Jammer Impact on Galileo and GPS Receivers

Daniele Borio, Cillian O'Driscoll, Joaquim Fortuny
EC Joint Research Centre, Institute for the Protection and Security of the Citizen, Ispra, Italy

***Abstract*—Global Navigation Satellite Systems (GNSSs) are vulnerable to several threats including jamming and spoofing. Jamming is the deliberate transmission of powerful Radio-Frequency (RF) signals which can easily overpower the much weaker GNSS components disturbing and, in some cases, denying GNSS operations. In recent years an increasing number of cheap, though illegal, jammers have become commercially available. In this paper, the impact of these jammers on Global Positioning System (GPS) and Galileo L1/E1 signal reception is investigated. It is shown that the signals of each system are affected in similar ways and this is due to the wide-band nature of the jamming signals. Narrow-band receivers are less impacted by jamming since they are able to filter out a greater portion of the interfering signal. Interestingly, the presence of a pure pilot channel in the Galileo E1 modulation allows receivers to use a pure Phase Lock Loop (PLL) which in turn allows signal reception in the presence of stronger jamming signals with respect to the GPS L1 C/A case.**

I. Introduction

GNSSs are able to provide precise location and timing information which find use in several applications. The usage of GNSSs is not limited to personal and car navigation but, for example, they can be employed for the tracking of goods and animals, to locate trains, navigate ships and for sport applications.

In addition to this, new GNSS applications are currently under development or consolidation. For example, GPS boxes can be used by insurance companies to monitor the behaviour of a driver and adjust the insurance premium accordingly. GPS and GNSSs in general enable 'pay-as-you-drive' applications which also require the monitoring of the user behaviour. This type of application inevitably introduces privacy issues since GNSSs are used to collect information on GNSS users. This motivates the development and use of devices which can deny GNSS signal reception [1].

A number of GNSS jammers have been acquired by the Institute for the Protection and Security of the Citizen (IPSC) of the Joint Research Centre (JRC) for the purpose of evaluating their potential impact on European Critical Infrastructure (CI). Several tests were performed and the impact on commercial, mass market and Software Defined Radio (SDR) GNSS receivers has been determined experimentally. The tests were conducted in a large anechoic chamber on the JRC premises, which is equipped with a Spirent GSS8000 simulator, which is able to generate both GPS and Galileo signals in the L1/E1 band. In this way, it was possible to assess the impact of jammers on both Galileo and GPS receivers. In the previous literature, only GPS receivers were considered and this is the first analysis including Galileo receivers. This allows a comparison between the two systems.

The remainder of this document is organized as follows. Models for GNSS and jammer signals are discussed in Section II. These models are used as a basis for interpreting the experimental results described in the subsequent sections. Section III describes the experimental setup and discusses the findings obtained testing the impact of jammers on GNSS receivers. Conclusions are finally drawn in Section IV.

II. GNSS and Jammer Signal Models

In this section, models for the GNSS and jammer signals are provided and the concept of coherent Signal-to-Noise Ratio (SNR) at the receiver correlator output is also introduced.

A. Received GNSS Signal

The signal at the input of a GNSS receiver in a one-path additive Gaussian channel and in the presence of interference can be modelled as

$$r(t) = \sum_{l=0}^{L-1} y_l(t) + i(t) + \eta(t), \quad (1)$$

which is the sum of L useful signals, the interfering signal, $i(t)$, generated by the GNSS jammer and a noise term, $\eta(t)$. Each useful signal, $y_l(t)$, can be expressed as

$$y_l(t) = \sqrt{2C_l} d_l\left(t - \tau_{0,l}\right) c_l\left(t - \tau_{0,l}\right) \times \cos\left(2\pi(f_{RF} + f_{0,l})t + \varphi_{0,l}\right), \quad (2)$$

where: C_l is the power of the lth useful signal; $d_l(\cdot)$ is the navigation message; $c_l(\cdot)$ is the lth pseudo-random sequence chosen from a family of quasi-orthogonal codes used for spreading the signal spectrum; $\tau_{0,l}$, $f_{0,l}$ and $\varphi_{0,l}$ are the delay, Doppler frequency and phase introduced by the communication channel; f_{RF} is the centre frequency of the GNSS signal. The spreading code, $c_l(\cdot)$, usually consists of several components

$$c_l(t) = \sum_{i=-\infty}^{\infty} c_l[i \mod N_c] s_b(t - iT_{ch}) \quad (3)$$

where $\{c_l[i]\}_{i=0}^{N_c-1}$ is a Pseudo Random Noise (PRN) sequence of length N_c and $s_b(\cdot)$ is the subcarrier. The sequence $\{c_l[i]\}_{i=0}^{N_c-1}$ is discrete in nature and it is interpolated by the subcarrier, a waveform of finite duration, T_{ch}, which determines the spectral characteristics of the GNSS signal [2]. The signal (1) is filtered and down-converted by the receiver front-end before being digitized. In the following, the effects of quantization are neglected and it is assumed that the signal is sampled without introducing significant distortion. In addition, due to the quasi-orthogonality of the spreading codes the L useful signals can be considered independently, such that, after down-conversion and sampling, (2) becomes:

$$r_{BB}[n] = y_{BB}(nT_s) + i_{BB}(nT_s) + \eta_{BB}(nT_s) \quad (4)$$

where the notation $x[n]$ is used to denote a discrete time sequence sampled at the frequency $f_s = \frac{1}{T_s}$. The index "BB" is used to denote a signal down-converted to base-band.
The noise term, $\eta_{BB}[n]$, is assumed to be complex Additive White Gaussian Noise (AWGN) with independent and identically distributed (i.i.d.) real and imaginary parts with variance σ^2. This variance depends on the filtering, down-conversion and sampling strategy applied by the receiver front-end and is given by $\sigma^2 = \frac{1}{2} N_0 B_{Rx}$, where B_{Rx} is the front-end two-sided bandwidth and N_0 is the Power Spectral Density (PSD) of the input noise, $\eta(t)$. The ratio between the carrier power, C, and the noise power spectral density, N_0, defines the Carrier-to-Noise power spectral density ratio (C/N_0), one of the main signal quality indicators used in GNSS.

B. Jammer Signal Model

The down-converted interference signal, $i_{BB}(nT_s)$, can assume different forms depending on the jammer that generates it and the effect of the GNSS receiver front-end. Some effort has previously been devoted to the analysis and characterization of civilian GPS jammers (see, for example, [3], [4]) and, despite significant differences, the transmitted signal is usually frequency modulated with an almost constant amplitude.
In this case $i_{BB}(nT_s)$ can be approximately modelled as

$$i_{BB}(nT_s) = A_i \exp\left\{j 2\pi \Phi(nT_s) nTs + j\varphi_i\right\} \quad (5)$$

where A_i is the interfering signal amplitude, $\Phi(nT_s)$ is its time-varying frequency and φ_i an initial phase term. It is noted that (5) neglects several signal properties and more complex models can be adopted [5]. Model (5) is however able to capture most important features of $i_{BB}(nT_s)$.

C. The correlation process

The base-band quantized signal $r_{BB}[n]$ is correlated with local replicas of the useful signal code and carrier. It is noted that the computation of correlator outputs is essential for the proper functioning of a GNSS receiver and they are used both in acquisition and tracking [6], the main receiver operating modes. Thus, the quality of a GNSS signal can be defined after correlation as [7], [8]:

$$\mathrm{SNR}_{\mathrm{out}} = \max_{\tau, f_d, \varphi} \frac{\left|\mathrm{E}\left\{P\right\}\right|^2}{\frac{1}{2}\mathrm{Var}\left\{P\right\}} \quad (6)$$

where P is the complex correlator output and $\mathrm{SNR}_{\mathrm{out}}$ is the coherent output SNR. The factor $1/2$ in (6) accounts for the fact that P is a complex quantity and only the variance of its real part is considered. The loss experienced at the correlator output due to the presence of jamming can be determined as the ratio between the measured SNR and the ideal coherent output SNR determined in the absence of interference.

Using the results derived in [7]–[9], it is possible to express the coherent output SNR as

$$\mathrm{SNR} = \frac{C}{\frac{N_0}{2T_c} + \frac{J}{2T_c} k_a} = 2\frac{C}{N_0} T_c \frac{1}{1 + \frac{J}{N_0} k_a}. \quad (7)$$

where J is the jammer power and T_c the coherent integration time. k_a is the Spectral Separation Coefficient (SSC) defined as [7], [8]

$$k_a = \int_{-B_{Rx}/2}^{B_{Rx}/2} G_J(f) G_c(f) df. \quad (8)$$

$G_J(f)$ is the PSD of the jamming signal normalised to unit power in the jammer transmit bandwidth B_J

$$\int_{-B_J/2}^{B_J/2} G_J(f) df = 1. \quad (9)$$

$G_c(f)$ models the effect of the correlation on the interfering signal. Correlation can be modelled as an additional filtering stage and $G_c(f)$ can be shown to be well approximated by the PSD of $s_b(t)$, the subcarrier used in the de-spreading process. $G_c(f)$ is also normalized to have a unit integral over its transmit bandwidth.

The ideal coherent SNR is obtained by setting $J/N_0 = 0$:

$$\mathrm{SNR}_{\mathrm{ideal}} = 2\frac{C}{N_0} T_c \quad (10)$$

and the loss due to the interference presence is given by

$$L_i = \frac{1}{1 + \frac{J}{N_0} k_a}. \quad (11)$$

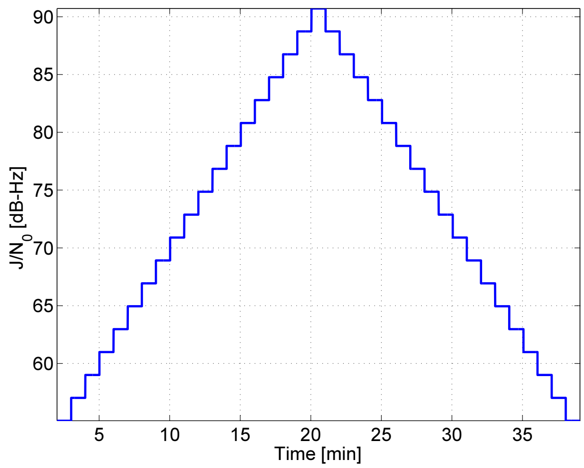


Fig. 1. Calibrated J/N_0 at the output of the active GNSS antenna vs time.

In the following, the loss L_i will be empirically determined. Most GNSS receivers estimate the C/N_0 by first estimating the coherent output SNR [10] then using relationship (10). Thus, C/N_0 estimates can be used for determining L_i and, hence, empirical estimates of k_a. This is a common approach [11]. Note that the k_a is strongly impacted by the receiver front-end: narrow-band front-ends better shield the receiver against interference. This will be seen in more detail in Section III.

III. Impact on GNSS receivers

In this section, the impact of jammers on Galileo and GPS receivers is analysed.

A. Experimental Setup

In order to determine the impact of a jamming signal on different GNSS receivers, experiments were conducted in the JRC anechoic chamber. A Spirent GSS8000 simulator was used to provide a controlled GPS and Galileo constellation, with a static receiver under nominal open sky conditions. The GNSS signals were broadcast from an RHCP antenna mounted on a movable sled on the ceiling of the chamber. A survey grade GNSS antenna was mounted inside the chamber and the sled was positioned at a distance of approximately 10 metres from this antenna. The GNSS receiving antenna was connected via a splitter to: a spectrum analyser for calibration purposes; an NI PXI-5663 RFSA for collecting raw base-band data with approximately 10 MHz RF bandwidth; 4 commercial GNSS receivers. For the experiment, a cigarette-lighter jammer broadcasting a single saw-tooth chirp signal was used. The jammer is able to span a 12 MHz bandwidth in about 9 μs. More details about the jammer used for the experiment can be found in [12] (jammer no. 6 was used).

The jammer's antenna port was connected through a programmable attenuator with up to 81 dB of attenuation to a linearly polarized standard gain horn antenna, positioned approximately 3 m from the GNSS receiving antenna. The attenuator was used to vary the transmitted power and simulate different values of received J/N_0.

The experimental procedure involved two trials, each lasting approximately 40 minutes. In the first the simulator and data collection equipment were both enabled, but the jammer remained powered off. The second was identical, but the jammer was enabled and the desired attenuation profile was applied. The received J/N_0 was computed as a function of the attenuator setting using the procedure described in [13], and is illustrated in Fig. 1. The following analysis is conducted using the J/N_0 as a measure of the impact of the jammer.

The experimental setup is described in more detail in [13].

B. Results

The experimental setup described above allows the collection of two different types of data:

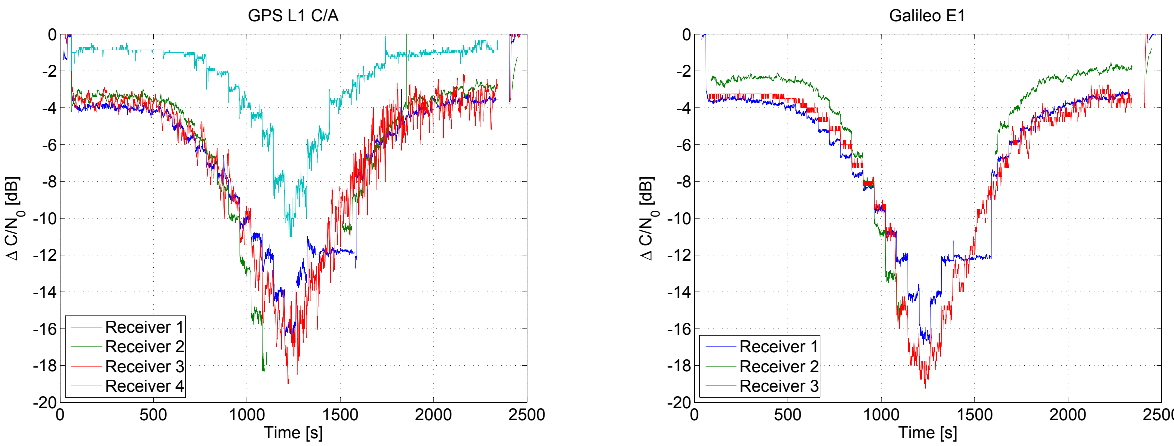
- Measurements from four commercial GNSS receivers.
- Raw base-band samples containing GPS and Galileo signals contaminated by a jamming component.

The raw data were subsequently processed with a SDR receiver able to track both GPS and Galileo signals. Similar to the case of commercial receivers, C/N_0 values computed with the SDR receiver were used to compute the C/N_0 loss caused by the jammer.

The four commercial receivers under tests were

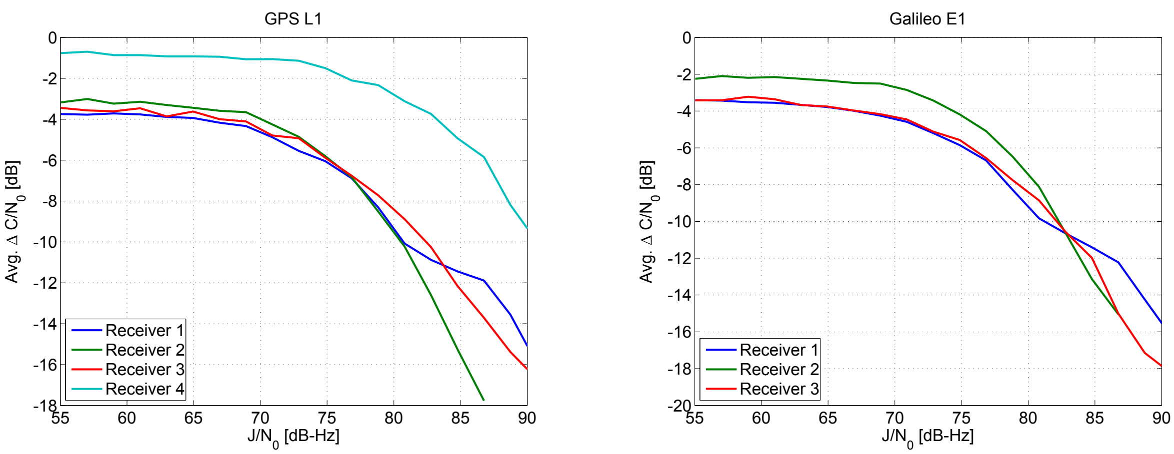
- Receivers 1–3: survey grade multi-frequency multi-system receivers from three different manufacturers
- Receiver 4: High Sensitivity (HS) single frequency GPS only receiver

Fig. 2 a) shows the loss in C/N_0 experienced in the presence of the jammer as a function of the J/N_0 for the four commercial receivers in the GPS case. When the jammer is turned on, a negative jump in the C/N_0 loss curves is clearly observed. This is due to the fact that even with a total attenuation of 81 dB (the maximum value obtainable with the variable attenuator used for the tests) the jammer still causes a significant noise increase. In particular, the noise power measured in a 12 MHz bandwidth in the absence of jamming was -74.85 dBm. When the jammer is turned on and the attenuation is set to 81 dB, the noise power measured with



a) GPS b) Galileo

Fig. 2. C/N_0 loss experienced by receivers in the presence of a jamming signal



a) GPS b) Galileo

Fig. 3. Average C/N_0 loss experienced as a function of the received J/N_0

the spectrum analyzer in the same bandwidth is -70.85 dBm. A 4 dB noise increase is experienced in a 12 MHz bandwidth. This justifies the results in Fig. 2 a): the HS receiver probably has a front-end bandwidth lower than 12 MHz and only a portion of the additional equivalent noise caused by the jammer enters the receiver. Thus, the initial loss is only about 1 dB. The other three receivers are wideband with front-end bandwidths equal to or greater than 12 MHz: for this reason all the C/N_0 loss curves experience an initial degradation of about 4 dB.

As expected the HS is the most resilient against interference and hence experiences the least loss. The other three receivers have similar performance. The impact of jamming on the Galileo E1 signal is analysed in Fig. 2 b). The C/N_0 loss curves exhibit a similar behaviour to those obtained for the GPS case. Since the jammer signal is wideband, GPS and Galileo signals are affected in a similar way. This fact is discussed in Section III-C where the SSCs for the different receivers and signals are determined and compared. C/N_0 losses are further analysed in Figs. 3 a) and b) where the loss is plotted as function the J/N_0 measured at the receiver antenna. The loss has been averaged over all time instants having by the same J/N_0. From the curves it emerges that professional receivers have similar performance whereas the HS is more resilient to jamming. Results obtained using a custom SDR receiver are shown in Fig. 4 where the average C/N_0 loss is plotted as a function of the jammer J/N_0. In this case, the initial loss due to the jammer activation is lower than in the case of commercial receivers. This is likely due to the front-end of the NI RFSA used for the data collection. As for the previous case, GPS and Galileo processing are affected in a similar way. This confirms that the receiver front-end has a

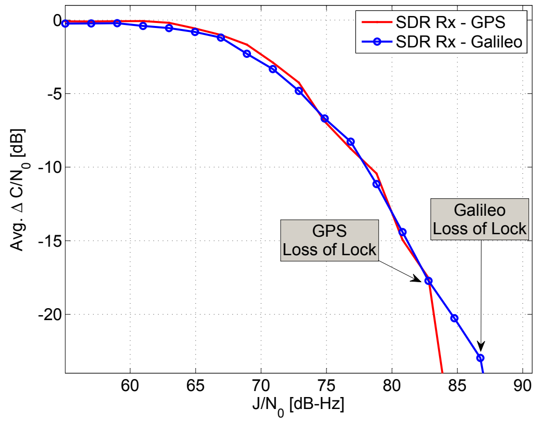


Fig. 4. Average C/N_0 loss experienced by a SDR receiver when processing GPS and Galileo signals in the presence of a jamming signal. The loss is provided as a function of the jammer J/N_0.

greater impact in determining the jamming impact than the signal type.

From Fig. 4, one noticeable difference emerges between the GPS and Galileo signals: the tracking threshold of the Galileo signals is approximately 6 dB lower than that for the GPS signals. This is due to the use of a pure PLL processing strategy using only the E1C (pilot) component of the Galileo signal.

C. SSC Analysis

In this section, the experimental results discussed in Section III-B are analysed in terms of the SSC theory introduced in Section II-C. In particular, experimental data are interpolated using an extension of model (11). As discussed above, when a jammer is activated a significant C/N_0 loss is introduced even if its signal is strongly attenuated. Thus, model (11) needs to be modified in order to account for this initial loss. This is achieved by introducing the term L_0 and adopting the following model

$$L_i = \frac{L_0}{1 + k_a \frac{J}{N_0}}. \quad (12)$$

In this way, the final loss is expressed as the combination of the activation loss, L_0, and the degradation due to the jamming signal itself.

Experimental data and model fit are compared in Fig. 5 for the four commercial receivers described above. For the interpolation, only loss values above -10 dB were considered, since model (12) does not account for quantization and Automatic Gain Control (AGC) scaling. For high J/N_0, i.e. for large loss values, these factors start to play a significant role and deviations from (12) are expected. From Fig. 5, a good agreement between experimental data and the corresponding model fit clearly emerges. Model (12) effectively describes the impact of a jamming signal on a GNSS receiver. As already indicated the model is particularly effective for low J/N_0 values.

TABLE I
ESTIMATED ACTIVATION LOSS AND SSC FOR THE FOUR COMMERCIAL RECEIVERS CONSIDERED.

Receiver	GNSS	L_0 (dB)	k_a (dB-Hz^{-1})
1	GPS	-3.8	-76.3
1	Galileo	-3.0	-76.3
2	GPS	-2.9	-74.8
2	Galileo	-2.0	-76.4
3	GPS	-3.6	-77.1
3	Galileo	-3.4	-76.6
4	GPS	-0.8	-82.8

Fig. 5 allows one to directly compare the impact of jamming on the processing of GPS and Galileo signals. In the case of receivers 1 and 3, GPS and Galileo signals are affected essentially in the same way. When receiver 2 is considered, the processing of GPS signals seems to be more affected by the jamming signal. The difference is mainly due to a higher activation loss, L_0. This difference is however less than 1 dB. The activation loss and the SSC, k_a, obtained interpolating the experimental data are reported in Table I.

IV. CONCLUSIONS

In this paper, five receivers (one mass-market, three professional and one software-based) were tested in the presence of jamming. Four of these receivers are Galileo capable and thus they were used for assessing the impact of jamming on both GPS and Galileo signal reception. From the analysis, it emerges that GPS and Galileo receivers are affected in a similar way by jamming signals. This fact was expected since jamming signals are perceived by the receiver as wide-band noise which has similar spectral separation with respect to the GPS L1 Coarse/Acquisition (C/A) and Galileo E1 modulations. On the other hand, the receiver type strongly influences the impact of jamming. For example, the HS receiver tested has a narrower front-end bandwidth than the professional ones. In this way, a reduced portion of the jamming signal enters the receiver which is, therefore, more resilient to this type of interference. Finally, it has been shown that the availability of a pure pilot channel in the Galileo E1 signal allows a receiver to operate in the presence of stronger jamming components. This is due to the fact that a pure PLL can be used for signal tracking.

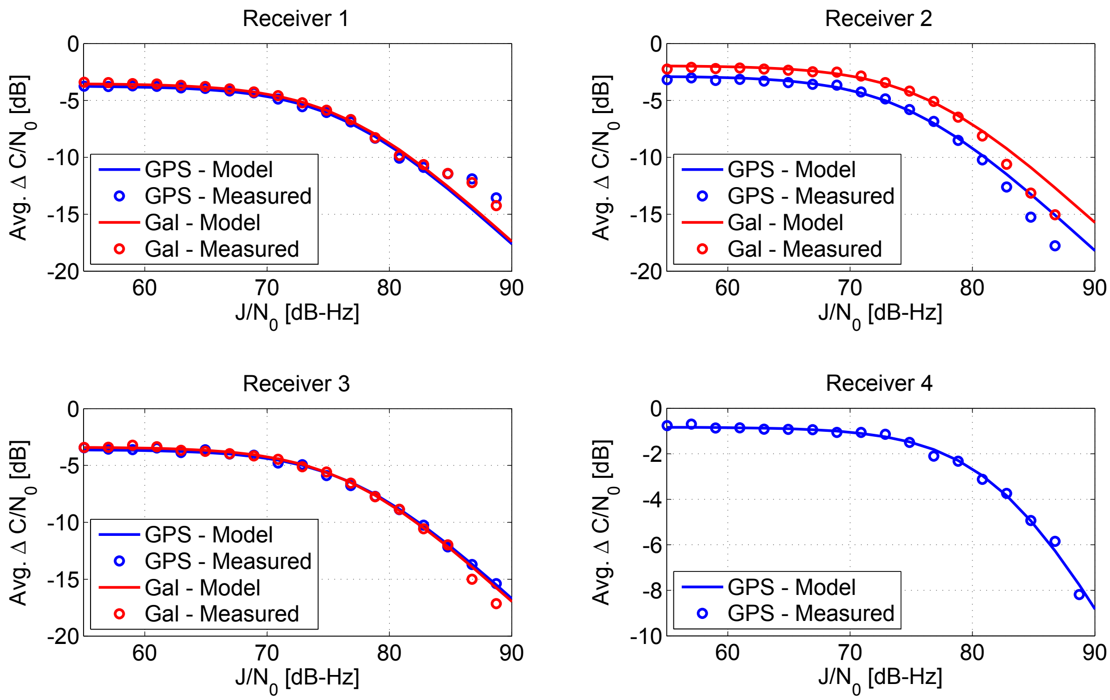


Fig. 5. Comparison of experimental data and model fit for different GPS/Galileo receivers.

ACKNOWLEDGMENTS

The authors would like to express their thanks to the partners of the GSA FP7 DETECTOR project for the support provided in this measurement campaign, in particular for the loan of the jammer used for the tests.

REFERENCES

[1] S. Pullen and G. Gao, "GNSS jamming in the name of privacy," *Inside GNSS*, pp. 34–43, March/April 2012.

[2] C. O'Driscoll and J. Fortuny-Guasch, "On the determination of C/A code self-interference with application to RFC analysis and pseudolite systems," in *Proc. of the 25th International Technical Meeting of the Institute of Navigation ION/GNSS*, Nashville,TN, Sep. 2012, pp. 3620–3631.

[3] R. H. Mitch, R. C. Dougherty, M. L. Psiaki, S. P. Powell, B. W. O'Hanlon, J. A. Bhatti, and T. E. Humphreys, "Signal characteristics of civil GPS jammers," in *Proc. of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION/GNSS)*, Portland, OR, Sep. 2011, pp. 1907–1919.

[4] T. Kraus, R. Bauernfeind, and B. Eissfeller, "Survey of in-car jammers - analysis and modeling of the RF signals and IF samples (suitable for active signal cancelation)," in *Proc. of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation ION/GNSS*, Portland, OR, Sep. 2011, pp. 430–435.

[5] R. H. Mitch, M. L. Psiaki, B. W. O'Hanlon, S. P. Powell, and J. A. Bhatti, "Civilian GPS jammer signal tracking and geolocation," in *Proc. of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation*, Nashville, TN, Sep. 2012, p. 20.

[6] E. D. Kaplan and C. Hegarty, Eds., *Understanding GPS: Principles and Applications*, 2nd ed. Artech House Publishers, Nov. 2005.

[7] J. W. Betz, "Effect of partial-band interference on receiver estimation of C/N_0: Theory," in *Proc. of the 2001 National Technical Meeting of The Institute of Navigation*, Long Beach, CA, Jan. 2001, pp. 817–828.

[8] ——, "Effect of narrowband interference on GPS code tracking accuracy," in *Proc. of the 2000 National Technical Meeting of The Institute of Navigation*, Anaheim, CA, Jan. 2000, pp. 16–27.

[9] D. Borio, "A statistical theory for GNSS signal acquisition," PhD Thesis, Politecnico di Torino, Apr. 2008.

[10] B. W. Parkinson and J. J. Spilker, *Global Positioning System: Theory and Applications Volume 1*, ser. Progress in Astronautics and Aeronautics. American Institute of Astronautics and Aeronautics, 1996, vol. 163.

[11] Technical Working Group (TWG), "Lightsquared-GPS technical working group final report," Federal Communication Commission, Washington, D.C., Tech. Rep., Jun. 2011.

[12] D. Borio, J. Fortuny-Guasch, and C. O'Driscoll, "Spectral and spatial characterization of GNSS jammers," in *Proc. of the 7th Annual GNSS Vulnerabilities and Solutions Conference*, Baska, Croatia, Apr. 2013, pp. 1–15.

[13] D. Borio, C. O'Driscoll, and J. Fortuny, "GNSS jammers: Effects and countermeasures," in *Proc. of the 6th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing*, Dec. 2012, pp. 1–7.