

ADV DSP Assignment

by Cameron Fitze

Submission date: 15-Jan-2025 12:52PM (UTC+0000)

Submission ID: 248536390

File name: 32803_Cameron_Fitze_ADV_DSP_Assignment_641246_210731079.docx (1.26M)

Word count: 2731

Character count: 14190

Advanced Digital Signal Processing
Assignment – Cameron Paul Fitze
2111737

**Implementation and Analysis of Narrow Band Frequency Modulation Jamming Techniques and RTL
Design using GNU Radio**

Cameron Paul Fitze

University of Wales Trinity St David

Course Number:

Course Name: BEng Embedded Electronic Systems



Abstract

This study evaluates FM signal transmissions using GNU radio, and the effect of implementing a noise signal on the same frequency band with the aim of jamming the FM signal. It is apparent through these evaluations that FM can be easily distorted with a noisy Gaussian signal on the frequency band. Techniques to avoid this include frequency hopping spread spectrum (FHSS). This enables the FM signal to hop rapidly between a set of pseudo-random set of frequencies, thus minimizing the effects of a noisy signal on a particular frequency.

The RTL-SDR can be used to receive a range of FM frequencies. For the purpose of this study, this was limited to the FM radio frequencies in the UK, 87.6MHZ to 107.9MHZ. GNU radio was used to implement the flow and receive the transmissions from the RTL-SDR hardware.

Abstract

Contents

1. Introduction	4
1.1 Aim	4
1.1 Report Layout.....	4
2. Background Research (Literature Review).....	5
2.1 FM communication	5
2.2 Anti-jamming techniques	5
2.2.1 RF Jamming	6
2.2.2 Anti-Jamming	6
3. Task 1: Jammer Techniques Using GNU Radio.....	8
3.1 NBFM Modulation.....	8
3.2 NBFM Demodulation	10
3.3 Add a Jammer	11
3.4 Implement FHSS for Anti-Jamming:.....	13
3.5 Ethics and Impact:.....	14
4. Task 2 Design and Analyse an RTL-SDR Receiver Using GNU Radio (40%)	16
4.1 Setup and Design	16
4.2 Ethics and Impact	17
5. Conclusions	19
6. Recommendations	20
References	21

1. Introduction

1.1 Aim

This assignment uses practical methods to explore frequency modulation (FM) signals in detail, and the how noise signals can be used to jam or distort that signal.

This assignment will explore Narrow Band Frequency Modulation (NFBM) jamming techniques, to include Wide-Band FM (WBFM) receiver design and Realtech (RTL) software defined radio (SDR) design using GNU radio.

Once the FM signal has been jammed, an anti-jamming technique will be introduced in order to ensure successful transmission and reception of the FM signal

Finally, the ethical implications of receiving FM using RTL-SDR and jamming will be explored.

1.1 Report Layout

The sections in this report are as follows:

1. Background research (see section 2)
2. Jamming Techniques using GNU Radio (see section 3)
3. Design and Analyse of an RTL-SDR Receiver (see section 4)
4. Conclusions (see section 5)
5. Recommendations (see section 6)

2. Background Research (Literature Review)

2.1 FM communication

FM communication techniques vary the frequency of the carrier signal $c(t)$, which mixes with the message signal $m(t)$ to enable successful propagation of the transmitted data to the receiver. The mixing of the message signal with the carrier signal is known as Encoding.

Figure 1 shows an FM communication system.

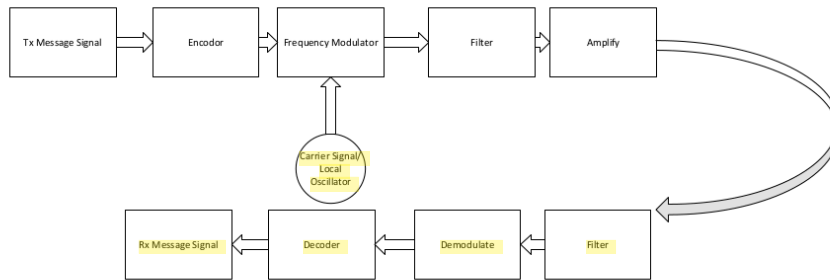


Figure 1 - FM Comms System

The component parts of an FM communication system are as follows:

1. Transmit message signal
2. Encoder
3. Modulator (Frequency)
4. Carrier Signal/ Local Oscillator
5. Filtering
6. Amplification
7. Filtering
8. Demodulate
9. Decode
10. Received Message

The part of the FM system that this project will focus on will be the filtering and the techniques used within the signals to enable the transmit signal to pass any RF jamming efforts.

2.2 Anti-jamming techniques

2.2.1 RF Jamming

RF jamming is a technique in which a specific frequency band within the EM spectrum encounters destructive interference. The aim of this is to deny anyone wishing to transmit in that frequency band the ability to do so. RF Jamming is done at the Open Standards Interface (OSI) Physical (PHY) Layer (Layer 1).

There are various reasons or uses for jamming. Military use cases are the main ones; where if Alice is trying to communicate with Bob, then Wally can transmit at high power on that frequency band, causing destructive interference, to deny Alice-to-Bob comms.

Destructive interference, as observed in RF jamming techniques, is not always due to nefarious intentions, and can be as a result of too many transmissions within a particular frequency band, causing collisions and potentially interference. This is important to recognize as various PHY layer techniques are borne out of the desire to have a robust signal transmission for a satisfactory user experience, for example, so that the end user does not experience signal interference, which could interrupt internet connection.

2.2.2 Anti-Jamming

Anti-jamming techniques have evolved as a means of avoiding disrupted comms. They enable Alice to transmit to Bob within their desired frequency band with minimal disruption to their comms. There are a large range of anti-jamming techniques, such as:

3. Frequency Hopping Spread Spectrum (FHSS)
4. Direct Sequence Spread Spectrum (DSSS)
5. Chirp Spread Spectrum (CSS)

These techniques will be referenced to or explored within this project; however, it is important to note that other techniques are used to avoid jamming. The above methods leave an RF signature that can be attributed to that particular technique. Discreet or covert applications cannot leave a signature that can lead to attribution. Therefore, techniques that aim to hide in the noise and obfuscate are also used as to avoid detections, and therefore, avoid being jammed.

The methods mentioned in the list are all spread-spectrum (SS) techniques. SS is a technique where a code independent to the data being transmitted determines the spreading pattern the signal will follow during its propagation [1]. With a frequency-based SS, this will follow a pattern of frequencies, within the desired frequency band, that the transmitted signal will hop between from transmit to receive.

This assignment focusses on FHSS. FHSS is a SS technique where the carrier signal hops rapidly between frequencies with respect to time. FHSS uses a pseudorandom sequence of frequencies. This provides protection against any jamming in a particular frequency band as the speed of the frequency hopping

ensures that the signal does not encounter destructive interference. Wireless communications technologies that use FHSS include WIFI, Bluetooth, and LoRa (Long Range).

3. Task 1: Jammer Techniques Using GNU Radio

The aim of this task is to simulate an NBFM communication system in GNU Radio. Then a jammer will be introduced at the transmitted, the effects of which will be analysed, before introducing an anti-jamming technique, specifically FHSS. Then the system's performance will be analysed under varying RF conditions.

This task comprises of the following sub sections:

1. NBFM Modulation and Demodulation (see section 3.1)
2. Introduction of Jammer (see section 3.3)
3. Implementation of FHSS for Anti Jamming (see section 3.4)
4. Ethics and Impact (see section 3.5)

The analysis is contained within each subsection, for example, the FM analysis is within the NBFM modulation section.

Each signal will contain the following analysis:

- Time sink
- Frequency sink
- Waterfall sink

The time sink has time (ms) along the x-axis and amplitude along the y-axis, and displays the amplitude of the signal across time.

The frequency has frequency (Hz) along the x-axis and relative gain (dB) along the y-axis. It displays the gain at across the frequencies.

The waterfall sink has frequency along the x-axis and time along the y-axis. It displays the signal strength/ energy, the colour part, as a function of frequency over a time period. The stronger the signal, the redder it will appear, and weaker signals are blue.

3.1 NBFM Modulation

- Bandwidth = 24KHz
- Frequency deviation = 12KHz



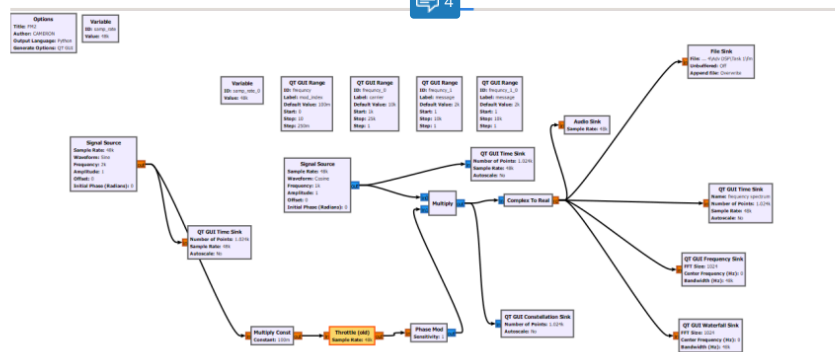
5

5

5

5

5



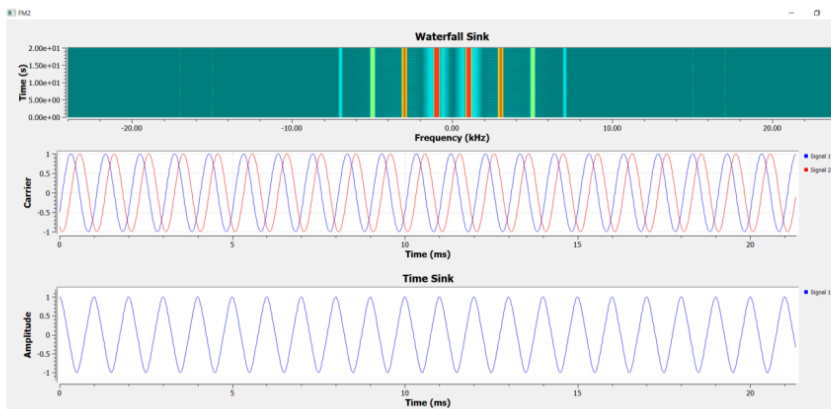


Figure 3 - NBFM Waterfall and Time Sink

Figure 4 shows the frequency sink for the NBFM.

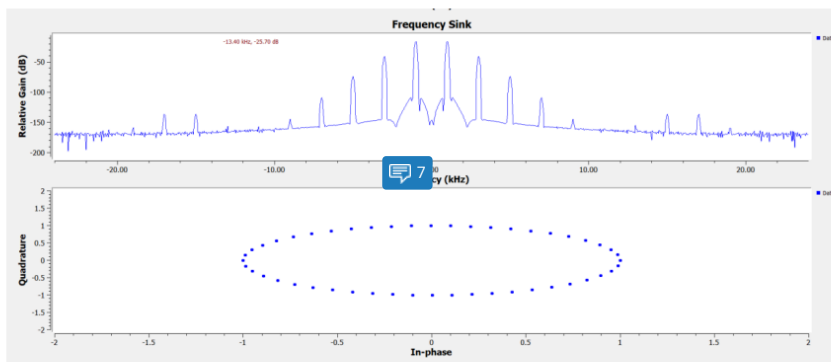


Figure 4 - NBFM Frequency Sink

3.2 NBFM Demodulation

Figure 5 shows the FM demodulation. This stage involves capturing the FM channel signal, and down converting it into its baseband I (real) and Q (imaginary) components. This involves taking the modulated signal through filtering: first band pass filter, then low pass filtering, to filter out any

unwanted signals. This ensures the original baseband signal is recovered, or demodulated, at the receiver.

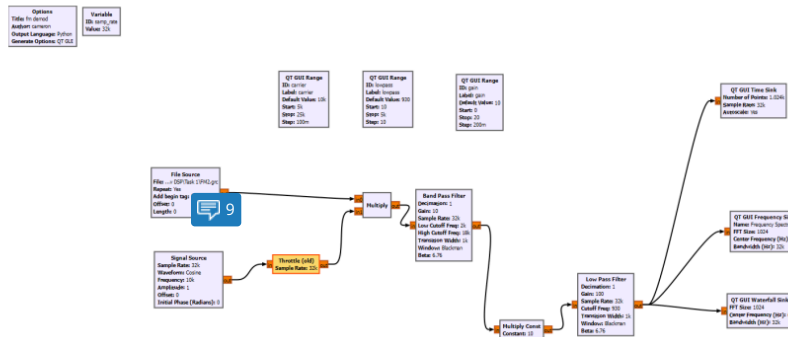


Figure 5 - NBFM demodulation

The demodulation flow show in the above figure failed to run, so it was not possible to obtain time, frequency and waterfall plots.

3.3 Add a Jammer

Figure 6 shows a jamming signal on an RF transmitter. The jamming was the noise source, Gaussian. The signal source is the FM signal used in the previous sections.

The signal source is observed on a QT GUI time sink before it is mixed with a jamming signal. This is to prove the FM signal was transmitting correctly. It is then mixed with the Gaussian noise jamming signal.

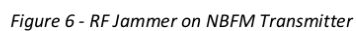


Figure 7 shows the effects of the jamming signal on the FM signal. As seen in the *frequency spectrum*, there is noise on the FM signal output, caused by the introduction of the Gaussian noise into that frequency band. The peaks of the transmit signal clearly show noise, which will cause distortion to the signal.

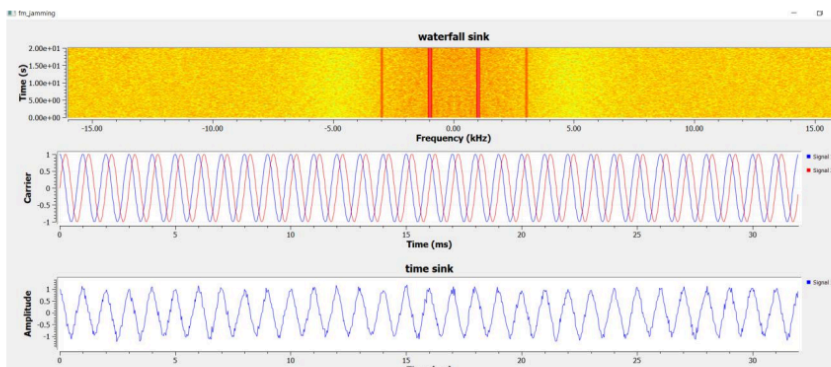


Figure 7 - NBFM Jamming Frequency Spectrum

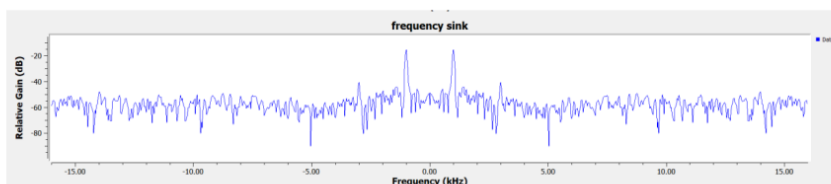


Figure 8 - NBFM Jamming Frequency Sink

The time sink shows an amplitude of 2 over time and is encounter significant interference.

The frequency sink shows a strong relative gain of around -15dB at around 1kHz and -1kHz, representing a change of around 5dB.

The waterfall sink shows significant interference across the spectrum. This is made apparent by the orange/red colour across that frequency band. This indicates that there are relatively strong signals across the band, in areas that are not desired.

3.4 Implement FHSS for Anti-Jamming:

Figure 9 shows the FHSS implementation flow to mitigate the effects of the RF jammer observed in the previous section.

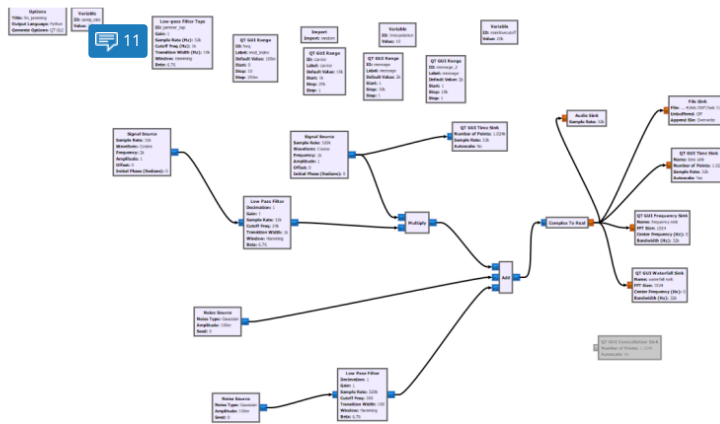


Figure 9 - FHSS Flow

Errors occurred in the code, which mean that the it was not possible to obtain the frequency, time, and waterfall sinks.

3.5 Ethics and Impact:

RF jamming is caused by destructive interference of a signal from another signal on the same frequency band. This can be accidental, for instance in a congested frequency band, or intentional. Intentional RF jamming is observed in military applications with the aim of interrupting enemy command and control (C2). Interrupted C2 causes difficulties for missions as tactical comms become impossible, leading to a higher chance of battlefield mortalities.

So, in a military application, RF jamming can cause casualties, which has various ethical impacts to consider if RF jamming is intentional.

RF jamming has led to technological innovation to improve comms by enabling RF signals to circumvent the effects of destructive RF interference. These methods not only benefit battlefield comms, but also wider society as personal comms technologies, such as Bluetooth and WiFi, are improved by these methods, and as such, wider society user experience is improved. This has even wider benefits to society when talking about aspects such as the economy, as societal comms lead to greater efficiency. FHSS,

which avoids interference by hopping quickly between a pseudorandom frequency sequence, has benefits for the military, as adversaries struggle to jam comms, but also in Bluetooth as a civilian using the protocol will have an improved experience.

4. Task 2 Design and Analyse an RTL-SDR Receiver Using GNU Radio (40%)

The aim of this task is to explore the design of an RTL-SDR receiver in GNU radio. Then, the receiver will be tuned into a desired frequency where it will be analysed. The analysis will focus on the signal quality at different stages. Then the ethical parameters around this process will be discussed.

This task comprises of the following sub-sections:

1. Setup and Design (see section 4.1)
2. Signal Analysis and Visualisation (see section **Error! Reference source not found.**)
3. Ethics and Impact (see section 4.2)

4.1 Setup and Design

The RTL-SDR is a type of software-defined radio that is low cost and enables users to receive various RF transmissions. It is used in applications such as receiving air-traffic control comms, FM radio, police radio, and more. It can only be used to receive, it cannot transmit. The receive transmit range is roughly 500KHz to 1.75GHz [2].

The kit list for a simple receiver is as follows:

- RTL-SDR dongle
- Low pass filter
- WBFM demodulator
- Audio output (e.g., soundcard)

Figure 10 shows the GNU flow for the RTL-SDR receiver. This is a simple design that enables the frequency spectrum to be obtained from the RTL-SDR hardware. The sampling rate is set to 2.048M as that is the maximum sampling rate for the RTL-SDR. The received signal is represented as follows:

$$s(t) = i(t) + jq(t)$$



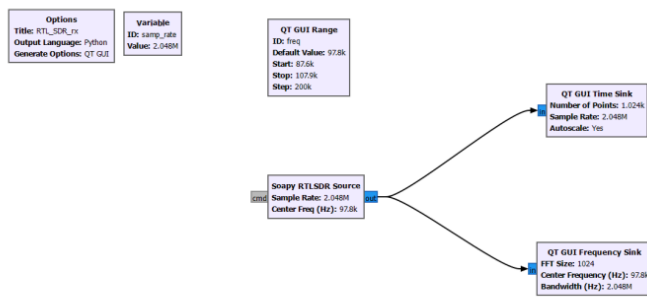


Figure 10 - RTL-SDR receiver flow

The next step involved adding filtering and interpolation to receive the audio. Figure 11 shows the completed flow for the RTL-SDR receive. This now includes a rational re-sampler, low-pass filter, and a WBFM receive.

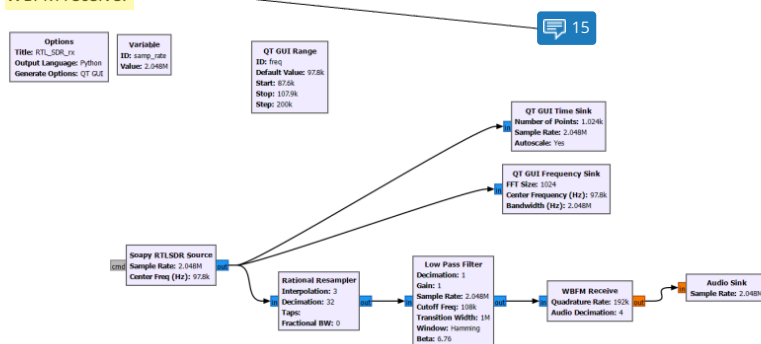


Figure 11 - RTL-SDR Complete Flow

Issues arose when compile the flow above as the error "cannot find RTL-SDR" device popped up. This was not able to be resolved.

4.2 Ethics and Impact

There are various ethical implications with using an SDR for personal use. As this can receive any FM signal within its specified range, a user can listen to air-traffic control, police radios, ambulance radios, and more. Some might argue that there are security implications around civilians listening to air-traffic control or police radios as those transmissions are for live and safety-critical applications – having anyone listen in on these could be deemed a security and safety threat.



5. Conclusions



There are various findings from the study.

GNU radio is a fairly easy-to-use software for modelling FM and the ability to write one's own python scripts and import into a project is very beneficial.

FM is an easy signal to jam, and as such, methods such as FHSS should be introduced in applications where safety and security is paramount.

Jamming can easily be observed on a frequency plot as interference on the peaks of the transmitted FM signal.

The RTL-SDR receiver flow is fairly simple, and is an easy method to receive a range of WBFM signals, which might be desirable for personal use such as listening to FM radio, air-traffic control transmission, and any other FM transmissions within the RTL-SDR frequency range. FM is a good method to use for receive as there is plenty of traffic that a user could receive to verify their software flow, which could potentially influence development of a hardware implementation.

6. Recommendations

There are various recommendations to come out of this study.

To start, other anti-jamming methods should be explored to enable the investigation of the benefits and disadvantages of the currently available methods. This is beneficial as the investigation could lead to the identifying of a more suitable method of anti-jamming for FM applications.

A hardware implementation could be created on the back of this study. This would consist of the RTL-SDR, a low pass filter, and WBFM demodulator wrapped up in a box that could be transported to a location of choice to receive the desired applications. This box could, for instance, be transported to an airport viewing area to enable airplane enthusiasts the chance to receive air traffic control traffic to inform them of the departures and arrivals at that airport.

Finally, the errors in running the flows for NBFM demodulation and FHSS implementation should be explored with more time in order to understand why these particular flows encountered errors. The errors running the RTL-SDR with GNU should also be resolved as this would enable real world analysis of FM signals to be conducted through GNU radio.

References

- [1] J. M. T. a. P. P. M. Hasan, "Design and Implementation of FHSS and DSSS," *International Journal of Signal Processing Systems*, vol. 4, no. 2, April 2016.
- [2] RTL SDR, "rtl-sdr.com," [Online]. Available: <https://www.rtl-sdr.com/about-rtl-sdr/#:~:text=Depending%20on%20the%20particular%20model,and%20provided%20free%20of%20charge..>
- [3] International Telecommunication Union (ITU), "Data format definition for exchanging stored IQ data for the purpose of spectrum monitoring," ITU, 2018.

ADV DSP Assignment

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

35/100

Feedback on A4HEP Learning Objectives

B1: Demonstrates a good application of knowledge in problem-solving. You have successfully met the requirements for this learning outcome.

B2: Inadequate analysis, leading to weak or unsupported conclusions. You have not met the requirements for this learning outcome. Improvement is needed.

B3: Incorrect or ineffective use of computational and analytical techniques. You have not met the requirements for this learning outcome. Improvement is needed.

B6: Fails to integrate a systematic approach, resulting in incomplete solutions. You have not met the requirements for this learning outcome. Improvement is needed.

B8: Demonstrates strong ethical analysis and informed decision-making. You have successfully met the requirements for this learning outcome.

B12: Insufficient practical skills lead to poor investigation outcomes. You have not met the requirements for this learning outcome.

Improvement is
needed.

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5



Comment 1 | **Engagement with Lit (20)**

The fundamentals of Frequency Modulation (FM) are well explained, and the components of an FM signal are properly identified.

PAGE 6



Comment 2 | **Knowledge & Understanding (20)**

The techniques of jamming and the underlying concepts are well described.



Comment 3 | **Knowledge & Understanding (20)**

The explanation of Frequency Hopping Spread Spectrum (FHSS) and its associated concepts is detailed and well-articulated. It is also commendable that the report discusses the applications of these techniques.

However, the inclusion of a conventional block representation would enhance clarity and make the explanations more intuitive.

PAGE 7

PAGE 8

PAGE 9



Comment 4 | **Cognitive Skills (20)**

The bandwidth and frequency deviation values are specified, which is good, but including the formulas used for these calculations and explaining how the values are derived would improve clarity and understanding.



Comment 5 | **Practical Skills (25)**

The GNU Radio blocks used in the implementation are documented, and there is a

well-presented.



Comment 6 | Cognitive Skills (20)

The mathematical expressions for FM are provided, which is appreciated. The sink observations, including SNR (Signal-to-Noise Ratio) and frequency values, are captured effectively.

PAGE 10



Comment 7 | Practical Skills (25)

The procedure and techniques followed for NBFM are correct, but the modulation index is very low.



Comment 8 | Cognitive Skills (20)

The NBFM demodulation is briefly explained, which is good. However, the NBFM source file used is a signal source, whereas an audio file should be used to meet the task requirements.

PAGE 11



Comment 9 | Transferable Skills (15)

In Task 1(ii), the File Source block is used instead of the WAV Source, which could be the reason why the block is unresponsive and why no sink outputs are observed.



Comment 10 | Knowledge & Understanding (20)

The addition of a noise source to the NBFM block is well-documented, which is commendable, and the signal distortion values are correctly noted.

PAGE 12

PAGE 13

PAGE 14



Comment 11 | Transferable Skills (15)

An error in the block due to an incorrect sampling rate has been identified. For proper audio output, the sampling rate should be 44 kHz or 48 kHz, but the current setup appears to use 32 kHz, which causes issues.



Comment 12 | Knowledge & Understanding (20)

The block does not demonstrate the use of FHSS as it lacks random blocks and channel switching across different frequencies.



Comment 13 | Knowledge & Understanding (20)

The discussion on the ethical impacts of SDR (Software-Defined Radio), particularly regarding destructive interference, interception, and communication system vulnerabilities, is well addressed.

PAGE 15

PAGE 16



Comment 14 | Cognitive Skills (20)

The mathematical expressions related to the SDR receiver's complex functions are missing and should be included.

PAGE 17



Comment 15 | Cognitive Skills (20)

The stages of block inclusion in the flowgraph are properly documented, which is appreciated.



Comment 16 | Transferable Skills (15)

One significant issue identified is that the RTL-SDR receiver settings were not properly configured before use. The SDR should be correctly set up to function in the current system, but this has not been resolved.

PAGE 18



Comment 17 | Cognitive Skills (20)

The report does include discussions on the impacts of misusing the SDR receiver, which is valuable.

PAGE 19



Comment 18

Overall, the report follows a logical flow, but it would benefit from including more references to strengthen its credibility. Some tasks do not fully meet the objectives due to unclear handling of the software, which should be addressed. Additionally, while ideas and concepts are present, deeper analysis and observations are required to draw meaningful and well-supported conclusions.

PAGE 20

PAGE 21

ENGAGEMENT WITH LIT (20)

Task 1: Demonstrate understanding of NBFM, jamming effects, and FHSS. Citations and research on related topics. Task 2: Show understanding of SDR receiver principles and signal representation. Evaluate research on SDR technology and related topics.



- Limited grasp of topics. Research and citations are vague, with noticeable gaps.
- Limited grasp of SDR principles. Research and evaluation are vague, with noticeable gaps.

9**KNOWLEDGE & UNDERSTANDING (20)**

Task 1 (i) Understanding NBFM, modulation, and demodulation. Exploring bandwidth, frequency deviation, and impact on signal quality. Task 1 (ii) Analysing jamming effects by studying noise sources and interference. Observing impact via frequency, time domain, and constellation diagrams. Task 1 (iii) Investigating FHSS to reduce interference and evaluating its effectiveness. Task 1 (iv) Comparing original, jammed, and FHSS signals. Studying Signal-to-Noise Ratio (SNR), clarity, and system efficiency. Task 1 (v) Understanding ethical issues in jamming. Discussing legal aspects and FHSS benefits for security. Task 2 (i) Designing a WBFM receiver using RTL-SDR and GNU Radio. Studying block functions and sampling. Task 2 (ii) Visualising signals via waterfall plots, frequency sinks, and time-domain analysis. Studying SNR, stability, and filtering. Task 2 (iii) Evaluating privacy and interference issues. Analysing societal benefits like improved efficiency and technology.



- Basic understanding of NBFM. Descriptions are incomplete, with noticeable gaps in coverage.
- Satisfactory understanding with basic explanations, but limited detail.
- Basic understanding. Explanations of FHSS are incomplete or unclear.
- No understanding. Signals are misunderstood, with no meaningful SNR or performance analysis.
- Satisfactory understanding. Basic descriptions,

8.5

but lacking clarity.

- Minimal knowledge. Little effort to explain concepts, with significant inaccuracies.
- No understanding of signal analysis. Sinks, SNR, and stage comparisons are either not addressed.
- Basic understanding. Explanations of ethics and benefits are limited.

COGNITIVE SKILLS (20)

Task 1 (i) NBFM Modulation and Demodulation: Understands modulation, demodulation, bandwidth, and clarity. Task 1 (ii) Add a Jammer: Evaluates noise, interference, and signal impact in frequency, time, and constellation domains. Task 1 (iii) Implement FHSS for Anti-Jamming: Applies FHSS to reduce interference and compare signal stability. Task 1 (iv) Analysis and Comparison: Compares original, jammed, and FHSS signals using frequency and time-domain tools. Task 1 (v) Ethics and Impact: Assesses legal and societal effects of interference in secure communication. Task 2 (i) Setup and Design of WBFM Receiver: Designs WBFM receiver, focusing on setup, bandwidth, and stability. Task 2 (ii) Analysis and Visualisation: Examines signal analysis, error detection, and filtering techniques. Task 2 (iii) Ethics and Impact: Reviews interference impact and decision-making in WBFM technology.



- Basic setup with unclear reasoning.
- Basic analysis with unclear reasoning.
- No understanding of FHSS.
- No comparison of signals.
- Minimal effort, significant inaccuracies.
- No evidence understanding of signal demodulation.
- No signal analysis or understanding of parameters like SNR or modulation index.
- Minimal effort in discussing ethics or societal impact, with significant inaccuracies.

4.3

PRACTICAL SKILLS (25)

Task 1: Hands-on experience in transmitter and receiver setup, understanding signal bandwidth and frequency deviation. Implementing noise sources and analysing interference effects using frequency, time, waterfall, and constellation sinks. Applying FHSS techniques for anti-jamming and evaluating signal clarity through SNR analysis and stage comparisons. Developing an awareness of secure

communication and legal implications. Task 2: Practical implementation of RTL-SDR receiver setup, signal representation, and processing. Understanding block functionality, decimation factors, and performing signal analysis using waterfall and frequency sinks. Visualising constellation diagrams and evaluating signal stability through SNR measurements. Comparing different demodulation stages for performance optimisation.



Task 1: Basic attempt at practical skills with incomplete NBFM setup and limited FHSS implementation. Jammer effects and visualisation tools are used inadequately, and signal comparisons lack meaningful insights. Task 2: No evidence of practical skills or understanding of the task requirements. Setup and analysis are absent, with no use of visualisation tools or stage comparisons.

7.6

TRANSFERABLE SKILLS (15)

Enhancing mathematical integration and simulation skills using GNU Radio and RTL-SDR. Developing ethical reasoning and effective communication for teamwork and professional interactions. Practising systematic reporting, structured problem-solving, and clear presentation skills.



Minimal effort with significant inaccuracies in setup, analysis, and documentation. Limited or no understanding of ethical aspects.

5.8