DETECTION, EVALUATION AND CHARACTERISATION OF THREATS TO ROAD APPLICATIONS

DETECTOR

APPLICATIONS AND THREATS ANALYSIS

Prepared by:	Kevin Sheridan (NSL), Tim Whitworth (NSL), Giulio Gabelli (UNIBO), Roberta Casile (UNIBO), Alessandro Guidotti (UNIBO), G. E. Corazza (UIBO), Carsten Hoelper (AGIT), Guy Fremont (SANEF)	06/06/2012
Checked by:	Giovanni E. Corazza (UNIBO), Kevin Sheridan (NSL)	06/06/2012
Authorised by:	Kevin Sheridan (NSL)	06/06/2012

Pages: 65

Document Classification: Public

Change Record

Issue Rev	Date	§: Change Record	Author(s)
1.A	06.06.2012	First version delivered to GSA for review	Detector team

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Purpose of Document

This document describes road applications which have a requirement for a robust and reliable GNSS service and identifies potential threats to such services caused by RF jamming and interference.

This document is produced in the scope of the following work package

- WP2: Technical Feasibility Study

1.2 DETECTOR Overview

The objective of the DETECTOR project is to carry out the design, development, validation and commercial feasibility assessment for the production of a low-cost GNSS interference and jamming detection device for use within road transport applications. The device will be capable of operating in a stand-alone mode or as part of a networked solution depending on the needs. Its purpose is to detect and characterise a denial of service attack. The intention is that the device will be sold to police forces, highways authorities, toll operators, ports authorities and governmental organisations to help combat low-cost and do-it-yourself GNSS jamming technologies.

The DETECTOR concept is proposed as a solution to support and enforce the growing use of GNSS in intelligent transport systems (e.g. demand/congestion management, pay-as-you-drive insurance, intelligent speed adaptation, stolen vehicle recovery, remote start inhibition etc). DETECTOR will address the concerns of government departments, road operators, ITS system providers and police forces across Europe and globally, due to the safety and financial threat to such applications presented by GNSS denial of service attacks.

1.3 DETECTOR Design Logic

The design phase is made up of a Technical Feasibility and a Commercial Feasibility Work Package which will result in a system design which fulfils the identified technical and commercial requirements.

Critical activities in this phase include applications identification, threat analyses, requirements definition, baseline design and commercial appraisals. In particular, different interference detection and characterisation schemes will be analysed. The relationships between these design activities and the documents in which they will be described are shown in figure 1.

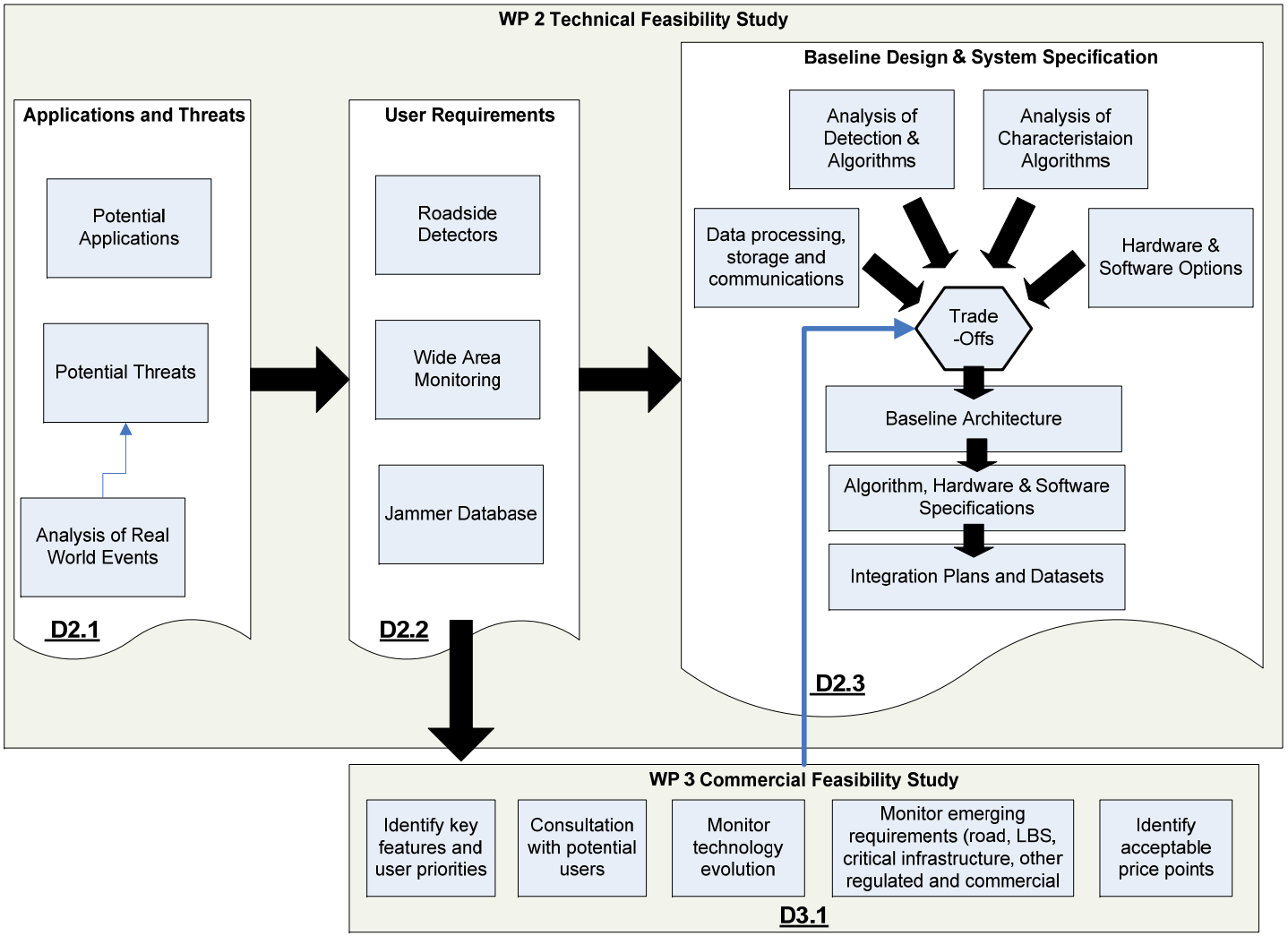

Figure 1: DETECTOR Design Logic

1.4 Document Overview

This document is arranged in the following sections:

- **Section 1** the current section, is an introduction which describes the purpose, scope and structure of the document.
- **Section 2** describes road applications with a reliance on GNSS positioning which makes them a potential user of an interference detection solution
- **Section 3** identifies potential threats to GNSS positioning, with particular focus on jamming
- **Section 4** describes recorded incidents of GNSS interference which helps verify the likelihood of potential threats occurring and their impact
- **Section 5** provides the conclusions of this activity

1.5 References

1.5.1 Applicable Documents

Ref.	Document title	Document reference	Issue	Date
AD1	DETECTOR Annex I to Grant Agreement (Document of Work)	DETECTOR DoW	1.1	15/02/12

Table 1-1: Applicable Documents

1.5.2 Reference Documents

Ref.	Document title	Document reference	Date
RD 1	GNSS Vulnerability and the Case for eLoran D. Last	GNSS Vulnerability Workshop, NPL, UK	22.02.2012
RD 2	Effects of GNSS Jammers on Consumer Grade Satellite Navigation Receivers H. Kuusniemi	ENC2012	April 2012
RD 3	Personal Privacy Jammers Joseph C. Grabowski	GPS World	April 2012
RD 4	Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System, US Department of Transportation VOLPE Centre		August 2001

Ref.	Document title	Document reference	Date
RD 5	Global Navigation Space Systems: Reliance & Vulnerabilities. Royal Academy of Engineering,		March 2011
RD6	Radio Frequency Interference Impact Assessment on Global Navigation Satellite Systems M. Wildemeersch & J. Fortuny-Guasch, EC JRC Security Technology Assessment Unit	EUR 24242 EN	January 2010
RD 7	Investigation on the effect of strong out-of-band signals on global navigation satellite systems receivers Beatrice Motella, Marco Pini and Fabio Dovis	GPS Solutions Volume 12, Number 2 (2008), 77-86	2008
RD 8	Car Jammers: Interference Analysis R Bauernfeind et al	GPS World	October 2011
RD 9	Analysis of Potential Interference Sources and Assessment of Present Solutions For GPS/GNSS Receivers Landry R.; Renard A	4th St Petersburg International Conference on Integrated Navigation Systems	May 1997
RD 10	A Review of the Interference Resistance of SPS GPS Receivers for Aviation Owen J.I.R	ION NTM 1993	January 20 - 22, 1993
RD 11	Assessment of Radio Frequency Interference Relevant to the GNSS L1 Frequency Band RTCA/SC-159 Ad Hoc Special Committee on GNSS Interference	RTCA/SC-159-DO235B	March 13, 2008
RD 12	Assessing GPS Robustness in Presence of Communication Signals Motella, B.; Savasta, S.; Margaria, D.; Dovis, F	IEEE International Conference ICC Workshops 2009 pp1-5	14-18 June 2009
RD 13	GNSS Interference Detection and Localization using a Network of Low Cost Front-End Modules Lindstrom, J.; Akos, D.; Isoz, O.; Junered, M.	ION GNSS 2007 pp. 1165-1172.	September 2007
RD 14	Development of a deployable low cost interference detection and localization system for the GNSS L1/E1 band Isoz, O.; Akos, D.	NAVITEC 2010	8-10 Dec. 2010

Ref.	Document title	Document reference	Date
RD 15	Automatic Gain Control (AGC) as an Interference Assessment Tool Bastide, F., Akos, D., Macabiau, C., Roturier, B.	ION GPS/GNSS 2003 pp. 2042-2053	September 2003
RD 16	GPS Interference Detection and Identification Using Multicorrelator Receivers Bastide, F.; Chatre, E.; Macabiau, C.	ION GPS 2001 pp. 872-881	September 2001
RD 17	An interference detection algorithm for COTS GNSS receivers Calcagno, R.; Fazio, S.; Savasta, S.; Dovis, F.	NAVITEC 2010	8-10 Dec. 2010
RD 18	Field Observations of Personal Privacy Devices Grabowski, J.	ION NTM 2012	30.01 to 01.02 2012
RD 19	GNSS Jamming in the Name of Privacy Pullen, S.; Gao, G	Inside GNSS	March/April 2012
RD 20	Survey of In-Car Jammers - Analysis and Modeling of the RF Signals and IF Samples (Suitable for Active Signal Cancelation) Kraus, T.; Bauernfeind,, R.; Eissfeller, B.	ION GNSS 2011	September 2011.
RD 21	In-Car Jammer interference detection in automotive GNSS receivers and localization by means of vehicular communication Bauernfeind, R.; Kramer, I.; Beckmann, H.; Eissfeller, B.; Vierroth, V.	Integrated and Sustainable Transportation System (FISTS), 2011 IEEE Forum pp.376-381	29.06 to 01.07 2011
RD 22	Mathematical Models and GNSS Interference Borio D.; Lo Presti, L.	Inside GNSS	March/April 2008
RD 23	Effect of Partial-Band Interference on Receiver Estimation of C/N0: Theory J. W. Betz	Technical Report, The MITRE Corporation p. 716-723	2001
RD 24	Effect of Narrowband Interference on GPS Code Tracking Accuracy J. W. Betz	ION NTM 2000	January 2000
RD 25	Interference Rejection Techniques in Spread Spectrum Communications Milstein, L.B.	Proc. of the IEEE vol. 76, no. 6, pp. 657–671	June 1988

Ref.	Document title	Document reference	Date
RD 26	Adaptive Algorithms for Estimating and Suppressing Narrow-Band Interference in PN Spread-Spectrum Systems Ketchum, J.W.; Proakis, J.G.	IEEE Trans. on Comm., vol. 30, no. 5, pp. 913–924	May 1982
RD 27	Narrowband Interference Suppression in CDMA Spread Spectrum Communications Rusch, L.A.; and Poor, H.V.	IEEE Trans. on Comm., vol. 42, no. 2/3/4, pp. 1969-1979	February/ March/April 1994
RD 28	A Single-Chip Narrow-Band Frequency-Domain Excisor for a Global Positioning System (GPS) Receiver Capozza, P.T.; Holland, B.J.; Hopkinson, T.M.; Landrau, R.L	IEEE Journal of Solid-State Circuits, vol. 35, no. 3, pp. 401–411	March 2000.
RD 29	Joint Time-Frequency Domain Interference Mitigation for Galileo L1 Band Receivers Villanti, M.; Pedone, R.; Corazza, G.E.; Crescimbeni, R.	Int. Symposium of Spread Spectrum Systems and Applications (ISSSTA2006)	Aug. 2006

Table 1-2: Reference Documents

1.6 Acronyms

Acronym	Organisation
ADAS	Advanced Driver Assistance Systems
ANPR	Automatic Number Plate Recognition
CEPT	European Conference of Postal and Telecommunications Administrations
CIT	Coherent Integration Time
DBC	Distance-Based Charging
DFT	Discrete Fourier Transform
DMR	Digital Mobile Radio
BTS	Base Transceiver Station
DIA	Detection Identification Adaptation
DSRC	Dedicated Short Range Communication
EDAS	EGNOS Data Access Service
EDGE	Enhanced Data GSM Environment
EFC	Electronic Fee Collection
EGNOS	European Geostationary Navigation Overlay Service
ETSI	European Telecommunications Standards Institute
FFT	Fast Fourier Transform
FPGA	Field Programmable Gate Array
GNSS	Global Navigation Satellite System
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
IFFT	Inverse Fast Fourier Transform
ITU	International Telecommunications Union
KMP	Kilometre beprijzen
LBS	Location Based Services
LORAN	Long Range Navigation
MSS	Mobile Satellite Service
NMEA	National Maritime Electronics Association
NSL	Nottingham Scientific Limited
OBDII	OnBoard Diagnostics interface
OBU	OnBoard Unit
MEMS	MicroElectroMechanical Systems
PAYDI	Pay As You Drive Insurance
PPD	Personal Privacy Device

Acronym	Organisation
PSD	Power Spectral Density
PVT	Position Velocity Time (positioning algorithms of a GNSS receiver)
RTCM	Radio Technical Commission for Maritime Services
RUC	Road User Charging
SBAS	Satellite Based Augmentation System
TDP	Time Distance Place (charging)
TTFF	Time To First Fix
UCP	Urban Charge Point
UHF	Ultra High Frequency
UMTS	Universal Mobile Telecommunications System
VHF	Very High Frequency

Table 1-3: Acronyms and Abbreviations

2 Potential Applications

2.1 Selection of Applications

The DETECTOR concept is proposed as a solution to support the successful use of GNSS in road transport applications. It is intended to help address the concerns of government departments, road operators, ITS system providers and police forces across Europe and globally, regarding the threat from GNSS interference. All road applications which have a degree of reliance on GNSS-based positioning are potential users of DETECTOR services. In many applications disruptions to GNSS positioning due to interference may be a nuisance but they can be tolerated as there is no critical assumption that positioning will always be possible. In other applications though, the ability to be able to determine a position with a known degree of confidence is far more critical because it has safety or financial implications. The applications described here are those with a degree of safety or financial criticality which makes them more relevant to the DETECTOR objectives.

The following applications have been identified as most likely to have a requirement for interference detection based on their reliance on GNSS to provide a critical element of their solution:

- Road User Charging
- Pay-as-you Drive Insurance
- Fleet Management
- Hazardous Goods Tracking
- ADAS (& related safety, including cooperative systems)
- Stolen Vehicle Recovery

In sections 2.3 to 2.9 each of these applications is introduced, describing its purpose, its use of GNSS and the potential consequences of GNSS disruption. The requirements that these applications have in terms of their need to detect interference sources are derived in the DETECTOR User Requirements Document (DTCR_D22).

2.2 Predicting Consequences of Service Disruption

For each application identified, an attempt is made here to predict the impact of a disruption to GNSS positioning. It should be noted though that this impact will depend on a combination of many factors including the following:

- *Size of area disrupted*

  Natural phenomena such as wide-scale ionospheric disturbances, or system-level GNSS faults could affects users over large areas. A low power jammer in a vehicle may only disrupt GNSS receivers within a radius of tens of metres.

- *Dynamics of disruption source*

  If the source of disruption is static and the area it affects remains largely stable, this presents a different problem to a dynamic disruption source.

- *Duration of disruption*

  A service disruption can vary from being almost instantaneous for a receiver (e.g. a low power jammer in a car disrupting other vehicles which it passes) to being a prolonged effect (e.g. a permanently operating RF transmitter with out of band interference which enters GNSS frequencies).

- *Frequency of occurrence of disruption*

  A service disruption may occur only occasionally or events may occur with a high frequency. If in-car jammers are very widely used there could be very frequent disruptions across the road network, but if they are not, there would only be occasional events.

- *Impact of disruption*

  There are multiple factors which will determine the impact that GNSS disruption has for an application, including:

  - The equipment used in the application

    Positioning solutions which do not rely solely on GNSS will be less affected by any disruption than those which use GNSS as the only positioning sensor. However, in many hybrid solutions GNSS is still the principal source of position so even if complementary sensors are present there will be some degradation in performance[1].

    Antennas and receivers will have different levels of robustness to interference sources. E.g. mild levels of ionospheric scintillation are an important issue for high accuracy solutions using carrier phase observables and will increase tracking noise in a receiver phase lock loop but may have little or no impact on consumer grade COTS code solution.

  - The positioning requirements of the application

    Applications will have widely varying positioning requirements in terms of accuracy, availability, continuity, integrity, and coverage area. Some applications will only require fairly low accuracy positions (tens of metres) and can tolerate significant gaps in the position solution because the final user needs are not stringent, e.g. position is only required to reference a vehicle to a large geo-object such as a City.

[1] Reports from maritime trials clearly show that in integrated navigation systems which theoretically have sufficient independent sensors to detect GNSS outages and transition to a degrade mode, in fact GNSS is so tightly integrated in many modern systems that any disruption can also affect the revisionary solutions [RD 1].

Degradation of the GNSS solution due to signal blockages, attenuation and reflection may already be part of normal operations and any additional disruption caused by interference is another inconvenience but it will not be the most significant perturbing factor.

Other applications may have a requirement for very reliable (high integrity) positions in certain areas, for example in a road user charging application that needs to discriminate on which of two adjacent roads a vehicle has travelled with a confidence level which allows a charge to be applied.

The general approach taken here is to first identify the impact on the GNSS receiver, predicting what may happen to estimated positions, and then to predict how this would affect the functioning of each application and the safety, economic or social/political impacts this might have. Receiver impacts will tend to be similar across applications although details may vary if the user equipment differs. The impact that disruption to the receiver then has on an application can vary considerably.

Interference sources increase the receiver tracking noise on one or more channels (satellite observations). Increased noise on all satellite measurements used in the solution will degrade the user position accuracy as each measured range includes additional error. It will also degrade the integrity because the level of nominal errors against which any consistency checks are attempting to identify outliers is increased.

If the induced noise increases to a level at which tracking is no longer possible on one or more channels, this will further degrade accuracy and integrity. As well as the increased measurement noise, accuracy is now degraded further by poorer geometry as satellites are removed from the solution. This impact will vary depending on the distribution of the satellites and the criticality of the measurement which is no longer available. Removing satellites which appear in one area of the sky from a user perspective can dramatically increase position error, in some case by a few hundred metres. Removing any observation reduces the redundancy of the solution (the excess number of observations relative to unknown states) which is a key driver of integrity so this is further degraded also.

If the induced noise level is so high that too few satellites are available to determine the receiver position at all this will clearly degrade availability and continuity. Availability and continuity can also be degraded in the previous cases where a position is still determined but with degraded accuracy and/or integrity because usually these parameters will be defined not simply to indicate that a position is estimated but that a position with an acceptable accuracy and integrity is estimated.

Slightly degraded position accuracy may not be an integrity issue, nor may a complete loss of service as this is easily detectable. For critical applications the most significant threat may be the case of significantly degraded positioning which can go undetected. In hybrid solutions there are opportunities to detect and mitigate the affects of poor GNSS, but it is also possible to exacerbate the impact of occasional poor positions. For example, a hybrid GNSS/IMU solution will use GNSS to calibrate the IMU sensors when it determines the GNSS can be trusted. If the GNSS solution is poor and this is not detected it will lead to a poor calibration of the sensors. Similarly, an erroneous position which is closer to a near-by road than it is to the road that the vehicle is actually on can disrupt routing algorithms using a map database. In both examples a limited period of poor GNSS positioning can have a much longer lasting impact on the navigation solution.

Within the receiver processing a stronger signal needs to be maintained in the acquisition (and re-acquisition) phase than in the tracking phase. For a certain level of interference it may be possible for a receiver already tracking satellites to continue but with degraded accuracy, but it would not be able to acquire signals from new satellites or re-acquire signals after an interruption. This again will impact availability and continuity.

In the case of low power interference sources which are not in close proximity to receivers, and for most naturally occurring GNSS disruptions, the effects are likely to be of the less severe type, i.e. some degradation in accuracy and integrity but not a total absence of position. In cases where a receiver is in close proximity to an interference source, which is the case if a jammer is inside the same vehicle for example, or in the presence of very severe ionospheric scintillation, the effects will be more severe including total loss of positioning.

2.3 Road User Charging

2.3.1 Purpose

The main reasons put forward for adopting Road User Charging (RUC) are to reduce congestion, to reduce levels of vehicle emissions and to generate revenue. Road pricing introduces a financial incentive for changing driving behaviour: using cars less overall and particularly at peaks times in busy areas, and encouraging shifts to alternative forms of transport. The main purpose of RUC is to provide revenues for road construction and maintenance, under the principle of “the user pays”.

The concept of charging tolls for the use of specific road infrastructure (e.g. bridges or tunnels) is not new of course. Tolls have been collected manually (i.e. by toll collectors) for many centuries; automatic machines have been introduced as well on some toll infrastructures, for example when the traffic is low, so that the presence of staff would not be economically justified. Since the early 1990’s Electronic Fee Collection (EFC) systems have been introduced to speed up the revenue collection process and therefore increase the utilisation and capacity of the infrastructure.

2.3.2 Role of GNSS

The majority of electronic charging systems today are based either on Dedicated Short Range Communication (DSRC), also known as tag and beacon, or on Automatic Number Plate Recognition (ANPR). A DSRC system works through communications between an Onboard Unit (OBU) installed within the vehicle and roadside equipment which is installed at entry and exit points of the tolled infrastructure (e.g. toll plazas). In these cases the charging scheme is “event” or “point” based, i.e. a vehicle with an onboard tag passes a beacon on a toll plaza and a fixed charge is applied.

A variant of the above is the “free flow” tolling system, where roadside equipment is installed on a gantry; vehicles do not need to reduce their speed or stop when passing under the gantry, but they are identified by their OBU or their LPR and charged.

ANPR is used primarily as an enforcement tool. In a self-registering system such as the London congestion charge, drivers are expected to inform the scheme operator that they will be, or have been, in the charging zone and pay the necessary charge. If a vehicle which is not declared is then detected in the zone a fine will be issued. Similar principles apply when DSRC and GNSS is the main positioning source – a vehicle detected in a charged area which is not “declaring itself” using the primary technology will then be subject to further investigation.

DSRC and ANPR will remain an effective solution for charging schemes which are applied only on limited infrastructure (specific roads, tunnels and bridges) or for specific cities. For more flexible Time, Distance, Place (TDP) charging schemes though solutions based on significant roadside infrastructure become impractical and GNSS-based OBUs provide a more feasible alternative. A number of GNSS based schemes are already operational, although so far they tend to be limited to specific classes of vehicles, e.g. trucks above a certain weight. The largest European schemes routinely using GNSS in an operational system are in Germany, Switzerland and Slovakia. The introduction of the Ecotaxe scheme in France in which vehicles over 3.5 tons will be charged on 15,000km of roads using GNSS equipment will also have a significant impact.

The basic concept is that the OBU in the vehicle determines its position on a regular basis and this is then related to road data to compute a charge. There are many variations in the way in which this process can be performed depending on the nature of the charging scheme and the solution used on the vehicle and at a back-office facility. For example, a charging scheme may be based on the distance travelled on a specific road within a certain time period, or it may only need to establish that a vehicle has entered a large zone. These two cases can lead to significantly different requirements on the accuracy, availability, continuity and integrity of the positioning solution.

GNSS can be expected to be the principal positioning technology but this does not mean that in all cases the OBU depends entirely on GNSS to determine its position. It could also use a variety of aiding sensors in a hybrid solution. Positions determined from cellular means, or speed input from the vehicle itself can be used to make the OBU more resilient to any GNSS outage.

Billing information may be computed within the OBU in a “smart-client” approach or journey records may be transferred to a back-office facility to compute the charge. The first approach (smart client) can help reduce communications loads as vehicle position data do not need to be transferred from the vehicle, which also helps address privacy concerns. The drawback is that it requires a quite complex and expensive OBU and mapping/charging data stored locally need to be kept up to date. In all configurations the OBU will have a communications capability, typically a GSM or GPRS modem.

2.3.3 Impact of GNSS Service Disruption

For a GNSS-based RUC scheme the impact of disruption to the GNSS will depend very much on the nature of the disruption and the specifics of the charging scheme. If GNSS-based positioning accuracy and integrity is reduced so that it is not adequate to charge a driver for some of their actual road usage with sufficient confidence *but* this is detected, then the charging availability is reduced resulting in a loss of revenue to the State or concessionaire. If the position accuracy is degraded and this is *not detected* it can result in incorrect charging, including overcharging.

Tolerances on overcharging tend to be most demanding (the probability of occurrence is generally specified an order of magnitude less than for undercharging) as frequent challenges to bills by drivers will have a very significant cost compared to the extra revenue to be gained by charging when the position confidence is too low. Perhaps more importantly, if there is a public perception of systematic over-charging then the acceptance of the scheme can be severely damaged. For most RUC schemes though it should be possible to meet charging objectives even with fairly low accuracy position

and limited integrity (high protection levels) by designing the scheme so that it is very unusual to need to discriminate between vehicle positions on roads in very close proximity.

Short outages of a position solution caused by interference are unlikely to affect charging to a great extent. In normal operations it can be expected that the GNSS position solution will be interrupted as the line of sight between a vehicle and satellites will be blocked by buildings, bridges, tunnels and sometimes other vehicles. Scheme designs and operating procedures would need to be robust to ensure that charging is not reliant on a 100% availability of GNSS positioning. This can be achieved by charging based on a small sample of reliable positions within a large geo-object, reconstructing a journey through a combination of reported positions and routing logic, or only requiring position reports in selected areas with good observation conditions creating a "virtual gantry".

In locations where GNSS positioning is not possible or not accurate enough (tunnels, urban canyons, etc.), a DSRC beacon can be installed on a gantry or pole, to broadcast positioning data to the OBU; these beacons are called ALC (Augmentation Localisation Communication).

The use of multiple GNSS constellations is another way of reducing GNSS outages. Many COTS chipsets now use both GPS and GLONASS which helps maintain a usable number of available satellites for positioning even in obstructed environments. In the coming years, the European Galileo should also be available.

Impacts would become more significant if interference effects were more widespread and persistent. If reported positions for many vehicles are regularly too inaccurate to satisfy the confidence criteria for applying a charge, or are simply not available at all, this would have a serious affect on scheme operations.

Enforcement technologies such as ANPR can detect the presence of vehicles which are not providing positions or charge data from their OBU but if the level of incidents detected in this way increases, so too do the scheme operating costs. If drivers are not paying for their road usage as the OBU is not reporting, and this is then detected through enforcement it needs to be investigated. Usually an investigation would start when a vehicle with a non-reporting OBU is detected on multiple occasions. A driver operating a jammer is likely to be detected in this way but it may not be possible to prove that the failure of the OBU to report position was caused by a jammer. In this case the scheme operator may need to pay for the costs of a new OBU and installation.

If this is a relatively rare occurrence it is manageable but if it was more widespread it would quickly become very labour-intensive and expensive. If the level of jammer usage or other interference sources became higher still, with jammers causing interference over a relatively large radius beyond the host vehicle, persistent non-reporting of OBU position could affect a large number of vehicles which are not operating jammers themselves. This problem would become much more significant if charging is extended from specific classes of vehicle, such at the present schemes for trucks, to include all vehicles. It is also likely that the OBUs needed for a more universal RUC on all vehicles would need to be less complex and expensive than those used in trucks today, increasing reliance on the core GNSS receiver[2].

[2] The tax revenue due from a commercial truck is much higher than that of a privately owned car, allowing a higher operating cost per vehicle to be feasible. With much reduced tax revenue due per vehicle, the cost of collection must be much lower too to be economically viable.

It is possible that increased use of GNSS for road charging will give people the incentive to operate jammers but it is other unrelated applications which would be more adversely affected. In other words, it is the indirect or unintended consequences which may be more significant. The same applies to the use of jammers with the intention of protecting personal privacy. Users of such devices may be completely unaware that their jamming device is interfering with GNSS receivers elsewhere. It would depend on prevalence of jammer use, their locations and the effective range of the devices but it is conceivable that in-car route guidance devices, pedestrian Location Based Services (LBS) and even ports and airports could suffer disruption.

OBU manufacturers can design and implement anti-jamming features in the OBU; as explained above, jamming can be detected by a combination of on-board sensors and signal processing: for example vehicle movement can be detected by motion sensors and information from GSM stations, even if the positioning from GNSS is not available. In that case, the OBU will enter into a “blocking state”, which can be unlocked only by the toll operator. When the OBU is blocked, the vehicle driver and/or owner is considered violator. He has then to contact the toll operator and ask for the unit to be replaced. It is his responsibility to have and use at any time a working OBU, otherwise he can be fined by the police of customs authorities.

2.4 Pay-as-you Drive Insurance (PAYDI)

2.4.1 Purpose

PAYDI charges the user an insurance premium based on the miles driven during specified periods and on certain road types. In addition some insurers are introducing policies which also take account of speed and driving style, based on acceleration and breaking, and also where the vehicle is parked overnight. It is often targeted at low mileage car owners and young drivers. Young drivers are considered a particularly high-risk group by insurers so therefore have high premiums. PAYDI gives them an opportunity to significantly reduce their premium if they do not drive at times and on roads with higher risk of accidents.

2.4.2 Role of GNSS

Vehicle position is determined using a GNSS-based OBU in a similar way to RUC. The data is communicated to a service centre (back-office) and often this journey information may also be made available to the driver on a personal on-line account so they can monitor their own usage and charges.

Usually the OBU can also act as a stolen vehicle recovery tracker and insurance policies will include theft clauses. If the vehicle is reported stolen and the OBU is still active this data can be provide to the police by the insurance company, or the agent maintaining the PAYDI service, to locate and recover the vehicle.

2.4.3 Impact of GNSS Service Disruption

There are many similarities here with the RUC case (§2.3.2). A low level GNSS disruption which causes occasional inaccurate positions or prevents position estimation altogether for limited periods is unlikely to have a significant impact on the overall functioning of the application. It is expected that the vehicle will sometimes operate in areas where good GNSS positioning cannot be guaranteed.

The disruption becomes more significant if large sections of journeys or whole journeys are not reported because no GNSS positioning is available. This would be the case if a user of the OBU was also operating a jammer in the vehicle. They may do this either to evade charges for specific trips which would incur a higher premium rate, or to systematically reduce their reported overall mileage. There are mechanisms in place to detect this type of fraudulent use though. This can be done automatically if the OBU is also able to access odometer data from the vehicle which is possible over the OBDII interface[3]. This allows the consistency of the distance travelled as reported by the GNSS OBU to be checked. The OBU may be able to detect that the vehicle ignition is on, to detect motion through a simple MEMS accelerometer, or to obtain a coarse position using cellular functions, all of which can quickly identify periods where a vehicle is moving but to GNSS-positions are being logged and reported. Also, when a vehicle has annual inspections (an “MOT” in the UK) its mileage is reported and this can be made available to insurers which again allow them to detect any major discrepancies.

[3] OBDII is a standard interface for accessing data from an engine management system to support diagnostics (equivalent to the European On Board Diagnostics, EOBD, regulations). It has been implemented on petrol vehicles since 2001 and diesel vehicles since 2004. With a simple low-cost dongle (approx. €20) any driver can capture this data to a logging device. For a GNSS OBU it is feasible to interface to this datastream to use speed data and engine status.

If large sections of journeys or whole journeys are not reported because no GNSS positioning is available and this is not due to isolated deliberate jamming by an individual the impacts can be more acute. If this is routinely the situation then the overall solution becomes unfeasible because the picture of the individual driving behaviour becomes too incomplete to fulfil the application objectives. A level of interference which prevents positioning over large areas and for long periods is unlikely though. If it was due to a single interference source (unusually high solar activity or badly tuned RF broadcast) it should be easily identifiable. To be caused by multiple local interference sources (most likely low power jammers) would assume a level of use by a very significant proportion of road users which seems unlikely.

As with RUC, the major potential issue for the scheme operator is likely to be the effort required to investigate frequent reports of non-reporting OBUs. Occasional exposure to interference is not likely to trigger investigations, but with high levels of interference on the road network it could become difficult to establish a workable detection threshold.

2.5 Fleet Management

2.5.1 Purpose

Fleet management systems allow a user to track and manage a group of vehicles. Functions may include vehicle maintenance, fuel management, driver management, speed monitoring and delivery optimisation (logistics). Overall the aim will be to improve operational efficiency and productivity. This may include demonstrating compliance with legislation (e.g. driving hours directives or animal welfare guidelines) in a cost-effective way. The scheme may be operated by the fleet owner or may be outsourced to a service provider.

2.5.2 Role of GNSS

A GNSS-based OBU reports the vehicle position either periodically or on demand via a cellular network, or more unusually satellite communications, to the control centre. It may also record position data locally at a higher rate than it reports this back to the control centre. This more detailed logged data can then be used for offline applications and analysis. In addition the OBU may support route guidance for the driver.

2.5.3 Impact of GNSS Service Disruption

As in previous applications, it is not expected that low level GNSS disruption which causes occasional inaccurate or unavailable positions will have a significant impact on the overall functioning of the application. There may be cases in which inaccurate positions mean the vehicle is matched to the incorrect road and this then disrupts routing algorithms temporarily, but this is something that can occur not just because of interference. It would again require substantial levels of external interference, affecting wide areas and persisting for long periods, to significantly disrupt the vehicle being tracked.

A more likely source of persistent disruption is a jammer being used on a vehicle equipped with an OBU. In this case it would prevent the vehicle position being reported and would reduce the efficiency of the fleet management. In normal working hours when the driver is going about his or her business there appears to be little incentive to operate a jammer and a non-reporting vehicle could be quite easily

detected. If however their use of a company vehicle was infringing rules in some way (e.g. unauthorised personal use) they may want to disrupt the tracking ability. This unrecorded use could again be detected by checking against other sources of information (mileage records, accelerometer and odometer inputs). In fact, a vehicle not reporting its position when it is expected to is likely to raise an alert with the fleet manager, so would actually draw attention to the driver.

High levels of interference not caused by a jammer on tracked vehicles but which prevents the OBU determining positions could be a significant nuisance. It degrades the ability of the system to meet its main goal of managing the fleet efficiently and it could trigger multiple false alarms which indicate that the OBU is faulty when in fact this is not the case.

2.6 Hazardous Goods Tracking

2.6.1 Purpose

Hazardous goods tracking comprises a set of functions which allow dangerous goods to be transported safely by road. This includes planning routes where the use of certain vehicles and cargoes is allowed, coordinating with the relevant public authorities (emergency services, highways agencies, traffic management and information centres) who may need to assist, authorise, or at least be aware of the operation, and then the monitoring of vehicles during the planned journey itself. In can also make use of geo-fences to define areas where a vehicle is not permitted to operate, or designate locations at which the vehicle can be unlocked to allow access to the cargo.

2.6.2 Role of GNSS

GNSS is again used in some form of OBU on the vehicle to report the position of the vehicle to a monitoring centre. Reported positions may then be shared with others. The OBU is also likely to provide route guidance to the driver. The onboard position may also determine whether the vehicle is within a geo-fenced region which either permits or prohibits an activity (e.g. unlocking the cargo area) and could alert the driver if the vehicle is approaching a prohibited area. In an extreme case the vehicle could be remotely disabled rather than allowing it to enter a prohibited area.

2.6.3 Impact of GNSS Service Disruption

There are safety as well as economic aspects to hazardous goods tracking, therefore the impact of GNSS service disruption can differ from the previous cases. The impact on a receiver is unchanged of course: interference will lead to degraded positioning. In the case of no position being available this may lead to a complete loss of service meaning the operation must be suspended. This is quite different from previous cases where a vehicle could still continue to operate with no position being reported. In hazardous goods tracking some cargoes are considered so high risk that if the vehicle position can no longer be determined at the monitoring centre immediate action is needed. Given this criticality though, it can be expected that GNSS would not be the sole source of positioning onboard and provision would be made for some level of degraded operation.

In the case of a position being determined with degraded accuracy, this could disrupt the onboard routing algorithm or trigger a false alert of a deviation from the designated route.

It is possible that further disruption could be caused through the use of geo-fences. If for example a vehicle can only be unlocked when the OBU determines with a high confidence that it is at a designated location, interference in this area may prevent the locks operating.

In this application there seems to be no incentive for a driver of the tracked vehicle to operate a jammer as any disruption to position reporting will be quickly detected. High levels of interference not caused by a jammer on tracked vehicles but which prevents the OBU determining positions could be a significant disruption

2.7 ADAS

2.7.1 Purpose

By definition Advanced Driver Assistance Systems (ADAS) are (electronic) additions to vehicles which support the driver in certain driving situations. Often safety or enhanced comfort are the main focus. An additional aspect is enhanced economy.

While ADAS act (partly) autonomous, most of them follow the concept of the driver still being fully responsible, i.e. the driver can overrule the ADAS system. Reason for that is the Vienna convention on road traffic (1968,Art.8,§5: “Jeder Führer muss dauernd sein Fahrzeug beherrschen oder seine Tiere führen können” – each driver has to be in control of his vehicle or his animals at any given time).

Examples of ADAS are

- Antilock Breaking
- Traction Control System
- Electronic Stability Control
- (Emergency) Braking Assistant
- Electronic Differential Lock
- Night Vision
- Hill Ascend/Decent Control
- (Adaptive) Cruise Control / Intelligent Speed Assist
- Distance Warning/Control
- Blind Angle Assistant / Side blind zone alert
- Congestion Assistant / Automated Stop&Go
- Lane Detection / Lane Keeping
- Lane Change Assistant
- Tyre Pressure Monitoring
- Parking Assistant / Automatic Parking
- Traffic Sign Recognition / Intelligent Speed Assist
- Driver Drowsiness Detection
- Car2Car Communication
- Pull-Out Assistant
- Ecodriving Assistant
- Safety Alert Seat
- Automatic Collision Alert / Preparation
- Adaptive Forward Lighting

- Rear Vision Camera with Dynamic Guidelines
- Head-Up Display

and in future

- Rural Driving Assistant
- Urban Driving Assistant
- Collision Warning / Collision Avoidance
- Autonomous Driving

Sensors in use include

- Radar
- Lidar
- Ultrasonic Sensors
- Cameras

and for functions like Adaptive Front Lighting, extended ACC, Pull-Out Assistant or simple navigation the GNSS positioning sensor.

2.7.2 Role of GNSS

GNSS is used not only for navigation, but usually to find a dedicated position (on a map) to be used as starting point of a route, indication of the (short term) route ahead (e.g. with Adaptive Front Lighting, where the light is directed into curves even before the steering wheel is being turned), fleet management or vehicle recovery (see above), telematics and information for others – today with eCall, later to communicate ones position to other vehicles for relative positioning. In addition, GNSS is used as an additional sensor for vehicle speed or heading.

2.7.3 Impact of GNSS Service Disruption

Applications using GNSS can generally be divided into three classes:

- Safety Critical (more and more ADAS / integrity is essential here)
- Liability Critical (comfort functions, tolling, PAYD, fleet management, Electric Vehicle range estimation)
- Non Critical (location based services, efficiency related applications)

ADAS, especially if they are relevant for safety, will never rely on a single sensor only. Thus, GNSS positioning can be regarded as one of several sensors and outages caused by, e.g. tunnels, garages, or street canyons must be handled within each system. Solutions to keep a valid position are, e.g., inertial positioning systems, wheel based speed sensors, or turning angle sensors. In case of a known degradation of the positioning system, the sensor fusion algorithm will change the bias of the individual sensors. If the position is lost completely, the last fall-back solution would be to warn the driver and to disable a system temporarily. While a loss of service while using that service already is unacceptable, an undetected loss of accuracy is even more critical.

At ENC2012, Heidi Kuusniemi stated a degradation of position accuracy of up to 130m caused by a simple cigarette-lighter-mounted jamming device [RD 2]. Looking at the pull-out assistant developed within the FAMOS project, the criticality of this gets obvious. While the car equipped with this feature approaches the Autobahn, a camera assists staying in the middle of the entering lane, lidar and (side-)radar detect obstacles

and the free gap where the Autobahn can be entered, while the GNSS position detects the placement within the range of the acceleration lane. If the calculated position deviates from the true position without awareness of the system, the car may already have reached the physical end of the acceleration lane while thinking there is still space for acceleration and pulling out. Or, looking at an eCall emergency call, with a degraded position, the rescue forces might arrive on the wrong side of a road with separated, directional driving, thus requiring a time-consuming detour to reach the other side.

Thus, unlike liability critical applications, even intermittent disruptions are quite significant if there is a safety element. Unfortunately, the danger emitting from small, mobile jamming devices has not been a topic in the automotive industry yet. Currently systems are being developed which are to go into production as soon as reliable positioning (e.g. with EGNOS, or later Galileo) is available. The focus here is more on what could be done with positioning of higher accuracy than on which sources might degrade this accurate positioning service again.

2.8 Other Road Applications

Other road applications where GNSS positioning and timing are essential include:

- Electric Vehicles – these need to calculate the remaining range to determine, whether the target destination can be reached / can be reached only if energy consumption of comfort features like air-conditioning is reduced / cannot be reached; it can also be used to determined is the vehicle is leaving the authorized zone (case of the “autolib” service in the Paris region)
- Multimodal mobility, where personal location, time, location of means of transport (car-sharing vehicle, bus, train) etc. is taken into account to calculate the fastest means of transport
- Synchronization of surveillance sensor to realize, e.g., an average speech check
- Stolen vehicle recovery
- Commercial telematic/infotainment services – emerging in-car services with a location element. These can be thought of “enhanced SatNav” which may for example provide real-time car parking capacity information, best petrol prices, car servicing offers which may also be linked to OBD data (e.g. best price in the area to get a replacement of a part which the OBD diagnoses as faulty) guidance to restaurants based on user reviews, etc.

These applications are not detailed further as the role of GNSS and the impact of any disruption will be similar to the applications already described in sections 2.3 to 2.7. In all cases, a low level of interference will be a nuisance in the same was as other factors such as signal obstructions and multipath which degrade GNSS positioning. Very high levels of widespread interference could begin to make entire applications untenable and would certainly undermine user confidence.

These applications have a lower level of criticality than some of those already described. Although some specific disruption to commercial services broadcasting restaurant or shop information might seem a small inconvenience, if this starts to impact the customer experience and reduces uptake of products and services it might have a substantial financial impact on the companies who have invested heavily in

developing such services over the last few years.

2.9 Non-Road Applications

The focus of the DETECTOR project is road applications. These applications may provide drivers with an incentive to operate jammers but it is possible, probable even, that it is other unrelated GNSS applications which may be more significantly affected. The case of truck drivers in New Jersey (USA) operating jammers to prevent their journeys being monitored and inadvertently interfering with GNSS at Newark airport near the highway has been widely reported [RD 3]. It is these sorts of inadvertent or secondary effects of intentional jamming which may pose the most significant threat to GNSS operations. Power or communications networks using GNSS timing can be disrupted just as the airport landing system was disrupted. There have been examples in the UK of train doors failing to open at stations because of faulty GNSS. This wasn't caused by interference, but it highlights the fact that solutions which rely on GNSS do not always include satisfactory reversionary systems.

In many companies, telecom or IT systems are synchronised by the GNSS signal which provides a very accurate clock. Interferences to GNSS could have a strong impact to the industry and economy.

Less critical commercial LBS and location-dependent telematics applications will be disrupted if there is a significant use of in-vehicle jammers in urban areas. In many respects these consumer applications are less critical than some of the regulated applications considered so far, but a significant disruption of these services would have a great economic and also political impact as they are so widely used by the general public.

From the earlier analyses it appears that in many road applications the scheme or service operator may not have a very strong incentive to detect and locate jammers. It is actually law enforcement bodies and telecoms regulators with an obligation to manage the radio spectrum to protect all applications that will ultimately need to detect, characterise and locate jammers. It is already illegal to place GNSS jamming equipment on the market in the EU as it cannot be made compliant with the EMC directive and in the UK their use is a serious offence under the UK Wireless Telegraphy Act 2006 [RD 5].

It is likely that developers of road applications using GNSS will come under increasing pressure from regulators to implement solutions where a user gains little or no advantage from jamming GNSS signals because of the impact this can have on other services [RD 5]. Rather than affecting the efficiency of their operation, it may be that demonstrating compliance with such a regulation will determine whether or not a service contract or concession is awarded. The means to detect jamming would be one element in a compliant solution.

3 Potential Threats

The vulnerabilities of GNSS to interference have been extensively studied and documented over the last decade and more. The publication of the VOLPE report in 2001 was an important milestone in raising awareness of this issue within the GNSS community [RD 4]. The subject features heavily at major GNSS conferences and is also the subject of dedicated events such as the GNSS Vulnerabilities and Solutions Conference held annually in Croatia. With the increasing reliance on GNSS across a multitude of applications, and way in which it has become an embedded technology largely invisible to most users, the consequences of GNSS disruption become ever more serious. This was clearly highlighted in a recent review carried out in the UK in 2011 by the Royal Academy of Engineering [RD 5] which noted that "*The wide range of applications dependent on GNSS signals provides many ways in which seemingly unrelated services could fail simultaneously as a result of disruption to the GNSS signals".*

The intention here is not to provide a comprehensive review of threats to GNSS. The aim is to give a brief overview of the types of interference which may affect a GNSS service because DETECTOR may need to be able to differentiate some of these from the intentional man-made interference and jamming it is seeking to identify.

The GPS signal received by the user is of a very low power, the minimum guaranteed value is approximately -160dBW (10^{-16}W) at the receiving antenna for the L1 C/A code. Consequently it only takes a signal a few orders of magnitude stronger to cause a GPS receiver to lose lock on the tracked signal. Due to the nature of the signal, during acquisition some 3 to 10dB more power is required than is needed during stable tracking. Thus the condition could arise where a receiver may work under adverse conditions provided the interference starts after it has acquired sufficient satellites to provide a position, and, as the satellites set or are dropped, it will be unable to acquire replacements and will ultimately stop positioning. The sources which could cause these types of interference are numerous.

Figure 2 presents a general logic describing how an interferer which is affecting a user receiver, and potentially being detected by a DETECTOR probe, could be classified in order to identify the likely cause. This helps identify the type of signals and signatures the detection system should be aiming to identify.

A first criterion is whether the interference is intentional or unintentional. Unintentional interference can then be divided further into man-made and natural sources. For DETECTOR is important to be aware of these causes and their consequences in particular to avoid false alarms where the system may indicate there is some intentional interference device in use when in fact the disruption being caused is from an entirely unintentional source.

Intentional interference can be categorised according to its purpose. Although operating a jammer in most countries is illegal, many people who purchase and use them may be genuinely unaware of this as they are marketed as Personal Privacy Devices (PPDs). Others may buy devices deliberately to disrupt GNSS equipment but only on a personal basis (e.g. evading a road charge, or preventing an employer being able to monitor a driver who is using a vehicle against company regulations). The motivations for using these devices in different scenarios is not a principal concern for the DETECTOR project but considering this helps to identify the type of devices which are likely to be most common and hence should be detected. DETECTOR should aim to detect and characterise the low-cost jammers which will be most likely to cause disruption to the targeted road applications.

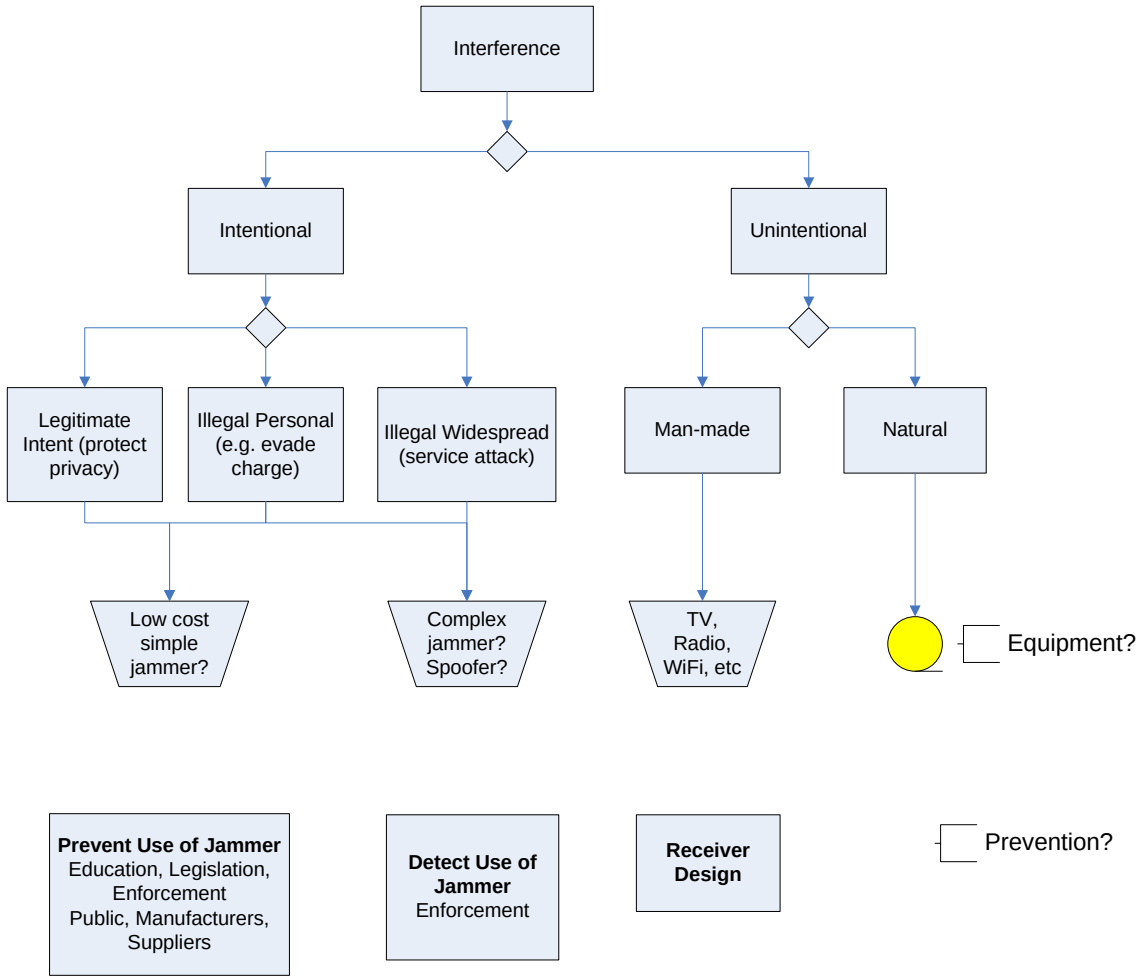

Figure 2: Classifying Interference Sources

For more malicious attacks on a system itself, rather than just an individual tracking device, the expectation is that more complex and powerful jammers would be used. Potentially these types of attacks could also include more sophisticated spoofing and meaconing. From description of the applications in section 2, and the original aims of the project, these types of attack are not the focus of DETECTOR and this therefore rules out a set of interferers that will not be considered further.

The final row in figure 2 identifies some potential methods to prevent or mitigate potential threats. If the majority of jammers in operation are actually being used as PPDs and the users are not even aware that they will also be disrupting other GNSS equipment in the vicinity, then raising public awareness and ensuring the correct regulations are in place regarding the sales and marketing of such devices could be an effective approach. Receivers and antennas can also be designed to be more robust to interference. This helps highlight that detection of jammers will be one element in addressing the threat.

3.1 Unintentional Interference

3.1.1 Natural Phenomena

Natural RF interference can be caused by solar activity which leads to a variety of phenomena on the Earth from short-term localised events through to much longer term trends. Solar activity influences the behaviour of charged particles in the atmosphere, principally the ionosphere. The charged particles in the ionosphere delay GNSS signals passing from satellites to user receivers. This delay can be corrected with varying levels of accuracy using dual frequency measurements (as the delay is proportional to the frequency of the signal) or models which are applied in positioning algorithms. This is a known error source in GNSS positioning and is considered part of normal operations. The interference threat comes from specific solar events which can greatly increase the density of high-energy charged particles.

Solar radiation bursts on contact with the Earth's plasma field cause an increase in the background noise level which can prevent GPS receivers from tracking the signals. As an example, a solar flare was recorded in December 2006 that caused disruption the GPS signal over a large part of the globe. Figure 3 shows the maximum effect of the solar radiation burst through the number of satellites tracked at a selection of GPS monitoring sites. The relative position of the Sun is marked to emphasize the direction from which the radiation burst emanated.

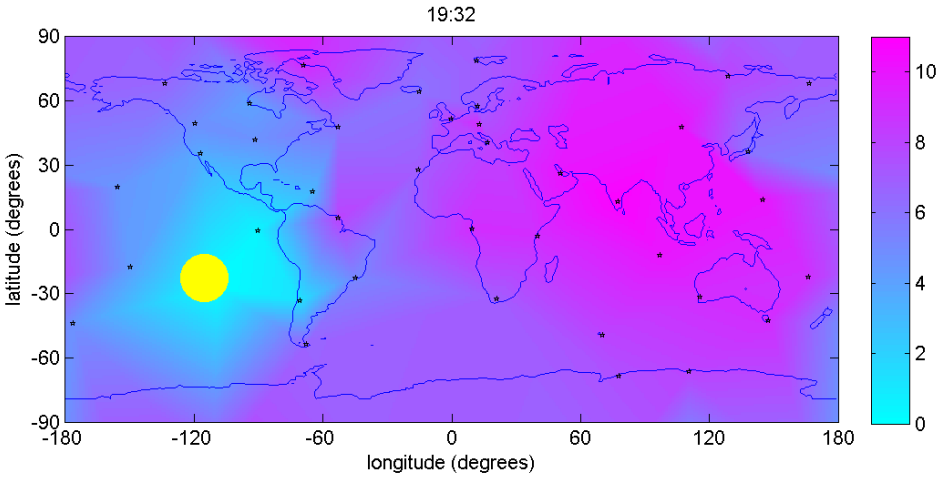

Figure 3: Maximum Effect of the Solar Flare Reported on 6 December 2006

Ionospheric scintillation is caused by irregularities in certain regions of the ionosphere. It causes high frequency scintillation in phase and amplitude (reducing received signal strength) which impairs the ability to maintain tracking, or to acquire, the GNSS carrier signal in the receiver phase lock loop (PLL). As scintillation increases phase tracking noise it principally affects carrier measurements so is usually a concern only for precise carrier phase solutions which would not typically be used in the road application described in section 2. However, in extreme cases of very strong scintillation, if the phase lock cannot be maintained on a particular channel then the satellite signal is effectively lost.

The challenge for DETECTOR is to include mechanisms which can discriminate whether disruption detected at user receivers could have been caused by "out-of-tolerance" ionospheric conditions.

3.1.2 Man-made

Man-made RF interference can be caused by a number of different sources, ranging from television signals to mobile communication devices. Careful management and planning of the RF spectrum internationally by the International Telecommunications Union (ITU), within Europe by the European Conference of Postal and Telecommunications Administrations (CEPT), and nationally by the Office for Communications (Ofcom) minimises the effects however sharing of frequency bands does occur with a primary and secondary users defined.

Television broadcasts have the potential to interfere with GNSS through the harmonics of the primary frequency in the event of a system malfunction or changes to the broadcast that increase the power of the 2nd or 3rd harmonics. In the UK candidate frequencies that could cause this type of interference are:

- Channel 27 (sound centred at 525.25MHz, 3rd harmonic = 1575.75MHz)
- Channel 35 (sound centred at 589.25MHz, 2nd harmonic = 1178.50MHz)
- Channel 38 (sound centred at 613.25MHz, 2nd harmonic = 1226.50MHz)
- Channel 60 (sound centred at 789.25MHz, 2nd harmonic = 1578.50MHz)

Similarly, there is the potential for TV antennas with internal pre-amplifiers to cause interference if the unit malfunctions.

To date, as far as is known, there have been no reports of this kind of interference within the UK, although there have been reports from other areas of the world. For example, in Torino Italy it has been documented that out-of-band interference from TV broadcasts is interfering with GNSS frequencies [RD 7].

Mobile satellite service (MSS) devices operating in the 1610MHz to 1660.5MHz range are another potential source of interference to GNSS. This is because they emit wideband power within the GNSS signal range that can increase the background noise level significantly. It has been reported that a single MSS transmitter could severely disrupt the reception of navigation signals within a range of 50km but this was reported for the satellite transmissions at the high end of the GLONASS frequency range (1609.875MHz to 1615.5MHz). This effect has, however, been reduced with the shifting of the GLONASS frequencies downwards and the use of 12 frequencies instead of the original 24. Should the use of MSS devices become widespread, then a large number of devices in close proximity to a satellite navigation receiver could affect performance.

DETECTOR may not be designed to detect these interference sources directly but it may need to be able to exclude this as a potential cause of any detected disruption.

3.2 Intentional Interference

3.2.1 Jamming

3.2.1.1 Introduction

In the following, a review of GNSS interference and jamming is presented, in order to provide a general description of the intentional threats to be considered in the Detector project. In recent years, interference in GNSS bands has gained increasing attention due to the central role of applications based on satellite navigation systems, including security and tolling systems. In fact, the development of low cost Personal Privacy Devices (PPDs) brought to the widespread utilization of interferers which nowadays

can be found very often in a multitude of environments.

GNSS jamming can be described as the generation of interference that significantly raises the RF noise floor within the satellite navigation band, preventing receivers from acquiring or tracking the incoming satellite signals. For the purposes of the Detector project, it is necessary to dwell deeper into definitions, classifications and actual products that relate to potential interfering threats. In section 3.2.1.2 a review of current literature on GNSS interference is performed, in which the most widespread signal characteristics are described and several implementation details are provided. A broad classification of possible interferers is proposed in section 3.2.1.3, where general signal characteristics have been considered, in order to make the analysis carried out in the Detector project complete and usable both for current and for future jammer implementations. An inspection on the available jammers on the market is then provided in section 3.2.1.4 and the manufacturer specification are reported. The impact of interference on GNSS receivers depends on many factors, such as the interferer power level, bandwidth, and repetition rate; in section 3.2.1.5 the most interesting figures of merit for the evaluation of the impact of interference on receiver performance are presented. Finally, an overview of the countermeasures currently adopted and present in the literature is presented in section 3.2.1.6

3.2.1.2 Current GNSS interferers

Interference effects range from the weak degradation of the positioning performance to the complete obscuration of the satellite signals, thus completely denying navigation services. In recent years, intentional interference events have been experienced, detected and analyzed, which provided information regarding the technical characteristics (transmitter, signal power, bands, waveforms) and the field of utilization (privacy purposes, terrorist attack, denial of service, etc.) of interferers. In particular, different interference measurement campaigns, aimed at identifying and characterizing interferer signals, have been performed. For example, in [RD 18] and [RD 19] the results of a measurement campaign carried out at the Newark International Airport have been published; these analyses were performed on an uncontrolled scenario, where no a priori information on people using jammers was available. As a matter of fact, this measurement campaign has been carried out in order to identify the interference sources and to characterize the emitted signals that caused anomalies in the Ground Based Augmentation System (GBAS) installed in the airport area. The measurement campaign has been carried out during the first months of 2010 and during 2011: hundreds of Radio Frequency Interferers (RFI) have been captured and the measurements have been exploited to perform estimation of the jammers emitting power. It has been observed that interference was due to in-car jammers, used to prevent people from being tracked or as a fraud attempt against charging systems. The results of [RD 18] show that most of the interferers are frequency modulated (FM) signals with different bandwidths and different spectra: Figures 4 to 7 show different examples of the demodulation of FM interferers: it is possible to observe that all of them can be modelled as sawtooth waveforms or superimpositions of them, with different durations and different “chirps”. The resulting FM signal can then be expressed as:

$$x(t) = A * \exp\left(j2\pi\varphi(t)\right) \quad (1)$$

where

$$\varphi(t) = \sum_{h=0}^{\infty} \left(\int_0^t f_{LO}^{(1)}(\tau - hT^{(1)})d\tau + \cdots + \int_0^t f_{LO}^{(N)}(\tau - hT^{(N)})d\tau \right) \quad (2)$$

and

$$f_{LO}^{(n)}(t) = \begin{cases} f_0^{(n)} + \alpha_U^{(n)} t, & \text{for } 0 \le t \le T_U^{(n)} \\ f_0^{(n)} + \alpha_U^{(n)} T_U^{(n)} + \alpha_D^{(n)} \left(t - T_U^{(n)} \right), & \text{for } T_U^{(n)} \le t \le T^{(n)} \end{cases} \quad (3)$$

being $f_{LO}^{(n)}(t)$ the *n*-th modulating sawtooth waveform, $\alpha_U^{(n)}$ and $\alpha_D^{(n)}$ the positive and negative chirps of the sawtooth function respectively, $T^{(n)}$ the duration and $f_0^{(n)}$ the initial frequency of the *n*-th waveform.

The term chirp is used in this context since the FM waveform determines an equivalent behaviour of the instantaneous frequency: in practice, the time representation of the demodulated FM signal corresponds to the time representation of the instantaneous frequency of the RFI: the bandwidth of the resulting RFI thus changes according to the demodulated signal.

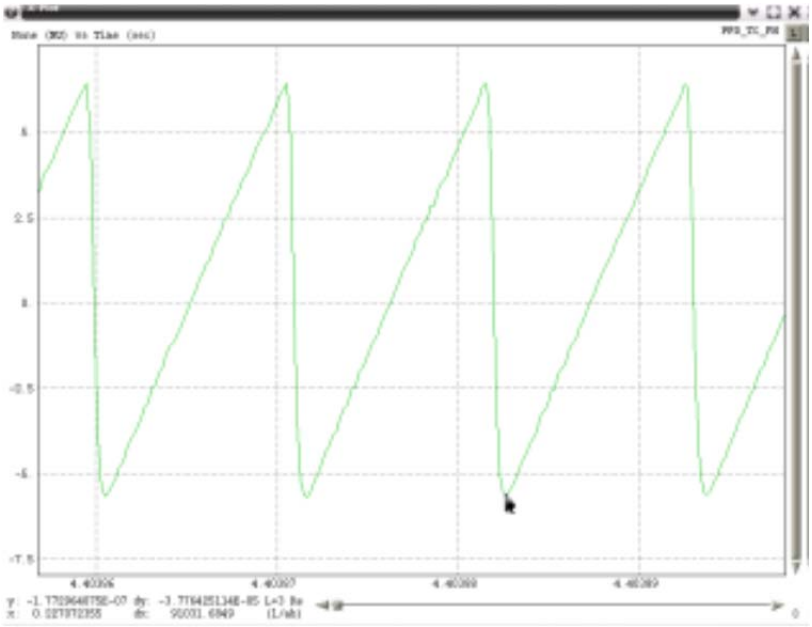

Figure 4 FM demodulated signal: time domain representation; E.g. 1 ([RD 18])

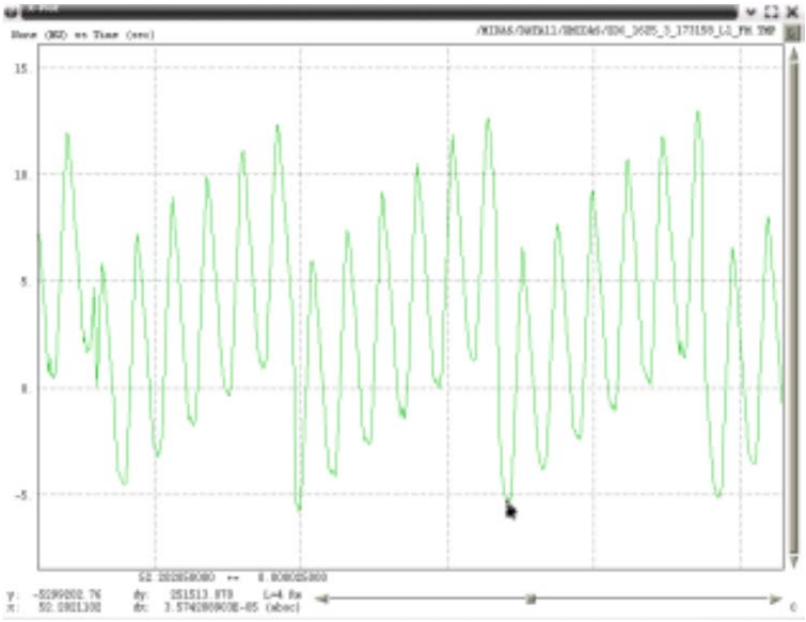

Figure 5 FM demodulated signal: time domain representation; E.g. 2 ([RD 18])

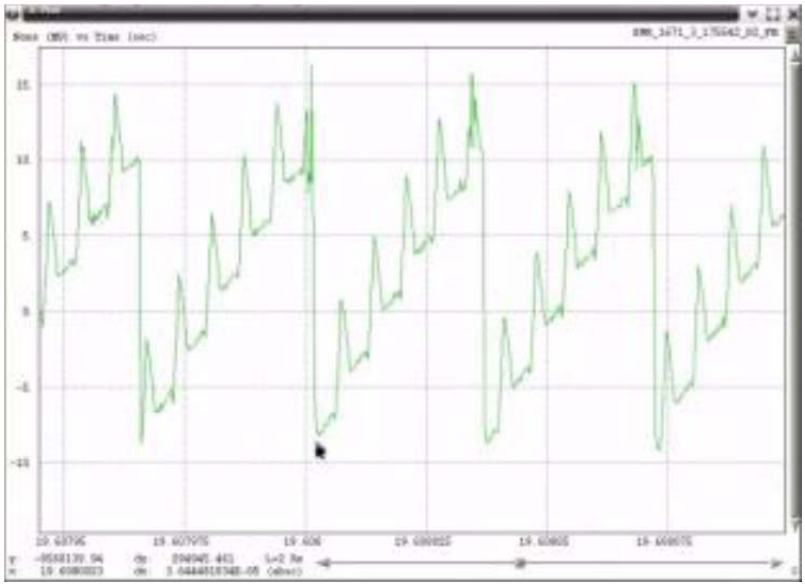

Figure 6 FM demodulated signal: time domain representation; E.g. 3 ([RD 18])

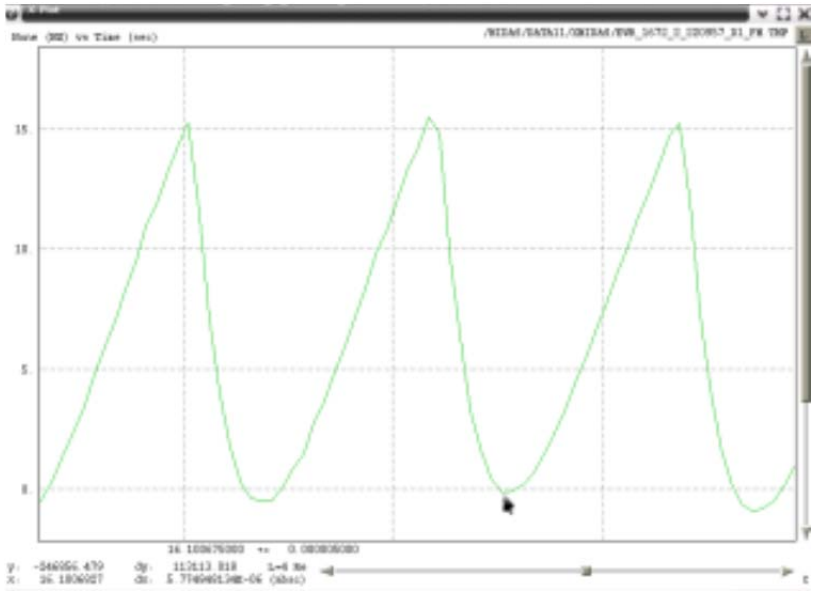

Figure 7 FM demodulated signal: time domain representation; E.g 4 ([RD 18])

Examples of RF spectra of RFI are plotted in Figure 8: it is possible to observe that all the signals are wideband, but they can be very different: the bandwidth changes as well as the central frequency position.

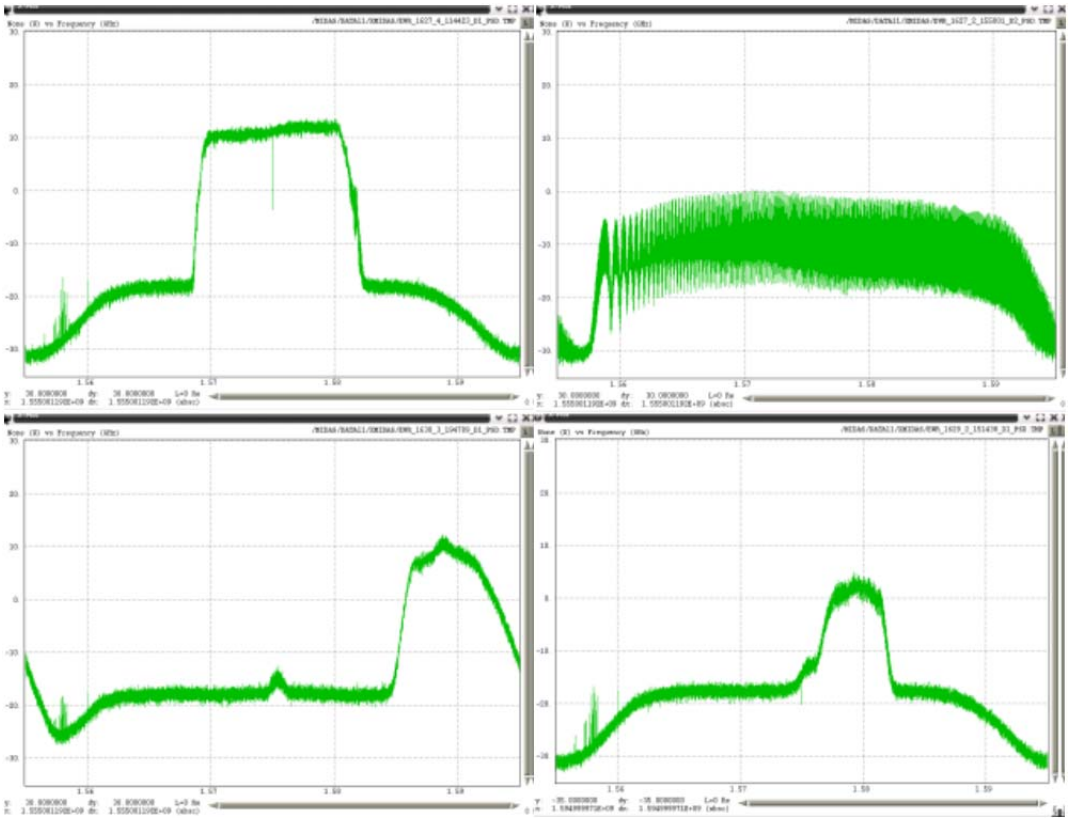

Figure 8 RF spectra (@[1562,1582] MHz) ([RD 18])

As already noted, these signals are the result of measurements performed by devices that are in fixed positions without knowledge on the jammer positions, thus making the correct estimation of the RFI parameters more difficult.

A different measurement campaign has been recently performed, the results of which are published in [RD 20] and [RD 21], on a controlled scenario on a selected set of seven jammers which have been chosen as the most present on the market (shown in Figure 9).

Figure 9 In-car low cost jammers ([RD 20])

Also according to this study, the vast majority of interferers are FM signals as those previously described, i.e. characterized by sawtooth waveforms, the exception being those jammers which transmit simple narrow band (less than 1 kHz) continuous wave (CW) signals. Examples of the RF instantaneous frequencies of the RFI transmitted by two different jammers are represented in Figure 10 and Figure 11: in particular in Figure 10 the instantaneous frequency of a signal modulated by a single sawtooth is represented, while in Figure 11 the effect of the superimposition of two different sawtooth waveforms is shown.

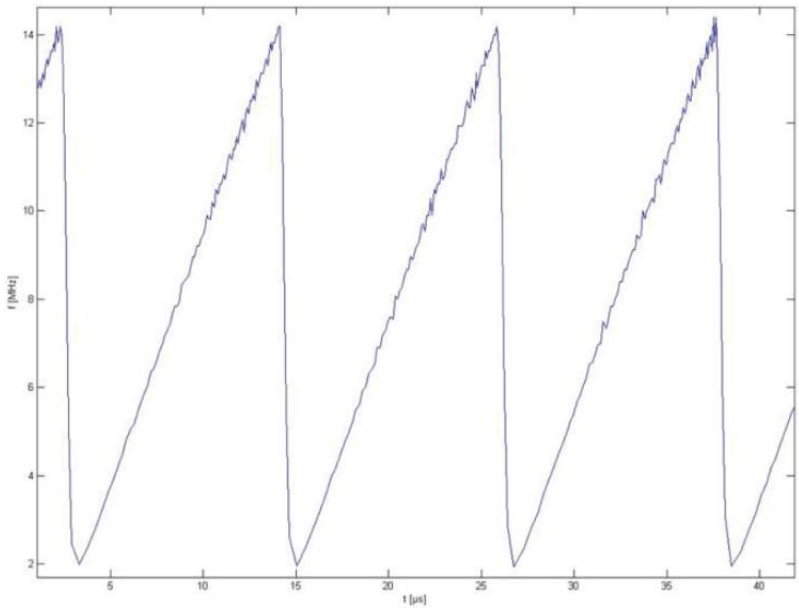

Figure 10 RF instantaneous frequency vs time: example 1 ([RD 20])

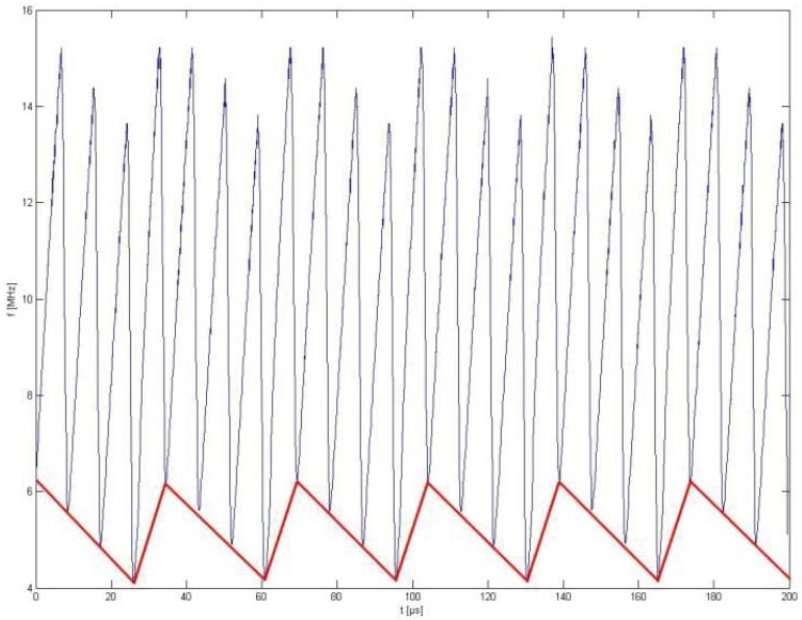

Figure 11 RF instantaneous frequency vs time: example 2 ([RD 20])

The previous interferers can be generated very easily according to the scheme of Figure 12: the jammer needs a number of oscillators equal to the number of sawtooth waveforms to be generated, and a voltage controlled oscillator that modulates the carrier frequency signal. This scheme results in a very cheap solution that justifies the success and the large diffusion of this kind of devices in the market of PPDs.

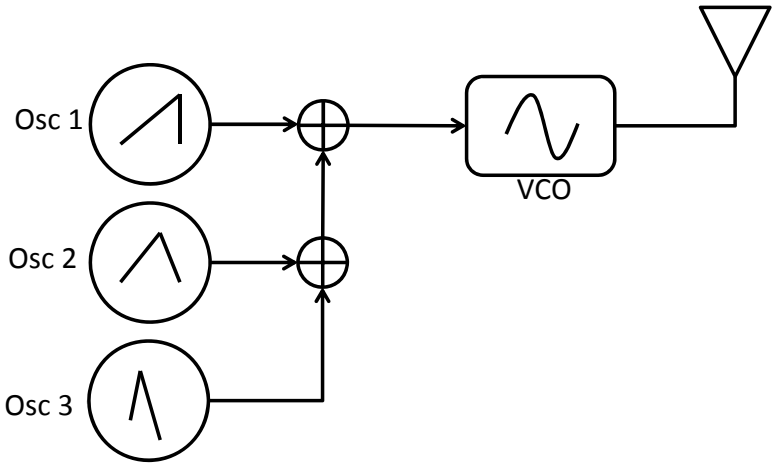

Figure 12 Generic schematic of an in-car jammer

3.2.1.3 Classification of GNSS interference

In this section, several classes of interferers are identified in order to take into account not only current interferers, but also possible different implementations, thus making the Detector characterization core amenable to future use. In order for any classification to be useful, we must accept the assumption that the interference level allows signal processing. Vice versa, when the receiver is fully jammed by the interference power, we simply speak of saturating interference. The identified interferer classes are distinguished according to two macro-criteria:

1. *Signal energy distribution*, providing different signal characteristics in the time, frequency and joint time-frequency domains.
2. *Signal source mobility*, which modifies several characteristics of the signal the GNSS receiver side, such as power or frequency.

As shown in Figure 13, the two above macro classes are further split using six specific criteria (**T1**, **T2**, **F1**, **TF1**, **TF2**, **M1**) described in the following:

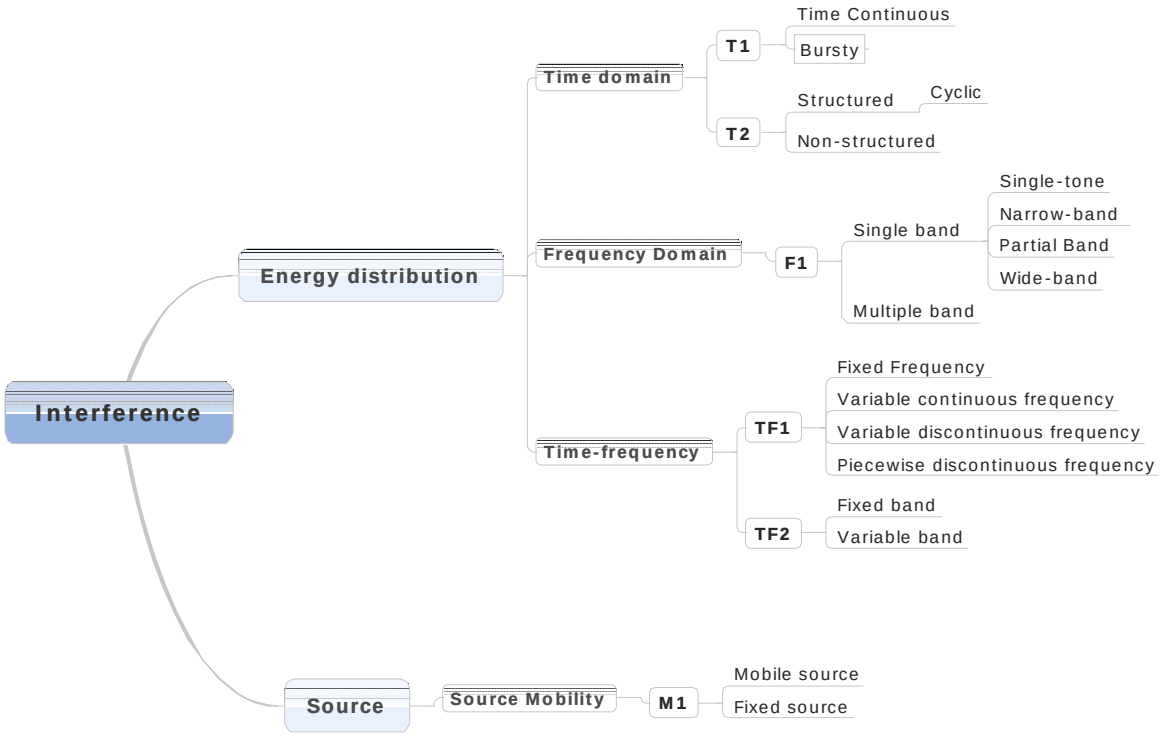

Figure 13: Interference classes

3.2.1.3.1 Assumptions and Definitions

In order to properly define the notation used throughout this deliverable, it is worth to define the minimal set of mathematical notations. In the following complex signals, which can be represented as complex functions of time, are considered. More specifically:

$$x(t) : \mathbb{R} \to \mathbb{C}$$

Signals can be divided in two classes: *finite energy signals* (FES) and *finite power signals* (FPS). Let E be the signal energy:

$$E = \lim_{T\to\infty} E(T) = \lim_{T\to\infty} \int_{\frac{-T}{2}}^{\frac{T}{2}} |x(t)|^2 \, dt \qquad (4)$$

and let P be the signal power:

$$P = \lim_{T\to\infty} P(T) = \lim_{T\to\infty} \frac{1}{T} \int_{\frac{-T}{2}}^{\frac{T}{2}} |x(t)|^2 \, dt \tag{5}$$

Signals satisfying the condition

$$0 < E < \infty$$

are defined as *Finite Energy Signals*, while signals satisfying the condition

$$0 < P < \infty$$

are called *Finite Power Signals.* It is worth noting that for FES the Fourier transform always exists.

Considering frequency domain representations, it is useful to introduce the *Energy Spectral Density* (ESD) and the *Power Spectral Density* (PSD). The ESD of a FES $x(t)$ is defined as:

$$S_E(f) = \mathcal{F}\{\mathcal{R}^{\mathrm{E}}(\tau)\} \tag{6}$$

that is the Fourier transform of $\mathcal{R}^{\mathrm{E}}(\tau)$, being $\mathcal{R}^{\mathrm{E}}(\tau)$ the FES autocorrelation function:

$$\mathcal{R}^{\mathrm{E}}(\tau) = \int_{-\infty}^{\infty} x(t+\tau)x^*(t) \, dt \tag{7}$$

Similarly, the PSD of a FPS is defined as:

$$S_P(f) = \mathcal{F}\{\mathcal{R}^{\mathrm{P}}(\tau)\} \tag{8}$$

where $\mathcal{R}^{\mathrm{P}}(\tau)$ is the FPS autocorrelation function:

$$\mathcal{R}^{\mathrm{P}}(\tau) = \frac{1}{T} \int_{-\infty}^{\infty} x(t+\tau)x^*(t) \, dt \tag{9}$$

For both FES and FPS we define the *Time Limited ESD (TL-ESD)*

$$S_T(t,f) = \left| \int_{t-T/2}^{t+T/2} x(\xi) e^{-j2\pi f\xi} d\xi \right|^2 \tag{10}$$

that is the Fourier transform on a limited support of the time domain.

3.2.1.3.2 Time domain classification

Considering the energy distribution in the time domain, we identify two classification criteria, which give origin to different classes:

- **T1 criterion:** *continuity* of the signal energy in the time domain. According to this criterion, we identify the following classes:
    - *Time continuous interferer:* signals characterized by the absence of interruptions during the interfering source activity period.
    - *Bursty interferer:* signals characterized by the presence of interruptions which can be periodic or (*pseudo*-) random. This kind of interferers can be modelled as:

$$x(t) = \sum_k s_k(t)\text{rect}\left(\frac{t - T_k}{\tau_k}\right) \quad (11)$$

where $s_k(t)$ is a generic time continuous signal (as previously defined), and T_k and τ_k are the k-th event instant of occurrence and duration, respectively. As a particular case of bursty interferers, we identify:

- *Time-hopping interferer,* that can be expressed as:

$$x(t) = \sum_k s(t)\text{rect}\left(\frac{t - T_k}{\tau}\right) \quad (12)$$

  where T_k is considered as a random variable which can take any of the possible values in a given time slot.

- *Pulsed interferer,* that can be expressed as:

$$x(t) = \sum_k s(t)\text{rect}\left(\frac{t - kT}{\tau}\right) \quad (13)$$

  where the signal is periodically repeated, with period T.

- **T2 criterion:** presence of structure in the signal. According to this criterion we identify the following classes:
  - *Structured interferer*: deterministic signal with a structure which can be identified repeatedly over the time axis. The signal structure can be identified in the amplitude or in the frequency domains. A structured signal can be expressed as:

$$x(t) = \sum_k a_k s(t - T_k)\text{rect}\left(\frac{t - T_k}{\tau}\right) e^{j2\pi f_k t} \quad (14)$$

    in case of structured amplitude, or in the form:

$$x(t) = \text{A} * \exp\left\{j2\pi \int_0^t \sum_{k=0}^{\infty} a_k s(\tau - T_k)\text{rect}\left(\frac{t - T_k}{\tau}\right) d\tau\right\} \quad (15)$$

    in case of structured frequency, being T_k the k-th time shift, and a_k a scaling factor possibly described as a random variable. As a particular case:

    - *Cyclic interferer*: signals having a cyclically repeated structure, which can be expressed as:

$$x(t) = \sum_k a_k s(t - kT)\text{rect}\left(\frac{t - kT}{\tau}\right) \quad (16)$$

      in case of cyclic amplitude structure repetition, or in the form:

$$x(t) = \text{A} * \exp\left\{j2\pi \int_0^t \sum_{k=0}^{\infty} a_k s(\tau - kT)\text{rect}\left(\frac{t - kT}{\tau}\right) d\tau\right\} \quad (17)$$

in case of cyclic frequency structure repetition.

- *Non-structured Interferer*: signals that have no identifiable deterministic structure.

Note that periodic signals are a particular case of cyclic signals. This classification allows to describe a very wide class of signals having specific characteristics in the time domain: for example, the pulsed interferer

$$x(t) = \sum_k s(t - kT)\mathrm{rect}\left(\frac{t - kT}{\tau}\right) \tag{18}$$

can be described as a time-hopping, structured signal.

Moreover, it is worth noting that the FM modulated interfering signals described in section 3.2.1.2 can be seen as time-continuous, structured signals; this characterization also allows to include a much larger variety of signals, thus generalizing the scope of the analysis.

3.2.1.3.3 Frequency domain classification

In the frequency domain we consider the spectral form of the received signal; we then define the following

- **F1 criteron**: continuity of the signal energy in the frequency domain. According to this criterion we identify the following classes:
  - *Single band interferers*: signals with energy concentrated in a single band of any size. This is the case of most of the implementable signals. In general, the ESD/PSD (respectively for FES and FPS) of a single band interferer can be expressed as:

$$S(f) = S'(f)\mathrm{rect}\left(\frac{f - f_0}{B}\right) \tag{19}$$

where $S'(f)$ is a generic non-zero function in f, and B is the maximum signal bandwidth. As particular cases, four sub-classes are identified according to the frequency interval of the interfering signal:

- Single-tone if $B < \xi_{ST}$;
- Narrowband if $\xi_{ST} < B < \xi_N$;
- Partial-Band if $\xi_N < B < \xi_{PB}$;
- Wideband if $B > \xi_{PB}$.

With reference to the GNSS L1 signal bandwidth, we assume the following values: $\xi_{ST} = 1$ kHz, $\xi_N = 1$ MHz, $\xi_{PB} = 10$ MHz.

  - *Multiple bands* interferers are signals with energy spread in multiple bands, separated by intervals larger than ξ_N. This means that a single interferer holds different frequency components. In general, a multiple band interferer ESD/PSD can be expressed in the form:

$$S(f) = \sum_k S_k'(f)\mathrm{rect}\left(\frac{f - f_k}{B_k}\right) \tag{20}$$

where B_k and f_k are respectively the bandwidth and the central frequency of the *k*-th component.

3.2.1.3.4 Time-Frequency domain

The time–frequency analysis comprises those techniques that consider the signal characteristics in the time and frequency domains jointly. Each signal is studied in a two-dimensional domain to better understand how time-frequency properties are distributed.

In order to characterize the time-localized frequency characteristics of the considered signals, we introduce the following definitions:

- *Instantaneous frequency* $f(t)$, which is the derivative in time of the signal phase $\Phi(t)$:

$$f(t) = \frac{d}{dt}\Phi(t) \tag{21}$$

- *Time-limited band* $B_T(t)$

$$B_T(t) = \left\{ [f_{\min}, f_{\max}] \quad \text{such that} \quad \int_{f_{\min}}^{f_{\max}} S_T(t,f)df = 0.9E(T) \right\} \tag{22}$$

where $E(T)$ is the energy of the received signal defined in equation (4).

Considering the energy distribution in the joint time-frequency domain we identify two possible classification criteria:

- **TF1 criterion**: instantaneous frequency variability. According to the dependence on time of the instantaneous frequency, we distinguish the following classes:
  - *Fixed frequency Interferer:* signals with constant instantaneous frequency;
  - *Variable continuous frequency interferer*: signals with instantaneous frequency changing continuously. Here we consider only linear an exponential chirp, which are respectively:

$$\begin{cases} f(t) = f_i + \alpha t \\ f(t) = f_i \lambda^t \end{cases} \tag{23}$$

    where f_i is the starting frequency and α and λ are the *chirp rates*, i.e. the rates of frequency increase/decrease that we assume constant in time
  - *Variable discontinuous frequency interferer*: signals with instantaneous frequency only changing abruptly, i.e.

$$f(t) \text{ discontinuous function}$$

  - *Piecewise discontinuous frequency interferer:* signals with instantaneous frequency changing both abruptly and continuously.
- **TF2 criterion:** Time-limited band variability. Considering how the allocation of the energy in the frequency domain changes in time, we identify two classes:
  - *Fixed band interferer*, characterized by $B_T(t)$= constant.

- *Variable band interferer,* characterized by $B_T(t) \neq$ constant.

It is worthwhile noting that the band definition also depends on the observation period duration T, which is not a parameter of the interferer signal.

3.2.1.3.5 Source Mobility classification

In order to consider not only the emitted interferer characteristics but also the effects of the source mobility on the signal, we introduce here the following criterion:

- **M1 criterion**: interference source mobility:
  - *Mobile source interferer:* signal transmitted by a mobile source;
  - *Fixed source interferer:* signal transmitted by a fixed source.

  The source mobility makes the received signal change according to the relative positions and velocity with respect to the receiver. The main effect of the mobile interferer source is that the Doppler frequency changes in time, causing Doppler spread. Furthermore, this effect determines a power change at the receiver side, greatly affecting GNSS receiver performance in signal detection.

3.2.1.4 GNSS Jammers: State-of-the-art

In this section, several data sheets with the main characteristics of the currently available jammers are provided. Except for very few cases, no information is given on the type of jamming signal adopted. However, some interesting information is provided:

- Operating band: frequency range or band at which the interferers operate;
- Gain: transmission antenna gain;
- Polarization: transmission antenna polarization;
- Antenna type: antenna diagram or structure;
- RF power capacity: maximum emitted RF power;
- Range: specified jamming range;

It must be noted that the range specification is not univocally related to the transmitted power level. It is simply a figure specified in the data-sheets.

ID	Manufacturer	Code	Jamming Mode	Operating band	Gain	Polarization	Antenna Type	RF Power Capacity	Range
1	Antenna Experts	JD-1018		1000-1800 MHz	2.5 dBi	Vertical	Omnidirectional	500 W	
2	Antenna Experts	JD-1850		1800-1880 MHz	10.0 dBi	Vertical	Omnidirectional	150 W	
3	Antenna Experts	JD-1820		1800-2000 MHz	3.0 dBi	Vertical	Omnidirectional	250 W	
4	Iran Electronic Industries	LBJ-50 & LBJ-200	Single Tone, Multiple Tones, Barrage for GPS, GLONASS Sweep and special algorithm for satellite	1000-2000 MHz	9.0 dBi	Circular clockwise	Directional Helix	50,200 W	
5	C.T.S. Technology Co., Limited	CTS VIP150G		Civil GPS at L1: 1565.42-1585.42 MHz Civil GPS at L2: 1217.60-1237.60 MHz Civil GPS at L5: 1176.45 MHz for critical and non-critical safety applications				150 W	100-400 m
6	C.T.S. Technology Co., Limited	CTS JG003		GPS L1/L2/L5 bands				1 W	20-30 m

7	C.T.S. Technology Co., Limited	CTS GBOX		GPS L1/L2/L5 bands				25 W	Up to 30 m
8	C.T.S. Technology Co., Limited	CTS BBOX		GPS L1/L2/L5 bands				100 W	500-1000 m
9	C.T.S. Technology Co., Limited	CTS-1000H125	Multiple Band	GPS L1/L2/L5 bands				2.4 W (800 W for each band)	10-20 m
10	C.T.S. Technology Co., Limited	CTS.3000A /B	Multiple Band	GPS L1,L2,GSM 900/1800, 850/1900 MHz CTS-3000B: GPS L1,L2,L3,L4,L5				12 W (0-4 W for each band)	10-20 m
11	C.T.S. Technology Co., Limited	CTS-JG3		GPS L1/L2/L5 bands				1 W	10-50 m
12	C.T.S. Technology Co., Limited	CTS.JG005		GPS L1/L2/L5 bands				200 mW	Up to 7 m
13	C.T.S. Technology Co., Limited	CTS.JG001		GPS L1/L2/L5 bands				200 mW	Up to 6 m
14	C.T.S. Technology Co., Limited	CTS.JG002		GPS L1/L2/L5 bands				200 mW	Up to 8 m
15	C.T.S. Technology Co., Limited	CTS.G5	Multiple Bands	GPS L1/L2/L5 bands			Omnidirectional	6 dBm for each band	10-15 m

16	C.T.S. Technology Co., Limited	CTS.GBOXG		GPS L1/L2/L5 bands				30 W	30-80 m
17	C.T.S. Technology Co., Limited	CTS.GBOG		GPS L1/L2/L5 bands				35 W	30-80 m
18	TanGreat Telecommunications Technology Co., Ltd	TG-VIP MB 1.0		GPS 1520-1580 MHz				360-500 mW	300-500 m
19	General Electric	AN/ALT-6	Continuous Wave	1-10 GHz				150 mW	
20	Shenzhen Wel-Try Technology Limited Shenzhen Qunxin Electronics Co., Ltd.	CGRJ4000		GPS L1 1575.42 MHz			Omnidirectional	2.5 W	Up to 20 m
21	Shenzhen Eastlonge Electronic Factory	EST-505F		1500-1600 MHz				2 W (5 dBm/30 KHz density)	Up to 50 m
22	Shenzhen Joint Technology Co., Ltd	GP5000		GPS L1 1575.42 MHz				21 dBm	1-5 m
23	Radixon Hadrian	RJ-G1575	Wideband Noise					Up to 1 W	

3.2.1.5 Interferers Impact on GNSS receiver performance

Due to the very low power of the GNSS signal the effect of interferers sent from localized emitters can strongly degrade the performance of the receivers. In [RD 9] and [RD 10] it is shown that also a simple 1 Watt emitter can jam most of the civil GPS receiver in a perimeter of kilometers from the source position. Such a problem led to the establishment of the maximum power level of interference at the antenna of a GPS receiver: institutions as the RTCA, have specified the profile of the maximum tolerable interference level in the GPS band [RD 11] in order to obtain satisfactory accuracy and reliability.

In general, the impact of an interferer on a receiver depends on the characteristics of the received signal. The analysis of the impact is not straightforward, however several examples are available in the literature: an extensive analysis of the impact of narrowband and partial-band continuous interferers on GNSS receivers is carried out in [RD 24] and [RD 23]: in these articles the effect of interferers whose power is concentrated in part of the receiver front end bandwidth is assessed by determining an effective figure of merit allowing to evaluate the performance of the acquisition, tracking and message demodulation tasks. The quality of a GNSS received signal can be described in terms of the effective C/N_0, that describes how the combination of partial band interference and noise affect the receiver functions of carrier tracking, data demodulation and acquisition. The $(C/N_0)_{\text{eff}}$ compared with its undisturbed value C/N_0 describes the degradation of the effective carrier-to-noise-density ratio caused by the presence of interferers. It is defined as:

$$\left(\frac{C}{N_0}\right)_{\text{eff}} = \frac{\frac{C}{N_0}\int_{-\beta_r}^{\beta_r} G_s(f)\mathrm{d}f}{\int_{-\beta_r}^{\beta_r} G_s(f)\mathrm{d}f + \frac{C_l}{N_0}\int_{-\beta_r}^{\beta_r} G_l(f)G_s(f)\mathrm{d}f} \tag{24}$$

where C is the received signal power, N_0 is the thermal noise power spectral density, C_l is the interference power, β_r the RF front-end bandwidth, $G_s(f)$ the normalized equivalent two-sided base band expression of the Power Spectral Density (PSD) of the desired GNSS signal and $G_l(f)$ the normalized equivalent two-sided base band expression of the PSD of the interference signal. The impact of interference is proportional to the k_{ls} factor

$$k_{ls} = \int_{-\beta_r}^{\beta_r} G_l(f)G_s(f)\mathrm{d}f \tag{25}$$

identified as Spectral Separation Coefficient (SSC). This factor accounts for the interaction of the interfering spectrum with the reference signal in the receiver, thus describing the filtering effect of the correlation on the interference signal and providing a quantitative measure of the interfering impact.

A different tool for the assessment of the impact of interference on GNSS systems is presented in [RD 12]: here the impact of interferers generated by systems working in adjacent bands is evaluated in terms of Interference Error Envelope (IEE): the IEE is defined as a measure of the maximum distortion of the discriminator function with respect to one (or more) parameters of the interfering signal: the worst case corresponding to the maximum and minimum ranging error values (expressed in meters) are plotted versus one

of the variable interference characteristics being considered (e.g. the carrier frequency, for a continuous wave interferer).

In general it is not possible to asses which jammers have the strongest impact on GNSS receiver performance; however the presented tools provide figures of merit that allow an objective impact measurement to be obtained.

3.2.1.6 Current countermeasures: detection and mitigation

For the purposes of the Detector project, it is useful to review the state-of-the-art techniques to counter interference effects. Due to the increasing reliability requirements, the positioning systems must be robust against interference, either intentional (such as jammers) or unintentional. Being direct sequence spread spectrum (DS-SS) systems, GNSS signals are inherently robust against interference. However, this intrinsic robustness vanishes when the interferer power becomes too large with respect to the useful signal power, which is typically very low. In this case other countermeasures become necessary: in the literature several techniques are present, that can be classified in 2 categories: detection and mitigation. Detection techniques are needed to identify the presence of interferers, while mitigation techniques are aimed to eliminate interference from the received signal, e.g. by means of filtering, or by means of beam-forming techniques.

In [RD 13] and [RD 14] the authors develop a network of low cost devices able to detect and localize interference sources by exploiting the observation after the Automatic Gain Control (AGC) logic; in fact in GNSS receivers, where the signal power is below that of the thermal noise floor, the AGC is driven by the ambient noise environment rather than the signal power. As a result, AGC can be a valuable tool for assessing the operating environment of a GNSS receiver [RD 15], since it leads to a good trade of between resource consumption and detection performance. The fundamental drawback of this approach is that this technique cannot be adopted when Components-Off-The-Shelf (COTS) are used to implement positioning functionalities and the monitoring of anomalies affecting the positioning solutions can only be performed processing the outputs of the chipset itself. In order to provide solutions to this problem in [RD 17] a different approach based on the observation of the post correlation C/N_0 statistics is proposed. Another solution is provided in [RD 16] based on the observation of the autocorrelation function shape, obtained by means of multi-correlator tracking circuits: according to this technique several interference characteristics are estimated using different methods monitoring the correlators outputs.

Examples of mitigation techniques are provided in [RD 25], [RD 26], [RD 27], [RD 28]: in these articles several interference rejection techniques operating in the time, frequency or in the space domains are proposed; the major drawback of these techniques is that operate only in a single domain, that gives advantages if the interferers have a fixed or slow-varying signature in the considered domain but otherwise are not optimal. In [RD 29] a joint Time-Frequency Domain Interference Mitigation (TFDIM) has been proposed for narrowband interference mitigation. In general, joint domain techniques are very useful to face interferers that are concurrently variable in more than one domain, because they provide additional degrees of freedom to distinguish the undesired signal from the useful contribution.

Mitigation will not be included in the purposes of the Detector project, but it is worth noting that the adoption of this kind of techniques is crucial to guarantee the reliability of the GNSS systems. Since mitigation is generally based on the knowledge of interference characteristics, the analysis tools that will be developed for Detector, aimed to enhance the awareness on interference, will strongly contribute to improve the reliability and the efficiency of future GNSS systems.

3.2.2 Spoofing

A spoofer emits a GNSS-like signal at a power a little above that of the incoming satellite signals. The presence of this signal of higher power causes a receiver to preferentially lock onto the false signal and not the real signal. This type of jamming is most effective against civil receivers since the pseodorandom noise (PRN) codes modulated onto the GPS carrier are in the public domain. Access to the military codes is strictly controlled to prevent this kind of attack.

With a comprehensive spoofer it is possible to spoof multiple channels and create false satellite signals which would cause the receiver to compute a consistent but wrong user position. Over time an entirely false trajectory could be generated. This type of attack is likely to be more coordinated and sophisticated that “normal” interference and certainly could not be caused innocently by someone who is only concerned about protecting their own privacy. It is not considered a principal concern for the DETECTOR design.

A significant and sustained spoofing attack would be easily detectable though using static receivers in a monitoring network. If receivers are continually operating and compute and report their own position, significant changes in this position would soon be identified.

3.2.3 Meaconing

Meaconing is the reception of real GNSS signals at one location and their re-broadcast at a different location at a slightly higher power. Technically it could be described as a form of spoofing using real signals, but to the user the receiver would still appear to be providing correct positions. The disadvantage of meaconing is that once detected the location of the source is known through the position information derived from the signals.

Like spoofing, meaconing is not considered one of the common interference sources which is likely to disrupt road applications relying on GNSS, so it is not considered a high priority within the DETECTOR project.

4 Early Interference Detection within DETECTOR

4.1 Objectives

The DETECTOR project was motivated by the need to detect jamming/interference that can give rise to problems in the use of GNSS services for critical road applications. In §3.2.1 a review of current GNSS interferers was presented with an analysis of the impact such devices can have on a GNSS receivers. This includes examples of jammers which have been detected in previous studies.

This section describes some initial investigations to determine if interference events could be detected in a similar way to previous studies (reported in §3.2.1.2) using some readily available datasets in the UK. This helps to better understand the nature of the interference threat which DETECTOR is addressing in terms of the type of jammers which are in use and the prevalence of their use. This is not a study which can quantify the number of jamming events which may be occurring in a comprehensive way but it helps determine if the levels of jammer use reported particularly in US studies are likely to be replicated elsewhere. It can also give an early indication of whether interference events are detectable using non-dedicated datasets or whether jammers need to be introduced in controlled trials in order have an interference source to analyse. By attempting to replicate the process followed in some previous studies it helps evaluate the state of existing components, datasets and proposed algorithms for the DETECTOR solution and identifies where future effort needs to be focused.

The objectives of this study are to:

- Make a preliminary assessment of the current level of threat from interference sources in road applications and to compare this against results from existing reports
- Help identify which locations or types of area are more likely to experience jamming, which can help inform further study or field trials
- Refine detection algorithms, tuning thresholds to prevent unacceptable levels of false alarms (event which trigger interference detection but are in fact simply part of nominal performance).
- Refine characterisation algorithms, in the event that events are detected
- Consolidate a number of hardware and software design aspects, e.g. antenna placement

4.2 Methodology

The approach taken in this investigation was first to determine whether interference events could be detected using data which is routinely being recorded for other purposes. NSL subscribes to a commercial service which gives access to data from continuously operating reference stations (CORS) located in the British Isles. This provides access to observation and navigation data in RINEX format from over 100 sites in Great Britain and Ireland. The dataset allows the position of the station to be estimated using existing PVT (Position Velocity Time) software at NSL. By comparing the estimated position against the

known reference coordinates it is possible to detect large errors in the observations provided. RINEX observation files also include the SNR values for all tracked satellite which can be monitored as another indicator of potential interference.

This network of stations was established primarily to serve the land survey and geodetic communities, so receivers tend to be located on roof tops and open sites with clear sky views. They are not deliberately sited next to roads however some are actually quite close. For this investigation a set of four stations was selected in areas where it was thought most likely that jammers may be detected. These stations were sited close to major roads in urban areas and in one case, close to a port. Data from these sites was processed to determine if interference events could be detected. Some sample results from this analysis are shown in section 4.3.

Having found sites where interference events appear to be detected quite frequently a dedicated test was then set-up to collect RF data in this area to allow a more comprehensive investigation and to calibrate the more coarse detection approaches.

As well as investigating a single UK site in more detail, datasets from permanent reference sites around Europe were also processed to see if similar trends were detected elsewhere.

4.3 SNR monitoring of Reference Stations

From analysing position solutions and SNR values for the selected sites a number of "events" were detected. In this context an "event" is an identified period where the observations at a site were not as expected. This is based principally on detecting significant drops in SNR which affect more than one satellite. Care needs to be taken before concluding that an event is due to intentional interference or jamming. Other factors which may lead to similar behaviour can include multipath, internal receiver tracking problems and unintentional interference sources.

Multipath should not be a significant factor as the antennas should be positioned away from reflective surfaces as much as possible. Despite this there are cases of multipath effects at reference stations, but these are identifiable as multipath will usually only affect one or two satellites at a time, it is related to satellite azimuth and elevation, and if it is genuine multipath signature the pattern is repeated daily.

Figure 14 shows the SNR from all satellites tracked at a selected reference site in London over 24 hours on a Wednesday in March 2012. The regular "arcs" from low SNR to a peak and then back down again are a characteristic feature of normal conditions and mirror the elevation angle of the satellites as they pass over the site. The more interesting features in this investigation are the cases of sudden drops in SNR. Four different detection thresholds have been set which reflect different severity levels of this SNR drop, considering the magnitude of the change (in dB), the number of satellites affected and whether signals continue to be tracked or not. The coloured crosses on the plot indicate which in each of these thresholds have been triggered. In this example there are 8 events which have triggered detection and therefore warrant further analysis.

Figures 15 and 16 are "zoomed in" periods from this day which show the SNR changes during some of these events in more detail. It is clear that all satellites signals are affected over periods of 30 seconds and more.

Figures 17 and 18 show results from performing similar analyses at sites in Budapest and Paris respectively. Similar events can be identified. In the case of Budapest the SNR is significantly degraded by up to 15dB for a period of almost 7 minutes, with signal from 4 of the 9 satellites in view being lost altogether. In Paris these is a five minute disturbance in which some satellite tracking is lost altogether and other signals show a drop of over 10dB.

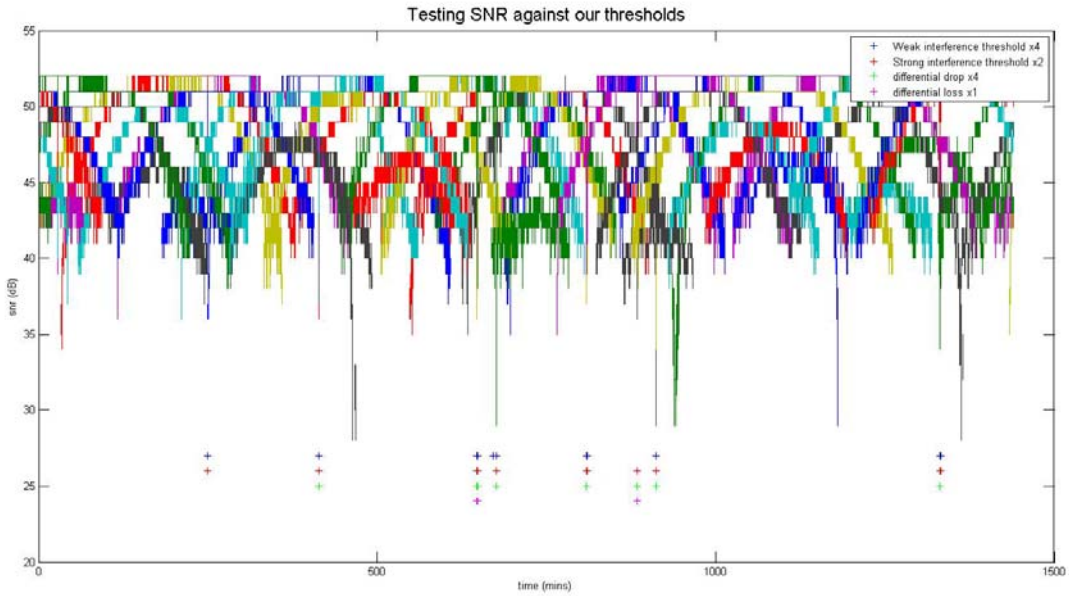

Figure 14: SNR plot of a London site with detection flags

Figure 15: Zoomed in on a portion of Figure 14

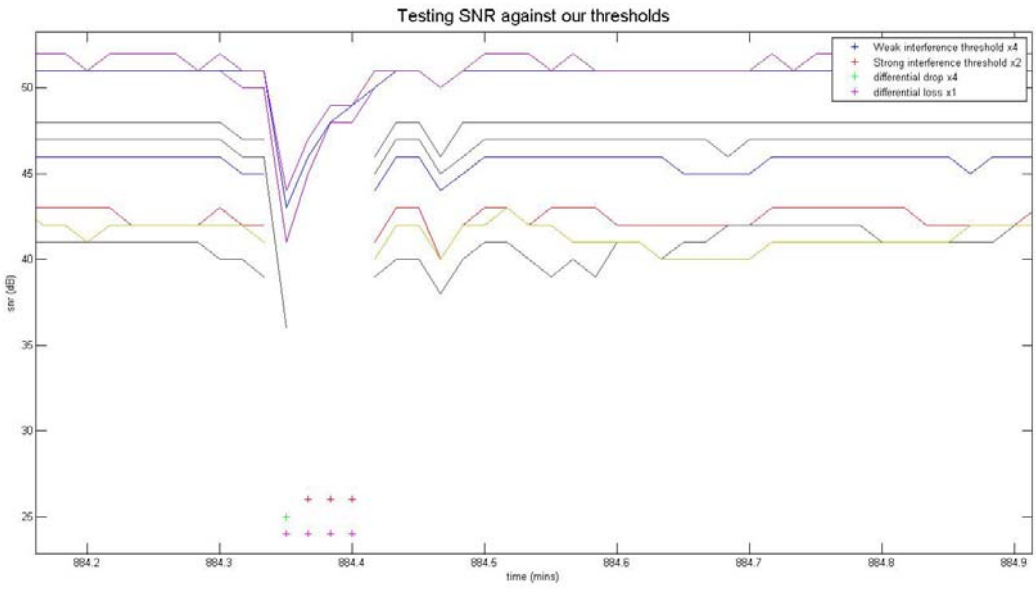

Figure 16: Zoomed in on a portion of Figure 14

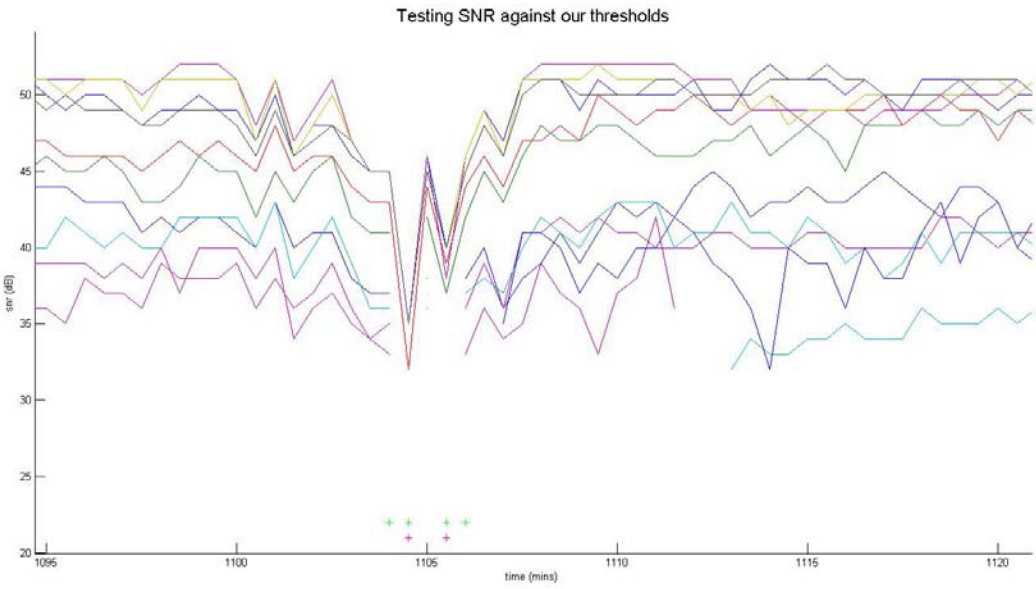

Figure 17: SNR plot from a site in Budapest with detection flags

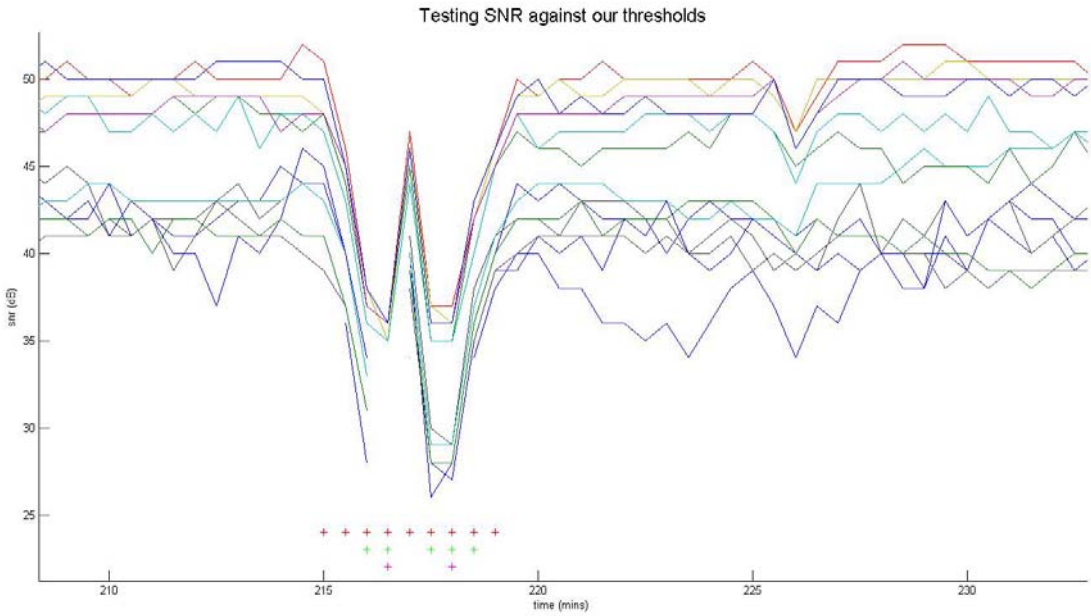

Figure 18: SNR plot from a site in Paris with detection flags

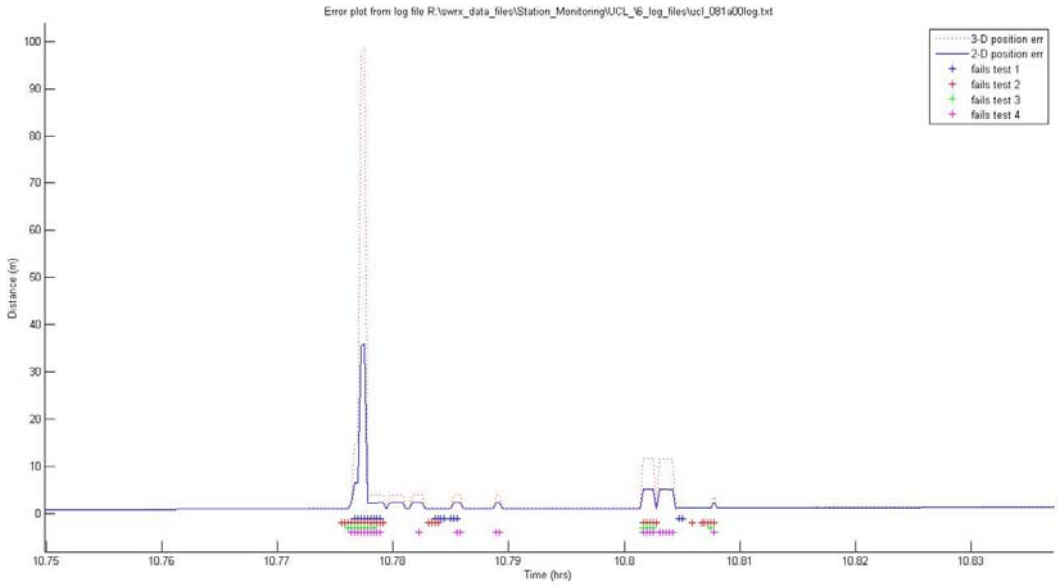

Figure 19: The position error associated with Figure 15

Figure 19 shows the position error using the data recorded over the same period shown in Figure 15 from the London test site. Due to the reduced number of satellites used and the impact this has on geometry, and the increased noise on the remaining signals, the 3D position error reaches nearly 100m. All detected interference events can be seen to degrade positioning accuracy to some extent. It is important to note here that these results are produced using data from reference stations which are fairly close to roads (typically less than 100m) but the impact on SNR and positioning for GNSS equipment in much closer proximity to an interference source will be more serious than this.

These sites have been studied over a period of time to look for trends. This can help rule out multipath and can also help build a picture of the times of day/week that are more likely to experience jamming. Figure 20 is a simple representation of the number of events which have been detected at the London site between 6th March and 8th April 2012. It can be seen that Wednesday and Friday are busier than the other days, whereas Sunday is very quiet.

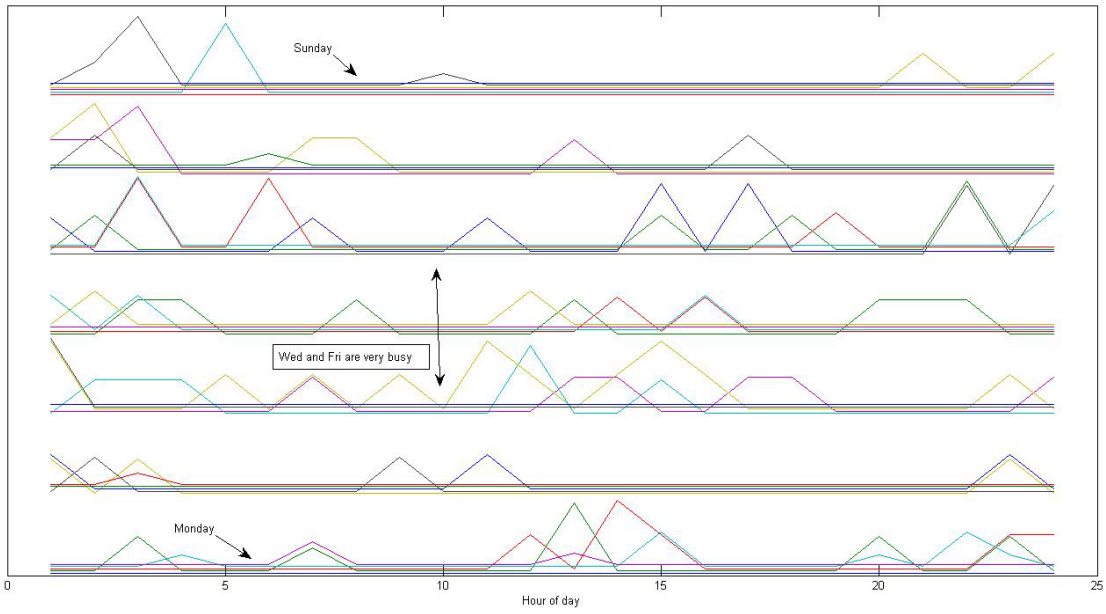

Figure 20: The disturbance events over a 34 day period, grouped by day (Monday bottom to Sunday top) and hour of day (left to right).

4.4 RF Data Collection and Analysis at London Site

Based on the initial results from analysing reference station data it was decided to collect some RF data close to the London reference site to allow more detailed investigation of detection and characterisation methods. Again, this mirrors the approach taken in some previous studies, e.g. [RD3], [RD18]. The data was collected over 2 days using components which are being evaluated within the DETECTOR equipment design. This includes a COTS receiver, a flexible RF Front End (NSL's Stereo[4] product) and standard patch antennas. This equipment was set up near the roadside approximately 150m from the reference station.

From this test many potential events were identified. The following figures are used to illustrate the investigation of one of these. Figure 21 shows the SNR values recorded at the reference station over a selected period which shows a clear drop over a period lasting approximately 3 minutes, triggering the detection thresholds. Figure 22 shows the positioning error over the whole day, with the event shown in figure 21 easily identifiable at around 01:30 due to the significant increase in position error. These provide clear evidence of an event which can then be further investigated using RF data.

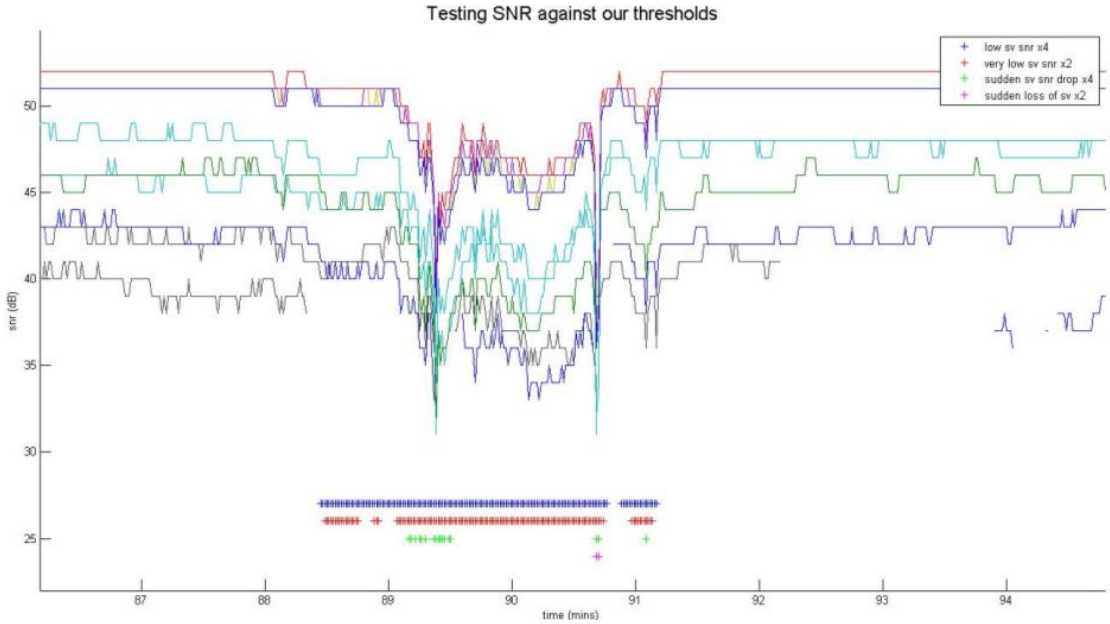

Figure 21: SNR monitoring at London reference site (9 minutes)

[4] http://www.nsl.eu.com/datasheets/stereo.pdf

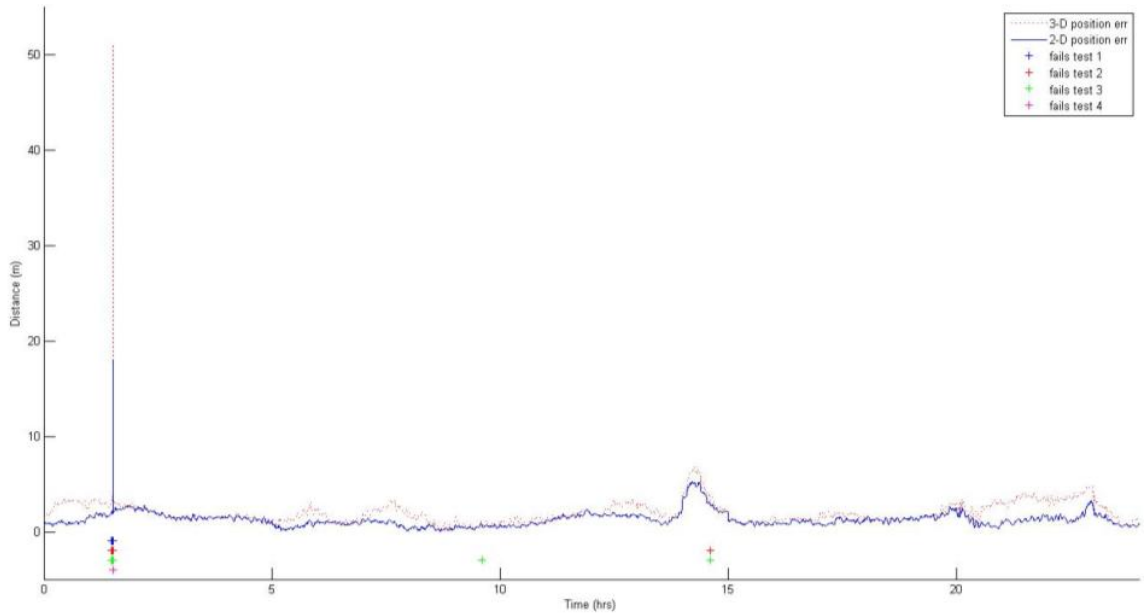

Figure 22: Position error at London reference site (24 hrs)

The RF data from this period has been analysed with prototype interference detection algorithms which form the starting baseline for DETECTOR. These are using pre-correlation techniques which complement the coarser post-correlation techniques (SNR monitoring) described so far.

Figures 23 and 24 show screenshots from the detection software at two points within this 3 minute period. In each case the Power Spectral Density (PSD) of a reference signal (that which is expected in clean observation conditions) is shown against the actual signal being received in this period. The lower portion of the plot shows the sampling frequency using a 2 bit RF chain. It is apparent that two distinctly different interference sources have been detected.

Figures 25 and 26 show screenshots from the characterisation software at the same two points showing the spectrogram of the received signals. The “saw-tooth” pattern is characteristic of chirp jammers as described in section 3.2.1, with the signal sweeping across GNSS frequencies. The second jammer appears to sweep a greater frequency range going outside the bandwidth sampled in these tests. These plots are based on data from the second RF chain of the Stereo front end which used 6 bit sampling (3 I and 3 Q) which allows a better resolution for characterising the signal.

Over the 2 days of this test more than 20 separate interference events were identified with a variety of chirp and single tone signatures being identified. This is a limited sample, but as a preliminary result it suggests the level of jamming and the types of jammer in use may be quite similar to the findings from previous studies (see §3.2.1.2).

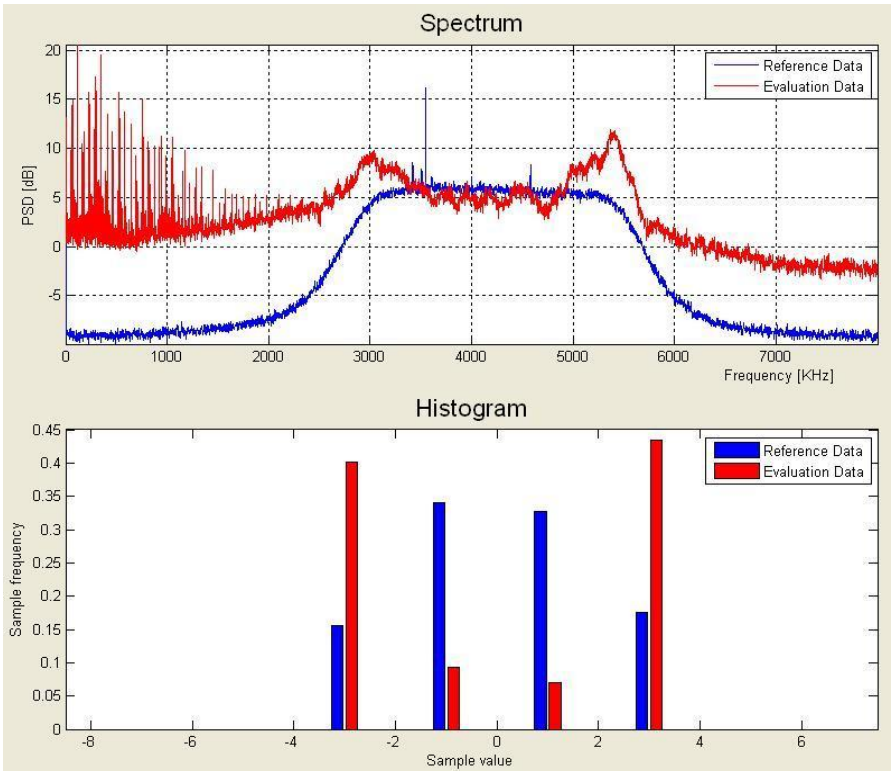

Figure 23: Detection SW showing PSD and Sampling Frequency (J1)

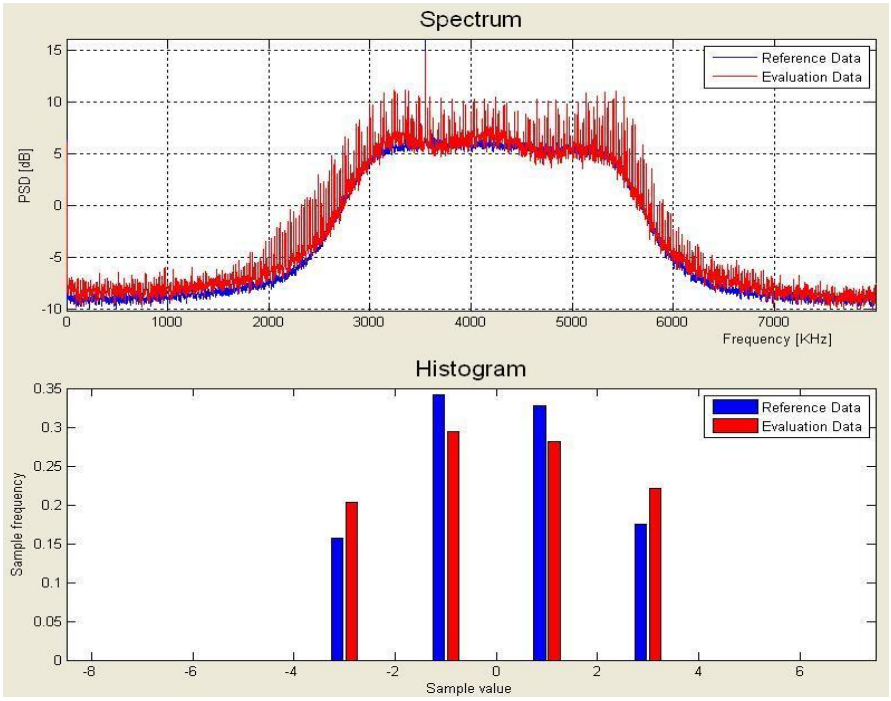

Figure 24: Detection SW showing PSD and Sampling Frequency (J2)

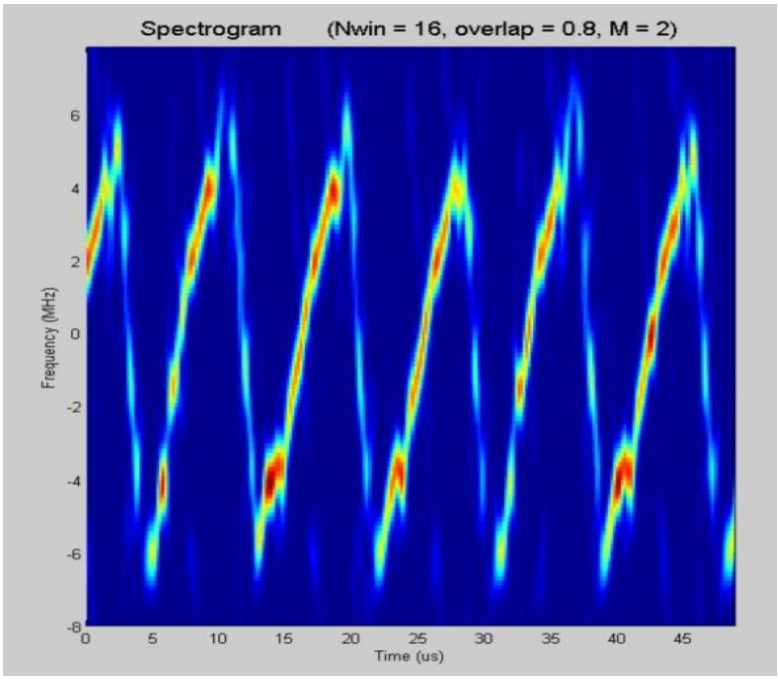

Figure 25: Characterisation SW showing spectogram (J1)

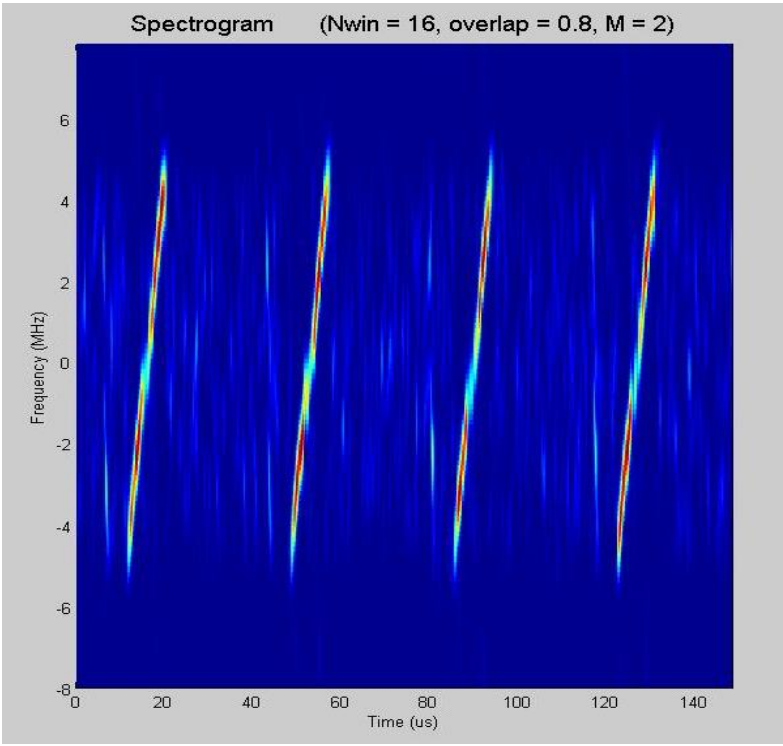

Figure 26: Characterisation SW showing spectogram (J2)

4.5 Initial Summary

These initial investigations have demonstrated the following:

1) Interference threats which are known to exist have been detected in real-world conditions, confirming that there is a threat to GNSS in the road environment from intentional interference;

2) Monitoring SNR from existing GNSS reference stations which are not dedicated to the road environment can provide an initial indicator of the level of interference events, and can be used to identify locations for deploying dedicated detection equipment;

3) Data from the monitoring networks can be used to tune detection thresholds for SNR-based detection algorithms;

4) The baseline detection and characterization algorithms for DETECTOR are a suitable basis for an effective solution, with scope for further refinement;

5) The baseline data collection equipment (COTS receiver, RF front end and antennas) has been shown to be a good basis for the DETECTOR solution

This investigation helps support the DETECTOR design and development activities. It is not a comprehensive assessment of the level of threat from interference but it is clear to see how the methods used here would form the basis of a long-term monitoring service on a local, national or regional basis.

5 Conclusions

Section 2 of this document provides brief descriptions of critical road applications which have some level of reliance on GNSS. From understanding how GNSS is used, the impact of disruption to this service can be estimated. Regarding the potential impact of jamming on road applications the following observations can be made:

1) Interference and jamming has the potential to degrade the accuracy, availability and integrity of GNSS solutions.

2) For most road applications it appears that a low level of users operating personal jammers could cause a nuisance for the operators of GNSS-based services and may impact operating efficiency through the need to investigate OBUs which are not reporting position. This may not be a significant or a new problem however as their solutions already need to be designed to cope with intermittent GNSS signal loss. A similar argument applies in safety-related applications where designs must already ensure that there is not a total reliance on a single technology.

3) Various means exist to detect a vehicle on the road network which has an OBU that is not recording its position. This can be achieved through cross checks with other sensors and information sources on the vehicle, as well as through system level enforcement, for example ANPR gantries. Rather than detecting the jamming source explicitly, the effect on the OBU, not recording position, is detected.

4) Very high levels of jammer use would start to undermine the feasibility of multiple applications though. For example, a massive use of GNSS jammers by users in protests of “civil disobedience” could totally jeopardize a RUC system and cause severe losses to a toll system concessionaire.

5) Road applications may create the incentive for drivers to operate jammers but it is other GNSS users who may suffer more significantly from degraded services.

6) The onus will be on law enforcement bodies and regulators to detect and prevent jamming but it is possible that regulations may be introduced to ensure that road applications are designed so that they give little or no incentive to operate a jammer. One element of such a design could be the ability to detect jammers.

Sections 3 and 4 highlight some of the major threats to GNSS services, in particular intentional interference using low-cost jammers. Section 3.2.1 in particular provides a comprehensive review of the types of jammers which are known to exist and proposes ways in which they can be classified. Initial investigations described in section 4 further confirm the presence of these devices and demonstrate ways in which they can be detected and characterised.

From existing studies reported in the public domain and the limited trials carried out for the DETECTOR project it appears that there are already a non-negligible amount of jammers in use on public roads, with the potential to disrupt GNSS services. The great majority of the devices in use appear to be “chirp” jammers with a few examples of single tone jammers also noted. From the power levels specified by jammer suppliers, and the reported impacts in the field, it is clear that so-called Personal Privacy Devices are interfering with GNSS services well beyond their intended target.

Distribution List

Quantity	Format	Name	Company
1	Electronic (PDF)	Marco Detratti	GSA
2	Electronic (PDF)	Renato Filjar	GSA reviewer
3	Electronic (PDF)	Salvatore Bellomo	GSA reviewer

Distribution List

END OF DOCUMENT