

# Hands-on Project: OFDM Signal Transmission and Reception Using Amateur SDR Devices

Meles Weldegabriell, Prince John (A paper written under the guidance of [Prof. Raj Jain](#))



## Abstract

Wireless systems and uses have boomed in the last decades. The use of Software Defined Radio (SDR), that moves Digital Signal Processing (DSP) closer to the antenna, have particularly contributed towards the rapid growth of wireless applications. In this hands-on project work, we experiment transmission and reception of Orthogonal Frequency Division Multiplexing (OFDM) signals using amateur Hackrf one SDR device. Using Quadrature Phase Shift Keying (QPSK) modulation OFDM subcarriers, we transmit IQ samples generated in python.

We use the open-source toolkit, GNU Radio Companion, to generate and detect the OFDM signals. Using 2 MHz bandwidth centered at 435 MHz in the UHF amateur radio band, we illustrate OFDM signal waveforms in frequency and time domains. Moreover, by deploying different antenna lengths, shadowing and antenna directions at the transceivers, we demonstrate wireless signal fading variations.

## Keywords

Wireless, OFDM, SDR, hackrf one, ham radio, amateur radio, GNU radio

## Table of Contents

- [1. Introduction](#)
- [2. System Design](#)
  - [2.1 System Block Diagram](#)
  - [2.2 System Components](#)
- [3. Methodology](#)
  - [3.1 OFDM Signal Transmission](#)
  - [3.2 OFDM Signal Reception](#)
  - [3.3 GNU Radio](#)
  - [3.4 UHF Antenna Design](#)
- [4. Results and Analysis](#)
  - [4.1 Received and Transmitted Waveforms](#)
  - [4.2 Effects of shadowing](#)
- [5. Future Work](#)

- [6. Conclusion](#)
- [7. References](#)
- [8. Acronyms](#)
- [9. Appendices](#)

## 1. Introduction

OFDM is a bandwidth efficient modulation scheme that is used in multiple extremely popular wireless technologies like LTE, WiFi 802.11a/n/ac. OFDMs prevalence in the modern computing devices that we all use make it an essential part of everyday life. Therefore, we decided to build a hands-on project to investigate this modulation scheme and understand and explore the challenges that come with real world wireless data transfer.

Amateur radio or ham radio experimentation has been a staple part of radio communication since the early 1900s. Today separate frequency bands of the electromagnetic spectrum have been allocated for experimental and hobby use by amateur operators by the FCC and other regulatory agencies around the world. Generally, ham radio bands are used for analog voice communication but digital data transmissions are allowed provided that they are prefixed with proper identification.

We decided to use the UHF(Ultra High Frequency) ham radio band from 420 to 450 MHz to experiment with our OFDM data transmissions. We used open source Hackrf One SDR(software defined radio) transreceivers along with GNU radio to transmit and receive our OFDM data streams.

## 2. System Design

### 2.1 System Block Diagram

The block diagram overview of the system design we used is shown in figure 1.

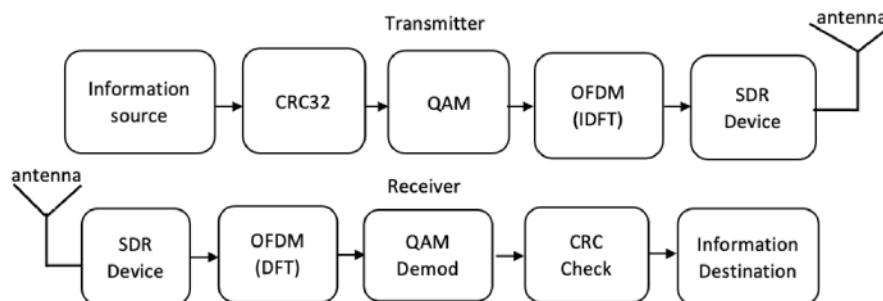


Figure 1: System Block Diagram.

### 2.2 System Components

- **Information Source:** This is any digital information to be transmitted.

- **Cyclic Redundancy Check (CRC32):** This is coding for error detection and correction at the receiver.
- **Quadrature Amplitude Modulation(QAM):** in this project, 4-QAM or equivalently QPSK is deployed. Every two bits in the incoming bit sequence are mapped into a QPSK symbol.
- **Orthogonal Frequency Division Multiplexing(OFDM):** Here, the generic OFDM similar to IEEE 802.11a/g is used. [\[Engels, 2002\]](#)
- **Software Defined Radio(SDR):** This is a versatile device to transmit and receive many different and custom waveforms at various frequencies and settings on a common hardware platform. We use GNU Radio to define transmitter parameters such center frequency, bandwidth and gain. Software is written in python.
- **Antenna:** This is a simple dipole antenna proportional to the wavelength of the signal we transmitter.

Note: The blocks in the receiver carry out the inverse task of the corresponding devices in the transmitter.

## 3. Methodology

### 3.1 OFDM Signal Transmission

The OFDM signal transmission is set up as follows. A digital information signal is sent to an CRC encoder which scrambles the data bits so that errors can be corrected at the receiver end. We used the builtin CRC32 encoder which is capable of correcting two errors. The output of the error correction encoder is then mapped into symbols at the QPSK modulator. We use a mapping table that takes every incoming two bits and maps it to one of four complex values called Inphase and quadrature phase components.

At the OFDM block, we use the generic IEEE 802.11a/g format i.e 48 data carriers, 4 pilot carriers and 6 guard carriers on each end. To Generate the time domain OFDM signal, we use 64 point IDFT(IFFT). The time domain signal is then sent to the SDR for transmission. For license issues, we use an amateur SDR device Hackrf One to transmit the signal. Attached to this device is a dipole antenna. Since we are using 435MHz as a center frequency, we used a dipole antenna of length 40 cm which is greater than half of  $\lambda = 70\text{cm}$ .



Figure 2: Transmitter Setup. From left to right: Dipole antenna, hackrf one SDR, Laptop running live image of pentoo linux executing the GNU radio flowgraph.

### 3.2 OFDM Signal Reception

During reception, a dipole antenna of length 40cm intercepts the EM wave which is tuned to 435MHz. This is fed to a Hackrf One SDR device which then outputs complex samples. The OFDM block carryout DFT(FFT) on the sampled values to produce the IQ samples. These IQ complex values are de-mapped by comparing them to a mapping table to give the required binary bits.



Figure 3: receiver Setup, from left to right: Desktop PC running live image of pentoo linux executing the receive GNU radio flowgraph, hackrf one SDR, Dipole antenna.

### 3.3 GNU Radio

To define the parameters and functionalities of a system, we use software written in python. First we defined the system requirements and then GNU Radio Companion was used to generate the python code. Figure 4 shows the main components of the transmitter flow graph in GNU radio. During transmission, data bit sequences are fed in the form of ASCII formatted text. Data bits are then generated after carrying out CRC32 coding. Since we use QPSK modulation on each OFDM subcarrier, we do mapping on the channel coded signals. Mapping is done as shown in the constellation diagram in Figure 9.

Figure 4 shows the main components of the transmitter flow graph in GNU radio. During transmission, data bit sequences are fed in the form of ASCII formatted text. Data bits are then generated after carrying out CRC32 coding. Since we use QPSK modulation on each OFDM subcarrier, we do mapping on the channel coded signals. Mapping is done as shown in the constellation diagram in Figure 9.

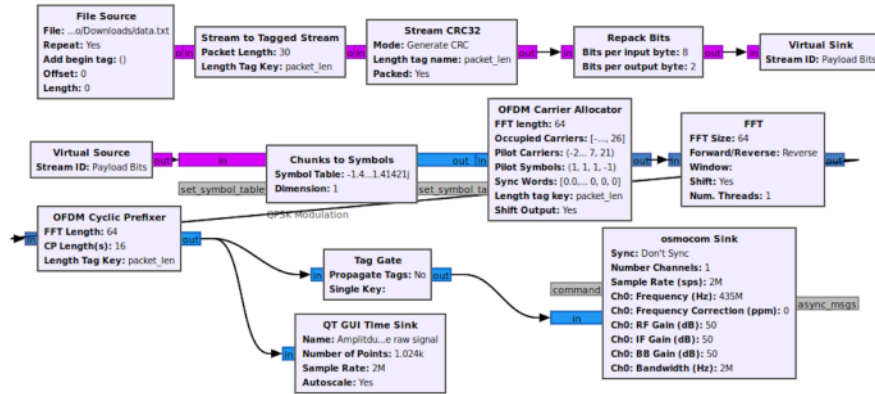


Figure 4: OFDM Transmitter Flowgraph. The screenshot shows the transmission flowgraph we created in GNU radio companion.

We also use the generic OFDM protocol where 48 subcarriers are for data, 4 subcarriers are pilots and 6 subcarriers as guard bands on each end. The next stage uses 64 point IFFT to generate the time domain samples. The final stage of the OFDM signal generation is A1/4 Cyclic Prefixing to produce an 80 point OFDM symbol which is transmitted via Hackrf one SDR device.

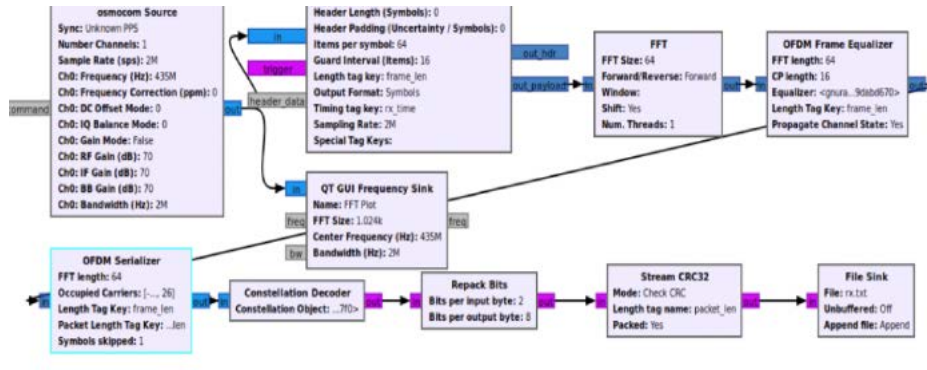


Figure 5: OFDM receiver Flowgraph. The screenshot shows the reception flowgraph we created in GNU radio companion.

We also use GNU radio companion to generate the python code for receiving the OFDM signal. Figure 5 shows the components of the receiver flow graph. OFDM signals are intercepted using a 40 cm dipole antenna connected to a Hackrf one SDR device.

### 3.4 UHF Antenna Design

We used simple telescopic dipole antennas for both reception and transmission. The dipole antennas were connected to the hackrf one SDR modules using SMA connectors and a coaxial cable. Since we had telescopic antennas we could finely tune their lengths to match the exact frequency we were using for TX and RX. As stated in the earlier sections, the antenna length was set at 40 cm to intercept a signal centered at 435 MHz.

$$\text{Antenna Length} = \frac{\lambda}{2} \text{ and } \lambda = \frac{c(\text{speed of light})}{f}$$

$$\text{So, Antenna length} = \frac{c}{2 \times f} = \frac{3 \times 10^8 \text{ m s}^{-1}}{2 \times 435 \times 10^6 \text{ s}^{-1}} \approx 0.345 \text{ m or } 34.5 \text{ cm}$$

## 4. Results and Analysis

### 4.1 Waveforms

OFDM signals were transmitted using the amateur Hackrf one device using 2MHz bandwidth at 435MHz. The generated time-domain OFDM signal waveform is as indicated in Figure 6. The Power Spectral Density (PSD) of the corresponding OFDM signal before it's amplified at the SDR device is also indicated in Figure 7.

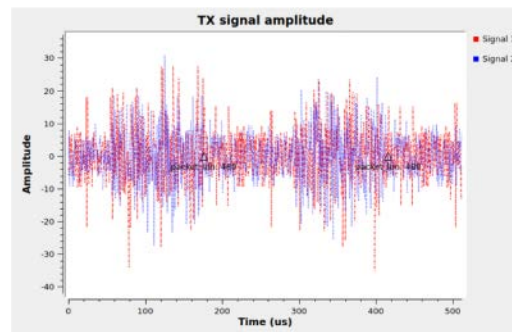


Figure 6: Transmission waveform. Time domain OFDM output transmitted from the transmission station.



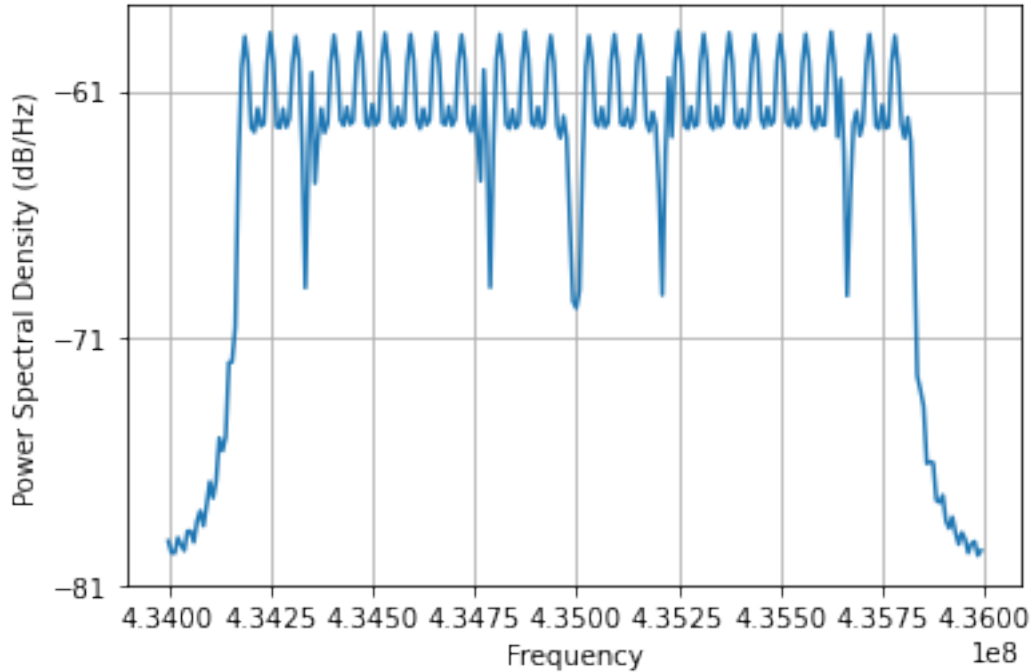


Figure 7: PSD of Transmitted OFDM signal. Frequency domain transmitted signal waveform.

At the receiver end, the similar SDR device, Hackrf one, was used to detect the OFDM signals. Our antenna was set to be 40 cm to detect the 435MHz signal. The spectrum occupied by the OFDM signal and the transmitted 2MHz wide signal centered at 435 MHz can be clearly seen in Figure 7, with the received signal spanning from 434 MHz to 436 Mhz. We have also sampled the received signal and plotted the IQ constellation as indicated in Figure 9.

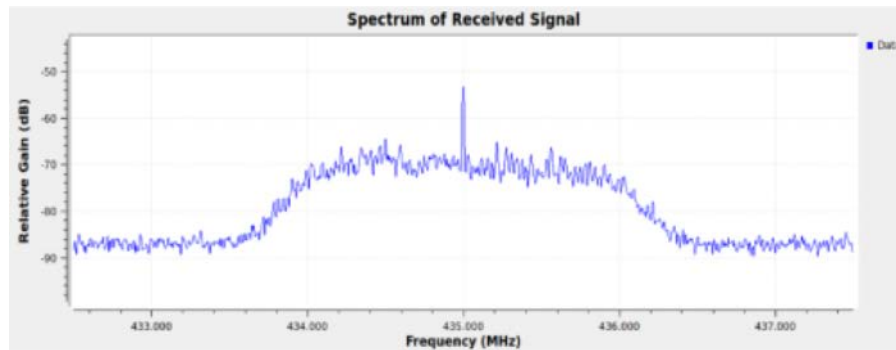


Figure 8: Spectrum of received signal. Frequency domain OFDM signal received from the receiver station.



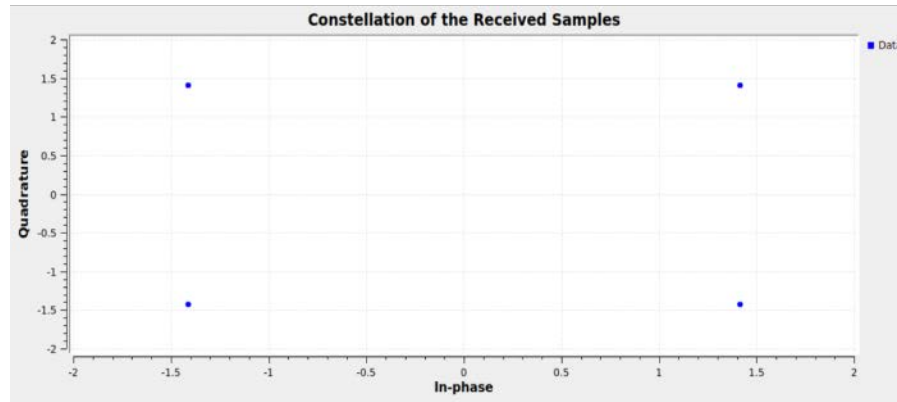


Figure 9: Constellation Diagram of Received Samples.

## 4.2 Effects of shadowing

We used a really low transmit power for all the experiments. This was done to minimize any interference to nearby ham radio operators. We also verbally announced our call sign every few minutes and monitored the frequency continuously to verify that there was no activity for the duration of our experiments.

A consequence of this very low power was a very anomalous observation during our experiments. Seemingly randomly we would get no received signal or a very attenuated signal with the same reception and transmission code and unaltered antenna conditions. This strange behavior would resolve itself and was very difficult to debug. We figured out the reason for this accidentally as well. During one of the experimental runs, the received signal stopped mid transmission as soon as one of us moved directly in front of the transmit station antenna to verify the transmission parameters on the computer.

We repeated this observation with several more runs and confirmed that the anomalous behavior was caused due to the effect of our bodies shadowing the signal. Since the transmit power was kept to the minimum level, any obstruction would cause a complete drop of the received data.

## 5. Conclusion

In this hands-on project, we have used different modulation techniques, antennas and SDR devices. We have also used GNU Radio Companion to transmit and receive OFDM signals. We have explored the effect of shadowing on signal strength where received signal varies as we move between TX and RX antennas in the lab. We have also experimented how antenna length with respect to signal wavelength affects signal transmission and reception. We plan to explore more into transmitting some predetermined data and demodulate them at the receiver. We probe into the effect of signal power and bandwidth in probability of bit error at the receiver.

## 5. Future Work

With this project we learnt a number of practical considerations required for wireless transmission of OFDM signal. We would like to expand this project by building a GUI and wrapper software to create a graphical text chat box.

Another aspect we would like to go further in is cognitive radio. We were manually sensing the frequency to know when we could transmit without interference. In the future, we would like to automate this process using principle of cognitive radio. Since the actual symbol time is very small compared to analog voice that is usually transmitted in the HAM bands, with automated sensing we could transmit data in the gaps of transmission even when the frequencies are occupied.

## 7. References

[Engels, 2002] Marc Engels, Wireless OFDM Systems: How to Make Them Work? The Springer International Series in Engineering and Computer Science, Springer, Year: 2002, [ISBN: 9781402071164](#)

Husheng Li, Zhen Hu, Michael C. Wicks, Robert Caiming Qiu, Cognitive Radio Communication and Networking: Principles and Practice, Wiley, 2012, [ISBN: 978-0-470-97209-0](#)

T. M. Schmidl and D. C. Cox, "Robust frequency and timing synchronization for OFDM," in IEEE Transactions on Communications, vol. 45, no. 12, pp. 1613-1621, Dec. 1997, doi: 10.1109/26.650240. <https://ieeexplore.ieee.org/document/650240>

Tony J. Roupheal, RF and Digital Signal Processing for Software-Defined Radio, Newnes, March 2009, ISBN: 978-0750682107, available on Safari Books

### Webpages used

"Basic OFDM Tutorial", [https://wiki.gnuradio.org/index.php?title=Basic\\_OFDM\\_Tutorial](https://wiki.gnuradio.org/index.php?title=Basic_OFDM_Tutorial), Part of the GNU Radio wiki; Gives a description of the basic flow blocks used for OFDM in GNU radio companion, accessed on November 21, 2022.

"Software Defined Radio with HackRF", <https://greatscottgadgets.com/sdr/5/> Tutorial series for the hackRF transmit hardware by the manufacturer.

## 8. Acronyms

OFDM: Orthogonal Frequency Division Multiplexing

DSP: Digital Signal Processing

EM wave: Electromagnetic Wave

DFT: Discrete Fourier Transform

FFT: Fast Fourier Transform

LTE: Long Term Evolution

Wi-Fi: Wireless Fidelity

FCC: Federal Communication Commission

UHF: Ultra-High Frequency

SDR: Software Defined Radio

CRC: Cyclic Redundancy Check

QAM: Quadrature Amplitude Modulation

QPSK: Quadrature Phase Shift Keying

IDFT: Inverse Discrete Fourier Transform

IFFT: Inverse Fast Fourier Transform

SMA: sub-miniature type A

IQ: In-phase and Quadrature-phase

TX: Transmitter

RX: Receiver

PSD: Power Spectral Density

## 9. Appendices

The source code for this project can be found at this github repository: [https://github.com/Prince-John/OFDM\\_with\\_hackrf](https://github.com/Prince-John/OFDM_with_hackrf)

---

Last modified on December 7, 2022

This and other papers on recent advances in Wireless and Mobile Networking are available online at <http://www.cse.wustl.edu/~jain/cse574-22/index.html>

[Back to Raj Jain's Home Page](#)