Studying the Effects of Interference on GNSS Signals

Paul Craven, Ronald Wong, *Spirent Positioning Technology*
Neal Fedora, Paul Crampton, *Spirent Federal Systems*

BIOGRAPHY

Paul Craven studied for his BSc (Mathematics) and PhD (Vehicle Control Systems and Navigation) at the University of Plymouth. He is currently a Senior Software Engineer, working on GNSS Positioning Systems at Spirent Communications Positioning Technology.

Ronald Wong received his BEng (Electronics), MSc (Satellite Engineering) and PhD (Satellite Engineering) from the University of Surrey. Currently, he is a senior Systems Engineer at Spirent Communications Positioning Technology where he is involved in verifying GNSS simulator software and hardware.

Neal Fedora is the Director of Engineering with Spirent Federal Systems Inc. He has a B.S. degree from Embry-Riddle Aeronautical University in Avionics Engineering Technology and a M.S. degree from the University of South Florida in Engineering. He holds three U.S. patents.

Paul Crampton is a Senior Systems Engineer with Spirent Federal Systems Inc. and has been involved with the GPS Industry for 20 years. Prior to joining Spirent Federal in 2003, he provided engineering services and technical support at Spirent Communications in the UK. Paul has a BSc (Honors) in Information Technology from De Montfort University in the UK.

ABSTRACT

Global Navigation Satellite System (GNSS) signals, such as those from United States Global Positioning System (GPS), Europe's Galileo, and Russia's Global Navigation Satellite System (GLONASS), typically have extremely low received signal strengths at the Earth's surface and are therefore susceptible to a range of interference signals. Such interference examples include, but not limited to, intentional sources such as Personal Privacy Devices (PPD) and unintentional sources such as Digital Enhanced Cordless Telecommunications (DECT) and Long Term Evolution (LTE) signal.

Recent studies into such interference sources have identified GNSS jamming as having a major impact on geo-location positioning and communications technologies. One such study is the U.K. government funded Sentinel trial which investigated the density of jamming technologies at various road-side locations across the U.K. Another is the THV Galatea trial conducted by the Ministry of Defence in 2009 which documented the impact of interference signals on maritime navigation and communication systems [6].

Assessing the vulnerability of GNSS signals to such interference sources in real world scenarios is a challenging and time-consuming task which is subject to numerous environmental uncertainties. This paper describes a synthetic test environment which can model the effects of interference sources on GNSS signals and thus provide accurate, repeatable control of the signal characteristics in the laboratory. The system provides real-time control of both the GNSS and interference signal characteristics including definition of the receiving vehicle dynamics, signal modulation type, on/off periods, power level and center frequency. Of particular interest is the ability to introduce custom or user-defined modulation types which enables easy utilization of application critical waveforms during testing.

This paper demonstrates the effect of several common broadband noise signals, as might be seen with a PPD, on a GNSS receiver. The results and conclusions of the investigation are supported by examining the receiver's carrier-to-noise density (C/N_0) and performance impact as a result of the interference sources throughout the test cases.

INTRODUCTION

GNSS positioning has become an increasingly important tool in a number of key military and commercial applications, such as aircraft and weapon navigation systems, warfighter positioning and targeting, timing, asset tracking and commercial navigation. However, the low transmit power of GNSS signals means that they are

particularly vulnerable to jamming from both intentional and unintentional interference sources.

Intentional interference can be caused by personal jamming devices such as broadband noise jammers, whereas unintentional interference can emanate from ubiquitous telecommunications signals such as DECT signals used in household portable telephone technology and from sources such as the Long Term Evolution (LTE) signal.

GNSS receivers are also vulnerable to spoofing signals, which can be another form of intentional interference. Whilst the goal of intentional jamming is generally nothing more than to swamp the receiving antenna with noise and cause the receiver to lose track of visible satellites, spoofing is the process of mimicking the GNSS signal. As such, spoofing can be considered as a form of deceptive jamming.

GNSS jamming devices are now becoming widely available and at little cost [4]. The subsequent threat to GPS signal reception posed by these devices has therefore increased. For example, in 2009 the Federal Aviation Authority discovered after a two month investigation that recent outages in GPS reception at Newark Airport had been caused by the installation of a $30 personal privacy device in a delivery vehicle. This vehicle had driven past the airport perimeter on a daily basis for a number of months [1],[5]. Whilst the underlying aim of this device was to obfuscate the movements of the vehicle from the driver's employer, this lead to an unintentional disruption to the GPS service at the airport. This is an example of an unintentional GNSS interference source and it highlights the threat posed to GNSS signal reception and the need for further investigation into the effects caused by such devices. Additional unintentional interference sources may be new communication systems, such as a LightSquared broadband signal that may directly infringe on the GNSS spectrums or indirectly produces an interference product signal that does.

As many of these interference sources are transmitting in the same portion of radio frequency spectrum as GNSS it is of paramount importance that receivers are characterized for their performance in such hostile electromagnetic environments. Indeed, a GNSS receiver will behave differently when exposed to different interference sources. Specifically, the jamming source affects the receiver post correlation carrier-to-noise density ratio C/N_0, where N represents the noise including the interference source [3], which directly impacts its measurement and positioning accuracy. It can also cause the receiver to completely lose its' lock on the available satellite signals impairing its navigation capability

The paper continues with a description of a test system which has been used to examine the effects of various interference signals on a GPS L1 C/A receiver. A Commercial Off-The-Shelf (COTS) signal generator was used in a modified manner to model certain interference signals; an explanation of how these signals are incorporated into a test system as interference sources is provided. Also, an illustration of how the GNSS and interference signals are controlled via a personal computer (PC) is documented. The results presented within this paper were collected using a Spirent GSS8000 GNSS Simulator, which was configured to generate 16 channels of GPS L1; this unit is paired with the Spirent GSS7765 interference simulator. The receiver used within the study is a COTS GNSS receiver. The results and conclusions of the investigation are supported by measuring the C/N_0 and the immunity of the receiver to the interference sources.

SIMULATION SYSTEM CONFIGURATION

Simulator Configuration

Spirent Communication Plc. based in Paignton, UK, specialize in making high fidelity GNSS simulators. These simulators are the industry standard for GNSS testing and are used across all facets of receiver testing and applications. These applications include development, performance, production and mission planning.

In our test system, the GSS8000 GPS L1 signal and GSS7765 interference RF signals are superposed with Spirent's interference combiner unit (ICU). Control of both signal generators is via a PC running the Spirent SimGEN™ software. An overview of the system configuration is shown in Figure 1.

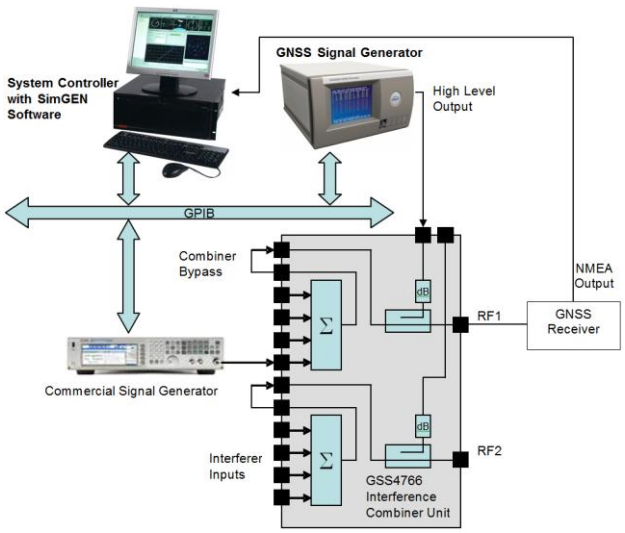

Figure 1: GSS8000 and Agilent Signal Generator Interference System

The SimGEN™ software suite, when combined with a compatible signal generator system, can be used to stimulate a satellite navigation receiver system in a laboratory environment. Additionally, SimGEN™ can be used to control the interference sources in terms of their positions and signal characteristics. When the receiver is subjected to these signals it behaves as though it were receiving 'live sky' radio frequency (RF) signals. A screenshot of SimGEN™ is shown in Figure 2.

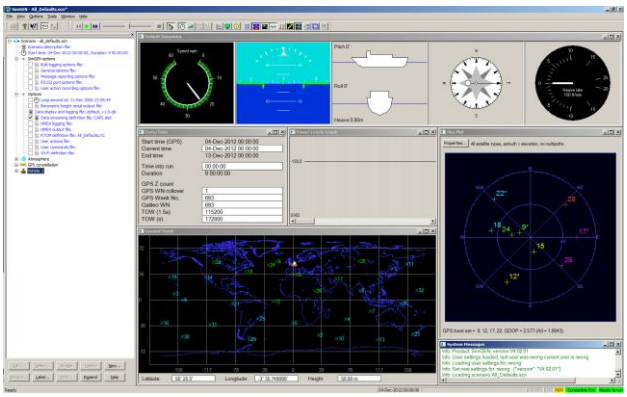

Figure 2: SimGEN™ Software Suite

SimGEN™ is able to calculate the positions and velocities of the satellites within each constellation by defining the constellation parameters within the relevant graphical user interface (GUI). Thus the orbits of the satellites can be accurately defined as per the relevant interface control document (ICD). The signals from the satellites which are visible at the simulated vehicle antenna position are generated simultaneously at each available RF output. The software applies the user-specified dilution-of-precision (DOP) algorithm to determine the simulated satellite set. Clock biases, ramps, atmospheric modeling and additional GNSS signal error effects can be defined and superimposed onto the simulated signals.

The vehicle trajectory models within SimGEN™ can be used to describe the vehicle dynamics during the test scenario. These models allow the scenario to exercise various aspects of the receiver's satellite tracking ability. A range of maneuvers subsequently describes the full 6-degrees-of-freedom (6DOF) motion of the platform. The maneuvers can be defined with SimGEN's motion models or alternatively from a user defined 6DOF file or remote source. SimGEN™ also supports modeling of the reception pattern of the navigation sensor's antenna in terms of amplitude and phase, the gain pattern representing the composite effect of the free-space reception pattern and the on-vehicle obscuration of the vehicle body. The patterns are fully linked to the vehicle trajectory, allowing automatic simulation of masking of satellite signals due to vehicle obscuration during maneuvers.

Receiver Configuration

The GPS L1 C/A code power level at the receiver input was measured as -119.7dBm which incorporates the simulator cable and combiner loss factors i.e. -130dBm GPS L1 C/A code nominal level plus 15dB of applied signal gain and minus 4.7dB of loss. This receiver has a data port that outputs navigation and other performance data via a series of messages in the National Marine Electronics Association (NMEA) NMEA-0183 standard. This is transmitted over a serial bus via RS-232C. This mechanism was used to collect receiver data for comparison with the truth data as output by SimGEN™.

Interference System Configuration

In order to use the test system illustrated in Figure 1 for the results in this paper, it has been necessary to modify the SimGEN™ software suite to interface with the Agilent Technologies N5182A MXG signal generator. This allows the COTS signal generator to generate jamming sources which are flexible and can be controlled in a number of ways. For example, the following interference source characteristics can be controlled in real-time from SimGEN™ in an interactive manner, from a schedule file or also via remote command:

1) Transmitter position
2) Modulation
3) Signal level
4) On/Off periods
5) Antenna pattern

Further to this, the system can generate the following types of interference modulation:

1) Amplitude Modulation (rate, waveform type and depth of modulation)
2) Frequency Modulation (rate, waveform type and frequency deviation from center frequency)
3) Additive White Gaussian Noise (control of 3dB bandwidth)
4) Swept Continuous Waveform (range of sweep and dwell at each frequency)
5) Continuous Waveform (both in/out of phase with other interference sources as required)
6) Customized Waveform (user defined via a prescribed binary file format from Agilent)

Of most interest within this study is the 'Customized Waveform' interference type. This option allows the end user to generate binary data tailored to their individual needs and re-play this data as a modulation type. This capability was exploited within this study in order to

model the communications signals used herein. This feature was used for modulation types 3 to 5 inclusive outlined in the following section.

The test system has the capability to switch interference characteristics at a rate of 1Hz, enabling dynamic and highly configurable test scenarios. Moreover, the GNSS hardware can be updated at a rate of 1 kHz which provides for a high level of fidelity in the resulting simulations.

Interference Modulation Types

The following interference sources have been analyzed within this study:

1) Figure 3 illustrates the Continuous Waveform (CW) signal which is centered at the GPS L1 frequency
2) Figure 4 illustrates the broadband Additive White Gaussian Noise (AWGN) signal (48MHz 3dB bandwidth) which is centered at the GPS L1 frequency
3) Figure 5 illustrates the GSM mobile communications signal which is centered at 900MHz
4) Figure 6 illustrates the Digital Enhanced Cordless Telecommunications (DECT) signal which is centered at 1900MHz
5) Figure 7 illustrates the Long-Term Evolution (LTE) communications signal which has a bandwidth of 10MHz and is centered at 1900MHz

These sources are applied independently of one another to the GNSS signal rather than as a collective interference source.

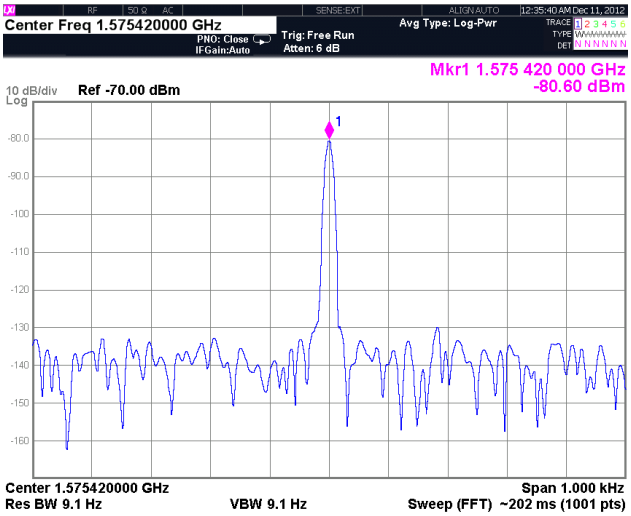

Figure 3: CW Interference Signal

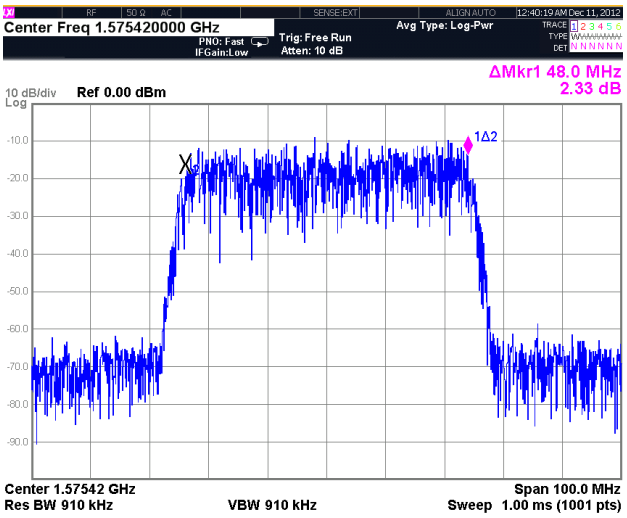

Figure 4: Broadband AWGN (48MHz 3dB bandwidth)

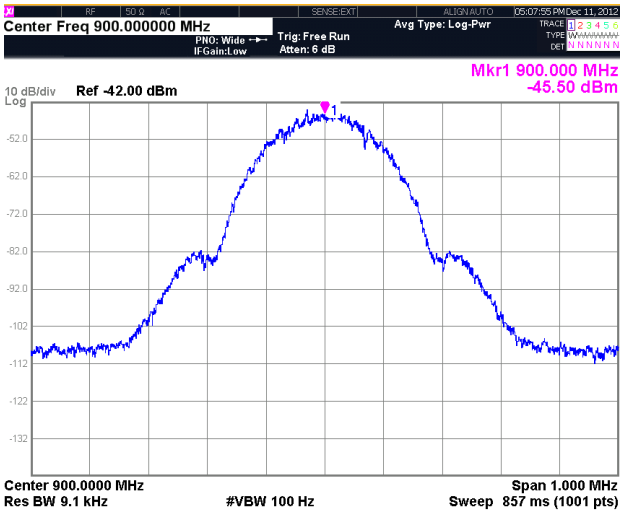

Figure 5: GSM at 900MHz

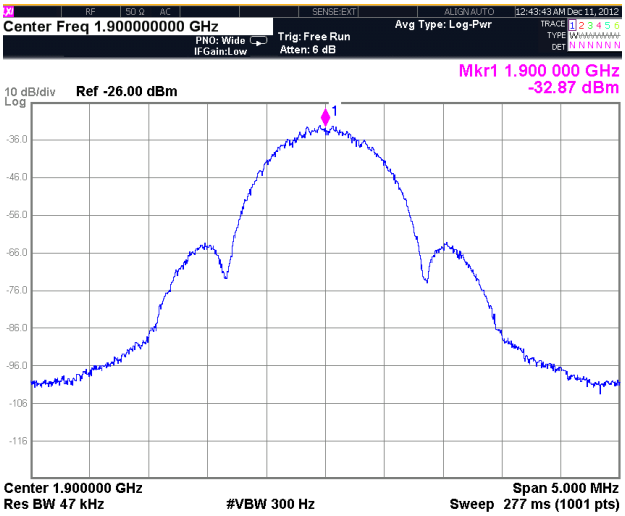

Figure 6: DECT at 1900MHz

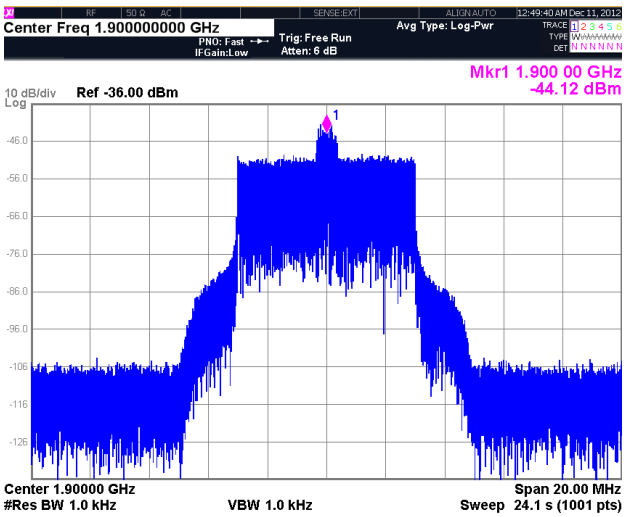

Figure 7: 10 MHz Bandwidth LTE at 1900 MHz

RESULTS

Effect of Interference Source on Receiver C/N_0

The test procedure was conducted as follows. The interference sources were generated and stored for subsequent playback using the COTS signal generator. A SimGEN™ scenario was configured such that the receiving antenna was located at a static position and a GPS L1 constellation transmitting the C/A signal was present. During the first 5 minutes of the scenario the interference source was turned off. This allowed the receiver to acquire and track the GPS satellites prior to the interference source being superposed onto the GPS signal. Subsequently, the interference power level was increased from -140.7dBm in increments of 1dB per minute until the receiver lost lock of the GPS satellites. This procedure was repeated for each interference modulation type. Only a single interference signal was used during each test case. Interference from multiple sources was beyond the scope of this initial investigation.

Figure 8 illustrates how the receiver C/N_0 varies as a function of the interference source power level for the CW, broadband noise (AWGN), GSM, DECT and LTE signals. It is clear from this result that, of the interference types studied, the CW and AWGN jamming causes the most disruption to the GPS L1 signal. This was expected because these interference sources are defined exactly at the GPS L1 center frequency of 1575.42MHz. Table 1 provides a summary of the measurement data for interference power level (dBm) and GPS Receiver C/N_0 (dB-Hz) for each interference source in the study.

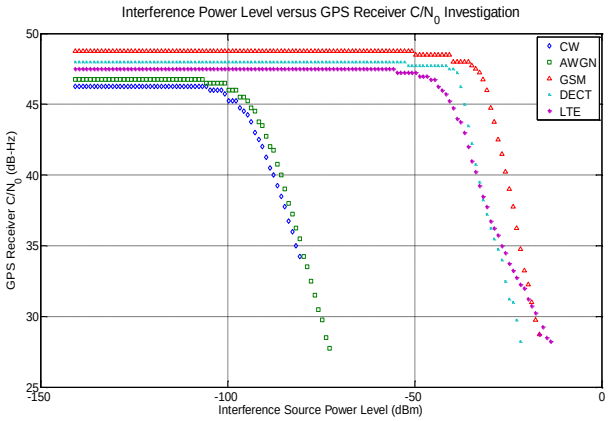

Figure 8: Interference Power Level versus GPS Receiver C/N_0

Interference source	Center Frequency, MHz	Interference Power Level, dBm	Receiver C/N_0, dB-Hz
Coherent CW	1575.42	-140.7 to -80.7	46.25 to 34.25
Broadband Noise	1575.42	-140.7 to -72.7	46.75 to 27.75
GSM	900	-140.7 to -16.7	48.75 to 28.75
DECT	1900	-140.7 to -21.7	48.00 to 28.25
LTE	1900	-140.7 to -13.7	47.50 to 28.25

Table 1: Interference Power Level versus GPS Receiver C/N_0 Summary

Effect of Interference Sources on Receiver Tracking Capability

CW Interference Source

The scenario configuration used to examine the effect of the CW interference source on the GPS L1 signal reception at the receiver comprised of the following:

a) The test duration was 40 minutes
b) Interferer turned off for the first 5 minutes of the scenario
c) Coherent CW signal power level increased from -110.7dBm to -80.7dBm in increments of 1dB per minute
d) Interferer turned off for the last 4 minutes of the scenario

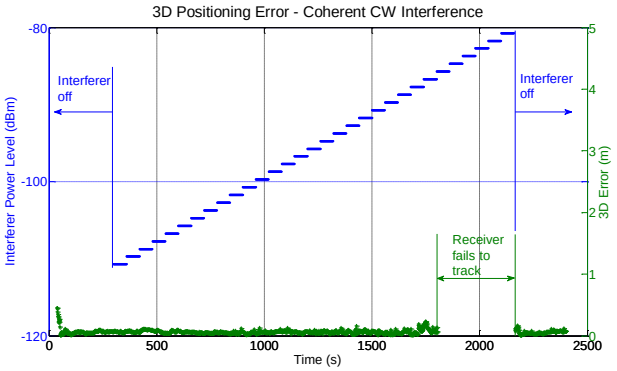

Figure 9: 3D Positioning Accuracy - Coherent CW Interference

According to Figure 9, the receiver 3D positioning accuracy does not deteriorate significantly as the power level of the coherent CW interference source increases. However, when the CW interference power exceeds a level of -86dBm the C/N_0 ratio drops significantly and the satellite signals are no longer tracked by the receiver. This result is as expected; the frequency of the interference source is centered on the GPS L1 signal.

Broadband Noise Interference Source

The scenario configuration used to examine the effect of the broadband noise interference source on the GPS L1 signal reception at the receiver comprised of the following:

a) The test duration was 50 minutes
b) Interferer turned off for the first 5 minutes of the scenario
c) 48MHz 3dB bandwidth broadband AWGN signal power level increased from -110.7dBm to -71.7dBm in increments of 1dB per minute
d) Interferer turned off for the last 5 minutes of the scenario

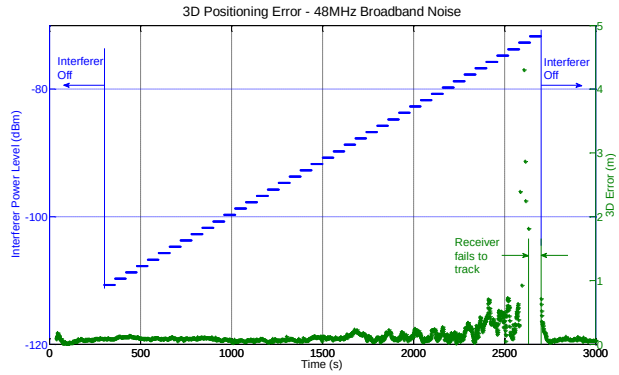

Figure 10: 3D Positioning Accuracy – 48MHz Broadband Noise Interference

In this instance it is notable that the receiver 3D positioning accuracy deteriorates significantly as the power level of the AWGN interference source increases (Figure 10). The GPS signal is completely drowned by the AWGN signal when the AWGN signal power level exceeds -72dBm. The receiver noise floor is gradually increased with escalating interferer source level. This causes the receiver to have difficulty in extracting the signal from the background noise.

GSM Interference Source

The scenario configuration used to examine the effect of the GSM interference source on the GPS L1 signal reception at the receiver comprised of the following:

a) The test duration was 60 minutes
b) Interferer turned off for the first 5 minutes of the scenario
c) GSM signal power level increased from -59.7dBm to -12.7dBm in increments of 1dB per minute
d) Interferer turned off for the last 7 minutes of the scenario

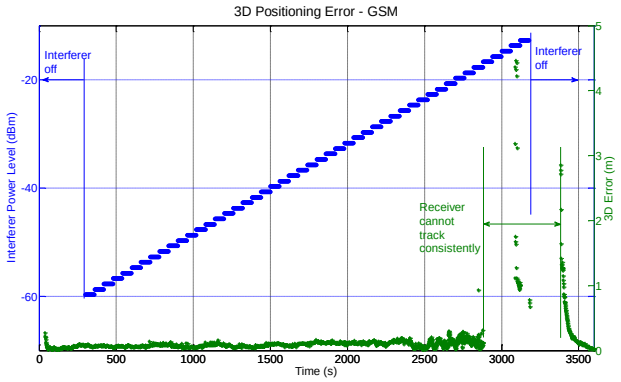

Figure 11: 3D Positioning Accuracy – GSM Interference

The receiver 3D positioning accuracy deteriorates as the GSM interference power level increases, even though the GSM signal is not centered on the GPS L1 frequency (Figure 11). When the GSM power exceeds a level of -17dBm the C/N_0 drops significantly and the satellites are no longer tracked by the receiver. The receiver then has the task of recovering the satellites again once this interference source is turned off. It is possible that this effect may be seen when the GPS L1 receiver is in close proximity to a GSM base station. Under such circumstances the GSM out-of-band side-lobes would interfere with the GPS L1 signal.

DECT Interference Source

The scenario configuration used to examine the effect of the DECT interference source on the GPS L1 signal reception at the receiver comprised of the following:

a) The test duration was 60 minutes
b) Interferer turned off for the first 5 minutes of the scenario
c) DECT signal power level increased from -59.7dBm to -14.7dBm in increments of 1dB per minute
d) Interferer turned off for the last 9 minutes of the scenario

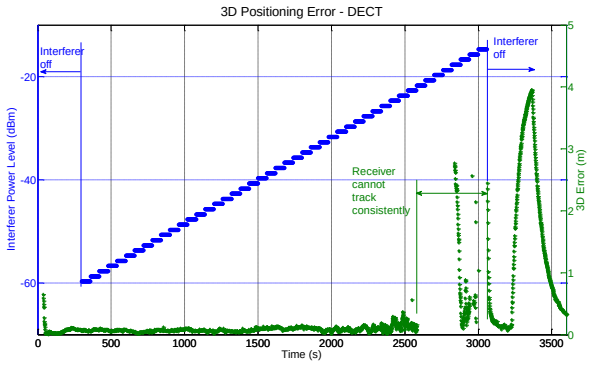

Figure 12: 3D Positioning Accuracy – DECT Interference

The receiver lost the ability to consistently track the GPS satellites when the DECT interference power level exceeded -22dBm (Figure 12). Once the DECT interference had been removed, the receiver momentarily deviates off course and subsequently takes ~12 minutes to recover its' position accuracy. The average transmit power of the DECT signal in Europe is 10mW (4mW in USA) [7]. Devices using this modulation are commonplace in the household and thus possess an obvious threat to GNSS receiver tracking.

LTE Interference Source

The scenario configuration used to examine the effect of the LTE interference source on the GPS L1 signal reception at the receiver comprised of the following:

a) The test duration was 65 minutes
b) Interferer turned off for the first 5 minutes of the scenario
c) LTE signal power level increased from -59.7dBm to -5.7dBm in increments of 1dB per minute
d) Interferer turned off for the last 5 minutes of the scenario

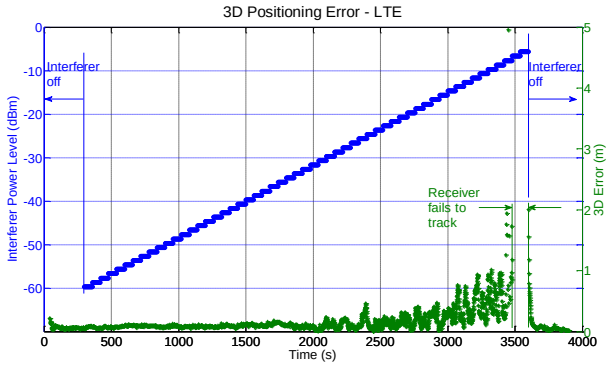

Figure 13: 3D Positioning Accuracy – LTE Interference

The receiver 3D positioning accuracy deteriorates as the LTE interference power level increases (Figure 13). The GPS signal is completely drowned by the LTE signal when the LTE signal power exceeds -7dBm. However, as the LTE signal is pulsing in nature, the receiver is more immune to the LTE interference source and thus can tolerate higher interference signal levels.

CONCLUSIONS

This paper examined the effect of various interference sources on the tracking capability and navigation performance of a commercially available GPS receiver. The C/N_0 for the GPS L1 C/A signal was measured to examine the receiver immunity to the interference sources. In addition, the receiver's navigation performance with respect to the interference power was also examined. The results were collected under laboratory conditions using a bespoke simulator system coupled with a COTS signal generator and proprietary Spirent SimGEN™ software.

It is evident from the results presented that the positioning accuracy of the receiver is compromised under all interference sources examined, with the magnitude of performance degradation dependent upon the interference type and received power. The tracking capability of the receiver is also affected by the presence of the interference sources; the level to which the interference source disrupts the GNSS receiver has been shown to be a function of the interference source modulation characteristics. Moreover, studying the effect that different interference types have on the performance of a GNSS receiver can provide some insight into how one might expect the receiver to operate in a hostile electromagnetic environment. However, it is evident from the literature [4] that even though two interference sources have an identical specification their effect can vary. The methodology presented within this study can easily be extended to take into account any temporal changes in the interference source.

Results also indicate that the interference source does not necessarily need to be located at the same frequency as the GPS signal in order for it to adversely affect the receiver performance. However, the detection of multiple GNSS frequencies in the receiver should provide some additional jamming immunity; the effect of an intentional interference source which is targeted at a particular GNSS frequency band will likely be less pronounced within an adjacent GNSS frequency band.

FURTHER WORK

The simulations performed during this study have highlighted the need for further investigation into the effects of different interference sources on GNSS receiver performance. Specifically, there is a need to examine how resilient receiver technologies are to various types of interference when the GNSS receiver is using additional constellations such as GLONASS, COMPASS and Galileo. Receivers which can employ multiple GNSS constellations simultaneously are purportedly less susceptible to interference [2]. Further to this, it is clear that multiple interference sources are likely to be present during the reception of the GNSS signal and this aspect should be studied further. Future investigations could also include the impact on aided GPS receivers, such as GPS/INS navigation systems, repeating the tests herein under signal acquisition conditions or incorporate additional interference signals, whether intentional or unintentional, to exploit Spirent's flexible custom waveform capability.

Recent modernization programs for existing GNSS services and new services such as COMPASS and GPS Block IIF and III, often provide higher transmission powers and improved modulation schemes which aid the receiver in tracking the satellites in the presence of interference [2]. Whilst various interference mitigation techniques have been developed, they are often reliant on the type of antenna technology deployed, for instance controlled reception pattern antenna (CRPA) systems. Such schemes are not generally available for commercial GNSS receivers purely based on cost implications or physical size and hence there is a need to further characterize the performance of COTS GNSS receivers in any combination of intentional and/or unintentional hostile electromagnetic interference environments.

ACKNOWLEDGMENTS

We would like to take this opportunity to express our gratitude to Spirent Communications Plc. who supported this initiative.

REFERENCES

1. Pullen S., Gao G., "GNSS Jamming in the Name of Privacy", Inside GNSS, March/April 2012.
2. Kuusniemi, H., "Effect of GNSS jammers and potential mitigation approaches", United Nations/Latvia Workshop on the Applications of GNSS, 2012
3. Kaplan E., "Understanding GPS: Principles and Applications", Artech House, 1996.
4. Mitch R.H., Dougherty R.C., Psiaki M.L., Powell S.P., O'Hanlon B.W., Bhatti J.A. and Humphreys T.E., "Signal Characteristics of Civil GPS Jammers", Proceedings of the ION GNSS conference, 2011.
5. Clynch, J. R., Parker A. A., Adler R. W., Vincent W. R., McGill P., and Badger G., "The Hunt for RFI," GPS World, January 2003.
6. http://www.nautilusint.org/Resources/Telegraph%20Files/January%202010.pdf
7. http://www.etsi.org/technologies-clusters/technologies/dect

White paper from the ITM 2013 Proceedings
30th January 2013 San Diego, California
The Institute of Navigation
8551 Rixlew Lane, Suite 360, Manassas, VA 20109
www.ion.org