

BEng Embedded
Electronic Systems
Advanced Digital Signal
Processing
ACDA6018
Joshua Ofosu Asare
2111739

Table of Contents

1	Introduction	3
2	Task 1 – HFSS.....	3
2.1	Background research	3
2.2	Base NBFM Modulation and Demodulation	3
2.3	Introduction of a Jammer	4
2.4	Implementation of an anti-jamming technique (FHSS)	6
2.5	Final GNU Radio implementation	7
2.6	Ethical considerations of jamming.....	7
3	Task 2 – RTL-SDR reception of local FM radio.....	7
3.1	Background research	7
3.2	FM Receiver in an SDR Block Diagram	8
3.2.1	Recap of analogue FM signal reception	8
3.2.2	Differences in SDR reception	8
3.3	FM Receiver implementation in GNU Radio	9
3.4	Ethical considerations of SDR technology.....	12
4	Conclusions	12
5	Suggested improvements	12
6	Bibliography	13

1 Introduction

This assignment examines how a communication system may be hardened against noise present at a particular frequency using Frequency Hopping Spread Spectrum (FHSS), and separately how a USB RTL-SDR may be used to receive audio from a local radio station.

2 Task 1 – HFSS

2.1 Background research

Narrowband Frequency Modulation (NBFM) gets its name from the properties the FM signals that are being transmitted have. Narrowband FM has “narrow” in the name because the frequency deviation is narrower than in other FM implementations [1]. This means that NBFM can be used for applications such as FM radio and point to point communication where bandwidth may be limited.

2.2 Base NBFM Modulation and Demodulation

Figure 1 below shows the sample audio file, a Cisco Jabber ringtone, after it has been demodulated.

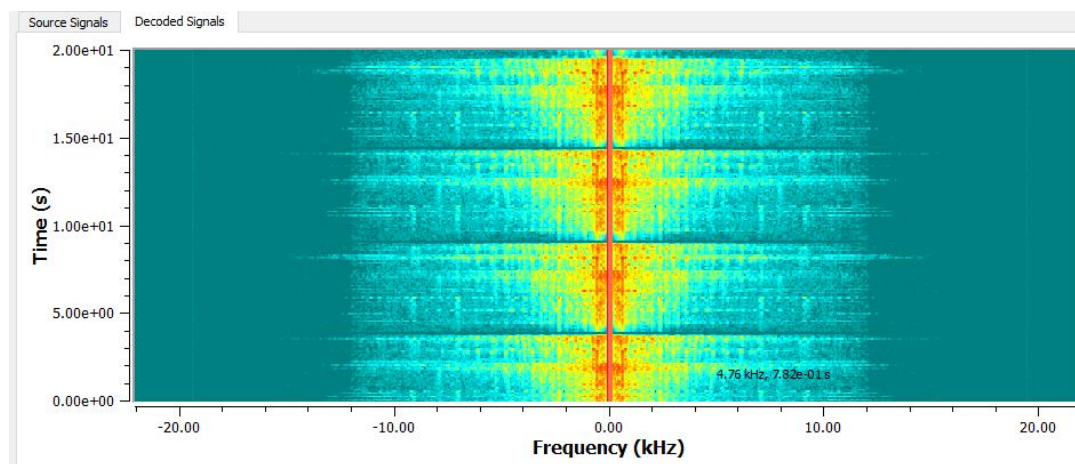


Figure 1: Waterfall sink showing the repeating Cisco Jabber ringtone

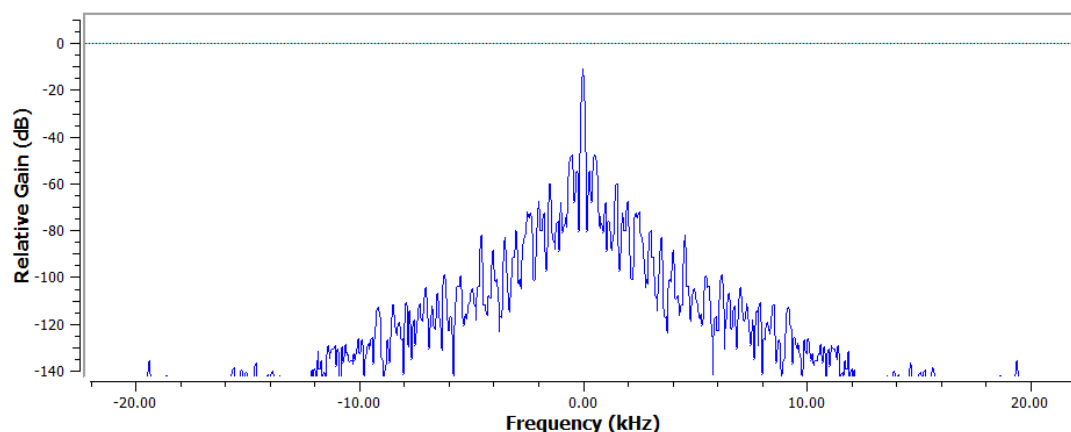


Figure 2: Frequency sink in GNU Radio showing the demodulated signal

The frequency deviation of the signal is 22,050 Hz, shown below.

$$\Delta f = k_f * A_f$$

$$k_f = \text{Modulation index}$$

$$A_m = \text{Audio frequency}$$

Equation 1: Frequency deviation [2]

$$\Delta f = 0.5 * 44,100$$

$$= 22,050 \text{ Hz}$$

The bandwidth of the signal is 88,200 Hz, calculated below:

$$B_T = 2(\Delta f + f_m)$$

$$B_T = 2(22,050 + 44,100)$$

$$= 88,200 \text{ Hz}$$

2.3 Introduction of a Jammer

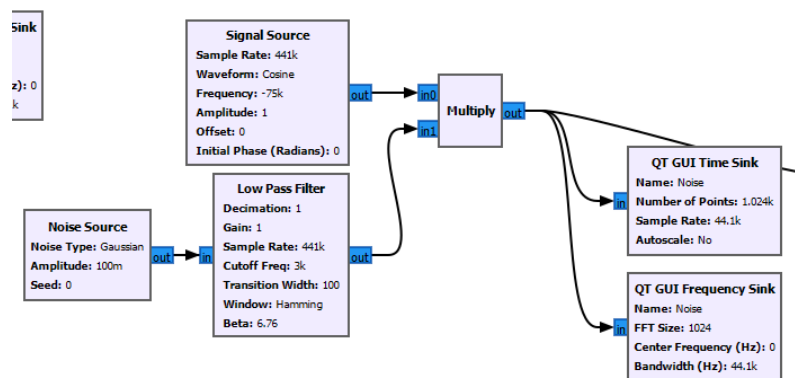


Figure 3: The blocks used to introduce a jammer in GNU Radio

The jammer introduced for this assignment has a variable power and is generated from a gaussian noise source with an amplitude of 0.1, which goes through a low pass filter that has low pass filter, so only a desired window of the original noise source will pass. The frequencies of human speech, which is often transmitted using RF, range from 85 Hz to 4-5 kHz [3]. A cutoff frequency of 3 kHz has been selected in order to jam most of the signal coming through after the noise has been mixed with the carrier frequency.

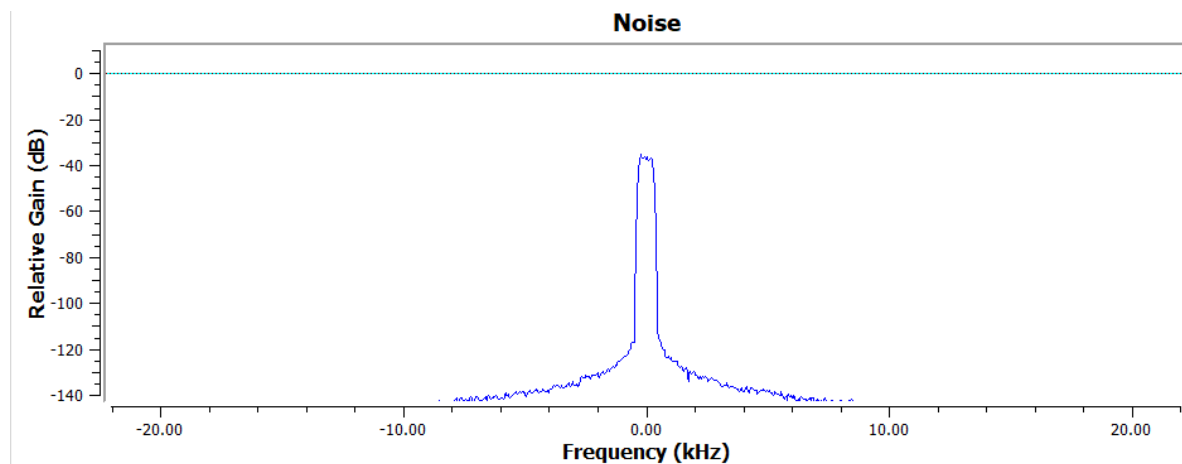


Figure 4: Frequency sink showing the presence of noise

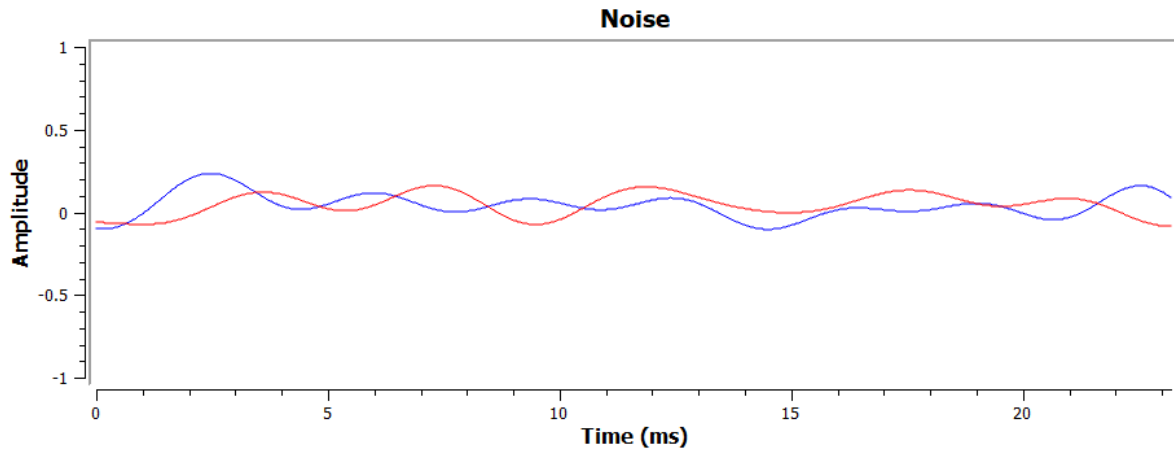


Figure 5: The same noise shown in the time domain

The noise is observed to have a window of approximately 3 kHz, shown above in Figure 4, which comes from the use of a low pass filter at the output of the noise source, with a cutoff frequency of 3000 Hz as shown below in Figure 6.

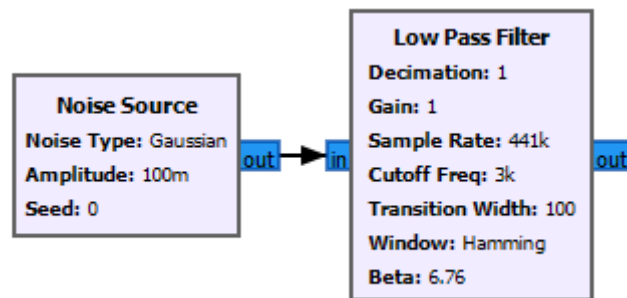


Figure 6: Noise generation block in GNU Radio

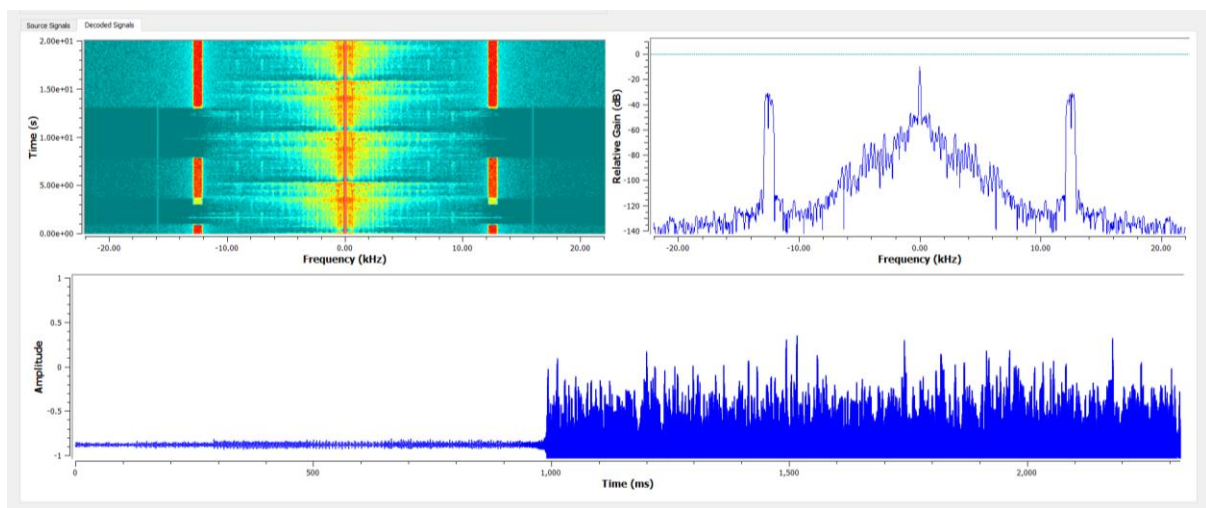


Figure 7: Jamming enabled after 1 second of simulation time in GNU Radio

Figure 10 above shows a screenshot of the demodulated signal before and after enabling jamming. The time domain signal clearly shows the introduction of a lot of noise in the decoded signal.

The constellation diagrams have been shown separately as the unjammed signal displayed an oscillating pattern over time.

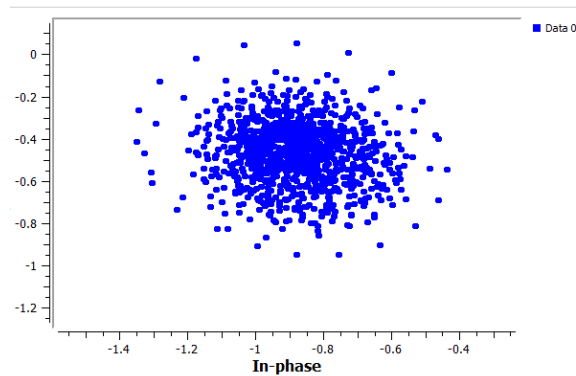


Figure 8: Constellation sink of the jammed signal in GNU Radio

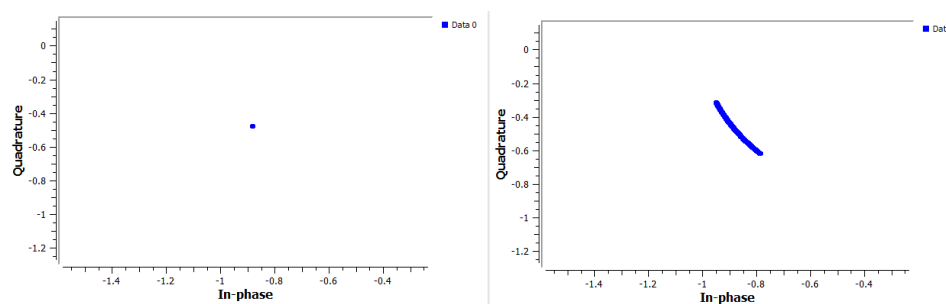


Figure 9: Constellation sink of the signal with no jamming present in GNU Radio

2.4 Implementation of an anti-jamming technique (FHSS)

In order to avoid the jammed signal, the message must be broadcast on a different channel that does not have any noise present. To do this, an option was added such that the frequency that is being used may be changed so that when a channel with noise is identified, the user can change to a different channel to avoid the interference.

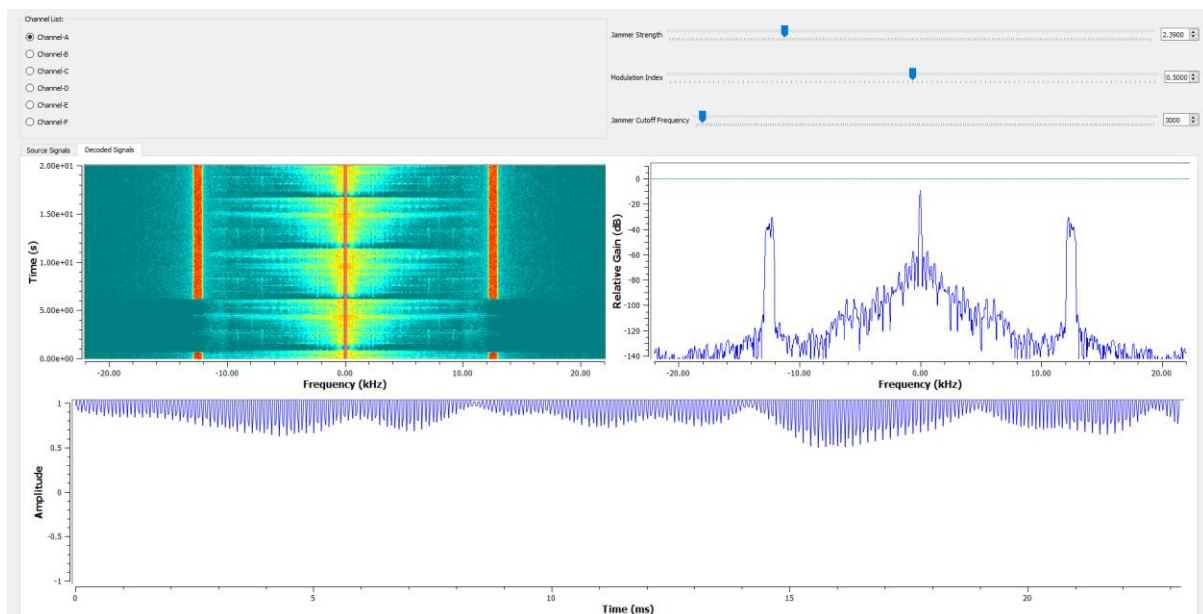


Figure 10: Jammer being turned off and on again in GNU Radio

2.5 Final GNU Radio implementation

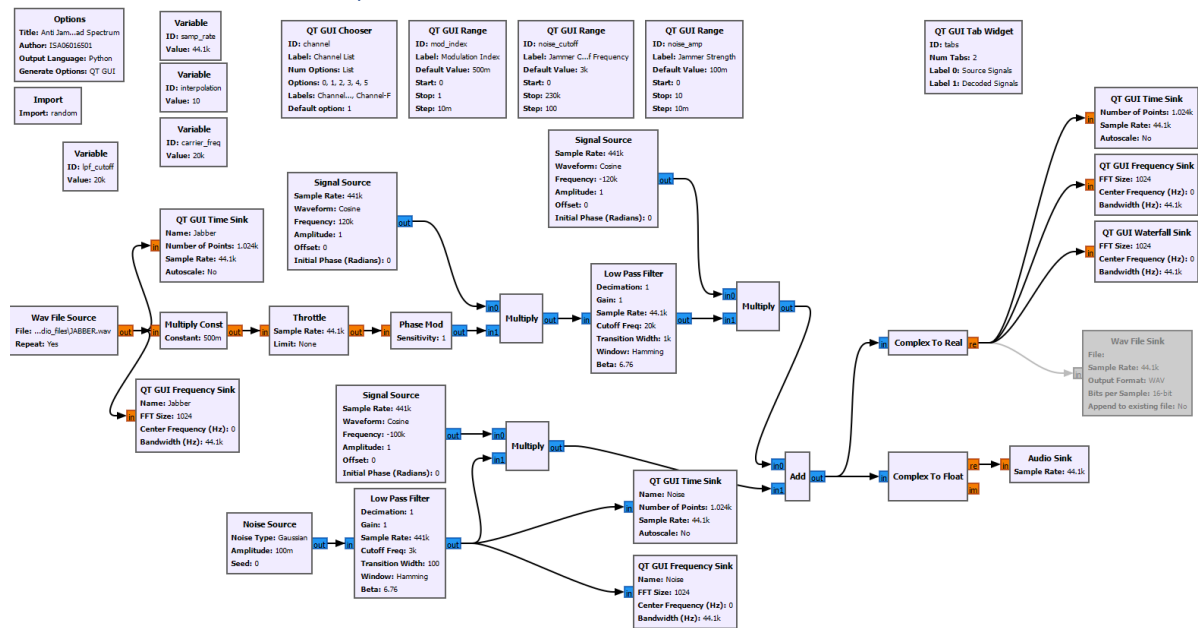


Figure 11: FHSS implementation in GNU Radio

2.6 Ethical considerations of jamming

Jamming can be used for public safety in extreme scenarios, such as terror attacks where a remote device sends a specific signal to an improvised explosive device (IED) [4]. The concept of operation of these devices is to wait in place for a pre-defined signal to be received which signals to the system that a material should be excited such that an energetic event is achieved.

Jamming could also be used in a negative manner to degrade the functionality of critical devices. A similar effect is also achieved by repeatedly sending messages on the same frequency [5], however this is discussed in the following task. Planes rely on GPS to give them accurate position information but jamming prevents this information from being properly demodulated. These events have been increasing in the last decade [6] and manufacturers have learnt from previous incidents and implemented internal navigation systems, however these are far less accurate and errors build up over time.

3 Task 2 – RTL-SDR reception of local FM radio

3.1 Background research

Radio broadcasts from the largest broadcaster in the UK, British Broadcasting Corporation (BBC), begun in 1922 [7]. FM radios were only available for local radio stations that were networked back to a central broadcasting hub. [8]

3.2 FM Receiver in an SDR Block Diagram

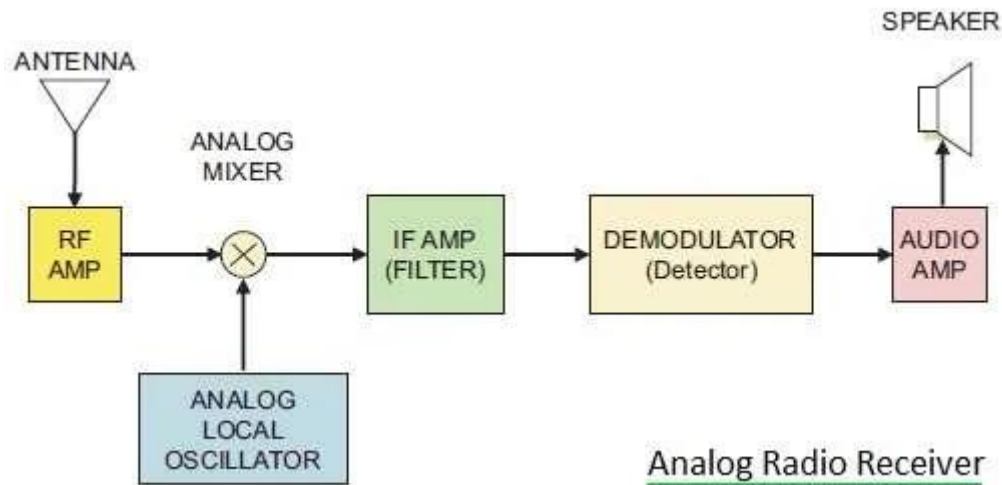


Figure 12: A block diagram of an analogue radio receiver [9]

3.2.1 Recap of analogue FM signal reception

The antenna is responsible for receiving the RF signal and passing it through an RF amplifier which mixes the signal with a local oscillator and intermediate frequency amplifier, before finally demodulating the signal using an envelope detector, or a low pass filter. This demodulated signal can now be passed through an audio amplifier to play it through speakers.

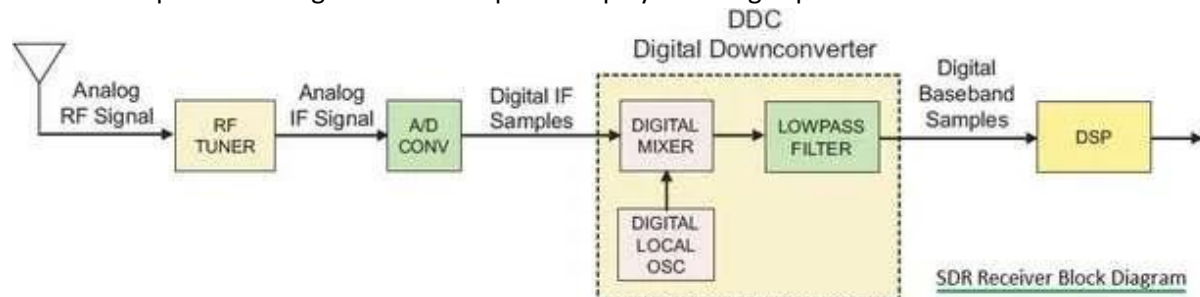


Figure 13: A block diagram of an SDR receiver [8]

3.2.2 Differences in SDR reception

First, an RF tuner is used instead of an analogue local oscillator which is used to down convert signal to an intermediate frequency in a range that the ADC is able to handle [10]. Next, a digital mixer which takes the intermediate frequency signal from the ADC and passes it through a low pass filter to attain discrete digital baseband samples. This stage is done instead of using an IF filter and envelope detector. From the point the DSP is able to pass the signals to a computer over a USB connection.

3.3 FM Receiver implementation in GNU Radio

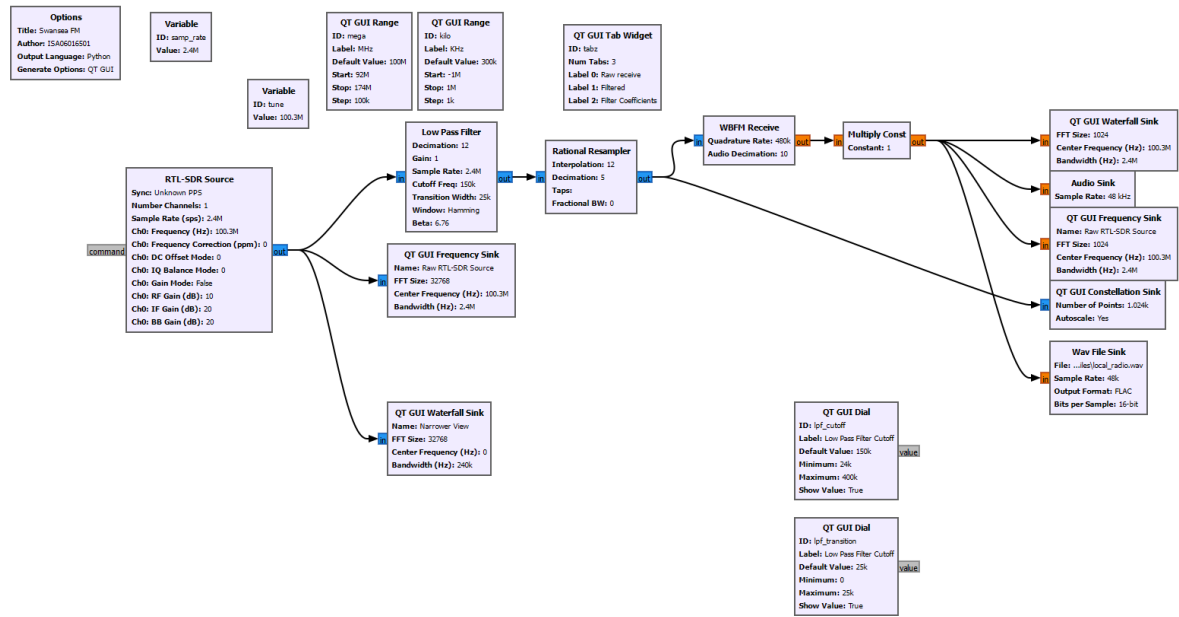


Figure 14: Design of an FM receiver in GNU Radio

A low pass filter (LPF) with a decimation value of 12 has been selected to reduce the sampling frequency entering the filter. As the RTL-SDR source has a channel frequency of 2.4 MHz, this decimation factor reduces the input frequency into the filter to 200 KHz. A hamming window [11] is used to implement the filter, as this has side lobes small with small magnitudes that have little effect on the output of the filter.

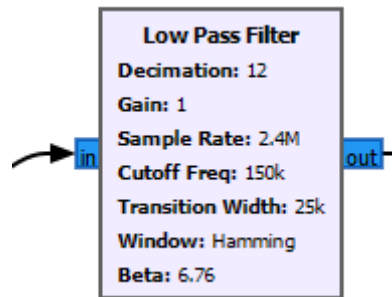


Figure 15: A low pass filter in GNU Radio

$$f = \frac{2,400,000}{12} = 200,000$$

Equation 2: Decimation of the signal received from the RTL-SDR

Following the LPF, a block called “Rational Resampler” is used to resample the 200 KHz signal to a frequency to be used with a Wideband Frequency Modulated (WBFM) Receiver block. To achieve a quadrature rate of 480,000, the signal is first interpolated before it is decimated. This is because it is not possible to use only interpolate to achieve a resample rate of 2.4 times. The smallest numerator and denominator that could achieve a resample rate of 2.4 was chosen. An interpolation of 12 was selected alongside a decimation value of 5.

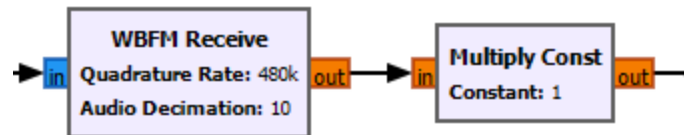


Figure 16: Gain applied to the output of the WBFM receiver

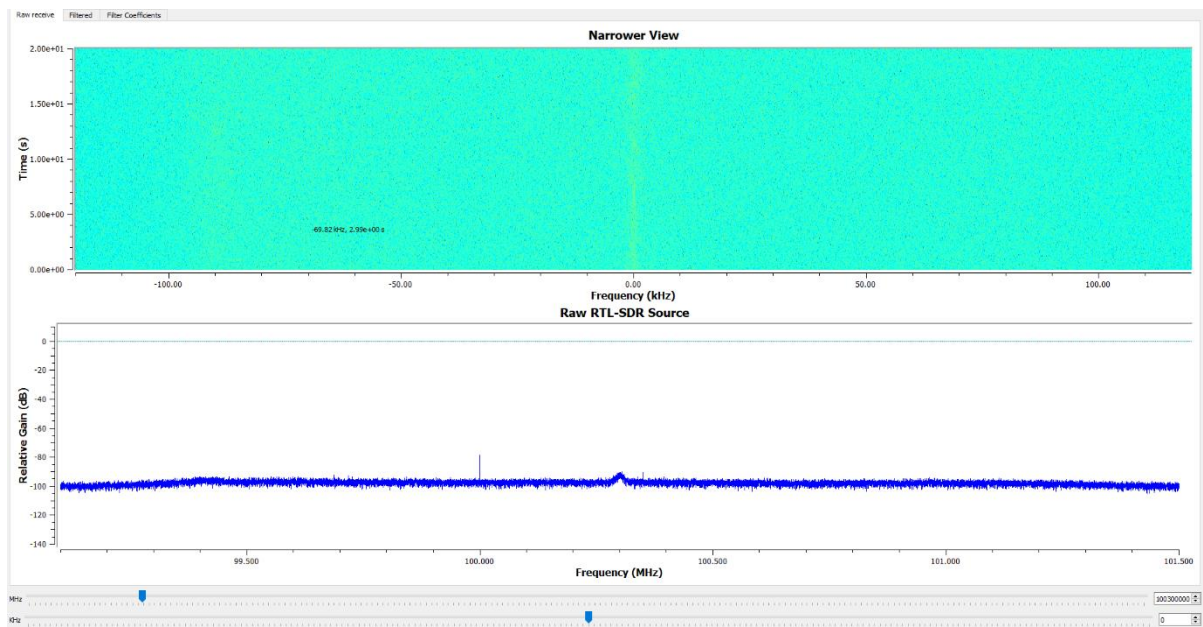


Figure 17: Waterfall sink and frequency sink on the raw RTL-SDR signal with a 0.23 m dipole

An additional stage to apply gain to the demodulated signal has the gain set to 1. During testing of hardware, it was found that using a shorter dipole antenna which can be extended from 5 to 13 cm resulted in a degraded signal as shown above in Figure 17, where it was found that setting the gain to a value greater of 1 was required to hear the transmitted audio from a local radio station. Instead, a dipole which can be extended from 0.23 to 1 m was used, as this is closer to the resonant frequency [12] of the dipole.

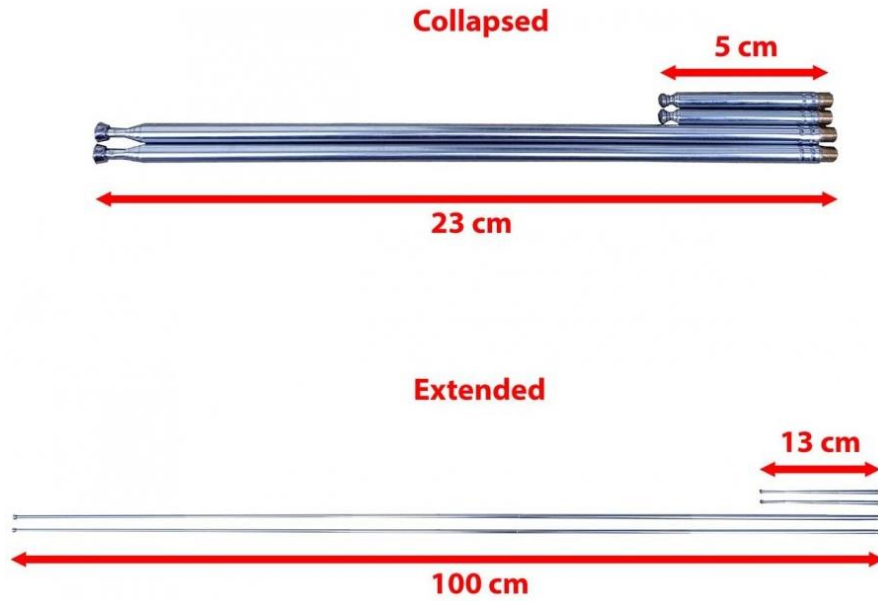


Figure 18: The two pairs of dipole antenna used with the RTL-SDR V4 [13]

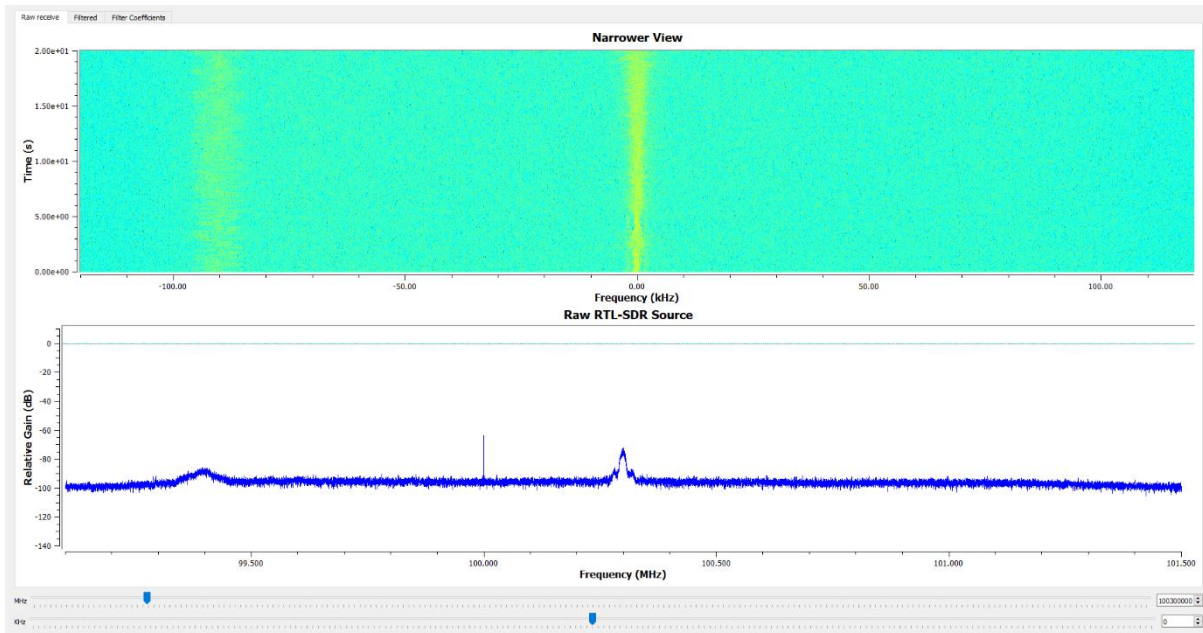


Figure 19: Waterfall sink and frequency sink on the raw RTL-SDR signal with a 1m dipole

After changing the dipole used on the RTL-SDR, an improvement of 20dB was observed, from approximately -90 dB shown in Figure 17 to approximately -70 dB in Figure 19.

For a 1 m dipole antenna, the resonant frequency is calculated by:

$$f = \frac{c}{2L}$$

Equation 3: Resonant frequency of a dipole antenna [12]

$$f = \frac{300,000,000}{2 * 1}$$

$$= 150,000,000$$

And the corresponding wavelength is calculated by:

$$c = f\lambda$$

Equation 4: The general wave relationship [14]

$$\lambda = \frac{c}{f}$$

$$\lambda = \frac{300,000,000}{150,000,000}$$

$$= 2 \text{ m}$$

Using a dipole which has a resonant wavelength of 2 m compared to 0.26 m is preferred as it is closer to the wavelength of the transmitted signals, which are approximately 100 MHz. The dipole with length 1 m has a resonant frequency of 150 MHz, whereas the dipole with length 0.23 m has a resonant frequency of 1.15 GHz.

3.4 Ethical considerations of SDR technology

The Flipper Zero [15] is an example of RF technology that is widely available and has amassed negative attention [16] [17] due to concerns of its potential use to aid criminal activity and case studies which have shown the device to be used for disruptive denial-of-service style attacks that impede the major function of wireless devices such as laptops and medical equipment [5].

The intended audience for the Flipper Zero is “pentesters and geeks” [15] however there are concerns that these types of technology allow criminals easier access to tools to aide illegal activities [16] [17].

While this device does not use SDR technology (it instead uses a discrete Texas Instruments Sub-1 GHz wireless transceiver [18]), it operates across frequencies that the RTL-SDR is able to operate across. Further development of RF technologies such as the Flipper Zero would certainly see benefit from using an SDR.

4 Conclusions

The FM based task looked at a radio broadcast across a single frequency, which in the presence of jamming, would not be lost. However, if frequency hopping were to be used on the broadcast side, the signal could be restored by tuning the SDR to a different frequency that doesn't have any jamming present.

5 Suggested improvements

The reception of local FM radio stations using the RTL-SDR would benefit from using a dipole antenna which has a resonant frequency closer to the carrier frequency of the modulated audio signal.

6 Bibliography

- [1] S. Haykin, *Communication Systems*, 4th edition, New York: Wiley, 2001.
- [2] B. Sklar, *Digital Communications: Fundamentals and Applications* (second edition), New Jersey: Prentice Hall, 2001.
- [3] D. O'Shaughnessy, *Speech Communication, Human and Machine*, 2nd edition, New York: Houghton Mifflin, 1979.
- [4] M. Tranchemontagne, "The Enduring IED Problem: Why We Need Doctrine," *Joint Force Quarterly*, vol. 80, no. 1, 2016.
- [5] B. Toulas, "'Wall of Flippers' detects Flipper Zero Bluetooth spam attacks," *Bleeping Computer*, 23 December 2023. [Online]. Available: <https://www.bleepingcomputer.com/news/security/wall-of-flippers-detects-flipper-zero-bluetooth-spam-attacks/>. [Accessed 30 November 2024].
- [6] CAST Navigation, "Addressing the GPS Signal Jamming Issue Plaguing the Aviation Industry," CAST Navigation, 14 October 2017. [Online]. Available: <https://castnav.com/addressing-gps-signal-jamming-issue-plaguing-aviation-industry/>. [Accessed 20 December 2024].
- [7] D. M. Linfoot, "The origins of BBC Local Radio," BBC, [Online]. Available: <https://www.bbc.com/historyofthebbc/research/local-radio>. [Accessed 15 January 2025].
- [8] M. R. A. I. a. Y. S. B. B. Harianto, "Design Indoor FM Communication Based on SDR and GNU Radio Using Validated Spectrum Analyzer," *Journal of physics. Conference series*, vol. 1845, no. 1, p. 12078, 2021.
- [9] RF Wireless World, "SDR architecture | Software Defined Radio architecture benefits," [Online]. Available: <https://www.rfwireless-world.com/Articles/SDR-Software-Defined-Radio-basics.html>. [Accessed 30 November 2024].
- [10] A. Pini, "Learn the Fundamentals of Software-Defined Radio," 30 June 2020. [Online]. Available: <https://www.digikey.co.uk/en/articles/learn-the-fundamentals-of-software-defined-radio>. [Accessed 20 December 2024].
- [11] J. O. S. III, *SPECTRAL AUDIO SIGNAL PROCESSING*, Stanford: W3K Publishing, 2011.
- [12] S. J. W. P. Dhas, "Advanced Radio Frequency Systems Lecture 3," 16 February 2024. [Online]. Available: <https://moodlearchive.uwtsd.ac.uk/moodle2324/mod/resource/view.php?id=560058>. [Accessed 21 December 2024].
- [13] TechnoFix UK, "RTL-SDR.com multipurpose dipole antenna kit - TechnoFix UK," [Online]. Available: <https://shop.technofix.uk/rtl-sdr-com-multipurpose-dipole-antenna-kit?search=rtl%20sdr>. [Accessed 10 September 2024].

- [14] R. Nave, "Wave Relationship," [Online]. Available: <http://hyperphysics.phy-astr.gsu.edu/hbase/wavrel.html#c2>. [Accessed 21 December 2024].
- [15] Flipper Device Inc., "Flipper Zero Portable Multi-tool Device for Geeks," Flipper Device Inc., [Online]. Available: <https://flipperzero.one/>. [Accessed 30 November 2024].
- [16] M. Kan, "Canada Walks Back Ban of Flipper Zero, Targets 'Illegitimate' Use Cases," PCMag, 24 March 2024. [Online]. Available: <https://www.pcmag.com/news/canada-walks-back-ban-of-flipper-zero-targets-illegitimate-use-cases>. [Accessed 20 December 2024].
- [17] M. Thalen, "Hacking tool Flipper Zero tracked by intelligence agencies, which fear white nationalists may deploy it against power grid," Daily Dot, 31 January 2024. [Online]. Available: <https://www.dailydot.com/debug/flipper-zero-racially-motivated-extremists-fusion-center-alert-nypd/>. [Accessed 30 November 2024].
- [18] Texas Instruments, "CC1101 Low-power Sub-1 GHz wireless transceiver," Texas Instruments, [Online]. Available: <https://www.ti.com/product/CC1101>. [Accessed 30 November 2024].
- [19] T. Wheeler, Electronic Communications for Professionals - Second Edition, Tom Wheeler, Independent, 2023.