Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers

INVITED PAPER

Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers

This paper provides a comprehensive discussion of jamming effects on commercial GNSS receivers. The main types of jammers are discussed as well as state-of-the-art detection methods.

By Daniele Borio, Fabio Dovis, Heidi Kuusniemi, and Letizia Lo Presti

ABSTRACT | Jamming is the act of intentionally directing powerful electromagnetic waves toward a victim receiver with the ultimate goal of denying its operations. This paper describes the main types of Global Navigation Satellite System (GNSS) jammers and reviews their impact on GNSS receivers. A survey of state-of-the-art methods for jamming detection is also provided. Different detection approaches are investigated with respect to the receiver stage where they can be implemented.

KEYWORDS | Detection; Global Navigation Satellite System (GNSS); interference; jamming

I. INTRODUCTION

Received Global Navigation Satellite System (GNSS) signals are very weak and thus vulnerable to both intentional and nonintentional radio-frequency interference (RFI). Jamming is a form of intentional RFI generated by devices, called jammers, which deliberately transmit powerful signals at the GNSS frequencies. Jammers can disrupt GNSS-based services in wide geographical areas with radii of several kilometers [1] and, despite the fact that their usage is illegal in most countries, their rapid diffusion is becoming a serious threat to satellite navigation. Several GNSS applications such as tracking of goods and of animals, train and ship localization, sport applications, and pay-as-you-drive services inevitably introduce privacy issues. In particular, these applications are used to collect user location information. This motivates the development and use of devices which can deny GNSS signal reception [2]. A well-known example is the case of a truck driver periodically passing close to the Newark Liberty International Airport. The driver was using a GNSS jammer to prevent his company from tracking his position. The jammer was however so powerful that problems were caused to the reception of wide area augmentation system (WAAS) and GNSS signals. Eventually, after three months of investigation, the authorities were able to identify the problem, locate the jammer, and fine the truck driver [3].

This paper describes the main types of GNSS jammers and reviews their impact on GNSS receivers. Jammer classifications from the literature are discussed and a composite description based on both signal and device characteristics is proposed.

The impact analysis considers the different receiver stages and shows the different effects which can be experienced by a GNSS receiver. Jamming effects strongly depend on the power of the jamming signal and range from a slight performance degradation to a complete loss of position.

The paper also provides a survey of state-of-the-art methods for jamming detection. While many methods are proposed for the more general topic of RFI detection [4]–[7], recent researches considered techniques specifically tailored for jamming signals [2], [8]–[14]. In this paper, different approaches are reviewed and analyzed

Manuscript received October 15, 2015; revised January 6, 2016; accepted February 15, 2016. Date of publication May 2, 2016; date of current version May 18, 2016.
D. Borio is with the Joint Research Centre (JRC), European Commission, 21027 Ispra (VA), Italy (e-mail: daniele.borio@jrc.ec.europa.eu).
F. Dovis and **L. Lo Presti** are with the Department of Electronics and Telecommunications (DET), Politecnico di Torino, 10129 Torino, Italy (e-mail: fabio.dovis@polito.it; letizia.lopresti@polito.it).
H. Kuusniemi is with the Finnish Geospatial Research Institute, National Land Survey, Masala FI-02430, Finland (e-mail: heidi.kuusniemi@nls.fi).
Digital Object Identifier: 10.1109/JPROC.2016.2543266

with respect to the different receiver stages where they can be implemented. The analysis of the countermeasures which can be adopted to mitigate the jamming effect are out of the scope of the paper. A survey on the main general techniques can be found, for example, in [15].

The remainder of this paper is organized as follows. Section II introduces the main characteristics of a jamming signal and discusses different jammer classifications. The impact of jamming is analyzed in Section III whereas jamming detection approaches are presented in Section IV. Finally, conclusions are provided in Section V.

II. SIGNAL MODEL IN THE PRESENCE OF JAMMING

GNSS signals are at first downconverted to intermediate frequency (IF) and transformed in a digital sequence, $s_{\mathrm{IF}}[n] = s_{\mathrm{IF}}(nT_s)$, by the receiver front-end. $T_s = 1/f_s$ is the sampling interval and f_s is the sampling frequency. Received satellite signals are buried in noise and the digital sequence provided by the receiver front-end can be modeled as

$$y[n] = s_{\mathrm{IF}}[n] + w[n] \tag{1}$$

where $w[n]$ is a realization of a zero-mean white discrete-time Gaussian noise $W[n]$ with variance σ_w^2. This random process is obtained by filtering and sampling a white noise, $W(t)$, with power spectral density (PSD) $N_0/2$. Since the bandwidth of the front-end filter is generally of the order of $f_s/2$, the variance of $W[n]$ is approximately

$$\sigma_w^2 = \frac{N_0 f_s}{2}. \tag{2}$$

The useful signal $s_{\mathrm{IF}}[n]$ is given by [16]

$$s_{\mathrm{IF}}[n] = \sum_{i=0}^{I-1} \sqrt{2C_i}\, d_i(nT_s - \tau_i) c_i(nT_s - \tau_i) \cdot \cos\left(2\pi(f_{\mathrm{IF}} + f_{d,i})nT_s + \varphi_i\right) \tag{3}$$

that is the summation of I components transmitted by the satellites in view. In (3), the index i indicates quantities specific to the ith satellite signal. C_i is the received signal power; and τ_i, $f_{d,i}$, and φ_i are the delay, Doppler frequency, and carrier phase introduced by the communication channel on the ith satellite signal, respectively. $c_i(\cdot)$ and $d_i(\cdot)$ model the spreading code and the navigation message whereas f_{IF} denotes the IF used by the receiver front-end. In (3), an IF representation for the useful signal is adopted. Different representations, for example, considering baseband signals [17], could have been adopted.

In the presence of jamming, the IF discrete-time signal recovered by the receiver front-end can be modeled as

$$y[n] = s_{\mathrm{IF}}[n] + vq[n] + w[n] \tag{4}$$

where $q[n]$ is the IF digital version of the signal $q(t)$, generated by a jammer, and v is an amplitude factor. In particular, assuming that $q[n]$ has unit power, the total received jamming power is given by

$$J = v^2. \tag{5}$$

Given these premises, it is possible to define the following metrics which are adopted in the literature to characterize signal and jammer power relationships.

- The carrier-to-noise density power ratio (C/N_0) defined as the ratio of the signal power C and noise PSD N_0. The C/N_0 is continuously estimated by the receiver and it is usually provided in logarithmic units, dB-Hz.
- The jammer-to-noise density power ratio (J/N_0) defined as the ratio of the jamming power J and N_0.
- The jammer-to-signal power ratio (J/S) defined as the ratio between J and C and usually expressed in dB.
- The jammer-to-noise power ratio (J/N) defined as the ratio between J and σ_w^2, the noise power.

A. Jamming Signals

Several papers [1], [2], [18]–[21] have addressed the problem of characterizing the jamming signal $q(t)$. From the analysis, it emerged that most jammers used in a civil context broadcast frequency modulated signals with an almost periodic behavior. Deviations from a perfectly periodic behavior are due to drifts in the local oscillators used for the signal generation. The signal center frequency varies according to a periodic pattern that, in most cases, corresponds to a saw-tooth function. More specifically, $q(t)$ can be modeled as

$$q(t) = \sqrt{2}\cos\left(2\pi\left(f_{\mathrm{RF}} + f_q(t)\right)t + \varphi_q\right) \tag{6}$$

where $f_q(t)$ is the instantaneous frequency of the jamming signal, f_{RF} denotes the radio frequency (RF), and φ_q models the signal phase. The amplitude variations of

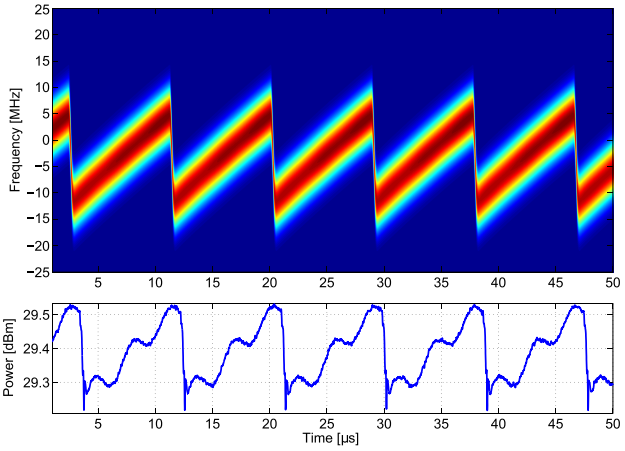

Fig. 1. ***Spectrogram and power of the signal emitted by a cigarette lighter jammer.***

$q(t)$ are usually small (less than 0.5 dB) [1] and thus they are neglected in (6). The amplitude of the jamming signal is accounted for by the multiplicative factor in (4), v, which is considered constant. $f_q(t)$ defines a practically periodic frequency pattern which is characterized by a sweep range, i.e., the frequency interval affected by the jammer signal, and a sweep period which is the time required to span the sweep range. The maximum and minimum values assumed by $f_q(t)$, $f_{\max}$, and $f_{\min}$, also play a fundamental role since they determine the spectral overlap between GNSS and jamming signals.

The spectrogram of the signal emitted by a cigarette lighter jammer is shown in Fig. 1. In this case, $f_q(t)$ defines a piecewise linear pattern with a sweep range of 16.7 MHz and a sweep period of about 8.9 μs. Although the frequency pattern shown in Fig. 1 is quite regular, more complex frequency behaviors can be found [1], [18]–[21]. Fig. 1 also shows the instantaneous power of the jamming signal. The power has been estimated using an analysis window sliding through the samples of the jamming signal: only small power variations can be observed.

The shorter the sweep period, the more difficult it is to mitigate the impact of the jammer. Fast frequency varying signals are more difficult to track and, for example, a notch filter [22] will have more difficulties to estimate the jammer instantaneous frequency and remove the disturbing signal. Sweep periods are typically around 10 μs whereas sweep ranges are usually in the 10–40-MHz interval [1], [21].

The signal model introduced in Section II is related to a single GNSS frequency. However, GNSS jammers can simultaneously broadcast several signals in different GNSS bands. Analysis from the literature [21] shows that no significant differences emerge from jamming signals broadcast in different bands.

Depending on the properties of $f_q(t)$, different classifications have been suggested for GNSS jammers. In particular, Rash [23] divided GNSS jammers into three categories based on the properties of the jamming signal transmitted. This classification was based on the characteristics of the Global Positioning System (GPS) L1 signal which was the only civil signal available in the late 1990s. Moreover, the only form of jamming was military in nature and devices for civil use were not considered. More appropriate classifications have been recently proposed [1], [18]. Kraus *et al.* [18] divided jammers into the following classes:

- class I: CW signals; the jammer transmits a continuous wave (CW) signal;
- class II: single saw-tooth chirp signals; the jammer transmits a frequency-modulated signal with a saw-tooth time-frequency (TF) evolution;
- class III: multi-saw-tooth chirp signals; the device transmits a frequency-modulated signal but its TF evolution is more complex and it is determined by the combination of several saw-tooth functions;
- class IV: chirp with signal frequency bursts; the device transmits a frequency-modulated signal and frequency bursts are used to enlarge the frequency band affected by the disturbing signal.

It is noted that model (6) is general and can be used to describe signals belonging to the four classes listed above. For example, CW signals (class I) are obtained for a constant jamming frequency $f_q(t)$. Periodic saw-tooth functions can be used to model the instantaneous frequency $f_q(t)$ of signals emitted by class II and class III jammers. The introduction of frequency jumps in the behavior of $f_q(t)$ allows one to model class IV jamming signals [18].

B. Jammer Devices

Jamming signals can be broadcast by a large variety of devices which can have different characteristics. A jammer classification based on the device characteristics was suggested in [1]. In particular, jammers were divided into three groups [1]:

- group I: cigarette lighter jammers; the device is designed to be plugged into an automotive cigarette lighter with a 12-V power supply;
- group II: SubMiniature version A (SMA) battery jammers; the device is powered by a battery and it is connected to an external antenna through an SMA connector;
- group III: non-SMA battery jammers; the device is powered by a battery and uses an integrated antenna for transmission.

This classification is complementary to that suggested in [18] and reviewed in Section II-A. The two classifications consider different aspects of jamming devices and can be combined as in Fig. 2. In this way, a composite jammer

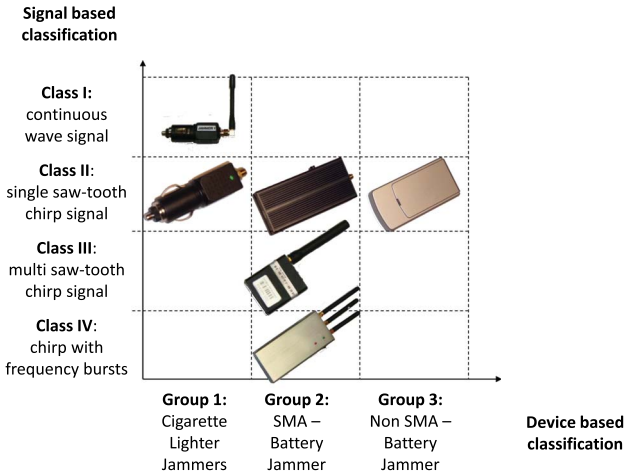

Fig. 2. ***Composite jammer classification accounting for both signal and device characteristics.***

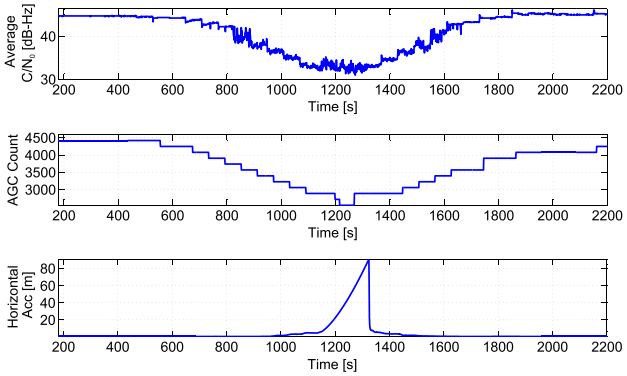

Fig. 3. ***Impact of a jamming signal on a high-sensitivity GNSS receiver. Different metrics sensitive to the jamming signal are provided.***

classification able to capture both signal and device characteristics is obtained. Although the two classifications considered are able to capture most jammer characteristics, the following aspects should also be taken into account:

- single-frequency versus multiple-frequency jammers: jammers can simultaneously affect several GNSS bands;
- single-antenna versus multiple-antenna jammers: some jammers are equipped with several antennas in order to broadcast signals in different frequency bands;
- single-system versus multiple-system jammers: some jammers simultaneously affect GNSS and other communications systems such as Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS).

These aspects are particularly relevant for the design of jamming mitigation and location techniques. For example, several location techniques are based on time difference of arrival (TDOA) which requires precise time synchronization. When GNSS services are denied, other communications signals can be used to achieve precise synchronization. When a multiple-system jammer is used, this type of approach is no longer valid and a different solution has to be adopted.

III. JAMMING IMPACT

In most cases, the goal of malicious jammers is to totally deny GNSS-based services in a certain geographical area. Despite the clear threat posed by a jammer broadcasting a sufficiently strong power, such a scenario is anyway clearly detectable and properly designed GNSS-based services are able to switch to backup non-GNSS positioning means or raise a warning for the users. Intermediate power values turn out to be the most dangerous cases, since sometimes they might be severe enough to significantly decrease the receiver performance, but not severe enough to make the receiver lose lock or to prevent the acquisition of satellite signals. For such a reason, in order to understand the effect of jamming, it is of interest to consider such cases of intermediate jamming power. As an example, the impact of a jamming signal on a high-sensitivity consumer GNSS receiver, a u-blox LEA-6T receiver, is shown in Fig. 3 which considers different receiver metrics sensitive to jamming. The jamming scenario considered in Fig. 3 is the one described in [22]. In this case, a cigarette lighter jammer was used to disturb GNSS signal reception in a controlled environment, a large anechoic chamber installed in the Joint Research Centre (JRC) premises in Ispra, Italy. The power emitted by the jammer was controlled using a variable attenuator and J/N_0 was varied between 55 and 92 dB-Hz. At the beginning of the experiment, the attenuation was set to the maximum value allowed. In this case, the jammer had a reduced impact on receiver operations. The attenuation provided was then progressively reduced and thus the jamming power was progressively increased. After about 20 min, the maximum jamming power was achieved. At this point the attenuation was increased again until the maximum value was achieved. Additional details on the experimental setup considered for this experiment can be found in [22].

The upper plot of Fig. 3 shows the average C/N_0 obtained considering only satellite signals with individual C/N_0 values greater than 30 dB-Hz: this was a conventional choice adopted to avoid artifacts due to discontinuous signal tracking. When the jamming power is maximum, the average C/N_0 is attenuated of about 15 dB. The second plot in Fig. 3 shows the automatic gain control (AGC) counts which assumes, for the u-blox receiver, values in the range 0–8191 [24]. In the

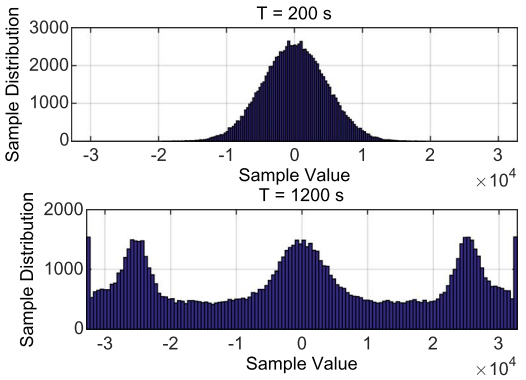

Fig. 4. *Histograms of the samples at the ADC output in the absence of interference (top) and in the presence of a swept jamming signal (bottom).*

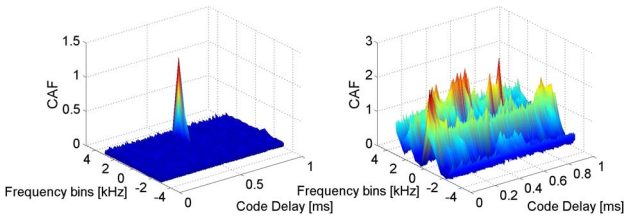

Fig. 5. *Comparison of the CAF for a GPS L1 C/A acquisition search space in an interference-free environment (left) and in the presence of an in-band CW signal at −130 dBW (right).*

presence of jamming, the AGC count is significantly reduced. Finally, the bottom part of Fig. 3 shows the horizontal accuracy of the position solution as estimated by the u-blox receiver. When the received jamming power is maximum, the position accuracy is significantly degraded.

In the following sections, the impact on the different stages of the receiver is briefly discussed. Other examples of impact assessment of interference on GNSS receivers can be found in [15], [25], and [26]. It has to be remarked that the detailed description of the receiver architecture is out of the scope of this paper. The interested reader can refer, for example, to [27].

A. Impact on the Front-End Stage

The front-end is the first receiver stage which can be affected by jamming. The front-end has the goal to filter the incoming signal in the bandwidth of interest, down-converting it to the chosen IF before performing the analog-to-digital (AD) conversion. Modern receivers are designed as multibit devices, thus requiring the presence of an AGC between the analog portion of the front-end and the analog-to-digital converter (ADC). Jamming impacts the AGC values as shown in the middle plot of Fig. 3 and modifies the distribution of the samples at the output of the ADC. This effect is shown in Fig. 4, where the case study described in Fig. 3 is analyzed at instants $T = 200$ s and $T = 1200$ s. When jamming appears, the statistic of the samples is clearly changed and deviations from a Gaussian distribution can be clearly seen. In the case considered in Fig. 4, the AGC is still able to compress the input signal. However, saturation effects start appearing and only a few levels of the quantisation scale are actually used to represent the useful signal.

The front-end is made of highly nonlinear components and in the presence of strong jamming signals several elements of the front-end (filters, amplifiers) may be led to work outside their nominal regions, generating nonlinear effects, or clipping phenomena (signal amplitude exceeding the hardware capability to treat them). In both cases, spurious harmonics are generated and mixed to the useful signal in the front-end itself.

B. Impact on the Acquisition Stage

The first digital signal processing stage of a GNSS receiver is the acquisition block which has to determine the signal presence and to provide a rough estimate of the signal code delay and Doppler frequency [16]. The main operation performed by the acquisition block is to correlate input signal (4) with local replicas of the signal code and carrier. In this respect, a bidimensional function, called cross-ambiguity function (CAF) is evaluated. The CAF is a function of the Doppler frequencies and code delays tested by the acquisition block. When the GNSS signal is present and in the absence of interference, a single dominant peak should appear in the CAF. The peak reveals the signal presence and it is located at the approximate signal code delay and Doppler shift. Fig. 5 compares CAFs evaluated in the absence and in the presence of a CW Interference (CWI). The interfering power is equal to −130 dBW and the CAF is evaluated using 1 ms of coherent integration time and three noncoherent accumulations. The peak-to-noise-floor separation decreases as the interfering power increases, thus increasing the probability of erroneously declaring the signal presence. Moreover, the acquisition block may provide erroneous Doppler and delay estimates. The effects of CWI interference on the acquisition block are analyzed in [28] whereas an extensive study of the effects of several kinds of interference on the acquisition probabilities can be found in [26].

C. Impact on the Tracking Stage

The signals detected by the acquisition stage are passed to the tracking block which is responsible for providing fine estimates of the signal parameters. These estimates are used to generate GNSS measurements such as pseudoranges, carrier phases, and Doppler shifts. Jamming has a direct consequence on the quality of the measurements produced by the tracking stage causing increased measurement variances, biases, and

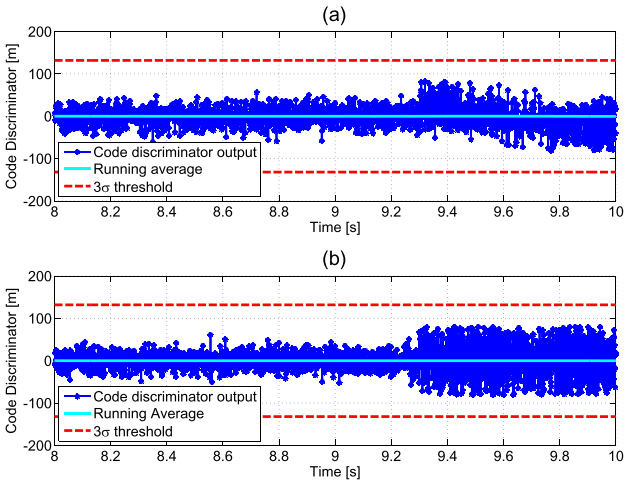

Fig. 6. *GPS L1 C/A tracking performance: code discriminator output in the presence of a −130-dBW in-band CWI (top) and in the presence of a single-saw-tooth chirp signal at −130 dBW (bottom).*

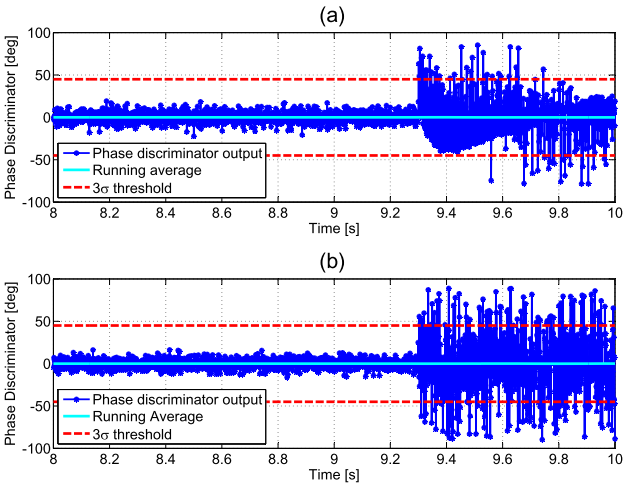

Fig. 7. *GPS L1 C/A tracking performance: carrier discriminator output in the presence of a −130-dBW in-band CWI (top) and in the presence of a single-saw-tooth chirp signal at −130 dBW (bottom).*

measurement outliers [15], [26]. The tracking stage usually adopts a closed-loop architecture where tracking loops are used to track the different signal components. A tracking loop is made of several components such as signal correlators, loop discriminators, and loop filters [16]. Correlators evaluate the correlation of the input signal $y[n]$, with locally generated replicas of the signal code and carrier. Such replicas are generated on the basis of signal parameter estimates and correlator outputs are affected by the errors between the estimated and actual signal parameter values (code delay, Doppler frequency, and carrier phase). In standard receiver architectures, three correlators, Prompt, Early and Late, are generally used for code tracking whereas the Prompt correlator alone is sufficient for carrier tracking [16]. Loop discriminators use the correlator outputs to provide a measure of the error between the estimated and actual signal parameters. Under normal conditions, the discriminator output is driven to zero by the loop. Thus, the discriminator output can be used to assess the impact of jamming. An example of the effect of interference is shown in Figs. 6 and 7 which consider the discriminator outputs of code and carrier tracking loops in the presence of two types of interference. In the upper parts of the figures, a −130-dBW in-band CWI is considered whereas in the bottom plots the effects of a −130-dBW single-saw-tooth chirp signal with a sweep range of 16.7-MHz bandwidth, centered around L1, and a sweep rate of 8.9 μs, are analyzed. In both cases, the receiver correctly locks on the GNSS signal during the first part of the experiments which are performed in the absence of interference. After 9.3 s, interference is injected with detrimental effects on the discriminator outputs.

In this example, the receiver is configured to have a phase lock loop (PLL) bandwidth equal to 10 Hz and a delay lock loop (DLL) bandwidth, $B_{\mathrm{DLL}} = 2$ Hz. The spacing between the early and late replicas of the local code is set to 0.9 code chips. The presence of a CW, shifted by 200 kHz with respect to the GNSS signal in space (SIS) [thus in correspondence of a spectral line of the GPS coarse acquisition (C/A) signal], not only increases the noise level but leads to a sort of oscillating behavior at the discriminator outputs. The effects on the PLL are shown in Fig. 7: when in the presence of a strong CWI, a sudden jump of the phase discriminator output is detected as soon as interference is injected onto the received signal. The presence of the jamming signal leads to an overall increase of both code and phase discriminator output variance. It can be noted that, when considering non-CWI, the ultimate effect of the jammer after the discriminator can be modeled as an increase of the noise power disrupting the useful signal. Furthermore, the phase tracking is more affected than the code tracking, and, as it can be noted, the discriminator output overcomes the typical 3σ threshold (evaluated on the noninterfered signal) considered as the upper bound value for the loop to keep the lock state [16].

When tracking data channels, as in the GPS C/A case, the Prompt correlator is also used for decoding the navigation message. Data decoding can be significantly affected by jamming: depending on the power received and on the type of jamming signal, different effects can occur. In general, an increased bit error rate (BER) is experienced and, in the worst cases, the receiver is unable to decode the navigation message. The detailed analysis