Impact of meaconers on aircraft GNSS receivers during approaches

Mathieu Hussong, Emile Ghizzo, Carl Milner, Axel Garcia-Pena, Julien Lesouple, Christophe Macabiau

Impact of meaconers on aircraft GNSS receivers during approaches

Mathieu Hussong, Emile Ghizzo, *Ecole Nationale de l'Aviation Civile (ENAC)*
Carl Milner, Axel Garcia-Pena, Julien Lesouple, Christophe Macabiau, *ENAC*

BIOGRAPHY

Mathieu HUSSONG is a second-year PhD student in the Signal Processing and Navigation group at ENAC, the French National Civil Aviation University. He holds a master's degree in aeronautics from ENAC and an additional master's degree in aerospace systems specializing in navigation and telecommunications. His PhD research focuses on aircraft GNSS spoofing detection through INS coupling.

Emile GHIZZO is a second-year PhD student in the Signal Processing and Navigation group at ENAC, the French National Civil Aviation University. He holds a master's degree in aeronautics from ENAC and an additional master's degree in aerospace systems specializing in navigation and telecommunications. His PhD research focuses GNSS spoofing and jamming detection.

ABSTRACT

This paper develops a classification to quantify the impact of a meaconer on an aircraft GNSS receiver, from the tracking loops up to the position estimation, during an SBAS-guided LPV-200 approach. Depending on the scenario, the impact of the meaconer on the estimated position can be catalogued for each GNSS signal at a given epoch into one of the four following situations - nominal, jamming, multipath or spoofing. In the nominal situation, the meaconer has no appreciable impact on the aircraft position. In the jamming situation, the meaconer induces higher noise levels resulting in greater errors in the position estimation than in the nominal situation. In the multipath situation, the meaconer effect on the position is similar to a GNSS multipath error. In the spoofing situation, the meaconer adds a deterministic bias on a subset of PRNs that can lead to significantly erroneous position estimations. Extensive simulations demonstrate that a meaconer with a high power and close to the aircraft trajectory can degrade the GNSS receiver performance and provoke faulty estimations of the aircraft position, which are not compliant with the civil aviation standards.

I. INTRODUCTION

GNSS in the L1/E1 frequency band is an Aeronautical Radio Navigation System (ARNS) and must be protected against external Radio Frequency Interference (RFI) threats, which include jamming and spoofing International Telecommunication Union (2001), (International Telecommunication Union, 2016, 4.10), Garcia Peña et al. (2020). The prevalence of these threats is escalating due to the widespread adoption of GNSS repeaters, commonly known as meaconers, and aircraft GNSS receivers might be prone to safety risks in the vicinity of such meaconers Berz (2018).

The literature has examined the impact of GNSS repeaters on GNSS receiver position estimates through simulations encompassing both static scenarios Bamberg et al. (2018); Peng et al. (2019) and certain dynamic scenarios Coulon et al. (2020). These simulations demonstrate that a meaconer presence can adversely affect tracking loop performance, pseudorange computation, and position determination, contingent upon specific geometric and power conditions. The consequences of meaconer activation can manifest as spoofing (tracking meaconer signals within tracking loops), jamming (meaconer degrading the C/N_0 of the authentic signal), or as yet unclassified deviations Bamberg et al. (2018). To the best of the authors' knowledge, the literature has yet to comprehensively analyze dynamic scenarios conforming to aviation standards and processing techniques ED259 (2019); DO229E (2016). Indeed, the complexity of the tracking loops coupled with the non-linearity of measurement checks procedures make the derivation of the analytical expressions of the meaconer impact a highly complex task. Additionally, the evolving geometry over time and the multitude of configurations compound the complexity of assessing meaconer effects.

Nevertheless, the assessment of the meaconing impact on civil aviation arises as a major priority since it might degrade the accuracy and availability of GNSS solutions ICAO (2022), leading to possible missed approaches, closed airspace around the airport Berz (2018), or undetected deflections of the aircraft position. Addressing this concern, this paper undertakes a comprehensive analysis of the meaconer influence on the aircraft GNSS processing chain and the resultant estimated GNSS position. The analysis is executed through categorization of the meaconer impact, employing highly realistic flight approach scenarios, and subjecting aircraft GNSS receiver simulators to meaconer-induced spoofing.

The study introduces a methodological framework for evaluating and quantifying the impact of meaconers on the accuracy of aircraft GNSS estimated positions. This methodology is employed in the assessment of a localizer performance with vertical guidance (LPV - an operation employing GNSS for both lateral and vertical guidance) approach trajectory with SBAS corrections at Toulouse-Blagnac airport with 1 meaconer rebroadcasting L1 C/A signals from a fixed on-ground position near the runway, with predefined meaconer gains and delays, and given satellite geometries derived from the SPS 24-satellite almanac. The scenario configurations under scrutiny are selected to be representative of the meaconer's impact on the estimated GNSS receiver position during an LPV approach.

This article is organised as follows: Section II analyses the characteristics of the authentic and meaconer signals as received by the aircraft GNSS receiver. Section III analytically classifies the different meaconer impacts on the aircraft receiver correlator outputs, and matches the analytical situations with geometrical considerations. Section IV details the meaconer impact on the processing chain of the aircraft receiver. Section V expounds the effect of the meaconer on the GNSS observables and on the estimated position. Finally, Section VII showcases some simulation results and assess the meaconer impact on an aircraft GNSS receiver, regarding C/N_0, pseudorange errors, and position estimation.

II. RECEIVED SIGNAL STRUCTURE

This section is dedicated to characterize the signal model at the RF Front-End (RFFE) output of the aircraft GNSS receiver.

1. Emitted signal model

The GPS L1 C/A equivalent baseband emitted signal of the j-th satellite, denoted as $s_j(t)$, is expressed as given by Kaplan and Hegarty (2017):

$$s_j(t) = \sqrt{C_{\mathrm{e},j}(t)}\, d_j\,(t)\, c_j\,(t) \tag{1}$$

where $\sqrt{C_{\mathrm{e},j}(t)}$ represents the emitted power, $d_j(t)$ the navigation message signal and $c_j(t)$ the Pseudo Random Noise (PRN) code signal.

2. Received signal model under nominal conditions

In the absence of Radio Frequency Interference (RFI) and multipath, referred to as nominal conditions in this paper, the baseband mathematical model of the received GPS L1 C/A signal from all in-view satellites at the receiver antenna output, denoted as $r_{\mathrm{a}}(t)$, can be expressed (neglecting multipath) as:

$$r_{\mathrm{a}}(t) = \sum_{j=1}^{N_{\mathrm{a}}} \sqrt{C_{\mathrm{a},j}(t)} d_j\,(t - \tau_{\mathrm{a},j}(t))\, c_j\,(t - \tau_{\mathrm{a},j}(t))\, e^{j\theta_{a,j}(t)} \tag{2}$$

where the subscript 'a' denotes the nominal (authentic) signal, N_{a} is the number of visible satellites, $C_{\mathrm{a},j}(t)$ represents the received power of the j-th satellite signal, $\tau_{\mathrm{a},j}(t)$ is the propagation group delay, $\theta_{\mathrm{a},j}(t)$ is the propagation phase delay.

In addition to the received GNSS signal, a natural Additive White Gaussian Noise (AWGN) generated by active receiver elements and environmental factors such as temperature (antenna temperature), denoted as $n_{\mathrm{a}}(t)$, is taken into account. This AWGN is typically characterized by its spectral density N_0.

3. Meaconer definition and mathematical model

A meaconer, also known as a GNSS repeater, is an electronic device designed to capture electromagnetic signals (using a first receiving antenna), amplify them, and rebroadcast them (using a second emitting antenna) around a specific GNSS central frequency. The meaconer is characterized by its gain G_{m}, intrinsic delay τ_{m}, and frequency offset f_{m}. In this paper, meaconer gain G_{m} is defined as the ratio between the signal power at the meaconer's receiving antenna input and signal power at its emitting antenna output. The meaconer introduces an intrinsic delay τ_{m}, which signifies the signal group delay between the meaconer's receiving antenna input and its emitting antenna output. The frequency offset f_{m} denotes the offset between the received and rebroadcast signal frequency.

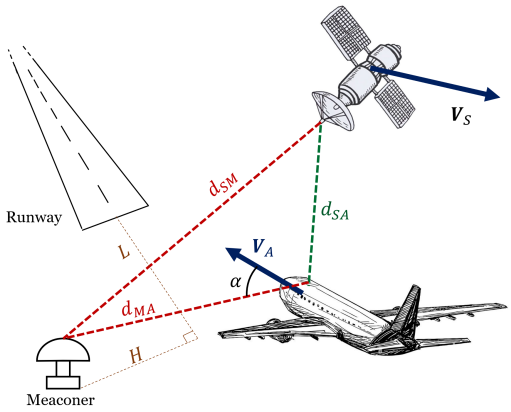


Figure 1: Illustration of the aircraft environment when exposed to a meaconer.

Fig. 1 presents the environment of an aircraft in the vicinity of a meaconer and the propagation of both nominal and repeated GNSS signal $s_j(t)$. d_{SA} represents the Euclidian distance between the satellite and the aircraft (i.e. the authentic signal distance), d_{SM} between the satellite and the meaconer and d_{MA} between the meaconer and the aircraft. It is important to note that $d_{SM} + d_{MA}$ represents the propagated distance of the repeated signal. Additionally, $\mathbf{v}_A$ and $\mathbf{v}_S$ denote the velocity vectors of the aircraft and the satellite, respectively, and α is the 3D non-oriented angle between $\mathbf{v}_A$ and the aircraft-to-meaconer vector.

From the previous descriptions, the N_s GNSS signals observed and rebroadcast by the meaconer are modelled to have the same structure as the authentic signals received at the aircraft's GNSS receiver antenna (2) but with different powers C_s (due to the meaconer gain and the different free space losses), time delays τ_s (due to the meaconer delay and the signal propagation time), and carrier phase offsets θ_s Coulon et al. (2020); Steindl et al. (2013). By defining the meaconing signal as the GPS L1 C/A signals rebroadcast by the meaconer, the equivalent baseband mathematical model of the meaconing signal at the receiver antenna input, $r_\mathrm{s}(t)$, can be represented (neglecting multipath from meaconing signals) as:

$$r_\mathrm{s}(t) = \sum_{j=1}^{N_\mathrm{s}} \sqrt{C_{\mathrm{s},j}(t)} d_j\left(t - \tau_{\mathrm{s},j}(t)\right) c_j\left(t - \tau_{\mathrm{s},j}(t)\right) e^{j\theta_{\mathrm{s},j}(t)}. \tag{3}$$

In addition to the repeated GNSS signal, the meaconer re-radiates an Additive White Gaussian Noise (AWGN) $n_\mathrm{s}(t)$, the summation of the captured noise and found noise in the meaconer.

The expression of the repeated signal can be defined relative to the authentic signal. In this paper, the relative parameters between nominal parameters $\boldsymbol{\eta}_\mathrm{a} = [\tau_\mathrm{a}; f_\mathrm{a}; \theta_\mathrm{a}; C_\mathrm{a}]^T$ and repeated ones $\boldsymbol{\eta}_\mathrm{s} = [\tau_\mathrm{s}; f_\mathrm{s}; \theta_\mathrm{s}; C_\mathrm{s}]^T$ are denoted as $\Delta\boldsymbol{\eta} = [\Delta\tau; \Delta f; \Delta\theta; \Delta g, \Delta N]^T$, and can be expressed based on the geometry presented in Fig. 1 and the meaconer characteristics, following the formulas presented hereafter.

The relative delay $\Delta\tau(t)$ represents the difference between the delay of the repeated signal and the delay of the authentic signal at the antenna input. It can be expressed as:

$$\Delta\tau(t) = \tau_\mathrm{s}(t) - \tau_\mathrm{a}(t) = \frac{d_{SM}(t) + d_{MA}(t)}{c} + \tau_\mathrm{m} - \frac{d_{SA}(t)}{c} + \Delta\tau_\mathrm{ant}(\psi_\mathrm{s}, \psi_\mathrm{a}) \tag{4}$$

c represents the speed of light, τ_m the intrinsic delay of the meaconer. $\Delta\tau_\mathrm{ant}$ accounts for the antenna group delay difference introduced by the different angles of arrival of the authentic ψ_a and of the meaconer ψ_s at the receiver antenna.

The relative Doppler shift Δf denotes the difference between the meaconer signal and the authentic signal Doppler shifts. It depends on the geometry and the velocities of the aircraft and the satellite, and can be expressed as (Spilker Jr. et al., 1996, p. 411):

$$\begin{aligned}\Delta f(t) = f_\mathrm{s}(t) - f_\mathrm{a}(t) &= \frac{(\mathbf{v}_S - \mathbf{v}_M)^T \mathbf{u}_{\mathbf{SM}} + (\mathbf{v}_M - \mathbf{v}_A)^T \mathbf{u}_{\mathbf{MA}}}{\lambda_1} + f_\mathrm{m} - \frac{(\mathbf{v}_S - \mathbf{v}_A)^T \mathbf{u}_{\mathbf{SA}}}{\lambda_1} \\ &\approx \frac{{\mathbf{v}_A}^T (\mathbf{u}_{\mathbf{SA}} - \mathbf{u}_{\mathbf{MA}})}{\lambda_1} + f_\mathrm{m}\end{aligned} \tag{5}$$

with $\mathbf{u_{SA}}$ the unit direction vector from S to A and λ_1 the wavelength of the GPS L1 C/A signal. Note that Eq. (5) assumes that the meaconer is fixed on the ground ($\mathbf{v}_M = 0$) and that the satellite is seen in the same direction from the meaconer and the aircraft point of view ($\mathbf{u_{SM}} \approx \mathbf{u_{SA}}$). In this paper, no frequency offset is considered ($f_{\text{m}} = 0$).

The relative phase $\Delta\theta$ is the phase difference between the nominal and meaconing signal, expressed as

$$\Delta\theta(t) = \theta_{\text{s}}(t) - \theta_{\text{a}}(t) = 2\pi f_1 \left(\frac{d_{SM}(t) + d_{MA}(t)}{c} - \frac{d_{SA}(t)}{c} \right) + \theta_{\text{m}} + \Delta\theta_{\text{ant}}(\psi_{\text{s}}, \psi_{\text{a}}) \tag{6}$$

with $f_1 = \lambda_1 / c$ the GPS L1 C/A signal carrier frequency, θ_{m} the meaconing phase shift and $\Delta\theta_{\text{ant}}$ accounts for the antenna phase shift difference introduced by the different angles of arrival of the authentic ψ_{a} and of the meaconer ψ_{s} at the receiver antenna.

The relative power denoted as Δg represents the ratio between the meaconer signal power C_{s} and the authentic signal power C_{a}:

$$10\log_{10}\left(\Delta g(t)\right) = 10\log_{10}\left(C_{\text{s}}(t)/C_{\text{a}}(t)\right) = 20\log_{10}\left(\frac{\lambda_1}{4\pi d_{MA}(t)}\right) + G_{\text{m}} + \Delta g_{\text{ant}}(\psi_{\text{s}}, \psi_{\text{a}}) + \Delta g_{\text{env}}(t) \tag{7}$$

where G_{m} represents the meaconer gain in decibels (dB), Δg_{ant} denotes the aircraft antenna gain difference in dB between the authentic and the meaconer signals, and Δg_{env} potential environment losses at the meaconer antenna such as building or tree occultations.

Lastly, the relative noise power spectrum density denoted as ΔN represents the ratio between the authentic noise density N_0 and re-radiated one N_{s}.

As a result, the equivalent baseband model of the meaconing signal at the receiver antenna input, $r_{\text{s}}(t)$, can be represented in terms of the relative parameters $\Delta\tau(t)$, $\Delta\theta(t)$, and $\Delta g(t)$:

$$r_{\text{s}}(t) = \sum_{j=1}^{N_{\text{s}}} \sqrt{\Delta g(t)\, C_{\text{a},j}(t)}\, d_j\left(t - \tau_{\text{a},j}(t) - \Delta\tau(t)\right) c_j\left(t - \tau_{\text{a},j}(t) - \Delta\tau(t)\right) e^{j\left(\theta_{\text{a},j}(t) + \Delta\theta(t)\right)}. \tag{8}$$

4. Signal at RF Front-end block

The equivalent baseband received signal at the aircraft Radio Frequency Front-End (RFFE) block output, while neglecting the effects of ADC/AGC for simplicity purposes, can be expressed as

$$r_{\text{IF}}(t) = (r_{\text{a}} + r_{\text{a}} + n_{\text{s}} + n_{\text{s}}) * h_{\text{RF}}(t). \tag{9}$$

The total noise contribution at the RFFE block output, denoted n(t), is characterized by its spectral density N_{eff}, expressed as

$$N_{\text{eff}}(f) = \left|H_{\text{RF}}(f)\right|^2 N_0\left(1 + \Delta N\right), \tag{10}$$

where $H_{\text{RF}}(f)$ is the transfer function of the RFFE block.

III. CLASSIFICATION OF THE MEACONER IMPACTS

The correlator quantifies the similarity between the incoming signal $r_{\text{IF}}(t)$ and the local replica. The correlator plays a crucial role throughout the entire processing chain, including the estimation of channel parameters (used for generating pseudoranges) and the demodulation of the navigation message. As a result, any distortion induced by the meaconer on the correlator output can directly and significantly impact the overall signal processing and reception performance.

This section illustrates the impact of the meaconer on the mathematical model of the correlator output. To simplify the analysis of the meaconer's impact, a classification of the meaconer's effect on the correlator output (and consequently on the reception chain) is proposed, categorizing it into four distinct scenarios: nominal, jamming, spoofing, and multipath.

In the following of the paper, the parameters $\boldsymbol{\eta}_{\text{a}}[k]$ and $\Delta\boldsymbol{\eta}[k]$ denote the continuous time parameters $\boldsymbol{\eta}_{\text{a}}(t)$ and $\Delta\boldsymbol{\eta}(t)$ taken in $t = (k + 1/2)T_{\text{i}}$. Assuming constant frequency, constant propagation time delay and constant power over the integration time T_{i}, the discrete parameters can be expressed as

$$\tau_{\text{a}}[k] = \tau_{\text{a}}(kT_{\text{i}}), \quad f_{\text{a}}[k] = f_{\text{a}}(kT_{\text{i}}), \quad C_{\text{a}}[k] = C_{\text{a}}(kT_{\text{i}}), \quad \theta_{\text{a}}[k] = \theta_{\text{a}}(kT_i) + \pi T_{\text{i}} f_{\text{a}}[k] \tag{11}$$

and

$$\Delta\tau[k] = \Delta\tau(kT_\mathrm{i}), \quad \Delta f[k] = \Delta f(kT_\mathrm{i}), \quad \Delta g[k] = \Delta g(kT_\mathrm{i}), \quad \Delta\theta[k] = \Delta\theta(kT_i) + \pi T_\mathrm{i}\Delta f[k] \tag{12}$$

1. Correlator output model

The correlator's output at epoch k, denoted as $\zeta[k]$, is defined as the result of the correlation between the incoming signal $r_\mathrm{IF}(t)$ and the local replica $c(t)$ over the integration time T_i. The incoming signal $r_\mathrm{IF}(t)$ has been shown as a linear combination of the nominal and meaconing signals in Section II. Therefore, the correlator's output is also a linear combination of the correlator outputs individually generated by the nominal signal, the meaconing signal, and effective additive white Gaussian noise (AWGN).

The contribution of the nominal signal $r_\mathrm{a}(t)$ on the prompt correlator output, also referred to as nominal peak and denoted ζ_a can be expressed at epoch k, assuming constant frequency, and no bit transitions over the integration time T_i as (Spilker Jr. et al., 1996, p. 364)

$$\zeta_\mathrm{a}[k] = \sqrt{C_\mathrm{a}}\, d[k] R_{\hat{c}}(\varepsilon_\tau[k])\,\mathrm{sinc}\left(\pi\varepsilon_f[k]T_i\right)\exp\left(j\varepsilon_\theta[k]\right) \tag{13}$$

Where, introducing the tracking parameters ($\hat{\tau}[k]$, $\hat{\theta}[k]$, $\hat{f}_D[k]$) as the propagation parameters estimated by the tracking loops at time $t = (k + 1/2)T\mathrm{i}$, ($\varepsilon_\tau[k]$, $\varepsilon_\theta[k]$, $\varepsilon_f[k]$) represent the errors between the tracking parameters and their nominal values, which can be expressed as

$$\varepsilon_\tau[k] = \tau_\mathrm{a}[k] - \hat{\tau}[k], \quad \varepsilon_\theta[k] = \theta_\mathrm{a}[k] - \hat{\theta}[k], \quad \varepsilon_f[k] = f_\mathrm{a}[k] - \hat{f}_\mathrm{D}[k] \tag{14}$$

and $R_{\hat{c}}(\tau)$ is the received PRN code autocorrelation (with orthogonality properties) reflecting the ideal PRN code autocorrelation filtered by the RFFE block h_RF. Similarly, the contribution of the repeated signal $r_\mathrm{s}(t)$ on the correlator output, referred to as meaconing peak and denoted ζ_s can be expressed as

$$\zeta_\mathrm{s}[k] = \sqrt{\Delta g[k]\; C_\mathrm{a}[k]}\; d[k] R_c(\varepsilon_\tau[k] + \Delta\tau[k])\,\mathrm{sinc}\left(\pi(\varepsilon_f[k] + \Delta f[k])T_\mathrm{i}\right)\,\exp\left(j(\varepsilon_\theta[k] + \Delta\theta[k])\right). \tag{15}$$

Additionally the nominal plus re-radiated AWGN at correlator output is denoted $\zeta_n[k]$. Assuming Gaussian characteristics for both the nominal and re-radiated noise and ensuring that the bandwidth of the Radio Frequency Front-End (RFFE) block is substantial compared to the spectrum of the GPS L1 signal, $\zeta_n[k]$ can be expressed by its power spectrum density $N_{\mathrm{eff},\zeta}$ as Betz (2001)

$$N_{\zeta,\mathrm{eff}} = N_0\left(1 + \Delta N\right). \tag{16}$$

In conclusion, the complex representation of the correlator output $\zeta[k]$ can be expressed as

$$\zeta[k] = \zeta_\mathrm{a}[k] + \zeta_\mathrm{s}[k] + \zeta_n[k], \tag{17}$$

introducing an additionnal correlation peak $\zeta_\mathrm{s}[k]$ separated from the nominal peak $\zeta_\mathrm{a}[k]$ by the relative time delay $\Delta\tau[k]$, relative frequency $\Delta f[k]$ and relative phase $\Delta\theta[k]$. These parameters evolve at each iteration k. The changes in these relative parameters create variations in the configuration between the two contributions to the total correlator output. In order to simplify the expression of $\zeta[k]$, a classification of the correlator expression is proposed in function of the relative parameters $\Delta\tau$, Δf and Δg.

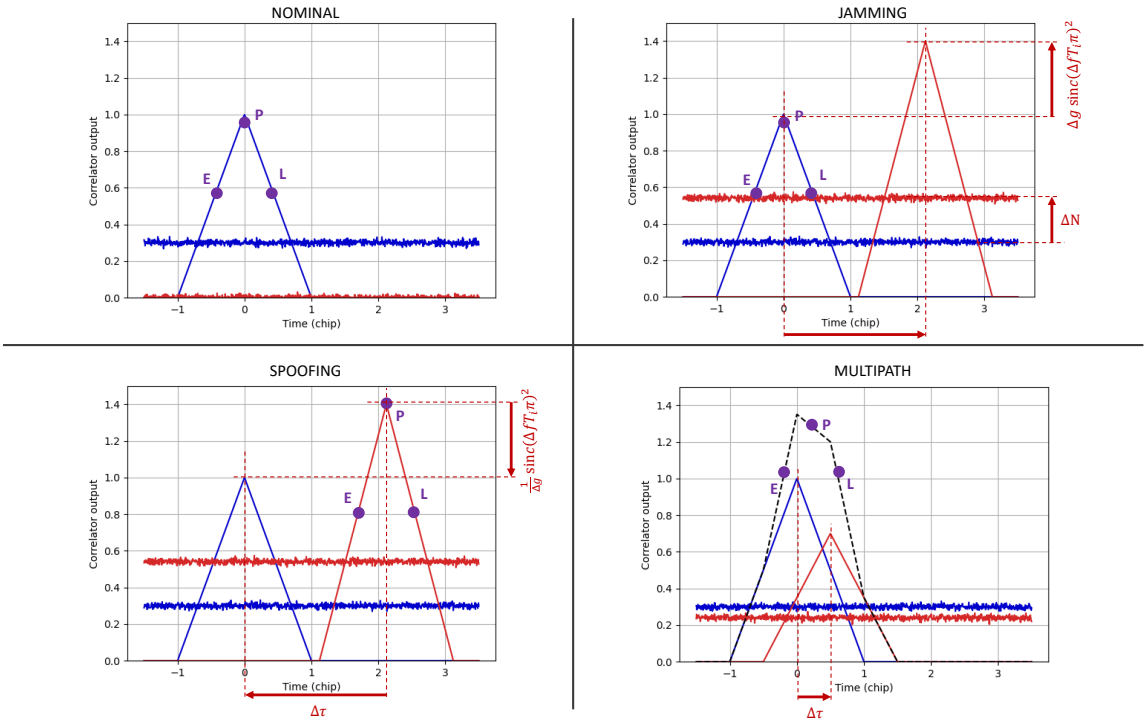


Figure 2: Illustration of the correlation peaks and noise for the different situations (nominal components in blue and meaconer components in red)

2. Nominal situation

In the nominal situation, the receiver is synchronized with the nominal signal parameters, without any signficant distortion induced by the meaconer. This includes both the repeated GNSS signal and re-radiated noise. Under these conditions, the correlator output can be simplified to:

$$\zeta[k] = \zeta_{\mathrm{a}}[k] + \zeta_n[k], \tag{18}$$

with noise power spectrum density $N_{\mathrm{eff}} = N_0$.

The condition to be in nominal situation can be translated into mathematical terms based on the relative parameters $\Delta\boldsymbol{\eta}[k]$. To ensure that there is no significant distortion introduced by the meaconer, two conditions need to be met, as depicted in Fig. 2 and expressed in Eq. (13). Firstly, the power of the re-radiated noise should be negligible, which can be described using the threshold γ_n as $[\Delta g < \gamma_n]$. Moreover, the meaconing peak must be positioned at a significant distance (either in terms of delay or frequency) or is sufficiently low in magnitude compared to the nominal peak, to disregard the distortion induced by the meaconing peak. Recognizing that $R_c(\tau) = 0$ for $\tau > T_c + c_\tau/2$ (with c_τ being the Early-Late spacing), and introducing a threshold γ_g where the meaconing peak's amplitude is considered negligible in comparison to the nominal peak's, the separation condition can be formulated as $\left[(|\Delta\tau| > T_c + c_\tau/2) \cup \left(\Delta g \,\mathrm{sinc}(\pi \Delta f T_{\mathrm{i}})^2 < \gamma_g\right)\right]$. Therefore

$$[\Delta g < \gamma_n] \cap \left[(|\Delta\tau| > T_c + c_\tau/2) \cup \left(\Delta g \,\mathrm{sinc}(\pi \Delta f T_{\mathrm{i}})^2 < \gamma_g\right)\right]. \tag{19}$$

3. Jamming situation

In the jamming situation, the receiver is synchronized with the nominal signal parameters, and the meaconing peak is positioned at a significant distance (either in terms of delay or frequency) or is sufficiently low in magnitude compared to the nominal peak, to disregard the distortion induced by the meaconing peak. The impact of the meaconer on the correlator output is thus primarily limited to the rebroadcast noise. This situation can be considered analogous to a jamming threat (hence the name), where a non-GNSS signal is transmitted to the receiver. Under these conditions, the correlator output can be simplified to

$$\zeta[k] = \zeta_{\mathrm{a}}[k] + \zeta_n[k], \tag{20}$$

with noise power spectrum density $N_{\mathrm{eff}} = N_0\,(1 + \Delta N)$.

Similarly to the nominal situation, the condition for the jamming scenario can be translated into mathematical terms. The separation condition, as introduced in Eq. (19), remains unchanged. However, to characterize a jamming situation, the noise spectral density is presumed to be greater than the threshold γ_n. To conclude, assuming that both of the aforementioned conditions are satisfied, the receiver must achieve nominal peak tracking at the initiation of the jamming situation (either during acquisition or transitioning from another situation), which can be expressed as $\varepsilon_\eta(0) \approx 0$. Therefore

$$[\varepsilon_\eta(0) \approx 0] \cap [\Delta N > \gamma_n] \cap \left[(|\Delta\tau| > T_c + c_\tau/2) \cup \left(\Delta g \,\mathrm{sinc}(\pi \Delta f T_\mathrm{i})^2 < \gamma_g\right)\right] \tag{21}$$

4. Spoofing situation

In the spoofing situation, the receiver is synchronized to the meaconing signal parameters (meaconing peak), and the nominal peak is positioned at a significant distance (either in terms of delay or frequency) or is sufficiently low in magnitude compared to the meaconing peak, to disregard the 'distortion' induced by the nominal peak on the parameters synchronization. This synchronization is disturbed by nominal plus re-radiated AWGN noise. Under these conditions, the correlator output can be simplified to

$$\zeta[k] = \zeta_\mathrm{s}[k] + \zeta_n[k], \tag{22}$$

with noise power spectrum density $N_\mathrm{eff} = N_0\,(1 + \Delta N)$.

For spoofing situation condition, two conditions must be fulfilled. Firstly, much like the conditions for the nominal and jamming situation, a separation criterion can be established. However, this time the focus is on the meaconing peak. As illustrated in Fig. 2 and shown in Eq. (15) and assuming $\varepsilon_f \approx -\Delta f$, the separation condition can be framed as $\left[(|\Delta\tau| > T_c + c_\tau/2) \cup \left(\mathrm{sinc}(\pi \Delta f T_\mathrm{i})^2/\Delta g < \gamma_g\right)\right]$. Additionally, upon confirming the fulfillment of the separation criterion, the receiver must achieve meaconing peak tracking at the initiation of the spoofing situation (either during acquisition or transitioning from another situation), which can be expressed as $\varepsilon_\eta(0) \approx -\Delta\eta$. Therefore

$$[\varepsilon_\eta(0) \approx -\Delta\eta] \cap \left[(|\Delta\tau| > T_c + c_\tau/2) \cup \left(\frac{1}{\Delta g}\,\mathrm{sinc}(\pi \Delta f T_\mathrm{i})^2 < \gamma_g\right)\right] \tag{23}$$

5. Multipath situation

In the multipath situation, the nominal and meaconing peaks are sufficiently close to each other (either in terms of delay or frequency) to both affect the synchronization process. The synchronization is also disturbed by the nominal plus re-radiated AWGN noise. Under these conditions, the correlator output cannot be simplified, and therefore, the original expression for the correlator output (17) is retained.

In this situation, the synchronization distortion is analogous to the effects observed with classical multipaths with only one ray. These effects are well studied in the literature, presented for instance in (Spilker Jr. et al., 1996, chap. 14). However, unlike typical multipath signals, the meaconer signal's amplitude can closely match or even exceed that of the nominal peak, and the re-radiated noise increase the effective power of received noise.

To reach multipath situation, the two peaks must be sufficiently close to each other and not negligible in relation to each other (Fig. 2). This condition stands in contrast to the separation criteria for both jamming (Eq. (21)) and spoofing (Eq. (23)) situations. Therefore

$$[|\Delta\tau| < T_c + c_\tau/2] \cap \left[\left(\frac{1}{\Delta g}\,\mathrm{sinc}(\pi \Delta f T_\mathrm{i})^2 > \gamma_g\right) \cup \left(\Delta g \,\mathrm{sinc}(\pi \Delta f T_\mathrm{i})^2 > \gamma_g\right)\right] \tag{24}$$

In the context of civil aviation, where the relative geometry between the aircraft and the meaconer undergoes rapid variations, the condition (24) is unlikely to be satisfied. Consequently, this paper focuses principally on jamming and spoofing situations.

IV. ARCHITECTURE OF THE GNSS RECEIVER

This section introduces the architecture of the aircraft receiver reception chain. A scheme of the signal processing and navigation solution blocks can be seen in Fig. 3. This processing chain adheres to civil aviation receiver standards and encompasses the required stages that contribute to signal processing up to navigation solutions.

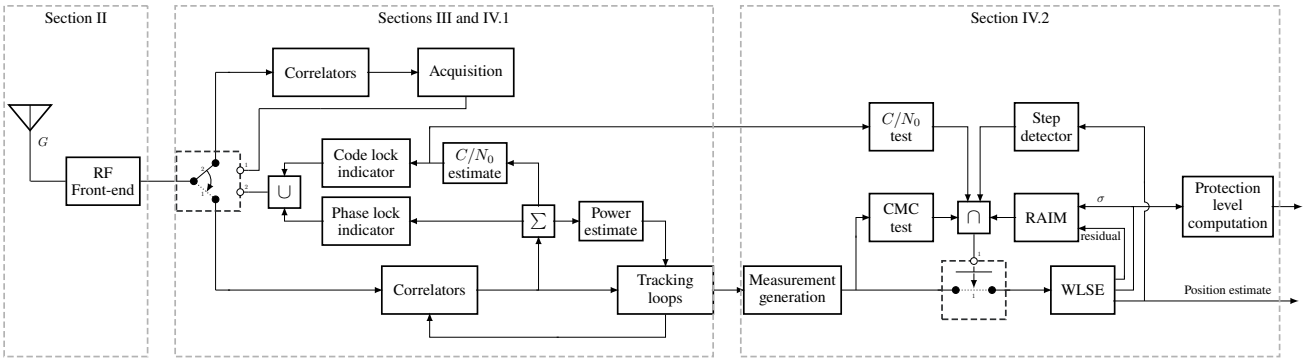


Figure 3: Receiver architecture.

1. GNSS signal processing

The signal processing chain performs the synchronization of the local replica with the GNSS signal and enables the demodulation of the navigation message. This chain typically encompasses the following stages: Acquisition, tracking (including tracking loops, Lock detectors and C/N_0 estimators) and demodulation.

a) Tracking loops

The tracking loop is responsible for maintaining a fine synchronization with the incoming satellite signals. This synchronization is crucial for successfully decoding navigation messages and accurately determining the pseudorange of a specific satellite. Each received GNSS signal is tracked independently by at least two tracking loops, which perform two crucial functions: carrier phase synchronization, accomplished through a phase-locked loop (PLL), and code delay synchronization, achieved through a delay-locked loop (DLL).

Commonly, the tracking loops incorporate a comparator, which evaluates the synchronization error between the incoming signal characteristics and the locally generated replica characteristics using correlator outputs presented in Eq. (17). The estimated signal characteristic synchronization error then undergoes filtering through a loop low-pass filter, and its output is supplied to the Numerical Control Oscillator (NCO). The NCO's frequency is adjusted based on its input to minimize the synchronization error (Spilker Jr. et al., 1996, p. 369).

b) Lock detectors and C/N_0 estimators

Lock detectors play a crucial role in monitoring the signal tracking quality. These detectors can be implemented for both code and phase synchronization. A comprehensive explanation and performance analysis of lock detectors is presented in (Spilker Jr. et al., 1996, p. 390). On one hand, code lock detection is closely linked to carrier-to-noise-density ratio (C/N_0) estimation which is commonly used to monitor the quality of the code synchronization. Various algorithms have been presented in the literature for C/N_0 estimation, including the Moments, Beaulieu's and the Narrowband-Wideband Power Ratio (NWPR) methods Pauluzzi and Beaulieu (2000). On the other hand, phase lock is commonly monitored using a normalized estimate of the cosine of twice the carrier phase (NECT), as detailed in Parkinson's work (Spilker Jr. et al., 1996, p. 393).

Both code and phase locks yield lock indicators, which are subsequently compared to predefined thresholds, are denoted as γ_τ and γ_θ, respectively. These comparisons determine whether the signal is being accurately enough tracked. If either of these indicators falls below its corresponding threshold, a loss of lock condition is triggered. In such cases, the signal tracking process is terminated, and the re-acquisition procedure is initiated.

c) Acquisition and re-acquisition

The Acquisition block ascertains the presence or absence of incoming GNSS signals and provides a preliminary estimation of the code delay $\hat{\tau}_0$ and the Doppler shift $\hat{f}_{\mathrm{D},0}$ to initiate the tracking loops.

For the signal acquisition of a selected PRN, the process involves searching for the corresponding correlator peak (17) across a discrete two-dimensional grid in time (code delay) and frequency. The validity of this peak is subsequently analyzed using a statistical test. It is important to note that the search grid may contain additional peaks caused by secondary frequency lobes, noise, or interference, potentially leading to false alarms in the acquisition procedure. Particularly, meaconing interference can induce additional peaks, as elaborated in Sec. III.1. In civil aviation, the acquisition of the GPS L1 C/A signal involves testing the highest correlation peak within the search grid. (ED259, 2019, REQ-235)

In a similar manner, re-acquisition is initiated after a loss of lock (Section IV.1 b)). However, re-acquisition is carried out on a single Doppler bin since the Doppler frequency is known at the end of the tracking process. (ED259, 2019, REQ-235)

2. GNSS observable processing

a) Nominal pseudorange model and carrier smoothing

The raw pseudoranges are derived from the tracking loop outputs Kaplan and Hegarty (2017). The frequency of the tracking loop outputs ($f_s = 1/T_i$) is higher than the frequency of the measurement generation, hence, not all the tracking loop outputs are used for measurement generation. κ denotes the discrete epochs at which the measurement are generated. In a nominal situation, they can be expressed as follows:

$$\rho_i[\kappa] = d_i[\kappa] - c\,\delta t_i[\kappa] + c\,\delta t_r[\kappa] + T_i[\kappa] + I_i[\kappa] + M_i[\kappa] + n_i[\kappa] \tag{25}$$

$$\phi_i[\kappa] = d_i[\kappa] - c\,\delta t_i[\kappa] + c\,\delta t_r[\kappa] + T_i[\kappa] - I_i[\kappa] + m_i[\kappa] + \Omega_i[\kappa]\lambda + n_{\phi,i}[\kappa] \tag{26}$$

where the subscript i denotes the satellite PRN, κ represents the discrete epoch at which the measurement are generated ($\kappa \neq k$), ρ signifies the pseudorange, d stands for the geometric distance between the aircraft GNSS receiver and the satellite's antenna phase centers, δt_i is the satellite clock bias, δt_r is the receiver clock bias, T represents the tropospheric delay, I indicates the ionospheric delay, M (resp. m) is the code (resp. phase) multipath error, Ω the integer ambiguity error, and n (resp. n_ϕ) the delay (resp. phase) tracking loop error. Ω is considered constant whilst lock is maintained.

Before they are employed in Weighted Least Squares (WLS) position estimation, the code pseudorange from satellite i at epoch κ is smoothed using the phase pseudorange Geng et al. (2019):

$$\begin{cases} \hat{\rho}_i[\kappa] = \frac{1}{\Gamma}\rho_i[\kappa] + \frac{\Gamma-1}{\Gamma}\left(\hat{\rho}_i[\kappa-1] + \phi_i[\kappa] - \phi_i[\kappa-1]\right) & \text{if available} \\ \hat{\rho}_i[\kappa] = \rho_i[\kappa] & \text{otherwise} \end{cases}. \tag{27}$$

In this equation, the smoothed pseudorange $\hat{\rho}_i[\kappa]$ for satellite i at epoch κ is calculated using the code pseudorange at epoch κ and the phase pseudoranges at both previous $(\kappa - 1)$ and current (κ) epochs. This smoothing effect is active only when both code and phase measurements are available during consecutive epochs. To comply with civil aviation standards ED259 (2019), $\Gamma = 100 f_s$, where f_s is the sampling frequency of pseudorange generation, achieving a smoothing effect with an exponential decay of characteristic time 100 seconds.

b) Measurement checks

Before pseudoranges are utilized for position estimation, they must pass three consecutive tests in accordance with aviation standards. First, a C/N_0 check screens pseudoranges with a corresponding C/N_0 ratio lower than 30 dB-Hz. Second, a step detector test removes pseudoranges when a step larger than 700 m is detected. If, retrospectively, the difference between the smoothed pseudorange at epoch κ and the smoothed pseudorange at epoch $(\kappa - 1)$ exceeds 700 m when clock bias estimations are available, the pseudorange is excluded by the step detector from the Weighted Least Squares Estimator (WLSE), and a new position is calculated based on the remaining smoothed pseudoranges ED259 (2019). Last, a measurement quality monitoring test (also known as the Code Minus Carrier - CMC test) removes pseudoranges with an unsmoothed-to-smoothed difference greater than 10 m ED259 (2019), meaning $|\hat{\rho}_i[\kappa] - \rho_i[\kappa]| > 10$ m.

c) WLS estimation

When there are at least 4 valid pseudoranges at a given epoch, a position estimation can be computed using (DO229E, 2016, Appendix E):

$$\hat{\mathbf{x}} = \mathbf{S}\mathbf{y} \tag{28}$$

$$\mathbf{S} = \left(\mathbf{G}^T\mathbf{W}\mathbf{G}\right)^{-1}\mathbf{G}^T\mathbf{W} \tag{29}$$

$$\mathbf{G} = \begin{bmatrix}\mathbf{g}_1^T & \dots & \mathbf{g}_{N_s}^T\end{bmatrix}^T \tag{30}$$

$$\mathbf{g}_i^T = \begin{bmatrix} -\cos(\omega_i)\sin(\phi_i) \\ -\cos(\omega_i)\cos(\phi_i) \\ -\sin(\omega_i) \\ 1 \end{bmatrix} \tag{31}$$

$$\mathbf{W} = \begin{bmatrix} \sigma_1^{-2} & 0 & \dots & 0 \\ 0 & \sigma_2^{-2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \sigma_{N_s}^{-2} \end{bmatrix} \tag{32}$$

$$\tag{33}$$

where $\mathbf{y}$ contains the smoothed pseudoranges $\hat{\rho}_i[k]$, and ω_i, ϕ_i represent the elevation and azimuth angles of satellite i with respect to the estimated aircraft position (the dependence of $\mathbf{y}$, $\mathbf{S}$, $\mathbf{G}$, $\mathbf{W}$, ω_i, and ϕ_i on κ is omitted in the notations for clarity).

d) Fault detection and exclusion

The software receiver implements Fault Detection and Exclusion (FDE) to detect and exclude faulty observables. The FDE procedure, described in Parkinson and Axelrad (1988) and summarized in Algorithm 1, is based on hypothesis testing of the sum squared WLSE residuals, which should follow a Chi-Squared distribution with $N_s - 4$ degrees of freedom. If all the PRNs are in the nominal situation, the sum squared WLSE residuals have a Chi-Squared distribution with a centrality parameter equal to zero. If at least one PRN is spoofed, the sum squared WLSE residuals also have a Chi-Squared distribution, but with a non-zero centrality parameter. The threshold is derived from the fault-free distribution with a false alarm probability set to $p_{\text{fa}} = 1.6\text{e}-5/\text{app}$ (DO229E, 2016, 2.1.4.2.2.2.3).

Algorithm 1: FDE procedure

for *every epoch with at least 5 usable signals* **do**
  compute T (35)
  compute a_{N_s} (36)
  if $T < a_{N_s}$ **then**
    no fault detected
  else
    $k = 1$
    while $N_s - k \geq 5$ **do**
      compute T for all subsets of $N_s - k$ satellites
      compute a_{N_s-k}
      if *only one subset gives a residual less that* a_{N_s-k} **then**
        the subset is considered to be fault-free
        others are excluded from the position computation
        end of the FDE procedure
      else
        $k \leftarrow k + 1$
      end
    end
    a fault is detected
    all the satellites are used for the position computation
  end
end

The test statistic T and the threshold a_{N_s} are given by Hewitson and Wang (2006)

$$\mathbf{r} = (\mathbf{I} - \mathbf{G}[\mathbf{G}^T\mathbf{W}\mathbf{G}]^{-1}\mathbf{G}^T\mathbf{W})\mathbf{e} \tag{34}$$

$$T = \mathbf{r}^T\mathbf{W}\mathbf{r} \tag{35}$$

$$a_{N_s} = F^{-1}_{N_s-4}(1 - p_{\text{fa}}) \tag{36}$$

$\mathbf{e}$ contains the N_s differences between the smoothed pseudoranges at epoch κ and the estimated pseudoranges at epoch κ, obtained using the estimated position and estimated receiver clock delay, and the known position of the satellites. r denotes the pseudorange residuals, and $F^{-1}_{N_s-4}$ represents the inverse cumulative distribution function (CDF) of the chi-square distribution with $N_s - 4$ degrees of freedom. When only 4 satellites are tracked, FDE is deemed non-operational and no FDE alarm can be raised. In this case, the position is still estimated but not used for navigation due to its unknown integrity. With only 5 satellites tracked, FDE can only detect a fault but cannot exclude it. If no fault is detected, the position is used for navigation.

V. MEACONER IMPACT MODELLING

This section presents a prediction of the impact of the meaconer following the classification presented in Section III. These different impacts are then used in the next section to predict the meaconer impact during an actual aircraft approach.

1. Impact on the $\mathbf{C/N_0}$

The C/N_0 ratio represents the relationship between the power of the useful signal C_{eff} and the noise density $N_{0,\text{eff}}$. In the presence of a meaconer, it is important to note that both the nominal and meaconing signals carry the navigation message, as evidenced by Eqs. (13) and (15). The characterization of C/N_0 can thus be established considering the multipath, jamming, and spoofing situations.

a) Jamming situation impact on the C/N_0

In a jamming situation, the receiver tracks the nominal peak without being affected by the meaconing peak. As a result, the effective signal power becomes $C_{\text{eff, J}} = C_{\text{a}}$. Moreover, the noise density, defined in Section III as $N_{\text{eff}} = N_0\,(1 + \Delta N)$, affects the effective C/N_0 as follows:

$$\left(\frac{C}{N_0}\right)_{\text{eff, J}} = \frac{1}{(1 + \Delta N)}\left(\frac{C}{N_0}\right)_{\text{a}} \tag{37}$$

where $(C/N_0)_{\text{a}}$ denotes the nominal C/N_0. Therefore, in a jamming situation, the effective C/N_0 experiences a reduction by a factor of $(1 + \Delta N)$.

In line with Section IV.1 b), signal tracking is considered lost if the effective C/N_0 falls below the threshold γ_τ. This condition can be expressed in terms of ΔN as (in linear)

$$\Delta N_{\text{loss}} = \frac{1}{\gamma_\tau}\left(\frac{C}{N_0}\right)_{\text{a}} - 1. \tag{38}$$

b) Spoofing situation impact on the C/N_0

In a spoofing situation, the receiver tracks the meaconing peak without interference from the nominal peak. The effective signal power becomes $C_{\text{eff, J}} = C_{\text{s}} = \Delta g C_{\text{a}}$. Similar to the jamming case, the effective noise density is $N_{\text{eff}} = N_0\,(1 + \Delta N)$. The effective C/N_0 is then given by

$$\left(\frac{C}{N_0}\right)_{\text{eff, S}} = \frac{\Delta g}{(1 + \Delta N)}\left(\frac{C}{N_0}\right)_{\text{a}} \tag{39}$$

Note that if ΔN is high, then

$$\lim_{\Delta N \to \infty}\left(\frac{C}{N_0}\right)_{\text{eff, S}} = \frac{\Delta g}{\Delta N}\left(\frac{C}{N_0}\right)_{\text{a}} = \left(\frac{C}{N_0}\right)_{\text{s}} \tag{40}$$

where $(C/N_0)_{\text{s}}$ represents the C/N_0 at the meaconer receiver.

In spoofing situations, signal tracking is lost when

$$\Delta N < \left(\frac{1}{\gamma_\tau}\left(\frac{C}{N_0}\right)_{\text{a}} - 1\right)^{-1} = (\Delta N_{\text{loss}})^{-1}. \tag{41}$$

2. Impact on the pseudoranges

Depending on the meaconer impact, the nominal pseudorange model of each satellite given in (25) and (26) can be modified as described in the next subsection.

a) Jamming situation impact on the pseudoranges

In a jamming situation, the C/N_0 of the PRN decreases accordingly to Eq. (37). Furthermore, as detailed in Kaplan and Hegarty (2017), the variance of the tracking loop's thermal noise errors is interconnected with the effective C/N_0. Consequently, jamming leads to amplified thermal noise errors and leaves the other equation terms unchanged, as the receiver tracking loops are unaffected by the meaconer's useful signal. In jamming situations, the pseudorange models become:

$$\rho_{i,\text{jam}}[\kappa] = d_i[\kappa] - c\,\delta t_i[\kappa] + c\,\delta t_r[\kappa] + T_i[\kappa] + I_i[\kappa] + M_i[\kappa] + \tilde{n}_i[\kappa] \tag{42}$$

$$\phi_{i,\text{jam}}[\kappa] = d_i[\kappa] - c\,\delta t_i[\kappa] + c\,\delta t_r[\kappa] + T_i[\kappa] - I_i[\kappa] + m_i[\kappa] + N_i[\kappa]\lambda + \tilde{n}_{\phi,i}[\kappa] \tag{43}$$

where $\tilde{n}$ (resp. $\tilde{n}_\phi$) represents the variance-increased code (resp. phase) thermal noise errors at the tracking loop output.

b) Spoofing situation impact on the pseudoranges

In a spoofing situation, the tracking loops follow the meaconer signal. The meaconer signal is nearly identical to the authentic one, but with a longer propagation time because it detours through the meaconer, resulting in an increased traveled distance. The spoofed pseudoranges have then the same characteristics as the authentic ones, along with an additional bias corresponding to the time offset between the authentic LOS transmission time and the meaconer signal's total transmission time. Particularly, Eq. (39) exposes that the spoofed C/N_0 is similar to the authentic C/N_0 when Δg is high (because $\Delta g = \Delta N >> 1$), and the thermal noise of the tracking loop outputs under spoofing is comparable to the thermal noise in nominal conditions. In spoofing situations, the pseudorange models become:

$$\rho_{i,\text{spo}}[\kappa] = d_i[\kappa] - c\,\delta t_i[\kappa] + c\,\delta t_r[\kappa] + T_i[\kappa] + I_i[\kappa] + M_i[\kappa] + n_i[\kappa] + c\,\Delta\tau_i[\kappa] \tag{44}$$

$$\phi_{i,\text{spo}}[\kappa] = d_i[\kappa] - c\,\delta t_i[\kappa] + c\,\delta t_r[\kappa] + T_i[\kappa] - I_i[\kappa] + m_i[\kappa] + N_i[\kappa]\lambda + n_{\phi,i}[\kappa] + c\,\Delta\tau_i[\kappa] \tag{45}$$

$$c\,\Delta\tau_i[\kappa] = d_{MA}[\kappa] + d_{SM}[\kappa] - d_{SA}[\kappa] + c\,\tau_m \tag{46}$$

Where d_{MA}, d_{SM} and d_{SA} are the distances defined in Fig. 1.

3. Impact on the position

The impact of the meaconer on the position during an approach can be predicted based on the classification of Section III on the incoming signals and the FDE algorithm 1. The estimated position can be categorized into different cases according to the classification of the different smoothed and valid signals arriving at the current epoch. Figure 4 classifies the position situations based on the previously described meaconer's impact on the pseudoranges.

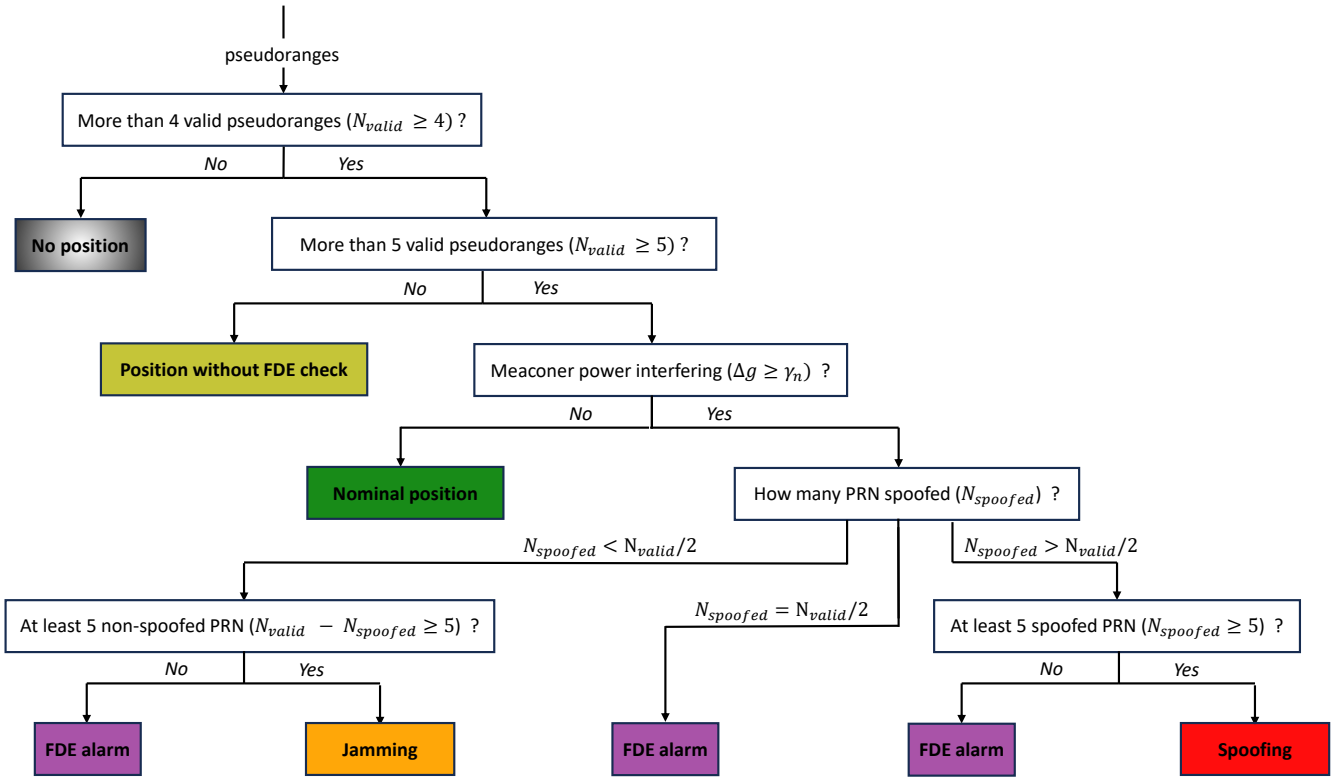


Figure 4: Classification of the meaconer impact on the position based on its impact on the pseudoranges.

The classification shown in Fig. 4 details the different impacts that the meaconer can have on the aircraft position estimation, and is based on the N_{valid} usable smoothed pseudoranges that have passed the approval processes outlined in IV.2 b) for the current epoch. $N_{spoofed}$ denotes the number of pseudoranges among the valid ones that are in the spoofing situation at the current epoch. The spoofed pseudoranges may successfully pass the approval processes because they mimick authentic pseudoranges characteristics. Moreover, the different tests are initialized when a re-acquisition is performed on the concerned PRN, so no consistency check can be performed between a previously tracked authentic signal and a currently tracked spoofed signal. However, the C/N_0 test removes the pseudoranges with an estimated C/N_0 lower than 30 dB $\cdot$ Hz. This situation occurs before a loss of lock due to the meaconer jamming effect, the C/N_0 test has an impact of the pseudorange validation process in the presence of meaconer interference. The quantity
γ_n is the power ratio below which the aircraft receiver is assumed not affected by the meaconer signals. This threshold is arbitrary and is set for simplicity purposes, the real transition from the nominal to the jamming situation is continuous.
The first two stages of the diagram discriminate the impact from the number of valid smoothed pseudoranges. These two steps depict general behaviours of the WLSE and are not specific to a meaconer interference scenario. WLS needs at least 4 measurements to derive a position (and a receiver clock offset estimation) ; when 4 pseudoranges are usable, FDE cannot be executed since it needs a minimum of 5 measurements to test the consistency of the pseudoranges.
When all the valid incoming signals are catalogued as in the nominal situation (when the meaconer signal power is negligible compared to the authentic signal power, $\Delta g < \gamma_n$), all the pseudoranges and C/N_0 estimations follow nominal behaviours. The resulting position estimation after WLS is well-documented in the literature Kaplan and Hegarty (2017), and is referred as a nominal position situation in this paper.
When $\Delta g \geq \gamma_n$, the meaconer power is no longer negligible and it impacts the aircraft receiver, at least because the meaconer broadcast noise is captured by the aircraft receiver and increases the thermal noise. The possible outcomes are a jammed position, a spoofed position, and an unavailable position (due to an alarm raised by FDE). The number of pseudoranges considered in the spoofing situation $N_{spoofed}$ helps to efficiently catalog the impact of the meaconer on the position estimation between the three potential situations.
The additional biases in the spoofed pseudoranges are so large that the probability of missed detection of FDE can be neglected in almost all spoofing cases, which leads to a guaranteed exclusion and the position estimated situation can be determined directly and not in probabilistic terms. When less than half of the valid incoming signals are spoofed and if at least 5 PRNs are not spoofed, the fault detection and exclusion process can detect and exclude faulty PRNs from the navigation solution. In this situation, the spoofed PRNs are excluded because they do not satisfy the residual criterion imposed by FDE and because the

largest coherent subset of PRNs is not spoofed. The position error increases due to the Dilution Of Precision (DOP) factor rise when excluding the faulty PRNs. The position error remains Gaussian-centered under the model, and it classified as position jamming. If fewer than 4 PRNs remain unspoofed, the FDE process detects an error but cannot exclude it, requiring a coherent subset of 5 PRNs to function. In this scenario, the position is inaccurately computed, and an error is raised by FDE to indicate the position's unusability.
When exactly half of the PRNs are spoofed, the FDE detects an error because the authentic and spoofed PRNs are not coherent with each other. This inconsistency cannot yet be resolved by removing some PRNs from the navigation solution, as no subset of PRNs predominates over the others so FDE cannot tell the unspoofed subset from the spoofed one. A position solution can still be calculated by WLSE, but an alarm is raised to indicate the position's unusability. The position error distribution in this situation is challenging to predict but can significantly deviate from the authentic position, even when the meaconer biases of the spoofed pseudoranges are small.
When more than half and at least 5 of the PRNs are spoofed, the fault detection and exclusion process can detect and exclude the authentic PRNs from the navigation solution. The authentic PRNs are excluded because they don't meet the residual criterion imposed by FDE and because the largest coherent subset of PRNs is spoofed. The estimated position shifts to the meaconer's position, and the estimated clock bias incorporates the additional propagation time delay between the meaconer's position and the aircraft's position. The position error is then Gaussian around the meaconer's position. If fewer than 4 PRNs are spoofed, the FDE process detects an error but cannot exclude it due to the requirement of a coherent subset of 5 PRNs. In this configuration, the position is inaccurately computed, and an error is raised by FDE to indicate the position's unusability.

VI. MEACONER IMPACT DURING AN AIRCRAFT APPROACH

This section presents the predicted impact of a meaconer on the ground during a LPV-200 approach. First, the approach under scrutiny is depicted along with the meaconer characteristics and the satellite geometry. Second, the relative parameters $\Delta\tau(t)$, $\Delta f(t)$ and $\Delta g(t)$ defined in section III.1 are computed for each visible PRN during the whole approach, based on the defined scenario of the approach. Third, the predicted impact of the meaconer on each visible PRN during the approach is catalogued after equations (19), (21) and (23) into the nominal, jamming or spoofing situation. Fourth and finally, this classification is used to predict the impact of the meaconer on the position domain during the approach, following the categorization previously presented in Fig. 4. In the next section (VII), these predictions of the meaconer impact on the different PRNs and on the position domain will be compared to highly-realistic simulation results.

1. Scenario definition

a) Flight profile and approach

The selected flight profile for conducting the tests involves an approach to Toulouse-Blagnac Airport, on runway 32L. The approach trajectory aligns with a heading of 323°, terminating at coordinates N43.624597°, E1.366270°, and an elevation of 497 feet above mean sea level (MSL) at the runway threshold. During this approach, the aircraft maintains a ground velocity of 131 knots. The glide path angle of the approach is set at 3° (equivalent to 5.2%), while the aircraft's pitch angle is established at 2°. Notably, this analysis excludes factors such as wind gusts, turbulence, and automatic pilot responses.
The lack of automatic pilot responses entails that the aircraft follows its desired trajectory throughout the approach, whatever the GNSS position estimations that are computed. Deriving automatic pilot responses is a challenging endeavor, particularly due to the lack of public disclosure by aircraft manufacturers regarding their specific autopilot models. However, it should be pointed that the expected position error distribution in the presence of a meaconer is centered (from previously described models) except in the spoofing situation. The meaconer should not induce additional automatic pilot responses when the position is not spoofed. When the position is spoofed, the defined spoofed position model estimates the meaconer position on the ground, whatever the aircraft actual position, and so whatever the automatic pilot responses. Therefore, the automatic pilot responses should not be a cause for concern for this paper, but may need further investigations to be proved marginal. The same reasoning can be done with respect to wind gusts and air turbulence.

b) Satellite geometry

The satellite positions are derived from SPS-almanacs featuring 24 GPS satellites. This paper centers on a specific satellite geometry depicted in Fig. 5. The satellite geometry holds significance when assessing the meaconer impact, as the satellite positions and velocities affect the classification of Section III. The geometry under scrutiny is chosen to reflect all the different situations catalogued in this paper, allowing easy generalization based on the model and observations established from the chosen geometry. With this geometry, 8 satellites are visible during the whole approach. The line in red in Fig. 5 highlights the apparent trajectory of the meaconer during the approach, from the aircraft point of view. The line is always outside of the skyplot because the meaconer is seen with a negative elevation angle.

c) Meaconer specifications

The meaconer under test is activated at a fixed position close to the aircraft's approach trajectory. It is positioned at a height of 10 m above the ground, 10 km before the runway threshold ($L = 10$ km in Fig. 1), and 150 m away from the aircraft trajectory on its right ($H = -150$ m in Fig. 1). The meaconer gain is set at either $G_{\mathrm{m}} = 112$ dB or $G_{\mathrm{m}} = 118$ dB, with an intrinsic delay of $\tau_{\mathrm{m}} = 0$ nanoseconds and an intrinsic Doppler shift of $f_{\mathrm{m}} = 0$ Hz. These parameters yield a pedagogic yet realistic scenario, wherein the meaconer's effects on the aircraft span the classification outlined in Section III. Both the emitting and receiving antennas of the meaconer adhere to the gain pattern of the aircraft's GNSS antenna, as illustrated in Fig. 6.

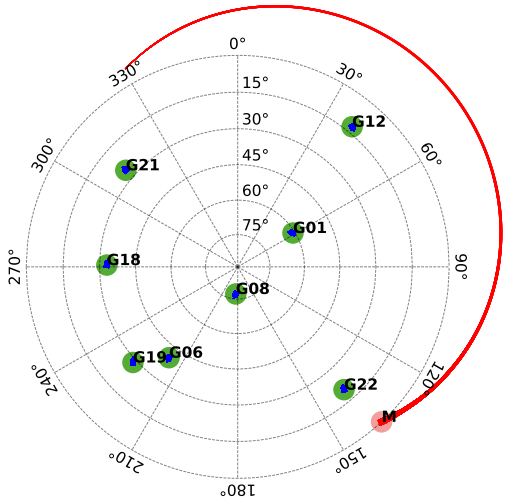


Figure 5: Skyplot of the satellite and meaconer positions during the approach, as seen by the aircraft.

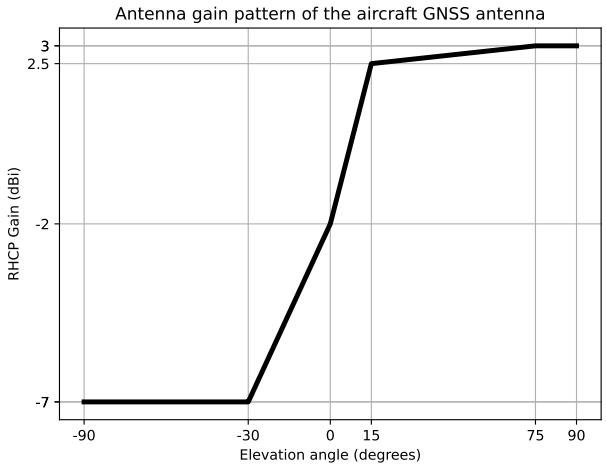


Figure 6: Antenna gain pattern of the aircraft GNSS antenna DO235C (2022).

d) Receiver specifications

The implementation of the receiver follows the architecture presented in Section IV and illustrated in Fig. 3. The specific parameters employed for the signal processing block are outlined in Table 1.

Table 1: Simulation signal processing block parameters.

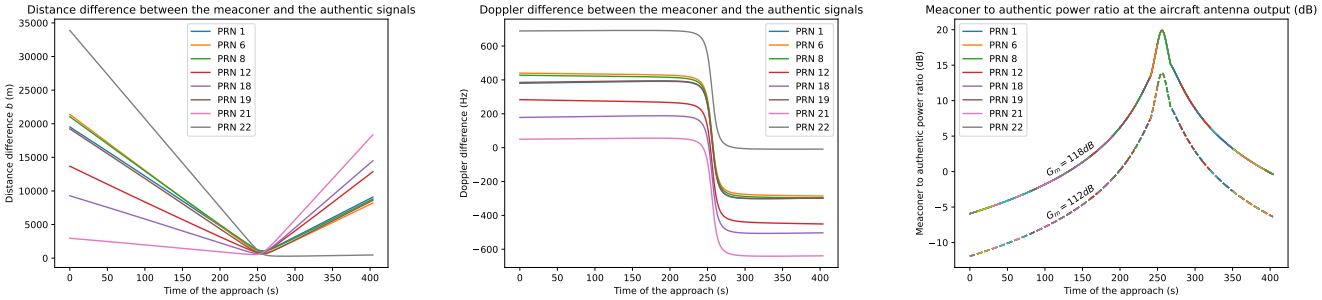
Acquisition DO235C (2022)		Coherent time = 1 ms, Incoherent number = 50 Test Pfa = 10^{-3}, Doppler limits = 1250 Hz (500 Hz for re-acquisition)
Tracking correlator		Integration Time (T_i) = 20 ms
DLL	**Discriminator**	NEMLP, Early-Late Spacing (c_τ) = $0.1T_c$
	Low-pass Filter	1st Order, Bandwidth (B_{DLL}) = 1 Hz
	Loss Indicator	Duration = 1 s, Type = Moment (C/N_0), Threshold $\gamma_\tau = 25$ dB·Hz
PLL	**Discriminator**	ATAN
	Low-pass Filter	3rd Order, Bandwidth (B_{PLL}) = 30 Hz
	Loss Indicator	Duration = 1 s, Type = NECT (Sec. IV.1 b)), Threshold = 0.85
C/N_0 **Estimate**	**Moment Estimator**	Estimation period = 1 s

2. Prediction of the relative parameters during the approach

Fig. 7 illustrates the relative parameters evolution $\Delta\tau(t)$, $\Delta f(t)$, and $\Delta g(t)$ defined in Section II.3, for both meaconer gains of 112 dB and 118 dB. The meaconer gain exclusively affects the relative power Δg, as evidenced by Eq. (7). The relative power reaches its maximum value at $t = 260$ s, coinciding with the aircraft flying over the meaconer.

In Fig. 7 as in the subsequent sections of the paper, several assumptions are taken into consideration. Both the meaconer and airplane receiver are assumed to be in open-sky environments. Then, environmental losses at the meaconer antenna are

neglected ($\Delta g_{\text{env}} = 0$), - no additional noise is generated by the amplification and emission materials in the meaconer device. Lastly, it is assumed that the received signal emitted by the j-th satellite arrives at both the antenna and meaconer antenna with the same angle. Consequently, under these assumptions, the GNSS signal and re-radiated noise are considered to have similar relative power levels, leading to $\Delta g \approx \Delta N$ and $(C/N_0)_{\text{s}} \approx (C/N_0)_{\text{a}}$.



(a) Relative delay $\Delta\tau$ (Eq. (4)). **(b)** Relative Doppler frequency Δf (Eq. (5)). **(c)** Relative power Δg (Eq. (7)).

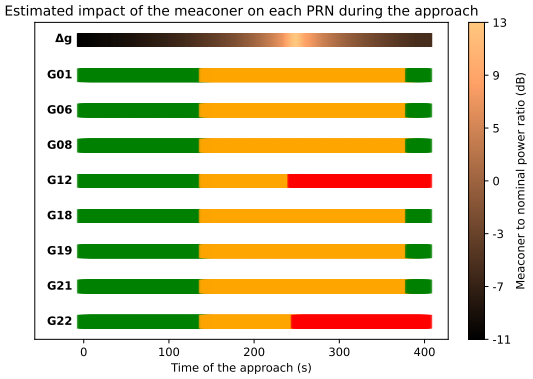
Figure 7: Meaconer signal characteristics with respect to the authentic signals during the approach.

The relative delays are expressed in meters after being multiplied by the speed of light. At the beginning of the approach, the largest delay as well as the largest Doppler difference are observed for PRN 22. Indeed, the meaconer is seen in front of the aircraft (heading $\approx 323°$) and the PRN 22 is seen behind the aircraft (heading $\approx 140°$). The relative delay incorporates then almost twice the distance between the aircraft and the meaconer, as the spoofed signal needs to reach the meaconer then to travel back to the aircraft. The relative Doppler is also high, because the aircraft is flying towards the meaconer (inducing a positive Doppler shift) and away from PRN 22 (inducing a negative Doppler shift). At the end of the approach, the lowest delays and Doppler differences are observed for PRN 22 because both the meaconer and the satellite are seen behind the aircraft. The meaconer is almost on the line-of-sight path so the spoofed signal stays close to the authentic one when passing through the meaconer. The small Doppler difference can be explained because the aircraft, the meaconer and PRN 22 are almost aligned, so the aircraft flies away from both the meaconer and PRN 22 with a similar radial velocity. Analogous explanations can be derived for the relative delays and Doppler of the other PRNs. Especially, the meaconer gain does not interfere in the computations of $\Delta\tau$ and Δf. All the different PRNs almost share the same power ratio profile, and this profile depends on the meaconer gain. Indeed, the meaconer and aircraft receiver antenna share the same gain pattern and propagation losses are almost equal at the aircraft and meaconer locations, so the satellite signals are received at the same power at the aircraft and at the meaconer antenna outputs. Moreover, all the re-broadcast signals of the meaconer are amplified with the same meaconer gain, travel the same distance to the aircraft and reach the aircraft antenna with the same angle of arrival. All in all, although the PRN signals arrive at the aircraft antenna with different powers, the power ratio between the authentic and the meaconer signals at the aircraft antenna output is almost the same.

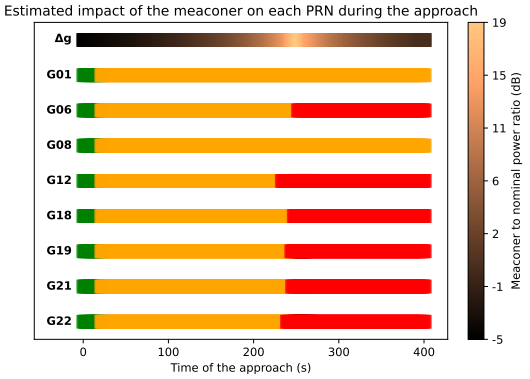
3. Prediction of the meaconer impact on each PRNs

The situations for each PRN during the approach can be predicted from the relative parameter values depicted in Fig. 7, from Eqs. (19), (21), and (23), and from the following acquisition procedure compliant with the civil aviation standards. If the code lock is lost (Eq. (38)) for a PRN, the receiver acquires the meaconer signal of that PRN only if $\Delta g > 1$ and Δf in smaller than a Doppler cell of the acquisition grid (ED259, 2019, REQ:025). If one of these two condition is not met, the receiver is assumed to acquire back the authentic signal.

The predicted pseudorange situations are illustrated in Fig. 8. In particular, losses of lock followed by re-acquisitions of the meaconer signals are predicted for PRN12 and 20 (with a 112 dB gain) as well as for PRN$06, 12, 18, 19, 21$, and 22 (with a 118 dB gain), occurring approximately around $t = 255$ s.



(a) With a meaconer gain of 112 dB.

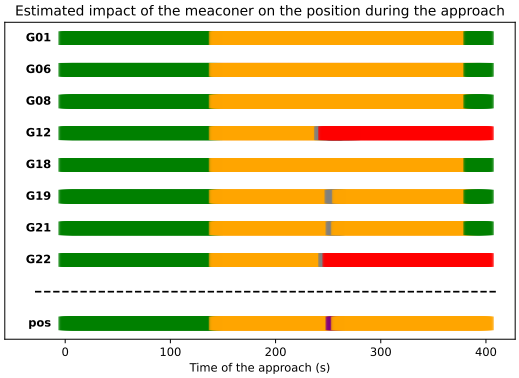


(b) With a meaconer gain of 118 dB.

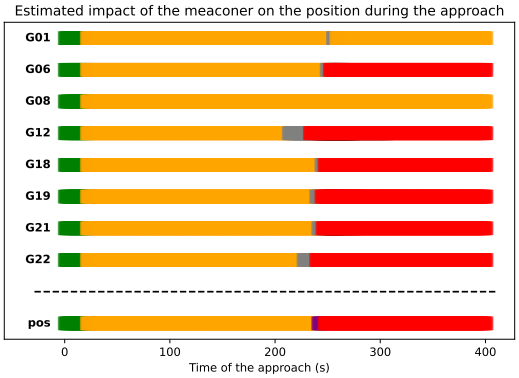
Figure 8: Predicted impact of the meaconer on each PRN throughout the approach. The green stands for nominal situations, orange for jamming, and red for spoofing.

4. Prediction of the meaconer impact on the position domain

From the pseudorange classification, the impact of the meaconer on the position can also be estimated at every epochs during the approach, using the diagram 4, and is detailed in Fig. 9. This figure takes into consideration the predicted impacts of the meaconer of Fig. 8 and adds on top of these impacts the regions (in grey) where the measurements are predicted not to pass the C/N_0 screening. With a meaconer gain of 112 dB, the position is mostly jammed by the meaconer, and FDE raises an alarm between 254s and 259s when the aircraft passes over the meaconer position. This alarm is raised because only 6 PRNs are usable between 254s and 259s (the 2 others, $G19$ and $G21$, do not pass the C/N_0 test) and 2 PRNs ($G12$ and $G22$) are spoofed among the 6 remaining. 4 non-spoofed PRNs are not enough for FDE to exclude the faulty ones, so an alarm is raised and the position is declared unavailable. As soon as $G19$ or $G21$ is available (at 260s and after), 7 or 8 PRNs are usable, and 2 PRNs ($G12$ and $G22$) are still spoofed. FDE can now detect and exclude the 2 faulty PRNs because the remaining ones form a coherent subset of at least 5 non-spoofed measurements. With a meaconer gain of 118 dB, a FDE alarm is raised between 241s and 247s. This alarm occurs because during these epochs, 6 PRNs are usable (the 2 others, $G19$ and $G21$, do not pass the C/N_0 test) and 2 PRNs ($G12$ and $G22$) are spoofed among the 6 remaining. 4 non-spoofed PRNs are not enough for FDE to exclude the faulty ones, so an alarm is raised and the position is declared unavailable. After 248s, 7 then 8 PRNs are usable, and 5 then 6 are spoofed. In this configuration, FDE checks for consistency between the measurements and the largest subset of PRNs that is found coherent is the subset of the 5 or 6 spoofed PRNs. A subset of 5 coherent PRNs is sufficient to exclude the other satellites from the navigation solution. $G01$, $G08$ (and $G06$ between 248s and 252s) are therefore removed from the position estimation, and the aircraft position is spoofed after 248 s.



(a) With a meaconer gain of 112 dB.



(b) With a meaconer gain of 118 dB.

Figure 9: Predicted impact of the meaconer on the position estimation throughout the approach. The green stands for nominal situations, orange for jamming, grey for refused pseudorange, purple for RAIM alarm, and red for spoofing.

VII. SIMULATIONS

A simulation software, incorporating the architecture detailed in Section IV, has been developed to investigate the influence of meaconing signals on aircraft GNSS receivers through comprehensive simulations. Each component of the software aligns with civil aviation standards and processing techniques. It is important to note that this simulation software does not integrate the mathematical predictions of the previous sections, but is only processing the GNSS signal that are generated at the aircraft antenna input. The results of the simulation are then independent from the previous predictions, and a good match between the two would confirm the mathematical assumptions and derivations of the prediction models of section VI. The following subsections provide a depiction of the subsequent simulation outcomes. The two approach scenarios used for the simulations are the ones described in VI.1.

1. Meaconer observed impact on the C/N_0

Fig. 10 illustrates the estimated C/N_0 during the simulated approach for the specific PRN18, considering meaconer gains of 112 dB and 118 dB. The anticipated behavior of PRN18 is presented in Fig. 8. For these approach the nominal $C/N_0 = 45$ dB.Hz.

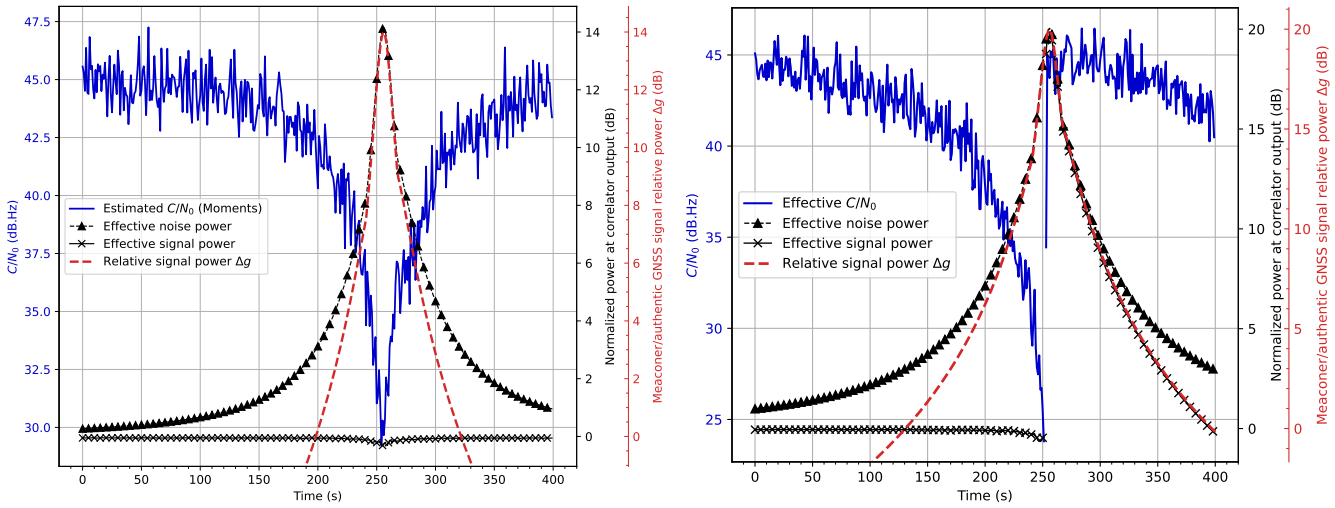
In Fig. 10, the Moments Method estimates of C/N_0 (shown in blue) are contrasted with the normalized effective signal power (represented by black crosses) and noise density (depicted as black triangles). The powers are normalized by the nominal signal power C_a and the nominal noise density N_0.

Within the initial phase of the approach ($t < 125$ s in Fig. 10a and $t < 5$ s in Fig. 10b), the signal power exhibits constancy, moreover the increasing of the noise density is lower than 1 dB (which is lower than the threshold $\gamma_n = 0.3$), signifying a nominal or undisturbed situation. In the subsequent time intervals for both figures (between 125 s $< t <$ 400 s and 5 s $< t <$ 260 s), while the effective signal power maintains a level of C_a, the noise density undergoes an augmentation by a factor of $(1 + \Delta N)$, leading to an equivalent reduction in C/N_0. This pattern arises from the jamming circumstance, as validated by Eq. (37) and predicted with the relative parameters in Fig. 8 ($\Delta\tau > 300$ m in Fig. 7a and $\Delta N > \gamma_n$). The effective noise attains its peak magnitude at $t = 260$ s, coinciding with the aircraft's passage over the meaconer. This event triggers a maximum degradation in C/N_0 of 14 dB and 20 dB, respectively.

At this point, the receiver behaves differently based on the gain setting. Firstly, with a gain of 112 dB, the reception is jammed but the receiver continues tracking the nominal peak. On the other hand, as seen in Fig. 10b, the effective C/N_0 drops below 25 dB, crossing the code lock threshold γ_τ, inducing a loss of lock of PRN18. This event prompts the activation of the re-acquisition procedure, which then captures the meaconer peak (since at $t = 260$ s, $\Delta g > 1$ as seen Fig. 7c).

In the spoofing situation (Fig. 10b, $t > 260$ s), the effective power shapes the meaconing power, i.e., $C_\mathrm{s} = \Delta g\, C_\mathrm{a}$ (represented by black crosses), while the effective noise density remains at $N_0(1 + \Delta N)$ (indicated by black triangles). The estimated C/N_0 aligns with the ratio of signal power to effective noise density as anticipated by Eq. (39). As an illustration, at $t = 350$ s, the ratio of signal power to effective noise density is -2.5 dB, which corresponds to the observed reduction in C/N_0 from $t = 260$ s.

To summarize, the examination of the observed C/N_0 and the corresponding situations for the specific PRN18 aligns with the forecast scenarios depicted in Fig. 8. This alignment provides an explanation for the significant disparity between the two predictions. This observation can also be confirmed for the other PRNs shown in Fig. 8, leading to similar outcomes.



(a) With a meaconer gain of 112 dB.

(b) With a meaconer gain of 118 dB.

Figure 10: Observed estimated C/N_0 for PRN18 during the approach for different gains.

2. Meaconer observed impact on the pseudoranges

Figs. 11 and 12 illustrate the DLL errors (in comparison to nominal tracking) for all PRNs during a single simulation approach. In the scenario with a meaconer gain of 118 dB, all PRNs except PRN1 and PRN8 have been subjected to spoofing by the meaconer throughout the approach. The DLL errors reflect the biases described by Eq. (44), which are also plotted in Fig. 7a. A closer examination in Fig. 12 of the non-spoofed DLL errors highlights the increased standard deviations caused by thermal noise during jamming situations. Fig. 13 is plotted for comparison purposes and represents the DLL errors during a approach without meaconing interference (nominal situation).

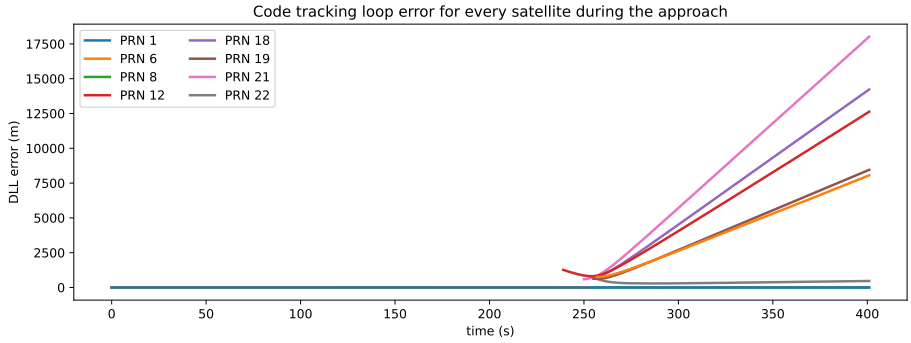


Figure 11: Observed DLL errors during one approach, with a meaconer gain of 118 dB.

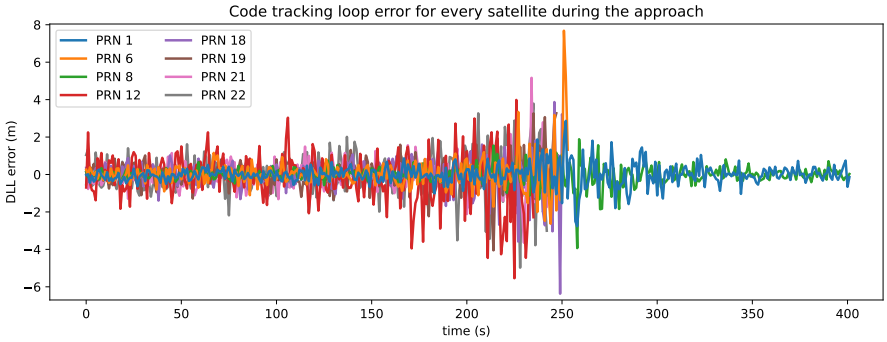


Figure 12: Zoom on the observed DLL errors during one approach, with a meaconer gain of 118 dB.

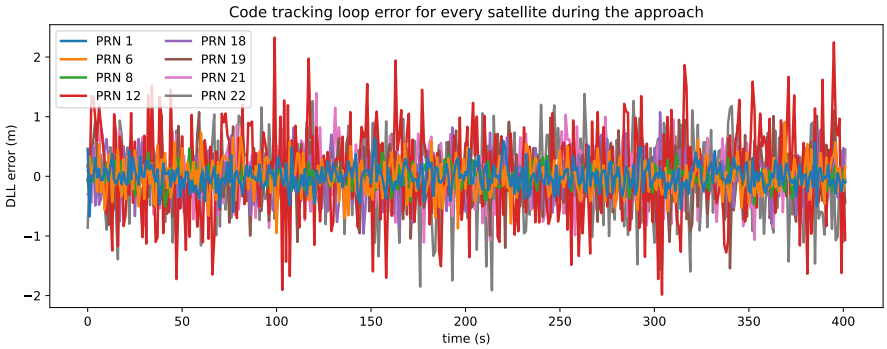
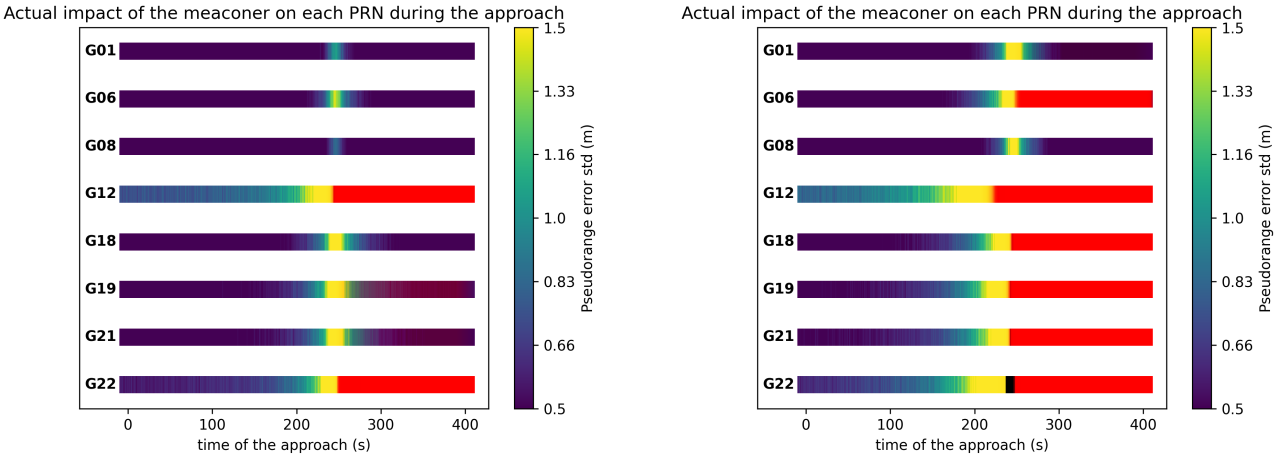


Figure 13: Observed DLL errors during one approach, without meaconing interference.

To quantitatively assess the impact of the meaconer on the thermal noise, Monte-Carlo simulations are conducted. The approach is executed 400 times, and for each PRN and epoch, the standard deviation of thermal noise is computed using values obtained from each run. The results are displayed in Fig. 14 for both scenarios. These results showcase the effects of meaconer jamming and spoofing during the approach. Notably, the prediction from geometrical considerations provides a good estimation of the actual meaconer impact. This alignment between prediction (Fig. 8) and observation (Fig. 14) is particularly striking in the spoofing situation, where the predicted affected PRNs are the ones getting spoofed in the simulations, and the instances of spoofing start closely match the observed data with $\pm 1s$.

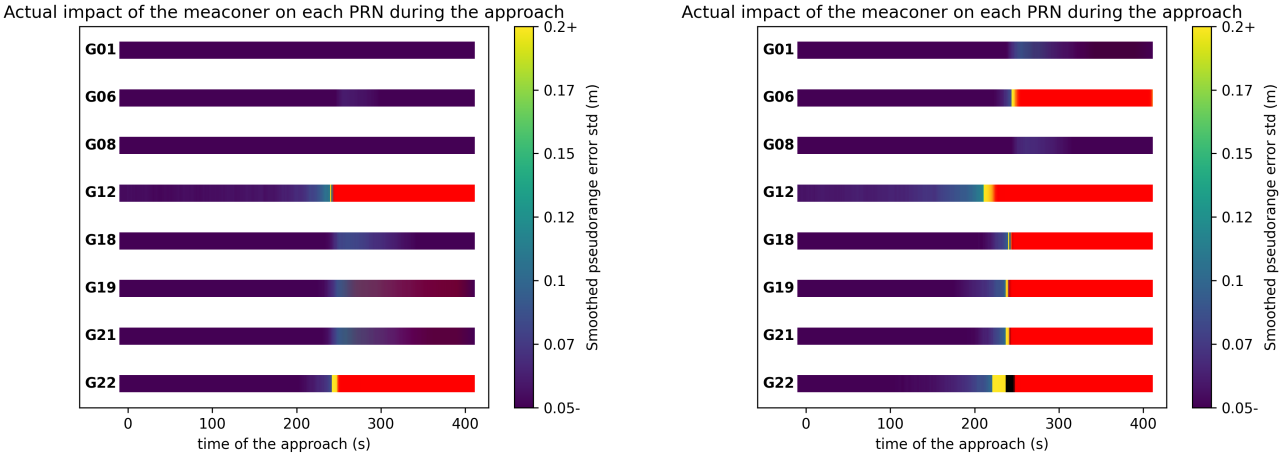


(a) With a meaconer gain of 112 dB.

(b) With a meaconer gain of 118 dB.

Figure 14: Thermal noise std observed during the approach for each PRN. The viridis color scale refers to the thermal noise std, red for spoofing, black when the signal is not tracked.

Before being used for positioning, the code pseudoranges are smoothed by the phase (27), reducing the thermal noise errors. The thermal noise std after carrier smoothing is represented in Fig. 15. The pseudorange errors are also delayed in Fig. 15 with respect to Fig. 14 for all the PRNs, due to the low-pass effect on the carrier smoothing filter. The PRNs that are not spoofed show an error still after the meaconer highest power reception (at about 260 s). The smoothed pseudoranges which thermal noise is depicted on Fig. 15 input the WLS positioning algorithm, the outputs of which are detailed in the following subsection.



(a) With a meaconer gain of 112 dB.

(b) With a meaconer gain of 118 dB.

Figure 15: Smoothed thermal noise std observed during the approach. The viridis color scale refers to the thermal noise std, and red for spoofing.

3. Meaconer observed impact on the position domain

The estimated position when exposed to a meaconer with a gain of 112 dB is depicted in Figs. 16 and 17.

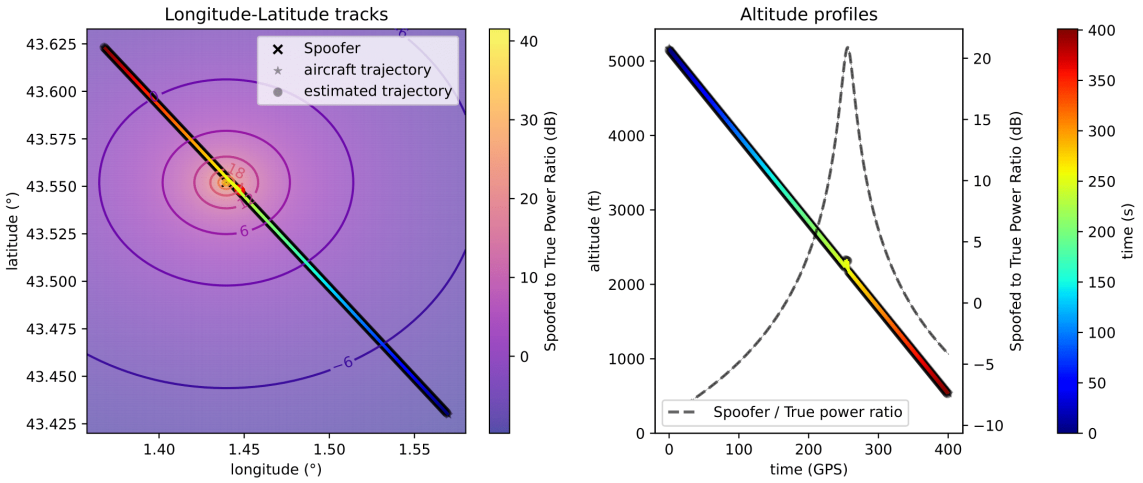


Figure 16: Desired and estimated positions during an approach with a meaconer gain of 112 dB.

Fig. 16 provides an overview of the desired and estimated positions of the aircraft during the approach. The figure encompasses both the longitude-latitude frame on the left and the altitude profile over time on the right. The color transition from blue to red corresponds to the passage of time during the approach. As the position errors between the desired and the estimated tracks are small, the two trajectories overlap on the plot and Fig. 17 is needed to visualize the position errors during the approach. The heatmap on the left of Fig. 16 illustrates the ratio of meaconer power to authentic power, considering an omnidirectional antenna. The projection of these heatmap values along the desired trajectory is shown as a dotted grey line on the right. This visualization effectively demonstrates that the meaconer's impact is mostly negligible, except during instances of significant power where it leads to loss of lock or loss of PRN availability in the aircraft receiver. A closer analysis of the position errors is facilitated with Fig. 17.

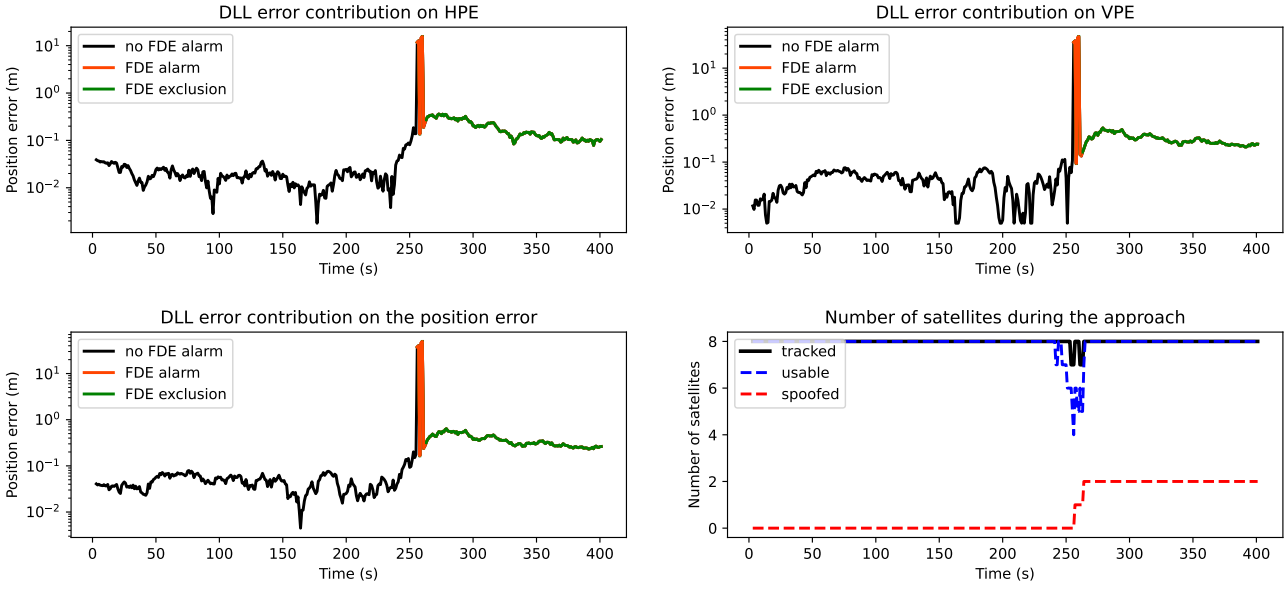


Figure 17: DLL error contributions on the horizontal (HPE), vertical (VPE) and total estimated position errors during an approach with a meaconer gain of 112 dB, along with the number of satellites (tracked, usable, and spoofed) observed during the approach.

In Fig. 17, the contribution of the DLL errors on the estimated position errors during the approach with a meaconer gain of

112 dB are plotted in plain line, along with their projections onto the horizontal plane (giving the Horizontal Position Error, or HPE) and vertical axis (giving the Vertical Position Error, or VPE). The plots also include color indications for Fault Detection and Exclusion (FDE) - orange for error detection and green for exclusion of faulty PRNs. The number of tracked, usable and spoofed satellites is plotted during the approach. The number of usable satellites refer to the number of tracked satellites that successfully pass the three measurement checks. Prior to 254 s, the position error remains minimal. Between 254 s and 259 s, an intolerable error arises because one then two PRN are spoofed, and FDE cannot exclude that faulty PRN due to the lack of a coherent subset of 5 usable pseudoranges. As the jamming effect subsides, more pseudoranges become usable for positioning. Starting from 260 s, FDE identifies a subset of at least 5 coherent pseudoranges and removes spoofed PRN12 and PRN22 from the navigation solution. The positioning error converges back to a centered distribution, indicating the absence of spoofing. The position error after 260 s is higher than during the first half of the approach, because FDE removes 2 PRNs from the navigation solution, increasing the DOP factor and thus the position error. Moreover, the jamming effect of the meaconer also increases the thermal noise of the measurements, inducing larger position errors. This observed behavior closely aligns with the prediction shown in Fig. 9a.

The estimated position when exposed to a meaconer of gain 118 dB is shown in Figs. 18 and 19. In this scenario, the DLL error contribution on the position is small and increases slowly between 0 s and 247 s, reflecting a nominal then jammed position situation. The position error increases due to the meaconer impact, increasing the thermal noise of the tracking loop outputs and lowering the C/N_0 of the measurement that reduces the number of tracked/usable satellites. Just before 250 s, one PRN is getting spoofed and FDE detects the spoofing. FDE can not exclude that faulty PRN from the navigation solution as it needs a minimum of six usable PRNs to exclude one. At about 255 s, the number of usable satellites drops below 4 and the position can not be estimated. After 260 s, 6 spoofed satellites are observed, and in the meantime the estimated position converges to the meaconer position on the ground. From there, over half of the PRNs are spoofed, and FDE selects the largest coherent subset of PRNs for positioning, which includes the spoofed PRNs, that converge at the meaconer's position. The shift to the meaconer position can be observed in the right plot of figure 18, where the altitude of the estimated track drops to the altitude of the meaconer (10 m above the ground) which is close to the altitude of the end of the approach (0 m above the ground at touchdown). The vertical error of 10 m between the actual trajectory and the estimated one at the end of the approach is clearly visible on Fig. 19 by looking at the VPE plot. Although not represented here, the receiver's clock offset estimate would also include the actual receiver clock offset and the additional time delay due to the distance between the meaconer and the aircraft. Once again, the observed positioning error matches the prediction in Fig. 9b, where the position was predicted to be nominal before 247s, to be faulty but with an alarm raised by FDE between 248s and 252s, and to be spoofed afterwards. A mismatch is however observed due to the acquisition procedure in the simulations that takes a few seconds and that is not considered in the prediction.

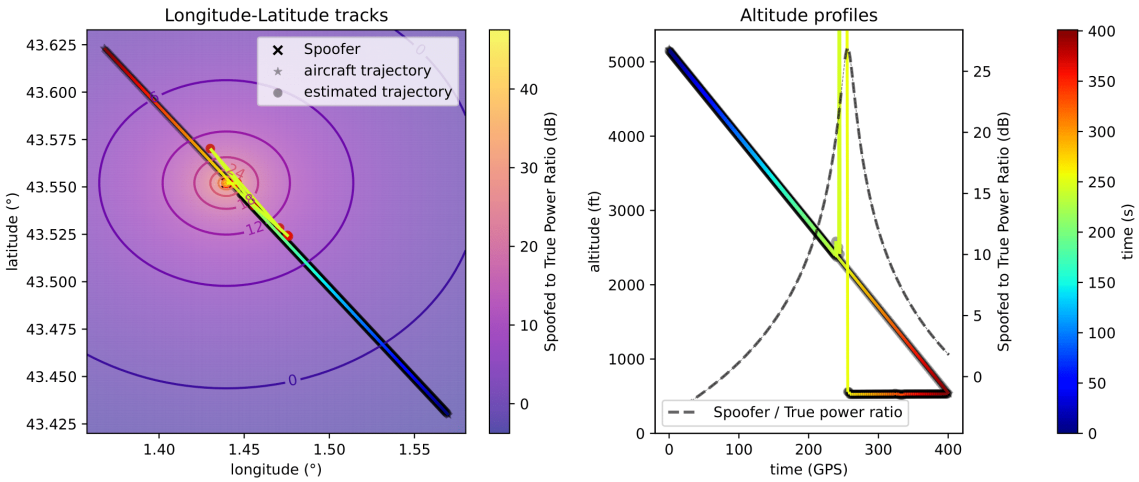


Figure 18: Desired and estimated positions during an approach with a meaconer gain of 118 dB.

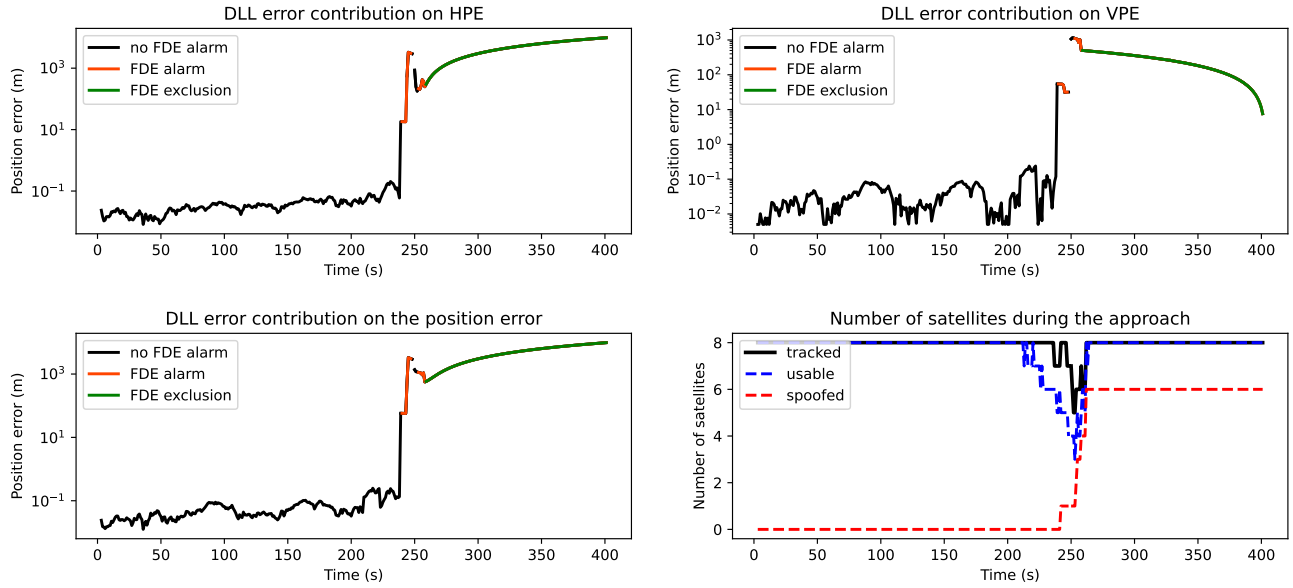


Figure 19: DLL error contributions on the horizontal (HPE), vertical (VPE) and total estimated position errors during an approach with a meaconer gain of 118 dB, along with the number of satellites (tracked, usable, and spoofed) observed during the approach.

VIII. CONCLUSION

This paper presented an investigation on the impact of meaconers on an aircraft GNSS receiver during an approach. The impact has been catalogued into four different categories - nominal, multipath, jamming and spoofing. These categories have been defined with respect to the different behaviours of the correlator output models of the aircraft GNSS receiver when exposed to the meaconer signals. Equivalently, these four situations have also been defined with respect to the geometry of the approach and the meaconer characteristics. The derivation of the mathematical models of the C/N_0 and pseudoranges have been designed based on this classification, and allows to predict the effect of the meaconer, with the knowledge of the meaconer position on the ground and its characteristics.

This paper also integrates a comprehensive simulation framework. Through extensive simulations, we observed that a meaconer poses substantial challenges to an aircraft GNSS receiver capability to estimate accurate and reliable positions. The effects of meaconer perturbations are most pronounced when the meaconer signal power exceeds a critical level at the aircraft's GNSS antenna output. Strong meaconer interferences induce degradation of the C/N_0 of the authentic GNSS signals, that might lead to loss of lock on the low C/N_0 satellites, and the receiver may reacquire the meaconer signal due to similarity with the authentic one. This study emphasizes the importance of robust algorithms and techniques to detect and exclude the meaconer signals as they can corrupt the navigation solution. The integrated fault detection and exclusion algorithms proved ineffective in detecting and excluding pseudoranges that were compromised by meaconing during high meaconer power attacks where more than half of the constellation is effectively spoofed.

By understanding the behavior of the receiver under different conditions, these findings contribute to the ongoing efforts to strengthen the security and reliability of global navigation satellite systems, ultimately ensuring the safety of aviation operations. Furthermore, they may be employed to aid regulation regarding the placement and operation of meaconers, or 'GNSS repeaters', in proximity to the aerodrome environment.

The precise mathematical distributions of the errors has not been yet analyzed. The effect of carrier smoothing on the pseudoranges has been observed but not quantified. Finally, the multipath situation is not under scrutiny and might need further research, as well as the integrity threat when exposed to a meaconer.

REFERENCES

Bamberg, T., Appel, M. M., and Meurer, M. (2018). Which GNSS Tracking Loop Configuration is Most Robust Against Spoofing? In *Proc. ION GNSS+ 2018*, pages 3587–3595, Miami, FL, USA.

Berz, G. (2018). GNSS Spoofing and Aviation: an Evolving Relationship. *Inside GNSS*, 25:54–59.

Betz, J. W. (2001). Effect of Partial-Band Interference on Receiver Estimation of C/N_0: Theory. In *Proc. ION ITM-21*, pages 817–828, Long Beach, CA, USA.

Coulon, M., Chabory, A., Garcia Peña, A., Vezinet, J., Macabiau, C., Estival, P., Ladoux, P., and Roturier, B. (2020). Characterization of Meaconing and its Impact on GNSS Receivers. In *Proc. ION GNSS+ 2020*, pages 3713–3737, St. Louis, MO, USA.

DO229E (2016). Minimum Operational Performance Standards for Global Positioning System/Satellite-Based Augmentation System Airborne Equipment - 2.5.10.3.1. Technical report.

DO235C (2022). Assessment of radio frequency interference relevant to the gnss l1 frequency band - 2.5.2.1. Technical report.

ED259 (2019). Minimum Operational Performance Standard for Duel-Frequency Multiconstellation Satellite-Based Augmentation System Airborne Equipment. Technical report, EUROCAE, Sant-Denis, France.

Garcia Peña, A. J., Macabiau, C., Novella, G., Julien, O., Mabilleau, M., and Durel, P. (2020). In-band RFI GNSS L5/E5a Mask Definition. In *Proc. ION GNSS+ 2020*, pages 188–205, St. Louis, MO, USA.

Geng, J., Jiang, E., Li, G., Xin, S., and Wei, N. (2019). An improved hatch filter algorithm towards sub-meter positioning using only android raw gnss measurements without external augmentation corrections. *Remote Sensing*, 11(14):1679.

Hewitson, S. and Wang, J. (2006). GNSS Receiver Autonomous Integrity Monitoring (RAIM) Performance Analysis. *GPS Solutions*, 10:155–170.

ICAO (2022). Annex 17 – Aviation Security to the Convention on International Civil Aviation. twelvth edition.

International Telecommunication Union (2001). The Protection of Safety Services from Unwanted Emissions. In *Recommendation ITU-R SM.1535-0*. International Telecommunication Union.

International Telecommunication Union (2016). *Radio Regulations: Articles*. ITU.

Kaplan, E. D. and Hegarty, C. (2017). *Understanding GPS/GNSS: Principles and Applications*. Artech house.

Parkinson, B. W. and Axelrad, P. (1988). Autonomous GPS Integrity Monitoring Using the Pseudorange Residual. *Navigation*, 35(2):255–274.

Pauluzzi, D. and Beaulieu, N. (2000). A Comparison of SNR Estimation Techniques for the AWGN Channel. *IEEE Trans. Commun.*, 48:1681 – 1691.

Peng, C., Li, H., and Lu, M. (2019). Research on the Responses of GNSS Tracking Loop to Intermediate Spoofing. In *Proc. ION GNSS+ 2019*, pages 943–952, Miami, FL, USA.

Spilker Jr., J. J., Axelrad, P., Parkinson, B. W., and Enge, P. (1996). *Global Positioning System: Theory and Applications, Volume I*, volume 164. AIAA.

Steindl, E., Dunkel, W., Hornbostel, A., Hättich, C., and Remi, P. (2013). The Impact of Interference Caused by GPS Repeaters on GNSS Receivers and Services. In *European Navigation Conference*.