR. In comparison, the developed protocol-aware jammer achieved successful jamming at 2 dB JSR. The 8 dB difference results in about 6 times smaller required output power by the developed protocol-aware jammer to completely jam the FASST remote control system at the same distance. However, that is the case with the ideal sweeping rate. If the optimal sweeping rate could not be studied and a different rate were to be used then the distinction would be larger.

Successful takeover required higher JSR than just protocol-aware jamming and takeover was achieved at 4 dB JSR. The higher JSR requirement for the takeover compared to the protocol-aware jamming is reasonable because from some JSR the remote control which is being taken over starts to jam the platform which is taking over the control. The takeover is successful when the takeover signal level is high enough to cancel the jamming effect of the remote controller. Taking over the UAV is somewhat less power efficient and more complex than using the protocol-aware jammer, but it can be used to prevent the neutralized UAV from behaving unexpectedly (the UAV can be forced to land for example).

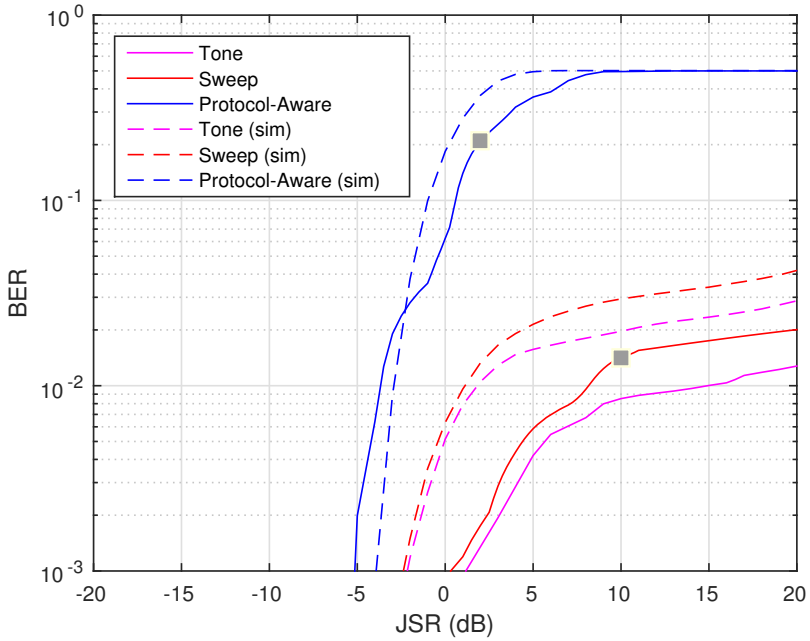

Figure 30. Measured efficiencies of different jamming techniques against the FASST system together with the simulated efficiencies. Datatips display complete jamming thresholds.

ACCST Against the ACCST system the efficiencies of tone, sweep and protocol-aware jamming were measured. Takeover of the ACCST system has not been tested because the packet structure used in ACCST has not yet been studied at the time of writing this thesis. For takeover to work however, knowledge of the packet structure is necessary to give valid commands and calculate a checksum. The experimental measurement results for the ACCST system are plotted in Figure 31. As discussed in Subsection 4.3.1, the ACCST system does not output a bit error rate and only the packet error rate can be measured. The system indicated loss of connection when the measured packet error rate reached above 0.5. This is therefore considered to be the threshold for complete jamming.

The tone jammer effectively jammed one of the channels used by the ACCST system from 0 dB JSR and above. As mentioned in Subsection 3.6 though, interfering with a single channel of frequency hopping UAV remote control systems is not sufficient to prevent the UAV from being remotely controlled. Complete jamming of the UAV remote control system was therefore not achieved with the tone jammer.

The sweeping jammer was found to be most efficient with sweeping rate of 6 kHz (in range of 0.5 kHz to 200 kHz) and achieved complete jamming of the ACCST system at 15 dB JSR. In comparison, the developed protocol-aware jammer accomplished complete jamming of the ACCST system at nearly -1 dB JSR. The 16 dB difference in the required JSR results in roughly 30 times smaller required output power by the developed protocol-aware jammer compared to the sweeping jammer to completely jam the ACCST remote control system at the same distance.

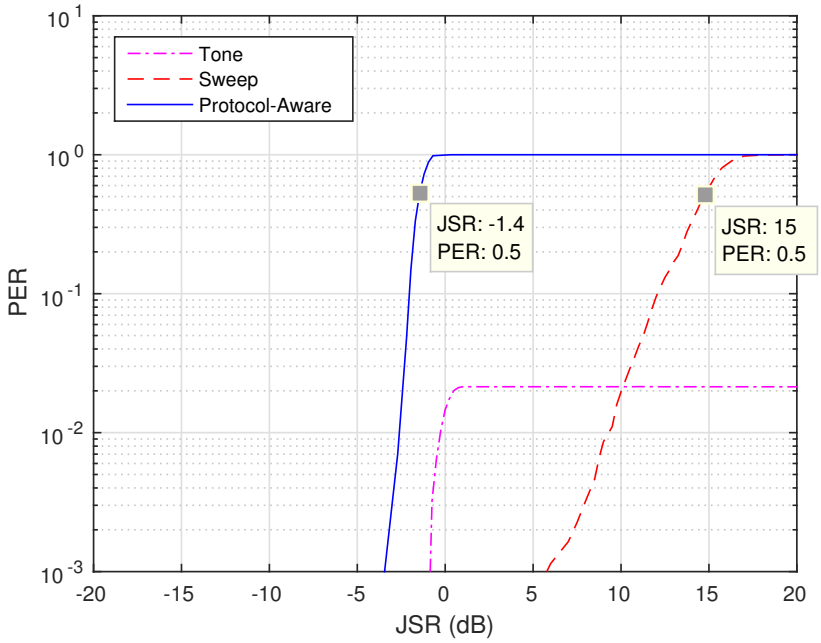

Figure 31. Measured efficiencies of different jamming techniques against the ACCST system. Datatips display complete jamming thresholds.

4.4 Conclusion

Based on the measurement described in Subsection 4.3, the developed protocol-aware jammer is theoretically capable of successfully jamming the remote control link of the FASST system from at least 4/5th of the distance from the UAV to the remote control with line-of-sight signal propagation and equal output powers. This theoretical limit is calculated with the Friis transmission equation (10) using the required 2 dB JSR measured in Subsection 4.3.2 for the FASST system.

$$P_r = P_t + G_t + G_r + 20log_{10}\left(\frac{\lambda}{4\pi R}\right) \tag{10}$$

In comparison, the sweeping jammer with optimal sweeping rate at the same output power theoretically jams the FASST system successfully from 1/3rd of the distance. These differences are illustrated in Figure 32 using an example in which the distance between the jammer and the remote controller is 1000 m. Both of the jammers and the remote controller in this exampe have equal output powers. It can be seen that the UAV can get much closer to the sweep jammer than it can to the protocol-aware jammer.

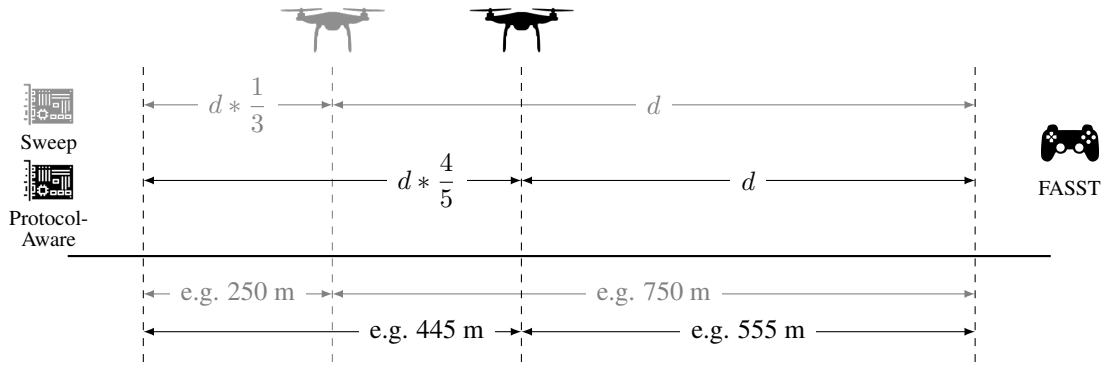

Figure 32. Calculated successful remote control link jamming distances of the sweep and the protocol-aware jammers against the FASST system at equal output powers.

For the ACCST system the theoretical maximum working distance of the developed jammer is even greater, becoming effective from 8/7th of the distance. The sweeping jammer however is even less useful in jamming the ACCST system than it is in jamming the FASST system. The sweep jammer becomes effective from 1/5th of the distance. These theoretical limits are compared in Figure 33 similarly to the previous example. Again the distance between the jammer and the remote controller is 1000 m and both of the jammers have output power equivalent to the remote controller.

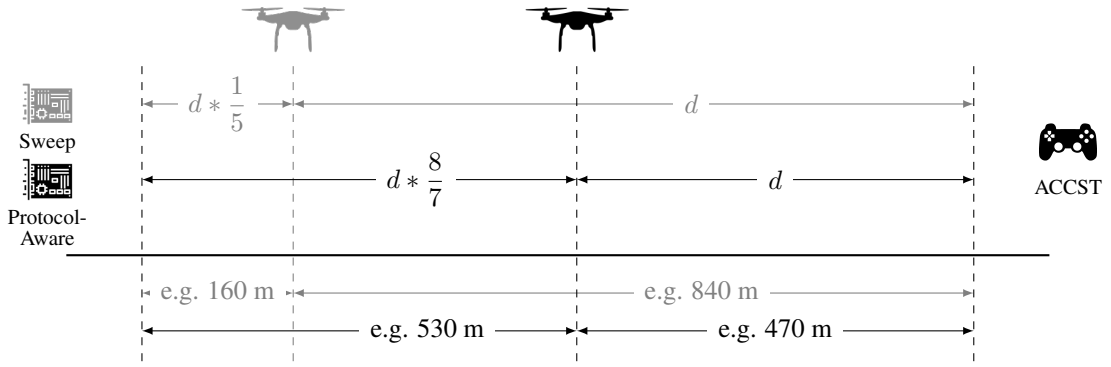

Figure 33. Calculated successful remote control link jamming distances of the sweep and the protocol-aware jammers against the ACCST system at equal output powers.

The developed protocol-aware jamming system therefore is considerably more efficient than the sweeping jammer. The exact differences in the efficiency gain depend on the targeted system, but to achieve similar results with the two considered jamming techniques the protocol-aware jamming technique requires at least 6 times less transmission power than the sweep jamming technique. Furthermore, since the developed jammer uses the power in a more purposeful manner and has lower transmission power requirements, then its effect on other communication systems in the same RF band can be expected to be much smaller.

Against both of the systems the optimal sweeping rate was different. This is probably caused by differences in the receiver implementations and also by the differences in the remote control system designs, specifically the varying hopping rates and the number of channels used. For the sweeping jammer to fulfill its potential it therefore needs a certain level of protocol-awareness as well since performance of the sweeping jammer would be further degraded by using different sweeping rates.

The jamming system proposed in this thesis is flexible and has been shown to successfully work against two dissimilar UAV remote control systems. The FASST and ACCST systems use different RF parameters along with various hopping patterns and rates. All of which is configurable due to the software defined nature of the implemented jammer. The developed system has also been shown to be capable of taking over the FASST remote control link due to its flexibility. At the time of writing this thesis the packet structure of the ACCST system is though not yet known and the ACCST remote control link can not be taken over.

5 Conclusion and Future Work

UAVs have become increasingly popular and their usage presents new challenges in security and surveillance. Their reckless usage can cause accidents and they can be used with malicious intentions. Detection and neutralization of rogue UAVs has therefore become an important research issue. Generally, UAVs have either a flight route preprogrammed and they follow it based on GNSS signals or they are being manually controlled. The possible detection and neutralization tactics which can be applied are consequently quite different depending on the way they are being operated.

The aim of this thesis has been to develop a jamming subsystem as a part of an UAV detection and neutralization system targeting the UAV remote control link. UAV remote control systems typically use spread spectrum technologies to prevent other communication systems from interfering with them. However, this also makes efficient jamming of the remote control link more complex. The following contributions have been made in this thesis to efficiently jam the remote control systems of UAVs.

- A hybrid spread spectrum (frequency hopping and direct sequencing combined) digital communication system model was developed based on commercially available UAV remote control systems. Performances of barrage, tone, sweep and protocol-aware jamming techniques against this model were simulated and a comparison of their efficiencies was provided. Protocol-aware jamming technique, which mimics the targeted signal, was found to be the most power efficient of those techniques.
- A configurable jamming subsystem was implemented to work together with a detection subsystem in the FPGA of an open source SDR platform. It provides a way for generating the jamming signal with different modulation types, data rates and spread spectrum characteristics to imitate the targeted signal and thus apply protocol-aware jamming. The jamming subsystem is also capable of transmitting arbitrary data, therefore being usable for UAV remote control takeover.
- Two widespread UAV remote control systems were studied in order to employ protocol-aware jamming against them. Efficiencies of different jamming techniques were measured against the two systems and as expected, based on the simulation results, protocol-aware jamming technique used in the developed system was the most efficient, requiring several times less power than the sweep jammer. After studying the data protocol used in one of the targeted systems, the developed system was also shown to be capable of taking over the remote control.

The developed system can therefore be used for protocol-aware jamming and takeover of UAV remote control systems. In addition to these methods being more power efficient than for example sweep jamming, protocol-aware jamming and takeover are also expected to be less influential against other communication systems in the targeted band. That is partially due to the lower power requirement but also because of less excessive RF spectrum usage. Essentially the protocol-aware jamming and takeover techniques do not interfere with other communication systems much more than the targeted remote control system itself does.

Still, the fact that only one of the remote control systems was managed to be taken over further illustrates how much effort is required in order to apply these techniques. Reverse engineering the remote control systems is a cumbersome task which is only expected to get more difficult as remote control technology advances. The sweep jammer in comparison required much less knowledge about the targeted system. Protocol-aware jamming, or takeover for that matter, and sweep jamming therefore present a trade-off between efficiency and simplicity.

This leads to the various aspects in which the jamming subsystem could be enhanced. Firstly, more UAV remote control systems could be studied and their parameters added to the developed system for protocol-aware jamming. It could be also improved to generate a sweeping signal in case the detection subsystem detects an UAV remote control system against which protocol-aware jamming can not be employed. This may be necessary if there is not enough knowledge about the targeted signal, for example if the frequency hopping pattern can not be determined. Furthermore, the jamming signal generation capabilities could be improved to include other modulation types than the currently available binary shift keying types, for example quadrature amplitude modulation could be added.

Moreover, the system presented in this thesis is only targeting UAV remote control signals and therefore is not capable of neutralizing UAVs which have a preprogrammed flight route. Jamming and spoofing of GNSS systems has been widely covered in literature and research suggests that commercially available UAVs which are flying a preprogrammed flight route can be taken over by spoofing the GNSS signals. Jamming or spoofing of the GNSS signals could be integrated as a countermeasure against such UAVs.

References

[1] Goldman Sachs Research. Drones: Reporting for Work, 2016. [WWW] http://www.goldmansachs.com/our-thinking/technology-driving-innovation/drones/.

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

[3] Rohde & Schwarz GmbH & Co KG. Protecting the Sky: Signal Monitoring of Radio Controlled Civilian Unmanned Aerial Vehicles and Possible Countermeasures. [WWW] http://www.rohde-schwarz-usa.com/rs/324-UVH-477/images/Drone_Monitoring_Whitepaper.pdf.

[4] Grace Xingxin Gao, Matteo Sgammini, Mingquan Lu, and Nobuaki Kubo. Protecting GNSS receivers from jamming and interference. *Proceedings of the IEEE*, 104(6):1327–1338, 2016.

[5] Victor C Chen, Fayin Li, S-S Ho, and Harry Wechsler. Micro-doppler effect in radar: phenomenon, model, and simulation study. *IEEE Transactions on Aerospace and electronic systems*, 42(1):2–21, 2006.

[6] Thales Group. SQUIRE Drone detection & classification. [WWW] https://www.thalesgroup.com/sites/default/files/squire/index.html.

[7] Kelvin Hughes Ltd. UAV & Drone Detection Radar. [WWW] https://www.kelvinhughes.com/security/uav-drone-detection.

[8] Aaronia AG. Real-Time RF Drone and Radar Detection System. [WWW] http://www.aaronia.com/Datasheets/Documents/Drone-Detection-System.pdf.

[9] Hocheol Shin, Kibum Choi, Youngseok Park, Jaeyeong Choi, and Yongdae Kim. Security Analysis of FHSS-type Drone Controller. In *International Workshop on Information Security Applications*, pages 240–253. Springer, 2015.

[10] Jan Farlik, Miroslav Kratky, and Josef Casar. Detectability and jamming of small UAVs by commercially available low-cost means. In *Communications (COMM), 2016 International Conference on*, pages 327–330. IEEE, 2016.

[11] Danh Nguyen, Cem Sahin, Boris Shishkin, Nagarajan Kandasamy, and Kapil R Dandekar. A real-time and protocol-aware reactive jamming framework built on

software-defined radios. In *Proceedings of the 2014 ACM workshop on Software radio implementation forum*, pages 15–22. ACM, 2014.

[12] Positive Technologies. PHD VI: How They Stole Our Drone. [WWW] http://2016.phdays.com/press/news/70461/.

[13] Jonathan Andersson. Hacker's Icarus machine steals drones midflight. [WWW] https://arstechnica.com/security/2016/10/drone-hijacker-gives-hackers-complete-control-of-aircraft-in-midflight/.

[14] Andrew J Kerns, Daniel P Shepard, Jahshan A Bhatti, and Todd E Humphreys. Unmanned aircraft capture and control via GPS spoofing. *Journal of Field Robotics*, 31(4):617–636, 2014.

[15] Robert Scholtz. The origins of spread-spectrum communications. *IEEE Transactions on Communications*, 30(5):822–854, 1982.

[16] Raymond Pickholtz, Donald Schilling, and Laurence Milstein. Theory of spread-spectrum communications–a tutorial. *IEEE transactions on Communications*, 30(5):855–884, 1982.

[17] Bradford W Parkinson and Stephen W Gilbert. NAVSTAR: Global Positioning System–Ten years later. *Proceedings of the IEEE*, 71(10):1177–1186, 1983.

[18] Earl McCune. *Practical digital wireless signals*. Cambridge University Press, 2010.

[19] John Fakatselis. Processing gain in spread spectrum signals. *Harris Semiconductor application note*, 1998.

[20] Bruce A Fette, Roberto Aiello, Praphul Chandra, Daniel M Dobkin, Dan Bensky, Douglas B Miron, David Lide, Farid Dowla, and Ron Olexa. *RF and Wireless Technologies: Know It All*. Elsevier, 2007.

[21] J Lindner. Binary sequences up to length 40 with best possible autocorrelation function. *Electronics letters*, 11(21):507–507, 1975.

[22] Marc Lichtman, Jeffrey D. Poston, SaiDhiraj Amuru, Chowdhury Shahriar, T. Charles Clancy, R. Michael Buehrer, and Jeffrey H. Reed. A communications jamming taxonomy. *IEEE Security & Privacy*, 14(1):47–54, February 2016.

[23] Kanika Grover, Alvin Lim, and Qing Yang. Jamming and anti–jamming techniques in wireless networks: a survey. *International Journal of Ad Hoc and Ubiquitous Computing*, 17(4):197–215, 2014.

[24] Claude E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27(3):379–423, July 1948.

[25] Tamer Basar. The gaussian test channel with an intelligent jammer. *IEEE Transactions on Information Theory*, 29(1):152–157, January 1983.

[26] Jae Hong Lee, Byeong Seok Yu, and Sang-Chul Lee. Probability of error for a hybrid DS/SFH spread-spectrum system under tone jamming. In *Military Communications Conference, 1990. MILCOM'90, Conference Record, A New Era. 1990 IEEE*, pages 410–414. IEEE, 1990.

[27] Dong-Yeol Choi, Won-Kyung Kim, Jae-Hyun Kim, and Huirae Cho. Performance of analog and digital modulation schemes under sweep jamming. In *Ubiquitous and Future Networks (ICUFN), 2016 Eighth International Conference on*, pages 13–15. IEEE, 2016.

[28] Ilkka Harjula, Jarno Pinola, and Jarmo Prokkola. Performance of IEEE 802.11 based WLAN devices under various jamming signals. In *Military Communications Conference, 2011-MILCOM 2011*, pages 2129–2135. IEEE, 2011.

[29] Abid Hussain, Nazar A Saqib, Usman Qamar, Muhammad Zia, and Hassan Mahmood. Protocol-aware radio frequency jamming in wi-fi and commercial wireless networks. *Journal of communications and networks*, 16(4):397–406, 2014.

[30] David Thuente and Mithun Acharya. Intelligent jamming in wireless networks with applications to 802.11 b and other networks. In *Proc. of MILCOM*, volume 6, page 100, 2006.

[31] MathWorks, Inc. Bluetooth Frequency Hopping. [WWW] https://www.mathworks.com/examples/simulink-communications/mw/comm_product-commbluetoothfreqhop-bluetooth-frequency-hopping.

[32] Nuand, LLC. Setting up Yate and YateBTS with the bladeRF. [WWW] https://github.com/Nuand/bladeRF/wiki/Setting-up-Yate-and-YateBTS-with-the-bladeRF.

[33] Takuji Ebinuma. Software-Defined GPS Signal Simulator. [WWW] https://github.com/osqzss/gps-sdr-sim.

[34] Nuand, LLC. bladeRF VHDL ADS-B decoder core. [WWW] https://github.com/Nuand/bladeRF-adsb.

[35] Lime Microsystems. LMS6002D: Multi-band Multi-standard Transceiver with Integrated Dual DACs and ADCs. [WWW] http://www.limemicro.com/download/LMS6002Dr2-DataSheet-1.2r0.pdf.

[36] Intel Corporation. Nios II Gen2 Processor Reference Guide. [WWW] https://www.altera.com/en_US/pdfs/literature/hb/nios2/n2cpu-nii5v1gen2.pdf.

[37] Lime Microsystems. LMS6002D: Programming and Calibration Guide. [WWW] http://www.limemicro.com/wp-content/uploads/2015/04/LMS6002Dr2-Programming-and-Calibration-Guide-1_1r5.pdf.

[38] Nuand, LLC. Frequency Tuning on the bladeRF. [WWW] https://www.nuand.com/libbladeRF-doc/v1.7.2/tuning.html.

[39] S Vaishnavi, B Titiksha, RJ Vinay, and J Manikandan. Design and evaluation of universal modulators. In *India Conference (INDICON), 2015 Annual IEEE*, pages 1–5. IEEE, 2015.

[40] Tore Ulversoy. Software defined radio: Challenges and opportunities. *IEEE Communications Surveys & Tutorials*, 12(4):531–550, 2010.

[41] Joseph Mitola. Software radios: Survey, critical evaluation and future directions. *IEEE Aerospace and Electronic Systems Magazine*, 8(4):25–36, 1993.

[42] D. Frizelle and F. Kearney. Complex RF Mixers, Zero-IF Architecture, and Advanced Algorithms: The Black Magic in Next-Generation SDR Transceivers, 2017. [WWW] http://www.analog.com/media/en/analog-dialogue/volume-51/number-1/articles/complex-mixers-zif-architecture-advanced-algorithms-black-magic-next-generation-sdr-transceivers.pdf.

[43] Jack E Volder. The CORDIC trigonometric computing technique. *IRE Transactions on electronic computers*, (3):330–334, 1959.

[44] John S Walther. A unified algorithm for elementary functions. In *Proceedings of the May 18-20, 1971, spring joint computer conference*, pages 379–385. ACM, 1971.

[45] Ray Andraka. A survey of CORDIC algorithms for FPGA based computers. In *Proceedings of the 1998 ACM/SIGDA sixth international symposium on Field programmable gate arrays*, pages 191–200. ACM, 1998.

A Zero IF Architecture in Software Defined Radio

The evolution towards SDR systems has been driven by the demand for more flexible and reconfigurable radio solutions and at the same time by the evolution of the enabling technologies, the DACs, the ADCs, the digital signal processors and the FPGAs [40]. Flexibility and reconfigurability allows the communication system to be upgraded, that is new software loaded, without actually upgrading the RF hardware. This makes applying new standards and innovations to the existing communication systems easier and more affordable [40]. Furthermore, this reconfigurability allows to develop cognitive radios, environment aware systems that can adapt to different circumstances.

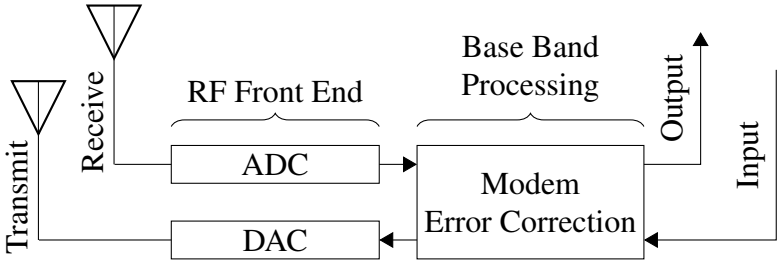

Figure A.1. An ideal SDR transceiver.

The concept of SDR was introduced by J. Mitola in [41] and in an idealized scenario SDR is able to communicate at any frequency, bandwidth, modulation and data rate by simply loading the appropriate software. This necessitates universal hardware that can provide the software with an interface to the RF domain. Figure A.1 shows an ideal SDR transceiver adapted from [41], which consists of an ADC, a DAC and a processing unit running the software (here modem and error correction). In this ideal transceiver, the converters are the only components involved with analog signals and everything else is done digitally.

The ideal SDR transceiver is not entirely achievable in practice due to technological limits, with the main problem being the conversion between the analog and the digital signals. The converters lack the ability to sample at very high rates while also maintaining high precision. Although RF sampling ADCs and DACs capable of sampling at few giga samples per second with 12-bit and 14-bit precision are already available, they are expensive and still bandwidth limited. Another challenge is to digitally process the signals fast enough to take advantage of the high sampling rates and precision.

Figure A.2 shows the architecture of an SDR transceiver with a RF front end, which is typically used to convert the analog signals from the antenna at some frequency to

an IF when receiving or the other way around when transmitting. This allows using ADCs and DACs with lower sampling rates than targeted carrier frequency would require. The following paragraphs describe in more detail the zero IF architecture, which is the underlying architecture of the SDR platform used in this thesis.

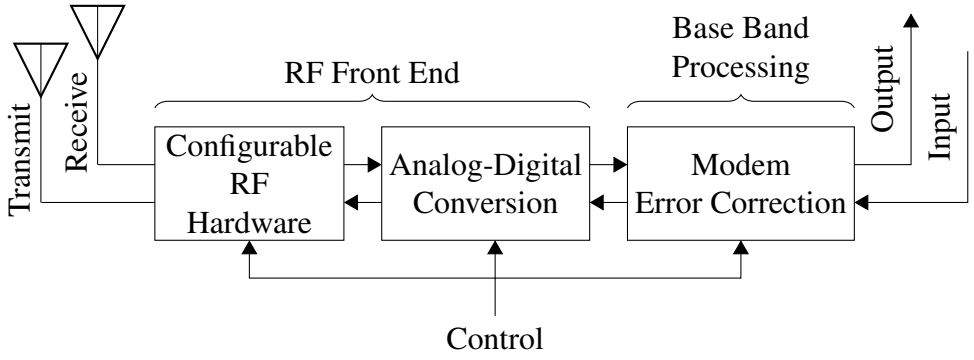

Figure A.2. Architecture of an SDR transceiver.

Zero IF Architecture Figure A.3 provides and overview of a complex transmitter with zero IF architecture. Two parallel paths (the I and Q signals) are upconverted with the same local oscillator signal whose output is 90° phase shifted for one of the paths. The independent paths are then summed to form the desired RF output signal with the useful consequence of removing negative frequencies.

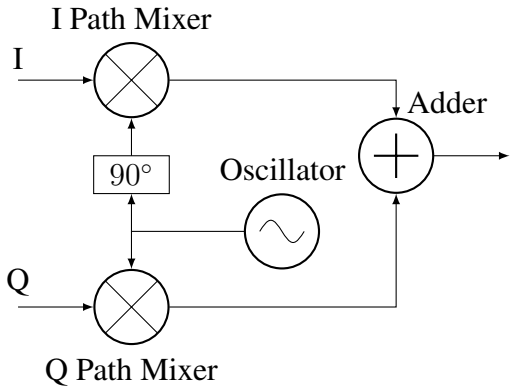

Figure A.3. Basic architecture of a complex transmitter.

Consider the I path analysis shown in Figure A.4a, with signal at x Hz input to the I path and no signal in the Q path input. The mixer in the I path produces an output at the local oscillator frequency $\pm x$ Hz. The mixer in the Q path does not produce an output since the Q path is not fed with a signal. The adder forms the output signal solely from the I path.

Similar behavior can be observed in the reversed case with the I path not fed with a signal and the Q path fed with signal at x Hz. As shown in Figure A.4b, the mixer in the Q

path produces an output at local oscillator frequency $\pm x$ Hz which passes to the complex transmitter output. In frequency spectrum the output for this case looks exactly the same as for when only the I path was fed with a signal at frequency x Hz. The difference is only in the phase of the output signal.

Given that the inputs I and Q are 90° out of phase, the upper sideband signals after mixers will be "in phase" and the lower sideband signals will be 180° out of phase. Therefore the lower sideband signals will cancel each other out, leaving only the upper sideband signal as illustrated in Figure A.4c. This removes the need for filtering one of the sideband signals at the output, as is the case for conventional single mixer architectures [42].

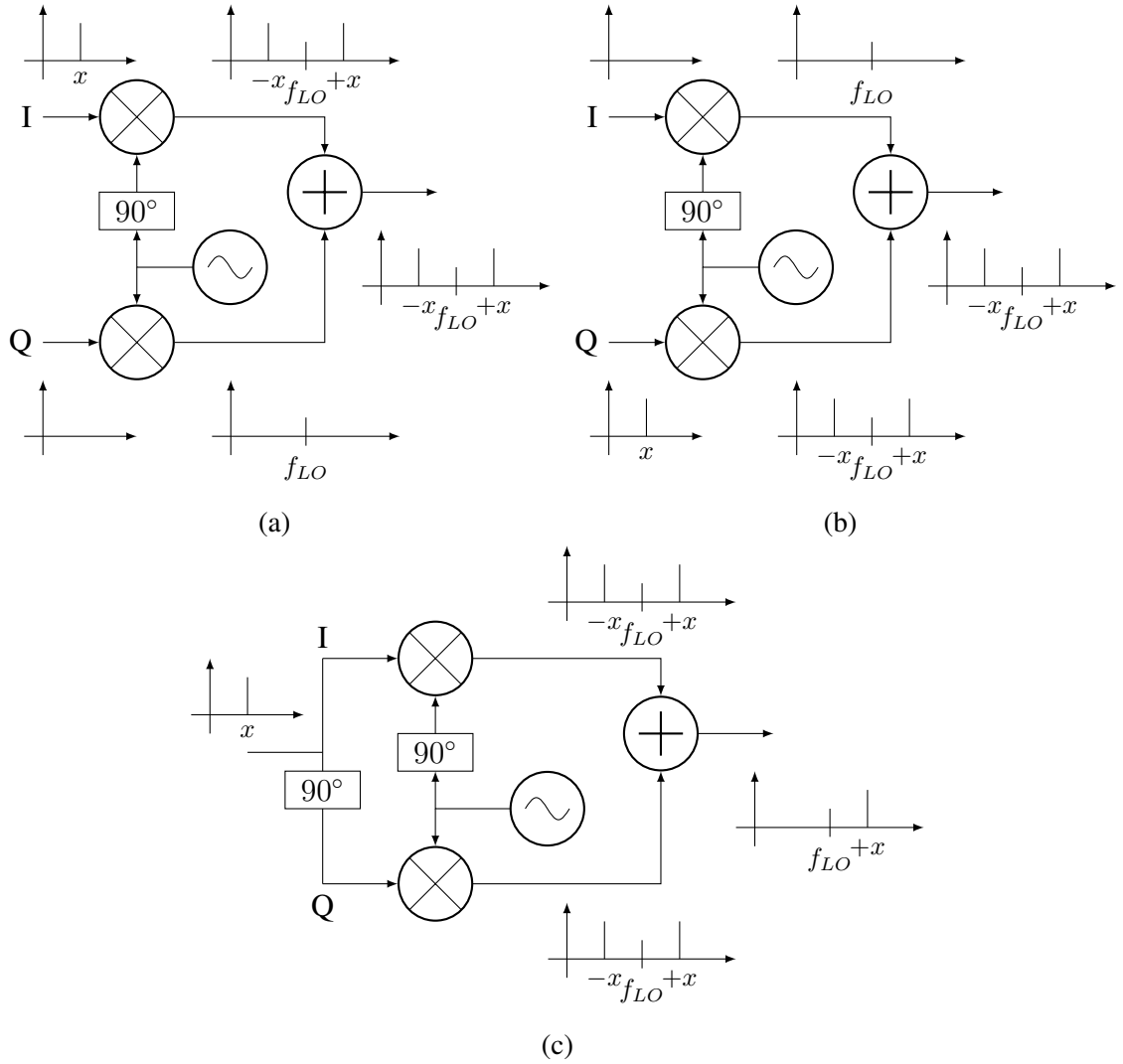

Figure A.4. I and Q signal path analysis in zero IF architecture (a): I path analysis; (b): Q path analysis; (c): I and Q path simultaneous analysis.

B Coordinate Rotation Digital Computer

This subsection introduces the CORDIC algorithm, which is used in this thesis to efficiently generate the IQ samples transmitted by the SDR platform. CORDIC is a shift-and-add type of algorithm used for evaluation of trigonometric, hyperbolic, linear and logarithmic functions proposed by Volder in [43] and further improved by Walter in [44]. Simplicity of the operations used in the CORDIC algorithm makes it suitable for implementation on a FPGA, where multipliers and dividers are a scarce resource. Different implementations, such as iterative and on-line, have been presented in literature [45].

In this thesis, the CORDIC algorithm is used in rotation computing mode to calculate the sine and the cosine simultaneously based on Equations B.1 and B.2. At each evaluation of this algorithm the vector magnitude and angle of rotation are provided and the coordinate components are computed. The algorithm begins by initializing an angle accumulator with the desired rotation angle. At each iteration a rotation decision is made to decrease the magnitude of residual angle accumulator. The rotation decision is made based on the sign of the residual angle in the angle accumulator. This basically results in a binary search on phase by adding or subtracting successively smaller phases to reach some target phase as illustrated in Figure B.1.

$$\begin{aligned} z_{i+1} &= z_i - d_i * \arctan(2^{-i}) & z_n &= 0 \\ x_{i+1} &= x_i - y_i * d_i * 2^{-i} & x_n &= A_n(x_0 \cos z_0 - y_0 \sin z_0) \\ y_{i+1} &= y_i + x_i * d_i * 2^{-i} & y_n &= A_n(y_0 \cos z_0 + x_0 \sin z_0) \end{aligned} \tag{B.1}$$

$$A_n = \prod_{i=0}^{N-1} \sqrt{1 + 2^{-2i}} \tag{B.2}$$

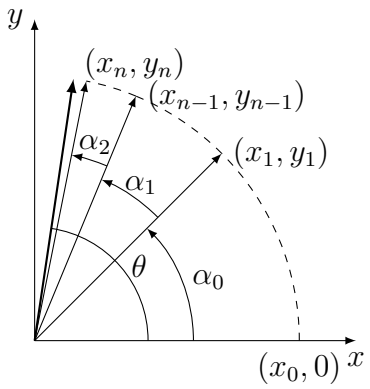

Figure B.1. Working principle of the CORDIC algorithm in rotation mode.

When the CORDIC algorithm is calculated for a fixed number of iterations at evaluation, as is the case in this thesis, it does not necessarily decrease the magnitude of the residual angle accumulator to zero. The fixed number of iterations can be based on hardware and timing limitations. Figure B.2 illustrates the errors introduced by the CORDIC algorithm in rotation mode with the number of iterations set to 12.

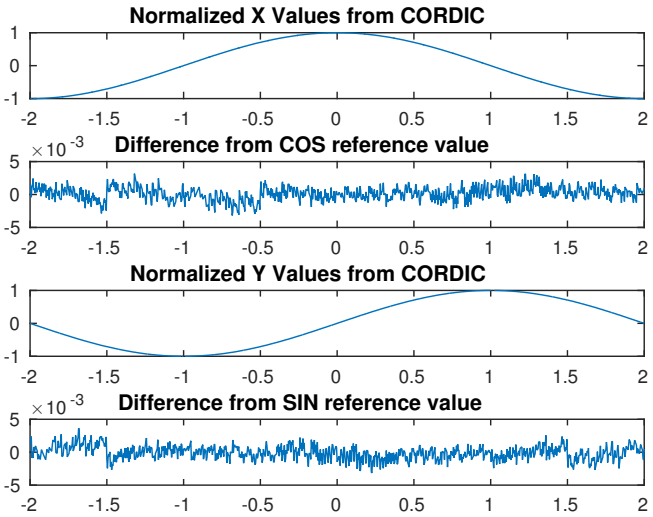

Figure B.2. Error of the CORDIC algorithm in rotation mode with 12 iterations and quadrant correction.