FFI Norwegian Defence
Research Establishment

23/00912

FFI-RAPPORT

Performance of a low-latency repeater jammer implemented on an SDR

Ulrik Aalborg Eriksen

Performance of a low-latency repeater jammer implemented on an SDR

Ulrik Aalborg Eriksen

Norwegian Defence Research Establishment (FFI) 23 November 2023

Keywords

Elektromagnetisk krigføring
Elektromagnetiske mottiltak
Jamming
SDR (Software Defined Radio)
FPGA (Field Programmable Gate Array)
Python

FFI report

23/00912

Project number

1557

Electronic ISBN

978-82-464-3496-4

Approvers

Tore Ulversøy, *Research Manager*
Tor-Odd Høydal, *Director of Research*

The document is electronically approved and therefore has no handwritten signature.

Copyright

Summary

Frequency-hopping spread-spectrum (FHSS) radio systems change their radio frequency (RF) rapidly to decrease their susceptibility to jamming. Time-correlated jammers have the ability to jam FHSS systems much more efficiently than conventional jammers if they react quickly enough to the frequency changes of the target system.

We implemented a low-latency repeater jammer on a USRP N321 software-defined radio (SDR) and studied the reaction time and jamming effectiveness of the repeater jammer. The fastest reaction time we achieved was 1.48 µs. However, the reaction time will depend on the required complexity of the jammer.

The repeater jammer samples incoming radio signals and then retransmits the same signal with a frequency shift. The frequency shift applied by the jammer is changed periodically. To gauge the jamming effectiveness of the repeater jammer, we tested it against several frequency shift keying (FSK) systems. Against an FHSS system with 10 kHz hopping rate, the repeater jammer performed more efficiently than a wideband noise jammer in the absence of propagation delay. Against a static frequency target system, the performance of the repeater jammer was similar to a narrowband noise jammer that focusses all its power in the active channel.

Sammendrag

Frekvenshoppende radiosystemer bytter bærebølgefrekvens jevnlig for å øke motstandsdyktigheten mot jamming. Mot slike frekvenshoppende radiosystemer kan reaktive jammere virke flere ganger mer effektivt enn tradisjonelle jammere. Det krever likevel at den reaktive jammeren kan reagere kjapt nok på målsystemets frekvensendringer.

Vi implementerte en reaktiv jammer med lav forsinkelse på en USRP N321 programvaredefinert radio, og målte både reaksjonstiden og jammeytelsen til denne reaktive jammeren. Den kjappeste responstiden vi målte, var på 1,48 µs, men den reelle forsinkelsen blir høyere jo mer sofistikert jammeren er.

Den reaktive jammeren fungerer ved å sample signalene fra målsystemet for så å sende dem i retur på en noe endret frekvens. Jammeren varierer hvor mye den forskyver frekvensen til signalet. Alle målsystemene vi testet den reaktive jammeren mot, benyttet frekvensskiftmodulasjon (FSK – frequency shift keying). I tester med et frekvenshoppende målsystem som hopper 10 000 hopp per sekund, så hadde den reaktive jammeren mye bedre jammevirkning enn en bredbåndsstøyjammer når det ikke var noen propagasjonsforsinkelse. Mot målsystemer som ikke er frekvenshoppende, er den reaktive jammer omtrent like effektiv som en smalbåndsstøyjammer med tilpasset båndbredde.

Contents

1 Introduction

1.1 Motivation

Having the ability to restrict other users' access to the electromagnetic spectrum is a considerable advantage on the battlefield. Therefore, robust military communication systems implement electromagnetic protective measures (EPM). One such protective measure is the use of frequency-hopping spread-spectrum (FHSS) radio systems, which change frequency rapidly in an seemingly unpredictable manner. This limits the impact of interference and limits the effectiveness of electromagnetic countermeasures (ECM) on link degradation. Hence, efficient jamming of enemy FHSS radio systems is of high interest for military applications.

It is certainly possible to jam FHSS radio systems with conventional jamming methods like a wideband noise jammer, but it is not efficient. With no knowledge of the hopping sequence, a noise jammer would have to jam all the possible radio channels simultaneously to block communications. The power advantage of the FHSS radio system is potentially very high, which requires the jammer to be powerful and costly to compete. A powerful wideband jammer also causes unintentional jamming of other spectrum users, which is not ideal. Although the hopping pattern cannot be predicted, it can be monitored; a reactive jammer can identify active radio frequency (RF) transmitters and initiate jamming. The power requirement of the jammer is thereby lowered significantly.

In order to perform successful reactive jamming, there is a fundamental challenge that must be overcome: the jamming signal has to reach the receiver before it switches frequency channel. The severity of this constraint increases with the hopping rate of the FHSS system, but in general, there is a maximum distance at which the reactive jammer can operate. The time that passes from the moment a jammer detects a signal until it emits a jamming signal will further limit the maximum operable path length difference.

Repeater jammers are a subclass of reactive jammers, which generate their jammer signals based on the radio signal they receive. To perform a successful repeater jamming attack, the retransmitted jammer signal should resemble the original transmission, while also differing enough to introduce errors at the intended receiver.

1.2 Scope

This report studies low-latency repeater jammers realisable on commercial-off-the-shelf (COTS) software-defined radios (SDRs). Experimentation is performed with a USRP N321 SDR platform from Ettus Research. This SDR is equipped with a field-programmable gate array (FPGA). The user-programmable FPGA can offload high-intensity digital signal processing (DSP) operations from the host computer, and thereby reduce the reaction time. Different approaches to reducing the reaction time of the repeater jammer is evaluated. Two test benches are created to measure the jamming effectiveness of different jamming schedules and parameters.

2 Background

2.1 Frequency-hopping Spread-spectrum

Communication systems with high reliability requirements implement EPM like FHSS to decrease their susceptibility to ECM [1]. An FHSS radio system varies its RF frequency in an unpredictable manner as a function of time. This is illustrated in Figure 2.1. The instantaneous bandwidth is a fraction of the larger spread bandwidth for such a system. If an opposing jammer is forced to cover the entire spread bandwidth simultaneously, this is a large power advantage for the FHSS radio system. For a given jammer, the effective jamming distance is reduced; at a given distance, a more powerful and expensive jammer is necessary to accomplish the same amount of link degradation.

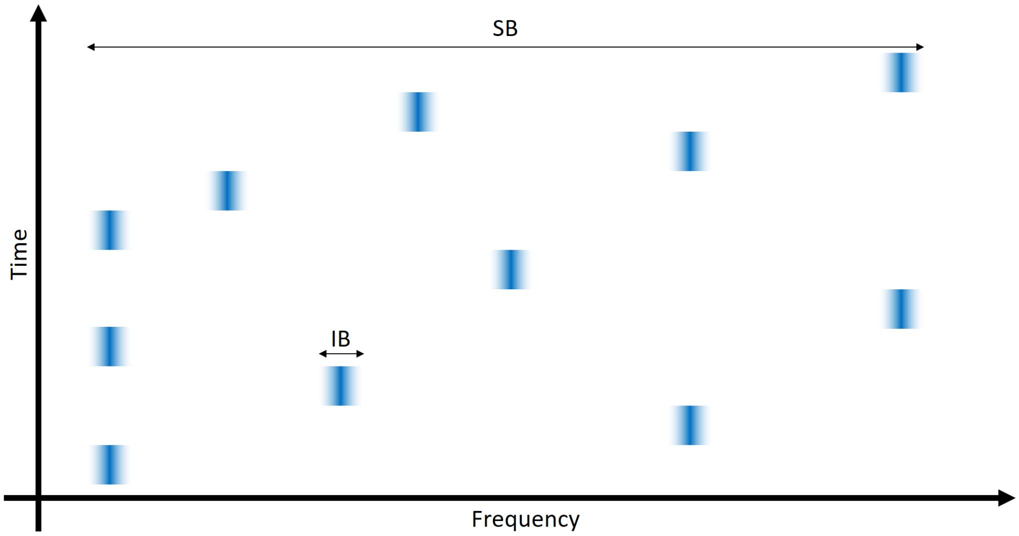


Figure 2.1 A waterfall diagram of an FHSS *radio system that varies the frequency of a signal. The instantaneous bandwidth (IB) is smaller than the spread bandwidth (SB).*

FHSS systems commonly employ non-coherent modulation techniques like frequency shift keying (FSK), because of the challenges associated with the phase alignment during frequency hopping [1–5]. Coherent demodulation is more challenging for higher hopping rates [5, 6]. High hopping rate is advantageous to an FHSS system, because it will force opposing reactive jammers to get physically closer in order to remain effective. However, it is worth noting that the modulation schemes of military transceivers are sparsely documented in open sources, and these platforms could utilise other formats.

2.2 Reactive Jammers

Reactive jammers are a class of jammers which are time correlated [7], meaning they essentially transmit only when the target radio system is communicating. To achieve this, the jammer must have integrated electromagnetic support measures (ESM) capabilities that monitor the spectrum for signals to intercept. This adds complexity to the jamming system. Reactive jammers can be protocol-aware or not, and can employ a wide variety of jamming waveforms [2, 3, 8, 9]. There have been several implementations of reactive jammers on COTS SDRs previously [4, 8, 9].

The main advantage of reactive jammers is their increased power efficiency. This is true for all adversaries due to the reduced uptime of the jammer, but is especially true versus FHSS capable systems. Against an FHSS radio system, the reactive jammer benefits from a potentially high gain compared to conventional jammers, because it can concentrate all its power output in the instantaneous frequency band of the opposing FHSS system. The extent of this gain is equal to the ratio between the spread bandwidth and the instantaneous bandwidth [1].

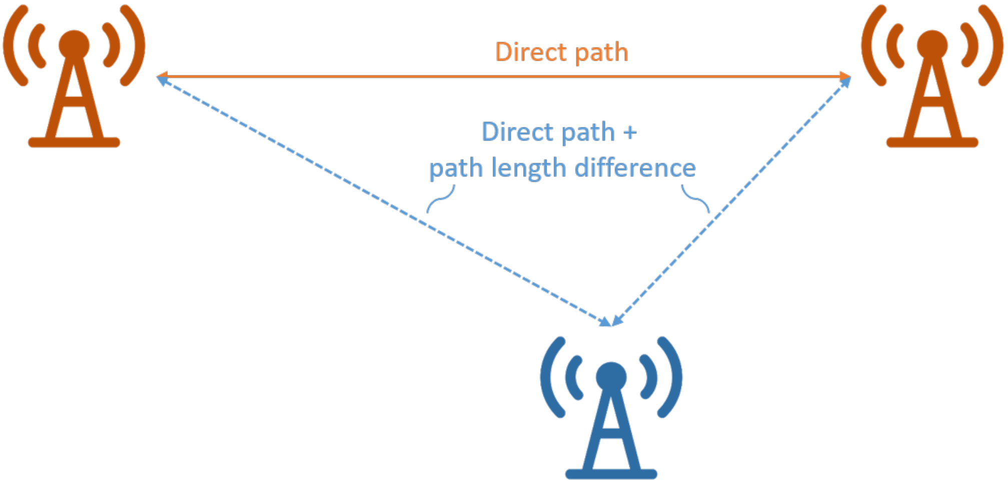


Figure 2.2 The path length difference causes the jamming waveform to reach the receiver at a delay compared to the direct path. The target radio system and the reactive jammer is depicted in red and blue respectively.

Efficient jamming of FHSS systems with a reactive jammer requires the jamming signal to overlap with the communication signal in time and frequency in the radio receiver. Ideally, the jammer signal overlaps with the communication signal at all times, but this is not achievable. Due to the path length difference between the direct signal path and the path interlinking the jammer, the jamming signal will arrive at a delay, as shown in Figure 2.2. Furthermore, the reaction time of the jammer adds additional delay to the jamming signal. A certain ratio of time-frequency overlap in the receiver is necessary in order to jam effectively. Hence, reducing the reaction time of the jammer will enable effective jamming further away from the target system.

A reactive jammer that uses the communication signal of the target system as basis for its own jamming waveform is called a repeater jammer [7]. In communications, transmitting exact copies of the radio signal is not a viable jamming strategy. Figure 2.3 illustrates how the jamming signal affect the receiver in this case. At best, this would subject the receiver to an artificial multipath environment, which could degrade some links depending on the jammer power and delay. However, more sophisticated receivers will actually improve their performance under such conditions [10], making this an unreliable jamming strategy. In order to perform an effective repeater jamming attack, the radio signals should be modified prior to retransmission, to ensure degradation of the target radio link.

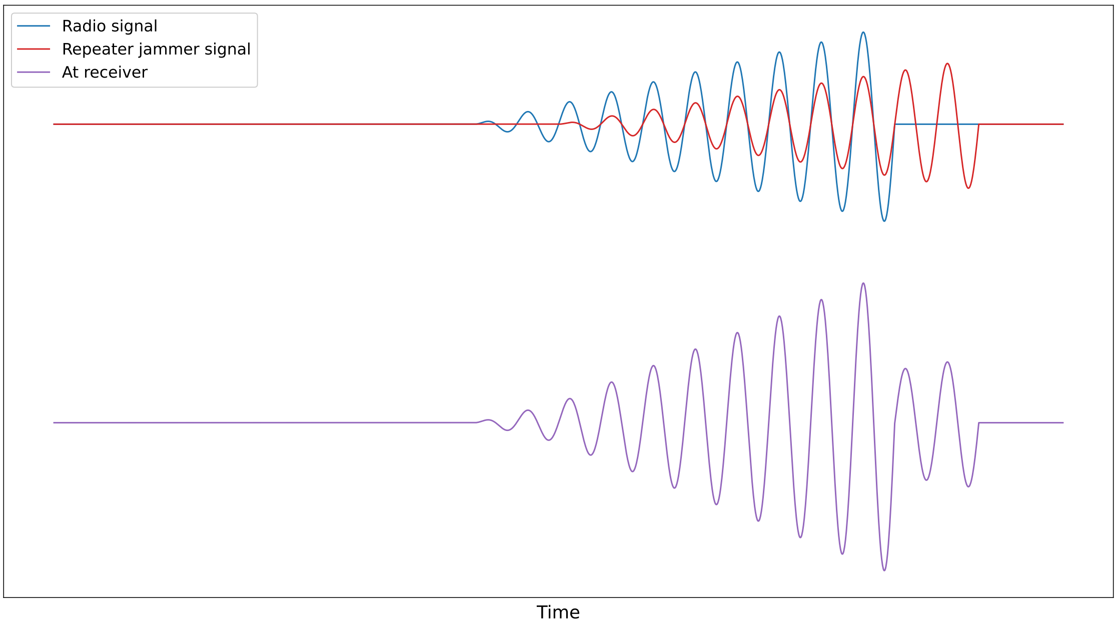


Figure 2.3 The principle of repeater jamming. Here, the jamming signal is a delayed and attenuated replica of the original signal, akin to a multipath component.

2.3 USRP & UHD

SDRs are versatile radios capable of modifying radio parameters within a wide range of values. On USRP SDRs, these parameters are configured in the USRP Hardware Driver (UHD) software. USRP is a line of SDRs produced by Ettus Research. In general, functionality implemented on one USRP unit is portable to a different model. UHD is a open source software written in C/C++, and there is also a Python API and GNU Radio support.

For newer USRP models (generation 3+), UHD can configure the FPGA of the USRP through the RF Network-on-Chip (RFNoC) API. Each version of UHD is shipped with default FPGA images, which include an assortment of blocks depending on the UHD version and USRP unit. With the RFNoC software, run time parameters of FPGA blocks can be changed, and the dynamic connections between the blocks are set. However, the number of blocks included in the default images is limited; hence the majority of the DSP must be performed in software on a host computer unless the image is modified. Transferring samples between the USRP and a host computer constitutes a bottleneck, which will significantly limit the achievable sample rate and introduce latency.

Every FPGA image consists of a number of RFNoC blocks, which can be connected by either static or dynamic connections. Static connections are not reconfigurable after the image has been synthesised, while dynamic connections are connected to a router through a stream endpoint (SEP). This router allows connections to be established and reconfigured between any two SEPs after synthesis. A series of RFNoC blocks with a set of connections constitutes a RFNoC graph. One FPGA image can contain several different RFNoC graphs.

The full capability of the USRP cannot be utilised without incorporating the FPGA in the DSP chain. In UHD there is a library of RFNoC blocks provided by Ettus, and it is possible to integrate your own blocks as well. There are also tools in UHD that streamline the process of writing your own FPGA images. However, the actual synthesis of new images requires the Vivado software, and possibly a paid license depending on the FPGA in question.

3 Experimental

This chapter consists of two parts. First, there is the latency analysis of the repeater jammer, henceforth known as Harvey. The time difference between incoming and outgoing samples is measured. Second, the jamming effectiveness of different jamming schedules is studied. To perform these measurements, the two test benches Steven and Claire were implemented in GNU Radio. In both parts, experiments were conducted solely over coaxial cables, without any antennas. An overview of all the platforms and their roles is shown in Figure 3.1. In all experiments, Harvey was controlled by an application based on the Python API in UHD 4.3.0. The master clock rate of Harvey was set to 245.76 MHz for all experiments.

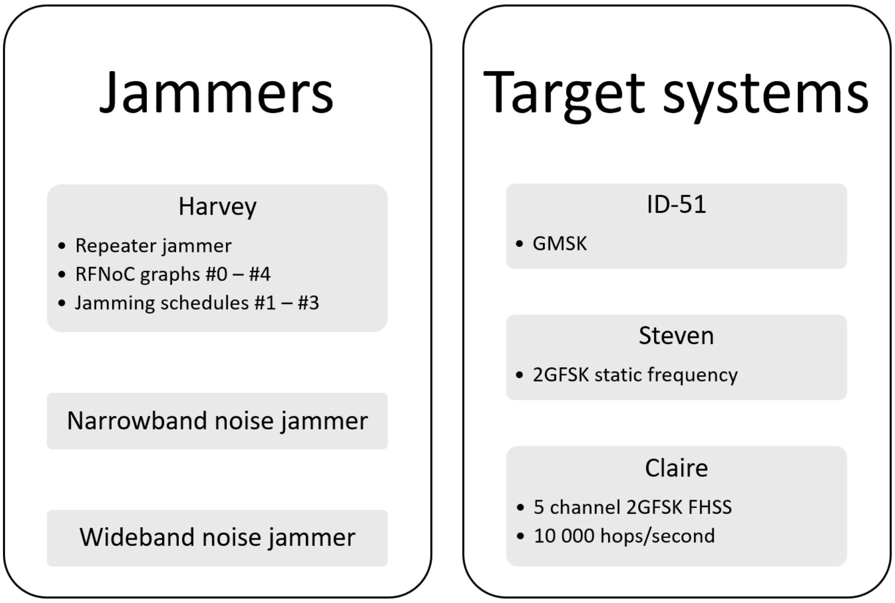


Figure 3.1 All the jammers and target systems utilised in this work.

3.1 Loopback Latency

The loopback latency of Harvey was examined using the experimental setup shown in Figure 3.2. A LimeSDR Mini produced a square wave modulated RF signal. The time difference between the radio signal and the jamming signal was measured with a Rohde & Schwarz RTA4004 oscilloscope. The experiment was repeated with different frequency square pulses to resolve any ambiguities.

The loopback latency was measured for several FPGA images, the RFNoC graphs of these images are shown in Table 3.1. Graph #0 is from the default FPGA image included in UHD 4.3.0, the other graphs are from custom images. In short, each block ID entry consist of a device number, block type, block instance number, and port number – in that order. For an in-depth explanation of these blocks and RFNoC graphs in general, the Ettus Knowledge Base is a great resource [11].

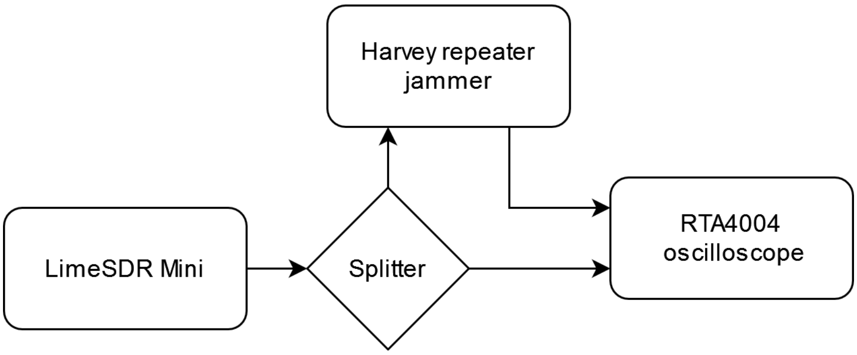


Figure 3.2 Setup for measuring the reaction time of the Harvey repeater jammer.

	RFNoC graph
#0	0/Radio#0:0==>0/DDC#0:0 0/DDC#0:0==>0/SEP#0:0 0/SEP#0:0==>0/DUC#0:0 0/DUC#0:0==>0/Radio#0:0
#1	0/Radio#0:0==>0/SEP#0:0 0/SEP#0:0==>0/Radio#0:0
#2	0/Radio#1:0==>0/Radio#1:0
#3	0/Radio#0:0==>0/DDC#0:0 0/DDC#0:0==>0/FFT#0:0 0/FFT#0:0==>0/FFT#1:0 0/FFT#1:0==>0/DUC#0:0 0/DUC#0:0==>0/Radio#0:0

Table 3.1 A summary of RFNoC *graphs referenced in this report.*

3.2 Jamming Performance

The jamming performance of Harvey has been studied with the setup sketched in Figure 3.3. Three qualitatively different jamming schedules were tested: in the first the receiver (RX) and transmitter (TX) local oscillators (LOs) were set to the same frequency, in the second the RX and TX LOs were set to different frequencies, and in the third the TX LO was changed periodically while the RX LO was kept constant. The RX LO was always set to 100 MHz, only the TX LO was changed. Power calibration was performed in the time domain using the Rohde & Schwarz FSW spectrum analyser. The power output of Harvey is tunable in steps of 1 dB, hence power calibration was rounded off to the nearest dB.

Initial investigations into the effectiveness of the repeater jammer were performed by testing the jammer against two Icom ID-51 radios. The radios were set to digital ("DV") mode, which employed a Gaussian minimum shift keying (GMSK) waveform with 4.8 kHz baud rate and bandwidth < 6 kHz. The ID-51 radios provided no measurement of the packet loss or bit error rate (BER), hence only a rough estimate of the jamming effectiveness could be inferred by this setup.

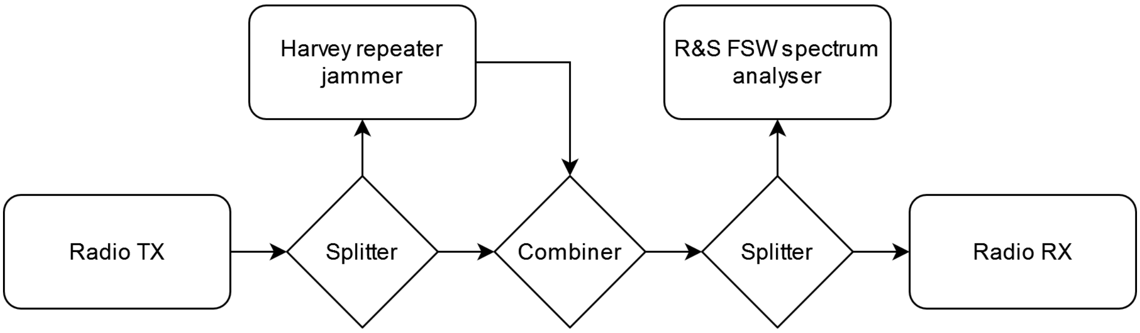
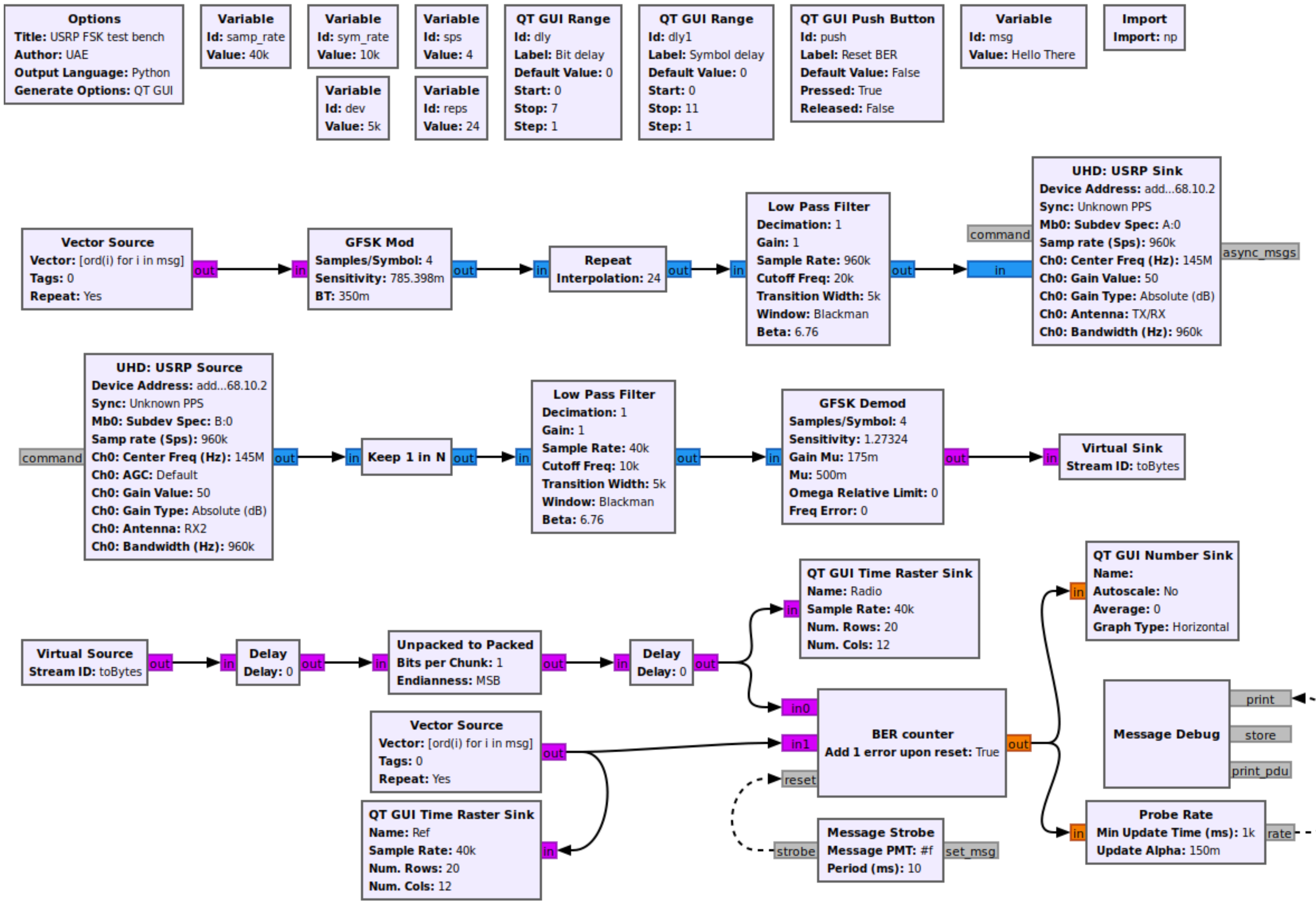


Figure 3.3 Setup for measuring the jamming performance of the repeater jammer. TX *and* RX *radios were either ID-51 radios, or the Steven or Claire test benches.*

The Steven test bench was developed in GNU Radio to measure the BER during jamming experiments. Its flow chart is shown in Figure 3.3. The test bench employs a binary Gaussian frequency shift keying (2-GFSK) waveform. In all experiments, the frequency deviation was set to 5 kHz and the baud rate was 10 kHz, which equals a modulation index of 1. The transmitter repeats the same ASCII message continuously, with no packetisation in the physical layer. The figure shows Steven being implemented on a USRP N321 SDR, but changing SDR hardware is trivial.

A second test bench called Claire was implemented in GNU Radio to study the jamming performance of the repeater jammer against FHSS systems. Its flowgraph share many similarities to the Steven flowgraph, and is shown in Figure 3.5. Claire utilises the same 2-GFSK modulation scheme, and was also set to 5 kHz frequency deviation and 10 kHz baud rate. The hopping rate was set to 10 kHz, which equates to 1 symbol per hop. 5 frequency channels were employed, and they were spaced 72.5 kHz apart.

All the blocks included in the two flow graphs of Figures 3.4 – 3.5 are part of the standard GNU Radio library, except for BER Counter and Periodic Frequency Shifter. These blocks were written in Python for these test benches specifically. The BER Counter block is mostly similar to the standard library block called BER. The one key difference is that BER Counter can reset its memory at run time with an async message. The Periodic Frequency Shifter applies a frequency shift to the input stream, and varies this shift with a set period. It is phase continuous and its frequency hopping pattern is deterministic. The block will pick frequencies from a supplied list, and go through them all before repeating.



Options
Title: USRP FSK test bench
Author: UAE
Output Language: Python
Generate Options: QT GUI

Variable
Id: samp_rate
Value: 40k

Variable
Id: sym_rate
Value: 10k

Variable
Id: dev
Value: 5k

Variable
Id: sps
Value: 4

Variable
Id: reps
Value: 24

QT GUI Range
Id: dly
Label: Bit delay
Default Value: 0
Start: 0
Stop: 7
Step: 1

QT GUI Range
Id: dly1
Label: Symbol delay
Default Value: 0
Start: 0
Stop: 11
Step: 1

QT GUI Push Button
Id: push
Label: Reset BER
Default Value: False
Pressed: True
Released: False

Variable
Id: msg
Value: Hello There

Import
Import: np

Vector Source
Vector: [ord(i) for i in msg]
Tags: 0
Repeat: Yes

GFSK Mod
Samples/Symbol: 4
Sensitivity: 785.398m
BT: 350m

Repeat
Interpolation: 24

Low Pass Filter
Decimation: 1
Gain: 1
Sample Rate: 960k
Cutoff Freq: 20k
Transition Width: 5k
Window: Blackman
Beta: 6.76

UHD: USRP Sink
Device Address: add...68.10.2
Sync: Unknown PPS
Mb0: Subdev Spec: A:0
Samp rate (Sps): 960k
Ch0: Center Freq (Hz): 145M
Ch0: Gain Value: 50
Ch0: Gain Type: Absolute (dB)
Ch0: Antenna: TX/RX
Ch0: Bandwidth (Hz): 960k

UHD: USRP Source
Device Address: add...68.10.2
Sync: Unknown PPS
Mb0: Subdev Spec: B:0
Samp rate (Sps): 960k
Ch0: Center Freq (Hz): 145M
Ch0: AGC: Default
Ch0: Gain Value: 50
Ch0: Gain Type: Absolute (dB)
Ch0: Antenna: RX2
Ch0: Bandwidth (Hz): 960k

Keep 1 in N

Low Pass Filter
Decimation: 1
Gain: 1
Sample Rate: 40k
Cutoff Freq: 10k
Transition Width: 5k
Window: Blackman
Beta: 6.76

GFSK Demod
Samples/Symbol: 4
Sensitivity: 1.27324
Gain Mu: 175m
Mu: 500m
Omega Relative Limit: 0
Freq Error: 0

Virtual Sink
Stream ID: toBytes

Virtual Source
Stream ID: toBytes

Delay
Delay: 0

Unpacked to Packed
Bits per Chunk: 1
Endianness: MSB

Delay
Delay: 0

QT GUI Time Raster Sink
Name: Radio
Sample Rate: 40k
Num. Rows: 20
Num. Cols: 12

Vector Source
Vector: [ord(i) for i in msg]
Tags: 0
Repeat: Yes

QT GUI Time Raster Sink
Name: Ref
Sample Rate: 40k
Num. Rows: 20
Num. Cols: 12

BER counter
Add 1 error upon reset: True

Message Strobe
Message PMT: #f
Period (ms): 10

QT GUI Number Sink
Name:
Autoscale: No
Average: 0
Graph Type: Horizontal

Message Debug

Probe Rate
Min Update Time (ms): 1k
Update Alpha: 150m

Figure 3.4 The GNU Radio Companion flowchart of the Steven test bench employed in jamming performance experiments. It produces a static frequency 2-GFSK *signal.*

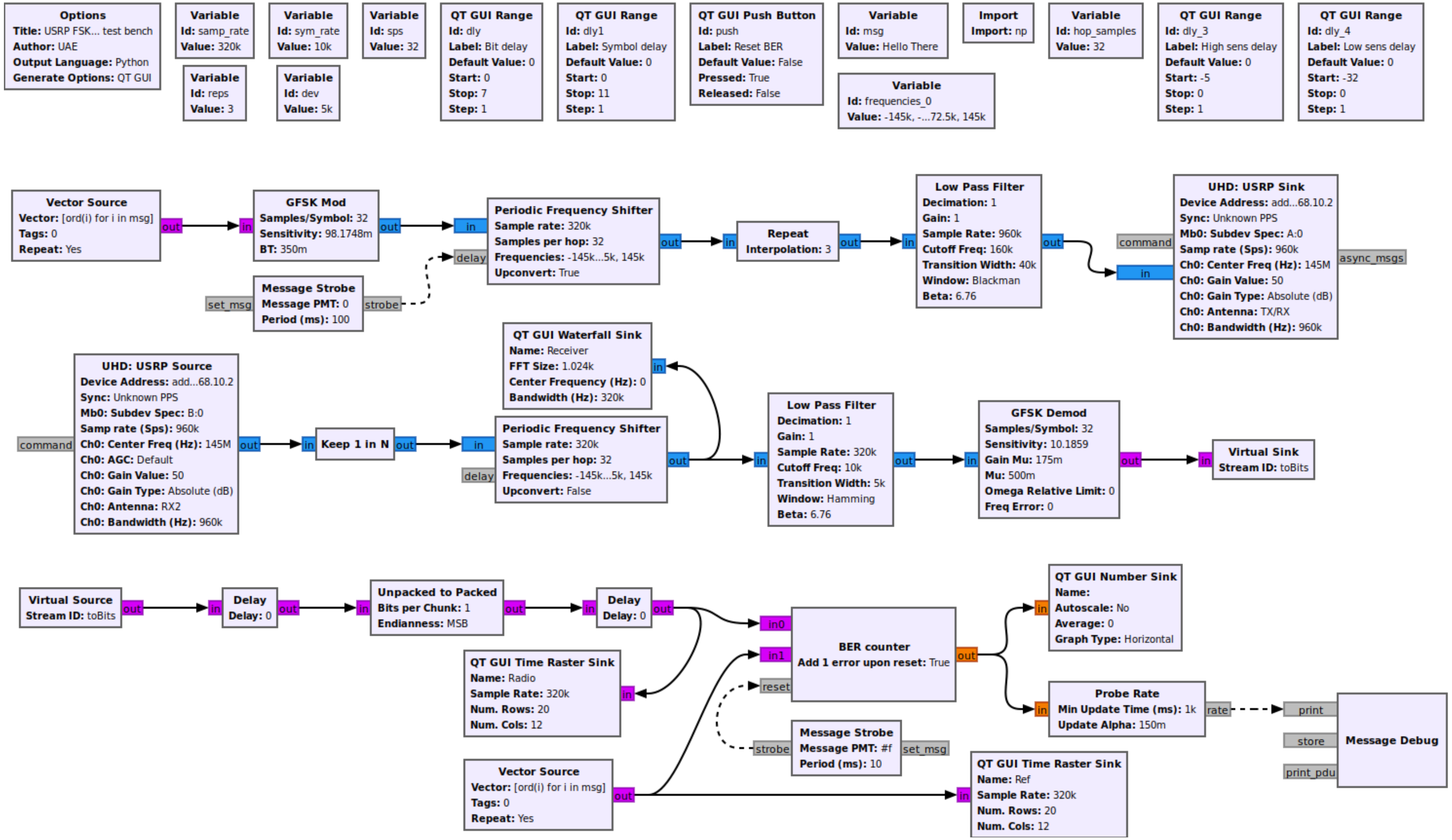


Figure 3.5 The GNU Radio Companion flowchart of the Claire FHSS *test bench employed in jamming performance experiments. It produces a frequency hopping* 2-GFSK *signal.*

4 Results and Evaluation

4.1 Reaction Time

Initial experimentation with the Harvey jammer aimed at estimating and improving the loopback latency resulting from capturing samples at the RX side, and then retransmitting those samples at the TX side. This loopback latency, or the reaction time of the jammer, is a key performance indicator. Faster reaction time enables effective jamming of FHSS systems with higher hopping rates, or allows the jammer to remain effective with a longer path length difference.

Several improvements has been made to the base configuration of the N321 to optimise the loopback latency of Harvey. Factors that have been identified to contribute latency are:

1. Data packets were transferred between the SDR and the host computer
2. DSP processes were performed in software by the host computer
3. The default number of samples per packet (SPP) is large
4. The default FPGA image is designed for versatility rather than latency optimisation

In particular, the transfer of data packets between the SDR and the host computer is undesirable. While the N321 has up to 200 MHz instantaneous bandwidth, if data is streamed between the SDR and the host computer, the achievable samples rate is much lower. Additionally, the delay introduced by transferring the data back and forth is highly variable, which is not ideal. Depending on the computational complexity of the DSP blocks, the sample rate can also be limited by the processing time on the host computer as well. Hence, the first step towards reducing the loopback latency is to implement all DSP blocks in the on-board FPGA, thereby eliminating the need to export data packets out of the SDR.

SPP	Loopback latency [µs]
2044	9.79 ± 0.04
1024	5.65 ± 0.02
64	1.71 ± 0.02
16	1.51 ± 0.02
4	1.48 ± 0.02

Table 4.1 Loopback latency for RFNoC *graph #2, with varying* SPP.

With the entire DSP chain contained within the SDR, the next significant improvement to the loopback latency comes from the reduction in the number of SPP. The default value of SPP is the maximum, which for the N321 is 2044. However, this can be reduced for applications that require low latency, at the cost of increasing overhead. Table 4.1 shows how SPP affect the loopback latency of Harvey, instrumented with RFNoC graph #2 from Table 3.1. The lowest SPP value the USRP can handle seems to vary depending on the RFNoC graph, and for graph #2 the lowest SPP achieved was 4. Higher SPP values introduce a longer packetisation delay, because the samples are waiting in a buffer for the packet to be filled. With a 245.76 MHz sample rate, the expected packetisation delay added by increasing the the SPP by 1 is the sampling period $\tau_s = (245.76 MHz)^{-1} = 4.07 \cdot 10^{-3}$ µs. The measured latency increases linearly with increasing SPP as expected; a best fit linear regression model of the measurements $y = ax + b$ has $a = 4.08 \cdot 10^{-3}$ and $b = 1.46$.

Another optimisation, which acts to reduce the overall loopback latency slightly, is redesigning the default FPGA image. RFNoC graph #0 is from the default FPGA image, and this graph has static connections between the radio blocks and digital down-converter (DDC)/digital up-converter (DUC) blocks. Downconverting the incoming RX samples is unnecessary if they are simply being retransmitted. RFNoC graphs #1 and #2 removed this versatility from the default image in order to reduce latency. In RFNoC graph #1 the DDC & DUC blocks are removed, and in graph #2 the connection between the radio blocks is changed from a dynamic connection to a static connection. More compact designs are possible with static connections, which are not connected to the router. The measured latency of these three RFNoC graphs with SPP of 28 is shown in Table 4.2. The simpler RFNoC graphs cause less delay as expected. 28 SPP was employed for this comparison, because it is the lowest value successfully applied to all the RFNoC graphs. Also, the decimation is set to a factor of 1 in the DDC included in RFNoC graph #0, likewise for the DUC interpolation; this way the graphs are more comparable, because decimation and interpolation add an additional latency component. The absolute fastest reaction time measured for any configuration of the repeater jammer is 1.48 µs, obtained using RFNoC graph #2 and 4 SPP.

RFNoC graph	Loopback latency [µs]
#0	2.81 ± 0.02
#1	1.93 ± 0.05
#2	1.63 ± 0.04

Table 4.2 Loopback latency for different RFNoC *graphs, with 28* SPP.

Harvey has an instantaneous bandwidth of 200 MHz; while capturing a large slice of spectrum is great for monitoring an opposing FHSS radio system, it also means that many interfering signal sources are likely to be captured as well. It is not ideal for the repeater jammer to transmit energy in the frequency band of these other interfering sources. In order to provide frequency selectivity, RFNoC graph #3 was developed with a pair of fast Fourier transform (FFT) blocks. The first FFT block is set to the forward direction, and the second is set to the inverse direction. The loopback latency of RFNoC graph #3 has been measured for various FFT sizes, the results are shown in Figure 4.3. The DDC decimation factor was set to 2 for these measurements, because the full 245.76 MHz sample rate through the FFT blocks caused a crash. The latency was measured for all possible FFT sizes, from 16 to 1024. Worth noting is that the SPP will always be the same numerical value as the FFT size for RFNoC graphs which include FFT blocks. The SDR uses packets as delimiters for each FFT frame in the DSP chain, which is necessary in order to affiliate each I/Q sample with its corresponding FFT frequency bin. Hence, a 2048-FFT is not possible, because the maximum SPP of the N321 is 2044.

FFT size	Loopback latency [µs]
16	3.78 ± 0.02
32	4.75 ± 0.012
64	6.03 ± 0.014
128	8.83 ± 0.02
256	14.02 ± 0.02
512	24.61 ± 0.02
1024	45.43 ± 0.03

Table 4.3 Loopback latency of RFNoC *graph #3, for different length* FFT*s.*

4.2 Effectiveness of Jamming

The effectiveness of Harvey has been studied against three target systems: ID-51 radios, and the Steven and Claire test benches. The first jamming tests were performed against the ID-51 radios. These radios have a digital mode that utilises a GMSK waveform, which is a subcategory of FSK. FSK waveforms are commonly applied by FHSS systems; hence the ID-51 radios were expected to yield some useful insight into the effectiveness against FHSS systems. However, the ID-51 radios do not provide any quantitative estimates of the jamming effectiveness. To address this, the Steven test bench capable of quantifying the jamming effectiveness was implemented using GNU Radio. Lastly, the Claire test bench was created to study the performance of the repeater jammer against FHSS systems.

Three different jamming schedules were implemented on Harvey, and their effectiveness versus the ID-51 radio link was investigated. Experiments with these schedules were conducted with both RFNoC graphs #2 and #3. However, because the performance of the two RFNoC graphs is very similar, the results reported herein are solely from measurements with RFNoC graph #3. RFNoC graph #3 is expected to be the most useful overall, due to the versatility of the FFT blocks. A summary of the effectiveness of these jamming schedules is shown in Table 4.4. Measuring the jammer power at which the target radio system is "jammed" is not straight forward. As jammer power increases, the BER also increases, and at some point, this will render the radio system useless due to a critical number of errors. There is a transition region between the not jammed and completely jammed states. Hence, a methodology must be adopted to make measurements of the jamming effectiveness comparable. The ID-51 radios are able to transmit a call sign by the click of button. The experiments were conducted by transmitting this call sign on repeat for 30 seconds. The minimum required jamming power is the lowest jamming power which lets at most one correct call sign through in that time period. To be clear: the radio system is still somewhat functional at this jammer power; voice transmissions are not scrambled to the point of being completely inaudible.

The first jamming schedule had Harvey transmitting exact copies of the received radio signal. Due to the reaction time of the repeater jammer, this copy of the original radio signal will reach the intended receiver at a delay. This essentially creates an artificial multipath environment with one reflection. The "reflection" can be either weaker or stronger than the original signal depending on the jammer power. This jamming schedule did not prove effective for any jammer power. This might be because the time dispersion introduced by the repeater jammer (< 10 µs) is small compared to

Schedule description	Min. required jamming power	Comment
#1 Artificial multipath	N/A	No effect
#2 Artificial multipath w/ Doppler	-13 dB J/S	Ineffective at high power
#3 Artificial multipath w/ varying Doppler	-11 dB J/S	1 ms hop period
Narrowband noise jammer	-7 dB J/S	Included for reference

Table 4.4 The effect of different jamming schedules on ID-51 GMSK *radios. The numbered schedules utilised the Harvey repeater jammer, equipped with* RFNoC *graph #3.*

the symbol time of the ID-51 radios (208 µs), hence the resulting intersymbol interference is not very significant.

The second schedule, introduced a Doppler shift in the jamming signal, by setting the RX & TX LOs to different frequencies. This is a trivial method of modifying the received signal at the repeater jammer, without affecting the reaction time. The frequency shift obviously has to be less than the bandwidth of the radio signal, to ensure frequency overlap with the radio signal. With a 64-FFT and a frequency shift of 2 kHz, this jamming schedule has minimum required jamming power of -13 dB jamming to signal ratio (J/S). With increasing J/S, the link degradation increased as expected. However, at J/S > 0, the trend reversed and the radio performance improved as the jammer power increased. Low jamming powers naturally has no effect, but high jamming powers are also ineffective. The artificial Doppler multipath jamming schedule is only effective when the incoming jammer power at the intended receiver is similar to the incoming radio power. When the jamming power is too high, the receiver can simply retune its LO to the jammer frequency to receive an error free message. Controlling the incoming power at the receiver would require the jammer to know the channel between the RX & TX radio system, and the channel between itself and the RX radio – which is extremely difficult, and in practice impossible due to incomplete information. Hence, this jamming schedule is not viable either.

To address the shortcomings of the second schedule, the third jamming schedule changed the Doppler shift introduced by the jammer periodically. With a varying Doppler shift, it is not trivial for the intended receiver to tune its frequency to compensate for the jammer signals. The frequency shift was changed every 1 ms. This was achieved by retuning the TX LO, which causes some interruptions to the uptime due to the retuning process, which was about 30–40 µs. An improvement on this design would be to implement the frequency translation process in the DSP chain of the FPGA to avoid this retuning. The frequency shifts applied in this experiment were randomly generated in the range $\pm[2, 3]$ kHz (aka. either ranges [-3, -2] kHz or [2, 3] kHz, including endpoints), and a 64-FFT was employed. Using this jamming schedule, the minimum required jamming power was -11 dB J/S, which is a slightly more than for the second schedule. However, this jamming schedule does not suffer from decreased performance at high jammer powers (J/S > 0), which is what makes this a viable jamming strategy. For this reason, only this jamming schedule has been employed in subsequent jamming performance experiments.

For added reference, a noise jammer was tested against the same radio link; the minimum required jamming power was -7 dB J/S, which is 4 dB higher than Harvey with the third jamming schedule. These results indicate that the repeater jammer is more efficient than Gaussian noise against the GMSK waveform of the ID-51, which is quite remarkable.

Experiments similar to the ones with ID-51 radios were conducted with the Steven 2-GFSK test bench implemented in GNU Radio, in order to measure the BER and quantify the effectiveness of different jamming parameters. This test bench was first implemented on a LimeSDR platform, but due to difficulties in reproducing results with the LimeSDR, the platform was later changed to a USRP N321. The N321 has two separate channels, so for both the Steven and Claire test benches, one channel was RX, and the other was TX. This is not the same N321 unit used for the Harvey jammer, but rather a second unit.

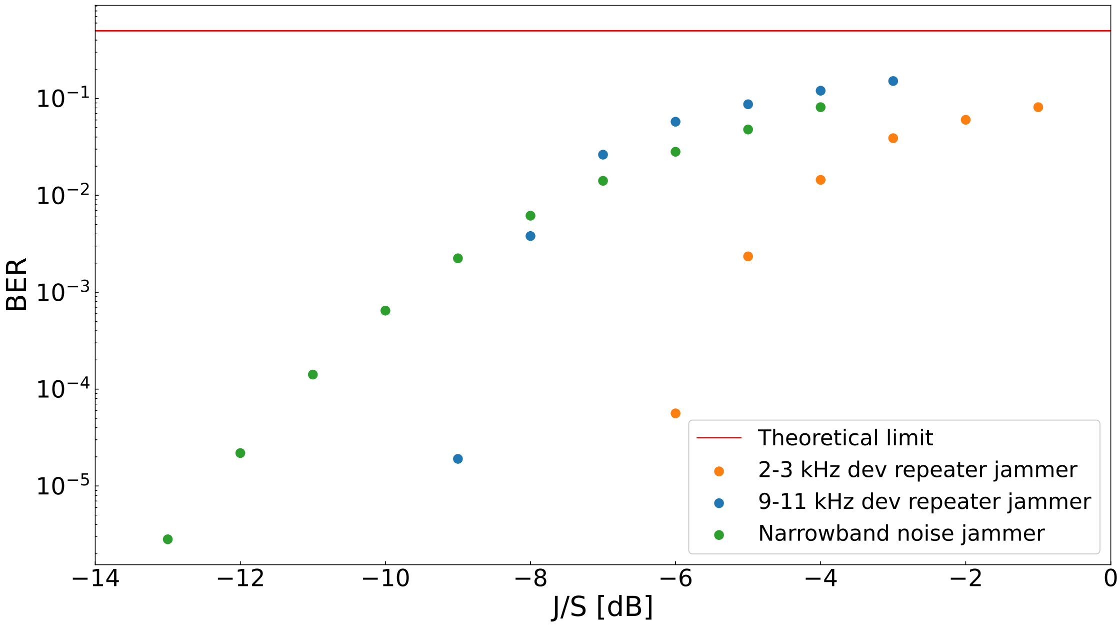
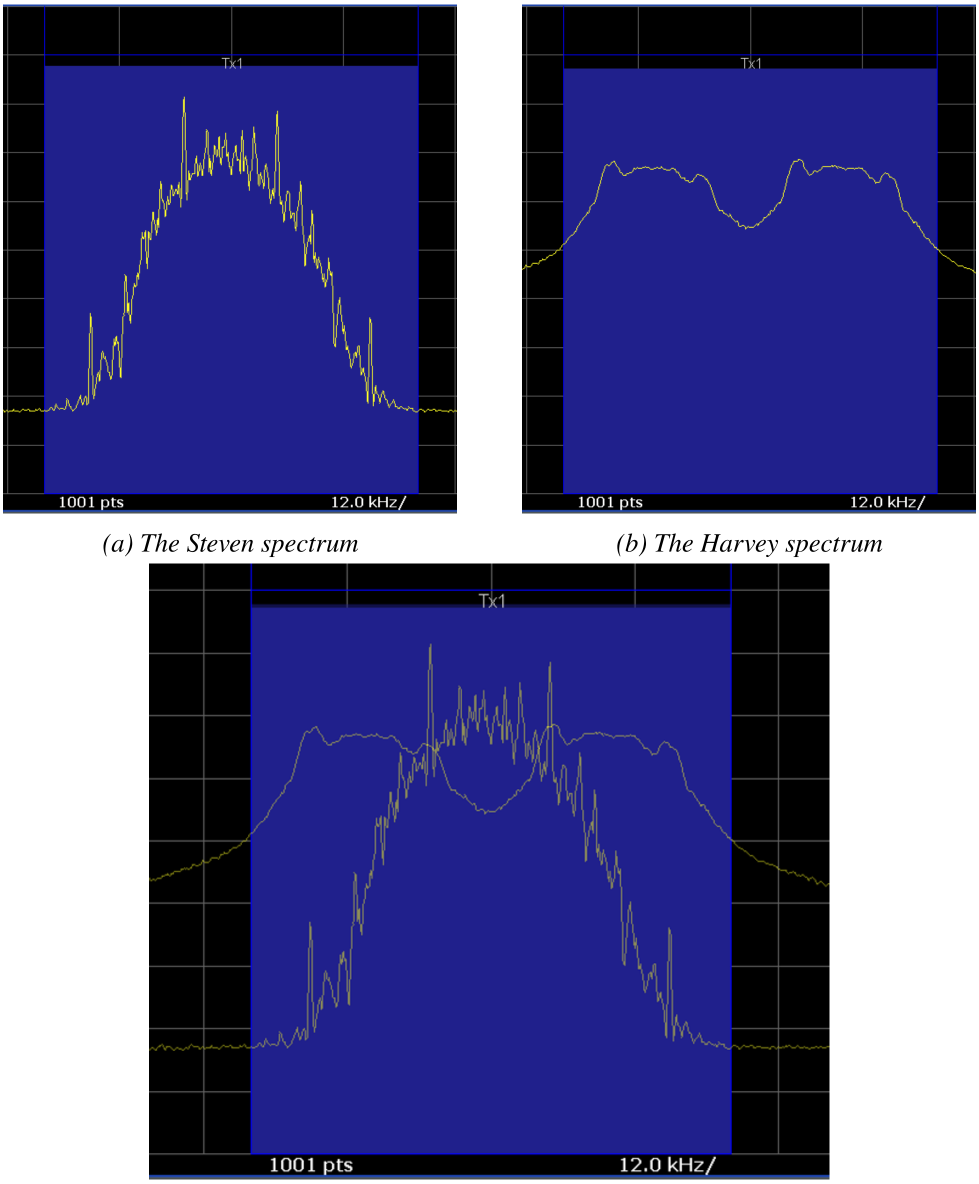


Figure 4.1 BER *of the Steven test bench in presence of the Harvey jammer and a narrowband noise jammer.*

The jamming effectiveness of Harvey and a narrowband noise jammer have been studied using the Steven test bench. The measured BER as a function of J/S is shown in Figure 4.1. The 99% bandwidth of the 2-GFSK signal was approximately 16 kHz. Therefore, the noise jammer signal was also 16 kHz wide. The hop period of Harvey was set to 10 ms, and different frequency deviation ranges were applied. One configuration of the repeater jammer employed the same $\pm[2, 3]$ kHz frequency deviation used against the ID-51 radios previously. However, here the effectiveness of these jamming parameters is lower than the noise jammer. A different configuration with $\pm[9, 11]$ kHz frequency deviation showed improved jamming performance, which surpasses that of a noise jammer at high J/S. BER measurements below 10^{-6} are not performed due to the long acquisition time necessary with the 10 kHz baud rate. The jamming performance of Harvey quickly diminishes at lower J/S. The steepness of the BER curves causes the reading to quickly fall below this 10^{-6} threshold.

Experimentation with different frequency deviations revealed that the jamming effectiveness rose considerably as the deviation was increased from the initially applied $\pm[2, 3]$ kHz. The reason for this is likely that the ID-51 and Steven test bench employ different frequency deviations. The ID-51 GMSK waveform has a baud rate of 4.8 kHz, which corresponds to a frequency deviation of 1.2 kHz. The 2-GFSK waveform of Steven has 5 kHz frequency deviation. When Harvey



(a) The Steven spectrum

(b) The Harvey spectrum

(c) Both spectra

Figure 4.2 Time-averaged spectra of (a) the Steven target system, (b) the $\pm[9, 11]$ *kHz deviation Harvey jammer response, and (c) the two spectra overlayed.*

applies a ±[9, 11] kHz frequency deviation, the jamming performance is several dB better than in the ±[2, 3] kHz case. ±[9, 11] kHz is about twice the frequency deviation of Steven. This observation is perhaps not very surprising, and is explainable by examining the radio and jammer spectra, shown in Figure 4.2. Notice how the Harvey spectrum is essentially two smoother copies of the Steven spectrum, frequency translated 10 kHz up and down in frequency. The frequency translation applied by Harvey is in this case equal to the frequency separation between the mark and space frequencies of Steven. The effect of this is that Harvey has a 50% chance to retransmit energy received at the mark frequency, at the space frequency, and the other way around. In Figure 4.2c, the high power spectral density of the repeater jammer in the proximity of the mark and space frequencies (the two sharp peaks in the Steven spectrum) is clearly visible.

There is a significant difference in jamming effectiveness of the repeater jammer depending on the frequency deviation applied by the jammer. Furthermore, the optimal frequency deviation of the repeater jammer is determined by the waveform of the target radio system. The implication of this is that a capable repeater jammer should be able to measure the frequency deviation of any given adversary, and adjust its own deviation in response. This of course, assumes that the adversary is even employing a FSK modulation scheme, which a repeater jammer also should be able to assert. This can be achieved by integrating a signal classification system. The target system is not expected to alter modulation scheme nor frequency deviation rapidly during operation, therefore the signal classification operation does not face the same time-constraints as the main DSP chain of the repeater jammer.

The Harvey jammer has up to 200 MHz instantaneous bandwidth, reaction time in the order of microseconds, and proven good jamming performance against FSK waveforms. These are qualities that in principle should enable the jammer to be effective against FHSS systems, as long as the hopping rate of the target system does not exceed some critical value. To validate the effectiveness against such systems, the Claire test bench, which changes frequency channels periodically, was developed in GNU Radio for the N321.

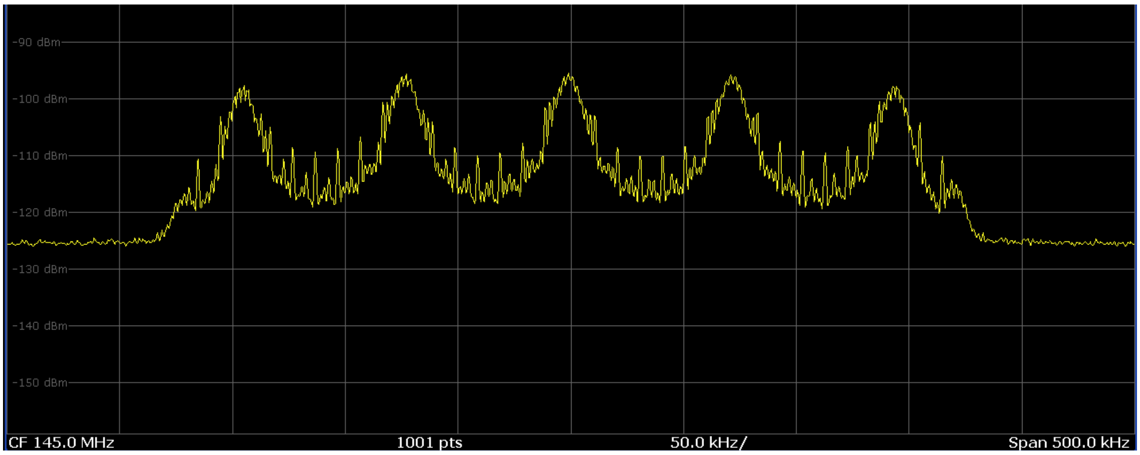


Figure 4.3 Time-averaged spectrum of the Claire test bench with 5 frequency channels.

Claire was configured to hop between 5 frequency channels with 72.5 kHz separation. The 99% spread bandwidth was approximately 315 kHz, and the hopping rate was 10 kHz. The spectrum generated in this configuration is shown in Figure 4.3. Claire produces a 2-GFSK waveform similar to the one by Steven, but the signal is frequency translated in intervals of 72.5 kHz. Harvey applied similar parameters as previously: 10 ms hop period and ±[9, 11] kHz frequency deviation. The BER induced in the Clarie test bench by Harvey and a 315 kHz wideband noise jammer is presented in Figure 4.4. The power advantage of Harvey against FHSS systems is apparent from the figure, with 7–11 dB less power required compared to the noise jammer. Target systems with larger spread bandwidth is expected to further increase the outperformance of Harvey.

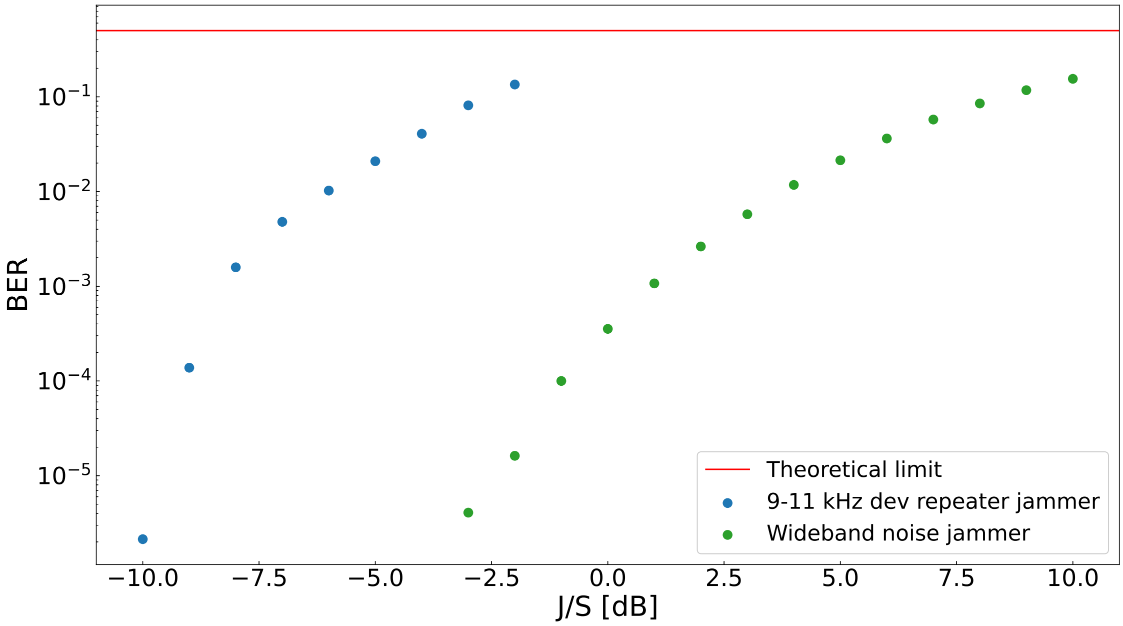


Figure 4.4 BER *of the Claire test bench in presence of the Harvey jammer and a wideband noise jammer.*

The jamming performance of Harvey with ±[9, 11] kHz frequency deviation against Claire is mostly unchanged compared to the experiment with Steven. The most notable effect of a frequency hopping target system on the repeater jammer, is the reduction in time-frequency overlap. In this laboratory setup. there is no propagation delay, so the reaction time is equal to the total delay. From latency measurements, we know that the 64-FFT architecture used in the jamming experiments introduce a 6.03 µs delay. The radio signals will be free from interference from Harvey in this time period, until it is able to react to the shift in frequency. However, the delay is in this case small compared to the 100 µs duration of a single frequency hop of Claire. The time-frequency overlap of Harvey and Claire was 94% in this experiment. Hence, it is understandable that the performance of Harvey is similar against Steven and Claire. Of course, the situation is quite different for the noise jammer, which has to cover a much wider bandwidth when jamming Claire. The necessary power output of the noise jammer is expected to increase about 13 dB when increasing the bandwidth from one 16 kHz channel, to five channels spanning 315 kHz. The measured difference is a little less at 10–12 dB. This discrepancy indicates that a lower channel noise power spectral density is sufficient to jam the FHSS Claire test bench, compared to the static frequency Steven test bench. Perhaps due to noise components stemming from the frequency hopping, or synchronisation errors.

Outside of laboratory conditions however, a repeater jammer will not actually know the time-frequency overlap in the receiver, because there will be an unknown propagation delay in addition to the repeater jammer reaction time. If the propagation delay is high, the time-frequency overlap might be small or even zero, which renders the repeater jammer ineffective. A capable repeater jamming system should avoid this situation by including ESM systems, which locate the adversary and estimate the propagation delay. The jammer might have to change jamming technique, if repeater jamming is impossible due to a high propagation delay.

The ability of Harvey to degrade FSK links, and the gain it experiences due to being time-correlated has been demonstrated. However, it is important to acknowledge that in order for the repeater jammer to perform as well in a real environment as herein, the jammer must be able to operate without look-through. If the jammer has to stop transmitting to perform acquisition, delays far greater than the loopback latencies reported in this report are introduced. A jammer capable of this is called a Full-Duplex jammer, and is a research topic in its own right. Antenna isolation, and digital and analogue self-interference cancellation techniques are strategies which are used to combat the issue of self-interference.

5 Conclusion

A repeater jammer has been implemented on a USRP N321 COTS SDR. The performance of the repeater jammer has been evaluated based on the reaction time and jamming effectiveness. The user-programmable FPGA of the N321 was reconfigured in order to reduce the loopback latency of the system, and the effectiveness of different jamming schedules was tested. Two test benches were developed in GNU Radio in order to evaluate the performance of the jammer. Based on the findings, the conclusions are:

- It is possible to achieve low latency in the order of microseconds on a USRP N321 SDR, by containing the DSP chain in its entirety on the SDR hardware.
- Some factors which influence the loopback latency of the repeater jammer are: SPP, FFT size, FPGA image design. Reducing latency is important to enable jamming of rapidly frequency hopping adversaries.
- Against 2-GFSK signals, repeater jammer waveforms can be as effective as Gaussian noise concentrated in the active channel.
- A repeater jammer is capable of jamming FHSS systems with wide spread bandwidths much more efficiently than a noise jammer, as long as the time-frequency overlap of the repeater jammer and target system is sufficient.
- In order to reach its full potential, a repeater jammer should operate in full-duplex mode, and be supported by signal classification and target localisation ESM systems.

Acronyms

2-GFSK	binary Gaussian frequency shift keying
BER	bit error rate
COTS	commercial-off-the-shelf
DDC	digital down-converter
DSP	digital signal processing
DUC	digital up-converter
ECM	electromagnetic countermeasures
EPM	electromagnetic protective measures
ESM	electromagnetic support measures
FFT	fast Fourier transform
FHSS	frequency-hopping spread-spectrum
FPGA	field-programmable gate array
FSK	frequency shift keying
GMSK	Gaussian minimum shift keying
J/S	jamming to signal ratio
LO	local oscillator
RF	radio frequency
RFNoC	RF Network-on-Chip
RX	receiver
SDR	software-defined radio
SEP	stream endpoint
SPP	samples per packet
TX	transmitter
UHD	USRP Hardware Driver

References

[1] M. Spellman, “A comparison between frequency hopping and direct spread PN as antijam techniques,” *IEEE Communications Magazine*, vol. 21, no. 2, pp. 37–42, 1983.

[2] J. Marin, M. Heino, J. Saikanmäki, M. Mäenpää, A.-P. Saarinen, and T. Riihonen, “Perfecting jamming signals against RC systems: An experimental case study on FHSS with GFSK,” in *2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications*. IEEE, 2020, pp. 1–5.

[3] J. Marin, M. Turunen, M. Bernhardt, and T. Riihonen, “Self-interference cancelation performance in full-duplex jamming and spectrum monitoring,” in *2021 International Conference on Military Communication and Information Systems (ICMCIS)*. IEEE, 2021, pp. 1–8.

[4] K. Pärlin, M. M. Alam, and Y. Le Moullec, “Jamming of UAV remote control systems using software defined radio,” in *2018 International Conference on Military Communications and Information Systems (ICMCIS)*. IEEE, 2018, pp. 1–6.

[5] R. Poisel, *Modern communications jamming principles and techniques*. Artech house, 2011.

[6] H. Li, H. Han, J. Lu, and Y. Hao, “Analysis of coherent fast frequency hopping communication system,” in *2021 IEEE 4th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, vol. 4. IEEE, 2021, pp. 880–884.

[7] M. Lichtman, J. D. Poston, S. Amuru, C. Shahriar, T. C. Clancy, R. M. Buehrer, and J. H. Reed, “A communications jamming taxonomy,” *IEEE Security & Privacy*, vol. 14, no. 1, pp. 47–54, 2016.

[8] D. Nguyen, C. Sahin, B. Shishkin, N. Kandasamy, and K. 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*, 2014, pp. 15–22.

[9] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, “Short paper: Reactive jamming in wireless networks: How realistic is the threat?” in *Proceedings of the fourth ACM conference on Wireless network security*, 2011, pp. 47–52.

[10] R. Price and P. E. Green, “A communication technique for multipath channels,” *Proceedings of the IRE*, vol. 46, no. 3, pp. 555–570, 1958.

[11] Ettus Knowledge Base contributors, “Getting started with RFNoC in UHD 4.0,” 2022, [Online; accessed 28-February-2023]. [Online]. Available: https://kb.ettus.com/index.php?title=Getting_Started_with_RFNoC_in_UHD_4.0&oldid=5261

About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

FFI's mission

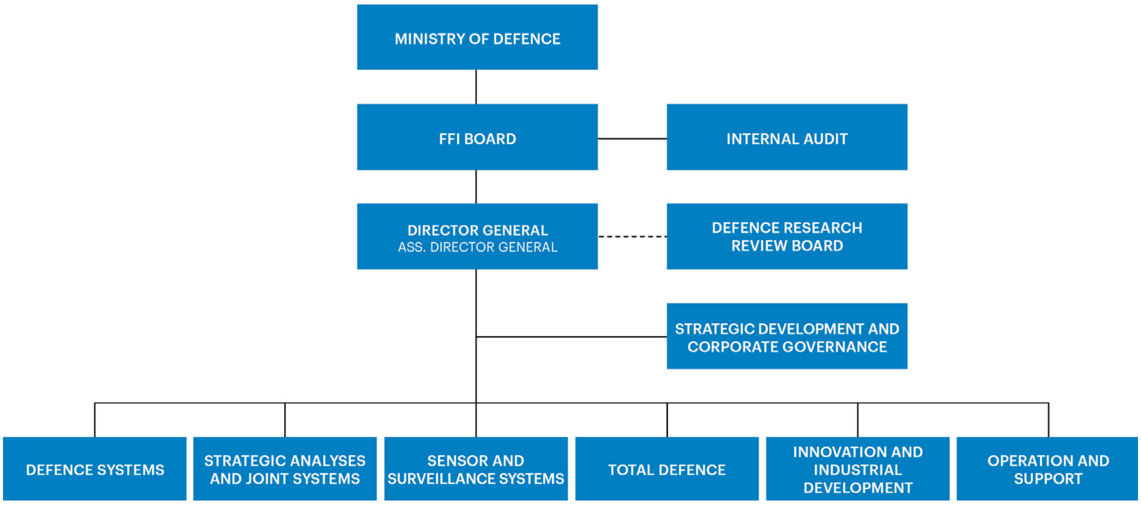
FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

FFI's vision

FFI turns knowledge and ideas into an efficient defence.

FFI's characteristics

Creative, daring, broad-minded and responsible.


MINISTRY OF DEFENCE

FFI BOARD

INTERNAL AUDIT

DIRECTOR GENERAL
ASS. DIRECTOR GENERAL

DEFENCE RESEARCH REVIEW BOARD

STRATEGIC DEVELOPMENT AND CORPORATE GOVERNANCE

DEFENCE SYSTEMS

STRATEGIC ANALYSES AND JOINT SYSTEMS

SENSOR AND SURVEILLANCE SYSTEMS

TOTAL DEFENCE

INNOVATION AND INDUSTRIAL DEVELOPMENT

OPERATION AND SUPPORT

Forsvarets forskningsinstitutt (FFI)
Postboks 25
2027 Kjeller

Besøksadresse:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telefon: 91 50 30 03
E-post: post@ffi.no
ffi.no

Norwegian Defence Research Establishment (FFI)
PO box 25
NO-2027 Kjeller
NORWAY

Visitor address:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telephone: +47 91 50 30 03
E-mail: post@ffi.no
ffi.no/en