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

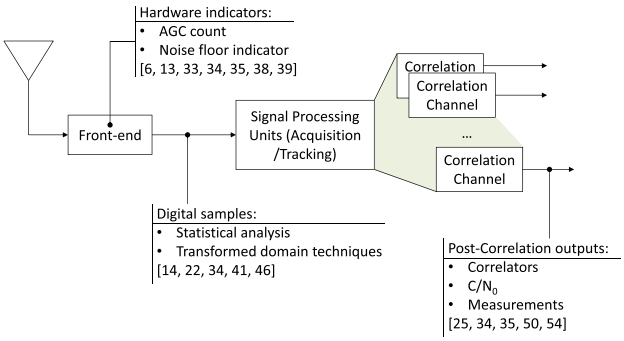

Fig. 10. ***Different approaches for jamming detection which can be implemented using measurements from different receiver stages.***

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, 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 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 postcorrelation techniques [33]. The interest of such techniques is that most commercial GNSS receivers provide the signal C/N_0 and thus postcorrelation 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 analyzed 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 [13], [34], [35].

More in detail, let $g_{\mathrm{AGC}}[n]$ 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 $g_{\mathrm{AGC}}[n]$ are below a certain threshold, the presence of jamming is declared

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

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, Izos *et al.* [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 $g_{\mathrm{AGC}}[n]$. Lindstrom *et al.* [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, Bhuiyan *et al.* [25] suggested the usage of the AGC level changing rate defined as

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

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 [32], [38].

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 nonparametric 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 superlinear 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]–[43], biology [44], and others, while a very few examples can be found in GNSS applications [6], [14], [45].

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 Pearson [46] and is known as chi-squared 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 [46], [47]. 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-squared test on GoF has also

been applied to postcorrelation 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, etc.). 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 2-D 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. Postcorrelation Domain Detection

Postcorrelation techniques exploit the observables provided by a GNSS receiver after the correlation process [33]. The advantage of such approach is that postcorrelation observables are available also in low-cost mass-market receivers such as the GPS chips integrated in smartphones. 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 smartphones [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]

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

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, C/N_0 estimated by the receiver can be significantly reduced. For this reason, C/N_0 has been adopted by several researchers [32]–[34], [53], [55], [56] 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 analyzed 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 predetermined false alarm probability. In this case, detection is performed considering a single satellite signal. In order to improve the detection performance, Calcagno *et al.* [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 [34] and [55], 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 in [53] to develop a form of ANalysis Of VAriance (ANOVA) for jamming