GPS Signal Spoofing

Prasann Viswanathan Iyer (190070047)
under the supervision of
Professor Sibi Raj B Pillai

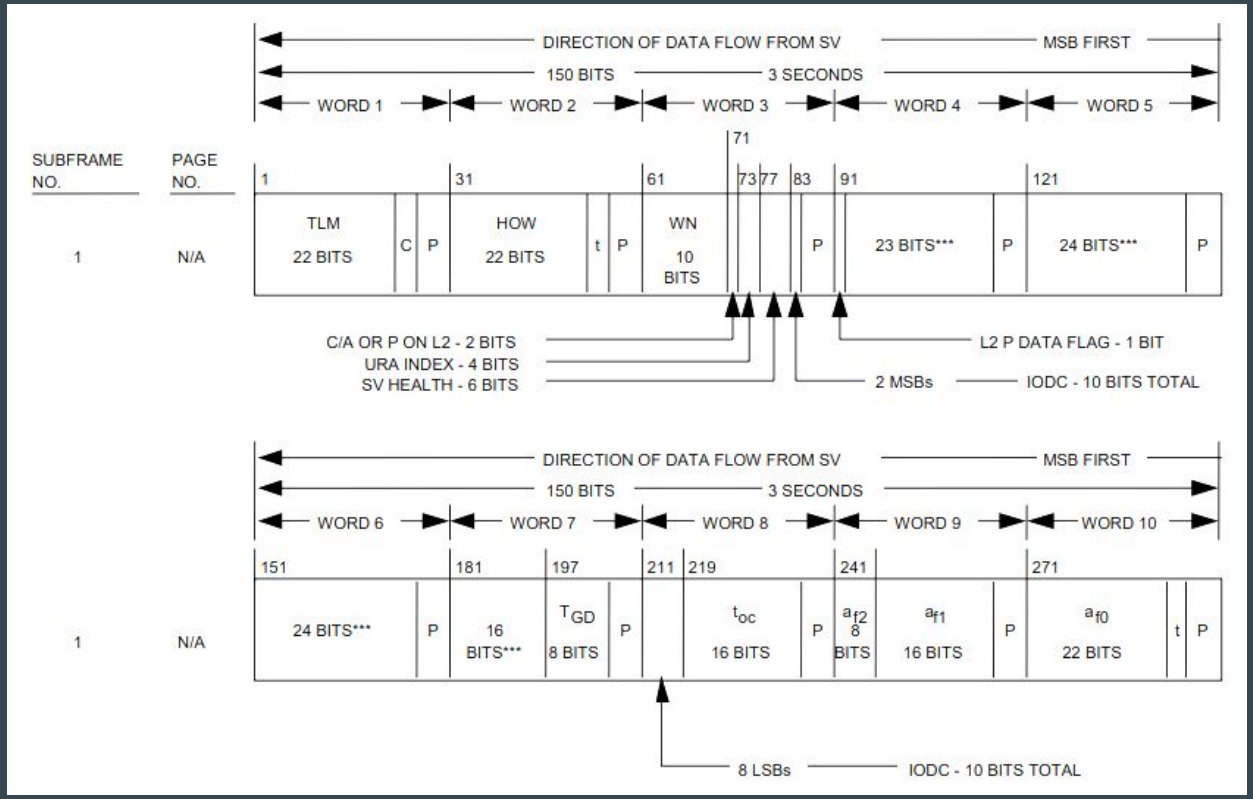
Overview

- GPS is a vital tool for everyday life but spoofing attacks are possible
- In this project we wish to search for methods to spoof GPS signals
- We explore methods in software defined radio devices to do so
- For this purpose we are using the open source library GNSS-SDR
- We are using USRP N210 devices as our software defined radios

GNSS-SDR software package

- Designed to process signals from a wide range of GNSS constellations
- It is built using the GNU Radio software development kit and is distributed under an open-source license
- Still need a radio frequency front-end that down-converts signals to a lower frequency - USRP N210 is used
- `gnss-sdr --config_file=file_name.conf`
- On execution, this creates .geojson, .kml and .gpx files

GPS Signal Structure for PRN 1-32



GNSS Signal Structure

- Carrier Signal, PRN code, Navigation Data

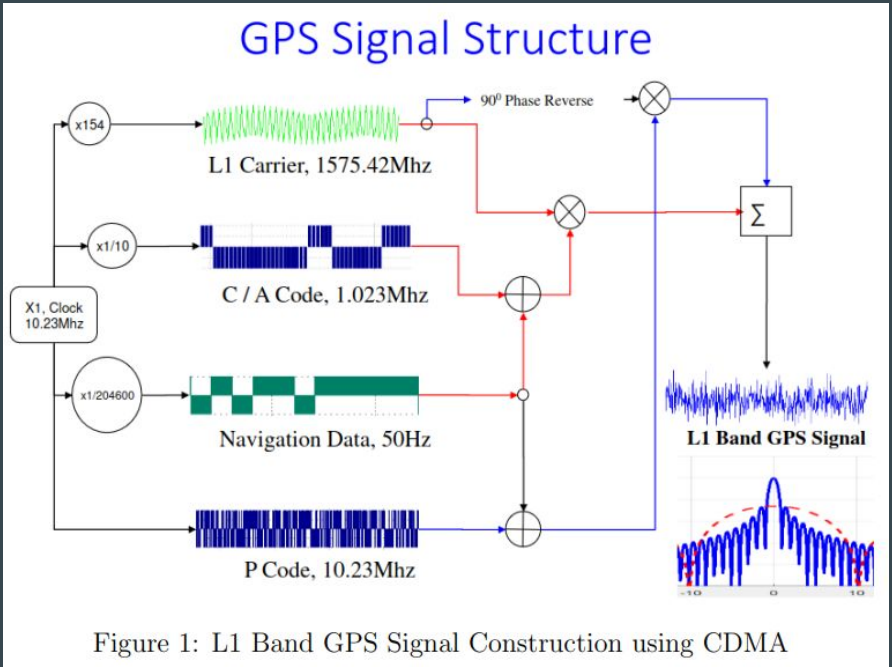


Figure 1: L1 Band GPS Signal Construction using CDMA

GPS PRN (Gold Codes) and Coarse Acquisition (C/A) code

- The Gold Codes are generated using a pair of shift registers with feedback
- C/A code, in GPS is made of two shift registers, G1 and G2

```
# init registers
G1 = [1 for i in range(10)]
G2 = [1 for i in range(10)]

# work out first 10 bits
ca = []
for i in range(10):
    g1 = shift(G1, [3,10], [10]) #feedback 3,10, output 10
    g2 = shift(G2, [2,3,6,8,9,10], [2,6]) #feedback 2,3,6,8,9,10, output 2,6 for sat 1
    ca.append((g1 + g2) % 2)

print ca
```

Exp 1: (Random PRN Generation With Fixed Navigation Data)

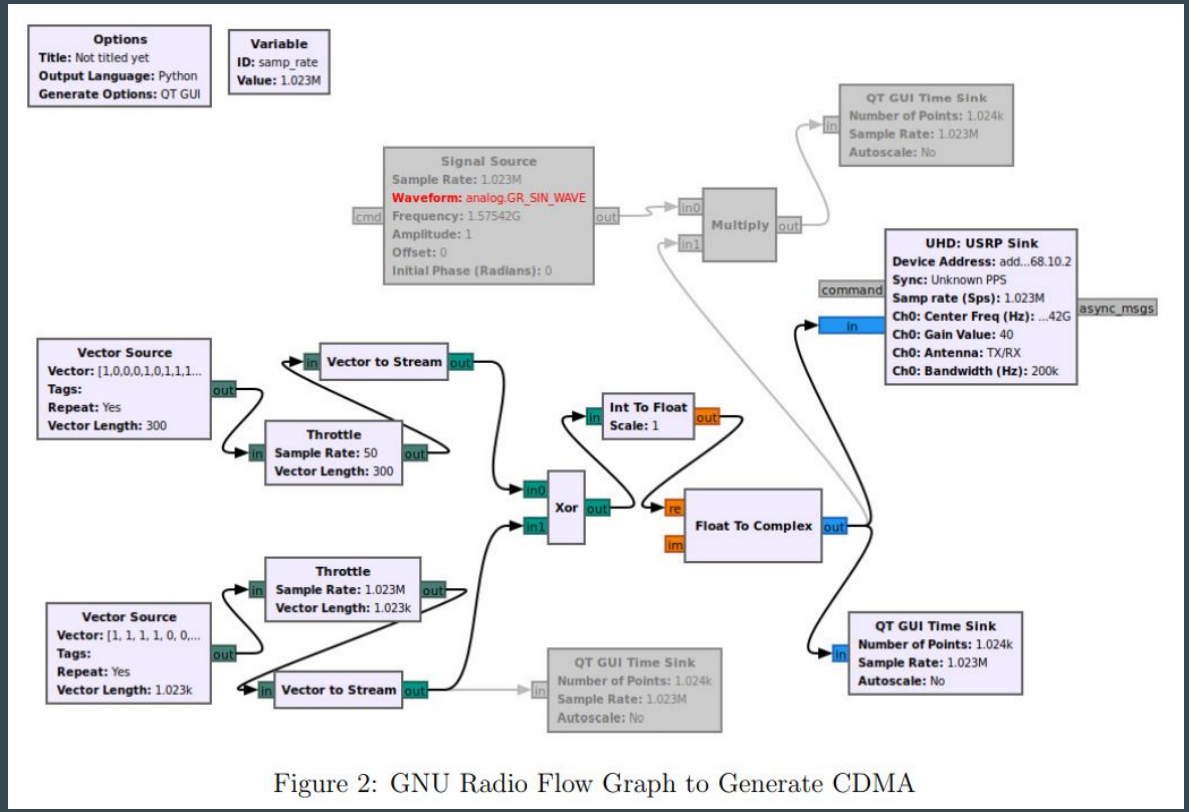


Figure 2: GNU Radio Flow Graph to Generate CDMA

Results of Experiment 1

Actual Position

Displaced Position

Figure 3: Effect of Experiment 1 on Google Maps

Exp 2 (Manipulation of just PRN of data) :

- On running the modified .mat file (with changed PRN number)
- The signal acts as a basic random stream jammer

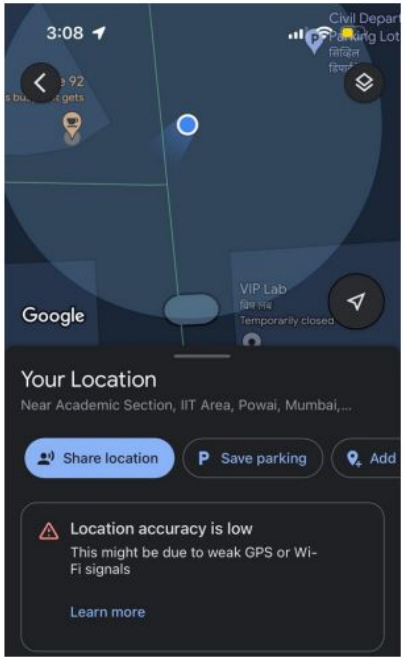


Figure 4: Google Maps on Signals from Changed PRN Signal Data

Conclusion and Future Work

- I have tried two methods but there are many more possibilities to explore, and different bits to try to manipulate to spoof the GPS signals
- In the future work it may be worth our while to explore the package at this link:
  - https://github.com/osqzss/gps-sdr-sim

Thank You!