Radio Frequency Interference Detection to Support the Use of GNSS in ITS

Kevin Sheridan, Yeqiu Ying, Timothy Whitworth
NSL, UK
Loxley House, Tottle Road, Nottingham, NG2 1RT, UK; +44(0)115 9682960;
kevin.sheridan@nsl.eu.com

Abstract
Global Navigation Satellite System (GNSS) technology is being used in an increasing number of applications in various sectors, including those regarded to be critical as they concern safety and financial transactions. Within ITS applications GNSS is often the primary means of providing vehicle location. It can provide flexible, accurate and reliable positioning at low-cost but there are some limitations of GNSS which need to be understood and taken into account in the design and operation of products and services. One such limitation of GNSS is its vulnerability to signal interference and jamming, which can severely degrade the GNSS service and impact performance. Effects range from a loss of accuracy to complete denial of GNSS services.

This paper describes the DETECTOR project, co-funded by the European GNSS Agency under the 7th Framework Programme and led by NSL, which is developing and validating a low-cost device for detecting GNSS interference and jamming within road transport applications. The device will be capable of operating in a stand-alone mode or as part of a networked solution to detect and characterize radio frequency interference.

Keywords: Global Navigation Satellite System (GNSS), Radio Frequency Interference (RFI), Jamming, Detection and Characterization, Software Defined Radio (SDR)

1. Impacts of radio frequency interference

GNSS signals are very susceptible to noise, due to their extremely low power, which leads to a very widely documented vulnerability (see for example [1] to [5]). Any increase in the noise level at the receiver antenna will adversely affect the performance of GNSS receivers. If the interference level is so high that the receiver electronic components are saturated, the signals might well be unrecoverable. When extra noise is present at the front-end, the receiver will encounter the following situations:

1. Low noise will affect measurement accuracy;
2. Medium noise will cause problems with tracking, and make it harder to (re-)acquire satellite signals. Satellites at low elevation may be lost;
3. High noise can prevent a receiver acquiring or tracking enough signals to provide a position solution.

There are a variety of potential RF interference sources, both natural and man-made. Natural interference can be caused by geomagnetic and ionospheric activity. Solar activity influences the behaviour of charged particles in the ionosphere which delay GNSS signals passing from satellites to user receivers. Under normal circumstances this delay can be corrected in a

standard GNSS solution, but there are a series of phenomena including solar radiation bursts and ionospheric scintillation which can severely disrupt GNSS signals over wide areas.
Man-made RF interference can be caused by a number of sources, ranging from television signals to mobile communication devices. 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. Similarly, there is the potential for TV antennas with internal pre-amplifiers to cause interference if the unit malfunctions. In Turin, Italy it has been documented that out-of-band interference from TV broadcasts is interfering with GNSS frequencies [6].

The principal focus in the DETECTOR project is the threat of disruption due to intentional interference or jamming. In recent years, intentional interference events have been experienced, detected and analyzed. The most widely reported case of RF interference caused significant disruption to a GNSS landing system at Newark Airport. After lengthy and costly investigation by multiple US government agencies, the source was found to be a low-cost (≈$30) jammer in a truck on the nearby highway. Dedicated data collection campaigns triggered by this case detected up to 25 separate interference events per day [7]. The current extent of jammer use and the impacts it may have on GNSS services is not precisely known, but with the wide availability of low cost devices (albeit illegal) and growing privacy concerns around tracking equipment, it is likely to be a growing problem.

For many road applications a low level of drivers operating personal jammers could cause a nuisance for the operators of GNSS-based services and may impact operating efficiency through the need to investigate On-Board Units (OBUs) which are not reporting position. In many cases this would not be a significant or a new problem however, as these solutions already need to be designed to cope with intermittent GNSS signal loss. A similar argument applies in safety-related applications such as Advanced Driver Assistance Systems (ADAS) where designs must already ensure that there is not a total reliance on a single technology. The greater problem is likely to be caused to unrelated GNSS services near roads that are more susceptible to disruption. Very high levels of unchecked jammer use could 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 jeopardize a Road User Charging (RUC) system and cause severe losses to a toll system concessionaire.

2. Detection and characterization methods

Measurements are available at many points in the GNSS receiver processing chain which can be used to detect the presence of RFI. One good indicator within the receiver is the gain value of the controllable gain amplifier before the analogue signals are fed into the analogue to digital converter (ADC). This is because the input signal to the ADC is required to be matched to the dynamic range of the ADC to guarantee the quantization accuracy. Therefore, within the GNSS receiver implementation an automatic gain control (AGC) circuit is normally implemented to adjust the gain value based on the output of the ADC. When the ADC input signal is higher than the nominal level due to the presence of excessive RFI, the AGC will try to lower the gain value of the adjustable gain amplifier, and vice versa.

The characteristics of the digital signals at the output of the ADC will be changed in the presence of different RFI. Since GNSS signals are below the noise floor when they arrive at the receiver, in the nominal scenario it will have the characteristics of the additive white

Gaussian noise (AWGN). When excessive RFI is present, these characteristics will be changed, allowing the digital signals at the output of ADC to be used to detect RFI.
The detection techniques used in this activity exploit the flexibility of software GNSS receiver concept, so that the above-mentioned measurements are accessible, some of which are not usually available from commercial off the shelf (COTS) receivers. The detection algorithms are composed of "pre-correlation" and "post-correlation" techniques. Pre-correlation algorithms make use of the digital signals at intermediate frequency (IF) that are available in the software receiver used within DETECTOR. The post-correlation algorithms can use signal to noise ratios (SNR) measurements either from our dedicated software receiver or from a COTS receiver.

The solution finally implemented in DETECTOR uses a combination of post-correlation and pre-correlation techniques to reach a detection decision. Using very distinct SNR drops across multiple satellites is an effective detection method for "strong" interference events and can be implemented simply based on existing (non-dedicated) sensors, e.g. standard GNSS receivers. However, it misses many weaker events which are not detectable with sufficient confidence to be flagged. Pre-correlation techniques are used in addition, helping to detect more jammer devices and to increase the confidence of any detections. A particular benefit of pre-correlation techniques is their ability to detect interference with a very narrow bandwidth. The overall jammer power may be low (so has little impact on SNR) put the power/frequency ratio may be very high so would have a significant impact on a receiver. Access to the digital samples also allows the interference signal to be analysed further to identify the nature of the interference source. Details of the algorithms used are provided in [8].

3. Detector architecture

The DETECTOR system is composed of two major elements: networked DETECTOR field sensors or probes, and a DETECTOR server at the back-office for data storage, processing and analysis. This is illustrated Fig. 1.

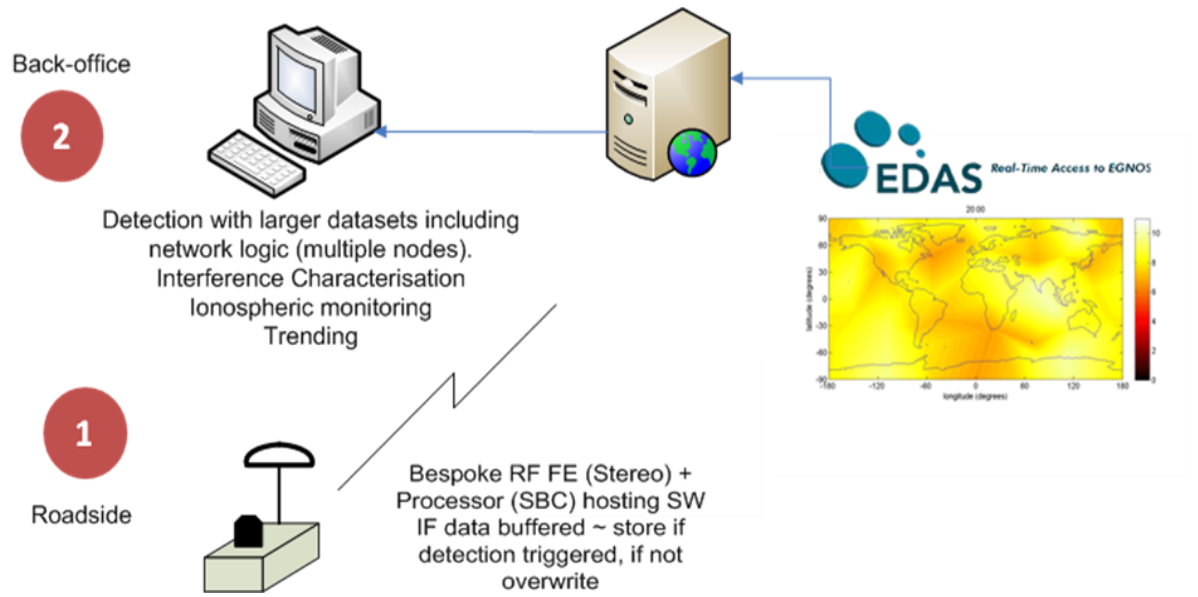

Figure 1- DETECTOR System Overview

Field Sensor

The field sensor is composed of an embedded computer which hosts the software receivers, all the detection algorithms, as well as managing the internal and external communications. A software receiver front end called Stereo, which can be configured to cover all GNSS frequency bands, performs the GNSS receiver front end processing. A COTS hardware receiver is also included to provide redundancy of measurements. Ethernet and wireless communication modems support data communications. A sample of digital data is stored in a circular buffer. If an interference event is detected the samples are stored, otherwise the buffer is overwritten. All elements of the design are selected to be low-cost, allowing for a scalable solution with large numbers of sensors in future operation.

Back-office Server

The back-office collects transmitted digital samples and detection logs from the networked field sensors and performs more comprehensive interference detection and characterization analyses. It also makes use of additional information such as road databases and dynamic motion models to determine if multiple detection events are likely to be due to a single jammer. In addition, it monitors the state of the ionosphere to identify disturbances which could impact many receivers, and prevents this from incorrectly being attributed to intentional interference.

A database of jammer "signatures" will be built up to help develop effective countermeasures. Results can be interrogated to determine trends in the numbers, types and usage patterns of jammers over time.

4. Results

4.1 Test at Targeted Site

DETECTOR algorithms have been tested in laboratories and in field trials using dedicated sensors, and also using data available from existing GNSS reference networks. The software can process RINEX and/or NMEA files, and perform post-correlation interference detection. In the UK, like many other countries, it is possible to obtain data from continuously operating GNSS reference stations which have been established to support land surveying and geodetic applications. Several of these are being continually monitored to check for potential interference events.

Preliminary tests identified a number of performance fluctuations which may have been caused by interference. Based on this, a location on an urban road close to an existing reference station was selected for collecting further data with DETECTOR equipment. Capturing digital samples in addition to more standard SNR data made it possible to use both post-correlation and pre-correlation detection and characterization techniques.

Processing data SNR values from the permanent reference station, 5 or 6 possible events were identified over a 2-day period, including one which coincided with a 50m horizontal positioning error. Figure 2 shows the estimated SNR centred on a 3 minute period where there is an obvious drop in SNR.

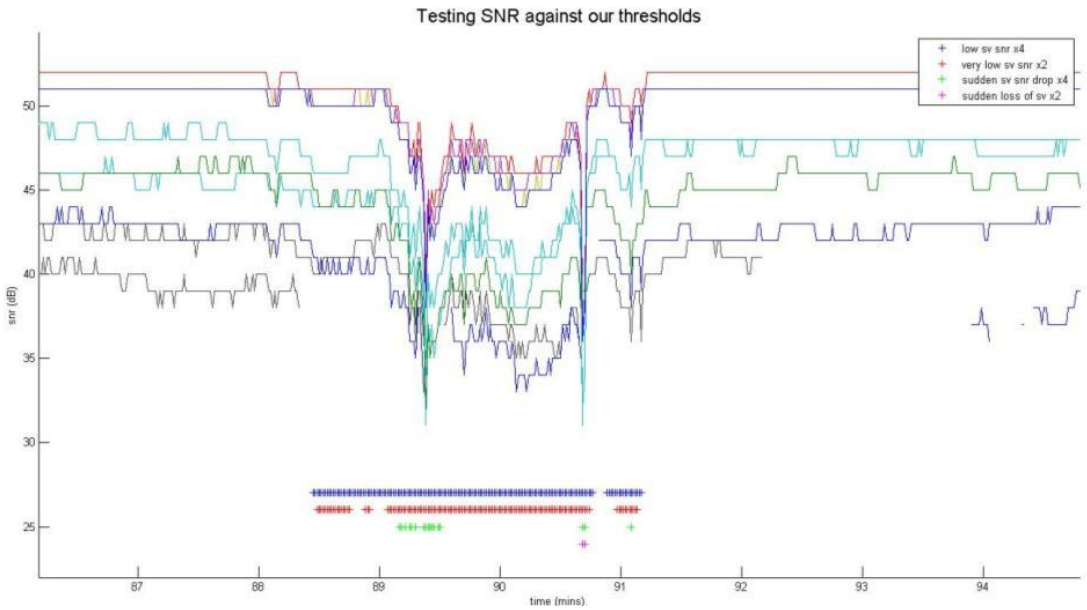

Figure 2 - SNR values at reference site during interference event

Using a reference receiver with a high-grade rooftop antenna, there should be very little multipath (reflected signals) present, which can also reduce SNR, so this observed effect can be attributed to interference. In more obstructed environments, where multipath is more significant, it becomes increasingly difficult to identify the effects of interference using SNR alone. However, the pre-correlation methods are still very effective, and the sensitivity is much higher.

Figure 3 shows the change in received power over this three minute period. For each sample the upper image shows the received signal power in the frequency domain centred on the GPS L1 central frequency, with the blue trace showing the power recorded during a nominal calibration period and the red showing the received power during the test. The histogram below shows how this continuous signal is sampled to 2 bits in the ADC process. Initially no interference source is present and the power spectral density and histogram matches expected values for nominal conditions. Over time the impact of the interference signal on the receiver increases, with higher power leasing to more samples in the outer bins. This reaches a point at which the signal being evaluated has a digital power more than 5 times that of the nominal reference signal (labeled 1 in figure 3). The trend indicates that the jammer was mobile, and was moving towards our site. Most satellites could no longer be tracked at this time leading to degraded positioning. As the jammer moves away the interference level naturally drops. 50 seconds later though, it builds up again (to a peak labeled 2 in figure 3). This indicates that this is in fact two instances of jamming within a 3 minute window.

These were not the only events of interference. In the space of 41 hours more than twenty separate potential events were detected using these techniques, far more than the 5 or 6 which were observable simply using SNR values.

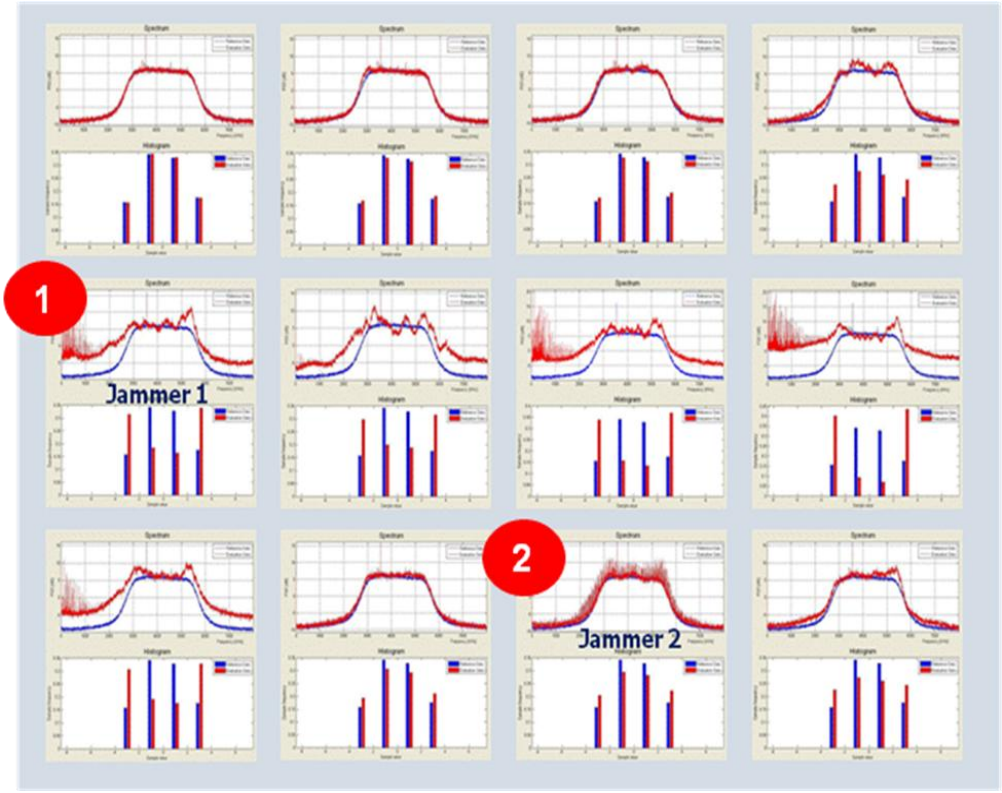

Figure 3 - PSD & Histogram over 3 minute period

The DETECTOR solution also characterizes the interference signals. This is a critical step in identifying the source of the interference, including differentiating between intentional and unintentional cases, and for providing evidence to support enforcement actions. Figure 4 shows the spectrogram for the two interference events. These plots show the interference to be of the "chirp" type - a continuous wave signal quickly swept through a wide frequency range. The two different signatures confirm that there are two jammers present, just a minute apart. Each of them is designed specifically to jam GNSS frequencies. Unintentional interference from badly tuned or malfunctioning equipment will not exhibit this behavior.

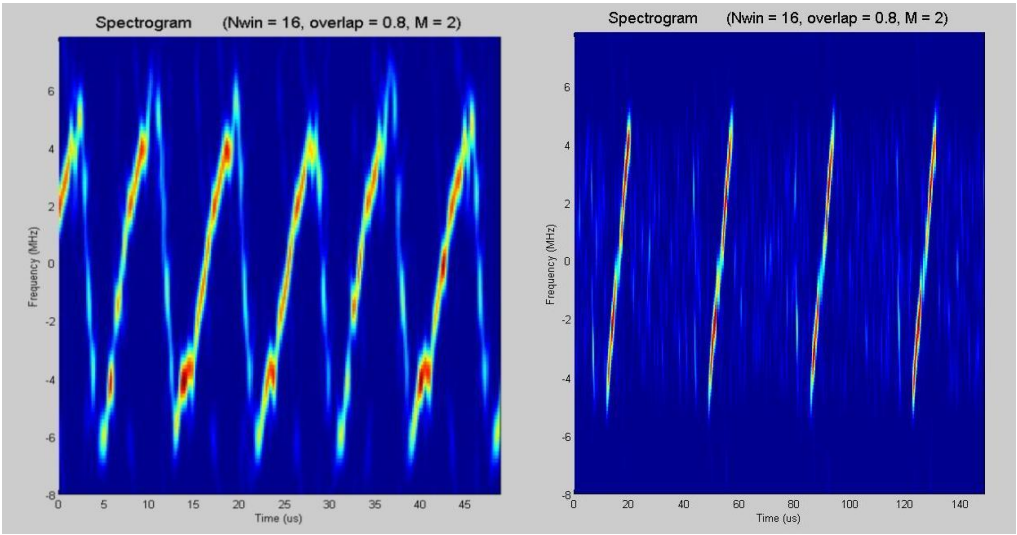

Figure 4 - Spectrograms from the two jammers

The DETECTOR software is able to characterize a signal automatically, based on; statistical periodicity, time periodicity, duty cycle, a swept signal test, a frequency hopping test, power, and bandwidth. In the case of the data here, the software correctly concludes that both the jammers are sawtooth (up) chirp, the first being continuous, the second pulsed. Note that in all likelihood the second signal will in fact be continuous, but the signal will travel outside the frequency of the pass-band of the receiver, i.e. it is the receiver hardware that is turning the signal from continuous to pulsed. DETECTOR identifies the type of interferer (classification) and also quantifies a set of attributes to describe the source (parameterization).

The other interference events characterized in this 41 hour data capture include several other chirp signals, some powerful single-tone signals, and a few narrow-band signals. The majority of these look to be attributable to jammers but there are also a number of signatures which are more likely to be from unintentional man-made sources.

4.2 Tests at Field Jamming Trials

DETECTOR has also been tested in a variety of scenarios where a known interference sources is introduced. In June 2012, NSL participated trials in Sennybridge, Wales, with the support of the Ministry of Defence and the Defence Science and Technology Laboratory (DSTL). In these trials, jammers with known and configurable characteristics were operated at a remote site. A variety of tests were performed with the jammers static and the detection equipment in a moving vehicle, then the situation was reversed with jammers moving and detection equipment static. In all cases the DETECTOR solution was able to detect and correctly characterize the jammer, and studying the results made it possible to determine the distance over which GNSS receiver performance will be degraded.

4.3 Laboratory Tests

DETECTOR has also been tested using the specialist laboratory facilities of the Institute for the Protection and Security of the Citizen (IPSC), one of the EC's Joint Research Centres, in Ispra, Italy. This facility allows jammers to be operated safely inside vehicles within an anechoic chamber (Figure 5 - left). A range of detection devices including high-grade spectrum analyzers can be used to sample the emitted RF signals. This allows the characteristics of the jammers to be analyzed in detail, identifying the emitted power and the frequency and periodicity of the signal. From this it is possible to determine both the likely disruption that each jammer could cause to GNSS services at various ranges, and also the distance over which the device could be effectively detected by monitoring equipment.

In initial tests a sample of commercially available jammers (Figure 5 - right) were operated in the anechoic chamber with the proposed DETECTOR equipment (Stereo RF Front End) and a more comprehensive spectrum analyzer recording and analyzing the signals.

Figure 5 - Car being tested in anechoic chamber at IPSC, JRC (left). Sample of commercially available jammers tested (right).

DETECTOR was again able to reliably detect and characterize a range of typical jammers. Controlled testing provides an opportunity to better understand the jamming signals produced by various low-cost devices in a clean environment, which is a critical step in developing effective counter-measures. Figure 6 shows the spectrogram of four of the jammers tested. It is interesting to note that many of the jammers tested will disrupt GNSS signals on multiple frequencies, including the proposed Galileo PRS side lobes on L1.

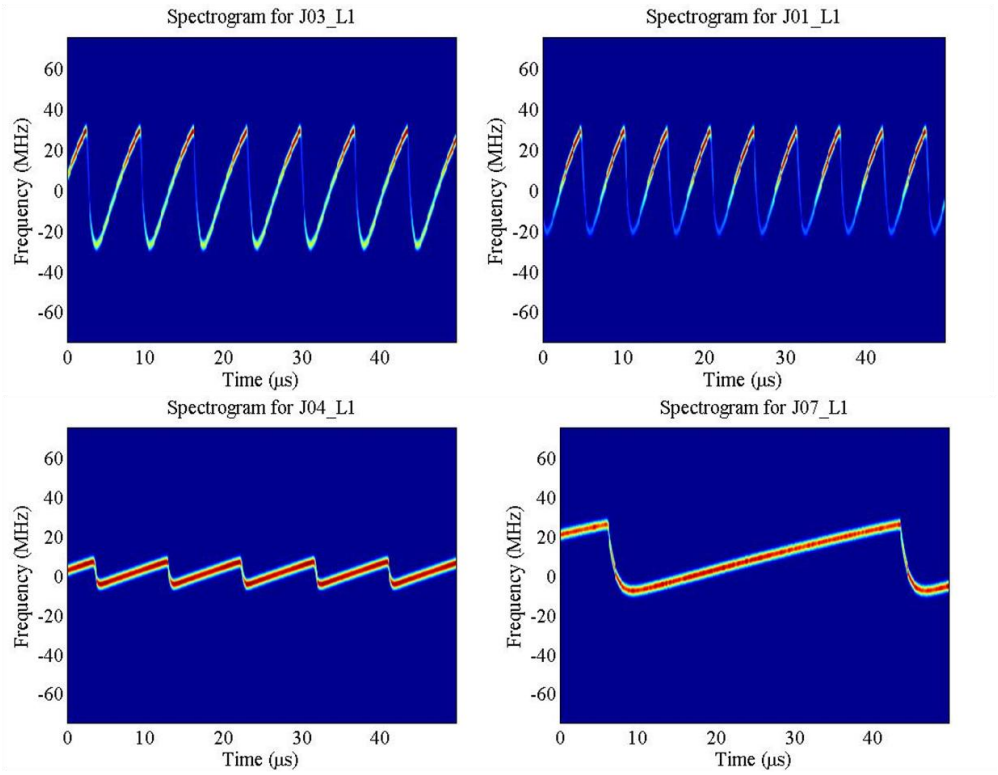

Figure 6 - Spectrogram of jammers in laboratory testing.

Future multi-frequency GNSS equipment will add some robustness to interference, particularly from unintentional sources which are unlikely to disrupt widely distributed frequencies simultaneously. This provides improved mitigation but does not offer full protection given the presence of multi-frequency jammers.

Further tests were then carried out in which jammers were placed in different locations within two vehicles and the detecting antenna scanned over a complete hemisphere around the vehicles. The two vehicles used in these tests were a small hatchback (Fiat Panda) shown in figure 5 and a large van (Fiat Ducato). Transmitting antennas were placed on the dashboard, in the glove compartment and in the back of the vehicles to mimic different cases of concealment. In these tests a network analyzer was used to accurately evaluate the channel over a very wide bandwidth. This made it possible to determine the path loss at each different GNSS band, and allowed samples to be taken at the receiving antenna from signals transmitted from each of the three antenna locations in the vehicle in turn.

These tests show how local obstructions influence the effective range of the jammers in different directions, so it is the differences in emissions which are of interest here rather than the absolute power of the interference signal. Figures 7 and 8 show the path loss from a transmitting antenna located on the dashboard of the small car, and the van respectively. The patterns clearly show the much stronger transmission of the signals through the windscreen and side windows. The metal back of the van provides an effective shield whereas the windows of the car allow the interference signal to propagate in all directions with a lesser reduction in received power.

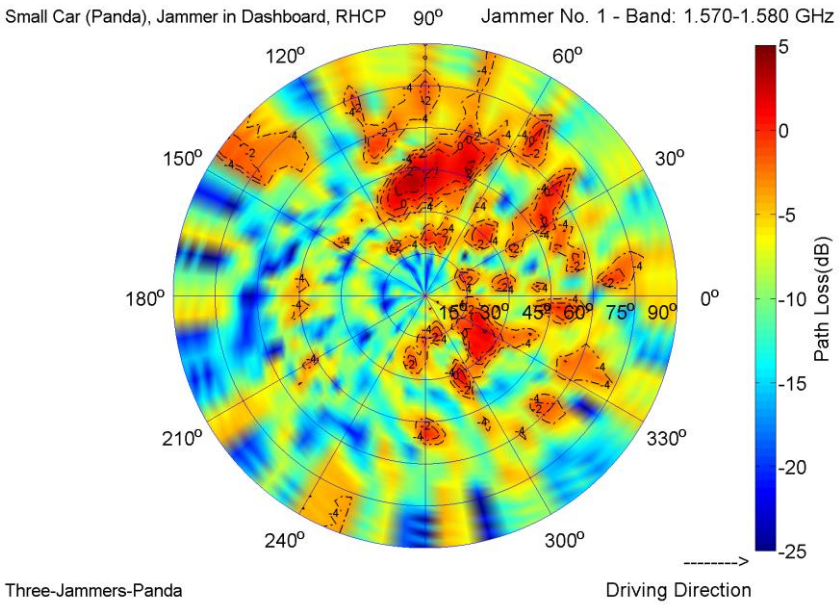

Figure 7 - Path Loss with Jammer on dashboard of car

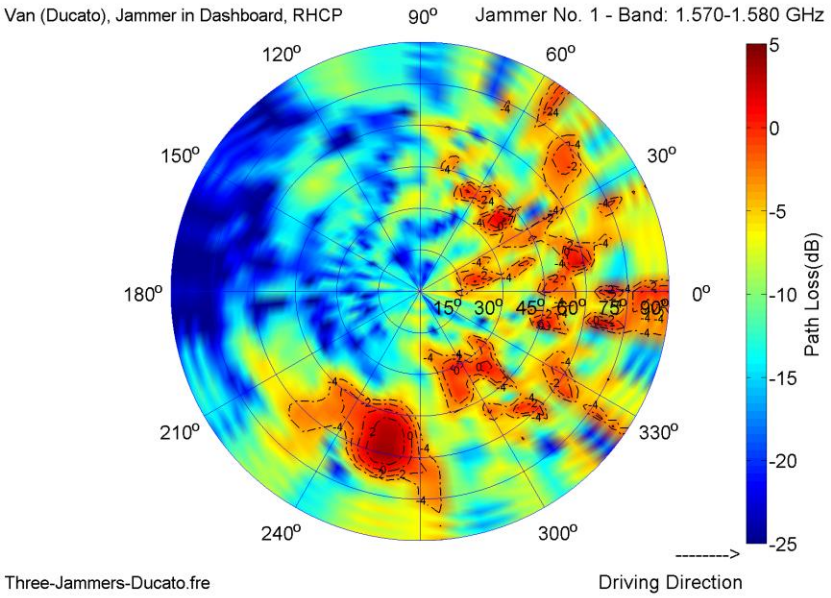

Figure 8 - Path Loss with Jammer on dashboard of van

These tests also confirm that a jammer plugged directly into the cigarette lighter will be more disruptive to other GNSS equipment in the vicinity but is also easier to detect. Jammer operators may conceal their jammers to make them more difficult to detect but this also limits the disruption caused to third-party GNSS equipment.

The main conclusions of these tests are largely intuitive and predictable. Some of the more detailed analysis is important though, as it informs decisions of where to place detection devices on a road gantry for example and also highlights some of the challenges in locating a jammer. A jammer in a vehicle cannot simply be treated as a point source uniformly emitting a signal in all directions. This makes it difficult to implement solutions which triangulate to the source based on the received signal strength at multiple detection devices. There are means to locate jammers, but these types of issues need to be addressed for an effective solution.

Data collection and analysis has been used to support the development of an operational solution. The amount of digital data which is collected, analyzed, communicated and stored is an important design issue. These tests have helped identify the length of sample, bandwidth and quantization level (number of bits) required for reliable detection and characterization. The flexibility of the Stereo RF Front End makes it an ideal platform for performing these types of investigation. For example, by configuring the two available RF chains differently and using them simultaneously, it has been possible to directly compare results using a 2 bit quantization with 6 bits (3I, 3Q) on the other chain.

5. Validation and deployment

An end-to-end prototype of the DETECTOR device will be validated in May 2013 at the "AutomotiveGATE" in Germany (figure 9 - left). The Aldenhoven Testing Center (ATC) is a proving ground for positioning systems for road applications. Using this facility, jammers, receivers and detectors can be operated in a realistic road environment. The testbed includes

road sections representative of urban, sub-urban and autobahn conditions. Jammers, receivers and interference detectors can be installed on vehicles and on roadside gantries in various combinations. For example, the impact on a GNSS receiver from a brief exposure to a jammer which is being used in a vehicle travelling in the opposite direction can be assessed. The ability to detect this jammer in slow and fast moving traffic can be assessed. The effectiveness of detectors installed on overhead gantries rather than at the roadside can be examined, taking into account alternative traffic conditions which could block the path between a jammer and detector.

Figure 9 - Overview of the AutomotiveGATE test site (left). Gantry for initial sensor installation (right).

DETECTOR has been designed with the aim of having multiple sensors deployed on road gantries. Following the validation of the prototype it will be installed at a Sanef operated site in northern France (Figure 9 - right). Data and experience gained in deploying the system in an operational context will help assess the potential disruption to road operations from the use of jammers and will evaluate one mechanism to help address this threat.

6. Conclusions

DETECTOR has been developed to provide an effective, low-cost means to detect and characterize RF interference sources which degrade GNSS performance in road applications. Tests have demonstrated the potential of the system to reliably detect and characterize jammers in real-world conditions, controlled field tests and in the laboratory.

Pre-correlation techniques, which are made possible through the use of a flexible RF Front End and software receiver, have been able to detect events which would likely go undetected using only post-correlation (SNR) methods. Characterization allows the type of interference signal to be identified which gives a good indication of whether it is unintentional interference or a jammer. Signal characteristics helps understand the nature of the threat to GNSS services and to develop effective counter-measures.

Acknowledgments

The work presented in this paper has been co-funded under the EC FP7 programme through the European GNSS Agency (GSA). This support is gratefully acknowledged. The project partners are Nottingham Scientific Ltd., Università di Bologna, Sanef, Black Holes B. V. and AGIT.

References

1. Wildemeersch M., J. Fortuny-Guasch (2010). RadioFrequency Interference Impact Assessment on Global Navigation Satellite Systems. *EC JRC Security Technology Assessment Unit, EUR 24242 EN*.
2. Bauernfeind R., T. Kraus, D. Dotterbock, B. Eissfeller, E. Lohnert, E. Wittmann (2011). Car Jammers: Interference Analysis. *GPS World*, October 2011.
3. Thomas M. (2011). Global navigation space systems: reliance and vulnerabilities. *The Royal Academy of Engineering GNSS Vulnerability Report*.
4. Storm van Leeuwen S. (2008). Electromagnetic interference on low cost GPS receivers. *National Aerospace Laboratory Report*.
5. Kuusniemi H. (2012). Effects of GNSS Jammers on Consumer Grade Satellite Navigation Receivers. In Proceedings of *ENC 2012*.
6. Motella B., M. Pini, F. Dovis (2008). Investigation on the effect of strong out-of-band signals on global navigation satellite systems receivers. *GPS Solutions*, Volume 12, Number 2, pp77-86.
7. Grabowski J. (2012). Field Observations of Personal Privacy Devices. In Proceedings *ION NTM 2012*.
8. Sheridan, K., Y. Ying, T. Whitworth (2012). Pre- and Post-Correlation GNSS Interference Detection within Software Defined Radio. In Proceedings *ION GNSS 2012*, Nashville.