FLINDERS UNIVERSITY

HONOURS THESIS

Local GPS Spoofing using a Software Defined Radio

Author:
Alastair WIEGELMANN

Supervisor:
Dr. Saeed REHMAN

A thesis submitted in fulfilment of the requirements for the degree of Bachelour of Engineering(Electrical and Electronic)(Honours)

May 8, 2021

Declaration of Authorship

I, Alastair WIEGELMANN, declare that this thesis titled, "Local GPS Spoofing using a Software Defined Radio" and the work presented in it are my own. I confirm that:

- This work was done wholly while in candidature for a degree of Bachelour of Engineering(Electrical and Electronic)(Honours).
- This document is in accordance with the plagiarism policy of Flinders University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed:

_____

Date:

_____

Abstract

Alastair WIEGELMANN

Local GPS Spoofing using a Software Defined Radio

As GNSS technology becomes more and more prevelant in society more needs to be done to ensure that it remains a robust system. There is a distinct issue with sattellite technology. That is that the design life time leaves them open to attack as technology propoells forward. Especially over the past 15 years the rate of expansion of technology has been high. While the GNSS system as a whole may have been technologically advanced compared to civilian technology when launched, that technology, and others, trickles down in to the hands of attackers. This thesis pointed out the ease in which a spoofing attack was able to be performed. The results show that with reletively low amounts of money and processing power, as well as technnical understasnding, successful spoofing attacks were performed with ease. While it is also true that with the setup used for testing that there were clear signs that the signal was spoofed, as shown by the comparison between real signals and spoofed signals, there are products that do not have the processign power to perform softawre based anti spoofing checks. These include embedded systems, as well as existing systems. Many industries are reluctant to change equipment for many years, even in important industries like energy. This leaves this infrastructure open to attacks from this kind of system especially given how portable it is [27].

Acknowledgements

I wish to thank all those that have supported me through not only my thesis, but my entire degree.

Contents

List of Figures

List of Tables

List of Abbreviations

BOC	**B**inary **O**ffset **C**arrier
BPSK	**B**inary **P**hase-**S**hift **K**eying
CDMA	**C**ode **D**ivision **M**ultiple **A**ccess
COTS	**C**ommerical **O**ff **T**he **S**helf
DSP	**D**igital **S**ignal **P**rocessing
EGA	**E**uropean **G**NSS **A**gency
EM	**E**lectro**M**agnetic
ESA	**E**uropean **S**pace **A**gency
FDMA	**F**requency **D**ivision **M**ultiple **A**ccess
GLONASS	**GLO**bal **NA**vigation **S**atellite **S**ystem
GNSS	**G**lobal **N**avigation **S**atellite **S**ystem
GPS	**G**lobal **P**ositioning **S**ystem
IGSO	**I**nclined **G**eo **S**ynchronous **O**rbit
IRNSS	**I**ndian **R**eginal **N**avigation **S**atellite **S**ystem
LEO	**L**ow **E**arth **O**rbit
MEO	**M**edium **E**arth **O**rbit
NavIC	**Nav**igation (with) **I**ndian **C**onstellation
NMEA	**N**ational **M**arine **E**lectronics **A**ssociation
OSNMA	**O**pen **S**ervice **N**avigation **M**essage **A**uthentication
PNT	**P**osition, **N**avigation and **T**iming
PVT	**P**osition, **V**elocity and **T**iming
QFSS	**Q**uasi-**Z**enith **S**atellite **S**ystem
RF	**R**adio **F**requency
RHCP	**R**ight **H**and **C**ircular **P**olarisation
SDR	**S**oftware **D**efined **R**adio
SNR	**S**ignal (to) **N**oise **R**atio
SPS	**S**amples **P**er **S**econd
UAV	**U**nmanned **A**erial **V**ehicle
V2V	**V**ehicle (to) **V**ehivle (communication)
V2X	**V**ehicle (to) (everything) (communication)
XML	e**X**tensible **M**arkup **L**anguage
WSF	**W**hat (it) **S**tands **F**or

Physical Constants

Speed of Light	$c_0 = 2.997\,924\,58 \times 10^8\,\mathrm{m\,s^{-1}}$ (exact)
Standard Gravitational Parameter of Earth	$\mu_{earth} = 3.986\,004\,418 \times 10^{14}\,\mathrm{m^3\,s^{-2}}$
Constant Name	$Symbol = ConstantValue$ with units

List of Symbols

Symbol	Name	Unit
a	distance	m
P	power	W ($\mathrm{J\,s^{-1}}$)
ω	angular frequency	rad
μ	standard gravitational parameter	$\mathrm{m^3 s^{-2}}$

Chapter 1

Introduction

1.1 Motivation

As society moves through the age of technology there is an exponential reliance on reliable access to position and time data. The main source of this infomation over the recent decades has been through GNSS constellations. GNSS services are now tightly integrated with many facets of life from personal navigation, public transport and management of energy infrastructure. This has made these services the target of attacks. In order to provide adequete defence knowledge of how the attacks are performed is required. There has been alot more research put into the defence of spoofing attacks, and not so into the method of performing a successful spoofing attack or circumventing existing anti-spoofing methods.

As it currently stands there is no active research or efforts to do so from within Flinders University. Therefore, to ensure that Flinders is able to keep up with moving trends and ever advancing technology this project was devised. This thesis will document background information on both GNSS operating principles as well as background research in spoofing. A workflow was generated and will be used as a starting point for continual research.

1.2 Aims and Benefits

The aims of this thesis are to investigate and perform a GPS spoofing attack in order to gain a better understanding of the operation of the GPS infrastructure and attack methodology. This will be used to create a baseline for SDR capabilities reasearch from within Flinders Universitywhere future reasearch can build upon this inital documentation. The depth of research into the most cutting edge SDR and GPS Spoofing technologies will therefore not be covered in this paper but will be the topic of future research within the College

of Science and Engineering at Flinders University. There will be some emphasis placed on the technical knowledge requried to perform such attacks and the cost of performing them now as opposed to the past. This will allow for further work in counter-measures of GPS spoofing. This thesis will purely concentrate on the research of and implementation of a spoofing device. There will be no implementation of anti-spoofing methodology.

relate this to the electronic warefare department / chair here at flinders. GPS SPoofing/jamming is one part of this section that can be used by students for research or testing.

1.3 Research Questions

1. What resources are required to perform a spoofing attack on commercial GPS receiver?
2. What effort and technical expertise is required for a spoofing attack on a commercial GPS receiver?
3. How can a prototype GPS spoofer be implemented in a controlled environment?
4. How could a prototype be implemented in a real-time static or dynamic environment?

1.4 Limitations

Due to hardware and software limitations, all testing will be performed on the Navstar GPS system only. There will be no multi constellation. However the theory and basic structure of the attacks are relevant to all constellations since the same trilateration technique is common to them all.

Since GPS and more speficically the L1 frequency band of GPS is so ubiquitous in society there is open source software available that made this project achieveable. While it would be possilbe to extend the project to encompass other constellations and frequency bands, this would require much more time that is allowed for.

1.5 Thesis Structure

The rest of this thesis will have a structure as follows, Chapter 2 will introduce the history and concepts in GNSS technology as well as defining and introducing GNSS spoofing. Chapter 3 provides a summary of relevant research in the area of GNSS spoofing attacks and defences. Spoof defence will include detection and mitigation. Chapter 4 outlines the method used in the spoofing attack. Chapter 5 will show the results gathered from the experimentation. Chapter 6 will provide discussion regarding the results of the experiments as well as issues and solutions encoutered while performing the experiments as well as recommendations for future work. Finally chapter 7 willl provide a conclusion to the project.

Chapter 2

GNSS Systems Overview

2.1 History of GNSS Systems

In 2021 there are many different GNSS systems that are in place that service the globe. It is a technology that has become deeply ingrained in the everyday lives of most people around the world. The first digital based navigation system similar to what we know today was the use of terrestrial based radio transmitters. The concept was similar to that of the current satellite based systems, namely the use of psuedoranges, although the accuracy was far lower than is acceptable today. The USA developed and commissioned the first satellite based nanvigation system.

As of 2021 there are six operational GNSS systems in use. These are GPS (USA), GLONASS (Russia), Galileo (EU), BeiDou (China), IRNSS/NavIC (India) and QZSS (Japan). The QZSS system currently acts to complement the coverage of GPS in the East Asian and Oceanic regions with 4 operational satellites. There are plans to increase this number of satellites to allow for stand alone use as a GNSS provider [3]. The Indian IRNSS similarly provides regional covereage around India with 8 satellites in geostationary orbit [25] . There are three categories of orbit, L EO, MEO and GEO. These are so categorised by how far from the earths surface the satellite orbits. Current GNSS systems utelise MEO orbits.

GNSS, and more specifically GPS and GLONASS, date back to 1957 during the space race between the USA and the then USSR [2]. When Russian satellite Sputnik 1 was launched scientists at the John Hopkins University were able to track its position and velocity by measuring the doppler shift of the craft. This tracking from Doppler shift measurements contniued with the launch of the subsequent satellites Sputnik 2 and Explorer 1. After this it was thought that the process could be reversed such that a satellite with a known position could be used to resolve an unknown position on earth. In the 1960's the TRANSIT satellite navigation system was made operational

for US Navy use, mainly for postion and navigation of nuclear ballistic missile submarines. TRANSIT received strong support due to the accuracy of up to 80ft (24m) which was a significant improvement over existing VLF (Very Low Frequency) hyperbolic navigation systems. After 32 years of operation the system was retired in 1996 after proving that space crafts could be reliable [6].

In 1973 the US combined two existing programmes in TIMATION and 'Project 621B' to form the 'NAVSTAR Global Positioning System' which would later become known more commonly as GPS. The initial intention for the use of GPS was for military only. However, in 1983 there was an incident that saw a Korean Airlines flight shot down by a Soviet fighter mistaking it for a US aircraft when it wandered off course. After this incident President Reagen announced that GPS would be made available for civilian use. The military insisted that the accuracy of the system be purposley degraded for civilian use though selective availabililty such that GPS could not be used by adversaries. In 1993 the system was declared operational. To combat the intentional accuracy reduction of the GPS system augmentation systems started to appear. Soon after there were Government funded versions of DGPS (Differetial GPS) systems [2]. Augmentation systems significantly increases the accuracy by using a receiver with a known location and having that reciever calculate its position from the satellite signals and compare with the known position. These corrections are then broadcast.

The Soviet Union launched their first GLONASS satellite in 1982, and in the following three years 10 more were launched. There are some technical differences between the GLONASS and GPS constellations. The orbital planes are different and GLONASS uses an FDMA (Frequency Division Multiple Access) scheme as opposed to the GPS's CDMA (Code Division Multiple Access). In 1993 president Yeltsin declared that the GLONASS constllation was fully operational, however this was not the case.

The TRANSIT satellite system orbit was in a LEO (Low Earth Orbit) polar orbit, whereas all modern GNSS systems utelise a MEO (medium earth orbit) ranging from 20,000km to 23,000km above the earths surface with multiple orbital planes. The number of planes differs between the different constellations as discussed below. The lower the orbit, the higher the velocity requried to maintain the orbit as shown by the orbital mechanics equation 2.1. Equally a higher orbit requires a lower velocity which has impact on the doppler shift at the receivers. Another factor is aerodynamic drag, which is higher the closer to the earths surface due to the atmosphere.

$$v \approx \frac{2\pi a}{T} \approx \sqrt{\frac{\mu_{earth}}{a}} \tag{2.1}$$

The history of the two other main GNSS systems is much shorter, with the Galileo constellation coming as a form of sovereignty for the European Union. The fist sattelite was launched in 2011, and the service became operational in 2016. There is also a network of GPS augmnetation sites that provide improved accuracy for those in the EU. This system is named EGNOS. This system provided an average of 1.5m accuracy over the EU territory. This was provided through the use of ground stations and a geostationary satellite broadcasting the timing corrections.

2.2 GNSS Systems

2.2.1 Introduction to GNSS Constellations

GNSS is a term used to describe any satllelite system that provides positon and timing information. All GNSS systems in use today have three sepearte segements that encompass the term GNSS. That is the ground segment, space segment and user segment. These are used in conjunction to allow the user to calculate with accuracy up to $\pm 10cm$. In order to calculate an unknown poistion on earth, the exact position of the orbiting satellite must be known. The satellite will send it's exact position as well as it's current time down to the earths surface. It's location, or ephemeris, can be tracked due to Kepler's laws and celestial mechanics. The time on board satellites is kept via the use of caesium based atomic clocks. The GPS clocks are accurate to approximatly 10 nanoseconds , however, receviers will lose timing due to the interpretation reference of signals and typically provide accuracy of 100 nanoseconds. The value of the clocks are constantly monitoed by the ground segment and updated when required. Part of the Receviers (the user segment) will pick up this signal. The components of the message sent are quite simple and consist mostly of the current time (of the satellite) and where the sattelite is in the WGS-84 coordinate system[1]. This coordinate system has its origin at the centre of mass of the earth with the Z axis pointing at the north pole, the X axis pointing towards the prime meridian and the y axis perpendicular to both other axes. Due to the reletive motion of the satllite and the reciever the transmitted signal will be shifted up or down the frequency range due to the doppler effect. The combination of this doppler shift, time taken to arrive

and the satellite current location can be used to solve the position in three dimensional space. In order to solve for all dimensions (including time) four satellites are reqruied since there are essentially 4 unknown terms to solve for as shown in equation 2.2 [1]. The ρ_i term indicates the distance from the recviever to that particular satellite and is known as a psudeorange. This method of position calculation is known as trilateration. The model shown below is a simplified model that ignores the effects of relativity.

$$\rho_i = \sqrt{(x_i - x_u)^2 + (y_i - y_u)^2 + (z_i - z_u)^2} + c\Delta t \tag{2.2}$$

As can be seen from the above equation 2.2 the accurate synchronisation of time betweeen the receiver and the satellites is required in order to calcaulte an accurate position. Due to the mathmatical requirements, a minimum of 4 satellites need to be in 'sight' of the receiver at all times.

look at RN32 for position and time calculations

Each of the operational constellations use the same fundamentals to provide accurate postion data, but each differ in some key aspects as discussed below.

2.2.2 Trilateration

The process of trilateration uses objects of known locations to calculate the unknown location of other objects. This is done through the use of overlapping circles based on how far the objects are apart. This is known as a psudeorange. To use satellites to determine the location of a reciever the exact location of the satellites must be known, as well as relitive distance. Each satellite sends its precise orbital location (ephemeris), as well as the coarse orbital location (almanac) of the rest of the constellation as part of the navigational data. This coupled with the psudeorange of the satellite allows for calculating the position of the reciever. Psuedoranges rely on the knowledge that electromagnetic radiation propagates at the speed of light, as shown in equation 2.3. By measuring the time taken for the signal to transition from the each of the satellites to the receiver, a sphere of radius d centred on the radius indicates all possible locations that the reciever could be. By adding a second satellite, and second sphere based on the psuedorange, the posible locations of the reciever are reduced based on where the spheres intersect. For 2D position only 3 satellites are needed to have only a single possilbe solution, whereas 3 dimensional position requires 4 satellites as shown in Figure 2.1.

$$d = c \times t \tag{2.3}$$

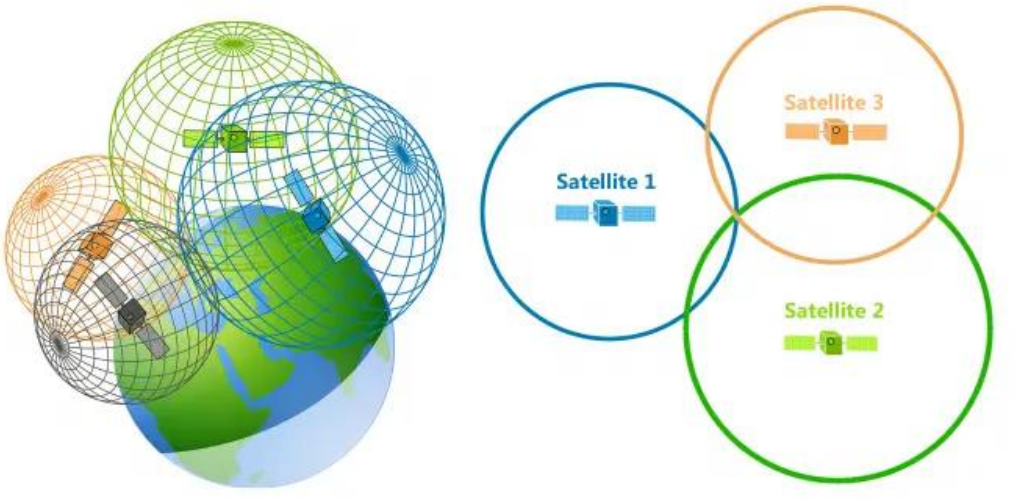

FIGURE 2.1: Illustration of trilateration used in GNSS positioning

2.2.3 Kepler's Laws of Planetary Motion

In the 1600's German astronomer Johannes Kepler described the orbits of the solar systems planets around the sun using three laws. These laws famously moved our understanding of orbits away from circles and described them as ellipses. The position of modern day satellites need to be accurtatly predicated and as such these laws have become important to the way we live our lives. Kepler's laws are as follows; First law states that the orbit of every planet is an elllipse with the sun at the one of the two foci. Second law states that a line joining the planet to the sun will sweep out equal area during equal intervals of time. The third law states that the ratio of the orbital period with the cube of the semi-major axis is the same for all objects orbiting the same primary. These laws can be adapted to objects that orbit other objects other than the sun. Examples are moons orbiting plantes and artifical satellites orbiting the earth.

2.2.4 GPS

The GPS constellation consists of a nominal 24 satelelites in 6 orbital planes (nominally 4 satellites per plane) to ensure that there is coverage globally at

all times. There are also some spare satellites that are in orbit in the event that a operational satellite malfunctions. The constellation orbits at an altitude of 20,200km which equates to an orbital period of 12hours. There are multiple frequencies of differeing propoerties that each satellite will transmit at. For GPS these are named the L1, L2 and L5 bands and have centre frequencies of 1575.42MHz, 1227.60MHz and 1176.45MHz respectively [18]. This is shown graphically in Figure 2.2. The L1 band is the most commonly used and was the first one to be made operational. In the past the L1 band was used for civilian purposes and the L2 band was a military band. Nowadays both have active cilivilan and encrypted signals co-exiting within their respective frequncy bands. GPS predominately uses BPSK but also utelises BOC for signal modulation accross all of the bands.

Initially the civilian C/A code was purposley degraded to ensure that adversaries of the USA could not use the system to its maximum effect. In May 2000 President Bill Clinton directed the removal of selective availabililty from the GPS service, and in 2007 it was announced that the newest version of GPS satellites would be manufactured without the selective availabililty capapbility [15] [20].

GPS hardware has had a number of revisions over the life of the system in the form of Blocks. Each block is a major revision, current generation satellites are Block III satellites. There are currenntly 4 block III satellites in service with 6 more planned for launch. There are 12 block IIF satellites in operation which were launched from 2010 to 2016. Block IIR has 8 currently operational from 13 launches, block IIR-M has 7 operational from 8 launches and there are no operational satellites from Block I, II or IIA. This totals 31 opeartional satellites, 24 in opeartion and 7 spares as summarised in Table 2.1

Accuracy of the GPS system has increased over the years, and since selective availabililty was legislated against, to approximatly 3m for public access and 3-4cm for encrypted.

2.2.5 Galileo

The Galileo constellation is a GNSS created by the ESA (European Space Agency) and operated by the EGA (European GNSS Agency) as a way of providing a modern navigation system that has global covereage. The Galileo constellation has 30 nominal satellites accross 3 orbital planes. The first Galileo

TABLE 2.1: Summary of current and former GPS satellites

Block	Launched	In Service
Block I	11	0
Block II	9	0
Block IIA	19	0
Block IIR	13	8
Block IIR-M	8	7
Block IIF	12	12
Block III	4	4
Total	**76**	**31**

satellite was launched in 2011. The orbit height of the Galileo constellation is higher than the GPS orbit at 23,222 km.

Galileo operates on 3 different frequency bands, E1, E5 and E6. E1 shares the same centre frequency as the GPS L1 band, 1575.42 MHz. The E6 band does not share a frequncy with the GPS ssytem and operates at 1278.75 MHz. The E5 band is split into E5a and E5b sub-bands with E5a sharing the same freqeuency as L5, 1176.45 MHz, and E5b at 1207.14 MHz. The arrangmeent of the frequency bands can be seen in Figure 2.2.

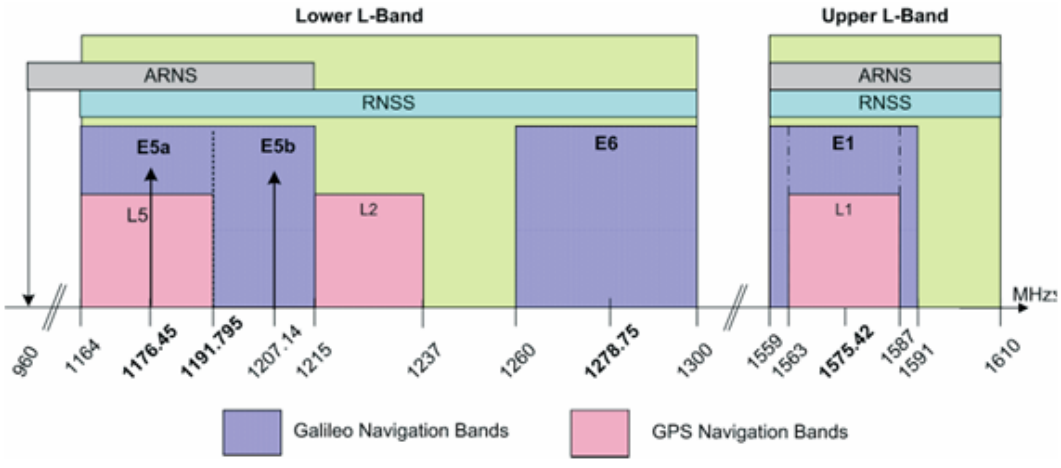

FIGURE 2.2: Galileo and GPS signal frequency arrangement

To maintain interoperability between receivers on the L1 and E1 bands the modulation scemes differ. The E1 band utileses Composite BOC modulation, E6 uetelises BPSK, and the E5 bands utelise Alternative BOC modulation.

Galileo offers superior accuracy than the other constellations with 1m for the public access and 1cm for encrypted service.

There are special satellites that are part of the Galileo constallation whose job it is to ensure validity. These are known as GIOVE (Galileo In Orbit Validation Element) satellites. There is GIOVE-A and GIOVE-B launched in 2005 and 2008 respectively. Initially these satellites transmitted GNSS test signals on the E1 and E6 frequyency bands to allow for monitoring and testing while the rest of the Galileo constellation was being commissioned [11]. Over this time they have provided great infomation on the short and long term reliabilty and accuracy of the on board atmoic clocks [22].

2.2.6 GLONASS

The Russian GLONASS constellation has it's hsitory tightly intertwined with that of GPS and the space race, as mentioned above in 2.1. GLONASS consits of a nominal 24 satellites in 3 orbital planes. Since GLONASS uses FDMA, each satellite needs to transmit on a unique frequency. This is in contrast to all other GNSS systems that use CDMA. Extra effort must therefore be applied to the reception of the signals since Doppler effects must be carefully considered. The use of FDMA does make GLOANSS more resilient against jamming and spoofing attacks. In a CDMA system, like GPS, all satellites share the same carrier freqeuency (ignoring the Doppler Effect), thus if an attack is performed all satellites are suceptible. Where as the GLONASS satellites all occupy seperate freqyency bands making a system wide attack much harder and more expensive to perform. This was the motivation of using FDMA over CDMA initially. The use of FDMA over CDMA also causes and interoperability issue when considering multi constellation support. The recever must become much more complex in order to support not only multiple carrier frequencies of different constellations but also due to the different access schemes. This increases cost and complexity where Galileo is much more compaitble for this use case. There are three freqeuency bands that GLONASS operates in, L1, L2 and L3. These are seperate to the L1, L2 of GPS.

GLONASS L1 band is from 1598.0625 MHz to 1605.375 MHz split into 14 channels. Each carrier is 562.5 kHz apart and is characterised by equation 2.4. k represents the channel number of the band and ranges from -7 to +6.

The L2 band ranges from 1242.9375 MHz to 1248.625 MHz with each carrier separated by 437.5 kHz.

The L3 band ranges from 1197.9375 MHz to 1203.625 MHz with the same carrier sepeartion as L2.

$$\begin{aligned} f_{k_{L1}} &= f_{0_{L1}} + k\Delta f_{L1} \\ f_{k_{L2}} &= f_{0_{L2}} + k\Delta f_{L2} \\ f_{k_{L3}} &= f_{0_{L3}} + k\Delta f_{L3} \end{aligned} \tag{2.4}$$

2.2.7 BeiDou

From the BeiDou official website it states that "BeiDou has been constructed and operated by China with an eye on the needs of the country's national sceurity, economic and social development", and was previously known as COMPASS. This is China's attempt at creating a sovreign navigation constellation.

The BeiDou constellation is made up of 35 satellites in total. This includes 5 geostationary satellites, 27 MEO satllites and 3 inclined geosynchronous sateliitels to give total earth coverage. The MEO satellites orbit at a height of 21,500km, and are distributed accross 3 orbital planes. Through the use of the geostationary and geosynchronous satellites there is a region around Asia that has higher accuracy than what is present at other areas of the globe. This accuracy for open service is approximatly 2.6m around the Asia Pacific region and 3.6m elsewhere. The constellation contains 3 operating bands, B1, B2 and B3, which have frequencies as shown in Table 2.2. Each of the bands use the CDMA access scheme.

2.2.8 Augmentation Systems

As mentinoned above there are two other GNSS constellations that act to improve availabililty and accuracy in regional areas. These are the Japanese QZSS and Indian IRNSS. Both of these extend the abilities of the USA GPS system. The 4 satellites that are operational for the QZSS constellation are able to transmit on the L1 and L5 band simultaneously. Doing so helps to resolve ionospheric errors by facilitating resolution of position from multiple frequencies [4].

The IRNSS constellation is different to the others mentioned above due to its orbit altitude of 36,000km making them geostation. All of the satellites are postiioned at this orbit. This allows for a very narrow and defined region of useability, which is over India.

TABLE 2.2: Sunmmary of BeiDou Signal Properties

Signal	Carrier Frequency (MHz)	Modulation Type
B1-I	1561.098	BPSK
B1-Q	1561.098	BPSK
B1-C	1575.420	MBOC(6,1,1/11)
B1	1575.420	BOC(14,2)
B2-I	1207.140	BPSK
B2-Q	1207.140	BPSK
B2a	1176.460	AltBOC(15,10)
B2b	1207.140	AltBOC(15,10)
B3-I	1268.520	BPSK
B3-Q	1268.520	BPSK
B3-A	1268.520	BOC(15,2.5)
B3	1268.520	BPSK

Other forms of augmentation as mentioned in Section 2.1 were through ground based stations that use receivers to determine the timing error and broadcast these values in order to make the solution to the positon cacluation more accurate. This type of system allows for sub 1m accuracy. These systems are typically rolled out geographically locally and run by those local Governments.

2.2.9 GNSS Receivers

Traditional GNSS receivers are specialised hardware components that are able to receive the spread spectrum signal from the GNSS satellite and perform the required calculations to acquire the PVT data. This data is then provided serially to a main processor of the system in the form of NMEA sentences. There are many sentence types and not all receivers will output all sentence types.

2.3 Applications of GNSS

GNSS applications are broad and deeply ingradined in the almost everyones everyday lives. These applications vary from providing postion and navigation information for maps on a smartphone or sat-nav devices to providing accurtate timing infomation for financial institutions or energy infrastructure [24] as shown in Figure 2.3. This

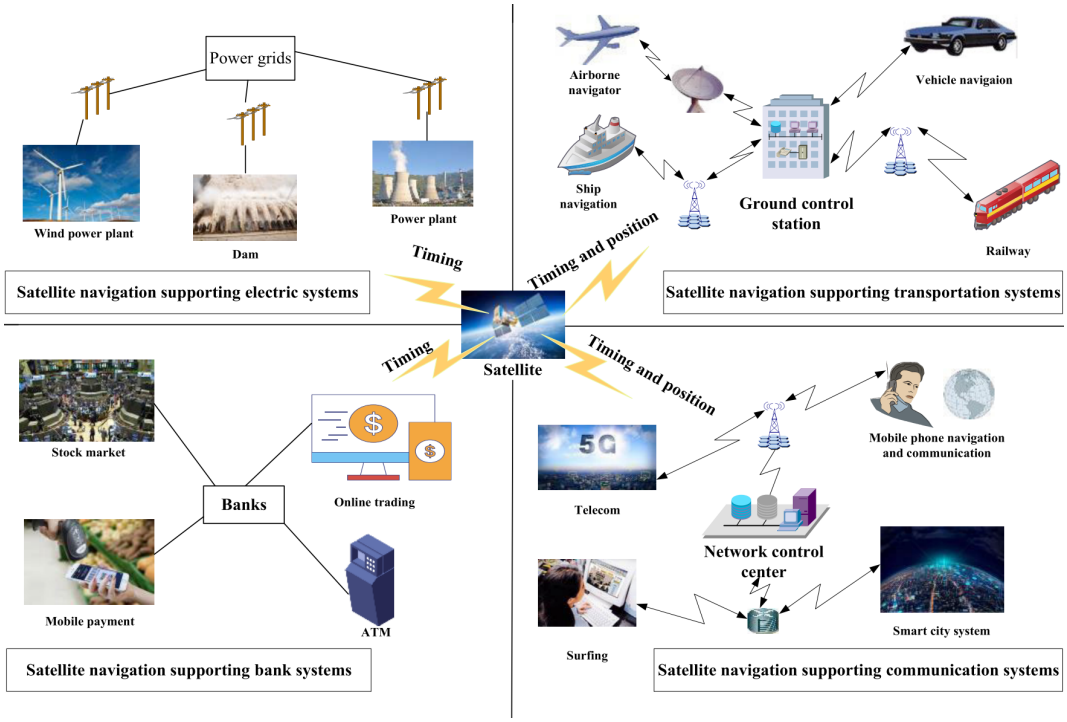

FIGURE 2.3: Applications of GNSS position and timing [24]

2.4 Errors within GNSS

The main fight against GNSS positional accuracy is the introduction of different types of errors. These can be narrowed into three main groups; Satellite errors, Propogation erros and Receiver errors. Propagation errors are most common. When the signals pass through the ionosphere and the troposphere the signals refract, extending the time taken to get to the receiver, thus making the psudeorange not accurate. Other propagation errors include multipath and obstructions errors. Both of which are most notable in built up urban environments of in valleys where direct view of the sky can be difficult.

Satellite errors occur when the predicated orbit differes to the actual orbit. Other causes of errors from the satellites are due to drift of the onboard

TABLE 2.3: Summary of GPS Errors

Source of Error	**Error Range**
Satellite Clocks	$\pm 2m$
Orbital Errors	$\pm 2.5m$
Ionospheric Delays	$\pm 5m$
Tropospheric Delays	$\pm 0.5m$
Receiver Noise	$\pm 0.3m$
Multipath Errors	$\pm 1m$

atomic clocks as well as low elevations where there are propotionally high dilution of precision.

Receiver errors occur due to the introduction of noise therough the reception process. GNSS jamming and spoofing also constitute receiver error although these are intentional and malicious.

What all of these errors have in common is that create an incorrect value of the psudeorange which in turn incorrectly calculates the reciever position.

2.5 Spoofing Overview

Attacks on the GNSS archtiecture can broadly be divided into two categories jamming and spoofing [24] [19]. Jamming can be described as causing intentional interference in the communicationn channel as to make the recovery of signal informaiton impossible. A successful jamming attack will make it impossibe to begin tracking satellites and thus be unable to calculate any of the PVT data. This differs from spoofing attacks where the main interest is to deceive any reciever that picks ups the signal into thinking it is elsewhere or else-when. This is done by different methods and stems from which property of the signal is being modified for the attack. A successful spoofing attack will have the receiver 'tracking' the signal produced by the spoofer and the receiver will not be aware that an attack is taking place. Common spoofing attacks are explained below.

2.5.1 Meaconing

Meaconing is a type of GNSS spoofing attack that involves recording a legitimate GNSS signal and re-broadcasting. This could be either instantly or at a different time or place. This requries little prior knowledge of the GNSS system that the attacker wishes to record other when used with existing open source software packages. Although there is a requirenment of having the right equipment to be able to capture the raw analog signal.

2.5.2 Signal Generation

There are software packages and off the shelf hardware that are designed for testing GNSS receivers in a laboratory setting. These can be used to generate a that can be played in such a manner as to perform a spoofing attack. This differes from meaconing because knowledge of the satellite ephemeris and almanac is required. The almanac is a record of the rough location of all satellites in a constellation and the ephemeris is the exact location of each individual satellite. This knowledge is requied as to produce the same results as recording the gps signal from the desired location.

2.6 SDR Basics

Software defined radios are devices that enable the user to increase the flexibility of transmissionn and reception of RF signals by moving processing typically reserved for the analog domain into the digital domain. Thus SDR's move the signal processing from rigid and expensive hardware into flexible and in-expensive software. This allows for a wide ranges of frequncies from Hz up to GHz from the same device with minor or no hardware changes. This can also be done in real time using software. SDR's are very sensitive to the processing pipeline of the computer that they are connected to. It is not uncommon to receive an underrun error (where 'U' is printed to the output) when transmitting a signal with high sps (samples per second). This error is caused by the host computer not being able to feed the data to the radio quickly enough.

This was solved by increasing the UDP buffer size manually to at least the sample rate, and over for better results. From limited experimentation this completely resolved the issue, and opened up oppertunities to perform spoofing with low powered embedded devices like the Rasperry Pi single board computer.

move this sentence to re-

Chapter 3

Literature Review

3.1 Introduction

This section will go through the existing literature around the topic of GNSS spoofing and anti-spoofing. References were chosen based on their relevance in terms of content as well as age. There have been some significant performance increases in technologies over the past 10 years. This literature review will focus mainly on GNSS spoofing methods, with emphasis on the GPS constellation, and on potential anti-spoofing methods. While development of anti-spoofing algorithms is not an aim of this thesis, knowledge of such methods allow for understanding potential attack vectors.

3.2 Literature Review

How GPS works has been covered in depth over the past few decades. The operating pricinpals for GPS and other GNSS systems is well known and was covered in the previous chapter 2.

From literature the consensus is that the same thing that has made GPS ubiquitous with navigation and positioning has also made it a target for exploitation and manipulation. That is the workings of the infrastructure are well known and public and are transparent and predictable [10] [28]. This is problematic since this infrastructure is seen as a critical service by many industries including utility management, healthcare/ emergency services and security. Wang, Chen, and Pan [23] noted that the signals presented to the receivers are usually trusted without any authentication or other checking. The authors show that this trust can be exploited without physical access to or altering the software of the target device. One of the signal properties that makes spoofing simple is the received signal power from space which is less

than -130dBm making overpower the legitimate signal a simple task. Having such a system so prone to threats is not ideal.

3.2.1 Spoofing Attack Literature

The further development of SDR platforms has driven down the cost of launching GNSS based spoofing attacks. Devices such as the Hack-RF, USRP, BladeRF and others have been documented for this use [28] [26]. These devices are all examples of Software defined radios that are capable of duplex operation. This combined with open source software, as described in [9] [12] [28]. The former is a software package, GPS-SDR, that converts a compatible SDR into a GPS receiver wihtout any knowledge of GPS or signal procssing required. With some understanding this could be modified to capture the raw signal for use in a Meaconing spoofing attack. The later refers to the setup and use of the GPS-SDR-SIM program. This program provides a method for producing a modulated GPS signal for transmission. It requires the RINEX file for the date and time of the spoof attack as well as a set of coordinates to reproduce. Since it is open source it can be easily modified for any use case.

Wang, Chen, and Pan [23] created a spoofing device based on the HackRF SDR platform in conjunction with the open source program GPS-SIM-SDR. Hack-RF was chosen as the SDR platform because of its open source nature, it also had the required specifications to perform the spoof attack. It was shown in this paper that the use of an SDR and open source software was able to fool client devices such as apple smartphones into thinking they were else where. This included specific apps that require location data such as Uber and DiDi. The authors provided a list of recommendations to minimise the risk of being spoofed. These recommendations are non trivial and some required alterations to how the receiver processes the signal data.

Tippenhauer et al. [21] investigated the exact requirements for successfully spoofing a receiver. From the experiments it was found that there are 4 parameters that have required values in order to successfully spoof a GPS signal. That is the relative signal power must be $\geq +2dB$, the constant time offset must be $\leq 75ns$, location offset must be $\leq 500m$ and the relative time offset must be $\leq 80ns$. These values correspond to situations where the reciver already has a lock on satellites. It was found that when values outside of those mentioned above, the lock would be lost and the spoofing would be unsuccessful. The more victims that are trying to be spoofed the more restrictive the locaiton for performing the spoof becomes.

Software based GPS simulation tools similar to that of GPS-SDR-SIM have also been created using a combination of C and MATLAB [8]. In this example the author used C to ensure processing efficiency of the modulated signal, and used MATLAB to simulate multipath errors and uncertainty. The resultant file was then saved to the hard drive of the host computer. This could then be loaded into an SDR for transmission, although this was not specifically touched on in the paper.

Over recent times there has been an increase in the industries that rely on the timing and postiional data provided by GNSS systems. One such industry is autonomous vehicles, in particular drones. Drones can be used for hobbies, professional photography/ videography or for surveilance purposes. They are small and can be controlled from great distances. All commercially available drones have some form of GNSS/GPS location service built in, and as such they become a target for spoofing attacks. Some drone manufactueres have built in auto landing features in the event that the drone flys into restricted airspaces. This was to combat civilians who were flying within airports, causing safety and security issues. This is one such way that spoofing attacks could be utelised now and in the future, by transmitting a signal that would make the drone perceive itself to be in a restricted airspace and land. This kind of attack has been successfully conducted as shown in [28]. Kerns et al. [16] developed a system to perform a series of spoof attacks on UAV's based on an SDR [13]. The goal of this was to be able to control the flight path of the UAV without raising any alarm's from the victim. This paper establishes the required conditions in which a UAV will be susceptible to being captured from a spoofing attack, as well as the range of post capture control that the spoofer will have over the victim. From testing it was found that spoof attacks were successful from up to 50m and up to a velocity of 10m/s. Simulations were produced for analysis of post capture control of the UAV. When testing, both covert and overt spoofing methods were used, distinguished by whether or not the spoofer made an attempt to avoid detection. For the most part there was no practical difference between covert and overt methods since the commercial GPS units did not trigger any anti spoof mechanism when being subjected to an overt attack. Field testing showed that the spoof attempt caused unrecoverable navigation errors which resulted in the UAV crashing. Future work should increase the sophistication of the attacks. This may decrease chances of the drone crashing due to unsuccessful attacks.

There has been research into ways that GPS spoofing attacks could be used in road navigation scenarios. Zeng et al. were able to implement an

algorithm for road network modelling and navigation spoofing using GPS. This algorithm coupled with a HackRF SDR meant that the authors were able to create a lunchbox sized spoofing device. Although in research it was found that the victim devices were able to register a difference in location from network based sources and GNSS based sources, the victims prioritised the location resolved from GNSS sources over network or cellular. While this attack strategy may be successful against people not familiar with their surrounding area, someone who is familiar or is paying close attention should be able to tell they are being led to an incorrect area. Where this is less likey to be the case is with driverless vechils. In the paper written by De La Torre, Rad, and Choo [7] regarding driverless vehicle safety, it was noted that there is a significant threat to these types of systems that rely heavily on reliable GPS signals. Although there have been proposed solutions to this problem through the use of other sensor information available locally to each vehicle and in the form of an ad-hoc network known as V2V (vehicle to vehicle) and more broadly V2X (vehicle to everything) [5], this is still in its infancy and will require joint work from all vehicle manufacturers.

Psiaki and Humphreys commented on the effect of GNSS spoofing of a cooperative victim. That is when someone is willing to aid the attacker in performing an attack. This may be implemented to circumvent position based restrictions or if being GPS tracked during certain activities. Psiaki and Humphreys used the example of a fisherman wanting their GNSS receiver to falsely report the boat had stayed out of protected areas [17].

In 2012 Jafarnia-Jahromi et al. [14] investigated the different spoofing and antispoofing techniques available. Jafarnia-Jahromi et al. noted that spoofing attacks can be divided into 3 main categories: GPS signal simulator, Receiver-Based spoofers and Sophisticated Receiver based spoofers. These attack strategies come about because of vulnerabilities in the GPS system. These vulnerabilities can be described in the three operational layers of GPS, signal processing, data bit, and position/navigation solutions. Testing spoofing techniques is difficult to achieve since there are regulations around the emission of EM radiation at certain frequencies and power levels. There were three methods used to test the spoofing/antispoofing techniques. These were Indoor re-transmissions, spoofing using recorded data (No RF transmission), and using RF combiners to combine authentication and spoofed signals. The results that were acquired showed that the commercial GPS receivers were vulnerable to a number of spoofing techniques. Previous research into the effects of spoofing can be found in [13]. This predates more modern methods

for launching a successful spoofing attack and uses a specialised DSP chip within a specilised hardware configuration. The findings of this paper was used to recommend anti-spoofing methods for unsophisticated spoofing attacks. Humphreys et al. was able to implement complex spoofing setups with multiple phase locked radios that were able to overcome some anti-spoofing techniques.

Detection	**Attack Techniques**												
Techniques	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13
D1	X	X	X	X	X	X	X	X	X	X	X	X	X
D2	∼	✓	X	X	∼	X	X	X	X	X	X	X	X
D3	∼	∼	∼	∼	∼	X	X	∼	∼	∼	∼	X	X
D4	∼	✓	∼	∼	∼	∼	∼	∼	∼	∼	∼	∼	∼
D5	✓	✓	✓	✓	✓	∼	∼	✓	✓	✓	✓	∼	∼
D6	X	✓	✓	X	X	✓	X	✓	✓	X	X	✓	X
D7	X	✓	✓	∼	X	✓	∼	✓	✓	∼	X	✓	∼
D8	X	✓	✓	∼	X	✓	∼	✓	✓	∼	X	✓	∼
D9	∼	✓	✓	✓	∼	✓	✓	✓	✓	✓	∼	✓	✓
D10	✓	✓	✓	✓	✓	✓	✓	✓	∼	∼	∼	∼	∼
D11	✓	✓	✓	✓	✓	✓	✓	X	∼	∼	∼	∼	∼
D12	X	✓	✓	∼	X	✓	∼	✓	✓	∼	X	✓	∼
D13	X	✓	✓	∼	X	✓	∼	✓	✓	∼	X	✓	∼

Detection probability matrix keys: ✓– high, ∼ – intermediate or case-dependent, X – low

	Detection Techniques Key		**Attack Techniques Key**
D1	Pseudorange-based RAIM	A1	Meaconing, single RX ant., single TX ant.
D2	Observables and RPM	A2	Open-loop signal simulator
D3	Correlation function distortion monitoring	A3	RX/SP, single TX ant., no SCER
D4	Drift monitoring (clock offset, IMU/position)	A4	RX/SP, single TX ant., SCER
D5	Observables, RPM, distortion, and drift monitoring	A5	Meaconing, multi. RX ants., single TX ant.
D6	NMA*	A6	Nulling RX/SP, single TX ant., no SCER
D7	NMA* and SCER detection	A7	Nulling RX/SP, single TX ant., SCER
D8	Delayed symmetric-key SSSC*	A8	RX/SP, single TX ant., sensing of victim ant. motion
D9	NMA*, SCER detection, RPM, and drift monitoring	A9	RX/SP, multi. TX ants., no SCER
D10	Multiple RX antennas	A10	RX/SP, multi. TX ants., SCER
D11	Moving RX antenna	A11	Meaconing, multi. RX ants., multi. TX ants.
D12	Dual-RX keyless correlation of unknown SSSC codes	A12	Nulling RX/SP, multi. TX ants., no SCER
D13	Symmetric-key SSSC* [e.g., P(Y) equiv.]	A13	Nulling RX/SP, multi. TX ants., SCER

* Detection techniques requiring changes to the Signal In Space (SIS); TX: Transmitter; RX: Receiver; RX/SP: Receiver-Spoofer

FIGURE 3.1: Summary of spoofing attack and defence methods and their effectiveness against each other as found in [17]

3.2.2 Anti-Spoofing Literature

It is common within research to investigate methods of spoofing attack and to combine this with recommendations for anti-spoofing. This was the case with Jafarnia-Jahromi et al. [14] and Humphreys et al. [13]. The later, as mentioned above in Section 3.2.1 a spoofing device was developed and tested against some anti-spoofing methods. From this anti-spoofing recommendations were developed. The recommedations are as per Jafarnia-Jahromi et al. Jafarnia-Jahromi et al. [14] investigated antispoofing techniques available. Antispoofing can be broken down into 2 groups spoof detection and spoof mitigation, with each of these being able to be further broken into subcategories. The effectiveness of each spoof detection technique was tabulated and

compared. As was the spoof mitigation techniques. Each detection and mitigation method was given a complexity, effectiveness and spoofing scenario generality rating with notes made about the received capability requirements and are summarised in Table 3.1 and Table 3.2. It was shown that with modest, low complexity spoof detection and mitigation strategies some of the spoof attacks were able to be overcome.

TABLE 3.1: Summary of Spoofing Detection Methods from [14]

Anti-Spoofing method	**Spoofing Feature**	**Complexity**	**Effectiveness**	**Receiver required capability**	**Spoofing scenario generality**
C/N_0 monitoring	Higher C/N_0	Low	Medium	C/N_0 monitoring	Medium
Absolute power monitoring	Higher amplitude	Low	Medium	Absolute power monitoring	High
Power variation versus receiver movement	Higher power variations due to proximity	Low	Low	Antenna movement/ C/N_0 monitoring	Low
L1/L2 power comparison	No L2 signal for spoofer	Medium	Low	L2 reception capability	Low
Direction of arrival comparison	Spoofing signals coming from the same direction	High	High	Multiple receiver antennas	High
Pairwise correlation in synthetic array	Spoofing signals coming from the same direction	Low	High	Measuring correlation coefficient	High
TOA discrimination	Inevitable delay of spoofing signal	Medium	Medium	TOA analysis	Low
Signal quality monitoring	Deviated shape of authentic correlation peak	Medium	Medium	Multiple correlators	Low
Distribution analysis of the correlator output	Perturbed amplitude distribution due to spoofing-authenntic interaction	Low	Medium	Distribution analysis of correlator outputs	Medium
Consistency check with other solutions	Inconsistency of spoofing solution	High	High	Different navigation sensors	High
Cryptographic authentication	Not authenticated	High	High	Authentication	High
Code and phase rate consistency check	Mismatch between artifical code and phase rate	Low	Low	-	Low
GPS clock consistency check	Spoofing/authentic clock inconsistency	Low	Medium	-	Medium

TABLE 3.2: Summary of Spoofing Mitigation Methods from [14]

Anti-Spoofing method	**Spoofing Feature**	**Complexity**	**Effectiveness**	**Receiver required capability**	**Spoofing scenario generality**
Vestigial signal detection	The authentic signal is still present and can be detected	High	Medium	Multiple receive channels	Medium
Multi-antenna null steering	Spoofing signals coming from same direction	Medium	High	Multiple receive antennas	High
RAIM	Higher residuals for spoofed measurements	Medium	Medium	-	Medium

3.3 Literature Review Conclusion

Some of the early assessments of the spoofing threat included methods for performing said attacks using specialised hardware [13]. This increased the technical knowledge required to be able to perform an attack.

Chapter 4

Methodology

4.1 Testing Methodology

In this section the method of creating a GPS signal spoofing device is detailed. The main part of this project is the upgradability of the SDR platform and in particular the USRP N210 SDR. As previously mentioned the benefit of using an SDR over using an ASIC is that with a new version of software new capacilities are availeble to the device. This could be benefitial to either the spoofer or spoof defense.

The success of the spoofing was dictated by whether the receiver was able to lock onto the signal and calculate the same location as expected or travel the same path depending on whether the test is a satic or dynamic spoofing test.

Testing was also performed on the reception of GPS signals. Such that they could be used in Meaconing attacks. Initally there was an attempt to receive a GPS signal using the GPS-SDR software as proof that the antennae were operational. This was then changed such that the reception was handled directly through GNURadio and the raw digitised version of the signal was saved to a file such that it could be replayed elsewhere.

4.2 Data Collection

To see the effectiveness of the GPS spoofing methods experiments were carried out and results were recoreded. The success of the experiments were dictated by whether or not the receiver was reporting false location or timing information. Using an adroid phone there is access to the raw GPS information which can be used to determine if the spoofing signal is being accepted. However, the use of a "maps" program was also used as a way to determine if there was any form of software/hardware anti-spoofing technique being

used post gps receiver. A simple COTS will also be used to log the NMEA sentences

4.3 Testing Workflow

Some preliminary testing was done with different software setups to see which would be the best for reproducing spoofing results. A combination of meaconing and signal generating techniques were investigated. Initially meaconing was chosen as the best way to perfom an attack, therefore an attempt was made to record real time GPS signals and store them for later transmission. Initial testing using a passive log periodic antenna resulted in no data being properly captured. Since a log-periodic antenna was used there was a mismatch in the polarisation of the wave. The transmitted GPS signal is polarised as RHCP, whereas by its nature log-periodic antennas are linearly polarised. This equated to a $3dB$ attenuation of the signal. This coupled with the lack of signal gain from the passive antenna and the directional nature of the antenna meant that the data within the signal was unrecoverable and an active antenna should be used. Unfortunately, none of the daughtercards on hand were able to feed an active antenna. A bias-tee was used in order to feed the antenna with the $5V$ requried for its operation while filtering out the DC to feed into the SDR. To interface with the bias-tee a USB cable was cut and used to connect to a perf board with a soldered SMA connector. Unfortunately this was unsuccessful. The GNSS-SDR program was unable to find or lock onto any of the GPS satellites at any time. It was found that another opensource program, gps-sdr-sim, could be used to create binary files that replicate the received signals from the satellites.

4.4 Using SatGen3

To generate the binary bitstream for use with an SDR RF front end a GGA NMEA data stream was created using the satgen3 software package. This NMEA stream was used to make the binary file using the gps-sdr-sim command line interface program. SatGen3 replaces the need for capturing the raw GNSS signals or GGA sentence stream thus increasing the flexilbilty of scenarios that can be tested. Although there is no guarentee that the simulated stream of information is going to be correct. Thus a capture replay attack should still be considered as more reliable.

4.5 Faraday Cage

A faraday cage was used for testing purposes for two main reasons. It will isolate the target device from existing legitimate GNSS signals and stop any transmitted radiation from propagating into the local environment. Isolation from receiving legitimate signals is important since a reciver that is tracking a satellite already is harder to jam or spoof than one that is not. More important is ensuring that the radiation does not enter the environment since transmitting any signals on the frequency band for GNSS systems is illegal in Australia.

Since the received signal strength from a GNSS satellite is so low ($\approx -150dBm$) any signal that is tranmsitted from Earth's surface will be able overpower these signals for up to 85km, assuming an omnidirectional antenna, as shown in equation 4.1. This calucation was performed with the assumed maximum transmission power of the SDR of $15dBm$ coupled with a $30dB$ attenuator and transmitting on the L1 GPS band. In practise the effective range will be much less due to attenuation due to objects between transmitter and receiver, but this calculation shows that performing the experiments within a controlled environment was requried.

$$\begin{aligned} Att_{dB} &= 10\log_{10}\left(\frac{c}{4\pi df}\right)^2 \\ d = \frac{c}{4\pi 10^{\left(\frac{Att_{dB}}{20}\right)} f} &= \frac{3\times 10^8}{4\pi 10^{-6.75} 1.57542\times 10^9} \approx 85km \end{aligned} \tag{4.1}$$

4.6 Experimental Issues

While performing experiments there were issues thaat were run into that were required to be overcome. Initially a Log Periodic antenna was used for transmission since its frequency range was appropriate for use transmitting L1 band signals. After experiments failed to pick up any signals it was swapped for a omnidirectional antenna. This was able to produce signals that were picked up by the GNSSLogger application. Observing the graphs of the carrier to noise figure showed that when there was an underrun issue the $\frac{C}{N_0}$ would drop to 0 and the GPS receiver in the phone would lose connection to the 'satellites'. This meant that no GPS lock was achievable.

In an attempt to overcome the underrun issue that was plagueing the experiments, a new PC was brought in with Ubuntu installed directly instead

of via a VM. This resulted in the radio working straight away. The underrun issues resurfaced when trying to read the serial data from a COTS gps receiver. This was less than ideal and required a second computer to act as a datalogger.

4.7 Experiments

Experimentation was performed at the Tonsley campus of Flinders University, which has GPS coordinates of $-35.007650, 138.572030$. At first it was decided to use the centre of the Adelaide CBD as the coordinates for spoofing, that is $-34.5571732282, 138.3599516878$. Therefore it would be considered successful if the gps receiver was to show that the current locaiton was in the CBD.

4.7.1 Hardware Setup

For all experiments the same hardware was used. This included the USRP SDR, laptop and GPS receiver. The laptop was an important piece of eqiupment since it needed to be powerful enough to be able to feed the data to the SDR quick enough to avoid the aformentioned underrun issues.

- Laptop
  - Dell Inspiron 15
  - CPU: Core i7 Quad Core/ 8 thread
  - RAM: 32GB
  - Ethernet Connection: gigabit
- Software defined radio
  - USRP N210
  - SBX-40 daughtercard
  - 30dB attenuator
  - Full duplex
  - Gigbit Ethernet connection
  - high performace FPGA
  - omnidirection antenna

- GPS Receiver (Phone)
  - Google Pixel XL
  - Android 10
  - Multi constellation GNSS support (GPS+QZSS, GLONASS, Beidou)
- GPS Receiver (COTS)
  - GPS L1 support only
  - NMEA output

4.7.2 Static Spoofing

Within this thesis static spoofing is defined as producing a signal that produces a calculated location that does not change over time. While in practise there was some minor movement caused by the uncertainty in trilateration, this change in position is minor and within the range of error of GPS positioning. Using the SatGen3 software a location was chosen as the spoof location. After setting the desired time and date of spoofing the scenario was created. THis

4.7.3 Dynamic Spoofing

Dynamic spoofing refers to the production of a signal that when used to calcluate position, will be shown to change over time. The path traced by the receiver will be set at the time of production of the binary file, see figure 4.1, but there will be perceived motion.

4.7.4 Real-Time Spoofing

Due to time constraints a real-time algorithm was not produced as part of this project. However, utelising the open source projects that have been used to complete this thesis it would be probable to be able to create a real time spoofing device that would be able to react to the positional changes of the receiver instead of following a pre-determined path when generating the binary file. The signals generation algorithm could be ported to a GNURadio block in C++ to allow for easy access to real-time GPS signal spoofing. If an SDR is a full duplex radio, such is the case for the USRP N210, then one

port can be receiveing the real GNSS signal and the other can be transmitting the spoofed signal. Care would need to be taken in the set up of this arrangement since any transmitted signal would also be picked up by the reciving antenna. Therefore a directional transmitting antenna and physical disctance should be employed to allow for legitimate GNSS signals to reach the reciever port.

4.8 Parameters required for successful spoofing

add screen shots of steps required to generate binary file

Due to the internal workings of the USRP, there needs to be an integer ratio between the clock rate and sample rate. Therefore is was required that the sample frequency was set to 2.5Msps instead of the default 2.6Msps that the software would normally use.

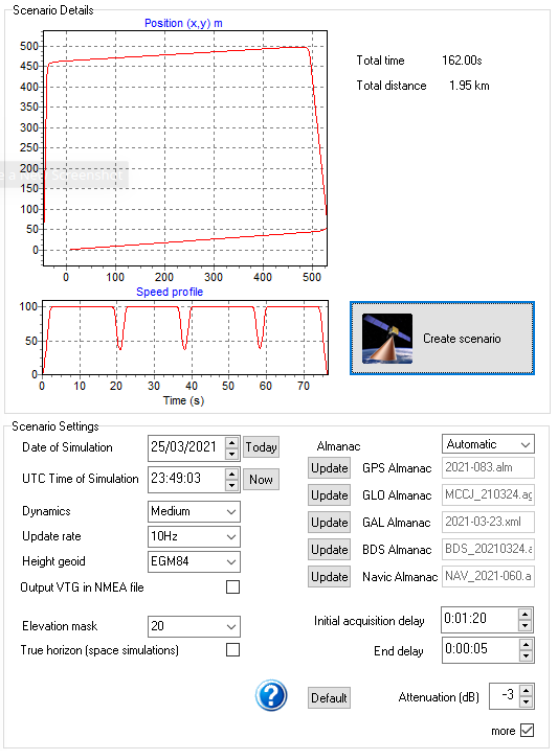

FIGURE 4.1: Settings of SatGen3 used to generate the dynamic path loop around Adelaide CBD. There is a graph that shows the offset from the origin and speed aver the journey

4.9 SDR Setup for GNSS Reception

Reception of GNSS signals is a compliated process which involves sychronising time values and solving simultaneous equtations for position, therefore

it was decided that the opensource program GNSS-SDR would be used to perform all of these functions. This sofware has been built over a number of years and is able to receive different GNSS signals and translate them into position.

The hardware setup for this was different. Since the signal strength of a GNSS transmission is so low when it reaches the earths surface ($\approx -160dBm$) an active antenna is typically requied for best performance, especially if there is no clear view of the sky or if there are many buildings that add multipath signals into consideration.

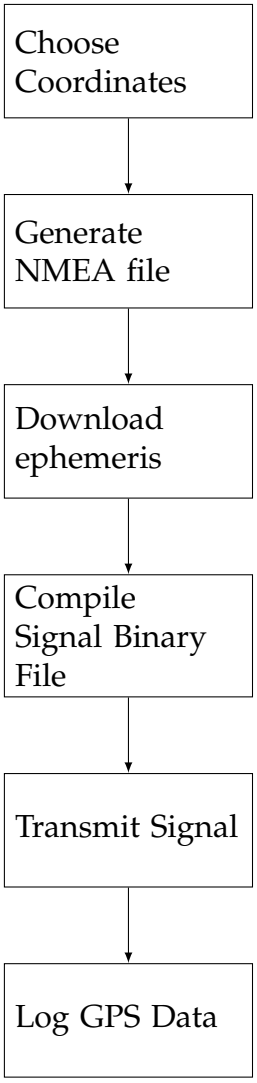

FIGURE 4.2: Flowchart of perfoming experimentation

Chapter 5

Results

5.1 GNSS Reception

Before testing the GPS transmission performance of the SDR, reception was tested, with less success. Three antenna setups were chosen each failing to lock and track the satellites. A log linear, an omnidirectional and an active patch antenna were all used. The active antenna should have given best results since it includes amplifiers and filters within the antenna module iteself. The failure could be to do with the bias-t used to inject the 5V DC into the antenna, however testing with a multi-meter showed that there was 5V on the RF+DC port of the Tee.

5.2 GPS Transmission

5.2.1 Meaconing Attack

Since the GPS reception failed with the SDR, there was no way of performing a meaconing attack. Therefore, the only viable attack strategy was to generate a binary file of the intended location.

5.2.2 Spoofing Attack

Once the workflow and hardware setup for the SDR was properly configured it was found that a smartphone was able to be spoofed. When attempting to spoof devices in the wild, the Pixel XL smartphone was succeptable to attack while more modern smartphones that were tested were not succeptable. These incuded the iPhone 12 Pro, Samsung Galaxy S10 and Google Pixel 3XL. The spoofing setup was not able to fool any of these devices. This could be down to software based anti-spoofing algorithms that have been

implemented including the useage of multiple constellations for position resolution.

5.2.3 Issues Encountered

The underrun issue was more or less solved by increasing the buffer size to 40× greater than the sampling size. There was an issue towards the end of the project where there was considerable leakage of EM radiation into the faraday cage that was causing the GPS receiver to produce wildly inaccuarate position (up to and over 500m error). This was much different to what had previously been recorded within the faraday cage. This amount of error does not consitute a successful spoof since the time to first lock was much greater than a real signal, or even spoofing attempts previously.

Just after the testing phase of the project the smartphone that was being used for some of the logging and graphing was rendered unusable. While there was no data lost, it was replaced with a newer model that experimentally was much harder to spoof than the previous model. This could be due to many factors including anti-spoofing algorithms. It would be a fair assessment that the newer device is able to receive more GNSS signals including augmented systems.

There were a number of unterminated cables that were running from outside of the cage to inside. This is seen as being the cause of the issues that were being faced. The suspect cables were removed or terminated and the results were more consistent with what was being achieved previously. Even with the new phone the GPS location was able to be spoofed.

Chapter 6

Discussion

6.1 Results

6.2 Future Work

All of the tests that have been conducted for use in this thesis have either been generating a signal based off a predetermined location (coordinate) or a predetermined path, or attempted meaconing attack. None of these options have a mechanism for position feedback. For example you cannot create a signal that has a linear offset from the actual position using these methods. This is something that could be achieved through combination and modification of the exitisting open source projects used in this thesis. This would allow for properly real-time gps spoofing, and could be extended further to have intelligent algorithms.

Current methods, as detailed in 4, requires downloading the Ephemeris for the date and time of the proposed spoofing attack. This makes real-time spoofing attacks not possible since there is a delay between the current time and the associated ephemeris. A potential fix for this could be to perform some analysis on the orbits of each satellite within the constellation over an arbitrary period of time to create a machine learning algorithm. This algorithm would be able to predict the location of the satellites ahead of time, thus binaries could be compiled for future attacks, or could be used for real-time attacks without the need for downloading/ retrieving the ephemeris from legitamate sources.

Extended to work on anti-spoofing for PhD.

Chapter 7

Conclusion

Appendix A

Project Code

This section will include all of the code that has been written for this project, including the code to fetch the ephemeris and the code to plot the position and signal quality

A.1 GPS Position and Signal Quality

Filename: NMEA.py
Description: This code will take a NMEA file as input and calculate the time to first fix, then plot the carrier to noise ratio of every satellite that was within view of the receiver, then plot the position given the output of the GPS receiver.

```
insert code here
```

Bibliography

[1] Geoffrey Blewitt. "Basics of the GPS technique: observation equations". In: *Geodetic applications of GPS* (1997), pp. 10–54. ISSN: 0280-5731.

[2] Norman Bonnor. "A Brief History of Global Navigation Satellite Systems". In: *Journal of navigation* 65.1 (2012), pp. 1–14. ISSN: 0373-4633. DOI: 10.1017/S0373463311000506.

[3] Government Of Japan Cabinet Office. *Overview of the Quasi-Zenith Satellite System (QZSS)*. 2021. URL: https://qzss.go.jp/en/overview/services/sv01_what.html.

[4] Government Of Japan Cabinet Office. *What is the Quasi-Zenith Satellite System (QZSS)?* 2021. URL: https://qzss.go.jp/en/overview/services/sv02_why.html.

[5] N. Carson et al. "GPS spoofing detection and mitigation using Cooperative Adaptive Cruise Control system". In: *2016 IEEE Intelligent Vehicles Symposium (IV)*. 2016, pp. 1091–1096. DOI: 10.1109/IVS.2016.7535525.

[6] Robert J Danchik. "An overview of transit development". In: *Johns Hopkins APL technical digest* 19.1 (1998), p. 19.

[7] Gonzalo De La Torre, Paul Rad, and Kim-Kwang Raymond Choo. "Driverless vehicle security: Challenges and future research opportunities". In: *Future Generation Computer Systems* 108 (2020), pp. 1092–1111. ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2017.12.041. URL: http://www.sciencedirect.com/science/article/pii/S0167739X17315066.

[8] G Arul Elango and GF Sudha. "Design of complete software GPS signal simulator with low complexity and precise multipath channel model". In: *Journal of electrical systems and information technology* 3.2 (2016), pp. 161–180. ISSN: 2314-7172.

[9] Carles Fernandez-Prades et al. "GNSS-SDR: An open source tool for researchers and developers". In: *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, pp. 780–794.

[10] Mahsa Foruhandeh et al. "Spotr: GPS Spoofing Detection via Device Fingerprinting". In: *arXiv preprint arXiv:2005.08787* (2020).

[11] G. X. Gao et al. "Understanding the GIOVE-B broadcast codes of the Galileo system". In: *2008 42nd Asilomar Conference on Signals, Systems and Computers*, pp. 2086–2090. ISBN: 1058-6393. DOI: 10.1109/ACSSC.2008.5074800.

[12] Yaqi Hu. "GNSS SDR Signal Generator Implementation Based on USRP N210". In: *Journal of Physics: Conference Series* 1314 (2019), p. 012016. ISSN: 1742-6588 1742-6596. DOI: 10.1088/1742-6596/1314/1/012016. URL: http://dx.doi.org/10.1088/1742-6596/1314/1/012016.

[13] Todd E Humphreys et al. "Assessing the spoofing threat: Development of a portable GPS civilian spoofer". In: *Radionavigation laboratory conference proceedings*. 2008.

[14] Ali Jafarnia-Jahromi et al. "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques". In: *International Journal of Navigation and Observation* 2012 (2012), p. 127072. ISSN: 1687-5990. DOI: 10.1155/2012/127072. URL: https://doi.org/10.1155/2012/127072.

[15] Malek Karaim et al. "GNSS error sources". In: *Multifunctional Operation and Application of GPS* (2018), pp. 69–85.

[16] Andrew J. Kerns et al. "Unmanned Aircraft Capture and Control Via GPS Spoofing". In: *Journal of Field Robotics* 31.4 (2014), pp. 617–636. ISSN: 1556-4959. DOI: https://doi.org/10.1002/rob.21513. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/rob.21513.

[17] M. L. Psiaki and T. E. Humphreys. "GNSS Spoofing and Detection". In: *Proceedings of the IEEE* 104.6 (2016), pp. 1258–1270. ISSN: 1558-2256. DOI: 10.1109/JPROC.2016.2526658.

[18] J.A Ávila Rodríguez. *GPS Signal Plan*. 2011. URL: https://gssc.esa.int/navipedia/index.php/GPS_Signal_Plan.

[19] Desmond Schmidt et al. "A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures". In: *ACM Comput. Surv.* 48.4 (2016), Article 64. ISSN: 0360-0300. DOI: 10.1145/2897166. URL: https://doi.org/10.1145/2897166.

[20] Navigation National Coordination Office for Space-Based Positioning and Timing. *Selective Availability*. 2018. URL: https://www.gps.gov/systems/gps/modernization/sa/.

[21] Nils Ole Tippenhauer et al. "On the Requirements for Successful GPS Spoofing Attacks". In: *Ccs '11* (2011), 75–86. ISSN: 9781450309486. DOI: 10.1145/2046707.2046719. URL: https://doi.org/10.1145/2046707.2046719.

[22] P. Waller et al. "The In-Orbit performances of GIOVE clocks". In: *IEEE Trans Ultrason Ferroelectr Freq Control* 57.3 (2010), pp. 738–745. ISSN: 0885-3010. DOI: 10.1109/TUFFC.2010.1472.

[23] Kang Wang, Shuhua Chen, and Aimin Pan. "Time and position spoofing with open source projects". In: *black hat Europe* 148 (2015).

[24] Z. Wu et al. "Spoofing and Anti-Spoofing Technologies of Global Navigation Satellite System: A Survey". In: *IEEE Access* 8 (2020), pp. 165444–165496. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.3022294.

[25] Safoora Zaminpardaz, P. J. G. Teunissen, and Nandakumaran Nadarajah. "IRNSS/NavIC l5 attitude determination". In: *Sensors (Basel)* 17.2 (2017), p. 274. ISSN: 1424-8220. DOI: 10.3390/s17020274.

[26] Kexiong Curtis Zeng et al. "A practical GPS location spoofing attack in road navigation scenario". In: *Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications*. 2017, pp. 85–90.

[27] Kexiong Curtis Zeng et al. "All your GPS are belong to us: Towards stealthy manipulation of road navigation systems". In: *27th USENIX Security Symposium (USENIX Security 18)*, pp. 1527–1544. ISBN: 1939133041.

[28] Xian-Chun Zheng and Hung-Min Sun. "Hijacking Unmanned Aerial Vehicle by Exploiting Civil GPS Vulnerabilities Using Software-defined Radio". In: *Sensors and Materials* 32.8 (2020), pp. 2729–2743.