GNSS Vulnerabilities & Robustness

Bento Miguel Ribeiro Martins | 200701906

Mestrado em Engenharia Geográfica

Departamento de Geociências, Ambiente e Ordenamento do Território

2014

Orientador

Dr. Luísa Bastos (Faculdade de Ciências da Universidade do Porto)

Coorientador

Dr. Chaz Dixon (Satellite Applications Catapult)

U.PORTO

FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

Todas as correções determinadas pelo júri, e só essas, foram efetuadas.

O Presidente do Júri,

Porto, _____/_____/_____

AGRADECIMENTOS | ACKNOWLEDGEMENTS

Satellite Application Catapult, was, undoubtedly, the best place to finish my Master Degree. An internship abroad is always a life-changing experience but it is the people you meet that make your journey remarkable. In the United Kingdom I found friendship and knowledge in its simplest and brightest form making me so grateful for what I achieved in those 6 months.

Muito obrigado Professora Luísa Bastos pela oportunidade que me deu de viver esta aventura.

During the internship interview to Satellite Application Catapult I was asked: *'What do you expect to be doing in five years? Investigation? Be a manager?'*

I still don't know a proper answer to that question, but I really hope that in five years I can be an example of knowledge, dedication, availability, optimism, support and joy as Dr. Chaz Dixon was for me.

I also would like to express my thankfulness to every single member of the PNT team for really making me feel as part of a team, trying to teach me as much as they could so I could be a Nav Man, just like them.

All the knowledge acquired goes far beyond what is written in this report, but if there is a person that I really owe something is Pedro Alfaro Sanz. A true example of cooperation and friendship that continued even after working hours, supporting and guiding me when I felt lost, giving me new future perspectives, believing in me and making me believe in myself, and well, for really everything.

To everyone else who crossed and accompanied my journey, thank you.

A todos os outros que se cruzaram e me acompanharam nesta jornada, obrigado.

RESUMO

Este relatório descreve algum do trabalho realizado ao longo do estágio curricular do Mestrado em Engenharia Geográfica, na empresa Satellite Applications Catapult, no Reino Unido, ao abrigo do programa Erasmus Estágio, pelo aluno Bento Miguel Ribeiro Martins. O estágio teve uma duração de 6 meses, tendo-se iniciado a 10 de Fevereiro de 2014 e terminado a 8 de Agosto de 2014, orientado pela Professora Dr. Luísa Bastos (Faculdade de Ciências da Universidade do Porto) e coordenado pelo Dr. Chaz Dixon (Satellite Applications Catapult).

O trabalho desenvolvido ao longo do estágio focou-se na radio-interferência e nos seus impactos nos sistemas globais de navegação e localização por satélite, designada por *jamming*. O apoio a outros projetos foi uma constante ao longo de todo o semestre e desse modo serão também adicionadas componentes de interesse que complementem este tópico.

Uma breve introdução aos sistemas de navegação (GPS, GLONASS, Galileo e BeiDou) irá permitir ter uma visão atual da componente espacial dos SGLNS, e em que aplicações estes são utilizados. As vulnerabilidades irão ser apresentadas, tanto quanto à sua regularidade como às suas consequências, salientando especialmente o papel nefasto que a interferência deliberada pode ter num recetor SGLNS, confirmando esta realidade através de testes realizados em laboratório. Por último, serão referenciadas tecnologias que poderão ultrapassar algumas destas vulnerabilidades, tornando os SGLNS mais robustos, seguros e viáveis.

Palavras-chave: SGLNS, GPS, GLONASS, Galileo, BeiDou, jamming, jammer, PPD, spoofing.

ABSTRACT

This report describes some of the work done during the curricular internship of the Geographic Engineer Master Degree, in the company Satellite Applications Catapult, in the United Kingdom, under the Erasmus Internship program, done by the student Bento Miguel Ribeiro Martins. This placement lasted 6 months, starting on the 10th of February of 2014 and finishing on the 8th of August of 2014, oriented by the teacher Dr. Luísa Bastos (Faculty of Sciences of the University of Porto) and coordinated by Dr. Chaz Dixon (Satellite Applications Catapult).

The work developed during the internship focused on radio-interference that disturbs the global navigation satellite systems, named jamming. The support on other projects was a constant during all the semester, so will be added some interesting components that will complement this topic.

A brief introduction to navigation systems (GPS, GLONASS, Galileo and BeiDou) will permit to have an actual vision of the spatial segment of the GNSS and in which applications they are used. The vulnerabilities will be presented, regarding their regularity and consequences, emphasizing the disastrous role that deliberate interference has in a GNSS receiver, confirming this reality through trials made in laboratory. At last, will be referenced technologies that can overtake some of these vulnerabilities, making the GNSS more robust, safe and viable.

Keywords: GNSS, GPS, GLONASS, Galileo, BeiDou, jamming, jammer, PPD, spoofing.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF GRAPHICS

ACRONYMS

AIS – Automatic Identification System
A-GNSS – Assisted Global Navigation Satellite Systems;
CDMA – Code Division Multiple Access;
CW – Continuous Wave;
DOP – Dilution of Precision;
EGNOS – European Geostationary Navigation Overlay Service;
ESA – European Space Agency;
FDMA – Frequency Division Multiple Access;
FOC – Full Operational Capabilities;
FSPL – Free-Space Path Loss;
GAGAN – GPS Aided Geo Augmented Navigation (Indian SBAS);
Galileo CS – Galileo Commercial Service;
Galileo OS – Galileo Open Service;
GEO – Geostationary Orbit;
GIOVE – Galileo In-Orbit Validation Element;
GLONASS – GLObal'naya NAvigatsionnaya Sputnikovaya Sistema (Russian GNSS);
GNSS – Global Navigation Satellite System(s);
GPS – Global Positioning System (United States of America GNSS);
HDOP – Horizontal Dilution of Precision;
HMI – Hazardous Misleading Information;
IGSO - Inclined geosynchronous orbit;
IMU – Inertial Measurement Unit;
LNA – Low-Noise Amplifier;
LORAN – Long Range Navigation;
MEO – Medium Earth Orbit;
PNT – Positioning, Navigation and Timing;
PPD – Personal Privacy Device;
PQN – Performance Quantification Network;

PRS – Public Regulated Service;
GIS – Geographic Information System(s);
QZSS – Quasi-Zenith Satellite System (Japanese SBAS);
RFID – Radio-Frequency Identification;
SAC – Satellite Applications Catapult;
SBAS – Satellite-Based Augmentation Systems;
SDCM – System for Differential Corrections and Monitoring (Russian SBAS);
SGLNS – Sistemas Globais de Localização e Navegação por Satélite (GNSS in English);
SME – Small And Medium Enterprises;
TEM – Transverse Electromagnetic;
UAV – Unmanned Aerial Vehicle;
VGA – Variable Gain Amplifier;
WAAS – Wide Area Augmentation System

CHAPTER I

INTRODUCTION

1. INTRODUCTION

Global Navigation Satellite Systems (GNSS) are one of the biggest inventions of the XX century, matching a broad number of technologies to give three modest pieces of information: position, velocity and timing (PVT). It may look simple but all the research behind, all the billions of money to put the system running is far behind people's common knowledge. Even the term people use is incorrect, and everything is called GPS (Global Positioning System, USA GNSS), when it's just a small part of this GNSS world.

GPS deserves all the credit for being the first fully functional system, though GLONASS (Russian GNSS) is now at his full strength, Galileo is coming with new services and better accuracies and BeiDou is getting stronger. But what does this development represent to the user? Better positioning, that's certain, and probably they will still call it GPS to everything related, even when the position derives from more than three constellations all combined, in a gigantic bird cage. As people can't see the satellites and their failures, the system seems smooth, always working, and always there for everyone, and if something were to happen they won't probably relate it to the system, but to the receiver or smartphone they are using. The disinformation of the people is tolerated, though the blindness when using it can be quite serious, depending on the application.

GNSS applications serve a vast number of areas, from transport to sports, from finance to scientific purposes. The system has a full range of vulnerabilities that can affect its performance, though most of them have only occurred one or two times since the system started operating. However, a new threat, deliberate interference, is getting in the way and users are not prepared for it. For example, a powerful jammer placed on central London can cause the chaos and have serious impact on the city's basic services, like transport systems, emergency services, late deliveries and traffic congestions.

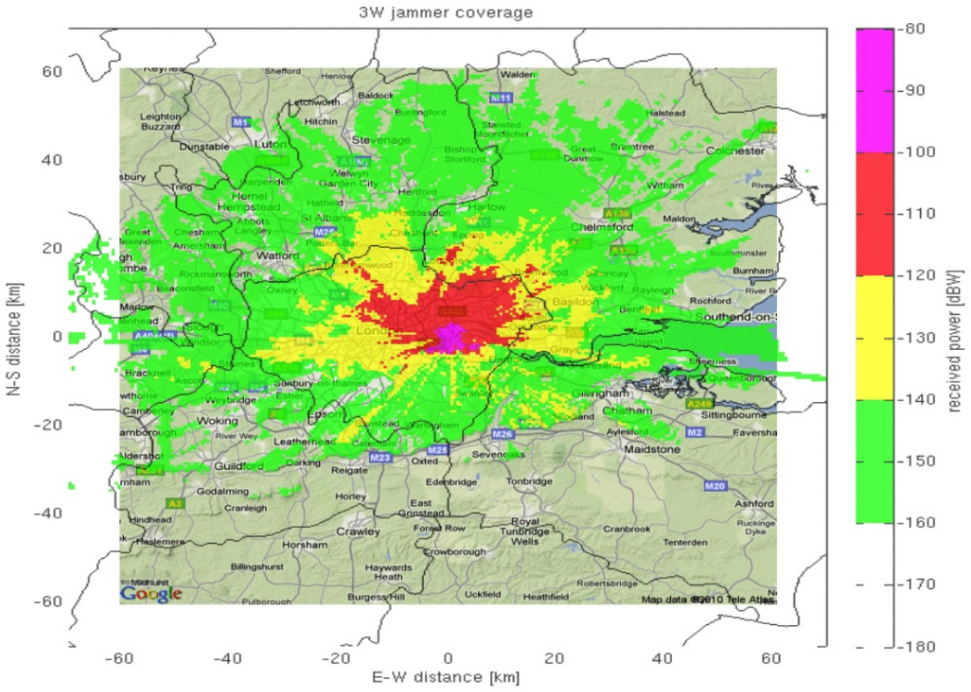


Figure 1 - Simulation of a 3 W jammer impact on London area (Source: University of Bath).

Even though a scenario like this has never happened, we shouldn't exclude its possibility. Is then necessary to understand the applications where GNSS sits, the vulnerabilities of the system and the way forward in case of failure. It is also necessary to study how jamming works and how it can impact a receiver and this report will state some conclusions on how it does.

1.1. OBJECTIVES

This report provides a summary of what was achieved during the internship on Satellite Applications Catapult (SAC), focused on GNSS capabilities, vulnerabilities and robustness.

The knowledge was acquired by practical experience, managing a PNT (Positioning, Navigation and Timing) laboratory, learning how to handle receivers, from low-end to survey grade ones, a state-of-the-art GNSS simulator, RF record & playback devices and the respective RF cross-connections. Moreover, it was a great opportunity to communicate with experienced people on this field, exchanging points-of-view, performing brain storming and attending business meetings, improving the

theoretical information around GNSS. Some of the themes discussed sparked an interest to know even more and research some particular topics. Work was performed in an environment of relative independence, improving responsibility and autonomy, providing a 'learn by doing' opportunity. Working on a multi-team company also enhanced the interest in other areas (telecommunications, space technology, earth observation) and provided areas of overlap and cross-support, as in the provision of GNSS in-lab capabilities to test other equipment that also use that technology.

This report is then a gathering of some interesting topics around the GNSS world, learnt by direct experience, shared information and research. It's certainly a hard task to do an internship report when so many tasks were performed, for different projects and various objectives. Though, it focuses one of the biggest problems: deliberate interference to GNSS signals, which it is a relative unknown issue for the common user, especially in Portugal (PT).

It was a *sui generis* internship, not developing a full-time project, but aiding anything when needed, which gave a wide point-of-view to other areas, which wouldn't be possible if it was only focused in one topic. Since this report is part of a Master Degree on Geographic Engineer, all the research analyses will be focused in terms of geographic positioning output from receivers, rather than the electronic behaviour of the equipment.

1.2. STRUCTURE

This report is divided in 7 chapters, finishing with a conclusion, contribution of the internship to the company and future work.

In chapter I a brief introduction to GNSS, its mass use and the objectives and structure of this report are shown.

In chapter II there is a presentation about the GNSS used during the internship (GPS, GLONASS, Galileo and BeiDou), their history, signals and especially orbits, using some imagery created using specific software.

In chapter III there is a list of some of the GNSS applications used nowadays.

In chapter IV GNSS vulnerabilities are presented, classified by type of origin.

In chapter V the work developed in the internship will be presented, like some Galileo relevant work and experiments regarding the impact of jamming and

spoofing, explaining the methodology adopted to create these trials and the respective results are documented.

In the chapter VI there is a list of proposed solutions that can be adopted to overtake GNSS vulnerabilities or enhance the services provided.

In the conclusion it is stated the results and outcomes of this internship, showing the most relevant knowledge obtained from it, followed by a small report about the contribution of the work to SAC and the bibliography.

In the annexes section the company where the internship was held will be presented (annexe 1) showing also some of the tasks performed (annexe 2), followed by an explanation of all the Galileo related work made (annexe 3) and respective results (annexe 4 and 5). Finally a project planning is attached to show how the work was intended to be executed. (annexe 6).

CHAPTER II

GLOBAL NAVIGATION SATELLITE SYSTEMS

2. GLOBAL NAVIGATION SATELLITE SYSTEMS

2.1. GPS

2.1.1. HISTORY

Global Positioning System is undoubtedly the most successful GNSS; its history is connected to the first satellite, Sputnik. When the Soviet Union launched Sputnik, a group of American physicists started to analyse the radio transmissions of the satellite. After a few hours, they managed to estimate the satellite position analysing the Doppler shift of the transmitted signal. This principle was the first step that led to the first navigation satellite system: Transit.

Successfully tested in 1960, Transit could give a position fix every hour, a great achievement, indeed, though it was not enough for United States Department of Defence. A new solution was required, with more coverage and with more accuracy, but the cost was too high to justify the demands. A few years later the perfect motivation was found: the Cold War arms race. Nuclear threats level was bigger than ever and for that reason USA (United States of America) wanted to be prepared, and be in front, of whatever may came. Consequently, United States military forces should have a system that could provide precise positions in order to use missiles more effectively.

In 1973, at the Pentagon, several military officers discussed the need for a Defence Navigation Satellite System and few months later the Department of Defence named the project as Navstar, Navigation System Using Time and Ranging, later Navstar-GPS, shortened to only GPS, Global Positioning System. In the following years the system was developed, tested and during the period 1978-1985 ten system validation satellites were launched.

In 1983 a plane crash where 269 people died, thus President Ronald Reagan issued a directive to make GPS freely available to all once it was in a mature state of development to avoid future accidents and improve aerial transport security. In December 1993, Initial Operation Capability was declared, with 24 operational satellites in orbit and achieving Full Operation Capability (FOC) in June 1995. 24 satellites compose the GPS constellation, though 32 satellites are currently in orbit and active.

Initially built for military purposes, GPS soon started to be a must-have in a lot of applications, although the highest quality signal was still reserved only to the military applications. Quality for civilian uses was intentionally degraded, in a process called Selective Availability. Depending on the purpose it would still be better than most other navigation systems available at the time, but for more demanding applications it was useless. However, in the 1st of May of 2000, there was a decision to shut down the SA and it was the start of the massive expansion of the GPS, reaching new areas of science, improving transports and even changing the way people do sports, etc. (Sullivan, 2014)

2.1.2. SIGNALS

GPS L1 band, at 1575.42 MHz, is the most important band for navigation purposes, and all GPS receivers use at least this band for PVT. In this band is modulated the Coarse/Acquisition (C/A) code, GPS's most famous open service. In this frequency also exists the P Code, a precision military code which is being replaced by the M Code, a new modernized military signal. The access to this military signals is restricted to users authorized by the US Department of Defence. Future satellites (currently planned to start in 2016) will also emit L1C, a new open code, more modernized than C/A, and interoperable with other international GNSS. GPS L1 uses CDMA (Code Division Multiple Access) protocol where every satellite emits a different code at the same frequency and it's that code that identifies the satellite.

GPS L2 is transmitted at 1227.60 MHz, initially built for military applications only, modulating the P code and the M code. Newer satellites (the first L2C capable satellite was launched in 2005, and currently 14 on orbit satellites are L2C capable) also emit a L2C code, a new open service to enhance the accuracy of GPS receivers. Combining L1 and L2 open signals will boost accuracy, by enabling the removal of ionospheric errors. L2C signal is also broadcasted at higher powers than L1 C/A, making it easier to track under trees or in some cases even indoor.

To finish, a new frequency L5 at 1176.45 MHz is made available as the new generation satellites are put in orbit (the first L5 capable satellite was launched in 2010, and currently 7 on orbit satellites are L5 capable). This way, GPS will provide open signals in three different frequencies, delivering a high robust service. L5 frequency band was implemented mainly for aviation safety services, but it is

foreseen that many applications will make use and benefit from the new signal. (Gps.gov, 2014)(Kaplan, 2006)

2.1.3. ORBITS

AGI Systems Tool Kit (http://www.agi.com/products/stk/) provides visualization capabilities to satellite orbits in a 3D, and 2D, environment. Adding the desired constellations or satellites it is possible to test the coverage of a broadcasted signal, the ground track, etc. In the following figure it is possible to see the orbit of a GPS satellite, with a repetition cycle of 24 hours, 1 day. The white track represents when the satellite is visible from the SAC premises. The GPS satellite orbit is just under 12 hours long; two complete orbits bring the satellite back to the same point (repeating ground track).

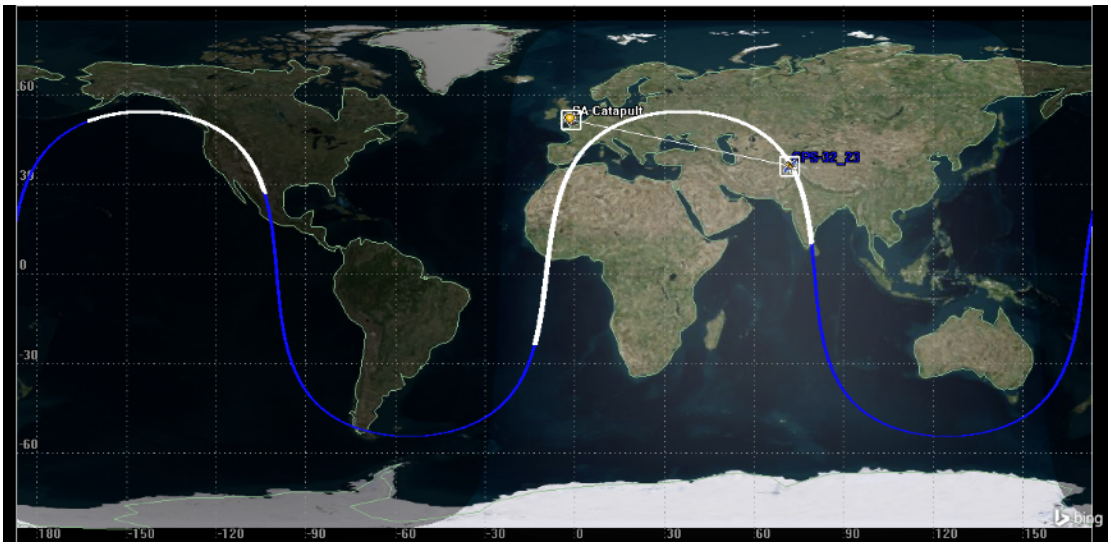


Figure 2 - GPS satellite groundtrack

In the next figure it is possible to see the six orbital planes where the 32 GPS satellites are placed. The white lines represent the visibility from the SAC premises. They have a semi-major axis of around 26560 Km and an inclination of 55º, considered a Medium-Earh Orbit (MEO). (Springer, 2014)

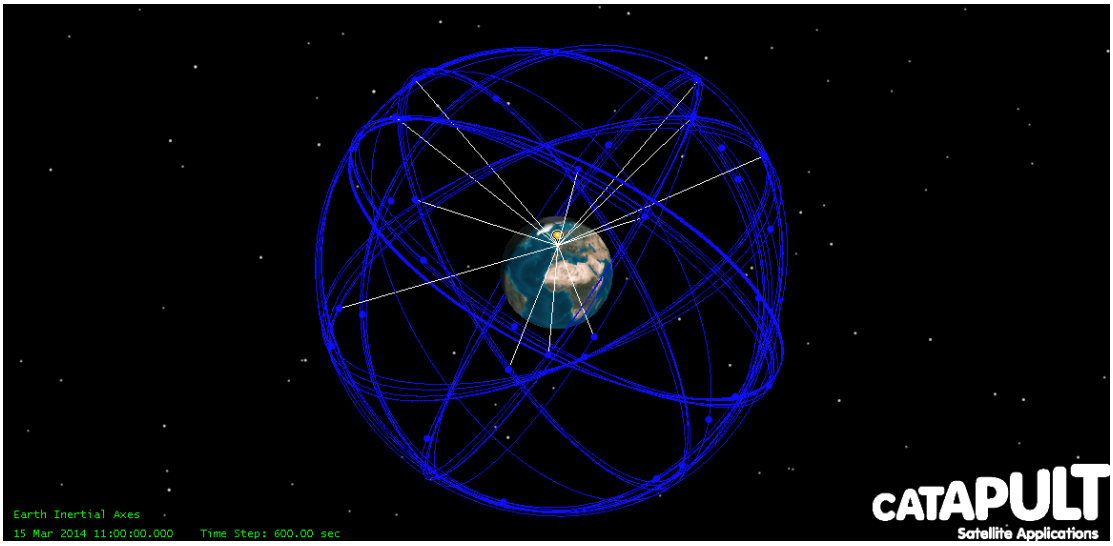


Figure 3 - GPS constellation

The next figure shows a satellite in orbit facing earth. The satellite displayed is a 3D model of an actual GPS satellite.

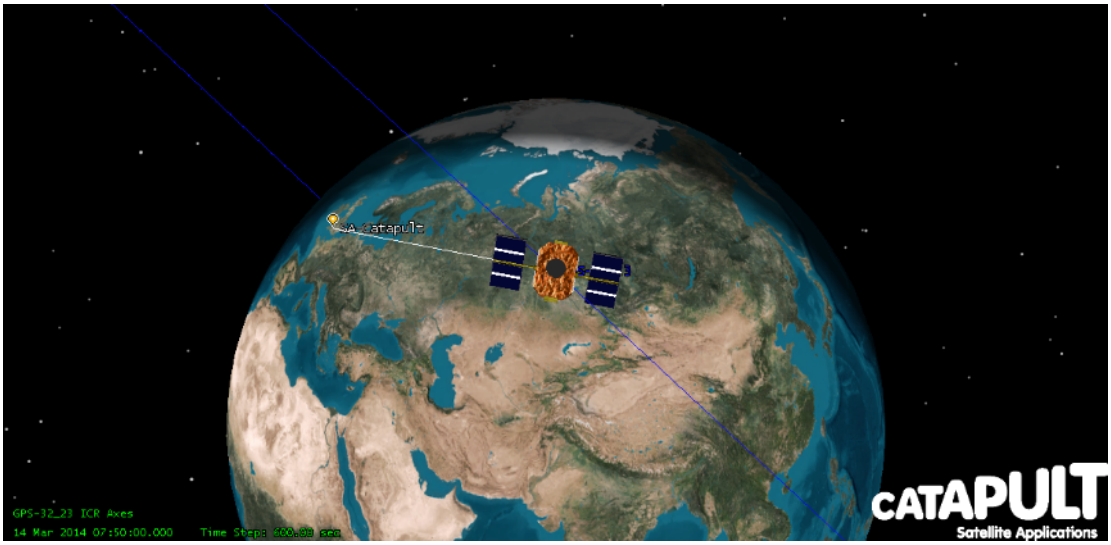


Figure 4 - GPS satellite view

2.2. GLONASS

2.2.1. HISTORY

During the Cold War, USSR was on top of space exploration and with the launch of Sputnik they proved their value, though it was not enough and they needed to overtake USA's new technologies. It's in this context that GLObal'naya NAvigatsionnaya Sputnikovaya Sistema, GLONASS, is proposed: a GNSS built, developed and managed by Russia (former USSR).

GLONASS beginnings are somehow similar to GPS, built for military purposes, based on former experimental GNSS that didn't meet the requirements to ballistic systems. The system was conceived in the late 1960s, but only in 1976 the government decided to develop it. The first launch happened in 1982 and until the dissolution of the Soviet Union in 1991, they've sent to space more than 40 GLONASS related satellites. Despite the dissolution, the program continued and reached full operational capability in 1995, with 24 satellites in orbit. By that time, the lifespan of the satellites was 3 years, so there was a constant need to replace them. Unfortunately, Russia suffered from a serious economic crisis in the following years, and the program was slightly abandoned due to lack of funding to support the need of launching ~8 satellites per year, making GPS more visible and trustworthy. Fortunately, a turnover happened in 2000, President Vladimir Putin recognized the importance and criticality of the GLONASS program and gave it a top priority. In 2001, this GNSS reached its lowest point with only 6 satellites in orbit and actions were taken: the funding was doubled and launches of new satellites restarted a few years later, with new, better and higher longevity technologies (almost the twice of the originals lifetime). GLONASS nominal constellation consists in 24 satellites but currently 28 satellites are in orbit and active.

Like GPS, military applications were top priority though President Putin demanded that the system should be available to everyone. In the 18th of May of 2007, all restrictions were removed and the military signal has been freely available to everyone since then.

Due to its ups and downs, GLONASS' reputation was clearly less than GPS and the number of users was lower than expected. To avoid this, and because Russia Federation has a huge economic market, Russia threatened to raise import duties to every GPS-enabled equipment, unless it was also GLONASS enabled.

Consequently top brands started adding GLONASS support and nowadays smartphones and other navigation tools also support the Russian system. (Glonass-iac.ru, 2014)

2.2.2. SIGNALS

GLONASS main signal is broadcasted through a process called FDMA (Frequency Division Multiple Access). It's also called L1, though it doesn't match with the GPS L1, and ranges from 1592.9525 MHz to 1610.485 MHz, centered at 1602.00 MHz. In a FDMA type of transmission every satellite emits the same code in its own frequency, and it's the frequency that identifies the satellite. On GLONASS L1, C/A code and a P code are modulated.

In the L2 band, the same codes are transmitted, but from 1242.9375 MHz to 1248.625 MHz, centered at 1246.00 MHz. A new band, L3, is planned to be introduced but is not fully guaranteed. The new generation of GLONASS will emit L1 and L2 using the FDMA protocol, but also L1, L2, and maybe L3, in CDMA. (staff, G. and staff, G., 2014)(Ashjaee, J., 2011)(Navipedia.net, 2014)

2.2.3. ORBITS

GLONASS satellites have an orbit period of 11 hours and 15 minutes, having a ground-track repetition cycle of 8 days, presenting a ground path similar to the shown in the following figure.

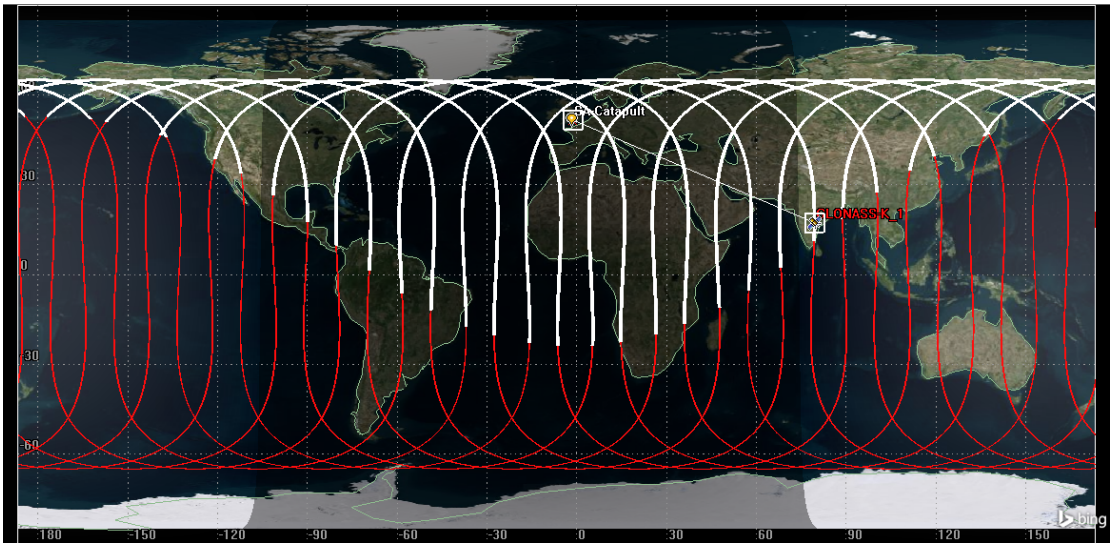


Figure 5 - GLONASS satellite groundtrack

The 28 satellites of the constellation are spread in three different orbit planes, enabling that in every moment more than 6 are visible in every point of the earth. By design GLONASS gives better coverage than GPS to high latitudes, to better serve the higher latitude where Russian territory is, since the orbits have 65º of inclination, having a semi-major axis of 25440 Km on a MEO orbit. (Springer, 2014)

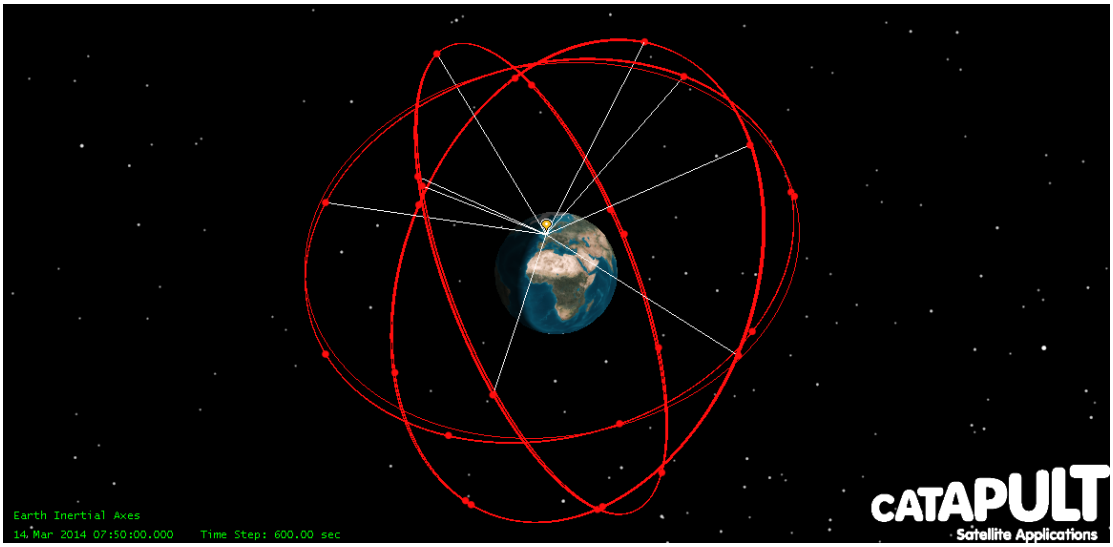


Figure 6 - GLONASS constellation

In the next figure is possible to see a GLONASS satellite model facing Earth on its orbit.

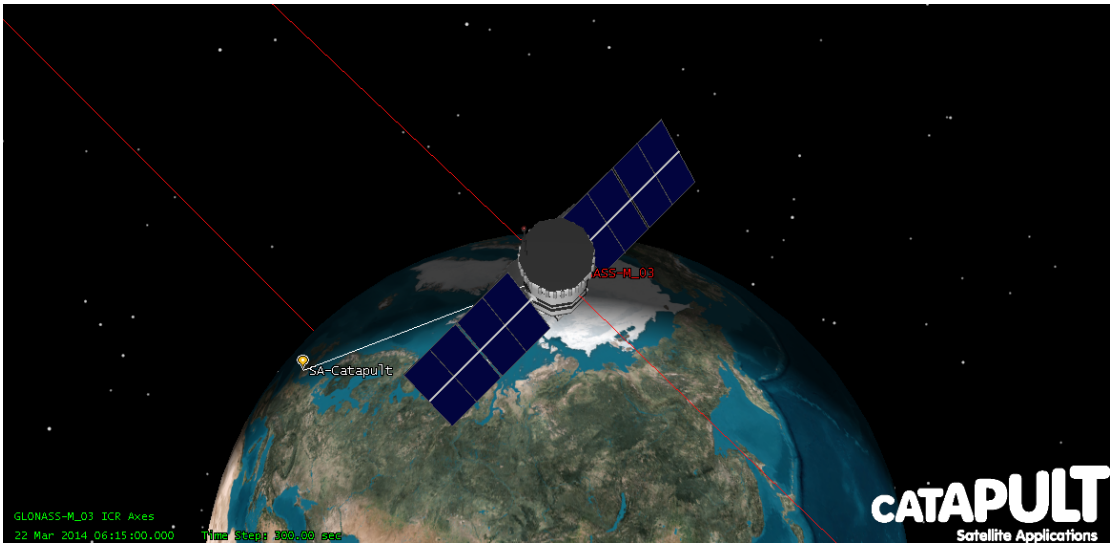


Figure 7 - GLONASS satellite view

2.3. GALILEO

2.3.1. HISTORY

Galileo system is quite new compared to GPS and GLONASS, but its ups and downs are a huge concern in its hope to be a state-of-the art GNSS and its validation as a useful European tool is being delayed by political and technical challenges year after year.

Galileo's first steps happened in 1999, when a group of engineers from four different countries (United Kingdom, Germany, France and Italy) gathered, discussed and came up with an idea for a European GNSS. Four years later, Galileo programme was officially agreed by the European Union and the European Space Agency.

Unlike GLONASS or GPS, Galileo is meant exclusively for civilian applications. This feature is quite remarkable since it's not dependent on military interests which could be concerned on turning off or degrading the signal in case of external conflicts. Therefore, positioning, navigation and timing using Galileo is going to be permanently available and reliable to anyone. It was also planned that satellites

would be equipped with the latest rubidium atomic clocks and passive hydrogen masers, assuring great timing precisions and consequently meter and sub-meter positioning accuracies using a standalone receiver, better than its GNSS rivals. USA and European Union also signed an agreement assuring the compatibility between their respective systems, improving PVT quality for the end-user.

In December 2005, GIOVE-A (Galileo In-Orbit Validation Element), the first test satellite was launched, followed by a second one, GIOVE-B, three years later. Signal testing and tracking was performed successfully, so Galileo entered in an In-Orbit Validation stage with the launch of two satellites in October 2011 and other two, one year later. With four satellites on space it was possible to get a Galileo-only position fix, which was achieved on the 12 of March of 2013. Although this launches have happened, most of them suffered from several postpones. Initially planned to have 27 satellites (plus 3 spare ones) launched between 2011 and 2014, Galileo suffered from serious concerns due to lack of funding and bad critics around this billionaire project. Then, when everything seemed to be in the right path another great step back happened. On August 2014 two satellites that were going to start the Full Operational Capability development stage were launched, but unfortunately they were placed in the wrong orbit, making them somewhat useless. (Navipedia.net, 2014)(Selding, 2014)

The importance of a European GNSS is questionable, some critics argue that is not worthy to invest so much when there is a fully functional GPS and even GLONASS, but for EU is a way to assure its independence, economic and scientific power and, undoubtedly, the end-user, European or not, will benefit a lot of this state-of-the art GNSS. (Navipedia.net, 2014)

2.3.2. SIGNALS

Galileo uses CDMA and will transmit signals in 3 bands:

Its main band is called E1, although it's collocated with GPS L1, 1575.42 MHz. This frequency transmits Galileo's Open Service (OS) code, Galileo's Commercial Service (CS) and Galileo's Public Regulated Service (PRS) code.

Galileo also transmits in the E5 band (1191.795 MHz), which can be further decomposed, for tracking and processing, in the E5A (1176.45 MHz) and E5B bands (1278.75 MHz) This band will be used for both the OS and Galileo's Search And

Rescue (SAR) service, that will enable the transmission of emergency messages to beacons in distress, supporting the International Cospas-Sarsat Programme.

Finally, in the E6 band, 1278.75 MHz, Galileo broadcasts CS and PRS signals.

Agreements between the European Union and the United States of America were made in order to make the signals from Galileo and GPS compatible, enabling higher precisions, and preventing the cross-jamming between GNSS constellations. (Navipedia.net, 2014)

2.3.3. ORBITS

Galileo satellites have an orbit period of 14 hours and 7 minutes, having a ground-track repetition cycle of 10 days, presenting a ground path similar to the shown in the following figure.

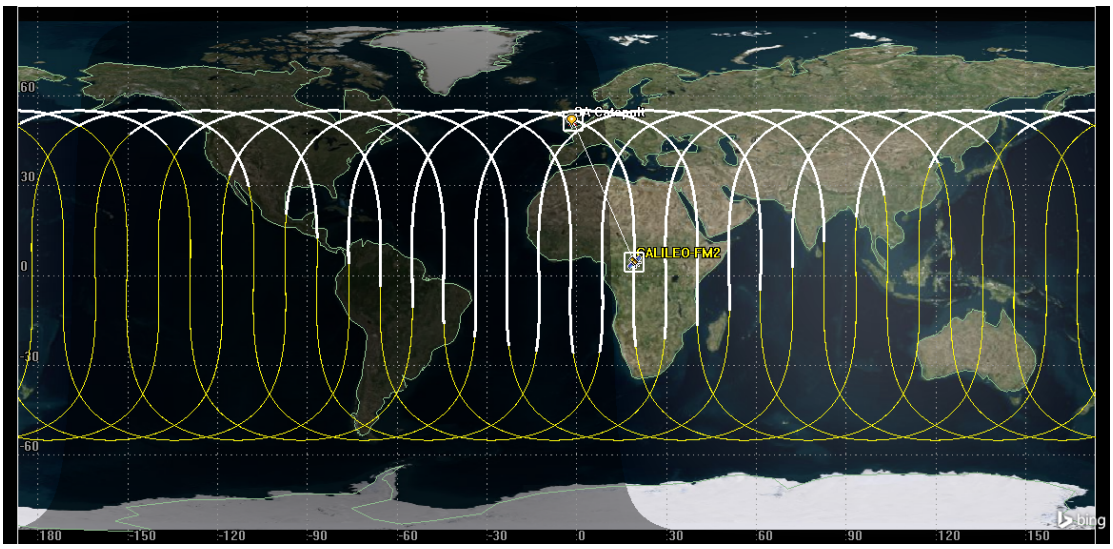


Figure 8 - Galileo satellite groundtrack

The following figure shows the current state of Galileo's constellation, presenting only 4 satellites in correct orbit. In the future is expected that 10 satellites will be placed in 3 orbital plans, with an inclination of 56º and a semi-major axis of 29600 Km, on a MEO orbit. (Springer, 2014)

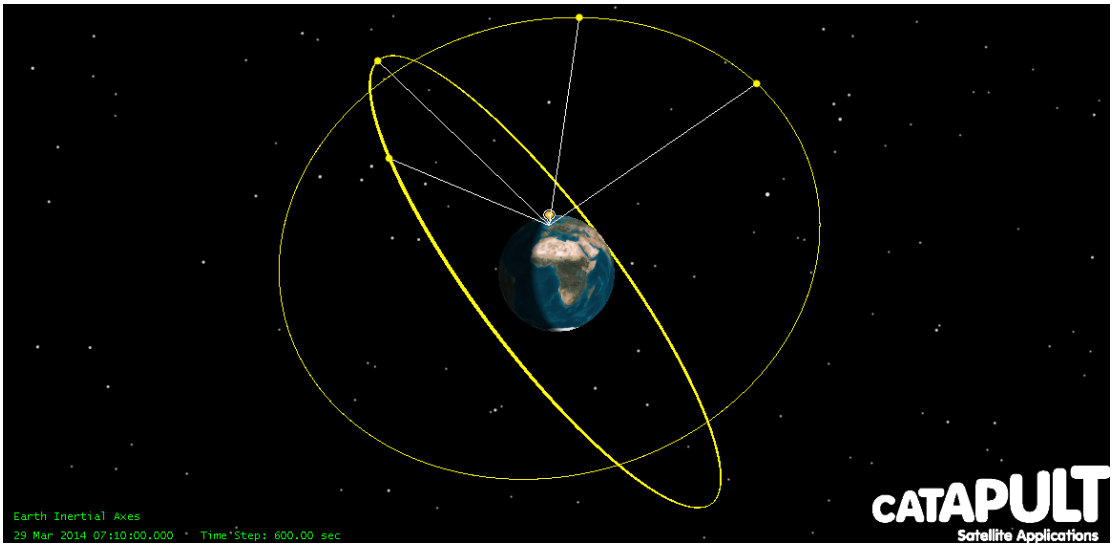


Figure 9 - Galileo constellation

In the subsequent figure it is possible to see a satellite in a Galileo orbit. In this case, the satellite is not a 3D model of an actual spacecraft.

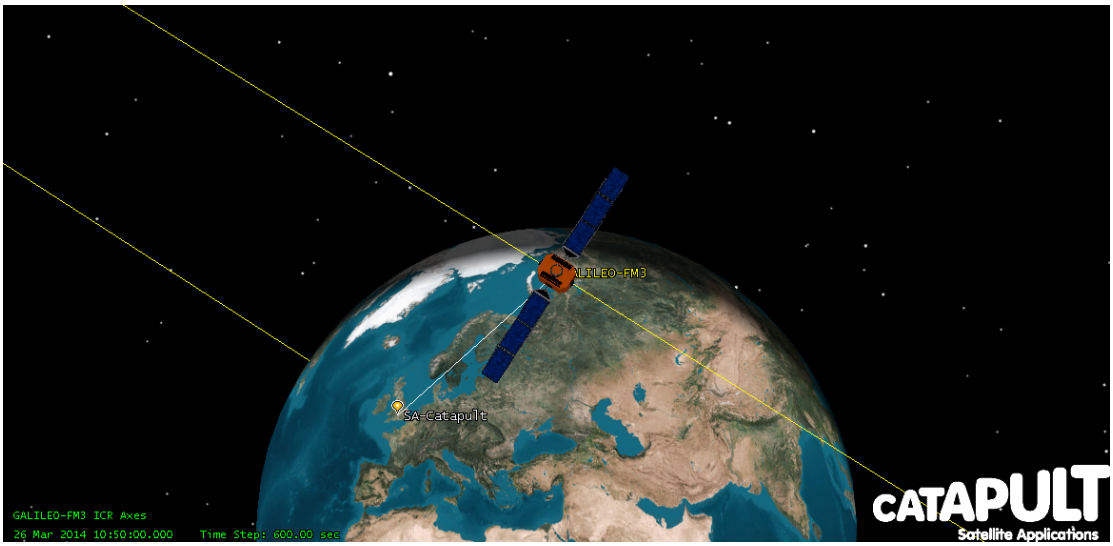


Figure 10 - Galileo satellite view

2.4. BEIDOU

2.4.1. HISTORY

BeiDou Navigation Satellite System is a Chinese GNSS, consisting in two different constellations, one deployed for testing and operating since 2000 (BeiDou-1) and the other one under construction, planned to reach full operability and global coverage by 2020.

BeiDou started in 1983 with a proposal to develop a regional navigation system using geostationary satellites that was proved to be functional in 1989. So, four years later the BeiDou program officially started. Two experimental satellites were put in orbit in 2000 and a spare third one in 2003, the BeiDou-1 constellation. This set of satellites provided basic services to the Chinese government and military, including positioning and timing within China's territory. Contrary to other previous GNSS, BeiDou required a receiver that could receive and transmit signals from and to satellites in order to obtain position. The system also required a control centre to do the PVT calculations for the users. These terminals were very expensive and by 2009 there were only 50000 BeiDou-1 enabled units.

The operational constrains of BeiDou-1 type of system made China announce a new constellation in 2006, BeiDou-2, using the same principles as GPS, GLONASS or Galileo, enabling precise PVT using passive receivers. During 2007-2009 several meetings were held among China and USA/Russia/Europe in order to establish compatibility and interoperability between systems.

The Beidou-2 constellation is very different from other GNSS since it will be composed of satellites in 3 different orbits: 5 in Geostationary Orbits (GEO), 3 on Inclined Geosynchronous Orbits (IGSO) and 27 (24 satellites plus 3 spares) on MEO. In 2014, there were 15 operational and active satellites, focused in Chinese territory. In 2020 global coverage is expected and by 2025 is estimated that the total number of BeiDou users will reach 900 million only in China, with an economic impact of € 65 billion, making it an important asset to the GNSS world. (Astronautix.com, 2014)

2.4.2. SIGNALS

BeiDou's signals are not fully defined and its constitution is not available yet though it's planned to be transmitted in 3 different bands, B1 at 1561.098 MHz, B2 at 1207.14 MHz and B3 at 1268.52 MHz, using CDMA protocol.

Each band will provide an open service, available to everyone, and an authorized service for special Chinese authorities, with better accuracies. (Navipedia.net, 2014)

2.4.3. ORBITS

BeiDou presents three different orbits, shown in the following picture. The yellow lines represents the orbit of the active four geostationary satellites, focusing Asian territory. In green the satellites with an inclined geosynchronous orbits. In white the satellites in MEO orbit.

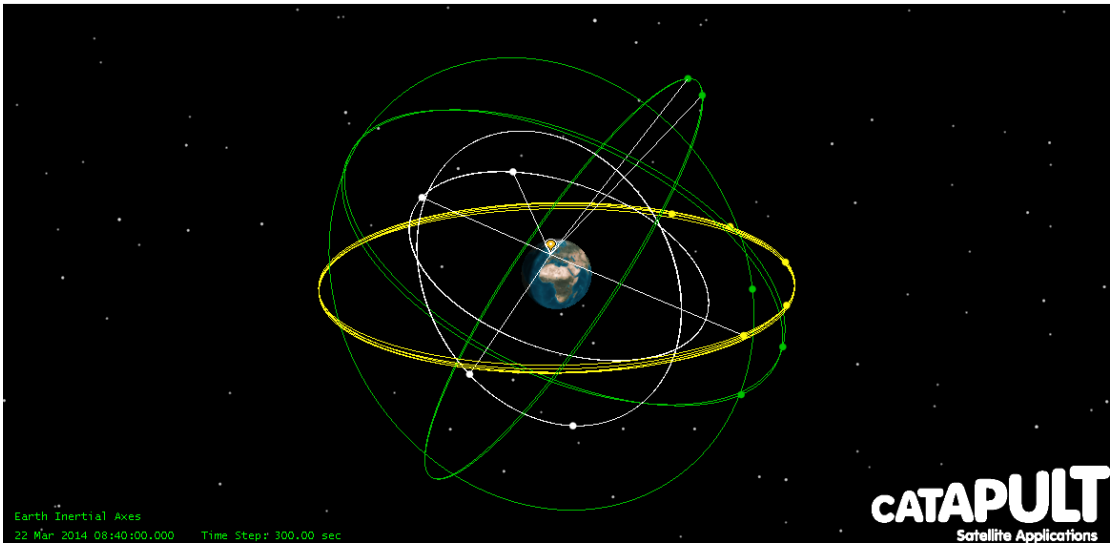


Figure 11 - BeiDou constellation

In an IGSO orbit satellites have a period of 24 hours, having a major axis of 35900 Km and an inclination of 55º. BeiDou MEO satellites

BeiDou MEO satellites have an orbit period of 12 hours and 55 minutes, having a ground-track repetition cycle of 6 days.

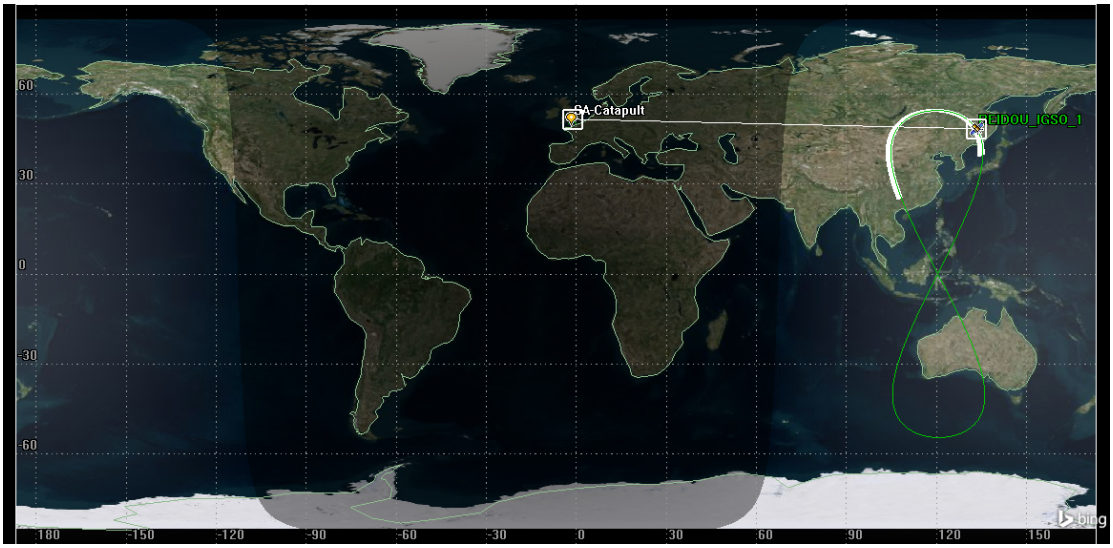


Figure 12 - BeiDou IGSO satellite groundtrack

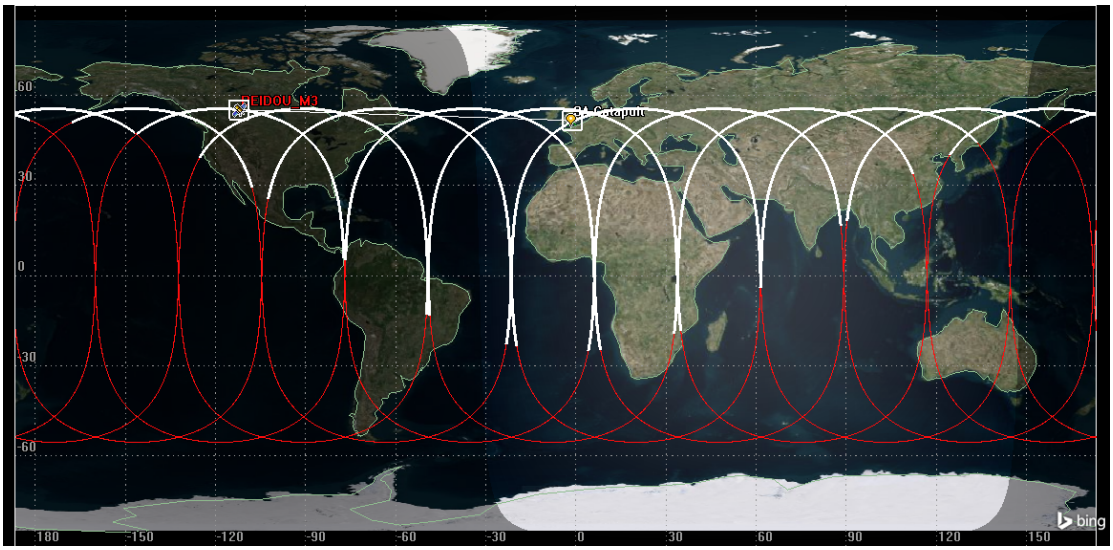


Figure 13 - BeiDou MEO satellite groundtrack

2.5. OTHER CONSTELLATIONS

In this internship, only the previous 4 GNSS were used, though other countries are creating also their own systems, with global or regional cover. Also Satellite-Based Augmentation Systems are being implemented, like EGNOS for Europe, WAAS for USA, GAGAN for India, etc. In the next figure is possible to see the actual status of the birdcage that surrounds us:

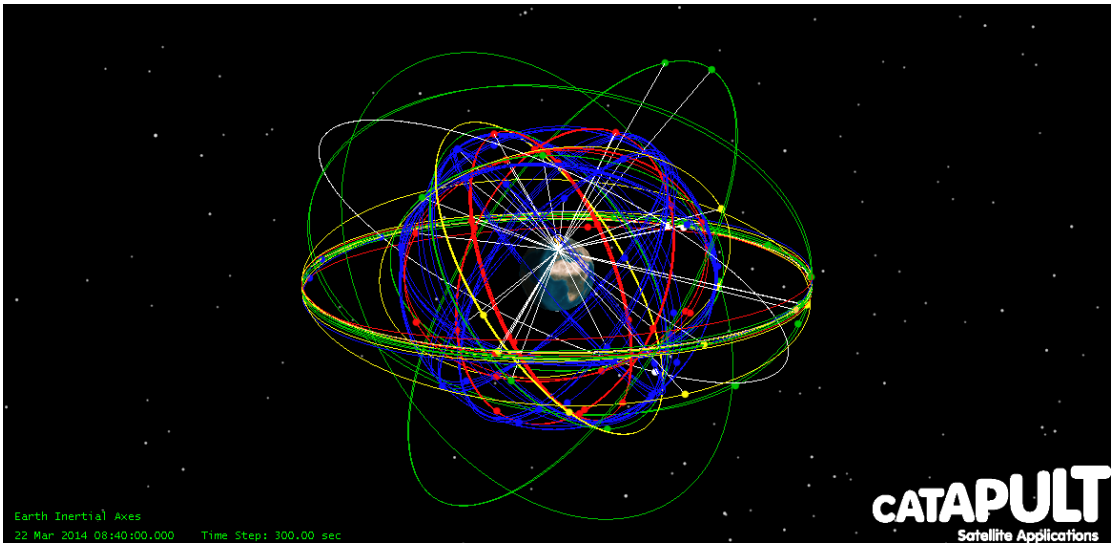


Figure 14 - GNSS birdcage

The colours represent the country of the system:

- Green – China (BeiDou)
- Yellow – Europe (Galileo, EGNOS)
- Orange – India (GAGAN)
- Red – Russia (GLONASS, SDCM)
- Blue – USA (GPS, WAAS)
- White – Japan (QZSS)

With so many satellites covering earth, once receivers are fully capable of detecting and tracking any signal, a lot of satellites will be visible from any point in the planet, any time, improving the quality of the positioning. In the following picture there is an example of the GNSS satellites visible from SAC premises in the 22nd of March 2014 at 8:40, with a total number of 32 satellites.

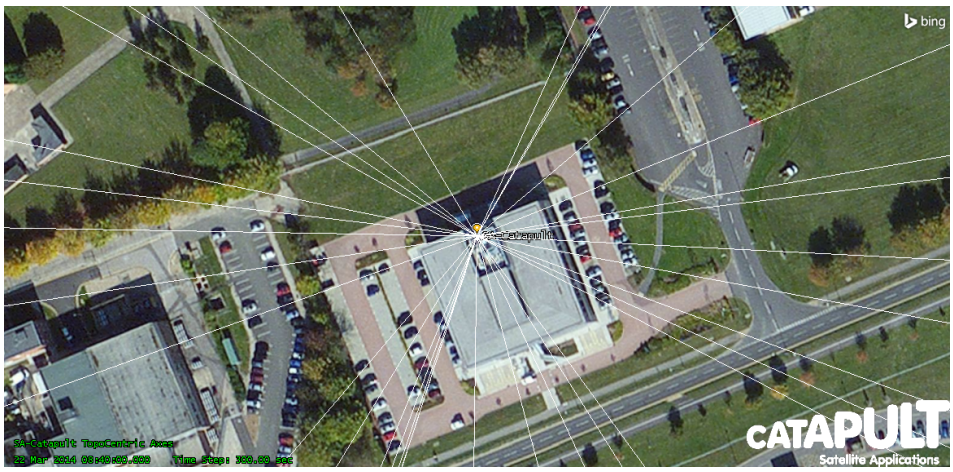


Figure 15 - Satellites in view from SAC premises

CHAPTER III

GNSS APPLICATIONS

3. GNSS APPLICATIONS

(The Royal Academy of Engineer, 2011)

As technologies evolve, becoming easier to use and more cost effective, they can become part of our daily life even without noticing it. If it's a solution to an older problem the development is even faster and this is the case of GNSS, that's the main reason why it has been adopted in an extensive list of applications.

GNSS can be used as a primary set of an application, accompanied or not with other technologies to improve it. However, it can also be used as a secondary back-up technology that will take over if other system stops working. From a few meters to a few centimetres, the offer is huge and the grade of accuracy needed is also an important factor to consider when adopting a GNSS solution, in positioning or in timing.

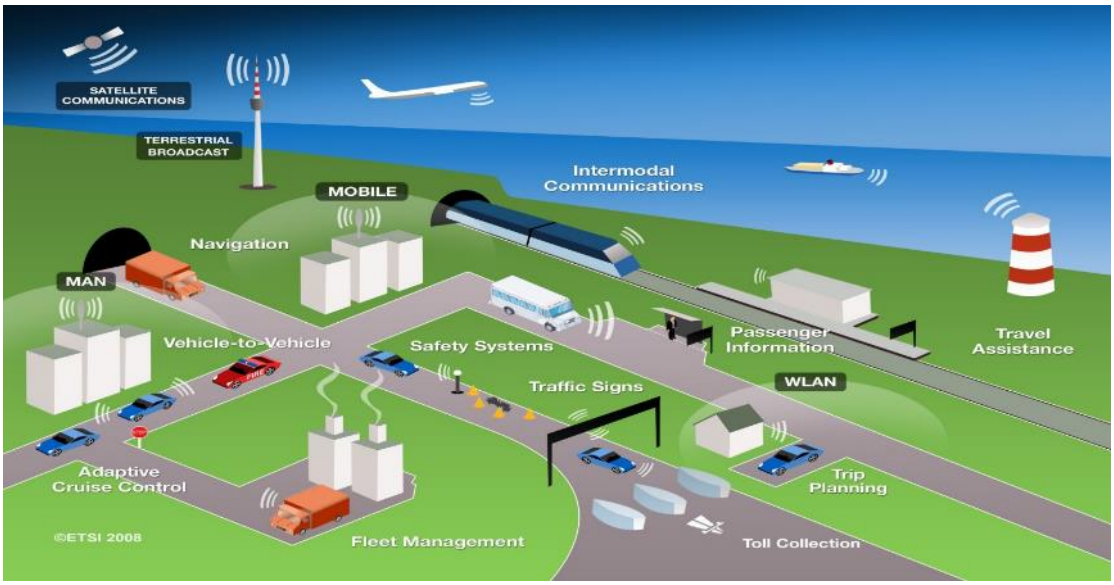


Figure 16 - GNSS applications network (Source: SAC)

The presented short list will showcase some important applications that are currently in use on some countries, and others that could be used in the near future due to the great asset they can become.

3.1. ROAD TRANSPORT

Road transport applications are the top users of GNSS signals, by market segment value. Location-based services (LBS) using smartphones are the most numerous users, but road transport GNSS receivers are more expensive making the total market larger. In-car navigation is the most common, from non to demanding users. Commercial fleet management, taxi services, public transport monitoring and information, emergency vehicles location, mail and dispatches are examples of applications. Some roads, especially motorways, also benefit from GNSS-based toll systems.

With the development of automated vehicles traffic management will evolve technologies like selective vehicle priorities, collision avoidance, dynamic route guidance, intelligent speed assistance and even lane control.

Car theft is a traditional problem and GNSS can aid on locate and recover stolen vehicles.

3.2. AVIATION

Nowadays, aircrafts use GNSS for in-route navigation, enabling auto-piloting in certain situations and some countries have authorised GNSS based approaches to certain airfields. GNSS enabled Automatic Dependent Surveillance – Broadcast (ADS-B) is used in areas where there's no radar coverage and enables to obtain position using GNSS and broadcasting to other aircrafts. It is also important in some specific tasks like flying in formation and mid-air refuel.

3.3. MARITIME TRANSPORT

Ocean and inshore navigation, port approaches, harbour entrance and docking is aided by GNSS. It also gives information to the Automatic Identification System (AIS) in order to identify a vessel, its position and communicate to other vessels nearby. Cargo handling can also have a GNSS receiver depending on the importance of the content.

3.4. Rail

Applications include the management of rolling stock, like location, speed, level crossings, trains separation and even power supply control. Some trains only open the doors when they are alongside the platform, when GNSS tells they are in the right position. Passengers also benefit from the system since they can have pre-trip and on-trip information.

3.5. Scientific

Scientific purposes using GNSS require a great level of accuracy and a lot of activities rely on it, like geodesy and surveying, geoids determination and reference systems, environmental monitoring, meteorology, climate research, ionosphere analyses, structural monitoring, photogrammetry and hydrography.

3.6. Timing

GNSS timing plays an important role on nowadays society. Synchronous technologies are more efficient than asynchronous ones but require a time source with a great level of accuracy, stability and reliability and GNSS can provide a cost-effective solution. Therefore GNSS is used in network synchronisations, like communications, digital broadcasting, power generation and distribution or satellite monitoring. Financial systems also need precise time stamping to prioritise trades and provide audit trail.

3.7. Agriculture and Fisheries

Precise agriculture is expanding hugely and evolving to automatic guidance of farm machines using GNSS as primary navigation source. Navigation systems are also useful in parcels mapping.

As stated previously, boats are equipped with GNSS receivers but in terms of fishing is also useful to monitor shoals, mapping best fishing areas.

3.8. CRITICAL APPLICATIONS

GNSS is now a significant aid in emergency vehicle location, dispatch and navigation, requiring a high level of availability and accuracy. New future Galileo services are expected to improve search and rescue, both for aviation and maritime, enabling communication between a receiver and satellites, and satellites to ground emergency bases, providing fast help, especially in remote areas where no network is available.

GNSS and other technologies like RFID (Radio-Frequency Identification) can be used for tracking criminals and suspects, lowering the criminal level and being evidence in court. New similar principles are used to tag children or even animals that could get lost or in danger, and even elderly, handicapped or blind people. GNSS tagging can also be useful to protect and study endangered animals.

CHAPTER IV

GNSS VULNERABILITIES

4. GNSS VULNERABILITIES

Nowadays it is so simple to identify a position on a map, or even getting from a point A to a point B easily. GNSS in-car navigation has become widespread and a broad range of motorists rely entirely on GNSS for navigation and, if they were to have a backup, it probably hasn't been used for a long term or is out-dated. This is a simple example of neglecting back-up systems but the list can be more serious when we take into account the applications on data networks, financial systems, science, shipping and air transport systems, agriculture, railways and emergency services. So, having a secure PNT solution is more essential than ever since it could impact national security and bring great economic losses. Today we just turn on our smartphone and everything is there, where we are, what's around us, where we want to go, etc. Though, the big question is what to do in case of a failure, failure that is expected to become more critical with the development of GNSS technologies and applications.

More important than adopting a GNSS technology because of its advantages is to be aware of its limitations. In critical services, GNSS vulnerabilities should be included in risk assessments, and reviewed regularly. For example, national or regional emergency services should review their GNSS dependencies, creating contingency plans for GNSS outages that could last from 10 min until several days, ensuring they have sufficient and efficient training in back up technologies.

Satellite constellations are designed and created with the latest technologies to avoid or mitigate certain problems they can face in space, especially their high precise clocks and signal transmission capabilities, to ensure that users on earth can effectively use their services. Still, there's a great distance between receivers and satellites, in between an atmosphere that can degrade signals quite easily, and an infinite range of scenarios on ground (urban canyons, forests, etc) that can block the signals. Human errors on operating satellites and receivers or hardware/software malfunctions, even though rare, can still happen, but, undoubtedly, the new GNSS threats that are growing faster are manmade, like jamming and spoofing. GNSS vulnerabilities can be broadly classified into three different categories:

- System (including signals and receivers);
- Propagation (atmospheric and multipath);
- Interference (accidental or intentional).

The impact that these vulnerabilities can have on users is quite different but can vary from partial to complete loss of positioning and timing service, poor accuracies, great jumps in position, velocity or timing, and hazardously misleading information (HMI): data that seems correct but is dangerously wrong in safety critical applications.

4.1. SYSTEM VULNERABILITIES

4.1.1. GROUND AND SPACE SEGMENT

The main responsibilities of the GNSS ground segment includes maintaining and monitoring system time, controlling satellites, uploading the navigation data (clock data, almanac and ephemeris data) that will be broadcasted to users, and supervising, consequently, the signal in stations all around the world. The GNSS satellites carry high-precision clocks, signal generations, amplifiers, antennas and other hardware with respective software that are also subject to failure. Any failure, disruption or misbehaviour in either the ground component or the space component could potentially compromise the end-user experience, even though the GNSS are designed with high reliability in mind.

4.1.1.1. FEW SATELLITES

GNSS constellations require a constant renewal of the satellite fleet, to prevent against potential simultaneous failures of multiple spacecrafts and late delivery of new and more developed ones. If the number of available satellites drops below the designed minimum of 24, users can experience a reduction in service, position outages or even bad accuracies related to bad satellite geometry. To avoid this situation it is then necessary that a GNSS is funded through a long-term strong political and economic agreement and under strict management. It's not expected that GPS will suffer from this, since it has been almost stable since its beginning. Though, the same does not apply to GLONASS that has been declared in FOC stage and later has seen the satellites number drop to 6, making the system almost unusable. Galileo is, unfortunately, an example of lack of political and economic

arrangements and this could compromise the launch of future satellites and consequent availability of the system.

4.1.1.2. UPLOAD OF BAD NAVIGATION DATA

Navigation data is uploaded to satellites routinely and it is the quality of that data that makes possible to have an accurate PVT. In case a bad page is uploaded to a satellite, the clock and the position of the satellite may be in error, which could confuse a receiver: not using that satellite or misleading it into wrong calculations. An extreme scenario of uploading bad data to every satellite on a constellation could happen, causing GNSS receivers to fail all over the world.

In June 2002, March 2000 and March 1993 GPS wrong data uploads happened without serious consequences. In April 2014 wrong messages where uploaded to the GLONASS satellites, which resulted in errors bigger than 200 Km on some GLONASS enabled receivers or even loss of position. (staff, 2015)

4.1.1.3. DRIFT OF SATELLITE CLOCKS

GNSS principle relies on the performance of the precise atomic clocks placed on-board the satellites. As every machine, these clocks can behave unpredictably, even though it's not likely, and consequently produce errors that can grow dangerously before a ground system or operator can notice and correct it or mark the satellite as unhealthy. In January 2004, the rubidium clock on-board a GPS satellite drifted for 3 hours before it was set as unusable, but by that time errors had grown until almost 300 Km. In July 2001 a similar case happened.

4.1.1.4. BAD SIGNAL SHAPES

Signal modulation hardware can be faulty and create unusual signal envelope that if transmitted can create unpredictable behaviour in receivers, ranging from dangerous errors to, in the best case, no impact, due to signal analyses implementation. In 1993 a GPS satellite transmitted an anomalous waveform, called 'evil waveform', which caused an error of up to 8 meters. In March 2009 also a GPS

satellite carried a faulty L5 signal generator that interfered with other frequencies resulting in some substantial errors in receivers, depending on the elevation angle.

4.1.1.5. ORBITAL ENVIRONMENT

GNSS satellites are subject to intense radiation through their orbits. When solar storms happen space-crafts are subjected to highly energetic particles that can impact their lifetime, even though their design can mitigate the impact. Unusual intense events can occur causing temporary shutdown of satellites. In the worst case possible, if a super-storm like a Carrington event occurs, a series of satellites can be shut down at the same time causing a big impact on receivers in the ground. The last super-storm happened in 1859 but it could occur at any time. It has been predicted that there is a 12% chance of one happening between 2012-2022, so it can't be ignored as a GNSS threat.

4.1.1.6. ATTACKS ON GROUND SEGMENT

The GNSS ground segments have been designed with the highest standards, but they are, as everything, still vulnerable to terrorism or cyber-attack, especially given that they are composed of worldwide distributed elements and considered high value installations. Even with the high standards at which they are operated and maintained, and the level of redundancies in place, an intentioned attack on the GNSS ground segment cannot be discarded as a GNSS vulnerability.

Within this scenario, the fact that the various GNSS are operated by independent organisations and countries, gives some level of protection to the end user.

4.1.2. USER SEGMENT

GNSS user segment is quite sparse and uncoordinated, comprising an infinite range of receivers and equipment belonging to a wide range of manufactures from decryption-capable military receivers to the mass-market of smartphones. Different levels of quality is then required but even the simplest receiver is a complex combination of radio and digital hardware and software capable of decoding the

broadcasted GNSS signals, with its unique algorithms and methods. This results in different receivers providing different response to the same input or combination of inputs, and coming with its own bugs and exploitable vulnerabilities.

Receiver's manufactures need to think in advance and be alert to the GNSS developments in order to make their receivers able to outstand any condition and avoid vulnerabilities.

4.1.2.1. WRONG TIME HANDLING

Manufactures seek the correct function of GNSS receivers but some events occur rarely and may have been incorrectly accounted or implemented when building particular equipment. GPS time is managed in terms of seconds of week, and respective week. In August 1999 the week 1024 was reached and a reset was done in order to proceed with correct data transmission, since weeks over 1024 needed more bits in the modulated signals. So, GPS satellites started emitting signals with time information regarding week 1. Some receivers wrongly interpreted the signals and calculated the time as January 1980, the beginning of GPS time-scale, because they weren't ready to handle this type of event and needed a firmware fix. A similar example happens with leap seconds that are introduced in the system when needed. Some receivers still don't work properly and cause a timing error, even though there are specifications in how to handle them.

4.1.2.2. SYSTEM UPGRADES

GNSS pursue stability but upgrades occur and cause unexpected performance in receivers. In April 2007, a 32nd satellite was added to GPS constellation and provoked some problems in receivers that were only capable of handling 31.

In January 2010, GPS ground segment software was updated resulting in a faulty performance of military and timing receivers.

4.1.2.3. RECEIVER BUGS

In some areas like military or aviation, receivers' performance needs to comply with demanding standards, therefore manufactures need certification to their

equipment. Other low cost systems just need to pass manufacturer's production test regime, and is probable that some are not free from software bugs that will affect their performance. Examples of common bugs are the wrong handling of unhealthy satellites, tracking of non-standard codes, behaviour when signals are stronger or weaker than expected, reaction to jamming or spoofing, changes or updates on GNSS, etc.

4.1.2.4. GNSS ENHANCEMENT TECHNOLOGIES

Systems created to enhance GNSS performance can introduce also some vulnerability into the system.

SBAS satellites (EGNOS, WAAS, etc) are becoming increasingly important in a series of applications, especially aviation, promising integrity and high accuracy. Though, as any GNSS satellite, they are also subject to failure, due to equipment fault or even to ionospheric disruptions.

A-GNSS is used broadly in smartphones, downloading external ephemeris data that can speed up satellite acquisition. However, a bad ephemeris download can degrade receivers' performance, increasing fix time or even causing poor accuracies.

4.2. PROPAGATION VULNERABILITIES

4.2.1. ATMOSPHERIC VULNERABILITIES

GNSS signals must pass through 20 000 Km to 25 000 Km of space and earth atmosphere before it reaches the ground based applications, and when a signal hits the surface the strength may be -130 dBm, almost as low as the noise floor. Consequently, GNSS signals are affected by the atmospheric medium they pass through. Space weather impacts the performance of space applications and even human health and safety, including direct effects from sun, solar winds, and changes in magnetosphere, ionosphere and thermosphere. Unfortunately the atmosphere is quite variable in time and space creating difficulties on minimizing the effects on GNSS signals.

The dry troposphere layer can impact modestly GNSS signals since delays can be largely mitigated with a model. However, the wet component can impact randomly and its behaviour is somehow unexpected.

The ionosphere layer can introduce the largest errors in GNSS if not properly corrected. Ionospheric impacts are more severe at high and low latitudes and can be quite severe in peaks of the solar cycle. Ionospheric errors are often refered to in terms of the Total Electron Count (TEC) through which the satellite signal passes. Slow and fast variations are described in the next two sections. Scintillations are another ionospheric effect and are described afterwards.

4.2.2. SLOW VARIATIONS IN TEC

GNSS signals are delayed in proportion to the TEC along the path between satellite-receiver. TEC variations are caused by the sun effect on the ionosphere indirectly, like: earth's diurnal rotation, sun variability, the sun's 27-day rotation and sun's activity cycle of 11 years, which can cause the electrons column to rise or fall. So, TEC can produce unmodelled variations on GNSS range measurements, which can be mitigated using estimated corrections, Differential GPS corrections, combining measurements/observations or using dual frequency GNSS receivers.

4.2.3. FAST VARIATIONS IN TEC

Solar flares and coronel mass ejections can produce fast variations in TEC, and depending on the gravity of the storm they can't be corrected by SBAS and other systems, though they can be detected. However, the disruption on GNSS signals will also affect SBAS systems. Mitigation can still be possible using dual frequency receivers.

4.2.4. SCINTILLATION

Scintillation is a small-scale perturbation in the ionosphere, occurring more frequently over the equator and near the poles, though it can be more widespread. If designed properly a receiver would be able to identify the fast variation in phase and amplitude, but if not it could lose signal lock. In October and November 2003 a solar

storm happened causing scintillation effects and disabled the WAAS network for 30 hours.

4.2.5. CARRINGTON EVENTS

As stated previously, a Carrington event can impact satellites directly causing temporary shutdowns, but even the signal transmission can be cancelled. Since it's not a predictable occurrence and the latest was 1859, far from satellite era, its potential impact and consequences are not fully well characterised.

4.2.6. NUCLEAR TESTS

Nuclear explosions in the upper atmosphere have been proposed as an effective manner of disrupting GNSS and other satellite and earth systems.

4.2.7. MULTIPATH

Multipath describes when a receiver tracks a reflected signal rather than the direct signal from the satellite. Since a reflected signal does not follow the minimum distance path (linear) between satellite and receiver, it provides a delayed measurement that will cause an error in timing and position.

GNSS signals can reflect in distant objects like buildings, or even trees, producing gross errors. Multipath is a quite well known phenomenon by scientists and receiver manufacturers but its mitigation is quite hard since there is a huge set of scenarios around where a receiver can be placed: from a full sky view to a urban-canyon (representative situation where just a small part of sky is clear). However mitigation techniques have been applied in antennas, rejecting signals bellow certain elevation angle, and in receivers filtering and processing techniques. For low-cost receivers multipath errors can range from tens to hundreds of meters, making GNSS not suitable, yet, to autonomous car navigation for example. Even though multipath can be considered as vulnerability, due to its unpredictability, is more common to treat it like an error source.

4.3. INTERFERENCE

4.3.1. ACCIDENTAL

GNSS signal has so low power on Earth surface that accidental interference can impact receivers. Harmonic emissions from commercial high power transmitters, ultra wideband radar, television, VHF, mobile satellite services and personal electronics are examples of interference that can in an extreme case cause complete loss of lock. In 2002 a CCTV camera in Douglas, Isle of Man, United Kingdom, caused GPS signal blockage within 1 Km.

4.3.2. DELIBERATE

There are two important types of deliberate interference than can easily impact GNSS receivers making them useless or misled: jamming and spoofing.

Jamming is, for sure, the biggest GNSS vulnerability that can impact even the most expensive and developed receiver. A jammer simply transmits a noise signal across usually one GNSS frequency (normally GPS/Galileo L1/E1), but could target multiple frequencies simultaneously, in order to raise the noise level or overload receiver's circuits causing loss of lock.

Jammers can be bought easily on the Internet for less than € 30, they fit into a pocket and to make it work you just need to simply plug it into a car lighter socket. Depending on the specifications, they can block signal from any constellation, even Galileo wish is not fully operational yet, and more expensive ones can block at the same time Wi-Fi and mobile phone frequencies. There is a broad range of jammers, from small devices that only impact a few meters around the jammer, to others that can go until a few kilometres. The use and selling of jammers is completely forbidden in most European countries, like Portugal and the United Kingdom. In the United States of America, homeland of GPS, is also considered a crime since it can impact dramatically critical safety GNSS applications.

Modern GNSS receivers with well-designed noise filtering and adaptive antennas can bypass low and medium levels of jamming (even with some difficulty),

although piracy is always some steps ahead and there are jammers that transmit structured signals rather than random noise, to bypass the filters.

Until this moment, critical events regarding jamming focus on car theft, avoiding fleet control systems and other events with limited consequences: like a jammer passing nearby Newark airport (New Jersey, USA) and affecting the airports' GNSS ground-based augmentation systems or North Korea jamming South Korean border.

Spoofing is a more sophisticated type of interference, requiring quite technical equipment, like GNSS simulators, and consists on sending false GNSS signals in order to mislead a receiver, outputting wrong and misleading PVT solutions. Spoofing is technically challenging to produce in a real world situation but its consequences can be catastrophic. Fooling a receiver, without any warning, can, for example, put a boat navigating in a specific route directly into pirate hands.

The University of Austin (Texas, USA) made successful tests on spoofing a vessel in high sea, putting a boat drifting in a wrong route without any warning. They also successfully tested and controlled remotely a UAV (Unmanned Aerial Vehicle), trying to reproduce and demonstrate the possibility that an USA drone was taken down using spoofing techniques in Iran in 2011. This study was quite impressive when we think that anyone can simply hijack a UAV, making it crash to a building, to the ground, fill it with explosives and have dramatic effects. (Utexas.edu, 2015)

In the next chapter, jamming and spoofing will be more developed and some in-lab tests results, produced during the internship, will be provided and used to assess the impact of jamming and spoofing on commercially available receivers.

CHAPTER V

JAMMING & SPOOFING TRIALS

5. JAMMING & SPOOFING TRIALS

5.1. JAMMING

Jamming is not a new phenomenon, it has been alive since the start of signal transmission via electromagnetic waves in order to intercept or block any kind of communication in a deliberate way. Common frequencies like Wi-Fi, GSM, UMTS, LTE or VHF can be easily jammed and its impact can vary as much as the reasons to do it. During wars jamming is frequent in order to impact the enemies, or in some places jammers can be placed to avoid communication to the outside for security purposes. Nowadays, new signals became important in a lot of applications, like GNSS frequencies, becoming a target for jamming.

Figure 17 - Detection of jammer location (Source: Pedro Alfaro Sanz)

Jamming can be split into four different types:

- Accidental;
- Criminal;
- Red Team;
- Blue Team.

Accidental jamming is generally caused by the transmission of signals close to GNSS frequencies and can easily disrupt communications due to the GNSS weak signal from space. This issue is usually something localized and potentially manageable once identified.

Criminal jamming is the most common type and is caused by people who seek to avoid GNSS tracking devices, like car thieves, toll evaders, and tracker evaders, drivers who want to avoid mileage limits or bosses' knowledge of their movements. These events are usually a result of low power jammers and its users don't usually care (nor understand) about power levels and the impact on other receivers nearby. It's usually a momentary event with small impact due to the movement of jammer.

Red Team (generic term for enemy/criminal/terrorism) jamming may be targeted at some specific aspects of critical infrastructures or applications, likely to be high power and may occur at a number of locations simultaneously.

Blue Team (generic term for friendly force) is used mainly to overtake hidden trackers. It can be compared to criminal jamming in terms of power however if stationary for long periods near critical infrastructures the threat can be considerable.

5.1.1. JAMMERS

Devices that claim to block GNSS signals are widely available on the Internet, having a cost of tens up to several hundreds of euros. Even though buying and using them is illegal, their popularity is increasing and starting to be a threat to GNSS integrity. Jammer's specification and effectiveness publicized by manufactures are usually beyond their actual power and their ranges can go from a few meters to several tens of meters, consuming a fraction of Watt to several Watts.

Small jammers are sometimes fitted in cars and trucks to block any GPS-based tracking on the vehicle. This type of low-power jammer is also called Personal Privacy Devices (PPD's) transmit at or near L1/E1 frequency (1575.42 MHz), thus new and more advanced models transmit also in L2 (1227.60 MHz), future L5/E5

(1176.45 MHz) and also GLONASS L1 (around 1602.00 MHz). It is expected that as more bands are introduced, jammers will follow the evolution.

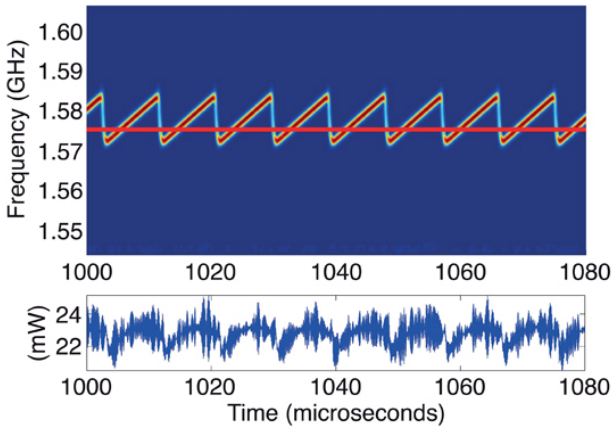
Ryan H. Mitch et al groups jammers in three different categories based on power-source and antenna type: the first group encompasses jammers designed to plug into a 12 V car lighter socket (powers can vary from 1 mW to 10 mW), the second category contains the ones powered by and internal rechargeable battery and have external antennas connected via SMA (powers can go from 1 mW to 250 mW); the third group includes the ones that have batteries but do not have external antennas (very low power, 1 mW). (Mitch et al., 2011)

Figure 18 - Types of Jammers (Source: Google)

There are many types of RF interference, including tones, swept waveforms, pulse narrowband noise, broadband noise and other multi-frequency and time-varying versions of the referred methods. *Thomas Kraus et al.* gathered several types of jammers from different manufactures and analysed their performance, grouping them by transmitted signal type:

- Class I: Continuous wave (CW signal);
- Class II: Chirp signal with one saw-tooth function;
- Class II: Chirp signal with multi saw-tooth functions.
- Class IV: Chirp signal with frequency bursts.

Most of PPD's belong to class II, having unidirectional chirp signals. They have one positive saw-tooth function describing the instantaneous frequency and a negative slope that is extremely higher than the positive one. Sweep times can vary from 8 to 30 μsec and the bandwidth goes from 10 to 30 MHz. (Kraus et al., 2011)



Graphic 1 - Chirp signal with one saw-tooth function (Source: Google)

5.1.2. TRIALS

(Dixon et al., 2013)

Commercial receivers behave unpredictably when there is jamming noise. Experiments have been conducted by several entities, especially maritime ones, to assess the impact of jammers in different applications, evaluating and quantifying the consequences. Some receivers gave wrong information rather than reporting an error, showing great inaccuracies like Km's a part from its actual position or speeds of more than 1000 Km/h for a simple ship. In some cases, when high precision was needed for safety situations, receivers reported HMI (Hazardously Misleading Information) of tens or hundreds of meters, and courses and speeds wrong in few degrees and knots. The consequences of HMI can be quite serious if vessels navigate in low visibility, broadcasting erroneous position to other ships through the AIS.

In order to measure the impact of jammers on receivers, Satellite Applications Catapult conducted several in-lab experiments, guided by the previous work done by Dr. Chaz Dixon, as documented in the STAVOG study. These trials were conducted during the period of May to August 2014, having as a prime objective to analyse the behaviour under jamming of two types of receivers (one low-end other high-cost) in terms of positioning output.

Project planning was executed and is presented as an attachment to this report (annexe 4). Initially planned to represent an in-land vehicle, was later changed to a maritime application, though the planning document was not updated, as the principles were not modified. The change was justified as it would allow to analyse

and validate SAC capabilities and its equipment against the reference work previously performed in STAVOG.

5.1.2.1. EQUIPMENT

The equipment used in these trials and its main connections can be seen in the following scheme:

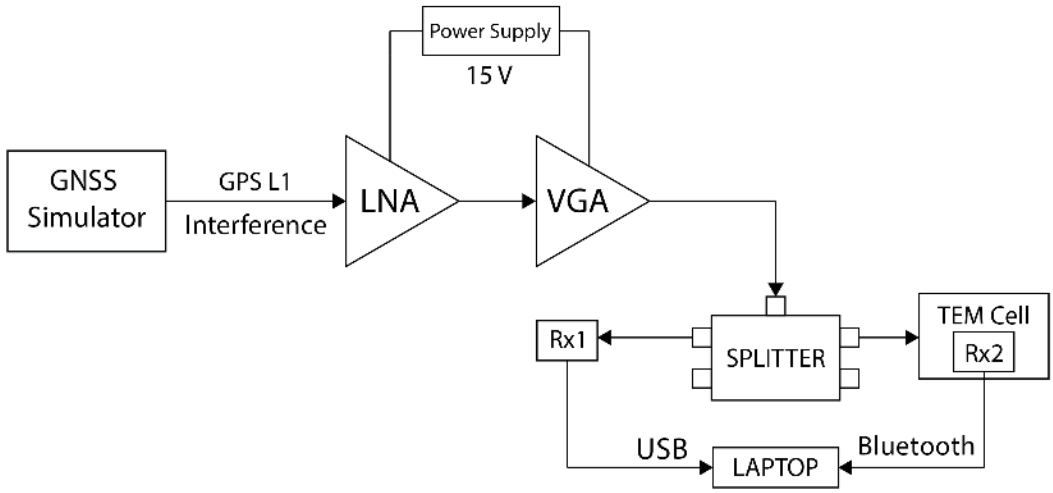


Figure 19 - Jamming trials equipment scheme

The GNSS simulator unit was responsible for producing the GNSS signal (GPS L1) and the interference as well. An alternative is to use the GNSS simulator to emit GNSS signals and to use a separate interference source connected in via an RF combiner. The advantage of the simulator-only approach is that all important parameters including jamming power can be controlled by the same software suite. In the circuit two amplifiers were introduced, one LNA (Low-Noise Amplifier) and a VGA (Variable Gain Amplifier). Both amplifiers were powered with two different power suppliers at 15 V in order to achieve the biggest signal amplification. A RF splitter divided the signal into two outputs, one that plugs directly to the high-end receiver (named Rx1), and the other plugs to the TEM (Transverse Electromagnetic) cell where the low-end receiver (named Rx2) is placed. A computer was connected by USB to Rx1 and via Bluetooth to the Rx2 in order to record the data. Receivers were fully reset at the beginning of every simulation.

Rx1 is a GPS/GLONASS/Galileo/BeiDou/SBAS enabled receiver, multi-frequency having phase and range measurements. Rx2 is an external Bluetooth

GPS/GLONASS/SBAS L1 receiver, with only range measurements. Rx1 and Rx2 manufactures and models are not presented in this report due to confidentiality terms.

The amplifiers were mainly used to compensate the TEM cell signal losses inside the chamber, so that the Rx2 could track GPS with normal C/N, and to also compensate for cable losses.

NMEA messages were recorded using Rx1 proprietary software and Quantum GIS for Rx2. Python was used to programme the necessary scripts for analysing data.

The simulator had a control centre software where every involved parameter was fully customizable. In order to run a simulation it was needed to set the time of simulation, upload the almanac for the desired week, add track file and arrange the interference times and power levels. As soon as these steps were completed and the connection scheme was in place, it was possible to start the simulation.

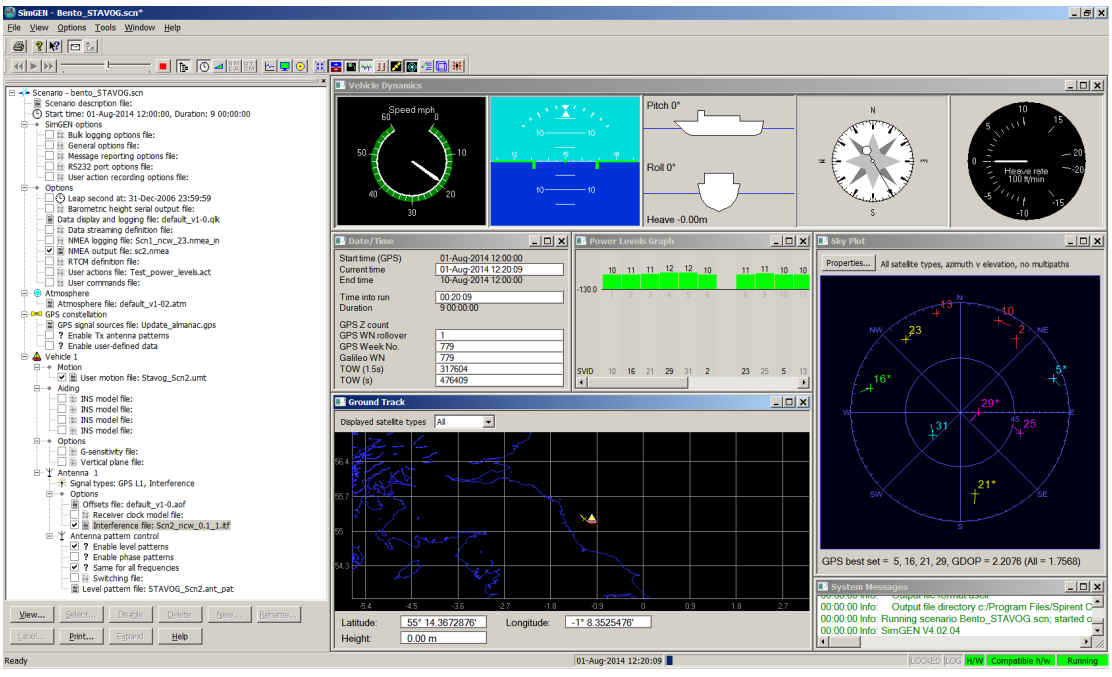


Figure 20 - GNSS simulator control software

5.1.2.2. DATA ANALYSES SCRIPTS

Python scripts were developed during the internship to analyse data. These scripts read the NMEA messages outputted by the simulator, the reference track, and compared them to the ones outputted by the receivers.

Python was the programming language chosen since it is open source and highly customizable, having also easy to use and powerful plotting modules.

The script processes the reference track, reads the $GPGGA messages and divides the information into a table with separate fields for timestamp, latitude, longitude, height, satellites in view and Horizontal Dilution of Precision (HDOP). Then, the same is done to the receivers' output.

In the next step, the script compares the time stamp of both NMEA files and analyses where they match, comparing the coordinates and calculating the error in meters. For this, it is calculated the meridian and parallel radius of curvature, and consequently how much is a meridian and parallel arc at the given latitudes, giving the distance between points in meters. It's a simple approximation, since the distance between points is very small and there is no need to calculate great-circle distances, since they would be roughly the same with these distances.

Once the planimetric error is calculated is given the average, standard deviation, maximum and minimum errors for horizontal and vertical measurements. It's then possible to plot the information in 5 different graphics:

- Planimetric error in latitude and longitude;
- Global horizontal error over time;
- Global vertical error over time;
- Satellites in view over time;
- HDOP over time.

The script also outputs the planimetric error over time to a *.csv file in order to create the graphs used on these report, using Microsoft Excel.

This is an example of the output of the script:

::::: TRACK ANALYSES ::::::

----- Analysis Period -----
Start: 12:15:0
End: 13:35:0

----- Reference Track -----
Filename: Scenario 1.txt
Start: 12:0:0.0
End: 6:27:14.0

------- Study File --------
Filename: rx2_cw25.txt
Start: 12:5:19.0
End: 13:38:50.5

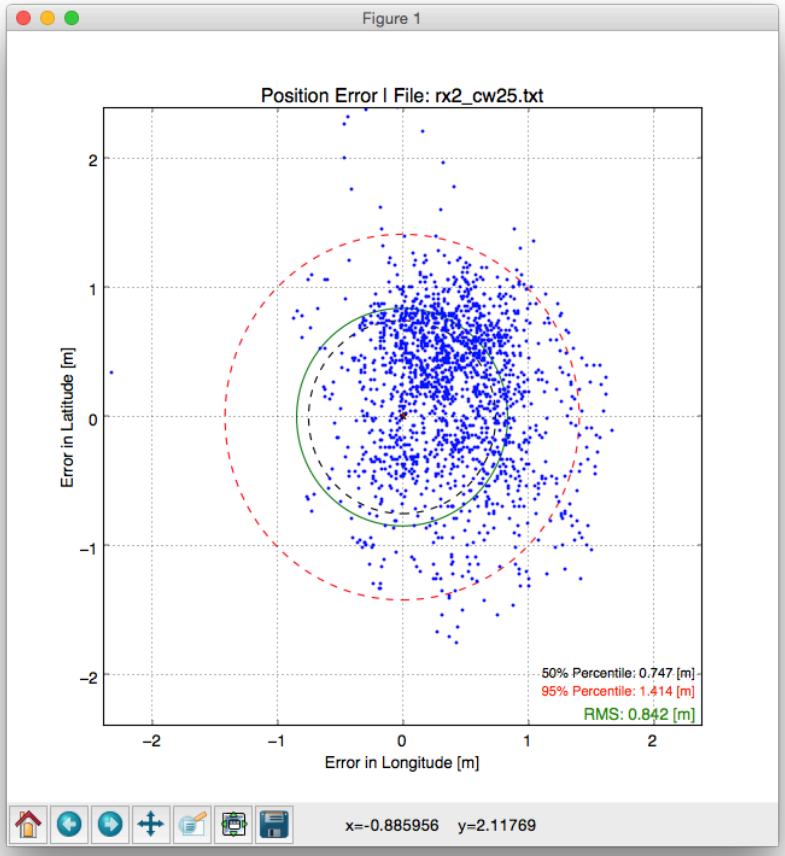
-- Horizontal Statistics --

AVG [m]: 0.762
STD [m]: 0.359
RMS [m]: 0.842
MAX [m]: 2.388
MIN [m]: 0.021
VAR [m]: 2.367

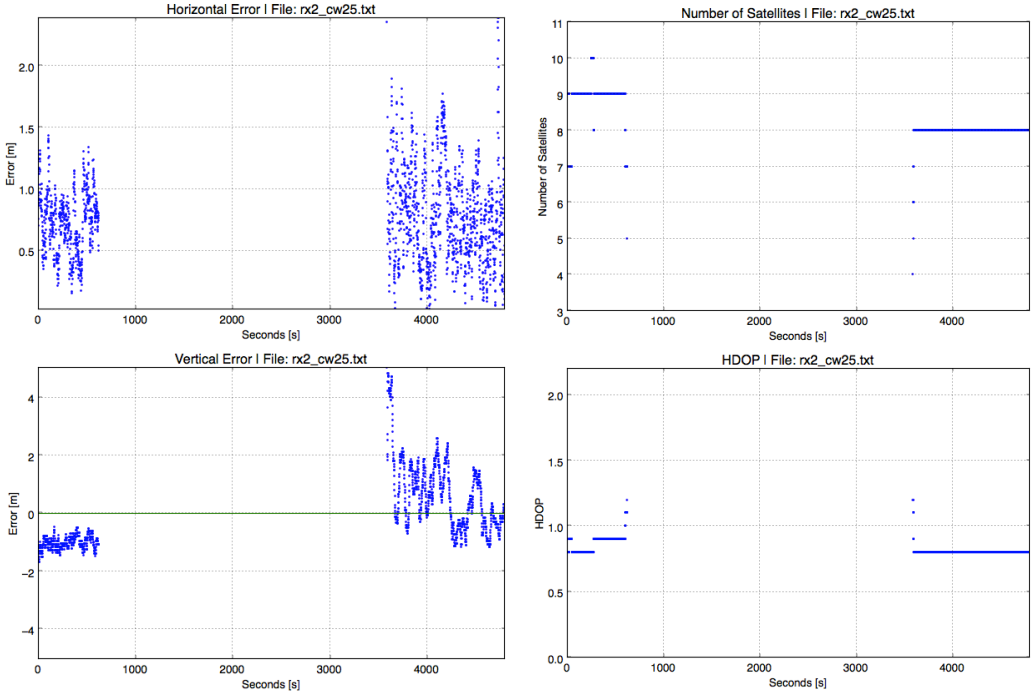
--- Vertical Statistics ---

AVG [m]: 0.073
STD [m]: 1.272
MAX [m]: 5.030
MIN [m]: -1.700
VAR [m]: 6.730

---> Measurements: 1801



Graphic 2 - Python script example of position error



Graphic 3 - Python script example of graphs

5.1.2.3. SCENARIO 1

The first scenario simulated a powerful jammer on shore as a vessel passes by it, approximately 6 Km away, near Flamborough Head, United Kingdom (approximately N 54.1160º W 0.0830º). The jammer was equipped with a yagi antenna, an antenna with a powerful centre main lobe followed by two weaker side lobes. The vessel starts its movement passing by a zone with no interference for a long time in order to acquire full almanac from satellites. After that period it would pass through jammer's first side lobe, experiencing moderate interference, followed by the main lobe with high jamming, the second side lobe and, finally, no interference again. The ship would move at, approximately, 10 knots (19 Km/h) in a uniform straight track of 14 nautical miles (25 Km).

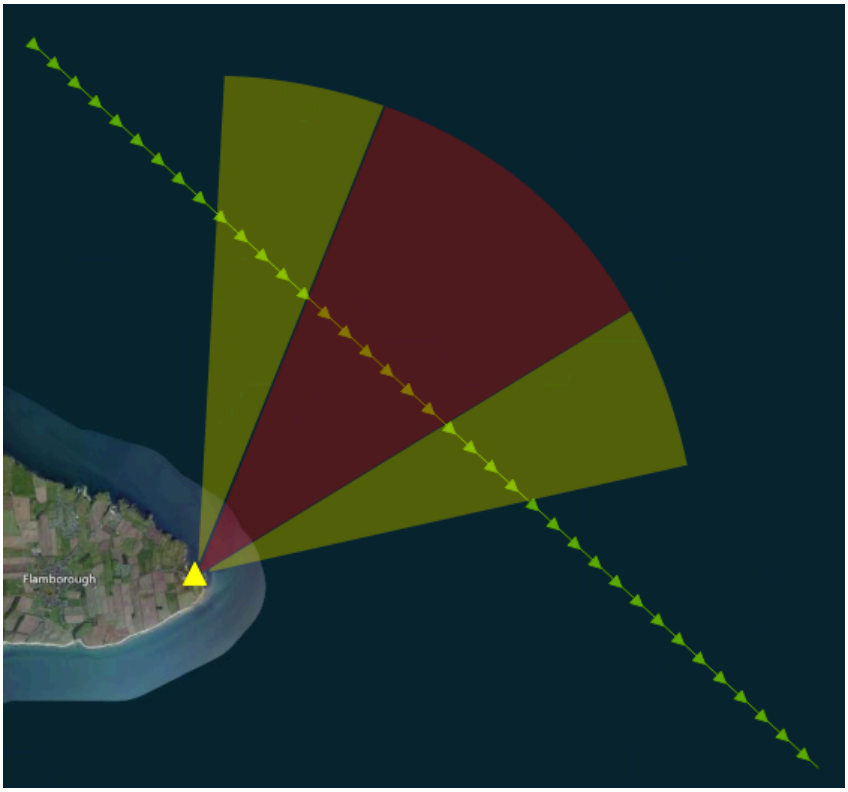


Figure 21 - Scenario sketch

A jammer on shore (yellow triangle) emits noise with the main lobe's area of action in red, and side lobes in yellow. The green line represents the ship movement.

5.1.2.3.1. SETUP

Simulated track files (*.umt) need to be created using a NMEA message file and to achieve this we need point's coordinates and vessel heading.

Start and end points were given, though two extra points were extrapolated in order to give more time for the vessel to acquire full navigation from satellites.

	Time	Latitude	Longitude	Height
Start Point	0 min	N 54.245980º	W 0.190758º	0 m
Study Period Start Point	15 min	N 54.215417º	W 0.131050º	0 m
Study Period End Point	95 min	N 54.080800º	E 0.118450º	0 m
End Point	110 min	N 54.054228º	E 0.166608º	0 m

Table 1 – Track 1 reference points

With the coordinates it was possible to create fake NMEA $GPRMC messages that the system could read and convert to the desired format. The headings, also necessary in this type of message, were calculated using a Matlab (http://www.mathworks.com/products/matlab/) function called azimuth. Since it was a straight line the heading was always the same, resulting in:

$GPRMC,114500,A,5414.7588,N,00011.4455,W,0,0,070314,0.0,E,D

$GPRMC,120000,A,5412.9250,N,00007.8630,W,10,132.6,070314,0.0,E,D

$GPRMC,132000,A,5404.8480,N,00007.1070,E,10,132.6,070314,0.0,E,D

$GPRMC,133500,A,5403.2537,N,00009.9965,E,0,132.6,070314,0.0,E,D

Finally, the respective converter was used and the *.umt files was imported to the simulator.

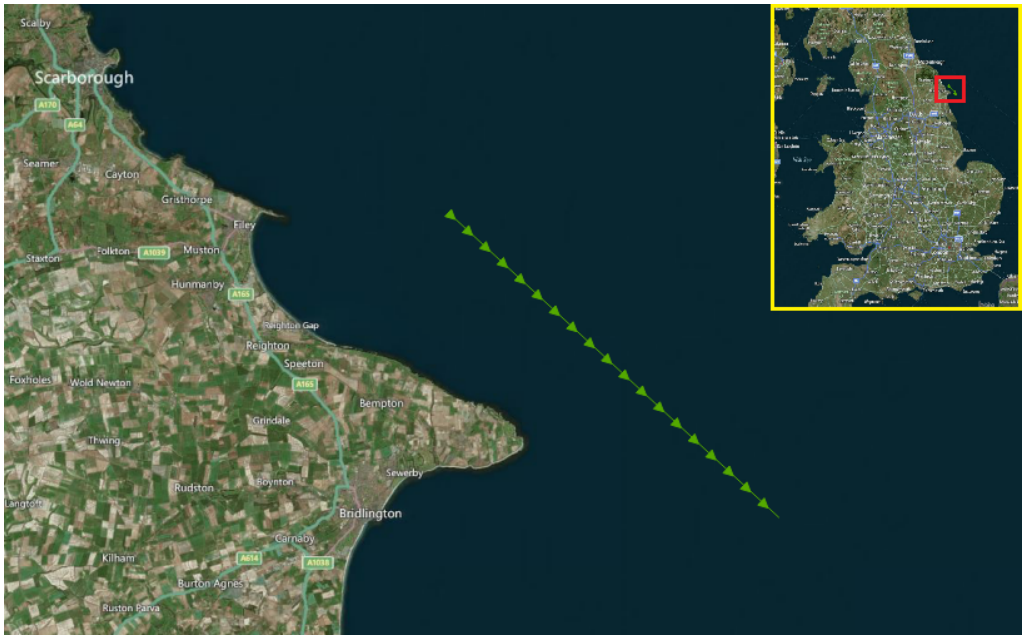


Figure 22 – Scenario 1 location

Three different types of jammers with different powers (23 mW, 640 mW and 25 W) and three types of interference [continuous wave (CW) signal, broadband 2 MHz and broadband 20 MHz] were simulated for the same track.

It must be raised that in the STAVOG study two of the most common types of interference were not tested: chirp signal and pulsed interference. Chirp signals were not possible to simulate due to hardware limitations regarding the sweep times of the needed signals and the pulsed interference didn't have any impact on receivers. Consequently only Kraus' Class I type of PPD was possible to test, completed with broadband noise.

Jammer's full power was desired in the middle of the track, in order to simulate a yagi antenna main beam, so, a middle point was calculated along the track and consequently the distance between jammer-vessel was obtained: 5.9 Km. Having the distance and the power level of the jammer, it was only necessary to get the signal power at the vessel's location. In order to achieve this a few calculations were made:

- Calculate the power ratio in dBm's at the transmitter using:

$$\mathrm{dBm} = \log_{10}(\mathrm{mW}) \times 10 \quad (1)$$

23 mW = 14 dBm | 640 mW = 28 dBm | 25 W = 44 dBm

- Get free-space path power loss (FSPL) for the desired distance (5.9 Km) at the GPS L1 frequency (1575.42 MHz) using antennas without gain or attenuation:

$$FSPL\ (dB) = \ 20\ log_{10}\ (5.9) + \ 20\ log_{10}\ (1575.42) + 32.45 = 112\ dB \quad (2)$$

So, in the receiver, the jamming signal power would be:

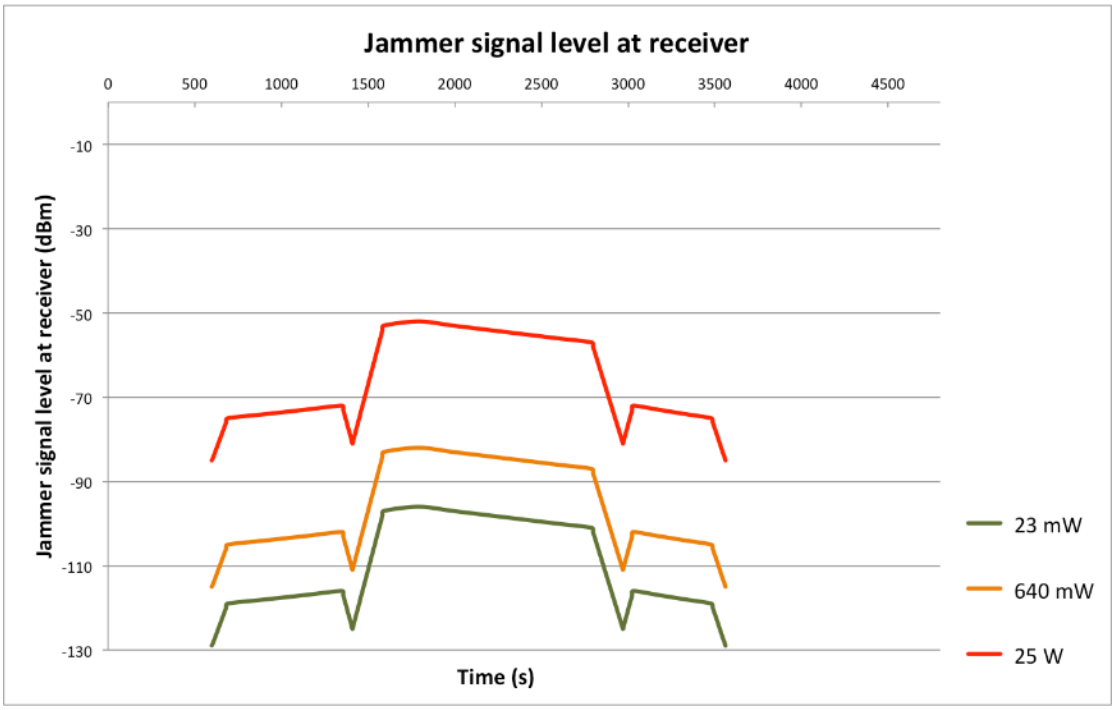
$$Power\ level\ at\ Rx = \ dBm - FSPL \quad (3)$$

23 mW = -98 dBm | 640 mW = -84 dBm | 25 W = -68 dBm

These power levels were a first approximation for the interference power to use in the simulator, though the actual simulated results vary 2 dB for a 23 mW and 640 mW and 16 dB for the powerful 25 W one, as used in STAVOG. In the graphic 5 it is possible to see that there is a powerful main beam followed by two side lobes slightly weaker, simulating a yagi antenna.

Finally the interference levels were added to the simulator and the scenario was played nine times, for three different types of interference at three different power levels:

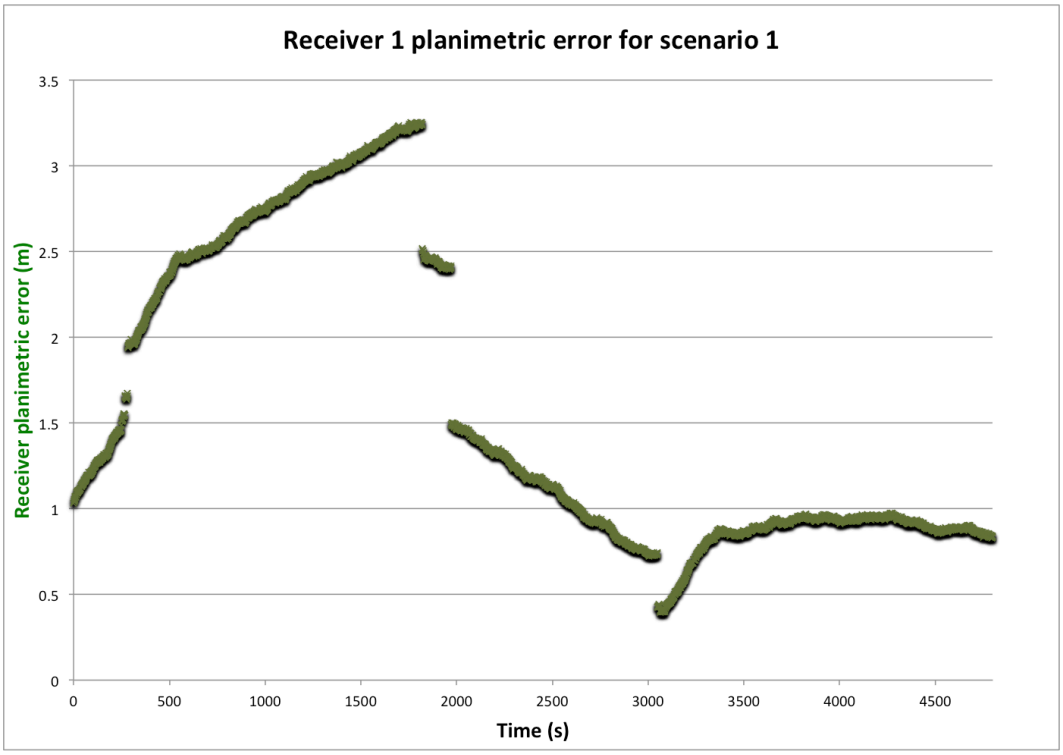
- 23 mW CW jammer signal;
- 640 mW CW jammer signal;
- 25 W CW jammer signal;
- 23 mW 2 MHz broadband jammer signal;
- 640 mW 2 MHz broadband jammer signal;
- 25 W 2 MHz broadband jammer signal;
- 23 mW 20 MHz broadband jammer signal;
- 640 mW 20 MHz broadband jammer signal;
- 25 W 20 MHz broadband jammer signal.



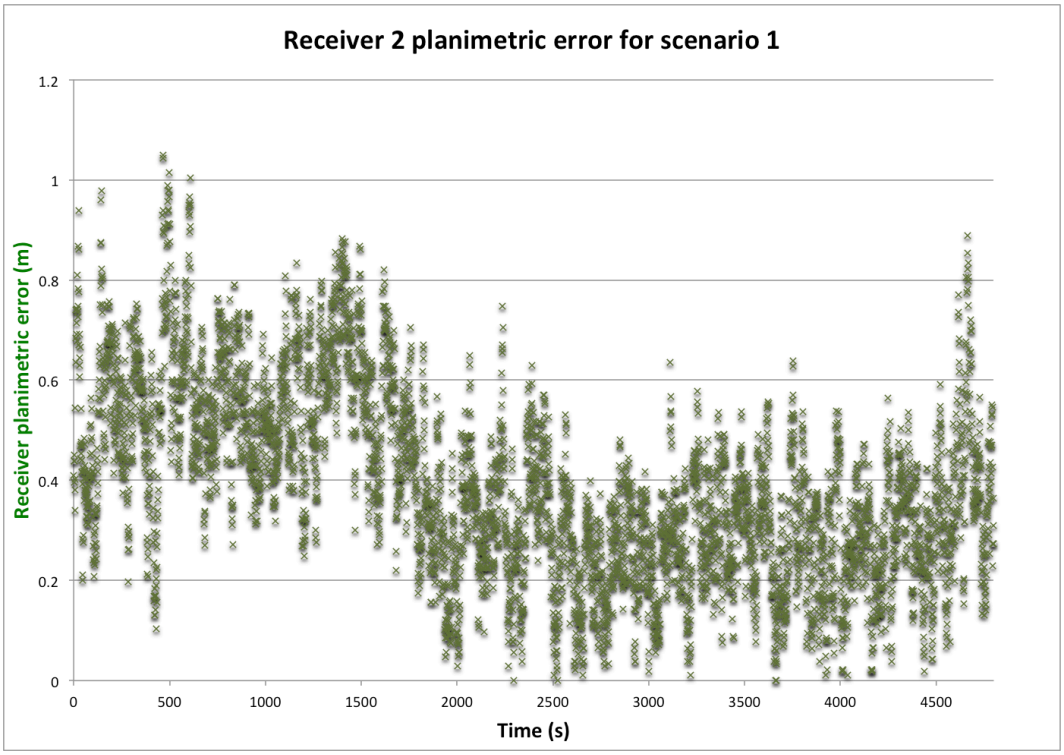
Graphic 4 - Jammer signal power at Rx over time for different PPD powers

5.1.2.3.2. RESULTS

The receivers present different behaviours when outputting position. When there is no interference applied, Rx1 presents more smooth measurements though the errors are higher than Rx2. Rx1, the high-end receiver, shows an error up to 3.5 m, getting below 1 m after 40 min, Rx2, the low-end receiver, goes up 1.2 m and after the same period lowers to 0.8 m. This results were obtained for a specific simulation time, so factors like satellite positions, and consequent DOP, can affect the receivers performance.

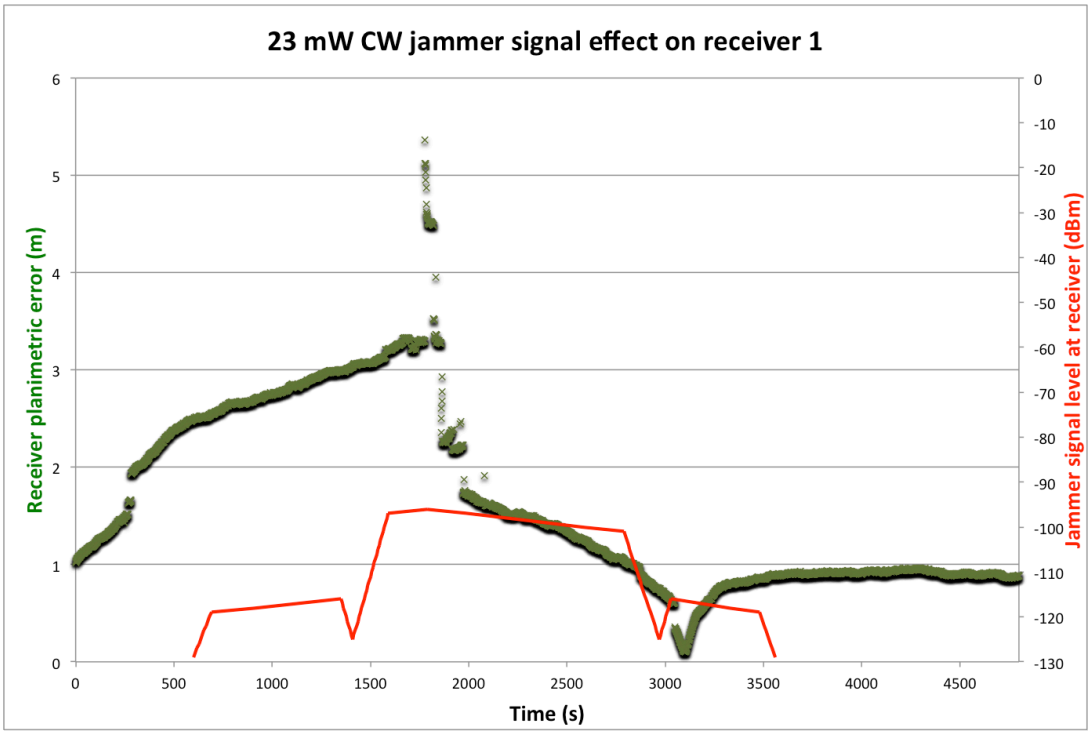


Graphic 5 - Planimetric error of receiver 1 over time when no jamming is applied



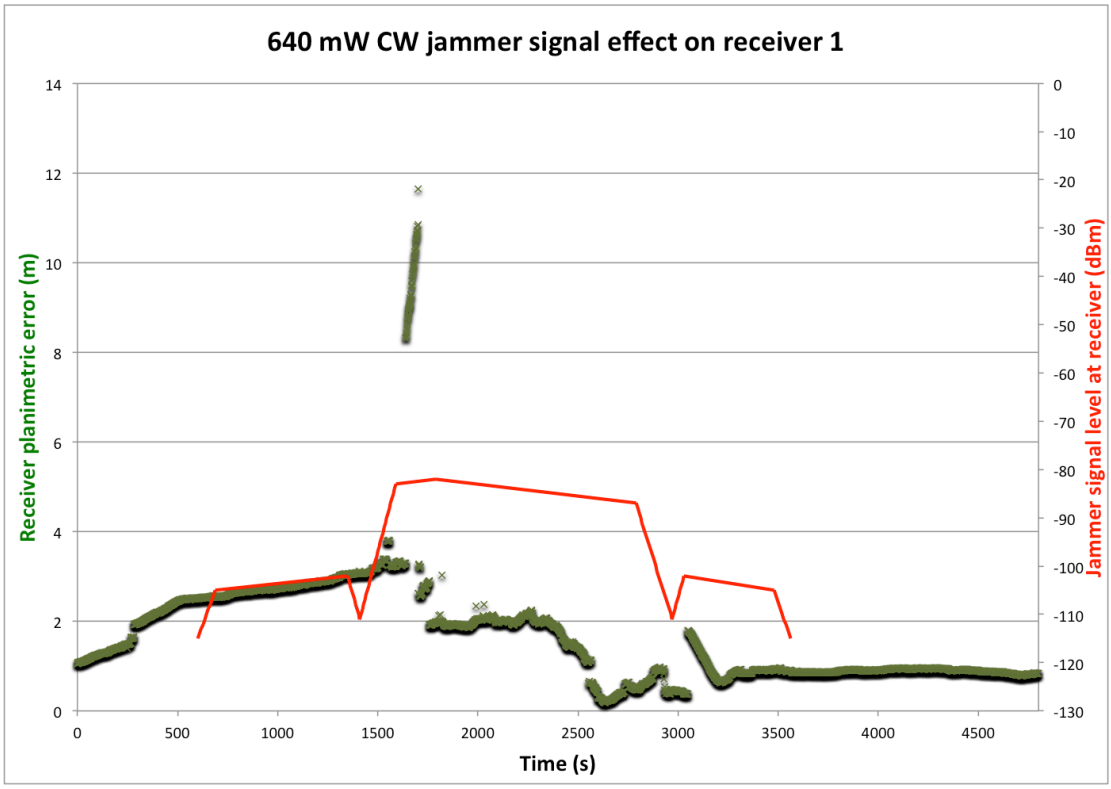
Graphic 6 - Planimetric error of receiver 2 over time when no jamming is applied

Applying 23 mW interference of broadband noise had no effect on the receivers. The CW signal provoked some jumps up to 5 m on Rx1 when the highest point of jamming was reached, approximately -100 dBm. Rx2 is not affected.



Graphic 7 - Planimetric error of receiver 1 over time when 23 mW CW noise is applied

A CW signal of 640 mW had effect on both receivers, especially on Rx1 where the planimetric error increased until 12 m for a few moments when approximately -80 dBm was applied. During the same period, Rx2 grew the error until 2.5 m, not significantly.

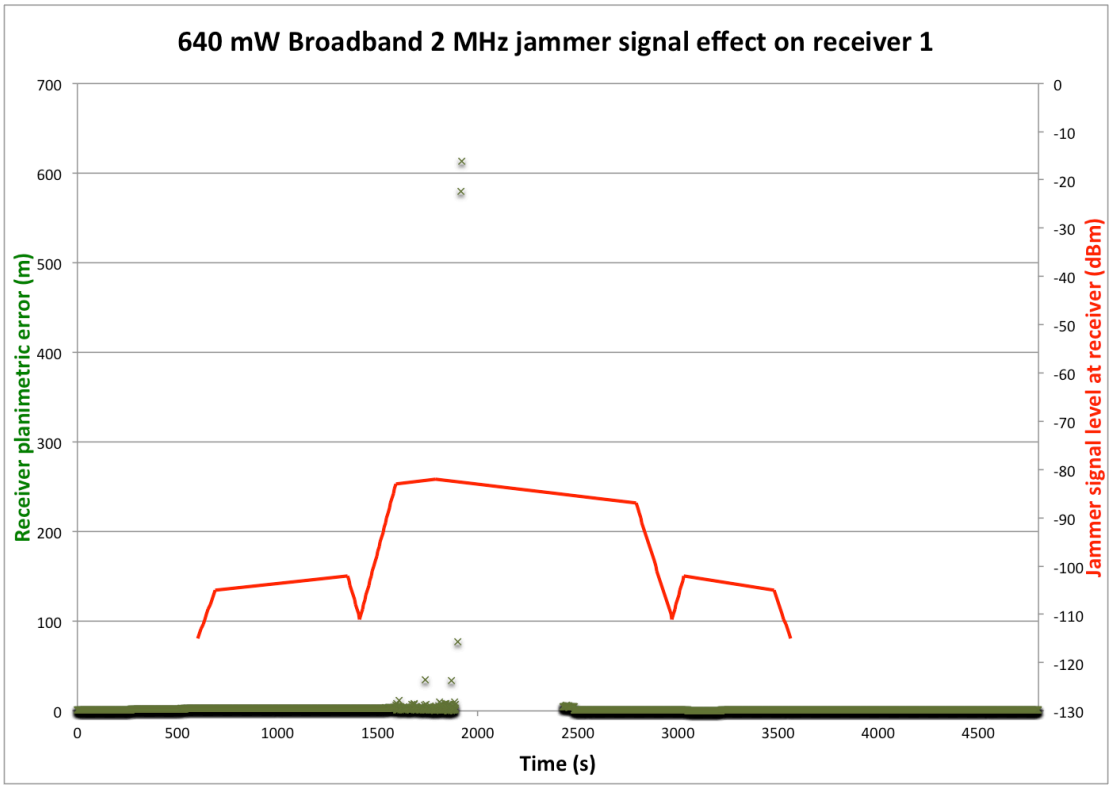


Graphic 8 - Planimetric error of receiver 1 over time when 640 mW CW noise is applied

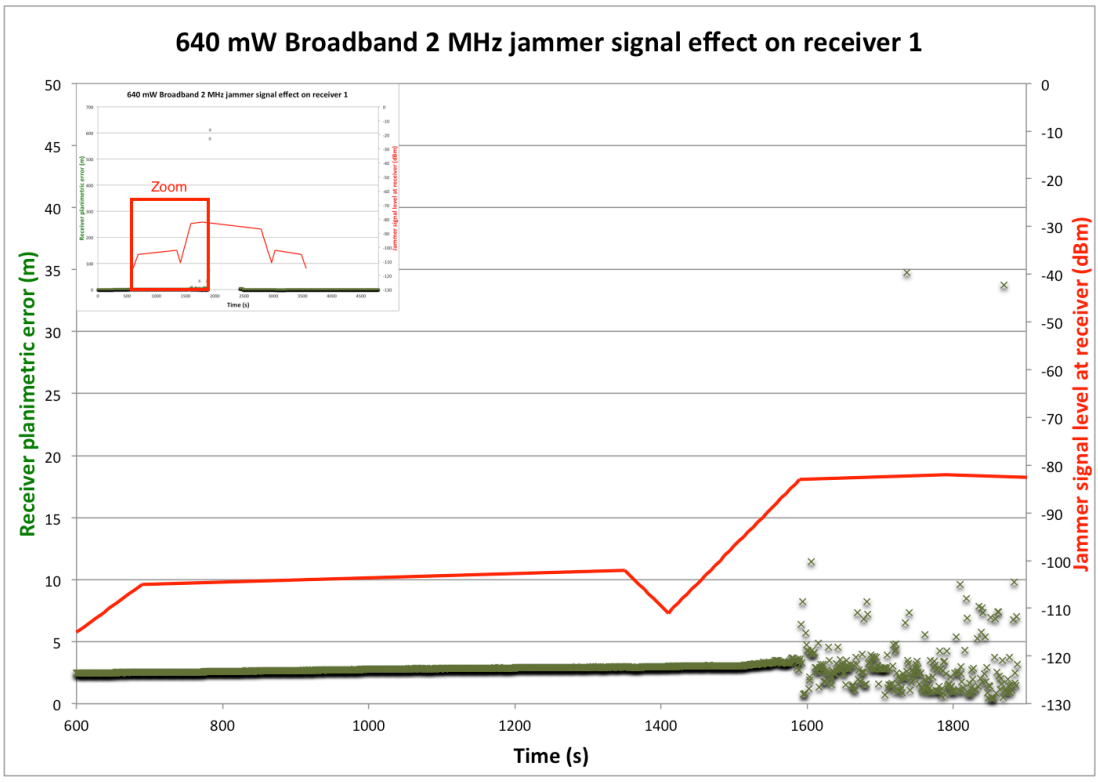
The 2 MHz broadband interference of 640 mW power trial had distinct effect on both receivers.

When Rx1 entered in the main lobe, around -85 dBm, it stopped its smoothness and started behaving randomly, reaching a peak of a dangerous 600 m (HMI) before losing signal. 8 minutes later the receiver got signal again and showed normal behaviour until the end.

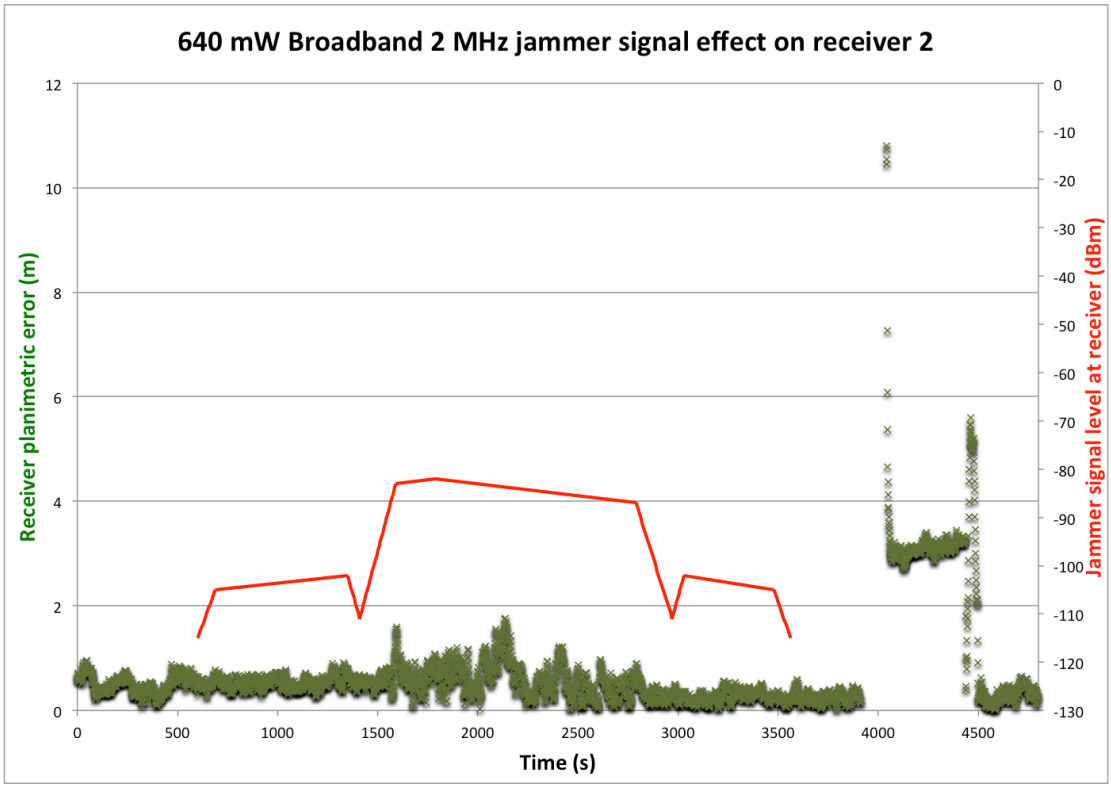
Rx2 seemed affected by the interference during its passage by the main lobe, though the error didn't present significant errors, below 2 m. After the interference ceased, the receiver passed through a period of no signal, followed by 11 m peak error, continuing with 3 m error for more than 10 min with 5 m peak in the end of that period, getting back to normal (less than 1 m) few moments before the end of the scenario. This behaviour may not be directly related to the jamming but an anomaly on the receiver's performance.



Graphic 9 - Planimetric error of receiver 1 over time when 640 mW 2 MHz BB noise is applied



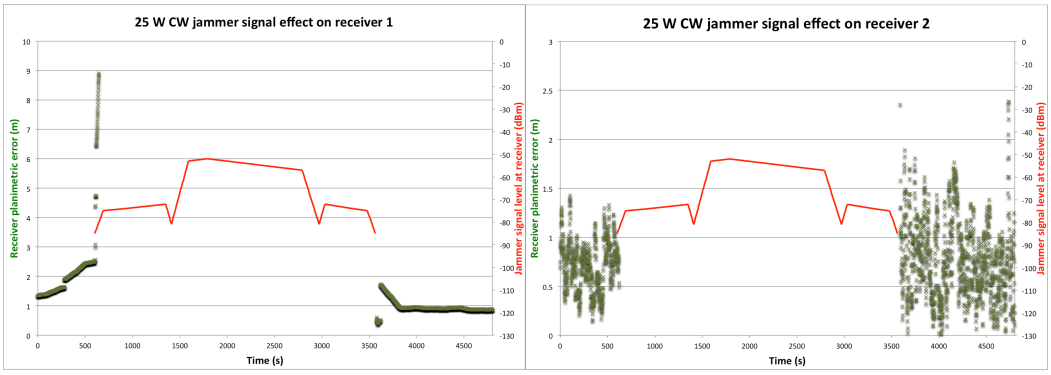
Graphic 10 - Planimetric error of receiver 1 over time when 640 mW 2 MHz BB noise is applied zoomed



Graphic 11 - Planimetric error of receiver 2 over time when 640 mW 2 MHz BB noise is applied

The 20 MHz broadband interference at 640 mW had not effect on the receivers.

A 25 W CW jammer on shore, 6 Km away from a vessel is effective, blocking completely as soon as the receiver enters the interference area of action, at -85 dBm.

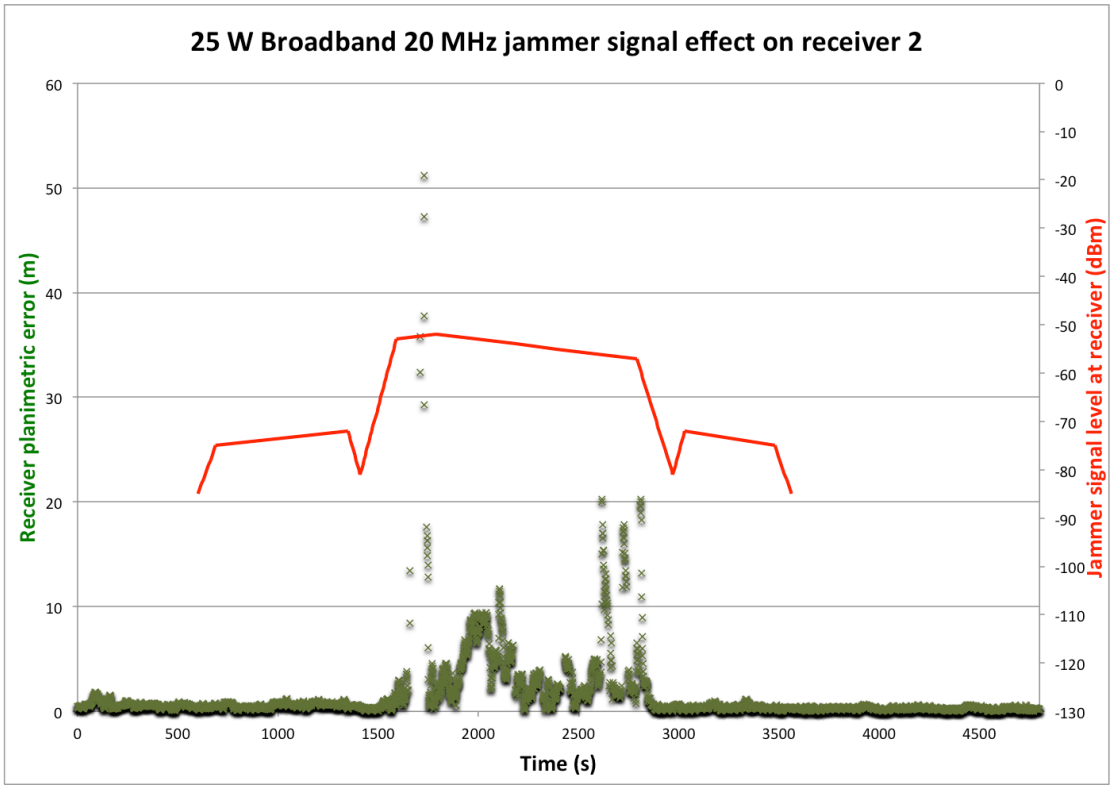


Graphic 12 - Planimetric error of receiver 1 (left) and 2 (right) over time when 25 W CW noise is applied

For Rx1 the 2 MHz broadband signal had almost the same effect as Rx2, complete loss of position as soon it receives jamming.

For the 20 MHz broadband signal, Rx1 took a little more time to lose position, giving errors ranging from 3 to 11 m in the first 5 min of interference. During the lobes there was no position except on the first gap between the side and main lobe with 7 m planimetric error.

In the 2 Mhz noise Rx2 had a similar behaviour to the Rx1 20 Mhz noise, though it recovered position with a big planimetric error (>10 m) in both side lobes. Surprisingly the Rx2 kept position almost all the time during the 20 Mhz broadband interference, with small moments with no position and errors ranging on average from 4 to 10 m, with a maximum of more than 50 m for a few seconds.



Graphic 13 - Planimetric error of receiver 2 over time when 25 W 20 MHz BB noise is applied

On a global analyses it is undoubtable that interference is a threat and can have a very dangerous impact on receivers. Rx1 showed big errors for a high-end receiver. Factory reset was performed before each of the tests, to start from a clean setup. It could not be discarded that the receiver was incorrectly configured, or that the same receiver would have shown a better behaviour with a different firmware. Rx2 affirmed to be very resistant to the types of jamming tested and presented very low errors (< 1 m) in almost every moment of the tests when giving PVT.

A continuous wave is the most effective type of noise signal that can interfere with the equipment even in low power, 23 mW.

A 25 W jammer can be assembled from equipment readily available in the internet or in many electronic laboratories or universities, and if enabled on shore, it can affect boats in a radius of 6 Km, or even more, which can have critical security impacts. In these trials errors of 50 m up to 600 m were obtained, which make the receivers quite vulnerable since it can be better not to have PVT and sound an alarm rather than giving HMI.

5.1.2.4. SCENARIO 2

On the second scenario a set of jammers inside a vessel, as it approaches Newcastle upon Tyne, United Kingdom (approximately N 55.0090º W 1.4450 º) was simulated. The vessel starts its movement passing by a zone with no interference time in order to acquire full navigation message from satellites. After that period and during its path the vessel encounters six types of jamming power, simulating different PPD powers and distances to a GNSS antenna. The ship movement lasts around 120 minutes during a 28 nautical miles path (52 Km), ending in a harbour. The jammer would be placed bellow the GNSS antenna, resulting in a 10 dB attenuation on the received signal.

5.1.2.4.1. SETUP

The track file for this scenario was slightly more challenging than the first one since it shows a turn on the vessel path. Start, middle and end points were given as reference:

	Time	Latitude	Longitude	Height
Start Point	0 min	N 55.30º	W 1.20º	0 m
Middle Point	50 min	N 55.10º	W 1.00º	0 m
End Point	120 min	N 55.01º	W 1.43º	0 m

Table 2 – Track 2 reference points

In Google Earth the path was drew and converted to a shapefile using Quantum GIS. Consequently the shapefile was converted from WGS84 (EPSG:

4326) to Ordnance Survey Great Britain's Grid (EPSG: 27700) in order to have measurements in meters, and consequently the perimeter of the path was calculated. With these values it was possible to calculate the velocity of the ship and how many meters the ship moves per second. Using GRASS' v.to.points (http://grass.osgeo.org/) function was possible to split the projected shapefile into points one second apart from each other. The coordinates were extracted from those points and converted again to WGS84, using PROJ4 (http://trac.osgeo.org/proj/). With the final coordinates it was then possible to calculate headings and finally create the fake NMEA file, convert it to *.umt file and import it to the simulator.

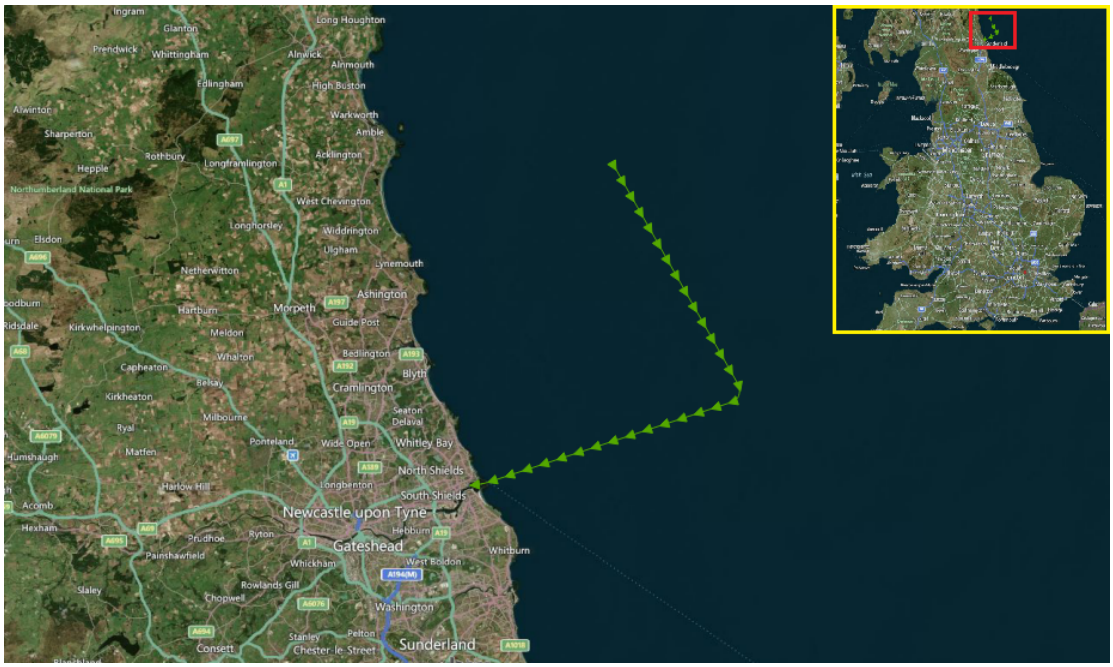


Figure 23 – Scenario 2 location

In these trials four different jamming powers (0.001 mW, 0.01 mW, 0.1 mW and 1 mW) at three different distances from PPD to antenna (5, 15 and 30 m) were tested. Using equation 1 is possible to calculate the power ratio for each power:

0.001 mW = -30 dBm | 0.01 mW = -20 dBm | 0.1 mW = -10 dBm | 1 mW = 0 dBm

The FSPL values (equation 2) are:

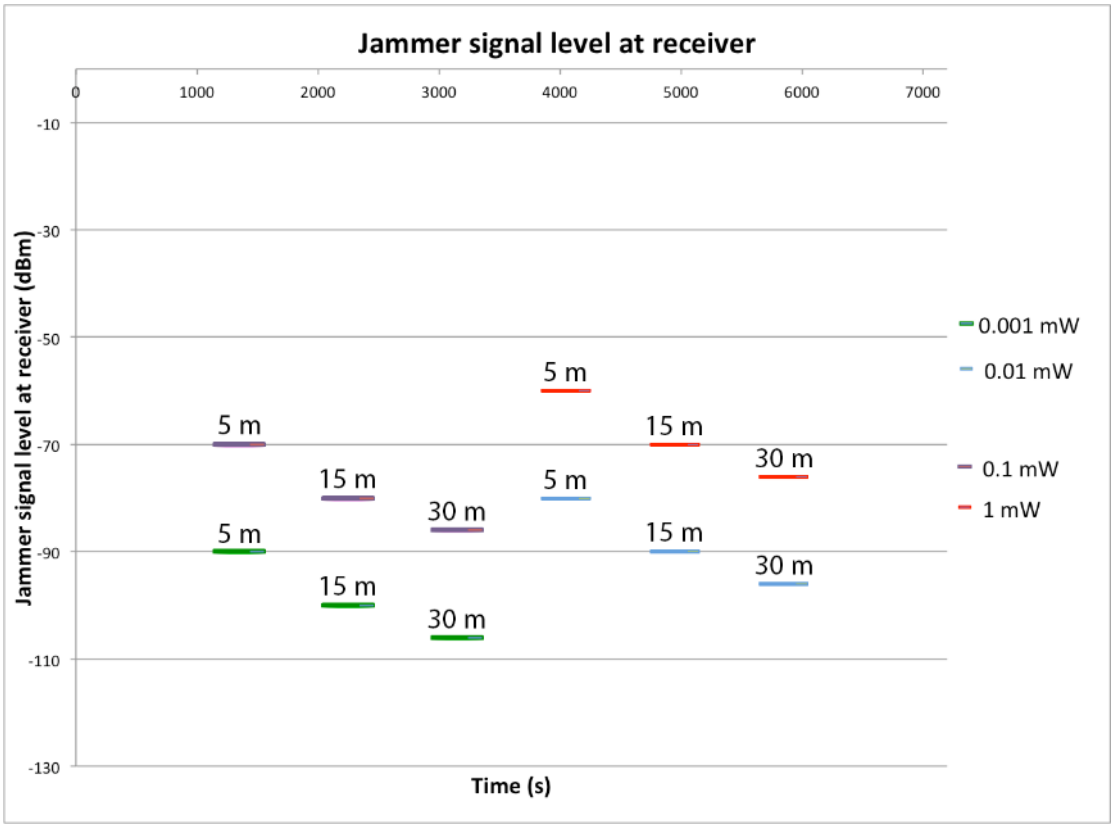
5 m = 50 dB | 15 m = 60 dB | 30 m = 66 dB

Consequently the jamming power at receiver is calculated using equation 3, adding 10 dB for the antenna attenuation, resulting in:

	5 m	15 m	30 m
0.001 mW	-90 dBm	-100 dBm	-106 dBm
0.01 mW	-80 dBm	-90 dBm	-96 dBm
0.1 mW	-70 dBm	-80 dBm	-86 dBm
1 mW	-60 dBm	-70 dBm	-76 dBm

Table 3 - Signal level at receiver for different jammer power at different distances

Jamming powers were applied to the track according to the following graphic:



Graphic 14 - Jammer signal power at Rx over time for different PPD powers and distances

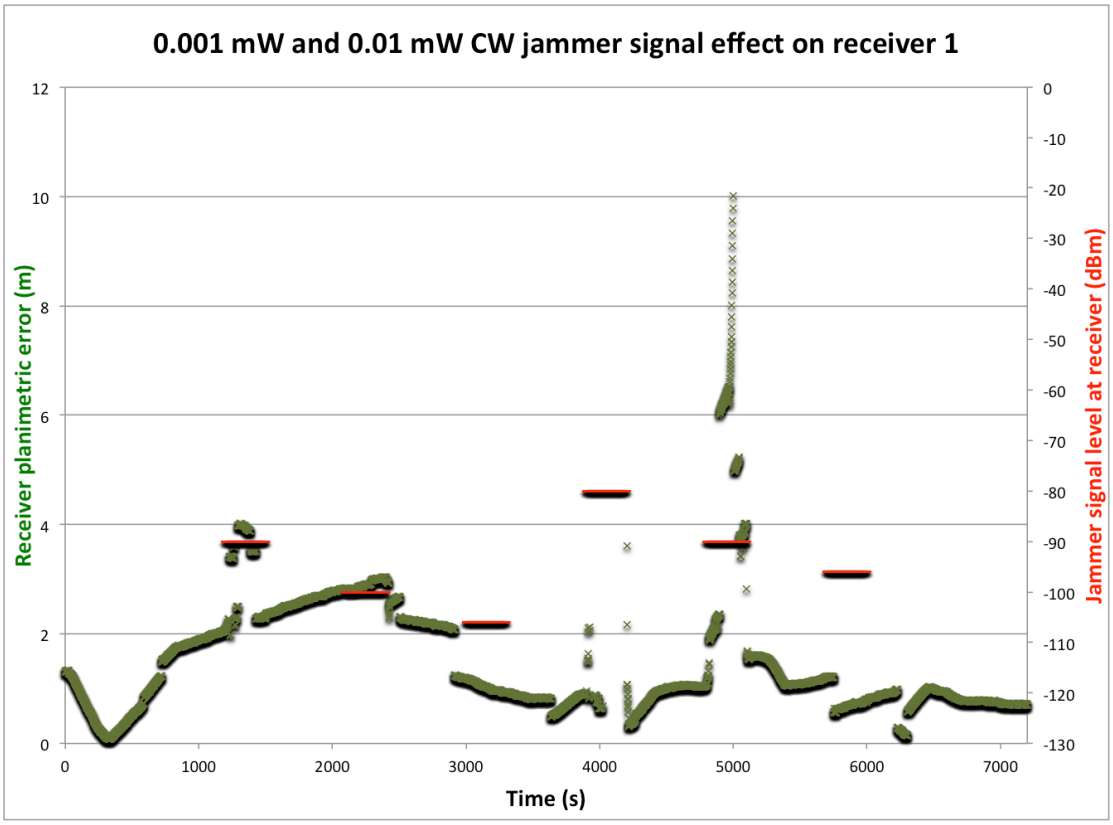
Jamming periods of 0.001 mW were combined in the same track with 0.01 mW, and similarly, 0.1 mW with 1 mW, at the times stated in the graph.

The interference levels were uploaded to the simulator and the scenario was played 6 times, using:

- 0.001 mW CW jammer signal at 5, 15 and 30 m followed by 0.01 mW CW signal at 5, 15 and 30m;
- 0.1 mW CW jammer signal at 5, 15 and 30 m followed by 1 mW CW signal at 5, 15 and 30m;
- 0.001 mW 2 MHz broadband jammer signal at 5, 15 and 30 m followed by 0.01 mW 2 MHz broadband signal at 5, 15 and 30m;
- 0.1 mW 2 MHz broadband jammer signal at 5, 15 and 30 m followed by 1 mW 2 MHz broadband signal at 5, 15 and 30m;
- 0.001 mW 20 MHz broadband jammer signal at 5, 15 and 30 m followed by 0.01 mW 20 MHz broadband signal at 5, 15 and 30m;
- 0.1 mW 20 MHz broadband jammer signal at 5, 15 and 30 m followed by 1 mW 20 MHz broadband signal at 5, 15 and 30m;

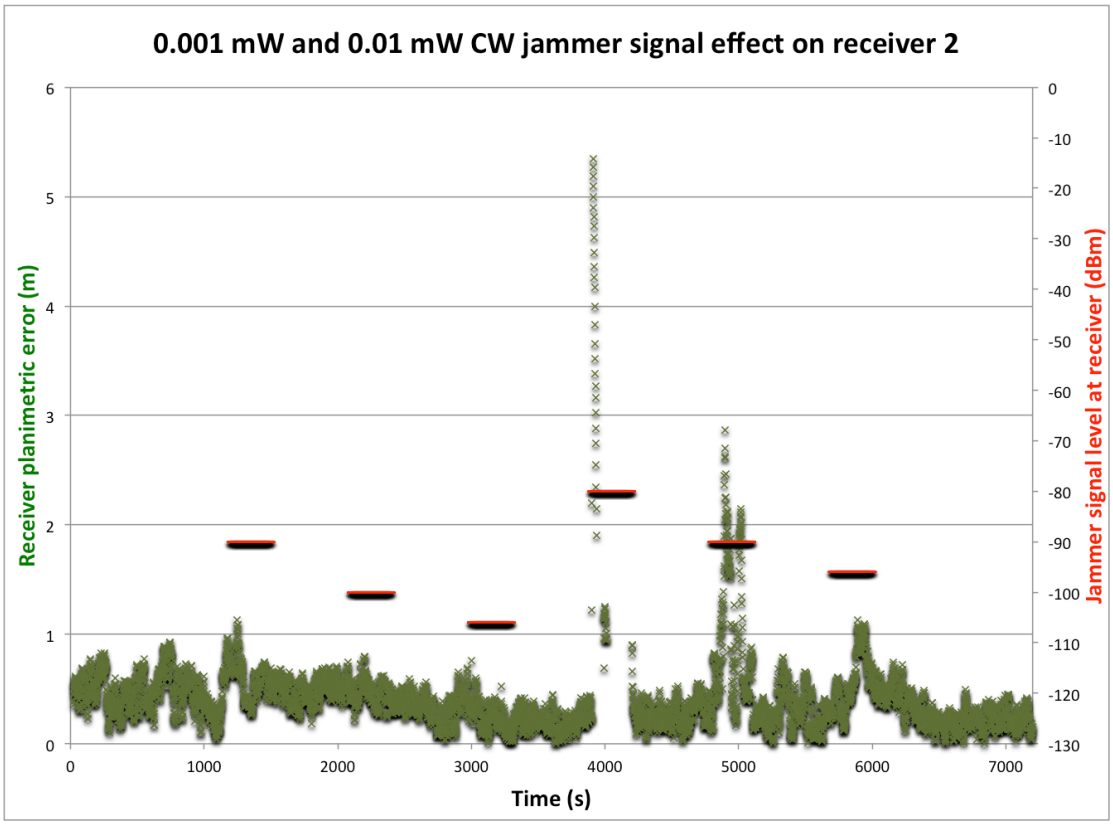
5.1.2.4.2. RESULTS

As in the previous scenario, CW noise is more effective than broadband one. Rx1 is affected even by the weakest power signal 0.001 mW at 5 m away from the interference source, at -90 dBm. The 0.01 mW jammer makes the receiver cease PVT output at 5 m (-80 dBm), and gives some considerable errors (6-10 m) when located 15 m away.



Graphic 15 - Planimetric error of receiver 1 over time when 0.001 mW at (5, 15 and 30 m) and 0.01 mW at (5, 15 and 30 m) CW noise is applied

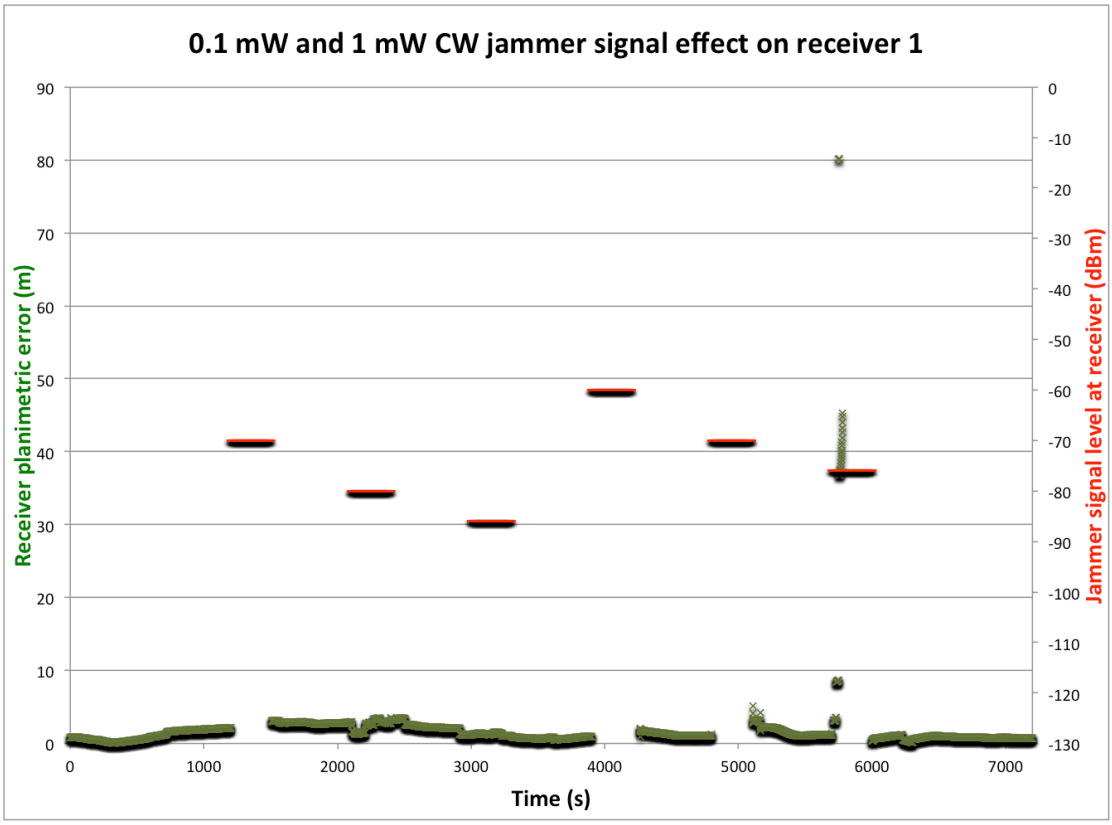
Rx2 also lost PVT at the same signal power as Rx1, still being affected at -90 dBm, giving positions with more planimetric error than in normal conditions. A 0.001 mW PPD seems to have no effect on receiver 2.



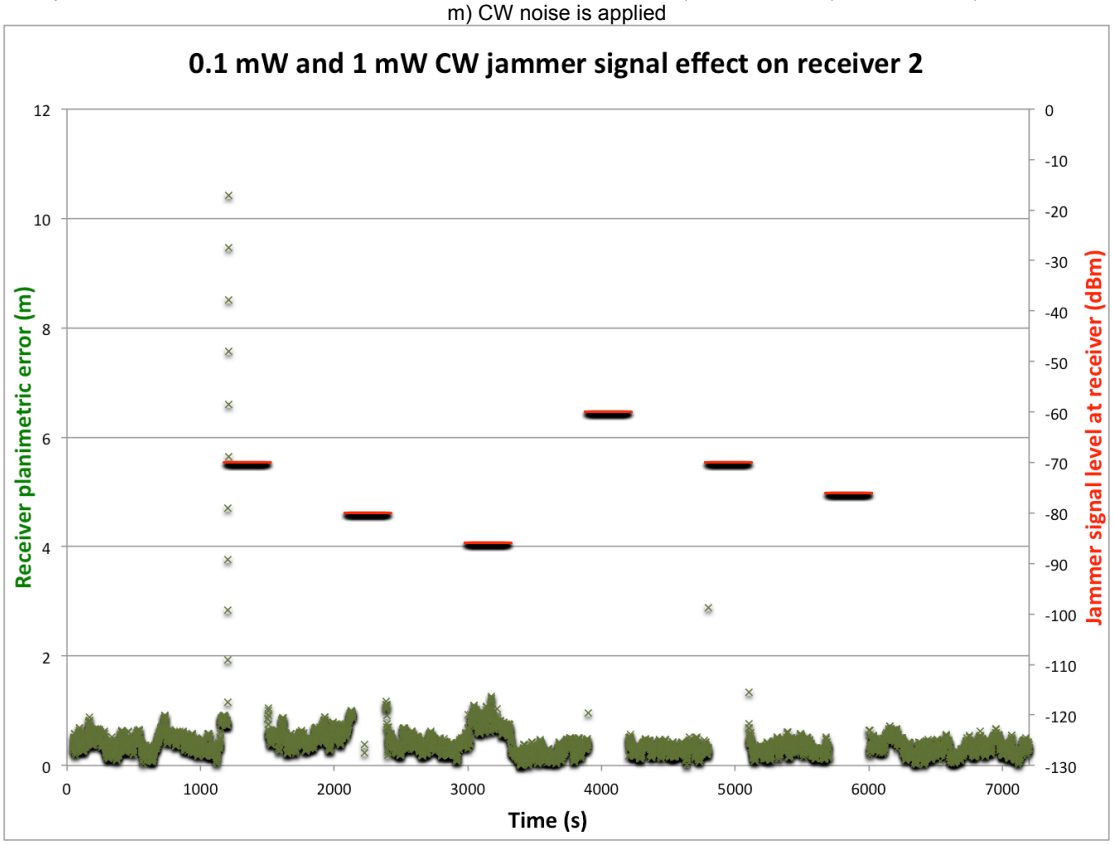
Graphic 16 - Planimetric error of receiver 2 over time when 0.001 mW at (5, 15 and 30 m) and 0.01 mW at (5, 15 and 30 m) CW noise is applied

The 0.1 mW jammer had effect at 5 m, though distances of 15 m and 30 m had small impact on Rx1.

Rx1 and Rx2 had similar impact by a 1 mW jammer at 5 m, 15 m and 30 m, no PVT at all. Although, Rx1 suffered a period of high HMI from 40 to 80 m. Is then possible to affirm that between -80 dBm to -70 dBm both receivers drop positioning for a CW type jammer.



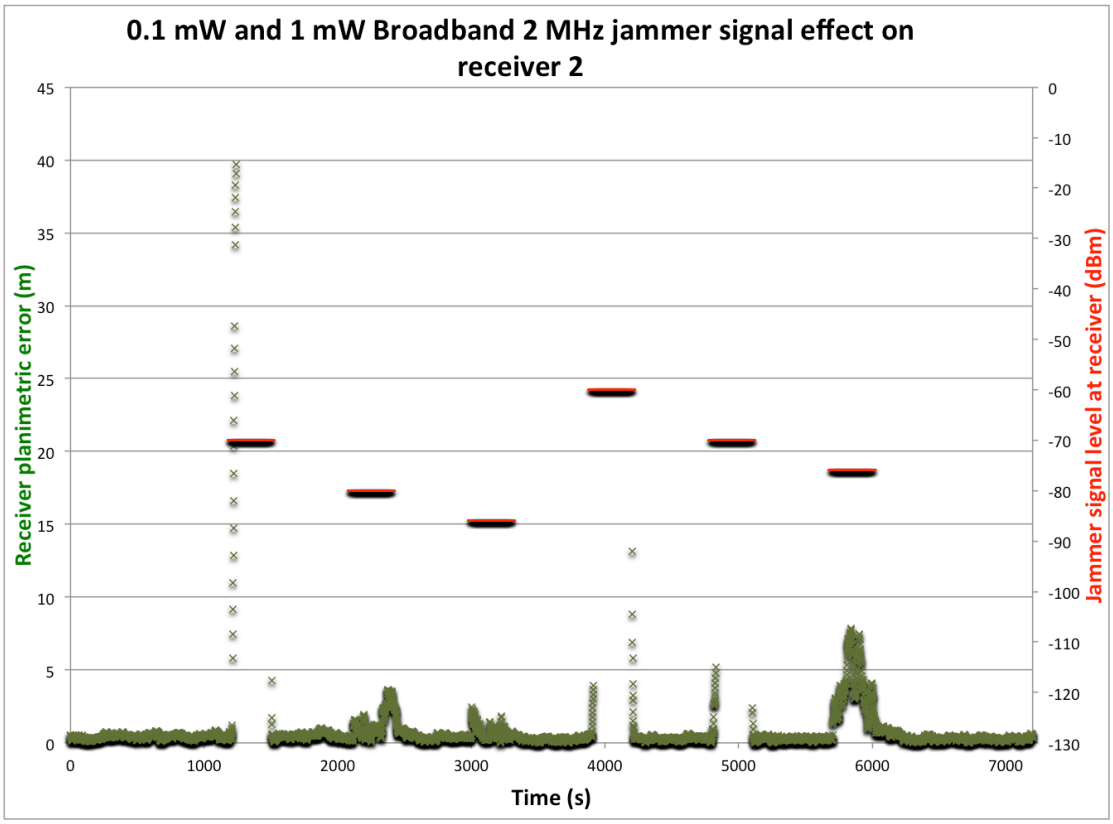
Graphic 17 - Planimetric error of receiver 1 over time when 0.1 mW at (5, 15 and 30 m) and 1 mW at (5, 15 and 30 m) CW noise is applied



Graphic 18 - Planimetric error of receiver 2 over time when 0.1 mW at (5, 15 and 30 m) and 1 mW at (5, 15 and 30 m) CW noise is applied

0.001 mW and 0.01 mW PPD transmitting 2 MHz broadband noise had similar effect on both receivers, only showing change of performance at -80 dBm, with Rx1 loosing PVT and Rx2 outputting erroneous position reaching 3 m during the interference interval.

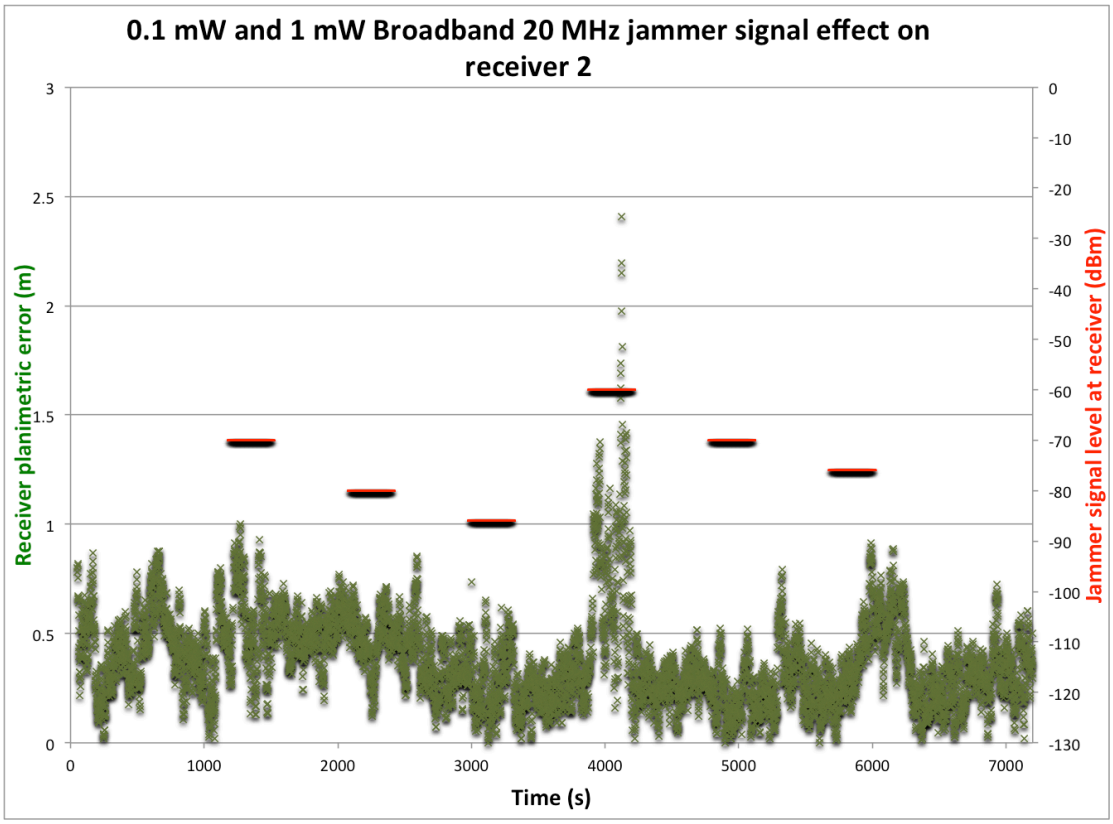
0.1 mW and 1 mW with 2 MHz broadband PPD had impact on both receivers as long as the power at the receiver was above -80 dBm, resulting in loss of PVT. Rx2 gave HMI up to 40 m for a few seconds as soon the 0.1 mW at 5 m jammer started emitting. It also gave PVT with errors from 2.5 to 7.5 m during the 1 mW jammer at 30 m (-80 dBm), contrary to Rx1 who lost PVT at all.



Graphic 19 -Planimetric error of receiver 2 over time when 0.1 mW at (5, 15 and 30 m) and 1 mW at (5, 15 and 30 m) 2 MHz BB noise is applied

0.001 mW and 0.01 mW with 20 MHz noise didn't have any impact on receivers at any distance.

Rx1 lost position with a 0.1 mW and 1 mW 20 MHz broadband noise when the power level was above -70 dBm. The effect on receiver 2 of this type of jamming was almost null, just some minor errors bellow 2.5 m.



Graphic 20 - Planimetric error of receiver 2 over time when 0.1 mW at (5, 15 and 30 m) and 1 mW at (5, 15 and 30 m) 20 MHz BB noise is applied

These trials were quite important since they simulated signal powers of cheap PPD's proving how effective they can be at short range. Both receivers seem to be affected and not outputting position at around -75 dBm with CW noise, making it possible to calculate the jammer action radius (with perfect propagation conditions) from PPD's with different powers using the equations used in the topic 6.1.2.3.2.:

- 1 mW = ~85 m
- 10 mW = ~270 m
- 50 mW = ~600 m
- 100 mW - ~850 m
- 250 mW - ~1350 m

5.2. SPOOFING

5.2.1. TRIALS

Spoofing tests were performed though the support was aimed on visualization capabilities. Moreover, the objective of these initial tests was not to scientifically explain and quantify spoofing but only create videos to show that spoofing can be done and is a real threat.

Spoofing tests were successful in every SAC receiver, each one showing different behaviour and resistance to spoofing, but in the end they were all spoofed.

5.2.2. EQUIPMENT

The equipment used in these tests is similar to the jamming ones, except that an external GNSS antenna plugs into the system according to the following scheme:

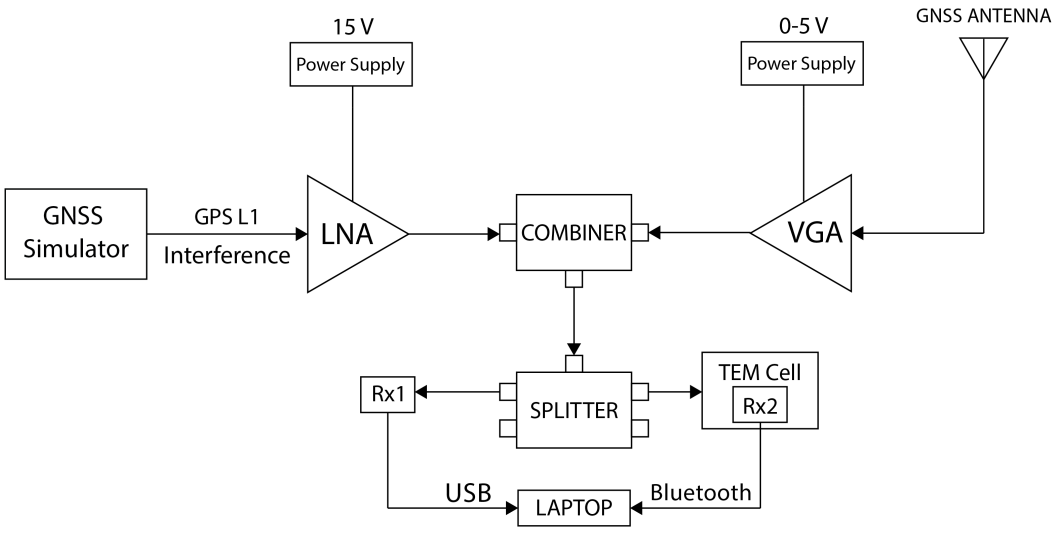


Figure 24 - Spoofing trials equipment scheme

5.2.3. SETUP

In a first phase C/N ratios at the receivers where measured independently, the ones that came from the simulator and the ones from the antenna. Since the ratios from the antenna were much higher compared to the simulator, the VGA was connected to the antenna to attenuate the real signal and approximate both ratios, as otherwise the spoofing demonstration wouldn't be possible since the receiver will always track the strongest signal.

Simulator scenario was created and the settings were quite simple: 6 minutes of static position on the antenna coordinates where the last 3 minutes were accompanied with high power jamming. After that period, movement starts in east direction at slow speed (10 Km/h) for 4 min, stopping a few Km away from SAC building. The simulator needs to be uploaded with the latest almanac to match the real-world conditions from the antenna. The simulation also needs to be approximately (less than 1 s difference) at the same time as the actual time: if not the receivers would detect a jump in time and reject the simulated signals.

The simulated scenario starts with the LNA disconnected, allowing the receiver to only acquire real signal for 3 minutes. After this, the LNA is powered, the circuit is jammed and the receiver loses position lock. After the jamming period, the receiver locks into the simulated signal after a few moments and starts wrongly moving.

5.2.4. RESULTS

Connecting the receiver to ArcGIS (http://www.esri.com/software/arcgis) made possible the live visualization of the output of the receiver and affirm that it has been spoofed since it has moved away from the SAC premises. Depending on the receiver, the tracking of the fake signal could take longer, from 30 seconds until a few minutes. If the simulation was stopped the receiver would lock immediately to the real signal and plot its position on top of the SAC building, where the GNSS antenna is.

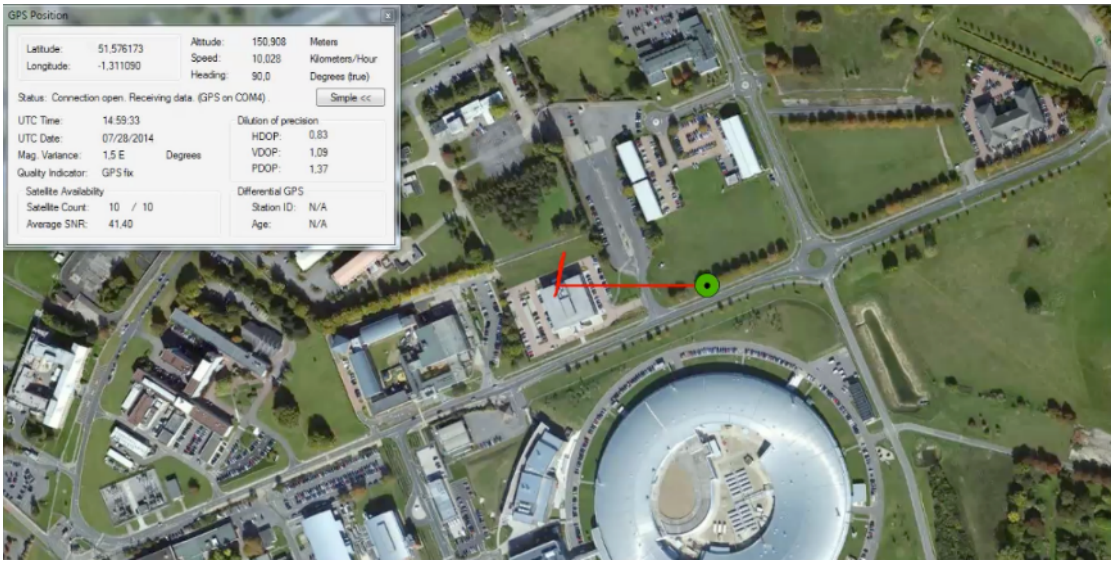


Figure 25 - GNSS receiver outputting position with spoofed signal

The same trials were done with an Android smartphone and spoofing was also a success, taking less than 10 seconds to lock on to the fake signal once the jamming had finished.

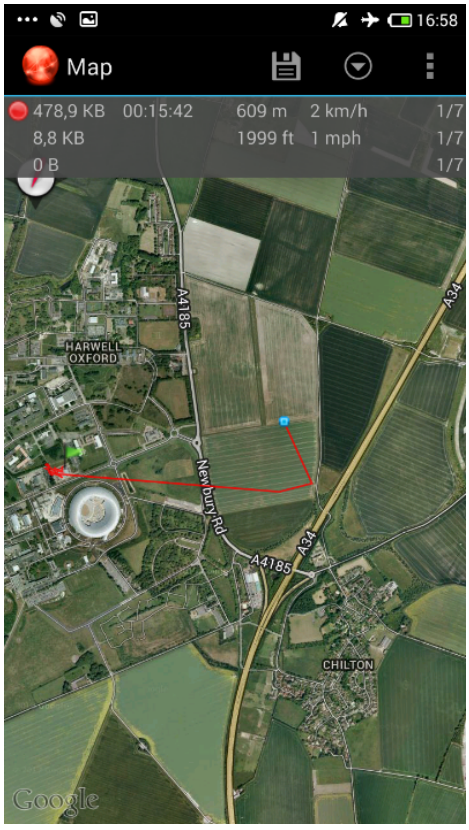


Figure 26 - Android smartphone outputting position with spoofed signal

These trials represent a great success on achieving spoofing in lab environment, though spoofing in real world conditions require other methodologies. In a live situation is not possible to attenuate the signal that is received in an independent antenna, so the output power from the fake signal needs to be very strong to overtake the real one. Even though these tests were performed, SAC is not developing spoofing mechanisms, they were only made for research purposes.

CHAPTER VI

ROBUST GNSS

6. ROBUST GNSS

As seen in the previous chapter, GNSS have a series of vulnerabilities that can impact negatively equipment that rely on the system. Even if most of them aren't a common threat, deliberate interference is for sure an enemy to every application. Some of the next solutions can help on mitigating the effects of jamming or spoofing, though some of them can also be, and certainly will as piracy evolves, a target for future and more developed jammers.

In a best case scenario, receivers and antennas should have the latest defence mechanisms, identifying jamming or spoofing and avoiding it, distinguishing the real from the fake signals. Even though a lot of research has been focusing on this problem, there is no completely effective solution yet. It's necessary to create jamming detector sensors network and analyse the signals and its effects. SAC is currently working on this, in order to provide this information to receiver manufactures so they can better understand the threat and make their equipment more robust. Combining sensors, new technologies and new systems, can be a solution to use as backup plan in case of GNSS failure, providing efficient solutions while the outage happens.

6.1. MULTI-FREQUENCY

Multi-frequency receivers give more accurate PVT, since they correct ionospheric delays, giving precision inferior to 1 m rather than a few ones. However, that's not the only advantage. With the expansion of open services in more than just one band on almost every constellation, if one band gets jammed, positioning would still be possible using another one.

Nowadays, GPS L1 and GLONASS L1 are the most used bands and jammers, especially the cheap ones, tend to focus power on them, denying completely GNSS service. When new bands are open, even if a jammer focus on L1 they won't have such negative impact as before. Unfortunately this solution is not 100 % effective, since new jammers can cover all other GNSS bands at the same time.

Spoofing gets also more challenging, since fake signals need to be transmitted in more bands at the exactly same time. If a fake signal is only emitted in one band, a

smart receiver can compare both bands and detect something is mistaken, denying the spoofed signal.

6.2. MULTI-CONSTELLATION

Each GNSS should be able to provide efficient PVT in a standalone mode using their own bands and respective signals. When combined with other constellations the final solution can get significantly better, rising the number of visible satellites, useful in low visibility areas, like forests or urban-canyons.

Since every constellation has its own independence, jamming a certain system won't influence another one, so, a receiver can keep its normal functioning. This feature is also useful in case of a system failure, assuring that PVT will still be provided with the efficiency of the system that its connect to.

Spoofing in these circumstances can be almost impossible, unless all bands for all constellations are spoofed, but it's extremely technical demanding. For example, if GPS is spoofed giving fake location, a receiver connected also do GLONASS can see that something is wrong since the positions obtained from the different systems are different and eliminate the error source.

6.3. ENCRYPTED SERVICES

GPS and GLONASS are primarily military systems created to enhance USA and Russian's army, respectively. Even though they provide open services, high accuracy ones are reserved for military purposes or very specific applications requiring authentication and special receivers.

Galileo system will offer services that need authentication and higher precision than the OS: PRS and CS. CS will be available to anyone who wants to use the service, paying a subscription fee. PRS will be used for government authorities that require special levels of security and availability, like police and other blue-light teams, coast-guards, customs, etc. To access the service, receivers adapted for that purpose need to be used and since the signal is encrypted, spoofing is not a threat to them.

'We've heard about the capacity of PRS to improve resilience in the civil environment. But the thread of course is evolving all the time – it's not just about the jamming any more – spoofing is the new game in town'

by Dr. Chaz Dixon in Navigationews Magazine (May/June 2014)

Using authentication services is a great advantage against spoofing however they are still vulnerable to jamming since this services sits on normal GNSS bands.

6.4. eLORAN

eLoran system has been, in the last few years, considered a system that can substitute GNSS in many non-demanding applications. A lot of discussion happened around this topic, though the best solutions is probably combine the best of both systems and provide a high robust solution.

Enhanced Loran is the newest technology on LOng-RANge navigation (LORAN), with the same principles as GNSS, though instead of satellites it has ground signal transmission stations that emit shaped radio signals at 100 kHz. Recent studies and trials achieved 5 meter-accuracy, enough for a lot of applications. Since the stations are ground-based the maintenance of the equipment is much cheaper than GNSS, but lacks one big thing: global coverage is not guaranteed since a lot of stations need to be placed on Earth, so it may just be useful in specific areas where maybe GNSS signals can be blocked. (Elorantechnologies.com, 2014)

Using eLoran as a stand-alone technology is not the perfect option, but in applications where availability is a need, a combine GNSS + eLoran receiver can be a solution in case of failure of one of them, since it would keep a PVT. As an independent solution to substitute GNSS is not viable and spoofing or jamming are also a threat to eLoran since they still transmit known radio signals, but at different frequencies.

6.5. IMU

Inertial Measurements Units (IMU) are electronic devices that measure and report angular velocities and linear accelerations, giving position information. If combined with a GNSS unit, it can be a solid and robust solution.

In a joined unit, GNSS provides position details and the IMU uses those coordinates to estimate the next positions using the parameters they measure with great precision. If worked independently an IMU can accumulate big errors after a certain period, it is then really necessary to synchronize the position with GNSS regularly. So, if GNSS service stops temporarily and for a short period, an IMU can still give precise positioning.

Since an IMU doesn't use any radio frequency it's robust against jamming or spoofing.

FINAL CONSIDERATIONS

Global navigation satellites systems are part of an exciting world, never stopping and always with new technologies coming up to improve the quality of the system. A general knowledge of the constellations available was learnt during academic formation, but working with them, knowing their particularities like orbits, signals and even history was a great asset. Even the previous contact with Galileo was quite sparse, however this has changed since it rouse interest about the future of this system and will to accompany the developments of it, defending its importance as a European citizen.

The implementation of the GNSS technologies in the United Kingdom is impressive, using them in a wide range of different applications, acknowledging the benefits they brought to UK and can bring to PT. With so many areas of implementation, especially in vital ones, GNSS seems to be the perfect system without any vulnerability. Is a wonderful system, indeed, but can be impacted easily by outside agents, especially deliberate interference. The lack of knowledge and complete trust in the system becomes then a scary scenario since the common user may not prepared for any outage. Is necessary to create backup plans and analyse the risks when adopting GNSS solutions.

It was impressive to see how famous jammers are becoming in the UK, and if they ever come to be a problem I now understand how they work and what they can achieve. PPD's can be easily brought in the Internet and it was very important to simulate the effects they can have on receivers, even at so low power like 1 mW. Even though it's illegal to use jammers, authorities are not prepared to lead with the issue due to lack of information and awareness. Spoofing was completely an unknown and consequently an interesting theme of research: the possibility of remotely controlling a GNSS enabled machine is exciting but at the same time quite dangerous. Jamming and spoofing are gaining their space and any new technology is welcome to overtake the effects they can have.

More lab trials should be performed evaluating the impact of jammer in different scenarios. The simulator is highly customizable and can simulate areas of tight sky visibility or active high levels of multipath. To validate the work, trials in real world conditions should be also done, since jammer signal propagation can vary significantly. The results obtained represent the behaviour of two receivers and

others can have a completely different comportment, so a battery of tests should be planned in order to always test the same scenarios to every receiver.

After understanding GNSS limitations, is expected that the system can give and keep the trust of the users. If something wrong happens to satellites, or even in receiver level, the system needs to keep integrity, distinguish what is bad or good information and raising alarms when needed, because sometimes is better lack of position than hazardous misleading information. GNSS also need to keep availability at any point, anywhere. One important factor is the interoperability between systems, and for example GPS and Galileo seek partnerships to deliver the best solution to users. Moreover, GNSS bands are quite close to each other and new ones are coming, so compatibility is more important than ever, assuring that signals from determined navigation system don't affect the proper use of others. To finish is important to identify and know technologies that can keep and improve the quality of the service even when a vulnerability is presented, ensuring robustness and resilience.

This internship allowed a great contact with the GNSS world in very different topics, in a fantastic working environment that permitted to be with people with a lot of expertise, sharing new perspectives and own ideas. The scope of this report is not close to the actual knowledge acquired during the 6 months period. Using GNSS receivers, simulators, RF recorders and players, dealing with different cables and connections, different receivers' software, etc is something that was not done during academic formation and was exciting to learn at this level, though previous knowledge and preparation is recommended.

Experiences abroad, in a different country, with another language is challenging but at the same time very enriching. As a final personal consideration I believe I came a different person, with new life and work perspectives, feeling that I did my best to absorb all the knowledge I could possibly take from SAC employees. It also improved my responsibility, assiduity, punctuality, team work and confidence, hoping that I left SAC better than I found it.

CONTRIBUTE TO THE COMPANY

All the work performed seek quality and innovation, never denying a challenge and an opportunity to learn, hoping that signs of competence, availability and friendship were left on the team's members.

The contribute to Satellite Applications Catapult, especially to PNT team, focus on the setup and integration of the PNT Lab, making it available and functional to SAC customers. This includes, in first place, making a presentable and nice environment to work in. All equipment was tested evaluating their capabilities, advantages and disadvantages, and in certain cases tutorials were made in order to others know how to use them properly. It also includes a full inventory of the assets, tagging also the most valuable items.

Some videos regarding team's projects and areas of action were done: GNSS overview, jamming and spoofing; that can be used in conferences and meetings. GIS capabilities were also left, like a concept platform for Performance Quantification Network (PQN) network, a jamming detection network, using Ordnance Survey maps and services.

The jamming trials were a great opportunity to evaluate the capabilities and test the GNSS simulator, learning how to create tracks, interference level files and antenna patterns files, and use the simulation platform.

The support to other teams was also important, providing GNSS testing capabilities to SAC members that lack that knowledge, permitting their projects to be developed.

Finally, SAC received one of 50 certificates to certify that a Galileo fix was obtained, doing all the lab work, from configuring receiver, planning observation times and analysing data.

BIBLIOGRAPHY

[i] Sullivan, M. (2014). A brief history of GPS. [online] TechHive. Available at: http://www.techhive.com/article/2000276/a-brief-history-of-gps.html [Accessed 31 Oct. 2014];

[ii] Gps.gov, (2014). GPS.gov: New Civil Signals. [online] Available at: http://www.gps.gov/systems/gps/modernization/civilsignals/ [Accessed 29 Oct. 2014];

[iii] Kaplan, E.D., Hegarty, C.J.; Understanding GPS – Principles and Applications, Artech House, Norwoord CA, USA, 2006, pages 113-151;

[iv] Springer, T. (2014). Global Navigation Satellit Systems Overview. GNSS Overview. [online] Positim.com. Available at: http://www.positim.com/navsys_overview.html [Accessed 29 Oct. 2014];

[v] Glonass-iac.ru, (2014). Glonass history. [online] Available at: https://glonass-iac.ru/en/guide/ [Accessed 31 Oct. 2014];

[vi] Ashjaee, J.; How GPS and GLONASS Got Together – and Other Recent Events, GPS World, June 2011, pages 60-66;

[vii] staff, G. and staff, G. (2014). GLONASS Modernization : GPS World. [online] Gpsworld.com. Available at: http://gpsworld.com/glonass-modernization-12232/ [Accessed 29 Oct. 2014];

[viii] Navipedia.net, (2014). GLONASS Signal Plan - Navipedia. [online] Available at: http://www.navipedia.net/index.php/GLONASS_Signal_Plan [Accessed 31 Oct. 2014];

[ix] Navipedia.net, (2014). Galileo Signal Plan - Navipedia. [online] Available at: http://www.navipedia.net/index.php/Galileo_Signal_Plan [Accessed 29 Oct. 2014];

[x] Selding, P. (2014). Galileo Launch, Initially Hailed as Success, Is a Failure - SpaceNews.com. [online] SpaceNews.com. Available at: http://spacenews.com/41650galileo-launch-initially-hailed-as-success-is-a-failure/ [Accessed 29 Oct. 2014];

[xi] Astronautix.com, (2014). Beidou. [online] Available at: http://www.astronautix.com/craft/beidou.htm [Accessed 31 Oct. 2014];

[xii] Navipedia.net, (2014). BeiDou Signal Plan - Navipedia. [online] Available at: http://www.navipedia.net/index.php/BeiDou_Signal_Plan [Accessed 31 Oct. 2014];

[xiii] The Royal Academy of Engineer; Global Navigation Space Systems: reliance and vulnerabilities, London, United Kingdom, March 2011;

[xiv] staff, G. (2015). The System: GLONASS in April, What Went Wrong : GPS World. [online] Gpsworld.com. Available at: http://gpsworld.com/the-system-glonass-in-april-what-went-wrong/ [Accessed 29 Oct. 2015];

[xv] Utexas.edu, (2015). UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea | News. [online] Available at: http://www.utexas.edu/news/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/ [Accessed 29 Oct. 2015];

[xvi] Mitch, R.H., R.C. Dougherty, M.L. Psiaki, S.P. Powell, B.W. O'Hanlon, S.P. Powell, J.A. Bhatti, T.E. Humphreys; Signal Characteristics of Civil GPS Jammers. ION GNSS 2011, 24th International Technical Meeting of the Satellite Division of the Institute of Navigation, Portland OR, USA, September 19-23, 2011;

[xvii] Kraus, T., R. Bauernfeind, and B. Eissfeller; Survey of In-Car Jammers – Analysis and Modelling of the RF signals and IF samples. ION GNSS 2011, 24th International Technical Meeting of the Satellite Division of the Institute of Navigation, Portland OR, September 19-23, 2011;

[xviii] Dixon, C., Smith, S., Hart, A., Keast, R., Lithgow, S., Grant, A., Šafár, J., Shaw, G., Hill, C., Hill, S., Beatty, C.; Specification and Testing of GNSS Vulnerabilities. ENC GNSS 2013, Vienna, Austria, April 23-25, 2013;

[xiv] Elorantechnologies.com, (2014). eLORAN technologies, enhanced loran, GPS jamming, global navigation systems —. [online] Available at: http://elorantechnologies.com/ [Accessed 6 Nov. 2014].

ANNEXES

ANNEXE 1

SATELLITE APPLICATIONS CATAPULT

ANNEXE 2

TASKS PERFORMED DURING THE INTERNSHIP PERIOD

ANNEXE 3

GALILEO RELATED WORK

ANNEXE 4

GALILEO FIRST FIX CERTIFICATE REPORT

ANNEXE 5

GALILEO FIRST FIX CERTIFICATE

ANNEXE 6

INTERFERENCE PROJECT PLANNING

ANNEXE 1

SATELLITE APPLICATIONS CATAPULT

PRESENTATION

The United Kingdom has always been a worldwide leader on innovation and technology. For this main reason, UK's Technology Strategy Board created a network of centres of excellence to enhance his capabilities and provide support to UK industry, baptized as Catapult.

Catapult intends to stimulate innovation, accelerate growth and be a high value development activity in the country. They are a group of private companies, funded by a core grant from the government, which customers can come from many areas of life and businesses: they can be individuals, university spinout companies, established SME's (Small and Medium Enterprises) or even large industries that want to expand and invest in new and innovative areas.

Catapult centres aim to have state-of-the-art facilities and equipment, joined with entrepreneur people that have experience, knowledge and are up to date on the latest trends of technology. All together they seek to help customers to develop their businesses, even from a scratch stage. Business come to the Catapults to benefit from their expertise and from the access they provide to world class facilities and tools at a limited cost, which is a great feature if you are a start-up, allowing to develop and idea rapidly and effectively.

In Autumn 2010, United Kingdom's Government announced an investment of more than £ 200 million, to create, establish and develop this network. Therefore, studies, analyses and decisions were made about the core areas to focus and where to engage them. Finally, the chosen areas of technology were:

- High Value Manufacturing;
- Cell Therapy;
- Offshore Renewable Energy;
- Satellite Applications;
- Connected Digital Economy;
- Future Cities;
- Transport System;
- Diagnostics to Stratified Medicine (to be established);
- Energy Systems (to be established).

In 2013, the global space economy was worth £ 150 billion and it's expected to grow to £ 400 billion by 2030. United Kingdom wants to be one of the leading countries on this business, having a target of delivering 10 % of the global space economy by 2030, representing approximately £ 40 billion per year and creating 100 000 new job opportunities. The challenge is quite demanding and to fulfil it UK needs to grow its space technology exports and services from the current £ 2 billion to almost £ 25 billion per year. It's going to be a tough challenge, requiring changing the vision of entrepreneurs and showing to the public the power of satellites and satellite based applications and how they can improve your daily life. To fill this gap and accelerate the market, Satellite Applications Catapult was established in May 2013.

The launch of the first satellite Sputnik, on 1957, was an enormous breakthrough on space exploration, allowing an all-new set of applications that permitted, significantly, an increase of quality of life, improving the way we see earth, how we navigate, how we communicate, etc. For the last 60 years, many new satellite based technologies have appeared, but, for the common user, most of this technology goes unnoticed, although, almost everyone uses satellite-based data and services in their lives. A few satellite technologies are well known to the public such as TV and GPS, but space is often considered secondary, rather than an increasingly essential asset.

It's in this context that Satellite Applications Catapult wants to act, improving existing technologies, creating new ones and delivering innovative, useful and exciting applications. To achieve this SAC is divided on three tech areas, based on the type of data that satellites can provide: positioning, navigation and timing, earth observation, and communications. Talented, skilled and pioneering professionals are in charge of delivering this to customers, offering experienced counselling. To be effective in their mission they also plan to educate and change perceptions of space tech providing workshops and conferences and making them available to everyone, partnering with academia and university on an early stage.

The areas of action of SAC are quite broad. In the last 6 months, they have been trying to reach an enormous set of areas that impacts our daily life: improving emergency services, using latest technologies so they can be faster, safer and effective; monitoring and managing illegal fishing, which has economic and environmental impacts; using latest EO data to provide mapping on harsh areas, analysing the melting of polar zones or even creating risk maps so authorities know how to react in case of emergency, minimizing losses; studying jamming of global

satellite navigation systems in order to minimize the impacts of them in GNSS reliant activities that go from fleet management, cargo shipping, bank transactions to electric power grids. These are just a few examples of SA Catapult's activities and just by these ones we can affirm the importance of satellites!

Unlike other companies, the success of Satellite Applications Catapult is not measured directly by the own economic grown it has, but by the success and impact it has on its customers and partners. Its aim is to support, help and launch new businesses based on space potential and this is the characteristic that makes it unique and a wonderful place to work in.

LOCATION AND FACILITIES

Satellite Applications Catapult is based in the Electron Building at Fermi Avenue, Harwell, Didcot, located on the heart of the Oxfordshire, 25 Km from the university city of Oxford and approximately 100 Km of UK's capital, London. It is part of a scientific campus where other satellite companies are based, especially the European Space Agency, which has a determinant role in some SAC actions, and Rutherford Appleton Laboratory, who took part in a great variety of satellite missions like the Galileo program.

Figure 27 - SAC premises (Source: SAC website)

The Electron Building includes a wide range of facilities that can be rented at limited prices, including a broad variety of meeting rooms with screens,

videoconference facilities and even video-walls. If research is needed there are two labs that include state-of-the-art equipment, from a wide range of technologies and purposes, like oscilloscopes, signal generators, satellite terminals, GNSS equipment, etc. One of these labs is highly secured in case sensitive work is done. There is also a server that people can use to store data, adaptable to customers' needs and applications, and certified by the European Space Agency. Furthermore, includes empty office spaces so customers can have their own space to start developing a business. The building also has a bar that serves meals, and a kitchen that can be used by staff. SAC employees possess excellent desks endowed with two screens, which improves productivity, in an open and light office.

The reference to SAC facilities is quite relevant because it accomplishes one of Catapults key features: having world-class facilities.

MISSION AND VISION

Satellite Applications Catapult's mission is:

"To innovate for a better world, empowered by satellites"

To achieve that, SAC pretends:

"To be a world-leading technology and innovation company, helping businesses of all sizes to realise the potential from space. By embracing a pioneering, agile, collaborative and entrepreneurial spirit, we create valued partnerships to deliver game changing results".

The strategy comprises six elements, describing how it's intended to deliver the ambition described in their vision.

Figure 28 - SAC strategy (Source: SAC website)

The first three strategic elements, represented by the red arrows around the wheel, relate to the impact they aim to deliver within their target community. The second three elements of their strategy, shown by the blue segments at the heart of the wheel, concern the foundations they need to build and sustain within the Catapult so they can deliver that impact.

ORGANIZATION STRUCTURE

Satellite Applications Catapult is organized according to the following chart:

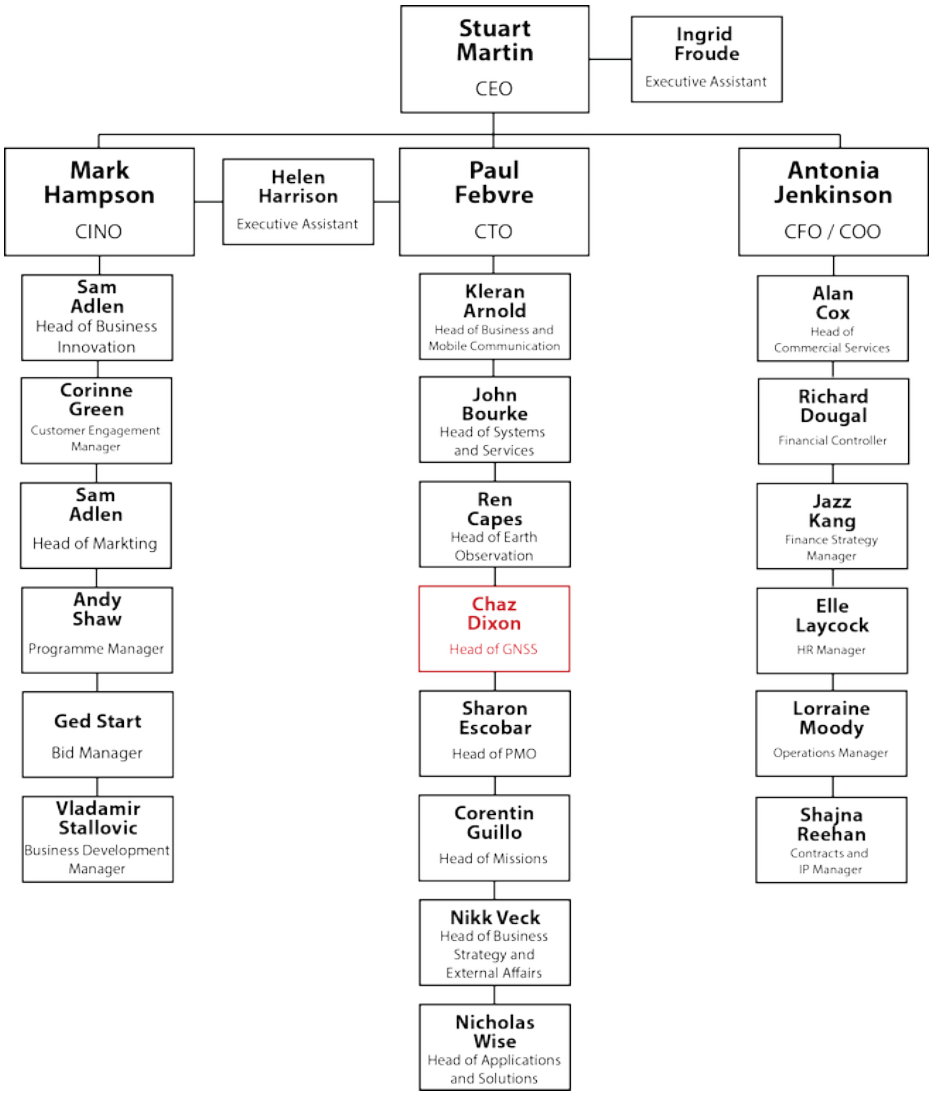


Figure 29 - SAC Structure

SAC employs around 80 people divided on the teams stated on the chart above, which are responsible for several different projects.

WORKING ENVIRONMENT

Besides working structure, all staff is divided randomly in four different houses, composed of around 20 people each. The names assigned represent the four moons of Jupiter: Ganymede, Io, Europa and Callisto. The main objective of this division is to create bonds with people that you are less likely to work with. So, some activities are held where you can get to know other SAC workers, like house lunches, team-building activities, presentations, etc.

Every year all the staff is invited to gather in a staff-day-out where they can get along with people away from working environment. In June 2014 the gathering happened in a forest resort where the houses faced each other in order to create an idea of an application using satellite data. The meeting also had different activities and games, including a dinner and party.

The firm offers a range of sport competitions between other companies in the campus. In terms of food, SAC provides free fruits and biscuits, and also coffee and tea. Staff training and development is highly valued, and in some days, “brown bags” were organised where all workers were invited to have lunch (food supplied) while some space related theme was presented. It’s also very important to refer that if some employee has an idea for an innovative satellite application, the company supports him, allowing 10% of working time to be spent on that.

The company philosophy was quite exciting and very different from what’s usual in Portugal, providing a healthy, happy and great environment to work in, caring about employee’s needs and aspirations.

PNT TEAM

The Position, Navigation and Timing team is responsible for all related subjects regarding global navigation and satellite systems, always paying attention to any development on other similar technologies. Chaz Dixon is the head of department, followed by Steve Hill, Alper Ucar, Pedro Alfaro Sanz and Justin Beasley as project manager. Guy Buesnel was also part of the team but left on May 2014. All elements come from different backgrounds, making the team more prepared to any challenge ahead. Moreover, they were very open-minded, experienced and always available to help out if needed, but providing independence on the work performed. Every

Tuesday the team gathered in a meeting in order to tell the work developments of each colleague.

The team possessed a wide variety of GNSS equipment and establishing a functional lab to perform PNT activities was a priority, not only for the team, but also for any customer who wants do to some research. Therefore, equipment tests were done in order to evaluate the capabilities and limitations of them.

PNT Lab facilities was located on the SatComs Lab and included an expansive list of GNSS equipment like:

- Two radio frequency recorders and players;
- Three high-end GNSS receivers;
- Two Bluetooth handheld receivers;
- One transverse electromagnetic cell;
- Other equipment such as signal generators, splitters and combiners, cables, etc.

Besides this Lab, PNT owned another space where security clearance was needed and it was the location for one of the team's most valuable item: a state-of-the-art GNSS simulator.

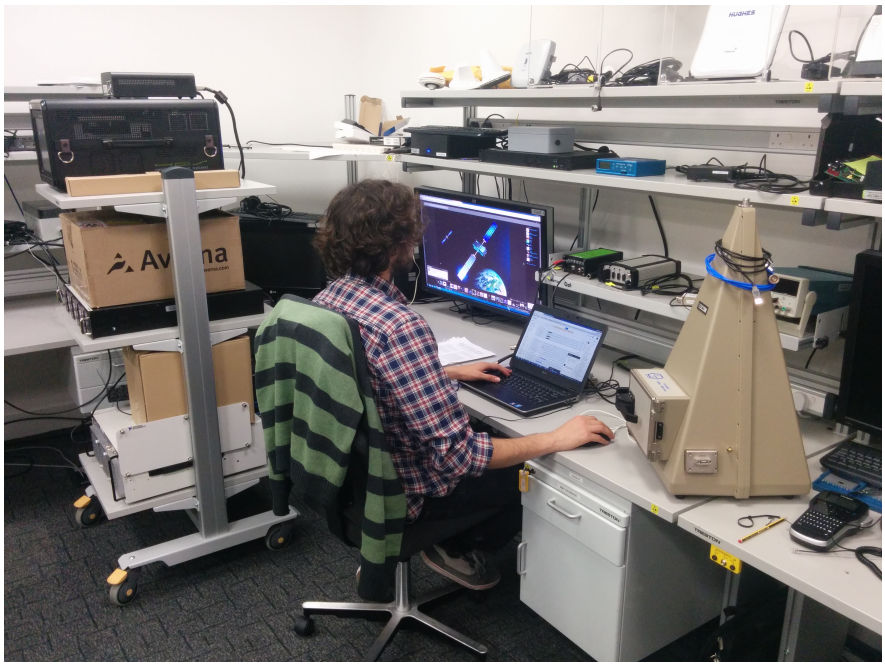


Figure 30 - PNT Lab (Source: Pedro Alfaro Sanz)

During the internship period, the PNT department developed activities concerning the impacts of jamming on GNSS receivers, creating a distributed network of sensors to assess types of jamming and study countermeasures to minimize the negative effect on the equipment. This network, designated as Performance Quantification Network (PQN) was a work in progress. As part of the internship, explanatory videos and presentations were made to showcase the project to prospective partners and sponsors. Jamming in-house sensors were also being developed and spoofing tests in lab conditions were executed.

SAC wanted to test Galileo satellite system, not only using the available free and open services but also the restricted and future commercial products, like the Public Regulated Service. The SA Catapult aspires to be the entity responsible of testing PRS in the United Kingdom.

This simple list sums up most the practical work done from February to August 2014, but a lot of background work was done during that period, like lab organization, tagging, support to other departments, etc. As the company was in an embryonic stage, a lot of brainstorming, long term planning and bidding was held for future projects, envisaging the development of the team and respective areas of action.

Figure 31 - Testing a GNSS antenna (Source: Pedro Alfaro Sanz)

ANNEXE 2

TASKS PERFORMED DURING THE INTERNSHIP

- Setup and Integration of the Navigation Laboratory within the Catapult's lab facilities:
  - Installation, integration and operation of GNSS Equipment: High End Geodetic Receivers (and control software), Commercial Receivers, Antennas, RF Splitters & Combiners, Constellation Simulator and RF Recorders & Players;
  - Set-up Lab PC, installing Windows OS and PNT related software to support PNT activities;
  - Generated documentation on how to output NMEA messages from Rx and how to connect to GIS software for visualization purposes;
  - Generated documentation on how to connect cables to use Averna RF Rec & Play;
  - Recognized faulty equipment (LabSat) and contact vendor who fixed it;
  - Obtained GNSS antennas location using online PPP services;
  - Performed calibration of the IONO monitoring station;
  - Created suite of Python scripts that read NMEA output from Rx and provide precision information for static and kinematic situations;
  - Produced PNT equipment inventory and organized PNT storage areas;

- Developed PNT visualization capabilities within the Catapult:
  - STK GNSS Constellations visualization;
  - Concept platform visualization for IDMS/PQN with Google Maps API, OpenLayers API and OS OpenSpace API;
  - Usage of Ordnance Survey Maps for PNT activities and demos;

- Performed tests regarding GNSS vulnerabilities and robustness:
  - ESMCP interference demonstration;
  - Reproduction of STAVOG Scenarios to assess the impact of jamming on GNSS Rx;
  - Assessed the advantages or disadvantages of multi-frequency and multi-constellation;
  - Creation of motion files, interference files and antenna patterns for Spirent Simulator;

- Additional support to other projects and teams:
  - Support on PPTI trials obtaining DOP values for the field work periods;
  - Support Spoofing Tests, creating tracks and providing GIS analysis;
  - Support to SAC Applications team on advising the design for the Galileo First Fix Event platform;
  - Support to SAC Communications team providing PNT test environment;

- Other tasks performed:
  - Galileo tracking, data recording, data analysis and written report to obtain ESA Certificate for the first 50 Galileo First Fixes;

- Performed Chloe's Half Marathon tracking analysis and produced report;
- Edited the PNT ESMCP and Spoofing demonstration videos;
- Exploration of Raspberry Pi capabilities for PNT activities;
- Attended Esri UK Annual Conference.

ANNEXE 3

GALILEO RELATED WORK

GALILEO POSITION FIX CERTIFICATE

To celebrate the first anniversary of Galileo's first fix, the European Space Agency launched a challenge to individuals or corporations to send their Galileo fixes, giving out 50 certificates to the first ones. The requirements were quite simple, just needing the entity name, address, details of the receiver, start and end date of the fix in UTC and a plot of the coordinates overlaid on a map, like Google Earth. The Satellite Application Catapult wanted to demonstrate its support to Galileo and show their capabilities, so they accepted the challenge, and proposed it to be performed as an internship learning experience.

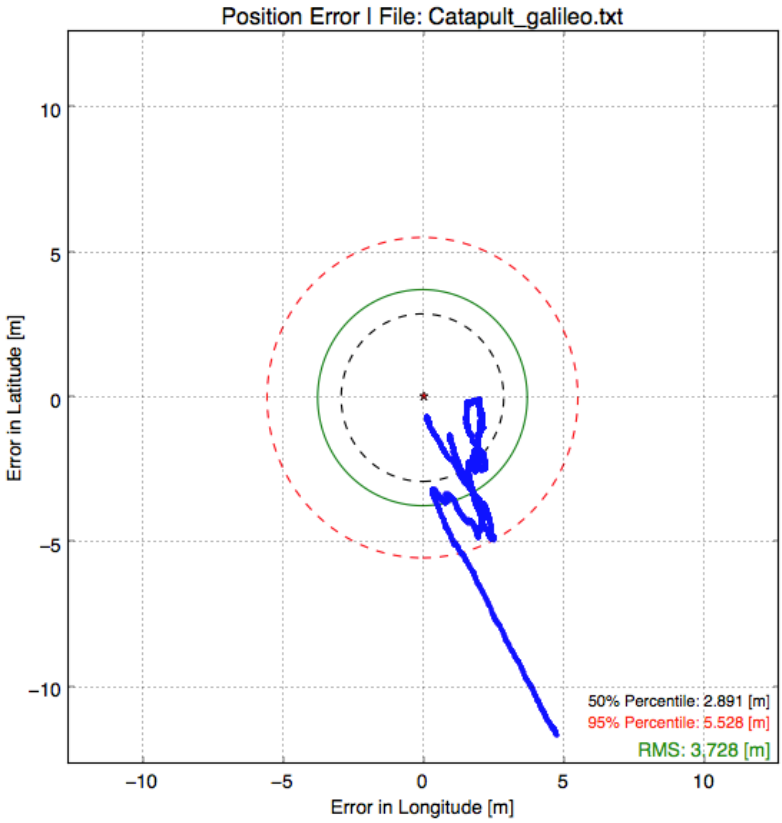
The first step was to determine a time window were the 4 satellites were visible from the office location, so Agi STK software was used to estimate it and was allocated a certain observation time: 2 of April of 2014 from around 08:30 to 09:30.

The receiver used was a Javad Sigma G3T fully configured to only receive Galileo signals, connected to a Galileo compatible antenna mounted on the roff of the SAC facilities. On the desired timestamp it recorded raw observation data (converted to RINEX format through the use of Javad JPS2RIN software) and NMEA messages.

The RINEX file showed that the receiver tracked three Galileo OS signals: E1 (L1), E5a and E5b in a total of 3226 observations/seconds.

NMEA messages were read using a Python (https://www.python.org/) script that converted the messages to a useful Excel (http://products.office.com/en-us/excel) file, usable for data analysis. Then, comparing the coordinates obtained in the observations with the precise antenna location (no datum corrections applied), it was possible to briefly evaluate the accuracy and precision. Using the outputted coordinates and Quantum GIS (Geographic Information Systems) (http://www.qgis.org/en/site/), was possible to create a kml file to open in Google Earth (https://www.google.com/earth/). Finally a small report with all the data needed was created and sent to the European Space Agency (ESA). (annexe 3)

The following graph is not presented on the final report because the script was created after the challenge and is stated here to show the accuracy and precision obtained using only 4 Galileo satellites.



Graphic 21 - Position Error of Galileo observations

The average HDOP was 4.6, normal for a four-satellite test, though the position results obtained were quite satisfactory for this limited observation, confirming Galileo quality and actual operation.

ESA validated the work done, providing a certificate (annexe 4) and consequently SA Catapult can affirm that is one of the first 50 entities to have achieved a Galileo fix in the world!

GALILEO FIRST FIX EVENT

In the 26th of June of 2014, the Royal Observatory of Greenwich was meant to host a Galileo First Fix celebration event and SA Catapult would support it. In a combined effort from SAC different teams it was planned to equip a van with a GNSS antenna and receiver, getting real time PVT using only Galileo Satellites, while the van was moving around London during the event. That vehicle would also be

equipped with satellite terminals to send the van's location data to the Observatory in Greenwich, casting it in a special web application created for the event.

On the 27th of May, Galileo satellite FM4 suffered from a malfunction and was declared unavailable, making it impossible to perform the planned event. The following figures show the sketches of the web application that was being developed through a collaboration between the SAC PNT and Apps teams:

Figure 32 - Galileo First Fix Event platform sketch 1

Figure 33 - Galileo First Fix Event platform sketch 2

DATA COLLECTION

SAC was planning on performing some Galileo fieldwork in June 2014, including the recording of OS and PRS data in a kinematic study. Because of the limited availability and coverage of the 4 operational Galileo satellites, observation times had to be planned carefully, taking in account the best sky visibility, DOP and tracks. In order to support this activity, the DOP values were calculated from the satellite's predicted position (azimuth and elevation) data as extracted from Agi STK. Unfortunately, the planned fieldwork could not be finally performed, due to the Galileo FM4 malfunction in late May.

ANNEXE 4

SA-Catapult Galileo Fix Report

Details

Name: Catapult Satellite Applications

Address: Electron Building, Fermi Avenue, Harwell Oxford,

Didcot, Oxfordshire, OX11 0QR, United Kingdom

Start: 2 April 2014 08:36:35.80

End: 2 April 2014 09:26:55.00

Receiver: Javad Sigma

Using a Javad Sigma receiver we successfully achieved position fix using only Galileo satellites. With the required software, Javad Netview, we were able to output NMEA messages and plot the information on Google Earth. We also recorded receiver's measurements, and we have attached to this document an RINEX 3.01 observation file and also the NMEA log.

Location

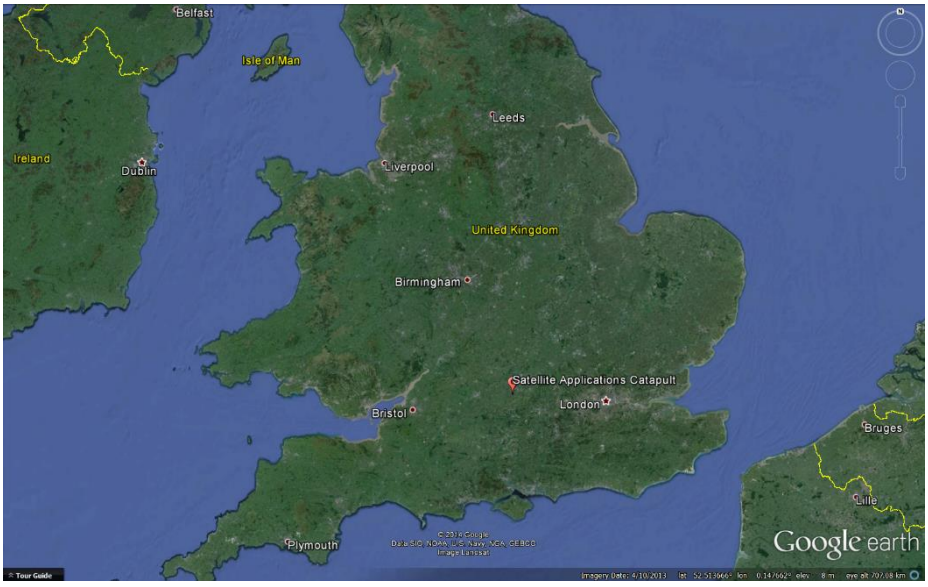


Figure 1 - Satellite Applications Catapult location in the United Kingdom

Figure 2 - Satellite Applications Catapult location in Harwell Campus

Figure 3 - Antenna location

Receiver details

SIGMA

SIGMA.
Universal standard GNSS receiver

SIGMA receiver includes TriPad (two LEDs, ON/OFF and function button), GSM/CDMA2000 module, UHF modem, Bluetooth and Ethernet capability, up to two serial ports, up to two event markers and 1PPS timing strobes, and recargeable batteries.

SIGMAD. Real-Time Heading

Usually, one needs two receivers interconnected through the serial ports. One of them is a moving base and another is a rover. SIGMAD combines both boards connected internally in one unit. SIGMAD is a powerful receiver for high accuracy applications, such as reference stations and CORS.

SIGMAQ.
Real-Time Attitude & Position calculation

The dual frequency code and carrier frequency data are processed to determine the three orientation angles and three-dimensional position up to 20 times per second.

SIGMAQ can also operate in the RTK or DGPS modes receiving differential corrections from an external base station to provide differentially corrected position and velocity.

Standard Configuration

- GPS L1/L2/L2C, L5 (G2T, G3T, G3TAJT only)
- GLONASS L1/L2 (G3T, G-3TAJ(T), D-G3D, Q-G3D only)
- Update rate 1 Hz
- In-Band Interference Rejection (G3TAJT only)
- RAIM
- TriPad interface
- RS232 serial port (460.8 kbps)
- External GNSS Antenna TNC Female connector
- Li-Ion Battery pack

Optional Features

- Galileo E1/E5A (G2T, G3T, G3TAJT)
- Galileo E5B (G3T only)
- GLONASS L3 (G3T only)
- QZSS
- Compass B1
- Compass B2 (G3T only)
- WAAS/EGNOS/MSAS (SBAS)
- Update rate 5Hz, 10Hz, 20Hz, 50Hz & 100Hz
- RTK rate 1 Hz, 5Hz, 10Hz, 20Hz, 50Hz & 100Hz
- Data recording up to 2048MB
- Multi-Base Code Differential Rover
- Code Differential Base
- Advanced Multipath Reduction
- Two event markers
- Two 1 PPS timing strobes
- 1 PPS level converter
- CAN port
- External Reference Frequency Input/Output
- External Reference Output Frequency converter
- IEEE1588 Master Clock (G3TAJT only)
- 2 high-speed RS232 serial ports
- High-speed RS232/RS422 serial port
- USB port
- Ethernet
- Bluetooth
- Internal UHF Modem
- Internal GSM/GPRS Module
- Internal CDMA2000 Module
- WAAS/EGNOS/MSAS (SBAS)
- 2x External Power Inputs
- Mounting Bracket

Features/Receiver Type	Sigma			SigmaD			SigmaQ
	G2T	G3T	G3TAJT	G2	G2D	G3D	
Channels	216						
GPS C/A, P1	√	√	√	2	2	2	4
GPS L2C (L+M), P2	√	√	√	-	2	2	4
GPS L5 (I+Q)	√	√	√	-	-	-	-
Galileo E1 (B+C)	√	√	√	2	2	2	4
Galileo E5A (I+Q)	√	√	√	-	-	-	-
Galileo E5B (I+Q), AltBOC	-	√	-	-	-	-	-
GLONASS C/A, L2C, P1, P2	-	√	√	-	-	2	1
GLONASS L3 (I+Q)	-	√	-	-	-	-	-
QZSS C/A, L1 (I+Q), SAIF	√	√	√	2	2	2	1
QZSS L2C (L+M)	√	√	√	-	2	2	1
QZSS L5 (I+Q)	√	√	√	-	-	-	-
Compass B1	√	√	√	√	√	√	√
Compass B2	-	√	-	-	-	-	-
SBAS L1	√	√	√	√	√	√	√
SBAS L5	√	√	√	-	-	-	-
Size, mm (WxHxD)	32 x 61 x 190						
Weight, g	1270	1277		1290		1310	1330
Autonomous Accuracy	<2m						
Static, Fast Static Accuracy	Horizontal: 0.3 cm + 0.5 ppm * base_line_length Vertical: 0.5 cm + 0.5 ppm * base_line_length						
Kinematic Accuracy	Horizontal: 1 cm + 1 ppm * base_line_length Vertical: 1.5 cm + 1.5 ppm * base_line_length						
RTK (OTF) Accuracy	Horizontal: 1 cm + 1 ppm * base_line_length Vertical: 1.5 cm + 1.5 ppm * base_line_length						
Real-time heading accuracy	-			~ 0.004/L [rad] RMS*			
Roll/Pitch	-						~ 0.008/L [rad] RMS*
DGPS Accuracy	< 0.25 m Post Processing, < 0.5 m Real Time						
Pos/ fix update rate	up to 100 Hz			up to 50 Hz RTK+heading			up to 20 Hz RTK+attitude
Cold start, Warm start	<35 s, <5 s						
Reacquisition	<1 s						
IBIR	-	√		-			-
GSM/GPRS Module	Internal GSM/GPRS quad-band module, GPRS Class 10						
UHF Radio Modem	Internal 360-470 MHz radio transceiver, up to 38.4 kbps						
Base Power Output	1 Watt						
External Reference Frequency	√			-			√
RS232	3						
RS232/RS422	1						
USB	1						
Ethernet	1						
Bluetooth	√						
CAN	1						
IRIG	1						
Event Marker	2						
IEEE1588 Master Clock	-	√		-			
1PPS	2						
Battery	Two internal Li-Ion batteries (7.4 V, 4.4 Ah each)						
External power input	2, 1 - primary, 1 - secondary port						
Input Voltage	+10 to +30 volts						
TriPad	Two buttons, two LEDs						
On-board flash	2048 MB						
Enclosure	Aluminum extrusion, waterproof IP67						
Operation temperature	-40° C to +75° C**						
Storage temperature	-45° C to +85° C***						
GNSS Antenna	External						
Real-time Data Input/Output	JPS, RTCM SC104 v. 2.x and 3.x, CMR						
Real-time Data Output	NMEA 0183 v. 2.x and 3.0, BINEX						

* where L is the antenna separation in [m]
** The operating temperature range of Li-Ion batteries is -30 ° C to +55°
***The storage temperature of Li-Ion batteries is -20 ° C to +45°

Specifications are subject to change without notice

JAVAD GNSS
www.javad.com
Rev.2.1 April 27, 2012

Figure 4 - Javad Sigma Datasheet

Results

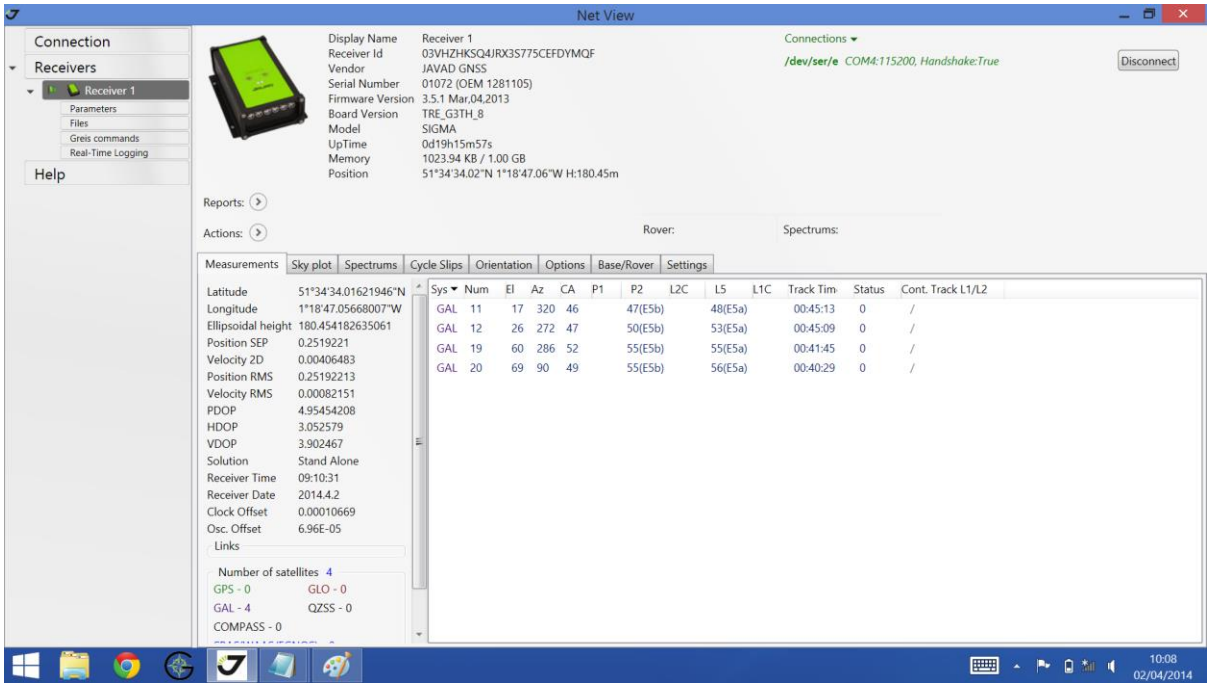


Figure 5 - Tracked Satellites

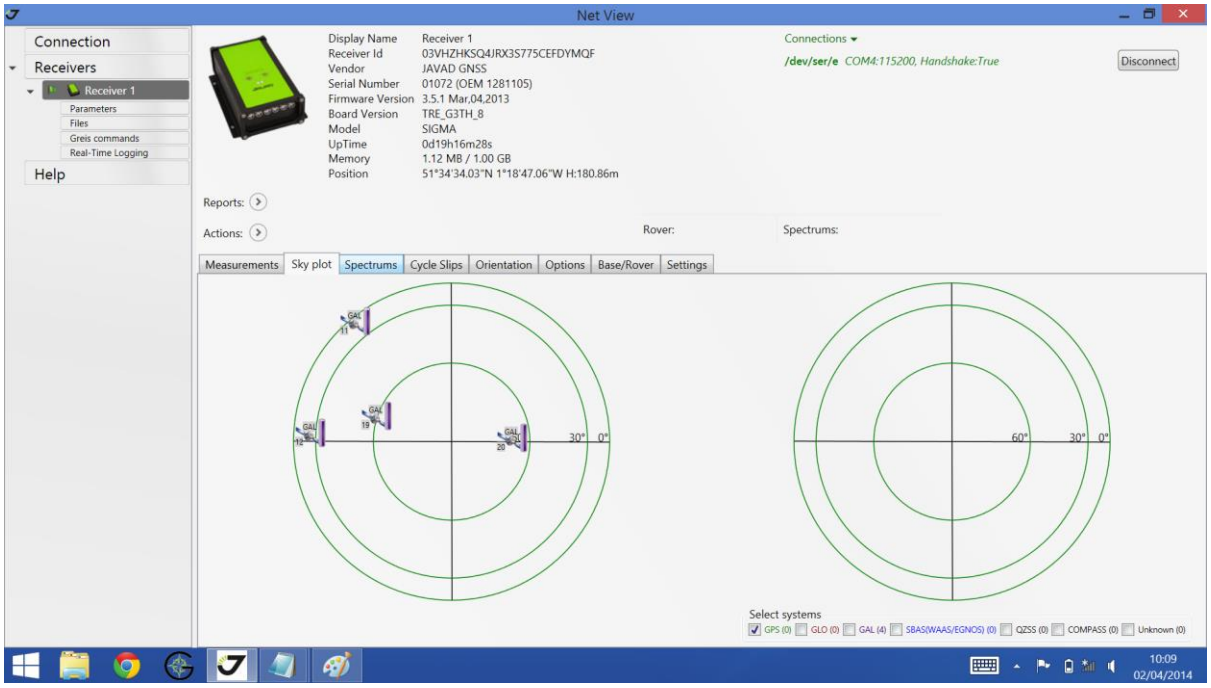


Figure 6 – Skyplot

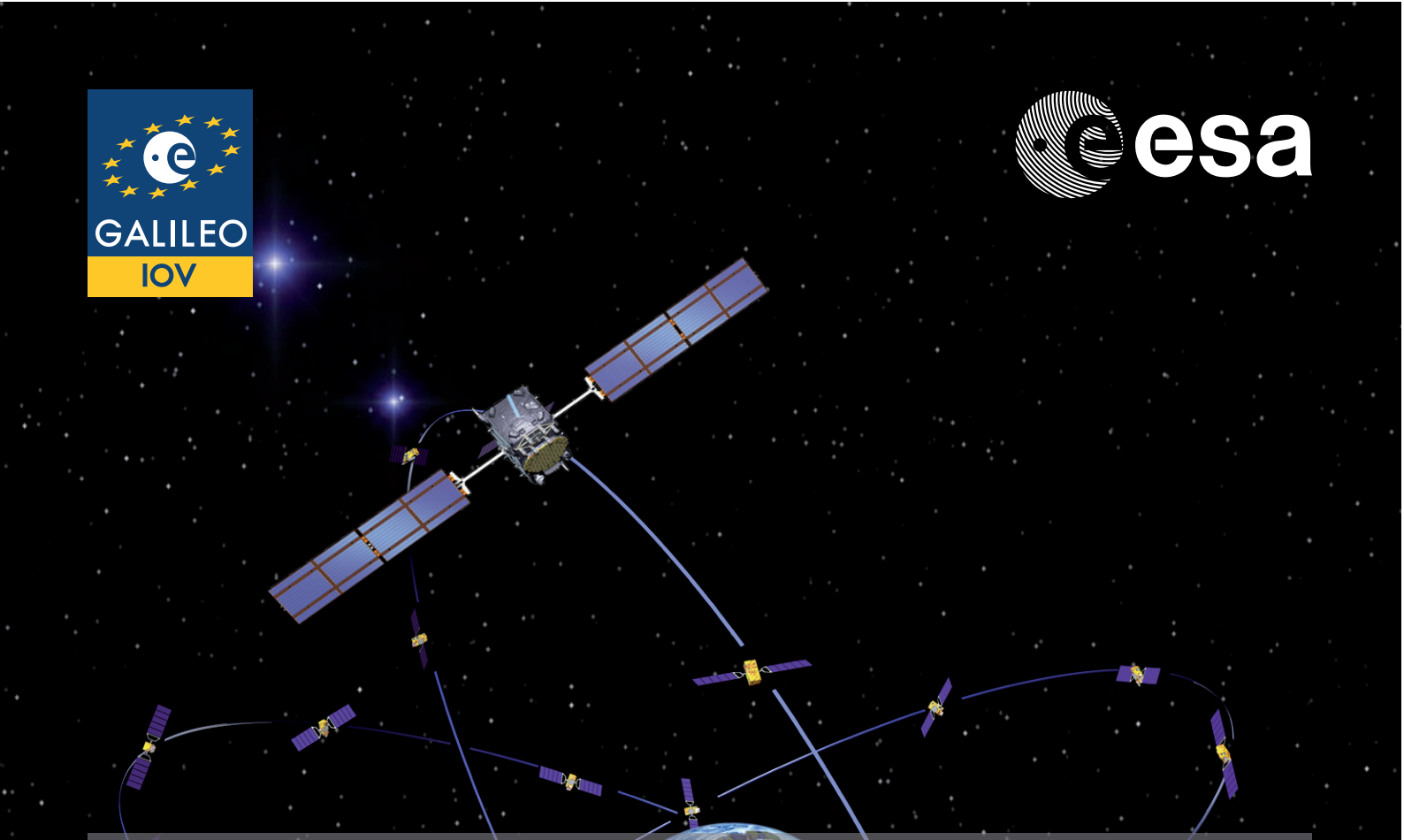
Figure 7 - Galileo Position Fix

Comparing with our precise antenna coordinates we have achieved this results:

RMS Error (m)	Latitude	Longitude	Height (ellipsoid)
	3.234	1.865	2.348
	3.734		

The average HDOP was 4.6.

ANNEXE 5



The European Space Agency wishes to thank

Satellite Applications Catapult
Positioning, Navigation & Timing
Electron Building, Fermi Avenue,
Harwell Oxford, Didcot,
Oxfordshire, UK

for the successful Galileo position fix made
on 2nd April 2014 from 08:36 to 09:26 UTC
in Harwell, Oxford
Lat: 51° 34' N
Lon: 1° 18' W
Alt: 180.45m

This award is granted to the first 50 users of the Galileo system.

Didier Faivre
Director of the Galileo Programme
and navigation-related activities

European Space Agency

ANNEXE 6

Effects of Interference on a GNSS Receiver

Scope

The main goal of this project is to evaluate the effect and impact of interference on diverse GNSS receivers and to develop the Catapult's capabilities in this area.

This project will be carried out in May - July 2014.

Introduction

This project will be held under Position Navigation and Timing team activities. The main goal is to evaluate the effect of interference on a GNSS receiver's output in order to achieve the following objectives:

- Test how GNSS receivers react to interference;
- Evaluate Catapult's equipment;
- Test equipment in real environments to validate the simulations;
- Create scenarios for future testing of receivers.

So, we will try to answer some of this questions using the adequate equipment and methodology:

- How does interference affect receivers output?
- What's the difference between a low-cost and a high-end receiver?
- Do all receivers behave the same?
- How does a receiver behave in real-world experiments and in lab?
- How does a jammer impact receiver's behaviour in real-world conditions and in lab?
- Which kind of receiver should we use in different transport applications?

As part of this project, it is also hoped to achieve a better understanding of the capabilities and limitations of the Catapult's PNT lab equipment.

Work Plan

The work will be held in different phases in order to achieve the goals step-by-step:

Phase 1 – Theoretical analysis

- Theory analysis and acknowledge of concepts related to area of action including brainstorms;
- Literature review;
- Learn how to use equipment and recognise capabilities and limitations (receivers, antennas, jammers, RF recorders and players, simulator, etc);
- Planning and preparation of Phase 2.

Phase 2 – Tool development

- Record test data;
- Create scripts to process data (Python programming language);
- Planning and preparation of Phase 3.

Phase 3 – Characterization of receivers in real-world

- Record real-track data;
- In lab testing;
- Improve scripts for specific needs;
- First results and analysis;
- Planning and preparation of Phase 4.

Phase 4 – Jamming test in lab

- In lab jamming tests;
- Improve scripts for specific needs (if needed);
- Results and analysis;
- Planning and preparation of Phase 5.

Phase 5 – Real world testing

- (constraint) – this phase requires that permission is granted;
- Real-world conditions jamming tests;
- Improve scripts for specific needs (if needed);
- Results and analysis;
- Report of work done and respective achievements.

The following page contains an initial schedule estimation. It must be noted that it might slip due to delays, bureaucracies, lack of availability of equipment or other reason.

Figure 1 - Work Plan.

Methodology

The first steps of the project will be performed through reading and acknowledging the concepts needed to realise this test, including getting the know-how about using all the equipment. Then, some data will be collected in lab and scripts will be built according to our needs. After this important step, real-world data recording should be done. The track should represent a real environment, and it should contain:

- Open spaces (full sky visibility);
- Urban canyons (lower sky visibility);
- Different speeds;
- Roundabouts;
- Turns;
- Straight lines.

In the next figure an installation on a vehicle is proposed to record data in real-world conditions. Rx1 (high-end) and Rx2 (low-cost) are the chosen receivers because both work at a 10 Hz update rate. Only GPS signal will be used on this project, except real-world tests with Rx2 because it's impossible to turn off GLONASS and SBAS tracking in the receiver.

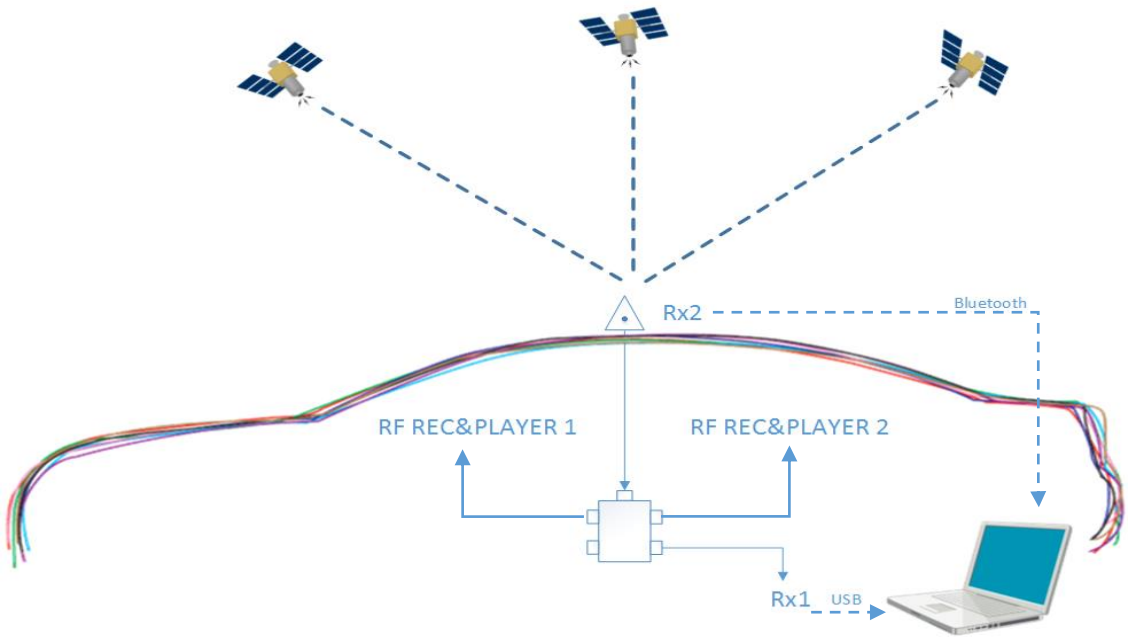


Figure 2 – Trials Vehicle Test Setup.

With this installation we are able to record simultaneously the following data:

- GPS Signal in Radio Frequency Recorder and Player 1 (RF_Rec&Player1);
- GPS Signal in Radio Frequency Recorder and Player 2 (RF_Rec&Player2);
- Track data produced by receiver 1 (Rx1);
- Track data produced by receiver 2 (Rx2).

In lab, with the data recorded, we can test receiver's behaviour applying the same signal twice (or more) for each signal recorded and comparing them.

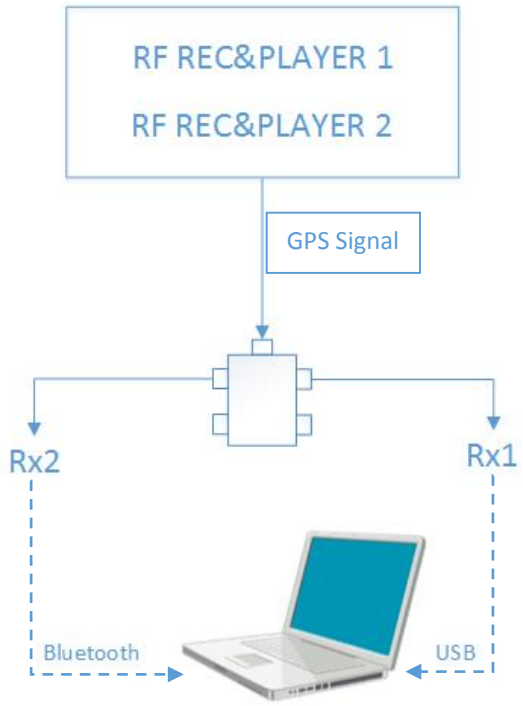


Figure 3 - Lab setup without interference.

Then, we can evaluate the differences between the multiple tracks:

TRACK COMPARISON			OBJECTIVE
Real Track from Rx1	vs.	Real Track from Rx2	Know the difference between receivers output
Track from Rx1 with RF_Rec&Player1	vs.	Real Track from Rx1	Compare Rx1 output on real-world tests against Sigma with RF_Rec&Player1 signal
Track from Rx1 with RF_Rec&Player2	vs.	Real Track from Rx1	Compare Rx1 output on real-world tests against Sigma with RF_Rec&Player2 signal
Track from Rx2 with RF_Rec&Player1	vs.	Real Track from Rx2	Compare Rx1 output on real-world tests against Sigma with RF_Rec&Player1 signal
Track from Rx2 with RF_Rec&Player2	vs.	Real Track from Rx2	Compare Rx1 output on real-world tests against Sigma with RF_Rec&Player2 signal
Track from Rx1 with RF_Rec&Player1	vs.	Track from Rx1 with RF_Rec&Player2	Compare Rx1 output with RF_Rec&Player1 signal and with RF_Rec&Player2
Track from Rx2 with RF_Rec&Player1	Vs.	Track from Rx2 with RF_Rec&Player2	Compare Rx2 output with RF_Rec&Player1 signal and with RF_Rec&Player2

Output information from the receivers can be obtained using the output NMEA message and we can study differences in position (latitude, longitude, height) using GGA/RMC messages, satellites in view and SNR using GSV and PDOP/HDOP/VDOP using GSA.

Once these tests are performed, in order to know signal recorder & player equipment and receiver's behaviour, we can introduce jamming on the system using a GNSS Simulator.

In the GNSS simulator we can create a scenario of a moving vehicle using the NMEA message obtained by the real-world data acquisition. In this equipment it's also possible to apply fixed jammers, in a given position and apply different types of interference and respective power.

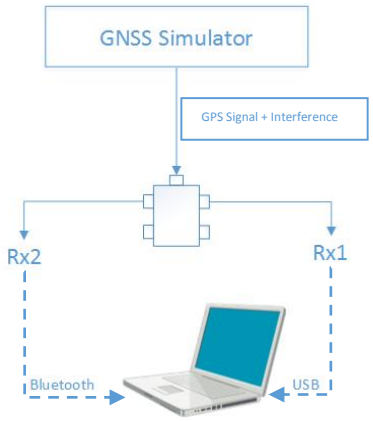


Figure 4 - Lab setup with interference.

Different types of jamming, at different powers in different positions should be simulated in order to evaluate the effect on receiver, like:

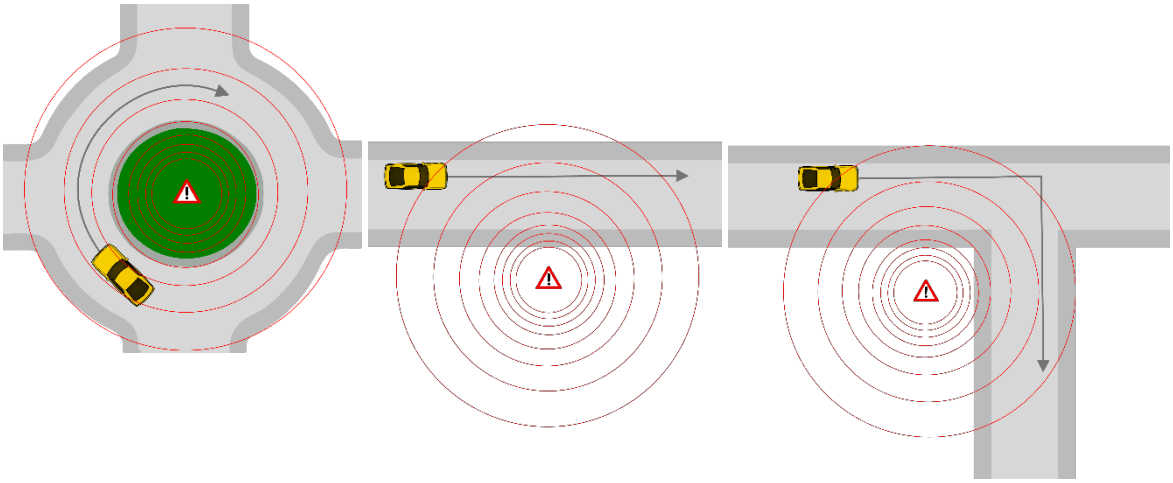


Figure 5 - Jamming power in different types of path.

In the roundabout the receiver experiences the same power of jamming as it moves in circles. In a straight line the jamming power gradually increases and after passing the jammer it decreases. If a turn is made, the car experiences variations of jamming power, increasing when it gets to the jammer radius, then decreasing and, after doing the turn, the interference increases again, after passing the jammer it will decrease as in a straight line.

Simulated jammers should be similar to common ones, available on the market, in order to verify the true impact of them in real-world scenarios.

Using the appropriate scripts, created for this purpose, final results will be achieved. We will try to perform real tests if we get permission/access to specific testing sites in the UK to validate the results that we may get in the lab tests.

Equipment

- ✓ Receiver 1;
- ✓ Receiver 2;
- ✓ Radio Frequency Recorder and Player 1;
- ✓ Radio Frequency Recorder and Player 2;
- ✓ TEM CELL;
- ✓ GNSS Antenna;
- ✓ GNSS Simulator;
- ✓ Signal splitter;
- ✓ Laptop;
- ✓ Bluetooth Dongle;
- ✓ Required Cables;
- ✗ Car;
- ✗ Power supply on the car;