ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/301791457

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

Article *in* Proceedings of the IEEE · May 2016

DOI: 10.1109/JPROC.2016.2543266

CITATIONS
6

READS
171

4 authors:

Daniele Borio
European Commission
118 PUBLICATIONS **828** CITATIONS
SEE PROFILE

Fabio Dovis
Politecnico di Torino
239 PUBLICATIONS **947** CITATIONS
SEE PROFILE

Heidi Kuusniemi
Finnish Geospatial Research Institute
105 PUBLICATIONS **898** CITATIONS
SEE PROFILE

Letizia Lo Presti
Politecnico di Torino
192 PUBLICATIONS **1,130** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

INSURE Project and Indoor Positioning View project

Finland's EGNOS Monitoring and Performance Evaluation (FEGNOS) View project

All content following this page was uploaded by Daniele Borio on 06 June 2016.

The user has requested enhancement of the downloaded file. All in-text references underlined in blue are added to the original document and are linked to publications on ResearchGate, letting you access and read them immediately.

© 2016 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.
The final version of this paper can be found at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7463455

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

Daniele Borio*, Fabio Dovis†, Heidi Kuusniemi ‡, Letizia Lo Presti†
*European Commission, Joint Research Centre (JRC) - Via Enrico Fermi, 2749, 21027, Ispra (VA) - Italy
Email: daniele.borio@jrc.ec.europa.eu †DET - Politecnico di Torino - Corso Duca degli Abruzzi, 24, 10129, Torino - Italy
Email: {fabio.dovis, letizia.lopresti}@polito.it
‡Finnish Geospatial Research Institute, National Land Survey, Finland
Email: heidi.kuusniemi@nls.fi

***Abstract*—Jamming is the act of intentionally directing powerful electromagnetic waves towards 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.**

***Index Terms*—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 non-intentional 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 kms [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], [5], [6], [7], recent researches considered techniques specifically tailored for jamming signals [8], [9], [10], [11], [12], [13], [2], [14]. In this paper, different approaches are reviewed and analysed 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 down-converted to Intermediate Frequency (IF) and transformed in a digital sequence, $s_{IF}[n] = s_{IF}(nT_s)$, 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

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

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

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

The useful signal, $s_{IF}[n]$, is given by [16]:

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

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, 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. $c_i(\cdot)$ 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 modelled as

$$y[n] = s_{IF}[n] + vq[n] + w[n] \quad (4)$$

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

$$J = v^2. \quad (5)$$

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], [18], [19], [20], [21], [2] 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 centre 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

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

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 $q(t)$ 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.

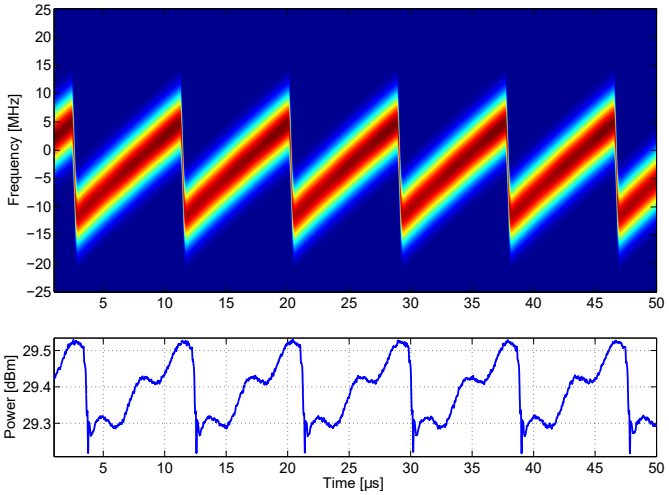

Fig. 1. Spectrogram and power of the signal emitted by a cigarette lighter jammer.

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 behaviours can be found [1], [18], [19], [20], [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, [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 90s. 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]. The authors of [18] divided jammers in 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 by [1]. In particular, jammers were divided in three groups [1]:

- *Group I: cigarette lighter jammers*, the device is designed to be plugged into an automotive cigarette lighter with a 12 volt 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 a 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 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* vs. *multi-frequency* jammers: jammers can simultaneously affect several GNSS bands.
- *single* vs. *multi-antenna* jammers: some jammers are equipped with several antennas in order to broadcast signals in different frequency bands.
- *single* vs. *multi-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).

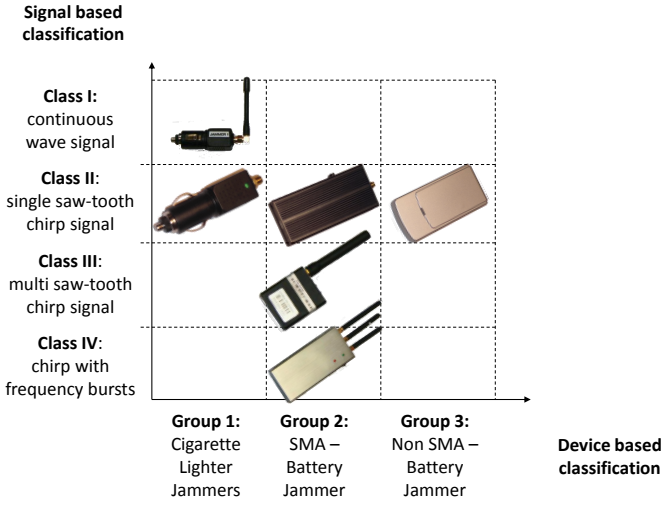

Fig. 2. Composite jammer classification accounting for both signal and device characteristics.

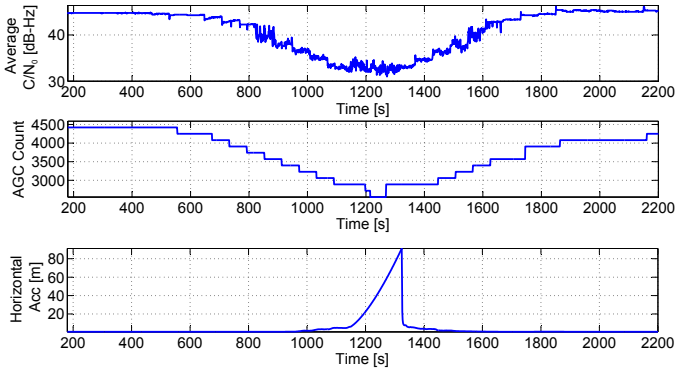

Fig. 3. Impact of a jamming signal on a high-sensitivity GNSS receiver. Different metrics sensitive to the jamming signal are provided.

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 multi-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 of 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 the 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 minutes 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 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 [25], [26], [15]. 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 multi-bit 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 analysed at time 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

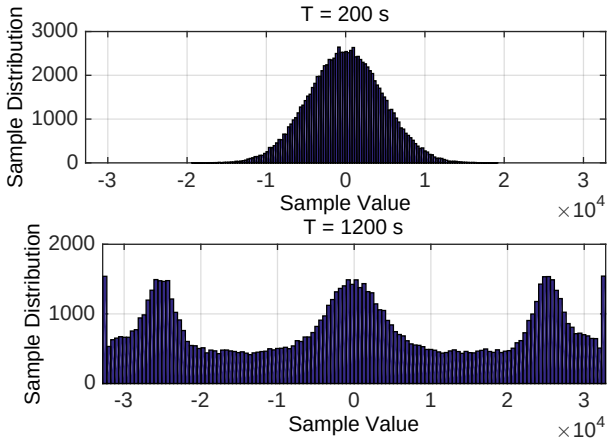

Fig. 4. Histograms of the samples at the ADC output in the absence of interference (top) and in the presence of a swept jamming signal (bottom).

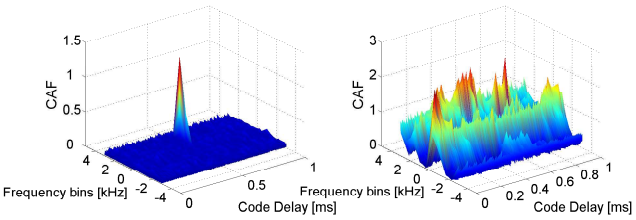

Fig. 5. Comparison of the CAF for a GPS L1 C/A acquisition search space in an interference-free environment (left) and in the presence of an in-band CW signal at -130 dBW (right).

only a few levels of the quantisation scale are actually used to represent the useful signal.

The front-end is made of highly non-linear components and in the presence of strong jamming signals several elements of the front-end (filters, amplifiers) may be led to work outside of their nominal regions, generating non-linear 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 bi-dimensional 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 3 non-coherent

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 is 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 measurement outliers [26][15]. The tracking stage usually adopts a close-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 analysed. 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 seconds, 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, $B_{DLL} = 2$ 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 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

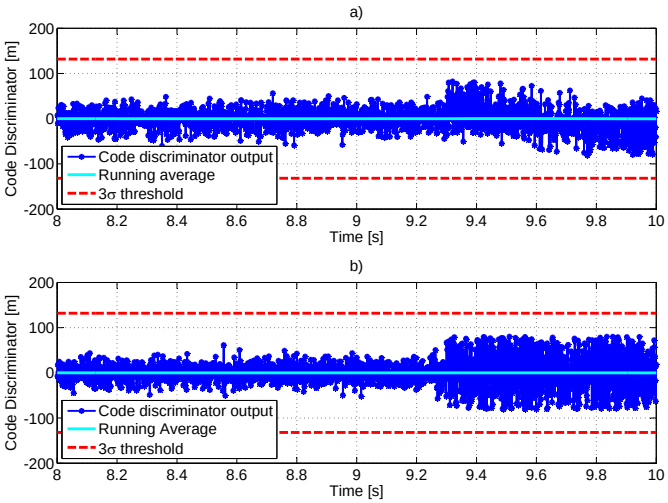

Fig. 6. GPS L1 C/A tracking performance: code discriminator output in the presence of a -130 dBW in-band CWI (top) and in the presence of a single saw-tooth chirp signal at -130 dBW (bottom).

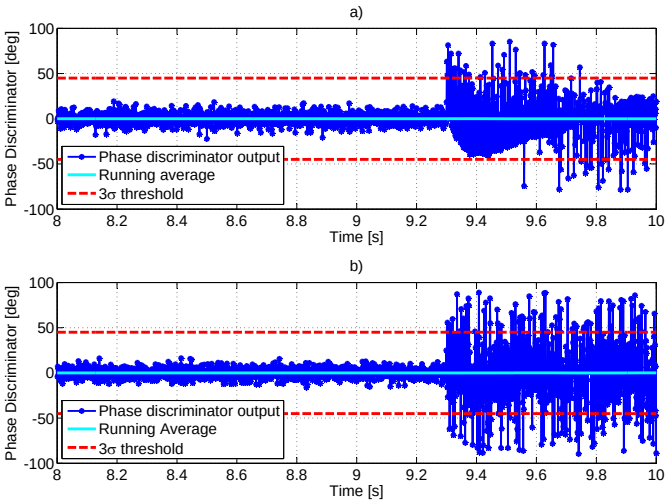

Fig. 7. GPS L1 C/A tracking performance: carrier discriminator output in the presence of a -130 dBW in-band CWI (top) and in the presence of a single saw-tooth chirp signal at -130 dBW (bottom).

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 non-interfered signal) considered as the upper-bound value for the 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

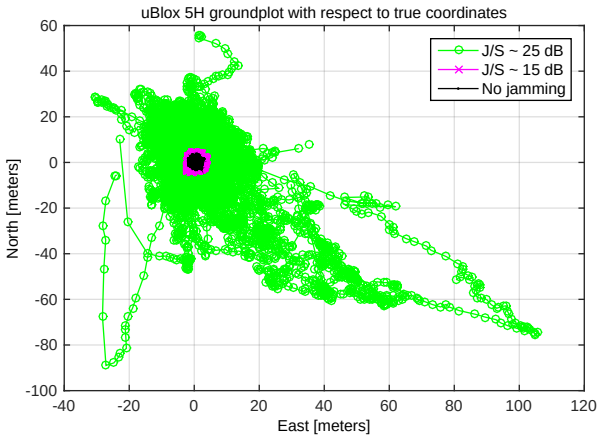

Fig. 8. Positioning results around the true coordinates of a u-blox 5H receiver in a single-frequency jamming test.

increased Bit Error Rate (BER) is experienced and, in the worst cases, the receiver is unable to decode the navigation message. The detailed analysis of the impact of jamming on the navigation message decoding process is out of the scope of this paper.

D. Impact on the position

Provided that the interfered signal can still be processed by both acquisition and tracking stages, the GNSS receiver would be able to output an estimate of the position, which will be degraded by the fact that it will be based on interference-affected pseudoranges. The actual error in the position domain is strongly dependent on the positioning algorithm employed, and a general rule to quantify the performance degradation in terms of positioning error is hard to be found. Typically, the jamming signal deteriorates the position solution or induces total loss of lock of the GNSS signals depending on the perceived J/S at the receiver. For sake of example, Fig. 8 presents in more detail the positioning accuracy of a u-blox 5H receiver where two test cases are considered. In the first case, $J/S = 25$ dB while for the second case $J/S = 15$ dB. Interference-free conditions are also considered. When $J/S = 25$ dB, a maximum horizontal error of 129.3 m was observed and the position solution was available only 16% of the time. The duration of the experiment was 24 hours.

IV. Jamming Detection

Jamming detection is the process of revealing the presence of a jamming source. It is generally formulated as a *binary hypothesis testing* [29] problem where it is necessary to decide between

$$\begin{aligned} H_0: &\quad \text{absence of interference} \\ H_1: &\quad \text{presence of interference} \end{aligned} \tag{7}$$

where H_0 and H_1 are the null and alternative hypotheses, respectively. Problem definition (7) is general and needs to be specified with respect to

- the source of information adopted to formulate the problem
- the characteristics of the source used to decide between H_0 and H_1.

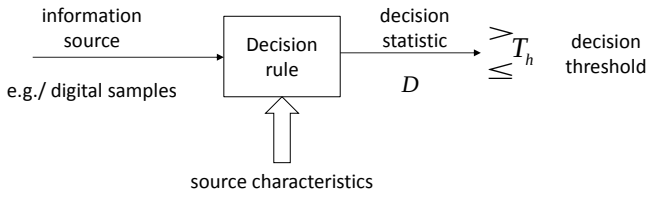

Fig. 9. Classical detection process: a decision variable is formed using the data from an information source. The decision statistic, D, is formed according to a decision rule based on the source characteristics. The final decision is taken by comparing D with the decision threshold, T_h.

In order to illustrate this principle, consider the digital samples in (4). The detection problem in (7) can be formulated as

$$\begin{aligned} H_0: &\quad y[n] = s_{IF}[n] + w[n] &&\text{for } n = 0, 1, ..., N-1 \\ H_1: &\quad y[n] = s_{IF}[n] + vq[n] + w[n] &&\text{for } n = 0, 1, ..., N-1 \end{aligned} \tag{8}$$

where additional hypotheses on $vq[n]$ could be made. In (8), a decision is taken using N digital samples. A general approach is to use such samples and construct a decision statistic, D. A decision between H_0 and H_1 is then taken by comparing D with a decision threshold, T_h, which can be set according to several criteria. This process is depicted in Fig. 9 where the decision variable is formed using the data from an information source. The decision statistic, D, is formed according to a decision rule based on the source characteristics. Such characteristics can be, for example, a statistical model describing the behavior of the digital samples in the absence and in the presence of jamming. Well-known approaches are available for the design of decision rules. In classical (or frequentist) statistics, the most popular approaches are the Likelihood Ratio Test (LRT) and the Generalized Likelihood Ratio Test (GLRT) [29] which need a (partial) statistical characterization of the information source under both H_0 and H_1.

Detection techniques are usually characterized in terms of Receiver Operating Characteristics (ROCs) [29] that are the plot of the detection probability as a function of the false alarm rate. The detection probability is the probability that the detector correctly reveals the presence of jamming. Conversely, the false alarm rate is the probability that the detector incorrectly declares the jamming signal present. These probabilities depend on several factors including the quality of the measurements provided by the information source adopted. For example, the J/N_0 introduced in Section II has a significant impact on the detector performance. In general, high J/N_0 values should favor the detection process, reducing false alarm rates. Under the same J/N_0 conditions and for a fixed false alarm probability, the algorithm with the highest detection probability should be preferred.

A possible criterion for setting the decision threshold is to choose it such that a constant false alarm rate is obtained. This criterion requires a probabilistic model characterizing the decision statistic, D, in the absence of jamming. In practice, this model may be difficult to obtain since it has to account for different operating conditions such as the number of

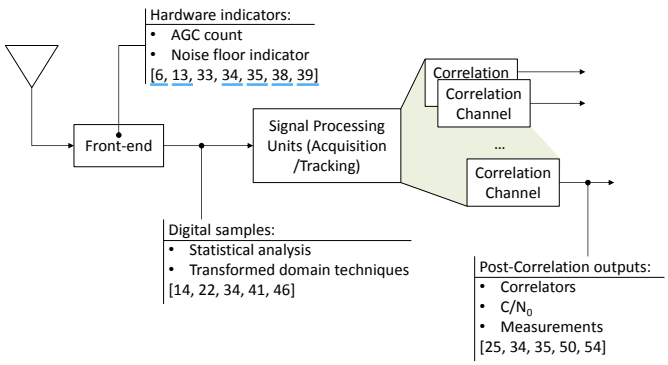

Fig. 10. Different approaches for jamming detection which can be implemented using measurements from different receiver stages.

satellites available, signal propagation conditions and receiver signal strength. For this reason, the decision threshold is often set using criteria based on Monte Carlo simulations or on empirical results.

The approach described above is usually referred to as classical detection theory [29] or block processing where N measurements are used jointly to take a decision, in block. Other techniques are possible such as the *sequential approach* [30] where information, e.g. signal samples, is progressively introduced until a decision is taken. The most known sequential approaches are the Sequential Probability Ratio Test (SPRT) and its variants [30]. Sequential approaches have been recently adopted for interference detection by [31].

The digital samples considered in (8) are just an example of information source which can be used to design jamming detection systems. In particular, information can be extracted from almost any stage of a GNSS receiver. A schematic representation of the different GNSS receiver stages and of the different information sources is provided in Fig. 10. In addition to the digital samples, the receiver front-end can provide hardware indicators such as the AGC count and the noise floor estimator [6], [32]. These hardware indicators usually assume anomalous values in the presence of jamming as shown in Fig. 3 and thus they can be used for the design of jamming detection algorithms. The correlators introduced in Section III-C, signal measurements, such as carrier phases, Doppler frequencies and pseudoranges, and signal quality indicators such as C/N_0 estimates can be used to design jamming detection techniques which are called post-correlation techniques [33]. The interest of such techniques is that most commercial GNSS receivers provide the signal C/N_0 and thus post-correlation techniques can be implemented in a large variety of devices.

In Fig. 10, the final stage of a GNSS receiver, i.e., the Position Velocity Time (PVT) estimation block is not considered. Although detection can be performed also at this stage, it is preferable to identify the presence of jamming as soon as possible, in order to activate appropriate countermeasures. Identifying jamming at the PVT level may be too late. The different detection approaches developed using the information sources described above are discussed in the following sections.

A. Hardware Indicators

In Section III, it was shown that jamming signals influence hardware components of the receiver front-end. In particular, the AGC has to reduce its gain in order to be able to minimize quantization errors and to effectively represent a powerful input signal with a limited number of bits.

The potential of the AGC as interference monitoring tool was at first analysed in [6] which considered the case of pulsed interference in the GPS L5 frequency band. Since then, several papers have investigated the potential of the AGC count for jamming detection [34], [35], [13].

More in detail, let $g_{AGC}[n]$ be the AGC count measured at the instant n. A simple criterion for detecting the presence of jamming is to consider N consecutive samples of the AGC count. If all the samples of $g_{AGC}[n]$ are below a certain threshold, the presence of jamming is declared:

$$g_{AGC}[n] < T_h \qquad \text{for } n = 0, 1, ..., N-1. \tag{9}$$

For example, in [13] jamming events were recorded if the AGC count was going below a certain value for at least 0.02 s. The main limitation of this approach is that the selection of T_h requires a thorough characterization of the AGC behavior. For example, [13] showed that three AGCs integrated in three front-ends of the same model provided slightly different AGC values in the presence of the same interference power. Generally, T_h, has to be set using an empirical approach.

More sophisticated approaches using the AGC count can be adopted. In [35], the usage of a median filter [36] followed by a low-pass filter is suggested to reduce the impact of noise and to remove outliers in the AGC time series. Detection is performed considering the filtered version of $g_{AGC}[n]$. Article [35] also recognized that the AGC count is directly linked to the distance between jammer and victim receiver. Thus, the AGC count can also be used for locating the jamming source [35], [37].

In order to mitigate the dependence of the AGC count on the actual hardware device, the authors of [25] suggested the usage of the *AGC level changing rate* defined as

$$g_r[n] = \frac{g_{AGC}[n] - g_{AGC}[n-k]}{kT_s} \tag{10}$$

where $k \geq 1$ is a selectable parameter and T_s is the sampling rate of the AGC count time series. Also in this case, $g_r[n]$ is compared against a decision threshold.

Several other metrics can be derived from the AGC count which can be coupled with other approaches for reveling the presence of jamming [38], [32].

Additional considerations on hardware indicators can be found in [39] which discusses a possible implementation of a J/N estimator using the hardware components available in a standard GNSS receiver.

B. Digital Signal Processing

Methods based on digital signal processing work on the signal samples at the output of the RF front-end, that is at the

early stage of the receiver chain. In this way, the receiver is able to raise an early warning in case a distortion is detected. An interfering signal impinging the antenna with the power level exceeding the noise floor is expected to be detectable via spectral analysis, by comparing the estimated PSD of the received signal with a spectral mask that appropriately represents nominal interference-free conditions. Basic spectral estimation can be implemented via simple normalized Fast Fourier Transform (FFT) or periodogram methods (which are based anyway on the use of sequences of shorter and windowed FFTs) as for example in [40]. Such non-parametric spectral monitoring techniques are conceptually simple, but their performance is inherently limited by a set of factors: they need relatively long observation windows (on the order of several hundreds of milliseconds) to produce spectral estimates with reduced estimation variance; periodograms (whichever they are: sample, Bartletts, Welchs) are biased estimators, which introduce spectral leakages in correspondence of sharp spectral peaks and nulls; finally, they are heavily based on the use of the FFT, which is a demanding resource whose complexity is super-linear with respect to the number of input samples. It results that the parameters of the FFT algorithm used in each specific implementation must be carefully chosen, taking into account the necessary frequency resolution, the digitization bandwidth and the computational resources available to compute each FFT. Indeed, the FFT length is directly related to the frequency resolution of the spectrum, normalized to the whole digitization bandwidth.

A different approach, working on the stream of samples in the time domain, is based on the observation of the signal, modeled as random process, in the "domain of the statistical characteristics". Methods working on this domain are widely used in disciplines as economics [41], [42], [43], biology [44] and others, while a very few examples can be found in GNSS applications [45], [6], [14].

The main idea behind these methods is that, in the absence of jamming, the sample provided by the ADC approximately follows a Gaussian distribution. This fact is highlighted in the upper plot of Fig. 4 which shows the histogram of the samples at the ADC output in the absence of interference. Jamming can make the probability density function (pdf) of the output samples significantly deviate from a Gaussian distribution. Thus, jamming can be revealed by detecting deviations from the Gaussian distribution. These deviations can be measured for example considering the skewness and the excess kurtosis of the ADC samples.

A method based on the statistical characteristics of the GNSS and RFI signals is described in [14]. The idea is to characterize the nominal signal, $y[n]$, in terms of its first order pdf, $p_Y(x)$, and to formulate the hypothesis testing problem by comparing $p_Y(x)$ with an empirical pdf, $p_X(x)$, which is estimated using N digital samples. The method proposed in [14] is based on a theorem due to K. Pearson [46] and is known as Chi-square test on Goodness of Fit (GoF). The test statistic is defined as

$$D = \sum_{i=1}^{k} \frac{(O_i - E_i)^2}{E_i} \tag{11}$$

where k is the number of bins of the estimated histograms, E_i refers to the ith value of the expected histogram while O_i is the ith value of the observed histogram. The two histograms represent $p_X(x)$ and $p_Y(y)$, respectively. This test statistic can be seen as an instance of a random variable, which is, for large N, approximately χ^2-distributed with $k-1$ degrees of freedom, as affirmed by the Pearson theorem [47], [46]. This characterization allows the selection of a proper threshold, given the specifications of the detector in terms of false alarm probability. In [14] the Chi-square test on GoF has also been applied to post-correlation samples. In this case the detection of anomalies can be done only after the evaluation of the search space and/or at the DLL output and allows the identification of SIS with anomalies. Other methods working in the domain of the statistical characteristics can be found in [48] and [49].

Recently, sophisticated detection approaches have been proposed. They exploit the availability of digital samples which are used to represent the signal received in different domains where the presence of the spurious interfering signals can be more easily detected. For example, TF analysis techniques can be applied using several TF distributions (e.g., Short-time Fourier, Wigner-Ville, Choi-Williams, ...). The goal is to select a transformed domain where the jamming signal is maximally concentrated leading to a clear pattern which can be more easily detected than in the time or frequency domain. Thus, the performance of such methods generally depend on the type of interference to be detected [50]. A critical issue with such family of techniques is the significant computational burden to be handled. Another transformed domain is defined by Time-Scale analysis techniques, based on the use of the two-dimensional wavelet transform. These techniques are gaining interest for GNSS interference monitoring [51][52].

All these techniques show good detection performance, but such a gain is traded off with a significant computational burden. However, due to the constantly growing computational capabilities of the processors in consumer receivers, they are an interesting perspective solution.

C. Post-correlation Domain Detection

Post-correlation techniques exploit the observables provided by a GNSS receiver after the correlation process [33]. The advantage of such approach is that post-correlation observables are available also in low-cost mass-market receivers such as the GPS chips integrated in smart-phones. In particular, the C/N_0 estimated for the different satellite signals is also available in the standard National Marine Electronics Association (NMEA) messages provided by Android smart-phones [32], [53]. In the presence of jamming, the victim receiver perceives a significant increase in the noise component. In particular, N_0 is significantly overestimated by the receiver. In the presence of jamming, the effective C/N_0 estimated by the receiver and expressed in linear units is given by [54]:

$$\left.\frac{C}{N_0}\right|_{eff,lin} = \frac{C}{N_0 + \alpha J} \tag{12}$$

where C, N_0 and J have been defined in Section II. α is the Spectral Separation Coefficient (SSC) [54] and takes into

account the filtering effect performed by a GNSS receiver when executing the correlation process. In (12), all the quantities are expressed in linear units. Thus, in the presence of jamming, the C/N_0 estimated by the receiver can be significantly reduced. For this reason, the C/N_0 has been adopted by several researchers [53], [55], [56], [34], [33], [32] as an indicator for jamming detection.
When considering C/N_0 measurements, two general approaches are possible:

- consider each C/N_0 value independently and take a decision specific to a single satellite signal
- consider jointly the C/N_0 values from all the signals and perform a collective detection.

An example of the first approach can be found in [56] which analysed the statistical properties of the C/N_0 estimated by a Software Defined Radio (SDR) receiver. A Gaussian model was adopted to describe the pdf of the measurements and it was shown that, in the absence of jamming, the mean and standard deviation of the Gaussian model mainly depend on the satellite elevation. In the presence of interference the mean of the C/N_0 estimates is severely affected and thus jamming can be detected by comparing the C/N_0 mean with a threshold selected according to a pre-determined false alarm probability. In this case, detection is performed considering a single satellite signal. In order to improve the detection performance, [56] also suggested to combine the decision taken over several epochs and using measurements from several satellites. In particular, a Bernoulli decision scheme was designed. In [55] and [34], detection approaches based on individual C/N_0 were also considered and it was confirmed that *"C/N_0-based detectors could work well in a static scenario, but are not suitable in a dynamic scenario, since they cannot distinguish between decreased GPS signal strength and an increased interference level"*. This is the so called C/N_0 *ambiguity problem*: the estimated C/N_0 can decrease either because the signal power, C, is attenuated or because of the additional noise power introduced by jamming. Signal attenuation can occur in difficult propagation environments such as in the presence of obstacles, urban canyons and foliage. This problem can be partially mitigated using collective detection approaches. For example, in urban canyons or in the presence of multipath, GNSS signals are hardly attenuated all in the same way: signals from high elevation satellites are usually less affected by such impairments. On the contrary, jamming causes a noise increase to all processed signals. This principle is illustrated in Fig. 11 which shows the C/N_0 values of the individual satellites tracked during the experiment considered in Fig. 3. The C/N_0 values are affected in a similar way by the jamming signal. Thus, jamming introduces correlated changes in the C/N_0 time series. This principle has been exploited by [53] to develop a form of ANalysis Of VAriance (ANOVA) for jamming detection. In particular, the following detection statistic was suggested:

$$\Lambda = \sum_{k=0}^{N-1} \left[\sum_{i=0}^{I-1} \left(\frac{C_i}{N_0}[n-k] - h_{LP}[n] * \frac{C_i}{N_0}[n-k] \right) \right]^2 \quad (13)$$

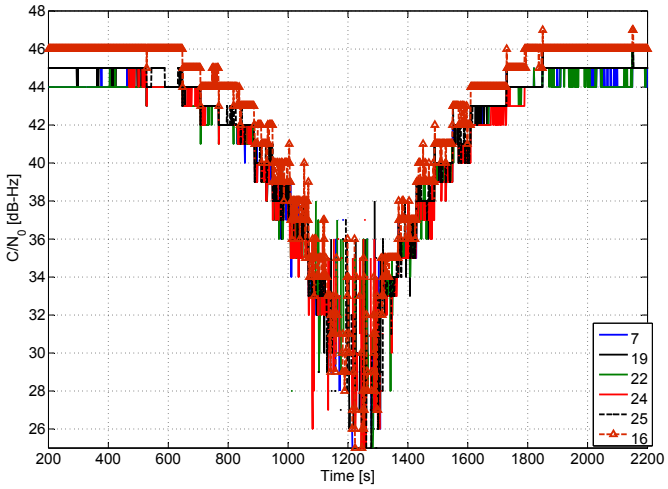

Fig. 11. C/N_0 values of the individual GPS C/A signals tracked during the experiment considered in Fig. 3. The C/N_0 values are affected in a similar way by the jamming signal.

where N is the number of time epochs considered and I is the number of satellites available. $h_{LP}[n]$ is the impulse response of a low-pass filter with unit gain at Direct Current (DC) and symbol '$*$' denotes convolution. $\frac{C_i}{N_0}[n]$ is the C/N_0 from the ith satellite at the instant n expressed in logarithmic scale (dB-Hz). A decision is taken by comparing Λ with a decision threshold.
Although, this method mitigates the C/N_0 ambiguity problem and can, for example, be used in dynamic scenarios [53], it can become unreliable when most of the signals are strongly attenuated such as indoors. In this case, additional information from other sources has to be adopted. A possible solution is considered by [32] which suggested a joint detection scheme combining C/N_0 values with AGC readings. Indeed the two time series provide complementary information. Additional detection approaches can be designed using the output of the digital tracking loops used to process each satellite signal. The authors of [25] considered the discriminator outputs of a non-coherent DLL and of a Costas PLL. Then an analysis window was used to select N consecutive samples and compute the sample variance of the discriminator outputs. If the sample variance passes a decision threshold, then the presence of jamming is declared.
In this case, a single decision is taken for each signal tracked. Then a combining rule, such as the Bernoulli scheme described in [56], has to be adopted for taking a final decision.
A similar approach can be adopted where the sample variance is computed using GNSS observables such as pseudoranges and Doppler measurements. In this case, the time-varying nature of such observables has to be accounted for. For example, N should be small enough to limit the time variations of these observables. Alternatively, measurements can be at first high-pass filtered.

V. Conclusions

In this paper, the characteristics of jamming signals and their impact on GNSS receivers have been reviewed. A survey

on the state-of-the-art methods for jamming detection was also provided. It was shown that jamming can practically impact all receiver stages, from the front-end to the navigation solution. Specific emphasis was given to intermediate power jamming attacks when jamming signals are sufficiently powerful to significantly degrade receiver performance without interrupting receiver operations. This case is considered the most dangerous since jamming may be undetected and GNSS users may continue their operations without realizing the degradation of performance experienced by their receivers. In this respect, detection is the first line of defense against a jamming attack. Several detection approaches were discussed and it is shown that detection can be implemented at almost any receiver stage. Interference detection units are becoming common accessories in new GNSS receivers and the constantly growing computational capabilities of GNSS chipsets are enabling new and more sensitive detection strategies.

REFERENCES

[1] 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.

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

[3] "No jam tomorrow," *The Economist*, 2011.

[4] J. A. Volpe, "Vulnerability assessment of the transportation infrastructure relying on the Global Position System," in *National Transportation Systems*, Jan. 2000.

[5] T. Buck and G. Sellick, "GPS RF interference via a TV Video Signal," in *Proc. of the 10th International Technical Meeting of the Satellite Division of the Institute of Navigation*, Kansas City, Missouri, Sep. 1997.

[6] F. Bastide, D. Akos, C. Macabiau, and B. Roturier, "Automatic gain control (AGC) as an interference assessment tool," in *Proc. of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS)*, Portland, OR, Sep. 2003, pp. 2042–2053.

[7] F. Butsch, "Radiofrequency interference and GPS," *GPS World*, pp. 40–46, Oct. 2002.

[8] B. Motella, M. Pini, and F. Dovis, "Investigation on the effect of strong out-of-band signals on Global Navigation Satellite Systems receivers," *GPS Solutions*, vol. 12, no. 2, pp. 77–86, Mar. 2008.

[9] P. F. De Bakker, J. Samson, M. Spelat, M. Hoolreiser, and B. Ambrosius, "Effect of radio frequency interference on GNSS receiver output," in *Proc. of the ESA Workshop on Satellite Navigation User Equipment Technologies (NAVITEC)*, Dec. 2006, pp. 1–9.

[10] A. T. Balaei, B. Motella, and A. G. Dempster, "GPS interference detected in Sydney-Australia," in *Proc. of the IGNSS conference*, Sydney, Australia, Dec. 2007.

[11] P. Fenton, "Can GPS and LightSquared coexist?" in *Panel Discussion - ION GNSS 2011*, Portland, Oregon, September 19-23 2011.

[12] P. Boulton, R. Borsato, B. Butler, and K. Judge, "GPS interference testing. Lab, Live, and LightSquared," *Inside GNSS*, pp. 32–45, July-August 2011.

[13] O. Izos, D. Akos, T. Lindgren, C. Sun, and S. Jan, "Assessment of GPS L1/Galileo E1 interference monitoring system for the airport environment," in *Proc. of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS)*, Portland, OR, September 2011.

[14] B. Motella and L. Lo Presti, "Methods of goodness of fit for GNSS interference detection," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 50, no. 3, pp. 1690 – 1700, Jul. 2014.

[15] F. Dovis, *GNSS Interference Threats and Countermeasures*. Norwood, MA (USA): Artech House, 2015.

[16] E. D. Kaplan and C. Hegarty, *Understanding GPS: Principles and Applications*. Artech House Mobile Communications Series, 2006.

[17] J. B. Tsui, *Fundamentals of Global Positioning System Receivers. A Software Approach*, 2nd ed. New York: John Wiley and Sons, 2005.

[18] 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.

[19] 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.

[20] H. Kuusniemi, E. Airos, M. Z. H. Bhuiyan, and T. Kröger, "Effects of GNSS jammers on consumer grade satellite navigation receivers," in *Proc. of the European Navigation Conference (ENC)*, Gdansk, Poland, Apr. 2012, p. 14.

[21] D. Borio, J. Fortuny, and C. O'Driscoll, "Spectral and spatial characterization of GNSS jammers," in *Proc. of the 7th GNSS Vulnerabilities and Solutions Conference*, Baska, Croatia, Apr. 2013, pp. 1–17.

[22] 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.

[23] G. D. Rash, "GPS jamming in a laboratory environment," in *Proc. of the 53rd Annual Meeting of The Institute of Navigation*, Albuquerque, NM, Jun. 1997, pp. 389–398.

[24] *u-blox 6 Receiver Description Including Protocol Specification*, u-blox A.G,, available on-line https://www2.u-blox.com/images/downloads/Product_Docs/u-blox6_ReceiverDescriptionProtocolSpec_%28GPS.G6-SW-10018%29.pdf, Apr. 2013.

[25] M. Z. H. Bhuiyan, H. Kuusniemi, S. Söderholm, and E. Airos, "The impact of interference on GNSS receiver observables - a running digital sum based simple jammer detector," *Radioengineering*, vol. 23, no. 3, pp. 898–906, Sep. 2014.

[26] M. Wildemeersch, E. C. Pons, A. Rabbachin, and J. F. Guasch, "Impact study of unintentional interference on GNSS receivers," European Commission, Joint Research Centre, JRC Scientific and Technical Reports, 2010. [Online]. Available: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC62607/lbna24742enc.pdf

[27] P. Misra and P. Enge, *Global Positioning System - Signals, Measurements and Performance*, 2nd ed. Ganga-Jamuna Press, 2001.

[28] D. Borio, "GNSS acquisition in the presence of continuous wave interference," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 46, no. 1, pp. 47–60, Jan. 2010.

[29] S. M. Kay, *Fundamentals of Statistical Signal Processing, Detection Theory*, ser. Signal processing. New Jersey: Prentice Hall, 1993, vol. II.

[30] A. Wald, *Sequential Analysis*. Dover, Jan. 2015.

[31] D. Egea-Roca, G. Seco-Granados, and J. Lopez-Salcedo, "On the use of quickest detection theory for signal integrity monitoring in single-antenna GNSS receivers," in *Proc. of the International Conference on Localization and GNSS (ICL-GNSS)*, Jun. 2015, pp. 1–6.

[32] E. Vallés, C. Yu, and R. Elasmar, "Interference detection algorithms for GNSS-enabled android devices," in *Proc. of the 28th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+)* , Tampa, Florida, Sep. 2015, pp. 1–8.

[33] K. Sheridan, Y. Ying, and T. Whitworth, "Pre- and post-correlation GNSS interference detection within software defined radio," in *Proc. of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS)*, Nashville, TN, 2012, pp. 3542–3548.

[34] E. Axell, F. M. Eklöf, M. Alexandersson, P. Johansson, and D. M. Akos, "Jamming detection in GNSS receivers: Performance evaluation of field trials," *NAVIGATION: Journal of the Institute of Navigation*, vol. 61, no. 1, pp. 73–82, Spring 2015.

[35] J. Lindstrom, D. M. Akos, O. Isoz, and M. Junered, "GNSS interference detection and localization using a network of low cost front-end modules," in *Proc. of the 20th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS)*, Fort Worth, TX, Sep. 2007, pp. 1165 – 1172.

[36] G. R. Arce, *Nonlinear Signal Processing: A Statistical Approach*. Hoboken, NJ, USA: John Wiley & Sons, Inc., Sep. 2004.

[37] O. Isoz, A. T. Balaei, and D. Akos, "Interference detection and localization in GPS L1 band," in *Proc. of the 2010 International Technical Meeting of The Institute of Navigation*, San Diego, CA, Jan. 2010, pp. 925–929.

[38] J. H. Yang, C. H. Kang, S. Y. Kim, and C. G. Park, "Intentional GNSS interference detection and characterization algorithm using AGC and

adaptive IIR notch filter," *International Journal of Aeronautical and Space Sciences*, vol. 13, no. 4, pp. 491–498, Dec. 2012.

[39] L. Scott, "J911: The case for fast jammer detection and location using crowdsourcing approaches," in *Proc. of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS)*, Portland, OR, Sep. 2011, pp. 1931–1940.

[40] A. Tani and R. Fantacci, "Performance evaluation of a precorrelation interference detection algorithm for the GNSS based on nonparametrical spectral estimation," *IEEE Systems Journal,*, vol. 2, no. 1, pp. 20–26, Mar. 2008.

[41] K. Wallis, "Chi-squared tests of interval and density forecasts, and the Bank of England's fan charts," *International Journal of Forecasting*, vol. 19, no. 2, pp. 165–175, Apr. 2003.

[42] C. S. Gouriéroux and C. Tenreiro, "Local power properties of kernel based goodness of fit tests," *Journal of Multivariate Analysis*, vol. 78, no. 2, pp. 161–190, Aug. 2001.

[43] M. L. Rizzo, "New goodness-of-fit tests for Pareto distributions," *ASTIN Bulletin*, vol. 39, no. 2, pp. 691–715, Nov. 2009.

[44] R. Parker, *Introductory Statistics for Biology*, 2nd ed. Cambridge University Press, 1991.

[45] L. Marti and F. van Graas, "Interference detection by means of the software defined radio," in *Proc. of the 17th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS)*, Long Beach, CA, USA, Sep. 2004.

[46] W. R. Pestman, *Mathematical Statistics*, 2nd ed. Berlin: Walter de Gruyter, Jan. 2009.

[47] S. S. Wilks, *Mathematical Statistics*. New York: John Wiley & Sons Inc., 1962.

[48] M. T. Gamba, B. Motella, and M. Pini, "Statistical test applied to detect distortions of GNSS signals," in *Proc. of the International Conference on Localization and GNSS (ICL-GNSS)*, 25-27 June 2013, pp. 1 – 6.

[49] M. Pini, B. Motella, and M. T. Gamba, "Detection of correlation distortions through application of statistical methods," in *Proc. of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+)*, Sep. 2013, pp. 3279–3289.

[50] D. Borio, L. Camoriano, S. Savasta, and L. Lo Presti, "Time-frequency excision for GNSS applications," *IEEE Systems Journal*, vol. 2, no. 1, pp. 27–37, Mar. 2008.

[51] M. Paonni, J. Jang, B. Eissfeller, S. Wallner, J. A. Rodriguez, J. Samson, and F. A. Fernandez, "Wavelets and notch filtering. innovative techniques for mitigating RF interference," *Inside GNSS*, vol. 6, no. 1, pp. 54–62, January-February 2011.

[52] L. Musumeci and F. Dovis, "Use of the wavelet transform for interference detection and mitigation in global navigation satellite systems," *International Journal of Navigation and Observation*, vol. 2014, pp. 1–14, Mar. 2014.

[53] D. Borio and C. Gioia, "Real-time jamming detection using the sum-of-squares paradigm," in *Proc. of the International Conference on Localization and GNSS (ICL-GNSS)*, Gothenburg, Sweden, Jun. 2015, pp. 1–6.

[54] 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.

[55] E. Axell, "GNSS interference detection," FOI - Swedish Defence Research Agency, Tech. Rep. FOI-R–3839–SE, Feb. 2014.

[56] R. Calcagno, S. Fazio, S. Savasta, and F. Dovis, "An interference detection algorithm for COTS GNSS receivers," in *Proc. of the 5th ESA Workshop on Satellite Navigation Technologies and of the European Workshop on GNSS Signals and Signal Processing NAVITEC*, Noordwijk, The Netherlands, Dec. 2010, pp. 1–8.

View publication stats