Impact of onboard meaconers on aircraft GNSS receivers

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

Impact of onboard meaconers on aircraft GNSS receivers

Mathieu Hussong, Emile Ghizzo, Carl Milner, Axel Garcia-Pena, Julien Lesouple
Fédération ENAC ISAE-SUPAERO ONERA, Université de Toulouse, France.

BIOGRAPHIES

Mathieu HUSSONG is a third-year PhD student at ENAC, the French Civil Aviation University. He holds a master's degree in aeronautics from ENAC and a master's degree in aerospace systems specializing in navigation and telecommunications from ISAE SUPAERO in Toulouse. His PhD research focuses on aircraft GNSS spoofing characterization and impact.

Emile GHIZZO is a third-year PhD student at ENAC. He received a master's degree in aeronautics from ENAC in 2021 and a master's degree in aerospace systems specializing in navigation and telecommunications from ISAE SUPAERO in Toulouse. His PhD research focuses on GNSS signal processing and jamming and spoofing detection.

Axel GARCIA-PENA is a researcher/lecturer with the SIGNAV research axis of the TELECOM team of ENAC, Toulouse, France. He received his double engineer degree in 2006 in digital communications from SUPAERO and UPC, and his PhD in 2010 from the Department of Mathematics, Computer Science and Telecommunications of the INPT (Polytechnic National Institute of Toulouse), France.

ABSTRACT

With the escalating prevalence of radio-frequency interference, the vulnerability of Global Navigation Satellite System (GNSS) receivers to potential jamming or spoofing threats has become a critical concern. The proliferation of GNSS repeaters, commonly known as meaconers (electronic devices that intercept GNSS signals, amplify them, and subsequently rebroadcast them to GNSS receivers in sight) contributes to this threat landscape, by compromising the operating performance of the nearby GNSS receivers. This work investigates the impact of onboard meaconers on aircraft GNSS receivers, emphasizing their detrimental effects on the accuracy, availability, and integrity of the GNSS estimated positions. Through mathematical modeling and highly realistic simulations, the influence of meaconing on the GNSS observables (code, phase, smoothed pseudoranges, carrier-to-noise density ratio C/N_0 estimations), and on the main processing blocks of a standardized aircraft GNSS receiver (C/N_0 threshold, measurement quality monitoring, step detector, fault detection procedure and protection level checks) has been deeply characterized. The findings indicate that onboard meaconers can induce substantial degradations in the GNSS signal tracking, resulting in significant positioning errors and availability drops that compromise both the flight operations and safety. For specific meaconer characteristics, the meaconer could completely jeopardize the aircraft's receiver ability to compute a position, induce position errors up to 40 meters, or provoke continuous misleading position information and integrity hazards. The study highlights the importance for aviation bodies to consider the onboard meaconing threats. Additionally, the findings present valuable guidance for pilots and manufacturers in identifying and interpreting onboard meaconing interference, thereby strengthening the reliability of GNSS-based navigation systems in the aviation sector.

I. INTRODUCTION

The increasing occurrence of in-band radio-frequency interference may render GNSS receivers susceptible to jamming or spoofing threats, potentially compromising their performance. The proliferation of GNSS repeaters, commonly referred to as meaconers (electronic devices that intercept GNSS signals, amplify them, and subsequently rebroadcast them), contribute to this threat landscape. Coulon et al. (2020) illustrated the significant degradation of the accuracy and availability of GNSS receivers in their vicinity, and Garcia-Pena et al. (2020) pointed out the importance to consider radio-frequency interference in critical GNSS applications nowadays, as they could impair the performance of GNSS receivers.

Multiple studies focused on the general impact of meaconers interfering with GNSS signals. Dovis (2015) discussed the various types of GNSS interference, including meaconing, jamming, and spoofing, highlighting their potential to disrupt GNSS-dependent systems. The study revealed that meaconing could cause significant deviations in positional accuracy, leading to substantial errors in navigation and timing information. Dobryakova and Ochin (2014) explored the impact of meaconing on the integrity monitoring of GNSS receivers, emphasizing the potential meaconing threat, leading to hazardous yet detectable misleading information. In general, the literature relates that meaconing interference are ubiquitous yet concerning, as they could easily deteriorate the operations of the systems relying on GNSS.

Hussong et al. (2023) has proposed a classification of the meaconer impacts at the correlator output level, laying the mathematical groundwork of meaconing interference from results of Bamberg et al. (2018) and Peng et al. (2019). The effects of the meaconer can be categorized as nominal (where the meaconer impact on the tracking loops is negligible), spoofing (where the tracking loops are locked on meaconer signal), jamming (where the tracking loops are locked in the authentic signal, yet the meaconer degrades tracking performance by rebroadcasting additional noise, and potentially causing loss of lock), or multipath-like errors (where meaconer signals distort the nominal behavior of the GNSS receiver as if it were exposed to multipath). In all the situations except nominal, the presence of meaconers can adversely affect tracking loop performance, pseudorange estimation, and position determination under specific geometrical and power conditions.

Notably, Hussong et al. (2024c) demonstrated in the multipath situation, the Carrier-to-Noise Density Ratio (C/N_0) and Delay-Lock Loop (DLL) degradations are significant . In this scenario, both the meaconer and the useful GNSS signals simultaneously affect the tracking of the GNSS receiver. The C/N_0 degradations can exceed 20 dB, and the DLL outputs can be distorted with errors having deterministic mean values up to ± 15 meters, and standard deviations reaching 6 meters. When the meaconer is on the ground, the multipath situation has been proved to marginally affect the GNSS performance of an aircraft. Indeed, the multipath situation requires strict geometrical conditions to be observed, that are not met -or during limited time- in civil aviation. The unique configuration provoking a multipath situation for several seconds is when the meaconer is onboard the aircraft. With an onboard meaconer, GNSS performance may deteriorate beyond civil aviation requirements, compromising flight safety.

Moreover, the characterization of the meaconing impact on civil aviation GNSS receivers is particularly concerning. Civil aircrafts rely heavily on GNSS for navigation, approach, and landing procedures. According to Lohan et al. (2019), the intentional or unintentional deployment of meaconers onboard aircraft could lead to severe disruptions in navigation systems, potentially causing navigation errors that exceed the tolerances set by aviation standards. Such interference could not only degrade positional accuracy but also compromise the integrity of the navigation solutions, leading to increased risks during critical flight phases.

The need to study onboard meaconing threats rises as a major priority. Apart from the unknown yet potentially significant effects of onboard meaconers on aircraft receivers, Skorupski and Uchroński (2018) conducted a comprehensive analysis of the airport security screening systems, emphasizing the ease with which a meaconer could be brought onboard and activated by a non-expert. Their findings underscore the necessity for robust detection and mitigation strategies to safeguard against such threats. Activating a meaconer in an aircraft can be done by a layperson for unintended or malicious reasons. Additionally, aviation regulatory bodies mandate for the inclusion of meaconing scenarios in GNSS receiver testing and certification processes to ensure resilience against this form of interference (International Civil Aviation Organization, 2022, 1.7.5).

These concerns motivated the authors to deeply investigate the impact of onboard meaconing on aircraft GNSS receivers, addressing a gap in the literature. Understanding the degradations caused by onboard meaconers at the position level is crucial for several reasons. First, aviation standardization committees could incorporate the onboard meaconer threat into the spoofing test procedures and define specific standards to mitigate or raise awareness on this risk. Second, pilots could benefit from these results by identifying and correctly responding when aircraft GNSS receivers are corrupted by onboard meaconing interference. Third, manufacturers could use these findings to test and alleviate the impact of onboard meaconers in GNSS receivers.

The objective of this study is thus to characterize and highlight, through mathematical models and highly realistic simulations, the impact of meaconing on the GNSS accuracy, availability, and integrity of the navigation solution when the meaconer is onboard the aircraft. To achieve this goal, the paper characterizes the onboard meaconer's impacts on code pseudorange, phase pseudorange, and C/N_0 estimations. These models are then used to derive the behavior of the smoothed pseudoranges that are used for positioning. The smoothed pseudorange models, combined with standardized pseudorange tests and receiver processing techniques, are employed to theoretically quantify the availability, accuracy, and integrity of the estimated GNSS positions. Finally, simulations of onboard meaconing present and validate the meaconer impacts on the position estimations, in terms of position availability, accuracy, and integrity.

This paper is organized as follows. Section II describes the meaconer model and mathematically classifies the meaconer impacts at the correlator outputs. Section III derives the impact of the meaconer on the GNSS observables and on the position estimation, while illustrating the effects of the meaconing interference on the main processing blocks of a standardized civil aviation receiver. Section IV assesses the degradations on the GNSS availability, accuracy and integrity, from the previously derived mathematical models. Finally, section V completes the paper by validating the theoretical degradations through highly-realistic simulations.

II. MEACONER CHARACTERISTICS AND CLASSIFICATION OF ITS IMPACTS

This section describes the main characteristics of a meaconer and proposes a mathematical representation of the signals rebroadcast by the meaconer at the aircraft's GNSS antenna. The classification of its different impacts at the correlator output level is then presented, along with their characterization.

1. Meaconer description

A meaconer, also known as a GNSS repeater, is an electronic device designed to capture electromagnetic signals, to amplify them, and to rebroadcast them around a specific GNSS central frequency, as illustrated on Fig 1. The meaconer is characterized by its gain G_m, intrinsic delay τ_m, frequency offset f_m and phase offset θ_m. In this paper, the meaconer gain G_m is defined as the ratio between the signal power at the meaconer's receiving antenna input and the signal power at its emitting antenna output. The intrinsic delay τ_m represents the signal group delay between the meaconer receiving antenna input and its emitting antenna output. The frequency offset f_m and phase offset θ_m respectively denote the difference between the carrier frequency (resp. instantaneous phase) of the signal at the emitting antenna input, compared to its carrier frequency (resp. instantaneous phase) at the receiving antenna output.

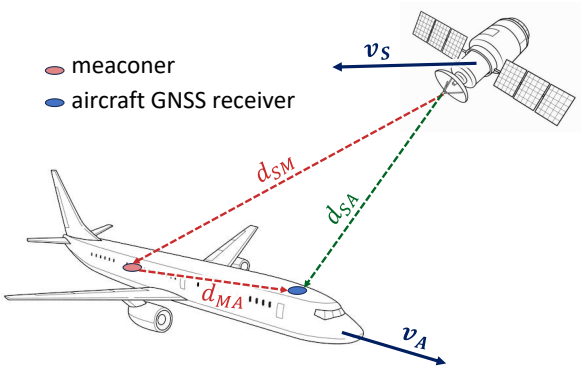

Figure 1: Sketch of the meaconer repercussion on nearby GNSS receivers, illustrated in the configuration of onboard meaconing.

The satellite signal is captured by the meaconer and the nearby GNSS receivers. The signal directly coming from the satellite to the aircraft GNSS receiver is called the authentic signal (in green in the figure), and d_{SA} represents the authentic signal propagation distance (the Euclidian distance between the satellite and the aircraft GNSS antenna phase centers). The satellite signal that detours through the meaconer is called the meaconer signal, and is depicted in red in the figure. d_{SM} represents the distance between the satellite and the meaconer antenna phase centers, and d_{MA} between the meaconer and the aircraft antenna phase centers. $d_{SM} + d_{MA}$ constitutes the propagated distance of the meaconer signal. The aircraft receives thus both authentic and meaconer signals, that interfere together inside its GNSS receiver.

2. Mathematical model of a meaconer

The meaconer signals have the same structure as the authentic signals received at the aircraft's GNSS antenna, but differ in power (due to the meaconer gain G_m, the different space and atmospheric losses, the antenna gains and the environments around the antennas), time delay (due to the meaconer intrinsic delay τ_m, the different signal propagation times and the aircraft's GNSS antenna hardware biases), carrier frequency and carrier phase offset (due to the relative motions between the satellite, the meaconer and the aircraft, and other propagation effects), as evidenced by Hussong et al. (2023) and Steindl et al. (2013). Moreover, the meaconer signal contains additional noise, received or generated by the meaconer active components. In this paper, the differences between the authentic and the meaconer signals are expressed and fully determined by five relative parameters of interest, defined as follows:

- The relative power, denoted as Δg, represents the ratio between the meaconer signal useful power and the authentic signal useful power at the aircraft's antenna output. The relative power can be linked to the distance between the aircraft's GNSS antenna and the meaconer, and to the meaconer gain with the formula from Hussong et al. (2024a) :

$$\Delta g = G_m + 20\log\left(\frac{\lambda}{4\pi d_{MA}}\right) + \Delta g_{\text{ant}} + \Delta g_{\text{env}} \qquad \text{in dB.} \tag{1}$$

  Where λ is the wavelength of the GPS L1 signal. Δg_{ant} accounts for the aircraft's antenna gain difference between the meaconer and the authentic signal. Δg_{env} account for the power difference between the meaconer signal and the authentic signal induced by the environment (for instance, to account for the power loss of the meaconer signal due to the propagation through the fuselage or the window of the aircraft).

- The relative noise power spectrum density, denoted as ΔN, represents the ratio between the thermal noise power spectrum density (PSD) at the correlator input that would have been observed without meaconing interference, and the thermal noise PSD that would have been observed if only receiving the meaconer signal. Mathematically, ΔN has been derived in Hussong et al. (2024a) as

$$\Delta N = G_m + NF_m + 20\log\left(\frac{\lambda}{4\pi d_{MA}}\right) + \Delta g_{\text{ant}} + \Delta g_{\text{env}} = \Delta g + NF_m \qquad \text{in dB.} \tag{2}$$

  Where NF_m represents the noise factor of the meaconer.

- The relative delay $\Delta\tau$ represents the difference between the propagation time of the meaconer signal and the propagation time of the authentic signal at the aircraft's antenna output. The relative delay has been computed in Hussong et al. (2023) as

$$\Delta\tau = \frac{d_{SM} + d_{MA} - d_{SA}}{c} + \tau_m + \Delta\tau_{\text{ant}}. \tag{3}$$

  Where c is the speed of light, and $\Delta\tau_{\text{ant}}$ accounts for the antenna group delay difference between the authentic and meaconer signal delays at the aircraft's receiver antenna output.

- The relative frequency Δf represents the difference between the received carrier frequency of the meaconer signal and the received carrier frequency of the authentic signal at the aircraft's antenna output. The relative frequency has been derived in Hussong et al. (2024c) as

$$\Delta f = f_m + \frac{\left(\mathbf{v}_S - \mathbf{v}_M\right)^T \cdot \mathbf{u}_{SM} + \left(\mathbf{v}_M - \mathbf{v}_A\right)^T \cdot \mathbf{u}_{MA}}{\lambda} - \frac{\left(\mathbf{v}_S - \mathbf{v}_A\right)^T \cdot \mathbf{u}_{SA}}{\lambda}. \tag{4}$$

  Where $\mathbf{v}$ represents the velocity vectors of the aircraft (A), the satellite (S) and the meaconer (M), and $\mathbf{u}$ denotes the unit direction vectors.

- The relative phase $\Delta\theta$ represents the difference between the received instantaneous phase of the meaconer signal and the received instantaneous phase of the authentic signal at the aircraft's antenna output. The relative phase can be derived from the other relative parameters as

$$\Delta\theta = \theta_m + \frac{2\pi c\Delta\tau}{\lambda} + \theta_{0,\tau} + \Delta\theta_{\text{ant}} \mod [2\pi] = \theta_m + 2\pi\Delta f\, t + \theta_{0,f} + \Delta\theta_{\text{ant}} \mod [2\pi]. \tag{5}$$

  Where $\theta_{0,\tau}$ and $\theta_{0,f}$ are constant initial phases, and $\Delta\theta_{\text{ant}}$ accounts for the phase difference induced by the receiver antenna between the meaconer and the authentic signals.

3. Classification of the meaconer impacts at the correlator output

For each authentic GNSS signal reaching the aircraft's GNSS antenna, the impact of the meaconer at the correlator output can be cataloged in one of the four situations introduced by Hussong et al. (2023). These four distinct situations are illustrated in Fig. 2 and briefly detailed below.

- *Nominal situation* : the receiver is synchronized with the nominal signal parameters, without significant distortion induced by the meaconer. By arbitrarily defining the nominal situation as when the code tracking standard deviation increase is limited to 10%, the nominal situation is observed when $\Delta N \leq -6.8$ dB and $\Delta\tau \geq T_{\text{max}} = T_c(1 + c_\tau/2)$, where T_c is the chip duration and c_τ is the chip spacing of the early and late correlators, as demonstrated by Hussong et al. (2024a). In the nominal situation, the meaconing interference can be neglected and the pseudorange models of the literature without meaconing interference can be used to derive the GNSS performance.

- *Jamming situation* : the power of the meaconer signal is not longer negligible ($\Delta N > -6.8$ dB), but the receiver is still synchronized with the nominal signal parameters, and the meaconing peak is significantly distant in terms of delay ($\Delta\tau > T_{\text{max}} = T_c(1 + c_s\tau/2)$) not to affect the values of the correlators. The impact of the meaconer on the correlator outputs is thus only dictated by the rebroadcast noise of the meaconer signal. This additional noise increases the standard deviation of the tracking loops estimation errors, resulting in larger errors in the code and phase pseudoranges. The rebroadcast noise also reduces the effective C/N_0 of the tracked signal, potentially causing losses of lock.

- *Spoofing situation* : the receiver is synchronized with the meaconing signal parameters, and the nominal peak is significantly distant in terms of delay ($\Delta\tau > T_{\text{max}}$) not to distort the values of the correlators. Only the increase of the noise PSD induced by the authentic signal can affect the tracking of the meaconer signal. This situation is analogous to the jamming situation, except that the authentic and the meaconer roles have swapped.

- *Multipath situation* : the nominal and meaconing peaks are sufficiently close to each other in terms of delay ($\Delta\tau \leq T_{\max}$) to both affect the synchronization process. The meaconer signal is comparable to a classical GNSS multipath reflection (hence the name of the situation), except that the meaconer signal power can be arbitrarily larger than the authentic signal power. This situation is often observed when the meaconer is located close to the GNSS receiver, as the extra propagation time of the signal detouring through the meaconer is reduced. With a meaconer onboard the aircraft, the multipath situation is likely to be observed.

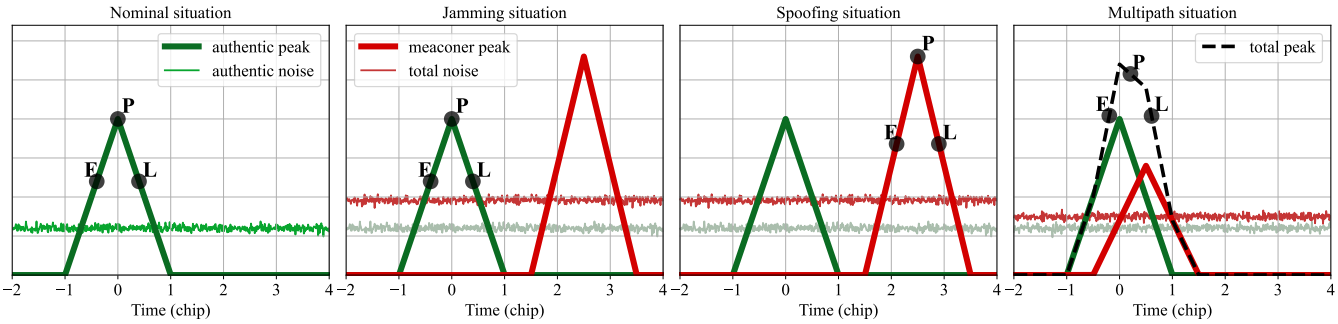

Figure 2: Classification of the situations at the correlator output. **E**, **P**, and **L** respectively represent the early, prompt, and late correlators.

III. MEACONING IMPACTS ON THE GNSS OBSERVABLES AND ON THE POSITION

This section describes the impacts of an onboard meaconer on the estimated position estimation. The impact is obtained by modeling the effects of the meaconing interference on the different GNSS observables as well as on the main measurement processing blocks of a standardized civil aviation GNSS receiver. At the end of this section (in III.6), an example of the meaconing effects is provided to illustrate the equations of each subsection, for a better understanding of the GNSS degradations under onboard meaconing.

1. Models of the correlator outputs and the tracking loops

GNSS implements direct-sequence spread spectrum (DS-SS). The received signal is correlated with a local replica controlled by the code and carrier Numerically Controlled Oscillators (NCOs) over the integration time T_{i}. Typically, GNSS receivers encompass at least three correlators - the early (Λ_{E}), prompt (Λ_{P}), and late (Λ_{L}) correlators, where the local replicas are respectively shifted in code by $-c_\tau/2$, 0, and $c_\tau/2$ (c_τ is the chip spacing). The chip spacing is set to $c_\tau = cT_c/10 \approx 30$ meters in this paper, accordingly to the nominal value used by standardized aircraft GNSS receivers. The correlator output expressions in the presence of meaconing interference have been derived as a function of the tracking errors $\boldsymbol{\varepsilon}_\eta = [\varepsilon_\tau, \varepsilon_\theta, \varepsilon_f]^\intercal$ and relative parameters $\Delta\boldsymbol{\nu} = [\Delta g, \Delta N, \Delta\tau, \Delta f, \Delta\theta]^T$ in Hussong et al. (2023). The tracking errors $\boldsymbol{\varepsilon}_\eta$ comprise the differences in code, phase, and frequency between the authentic signal code, phase and frequency, and the estimated ones obtained with the tracking loops. The early, late, and prompt correlator outputs at epoch k are expressed as linear combinations

$$\Lambda(\boldsymbol{\varepsilon}_\eta, \Delta\boldsymbol{\nu}) = \Lambda_{\mathrm{a}}(\boldsymbol{\varepsilon}_\eta) + \Lambda_{\mathrm{s}}(\boldsymbol{\varepsilon}_\eta, \Delta\boldsymbol{\nu}) + \Lambda_n \tag{6}$$

where Λ_{a} and Λ_{s} are respectively the nominal and spoofing contributions, expressed as

$$\Lambda_{\mathrm{a}}(\boldsymbol{\varepsilon}_\eta) = \sqrt{C_{\mathrm{a}}}\, d_k\, \zeta_\tau(\varepsilon_\tau)\, \zeta_f(\varepsilon_f)\, e^{j\varepsilon_\theta} \quad \text{and} \quad \Lambda_{\mathrm{s}}(\boldsymbol{\varepsilon}_\eta, \Delta\boldsymbol{\nu}) = \sqrt{\Delta g\, C_{\mathrm{a}}}\, d_k\, \zeta_\tau(\varepsilon_\tau + \Delta\tau)\, \zeta_f(\varepsilon_f + \Delta f)\, e^{j(\varepsilon_\theta + \Delta\theta)}. \tag{7}$$

Here, ζ_τ and ζ_f are the code and frequency synchronization mismatch functions defined in (Ghizzo et al., 2024b, Eq. (7)). C_{a} is the nominal received signal power, and d_k is the navigation message bit (considered constant over the integration time). The noise contribution, Λ_n, can be defined as Gaussian noise with power P_n, expressed in Ghizzo et al. (2024b) by

$$P_n = \frac{N_0}{T_{\mathrm{i}}}(1 + \Delta N)\, \zeta_\tau(0). \tag{8}$$

2. Model of the tracking loop distortions

The dynamic behavior of the tracking loops has been modeled in Ghizzo et al. (2024a) as a non-linear system of two differential equations. This paper focuses on the system's dynamic value at lock (i.e., where the loop has successfully established and maintains synchronization with the incoming signal dynamics). The tracking errors at lock have been shown to be equivalent to the system's stable equilibria (SE) expressed as (without stress error)

$$D_\phi\left(\boldsymbol{\varepsilon}_\eta, \Delta\boldsymbol{\nu}\right) = 0, \quad \frac{\partial D_\phi\left(\boldsymbol{\varepsilon}_\eta, \Delta\boldsymbol{\nu}\right)}{\partial \varepsilon_\phi} > 0 \;\; \forall \phi \in \{\tau, \theta\} \quad ; \quad \chi_\theta\left(\boldsymbol{\varepsilon}_\eta, \Delta\boldsymbol{\nu}\right) \quad = 0, \frac{\partial \chi_\theta\left(\boldsymbol{\varepsilon}_\eta, \Delta\boldsymbol{\nu}\right)}{\partial \varepsilon_f} \quad > 0. \tag{9}$$

D_ϕ is the code and phase discriminator outputs and χ_θ the phase discriminator difference, expressed as

$$D_\tau\left(\boldsymbol{\varepsilon}_\eta, \Delta\boldsymbol{\nu}\right) = \tfrac{C_a}{2P_d}\left(\zeta_f(\varepsilon_f)^2\, Z_0(\varepsilon_\tau) + \Delta g\, \zeta_f(\varepsilon_f + \Delta f)^2\, Z_0(\varepsilon_\tau + \Delta\tau) + 2\sqrt{\Delta g}\cos(\Delta\theta)\, \zeta_f(\varepsilon_f)\, \zeta_f(\varepsilon_f + \Delta f)\, Z_{\Delta\tau}(\varepsilon_\tau)\right) \tag{10}$$

$$D_\theta\left(\boldsymbol{\varepsilon}_\eta, \Delta\boldsymbol{\nu}\right) = \varepsilon_\theta + \frac{\Delta\theta}{2} - \operatorname{atan}\left(\gamma_\Delta\left(\varepsilon_\tau, \varepsilon_f\right)\tan\left(\frac{\Delta\theta}{2}\right)\right) - p\pi \tag{11}$$

$$\chi_\theta(\boldsymbol{\varepsilon}_\eta, \Delta\boldsymbol{\nu}) = \varepsilon_f + \Delta f - \frac{1}{2\pi T_{\mathrm{i}}}\left[\operatorname{atan}\left(\gamma_\Delta(\varepsilon_\tau, \varepsilon_f)\tan\left(\frac{\Delta\theta}{2}\right)\right) - \operatorname{atan}\left(\gamma_\Delta(\varepsilon_\tau, \varepsilon_f)\tan\left(\pi\Delta f T_{\mathrm{i}} + \frac{\Delta\theta}{2}\right)\right) - \pi p'\right] \tag{12}$$

The integers p and p' represent the phase and frequency ambiguity respectively and

$$Z_{\tau'}(\tau) \triangleq \zeta_\tau\left(\tau + \frac{c_\tau}{2}\right)\zeta_\tau\left(\tau + \tau' + \frac{c_\tau}{2}\right) - \zeta_\tau\left(\tau - \frac{c_\tau}{2}\right)\zeta_\tau\left(\tau + \tau' - \frac{c_\tau}{2}\right) \tag{13}$$

$$\gamma_\Delta(\varepsilon_\tau, \varepsilon_f) \triangleq \frac{\zeta_\tau(\varepsilon_\tau)\,\zeta_f(\varepsilon_f) - \sqrt{\Delta g}\,\zeta_\tau(\varepsilon_\tau + \Delta\tau)\,\zeta_f(\varepsilon_f + \Delta f)}{\zeta_\tau(\varepsilon_\tau)\,\zeta_f(\varepsilon_f) + \sqrt{\Delta g}\,\zeta_\tau(\varepsilon_\tau + \Delta\tau)\,\zeta_f(\varepsilon_f + \Delta f)} \tag{14}$$

The code and phase tracking errors at lock $\boldsymbol{\varepsilon}_\eta$ can be found solving (9). The solution of (9) is given for two examples of onboard meaconing in Fig. 4 (section III.6), for a better understanding of the meaconer impact.

The code and phase SE can be respectively assimilated to the code and phase tracking loop outputs under onboard meaconing interference. Indeed, the low dynamic between the meaconer and the aircraft's antenna allows the tracking loops of the aircraft's receiver to converge to their SE. In this paper, the SE and the tracking loop outputs are considered equal and the two notions can be swapped. The low dynamic under onboard meaconing is exposed in Appendix VII.3 and the equivalence between SE and tracking loop outputs with such dynamics is demonstrated in Ghizzo et al. (2024a).

3. Impact of the tracking loops distortions on the pseudoranges

a) Code and phase pseudorange models

Using the models of Kaplan and Hegarty (2017), the estimated code $\hat{\rho}$ and phase $\hat{\phi}$ pseudorange models can be represented as

$$\hat{\rho}_i[\kappa] = \rho_i[\kappa] + \epsilon_i[\kappa] \tag{15}$$

$$\hat{\phi}_i[\kappa] = \phi_i[\kappa] + \epsilon_{\phi,i}[\kappa]. \tag{16}$$

where κ denotes the epoch at which the measurements are generated, the subscript i refers to the PRN number, ρ and ϕ respectively represent the code and phase ideal pseudoranges, that are corrupted by the code ϵ and phase ϵ_ϕ estimation errors. The code and phase ideal pseudoranges are defined in Hussong et al. (2024b) as:

$$\rho_i[\kappa] = d_{SA,i}[\kappa] + c\,\delta t_r[\kappa] - c\,\delta t_i[\kappa] + T_i[\kappa] + I_i[\kappa] \tag{17}$$

$$\phi_i\kappa] = d_{SA,i}[\kappa] + c\,\delta t_r[\kappa] - c\,\delta t_i[\kappa] + T_i[\kappa] - I_i[\kappa]. \tag{18}$$

δt is the satellite clock offset, δt_r is the receiver clock offset, T is the tropospheric delay, and I is the ionospheric delay. The code and phase estimation errors can be modeled as

$$\epsilon_i[\kappa] = -\varepsilon_{\tau,i}[\kappa] + M_i[\kappa] + n_i[\kappa] + \nu_i[\kappa] \tag{19}$$

$$\epsilon_{\phi,i}[\kappa] = -\varepsilon_{\theta,i}[\kappa] + \lambda N_i[\kappa] + m_i[\kappa] + n_{\phi,i}[\kappa] + \nu_{\phi,i}[\kappa]. \tag{20}$$

Where ε_τ and ε_θ are the DLL and PLL SE given by Eq. 9. M (resp. m) is the code (resp. phase) classical multipath tracking loop estimation error, N is the carrier phase integer ambiguity term, n (resp. n_ϕ) represents the code (resp. phase) thermal noise tracking loop estimation errors. Finally, ν (resp. ν_ϕ) corresponds to the DLL (resp. PLL) transitory error of the tracking estimation due to the signal dynamic. The antenna code and phase biases are omitted in this study, as well as the tracking loop estimation errors due to the oscillator phase noise and vibrations.

b) Smoothed pseudorange model

The code estimated pseudoranges, while unambiguous, are characterized by high measurement noise. Conversely, the estimated phase pseudoranges exhibit lower noise levels but are inherently ambiguous. In civil aviation, a composite measurement known as the smoothed pseudorange is derived by integrating both code and phase pseudoranges, resulting in a pseudorange that is both unambiguous and has reduced noise compared to the code measurements alone. Mathematically, the smoothed pseudorange $\tilde{\rho}$ is obtained by smoothing the code pseudoranges with phase information, as follows:

$$\tilde{\rho}_i[\kappa] = \begin{cases} \frac{1}{\Gamma}\hat{\rho}_i[\kappa] + \frac{\Gamma-1}{\Gamma}\left(\tilde{\rho}_i[\kappa-1] + \hat{\phi}_i[\kappa] - \hat{\phi}_i[\kappa-1]\right) & \text{if available} \\ \hat{\rho}_i[\kappa] & \text{otherwise.} \end{cases} \tag{21}$$

The diacritic $\tilde{}$ refers to a carrier smoothed value. The smoothed pseudorange $\tilde{\rho}_i[\kappa]$ for PRN i at epoch κ is calculated using the estimated code pseudorange $\hat{\rho}_i$ at epoch κ and the estimated phase measurements $\hat{\phi}_i$ at both the previous $(\kappa-1)$ and current (κ) epochs. To comply with civil aviation standards (ED259 (2019)), $\Gamma = 100\, f_s$, where f_s is the sampling frequency (in Hz) of the pseudorange generation, achieving a smoothing effect with an exponential decay of characteristic time 100 seconds.

The smoothed pseudorange model has been derived in Hussong et al. (2024b) by merging Eqs. (15) and (16) into (21). The pseudorange after carrier smoothing is modeled as

$$\tilde{\rho}_i[\kappa] = d_{SA,i}[\kappa] - c\delta t_i[\kappa] + c\delta t_r[\kappa] + T_i[\kappa] + \tilde{I}_i[\kappa] + \tilde{M}_i[\kappa] + \tilde{\epsilon}_i[\kappa]. \tag{22}$$

$$\tilde{\epsilon}_i[\kappa] = \tilde{\varepsilon}_{\text{smo},i}[\kappa] + \tilde{n}_i[\kappa] \tag{23}$$

Where $\tilde{I}$, $\tilde{M}$ and $\tilde{\epsilon}$ are respectively the smoothed ionospheric error, the smoothed multipath error, and the smoothed tracking loop estimation error. The smoothed tracking loop estimation error can be decomposed into a deterministic part $\tilde{\varepsilon}_{\text{smo}}$ that represents the results of the DLL and PLL SE (ε_τ and ε_θ) when passed through the carrier smoothing filter (Eq. 21), and a random part $\tilde{n}$ that corresponds to the remaining error terms of Eqs. (19) and (20) when passed through the carrier smoothing filter. After applying Satellite-Based Augmentation System (SBAS) corrections, DO229E (2016) provides the mathematical model of the smoothed pseudorange error distributions as

$$\tilde{\rho}_i[\kappa] = d_{SA,i}[\kappa] + \tilde{\epsilon}_i[\kappa] + \tilde{\omega}_i[\kappa] \qquad \text{with} \qquad \tilde{\omega}_i[\kappa] \sim \mathcal{N}\left(0; \sigma_i^2\right). \tag{24}$$

The exact distribution of $\tilde{n}$ under meaconing interference is given in Hussong et al. (2024b), while σ_i represents the standard deviation of the residual error for post-SBAS correction for non-failed GPS satellites. This residual error is not modified by the meaconing interference, as it models the errors of the atmospheric and multipath terms, as well as the satellite health and the SBAS error mitigation quality. σ_i is computed using (DO229E, 2016, Appendices A,J) as

$$\sigma_i^2 = \sigma_{i,\text{flt}}^2 + \sigma_{i,\text{IURE}}^2 + \sigma_{i,\text{air}}^2 + \sigma_{i,\text{tropo}}^2$$

$$\sigma_{i,\text{flt}} = 0.562 \text{ m} \qquad \sigma_{i,\text{IURE}}^2 = 0.432^2 \left[1 - \left(\frac{R_E \cos(\psi_i)}{R_E + h_I}\right)^2\right]^{-1} \text{ m}^2 \tag{25}$$

$$\sigma_{i,\text{air}}^2 = 0.36^2 + (0.13 + 0.53e^{-\psi_i/10^\circ})^2 \text{ m}^2 \qquad \sigma_{i,\text{tropo}} = \frac{0.12012}{\sqrt{0.002001 + \sin^2(\psi_i)}} \text{ m}.$$

Where ψ_i is the satellite elevation, R_E is the Earth semi-major axis from WGS84, and $h_I = 350$ km is the characteristic height of the ionosphere.

4. Impact of the tracking loops distortions on the C/N_0

The expected value of the C/N_0 is modified by meaconing interference and depends on the correlator output situation of Fig. 2.

- *Jamming situation* : The effective C/N_0 is computed by Hussong et al. (2023) as follows:

$$\left(\frac{C}{N_0}\right)_{\text{eff, J}} = \frac{1}{(1+\Delta N)}\left(\frac{C}{N_0}\right)_{\text{a}} \tag{26}$$

  where $(C/N_0)_{\text{a}}$ denotes the nominal C/N_0 (i.e., the C/N_0 of the authentic signal without meaconing interference). In the jamming situation, the estimated C/N_0 is therefore reduced because of the meaconing interference.

- *Spoofing situation* : The effective C/N_0 is also given by Hussong et al. (2023) as

$$\left(\frac{C}{N_0}\right)_{\text{eff, S}} = \frac{\Delta g}{(1+\Delta N)}\left(\frac{C}{N_0}\right)_{\text{a}} \tag{27}$$

  In the spoofing situation, the estimated C/N_0 is also reduced because of the meaconing interference, but less than in the jamming situation due to the increase of the useful signal power by Δg.

- *Multipath situation* : The C/N_0 (with the moment method) has been modeled in Ghizzo et al. (2024b) as

$$\left(\frac{C}{N_0}\right)_{\text{M}} = \frac{1}{T_{\text{i}}}\frac{\sqrt{\overline{P_d}^2 - {C_{\text{a}}}^2\sigma_d^2}}{P_n + \overline{P_d} - \sqrt{\overline{P_d}^2 - {C_{\text{a}}}^2\sigma_d^2}}. \tag{28}$$

  with

$$\overline{P_d} = \left(\zeta(\boldsymbol{\varepsilon}_\eta)^2 + \Delta g\zeta(\boldsymbol{\varepsilon}_\eta + \Delta\boldsymbol{\eta})^2 + 2\sqrt{\Delta g}\zeta(\boldsymbol{\varepsilon}_\eta)\zeta(\boldsymbol{\varepsilon}_\eta + \Delta\boldsymbol{\eta})\frac{\sin(\pi M\Delta f T_i)}{M\sin(\pi\Delta f T_i)}\cos(\overline{\Delta\theta})\right)C_a \tag{29}$$

$$\sigma_d^2 = 2\Delta g\zeta(\boldsymbol{\varepsilon}_\eta)^2\zeta(\boldsymbol{\varepsilon}_\eta + \Delta\boldsymbol{\eta})^2\left[1 + \frac{\sin(2\pi M\Delta f T_i)}{M\sin(2\pi\Delta f T_i)}\cos(2\overline{\Delta\theta}) - 2\frac{\sin^2(\pi M\Delta f T_i)}{M^2\sin^2(\pi\Delta f T_i)}\cos^2(\overline{\Delta\theta})\right]. \tag{30}$$

  where T_{e} is the C/N_0 estimation time, $\overline{\Delta\theta} = \pi M\Delta f T_i + \Delta\theta$ is the mean relative phase within T_{e} and $M = T_{\text{e}}/T_{\text{i}}$ is the number of integration periods within T_{e}. The effective C/N_0 in the multipath situation strongly depends on the relative frequency Δf and phase $\Delta\theta$, and can either by greater or smaller than the nominal C/N_0 depending on the interference between the meaconer and authentic signals.

5. Position and protection level computations

This subsection presents the mathematical models to compute a position from the smoothed pseudoranges are their corresponding C/N_0. The procedures are standards of civil aviation are used to obtain the estimated position of the aircraft, in compliance with DO229E (2016) and ED259 (2019). First, the pseudorange approval checks that remove the unhealthy measurements are exhibited. Second, the position estimation model is explained. Third, the FD procedure that monitors the consistency of the position estimation is detailed. Fourth, the protection levels validating the integrity of the estimated position are introduced.

a) Pseudorange approval checks

The received pseudoranges shall be approved by 3 different checks before being used to estimate the aircraft position. The 3 pseudorange approval tests are detailed hereafter.

- C/N_0 *threshold* :
  According to ED259 (2019), the GNSS receiver shall not use a measurement for positioning when its estimated C/N_0 (denotes as $\hat{C/N_0}$) drops below 30 dB.Hz. If so, the signal is still tracked but is not used to estimate the position.

Mathematically, the C/N_0 threshold is computed for PRN i at epoch κ as

$$\mathcal{T}_i^{CN0}[\kappa] = \begin{cases} 1 & \text{if} \quad \hat{C/N}_{0i}[\kappa] < 30 \text{ dB.Hz} \\ 0 & \text{otherwise.} \end{cases} \tag{31}$$

The smoothed pseudorange of PRN i is approved by the C/N_0 threshold at epoch κ if and only if $\mathcal{T}_i^{CN0}[\kappa] = 0$.

- *Measurement quality monitoring (CMC test)* :
  A quality test (sometimes known as the Code Minus Carrier - CMC test) is performed on the measurements, and originally aims at detecting any slip of the carrier phase measurement that could bias the smoothed pseudoranges and induce wrong position estimations. The CMC test is computed for PRN i at epoch κ as

$$\mathcal{T}_i^{CMC}[\kappa] = \begin{cases} 1 & \text{if} \quad |\tilde{\rho}_i[\kappa] - \hat{\rho}_i[\kappa]| > 10 \text{ m} \\ 0 & \text{otherwise.} \end{cases} \tag{32}$$

  The smoothed pseudorange of PRN i is approved by the CMC test at epoch κ if and only if $\mathcal{T}_i^{CMC}[\kappa] = 0$.

- *Step detector* :
  In compliance with ED259 (2019), the airborne GNSS receiver shall be able to detect and exclude any pseudorange step larger than 700 meters used in the position estimation. This test is far less effective than the FD procedure (explained after) to detect pseudorange steps. The step detector is therefore not presented in this paper.

When a measurement successfully passes the 3 tests, the smoothed pseudorange is declared *usable* and can be used for positioning. As the step detector is never activated, a pseudorange i is considered usable at epoch κ if and only if $\mathcal{T}_i^{CN0}[\kappa] + \mathcal{T}_i^{CMC}[\kappa] = 0$.

b) Position estimation from the GNSS observables

When at least 4 smoothed pseudoranges are usable at a given epoch, an estimation of the aircraft's position $\hat{\mathbf{x}}$ can be computed using (DO229E, 2016, Appendix E):

$$\begin{aligned} &\hat{\mathbf{x}} = \mathbf{S}\mathbf{y} \\ &\mathbf{S} = \left(\mathbf{G}^T\mathbf{W}\mathbf{G}\right)^{-1}\mathbf{G}^T\mathbf{W} \qquad \mathbf{G} = \begin{bmatrix}\mathbf{g}_1^T & \dots & \mathbf{g}_{N_s}^T\end{bmatrix}^T \\ &\mathbf{g}_i^T = \begin{bmatrix} -\cos(\psi_i)\sin(\phi_i) \\ -\cos(\psi_i)\cos(\phi_i) \\ -\sin(\psi_i) \\ 1 \end{bmatrix} \qquad \mathbf{W} = \begin{bmatrix} \sigma_1^{-2} & 0 & \dots & 0 \\ 0 & \sigma_2^{-2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \sigma_{N_s}^{-2} \end{bmatrix} \end{aligned} \tag{33}$$

where the vector $\mathbf{y}$ contains the smoothed pseudoranges $\hat{\rho}_i[k]$ of all the usable satellites at epoch κ, and ψ_i, ϕ_i represent the elevation and azimuth angles of the satellite i with respect to the previously estimated aircraft position. The values of σ_i are given by Eq. (25). The dependence of $\mathbf{y}$, $\mathbf{S}$, $\mathbf{G}$, and $\mathbf{W}$, on κ is omitted in the notations for clarity.

c) Fault detection procedure

The Fault Detection (FD) procedure, described in Kaplan and Hegarty (2017) is built on a statistical test of the measurement residuals to detect inconsistency among the usable pseudoranges. The FD procedure is computed as

$$\mathcal{T}^{\text{FD}}[\kappa] = \begin{cases} 1 & \text{if} \quad q[\kappa] \geq T_q \\ 0 & \text{otherwise.} \end{cases} \tag{34}$$

Where $q[\kappa] = \mathbf{r}^T\mathbf{W}\mathbf{r}$; $\mathbf{r} = (\mathbf{I} - \mathbf{G}(\mathbf{G}^T\mathbf{W}\mathbf{G})^{-1}\mathbf{G}^T\mathbf{W})\mathbf{e}$ and $T_q = F_{N_s-4}^{-1}(1 - p_{fa})$.

$\mathbf{e}$ contains the differences between the smoothed usable pseudoranges at epoch κ and the predicted usable pseudoranges at epoch κ (DO229E (2016)), $\mathbf{r}$ denotes the pseudorange residuals, N_s is the number of usable pseudoranges at epoch κ, and $F^{-1}_{N_s-4}(1-p_{fa})$ represents the inverse cumulative distribution function of the chi-square distribution with N_s-4 degrees of freedom. The probability of false alarm p_{fa} is set to $2e^{-9}$ to comply with aviation standards.

When only 4 satellites are usable, FD is deemed non-operational, and no FD alarm can be raised. In this case, the position is still estimated and used for navigation despite its unknown integrity. With 5 or more usable satellites, FD can detect a fault. If no fault is detected, the position is used for navigation, otherwise, a FD alarm is raised and the estimated position is not used for navigation.

d) Protection level computation

SBAS-based aviation integrity is based on the computation of protection levels for en route through LPV approach. The Horizontal and Vertical Protection Levels (resp. HPL and VPL) in SBAS mode are defined in (DO229E, 2016, Appendix J), and recapped hereafter.

$$\begin{aligned} HPL[\kappa] &= K_{\text{H, NPA}}\, d_{\text{major}}[\kappa] = 6.18 \times d_{\text{major}}[\kappa] \\ VPL[\kappa] &= K_{\text{V}} d_{\text{U}}[\kappa] = 5.33 \times d_{\text{U}}[\kappa] \end{aligned} \tag{35}$$

Where

$$\begin{aligned} d_{\text{major}} &= \sqrt{\frac{d^2_{\text{E}} + d^2_{\text{N}}}{2} + \sqrt{\left(\frac{d^2_{\text{E}} - d^2_{\text{N}}}{2}\right)^2 + d^2_{\text{EN}}}} \\ d^2_{\text{E}} &= \sum_{i=1}^{N_s} s^2_{\text{east},i}\sigma_i^2[\kappa] \qquad\qquad d^2_{\text{N}} = \sum_{i=1}^{N_s} s^2_{\text{north},i}\sigma_i^2[\kappa] \\ d^2_{\text{EN}} &= \sum_{i=1}^{N_s} s_{\text{east},i}s_{\text{north},i}\sigma_i^2[\kappa] \qquad\qquad d^2_{\text{U}} = \sum_{i=1}^{N_s} s^2_{\text{up},i}\sigma_i^2[\kappa] \end{aligned} \tag{36}$$

and $s_{\text{east},i}$, $s_{\text{north},i}$ and $s_{\text{up},i}$ are respectively the east, north and up components of the i^{th} row of matrix $\mathbf{S}$ (33). The protection levels monitor the integrity of the position throughout the flight, by comparing the Horizontal and Vertical Alert Limits (resp. HAL and VAL) to the protection levels, and by raising an alarm if at least one protection level exceeds its corresponding alert limit. If an alarm is raised, the position is declared unavailable. Mathematically, the protection level check is computed as

$$\mathcal{T}^{\text{PL}}[\kappa] = \begin{cases} 1 & \text{if} \quad HPL[\kappa] > HAL \quad \text{or} \quad VPL[\kappa] > VAL \\ 0 & \text{otherwise.} \end{cases} \tag{37}$$

Where the values of HAL and VAL are given in the standards and depend on the considered phase of flight. The estimated position at epoch κ can be used for positioning if and only if $\mathcal{T}^{\text{PL}}[\kappa] = 0$ and $\mathcal{T}^{\text{FD}}[\kappa] = 0$.

6. Example of the meaconing impact under onboard meaconing

After modeling the primary processing blocks of a standardized aircraft GNSS receiver under meaconing interference, this section illustrates the effects of the meaconer on two different examples that are representative of onboard meaconing scenarios. First, the two scenarios under scrutiny are defined and their relative parameters are provided. Second, the different mathematical models of the previous sections are applied on the two scenarios and their results are explained. This section serves as an example to better understand the different meaconing impacts on the aircraft GNSS receiver, along with their causes and consequences.

a) Definition of the two pedagogic scenarios

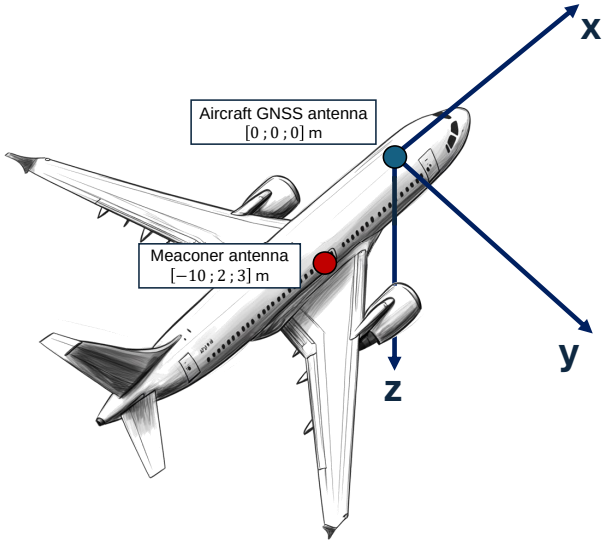

Figure 3: Illustration of the meaconer position in the aircraft frame.

The two pedagogic scenarios are representative of a situation where the meaconer is onboard the aircraft, as if a passenger carries the meaconer with him in the cabin. In both scenarios, the meaconer is placed at a relative position of $[-10, 2, 3]$ meters in the aircraft frame from the aircraft's GNSS antenna, so that the meaconer is about 10.2 meters horizontally behind the aircraft's antenna, and 3 meters vertically below the aircraft's antenna (as illustrated in Fig. 3). The aircraft is flying in straight line at cruise speed (540 kt) and at an altitude of 30000 ft, to represent nominal cruise conditions in civil aviation. The two scenarios under scrutiny represent the same flight profile, but each one monitors a different satellite signal (a different PRN) of the GPS constellation, resulting in different relative Doppler Δf and relative phases $\Delta\theta$ in the two scenarios.

The scenarios can also be fully described with respect to the relative parameters $\boldsymbol{\Delta}\eta = [\Delta g, \Delta N, \Delta\tau, \Delta f, \Delta\theta]$. The relative parameters corresponding to the two scenarios are presented in Eqs. (38) and (39) and have been chosen to represent realistic profiles of relative parameter variations under onboard meaconing.

In the case of onboard meaconing during a flight in straight line, Δg, ΔN, $\Delta\tau$ and Δf are almost constant, because all the quantities involved in their formulas (Eqs. (1) to (4)) undergo very little variations. However, the relative phase $\Delta\theta$ (5) varies linearly during the flight, as it depends on the time t of the flight. The actual values of the relative parameters under onboard meaconing are exposed in Appendix. VII.3 to validate the assumptions made on the relative parameter variations. In the two scenarios, the gain G_m of the meaconer is increased twice for pedagogic reasons, to illustrate 3 different meaconer gains in each of the 2 scenarios. All in all, 6 situations are thus shown, to cast the light on the different behaviors of the GNSS observables when exposed to 6 different onboard meaconing scenarios.

The first profile (in red) is a 30-minute long scenario with relative parameters given by Eq. (38). In the first 10 minutes of the scenario, the gain of the meaconer is small, such that the tracking process (and its cascading effects) is barely affected by the meaconing signals. Between 10 and 20 minutes of flight, the gain of the meaconer is adjusted such that the meaconing signals arriving at the aircraft's antenna output have the same power as the authentic signals (i.e., $\Delta g = 0$ dB). In the last 10 minutes of flight, the gain of the meaconer is once more increased, so that the tracking process is now mainly driven by the meaconing signals. The meaconer noise factor NF_m is considered equal to 0 dB to simplify the examples, thus, $\Delta g = \Delta N$ during the whole profile. The meaconer has a small intrinsic delay $\tau_m > 0$, chosen to have $c\Delta\tau_1 = 25$ meters with Eq. (3), and such that the multipath situation is observed (because $\Delta\tau_1 < T_{\text{max}}$). Finally, the motion of the considered satellite creates a tiny relative Doppler Δf, considered constant at 0.003 Hz during the whole flight.

The second profile (in blue) is also a 30-minute long scenario with relative parameters given by Eq. (39). The relative gain Δg and relative noise ΔN are kept the same as in the first profile. The meaconer has a different small intrinsic delay $\tau'_m > 0$, chosen to have $c\Delta\tau_2 = 35$ meters with Eq. (3), and such that the multipath situation is also observed during the whole flight (because $\Delta\tau_2 < T_{\text{max}}$). Finally, the motion of the considered satellite creates a tiny relative Doppler, considered constant at $\Delta f = 0.006$ Hz during the whole flight. A different relative phase at origin is chosen is this scenario, not to observe the meaconing interference at the same epochs in the two scenario.

$$\Delta g(t) = \Delta N(t) = \begin{cases} -20 \text{ dB} & \text{if} \quad 0 \leq t < 600 \text{ s} \\ 0 \text{ dB} & \text{if} \quad 600 \leq t < 1200 \text{ s} \\ 20 \text{ dB} & \text{if} \quad 1200 \leq t \leq 1800 \text{ s} \end{cases}, \quad c\Delta\tau_1 = 25 \text{ m}, \quad \Delta f_1 = 0.003 \text{ Hz}, \quad \theta_{0,f} = 0 \text{ rad} \tag{38}$$

$$\Delta g(t) = \Delta N(t) = \begin{cases} -20 \text{ dB} & \text{if} \quad 0 \leq t < 600 \text{ s} \\ 0 \text{ dB} & \text{if} \quad 600 \leq t < 1200 \text{ s} \\ 20 \text{ dB} & \text{if} \quad 1200 \leq t \leq 1800 \text{ s} \end{cases}, \quad c\Delta\tau_2 = 35 \text{ m}, \quad \Delta f_2 = 0.006 \text{ Hz}, \quad \theta_{0,f} = 1 \text{ rad}. \tag{39}$$

The impact of the onboard meaconer on the two satellite signals (characterized by the two profiles of Eqs. 38 and 39) is presented in Figs. 4 to 8, and detailed in the next subsections.

b) Example of the onboard meaconing interference on the DLL and PLL stable equilibria

The DLL and PLL SE (respectively ε_τ and ε_θ) are computed by solving Eq. (9) for the two profiles, and represent the deterministic part of the tracking estimation errors inside the code and the phase pseudoranges. The results are shown in Fig. 4 and explained hereafter. The values from the first profile are drawn in red, whereas the values of the second profile are depicted in blue.

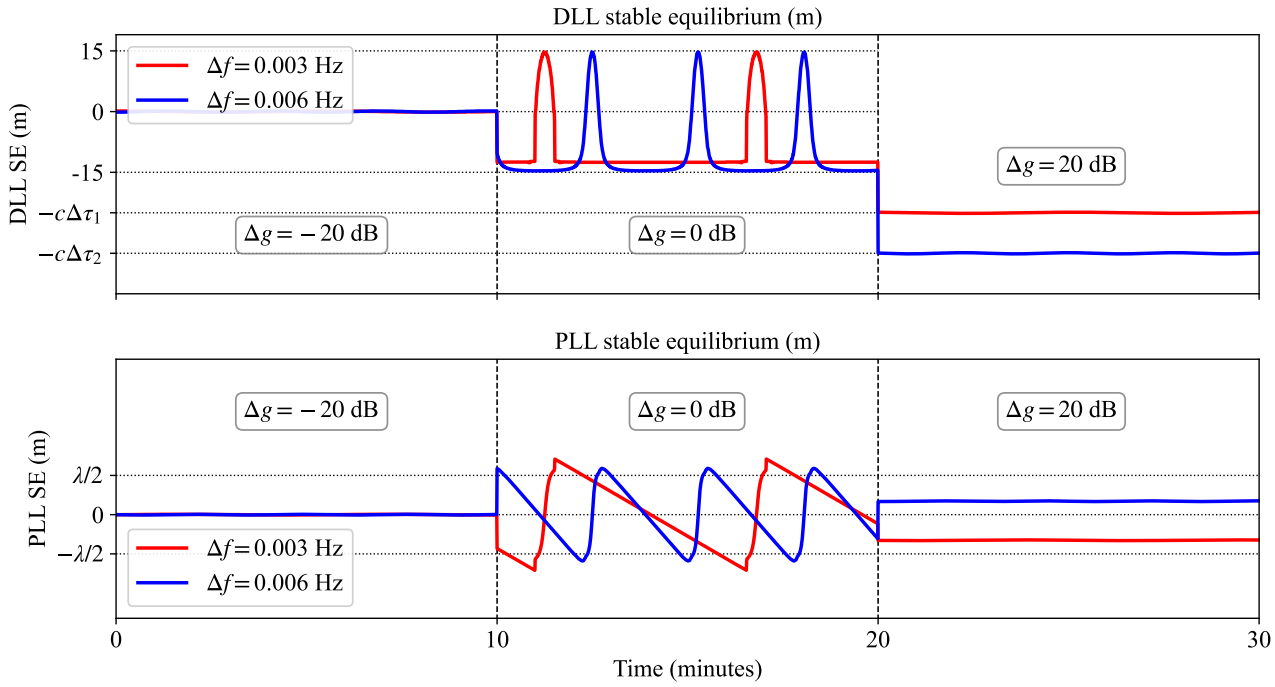

Figure 4: Theoretical DLL and PLL SE for the two pedagogic scenarios representative of onboard meaconing interference.

When $\Delta g = \Delta N = -20$ dB, Fig. 4 highlights that the tracking errors at lock are really close to zero, because the tracking is barely deteriorated by the meaconer signal or by the meaconer re-radiated noise. The aircraft's receiver, although in the multipath situation, is marginally impacted by the onboard meaconing interference, similarly to the nominal situation.

When $\Delta g = \Delta N = 0$ dB, the aircraft receives both authentic and meaconer signals with the same power, and the DLL SE values can reach up to $\pm c_\tau/2 = \pm 15$ meters, accordingly to the maximum multipath error that can be found in the literature for classical GNSS multipath (Kaplan and Hegarty (2017)). Especially, when $\Delta\theta \approx 0 \mod [2\pi]$, the two signals add up with constructive interference, and the correlators are attracted towards the meaconing signal parameters. As the meaconer signal detours through the meaconer before reaching the aircraft antenna, its propagation time (so its delay) is always larger than the one of the authentic signal ($\Delta\tau > 0$). The correlators are thus attracted towards larger delays, and the DLL error at lock is negative. When $\Delta\theta \approx \pi \mod [2\pi]$, the opposite situation happens. The meaconer signal and the authentic signal add up with negative interference, the correlators are repelled from the meaconer signal characteristics, and the DLL error at lock is therefore positive. Additional information is brought in Appendix VII.4 about the SE deflections. In this configuration, the SE spends more time at -15 m than at $+15$ m, because the relative delay in both scenarios is small. If the relative delay is larger ($T_{\max}/2 \leq \Delta\tau \leq T_{\max}$), then the variations of the DLL SE are more equally split between positive and negative values, and the DLL SE variations mimic sinusoidal variations. This scenario is not shown here because a lager delay would degrade the viewing of the plots where $\Delta g = \Delta N = 20$ dB.

When $\Delta g = \Delta N = 20$ dB, the magnitude of the meaconer signal is significantly larger than the authentic signal magnitude. The tracking loops follow the meaconer signal and both the DLL and PLL SE are centered around the meaconer signal characteristics. In this configuration, $\varepsilon_\tau \approx -c\Delta\tau$ and $\varepsilon_\theta \approx -c\Delta\tau$ (the PLL SE ε_θ is represented modulo λ to observe in the same plot the small phase variations when $\Delta g = 0$ dB, and the large phase offset when $\Delta g = 20$ dB.

The tracking error at lock (i.e., the SE), does not represent the actual errors, but rather the tracking error to which the system tries to converge. The full behavior of the system is further analyzed in Ghizzo et al. (2024a). However, in the context of onboard meaconing, the relative parameters vary very slowly so that the actual tracking loops have time to converge to the SE. Thus, the DLL and PLL SE values correspond to the mean values of the tracking loop estimation errors, retrieved in the pseudorange models. The SE is therefore an excellent approximation of the actual DLL and PLL mean errors for onboard meaconers.

c) Example of the onboard meaconing interference on the smoothed pseudorange

When passing the DLL and PLL SE presented in Fig. 4 into the carrier smoothing filter (21), the smoothed SE is obtained and can be assimilated to the deterministic part of $\tilde{\epsilon}$ (denoted $\tilde{\varepsilon}_{\text{smo}}$) in Eq. (24). Fig. 5a presents this smoothed SE for the two profiles under scrutiny. When adding the post-SBAS correction residual errors $\tilde{\omega}$ of Eq. (24), the total error of the smoothed pseudorange after SBAS corrections is obtained and is plotted in Fig. 5b.

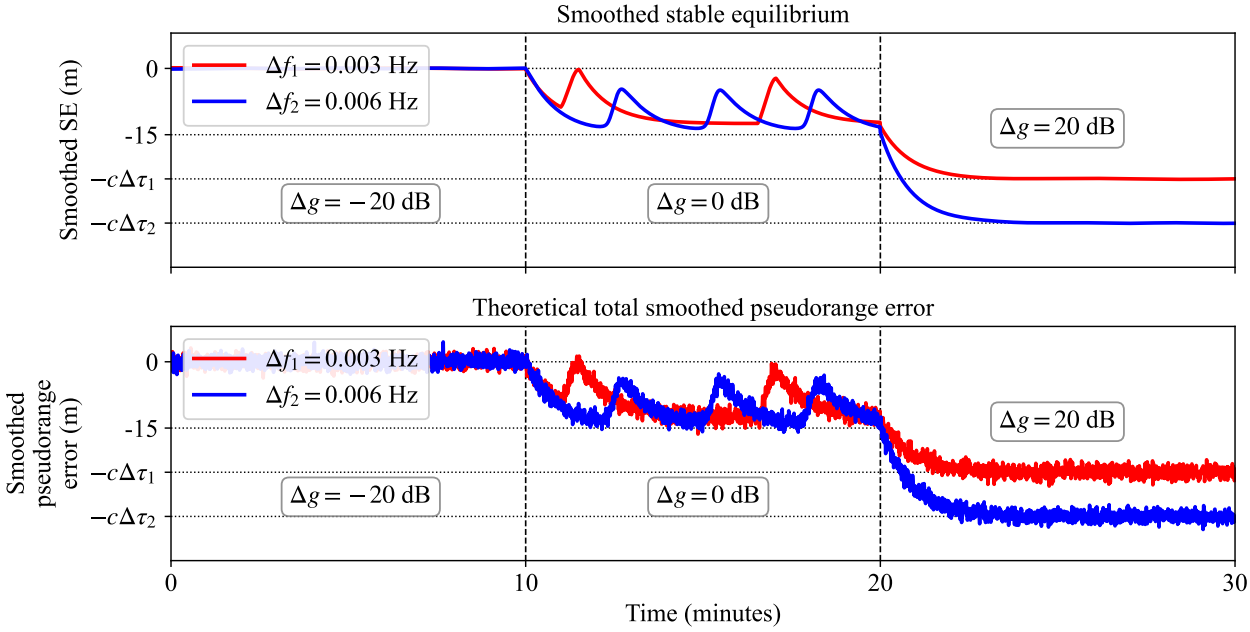

Figure 5: Theoretical smoothed SE, and total pseudorange error for the two pedagogic scenarios.

Fig. 5 highlights the low-pass effect of the carrier smoothing filter, that reduces the rapid variations of the code and phase pseudorange errors. When $\Delta g = 0$ dB, the the deterministic errors induced by the smoothed SE $\tilde{\epsilon}$ reach 10 meters, and they can be larger than the errors induced by the other pseudorange errors after SBAS corrections ($\approx$ 3m). It can also be noticed that the smoothed SE errors largely exceed the error budget allocated for the smoothed tracking errors by the standards (DO229E, 2016, Appendix J) that shall be smaller than 0.36 meters in all circumstances. Above all, when $\Delta g = 20$ dB, the smoothed pseudorange error converges to $-c\Delta\tau$, that can be arbitrarily larger (up to $-cT_{\text{max}} \approx -308$ m to stay in the multipath situation), and could potentially degrade the GNSS position estimation.

d) Example of the onboard meaconing interference on the mean estimated C/N_0

The mean estimated C/N_0 (by the moment estimator) can be computed thanks to Eq. (28) and is shown in Fig. 6 for a nominal $C/N_{0,\text{a}}$ of 40 dB.Hz.

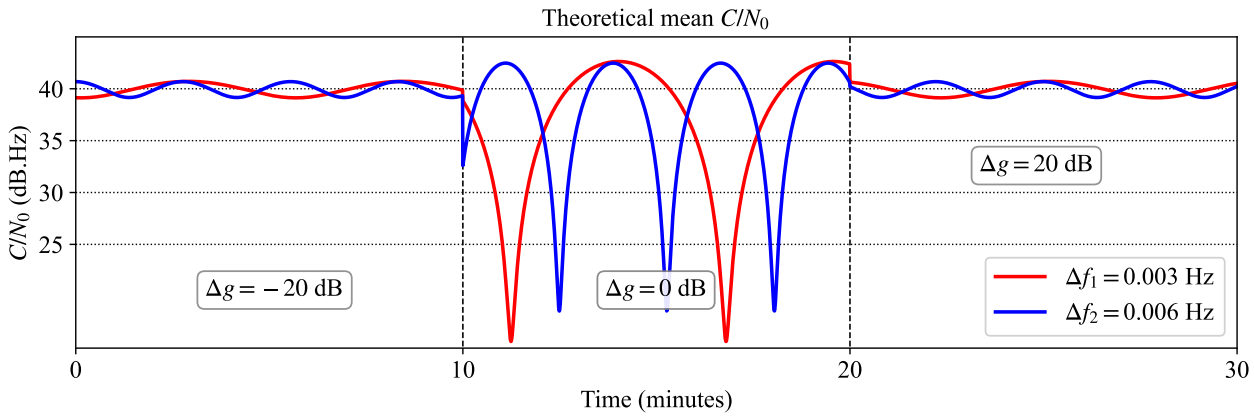

Figure 6: Mean theoretical C/N_0 for the two pedagogic scenarios.

When $\Delta g = -20$ dB, the estimated C/N_0 is marginally deteriorated by the meaconing interference, and barely oscillates around the nominal $C/N_{0,\text{a}} = 40$ dB.Hz at a frequency of Δf.

When $\Delta g = 0$ dB, the relative phase $\Delta\theta$ plays a prominent role in the C/N_0 estimation. When $\Delta\theta \approx 0 \mod [2\pi]$, the authentic and the meaconer signals add up constructively, resulting in a higher C/N_0 than in the nominal situation. When $\Delta\theta \approx \pi \mod [2\pi]$, the meaconer signal causes destructive interference with the authentic signal, significantly reducing the C/N_0 up to 15 dB.Hz.

When $\Delta g = 20$ dB, the situation is the same as when $\Delta g = -20$ dB, except that the roles of the meaconer and the authentic signals have swapped. Note that is this scenario, the meaconer does not generate additional noise ($NF_m = 0$ dB), so the meaconer signal has the same quality (hence the same C/N_0) as the authentic signal. If $NF_m > 0$ dB, the estimated C/N_0 would have been smaller in this configuration.

e) Example of the onboard meaconing interference on the pseudorange approval checks

The C/N_0 threshold and the CMC test statistics can be computed for the 2 profiles. The step detector is not presented here, but it can be easily demonstrated that the step detector would never activate under onboard meaconing, as the largest observed pseudorange errors are smaller than 700 meters (the step detector threshold). Hussong et al. (2024b) establishes that the CMC test (32) can be rearranged using Eq. (17) and (22) as

$$\mathcal{T}_i^{CMC}[\kappa] = \begin{cases} 1 & \text{if} \quad \left|\tilde{\varepsilon}_{\text{smo},i}[\kappa] - \varepsilon_{\tau,i}[\kappa] + \omega_i^{CMC}[\kappa]\right| > 10 \text{ m} \\ 0 & \text{otherwise} \end{cases} \qquad \text{where} \qquad \omega_i^{CMC}[\kappa] \sim \mathcal{N}\left(0 : \sigma^2_{i,CMC}[\kappa]\right). \quad (40)$$

Where ω_i^{CMC} contains the combination of the smoothed and code estimation errors (correlated) and the combination of the smoothed and code multipath errors (also correlated), according to the derivation of Hussong et al. (2024b). As the exact value of $\sigma^2_{i,CMC}$ has not been computed in Hussong et al. (2024b) in the multipath situation, the values of the CMC test for the 2 profiles are computed neglecting the noise (i.e., using $\sigma^2_{i,CMC} = 0$). This choice also allows for better observation of the test statistics, as it is not tarnished by the additional noise of the test.

The epochs of activation of the C/N_0 threshold and of the CMC test, as well as the 2 corresponding test statistics without noise are shown in Fig. 7.

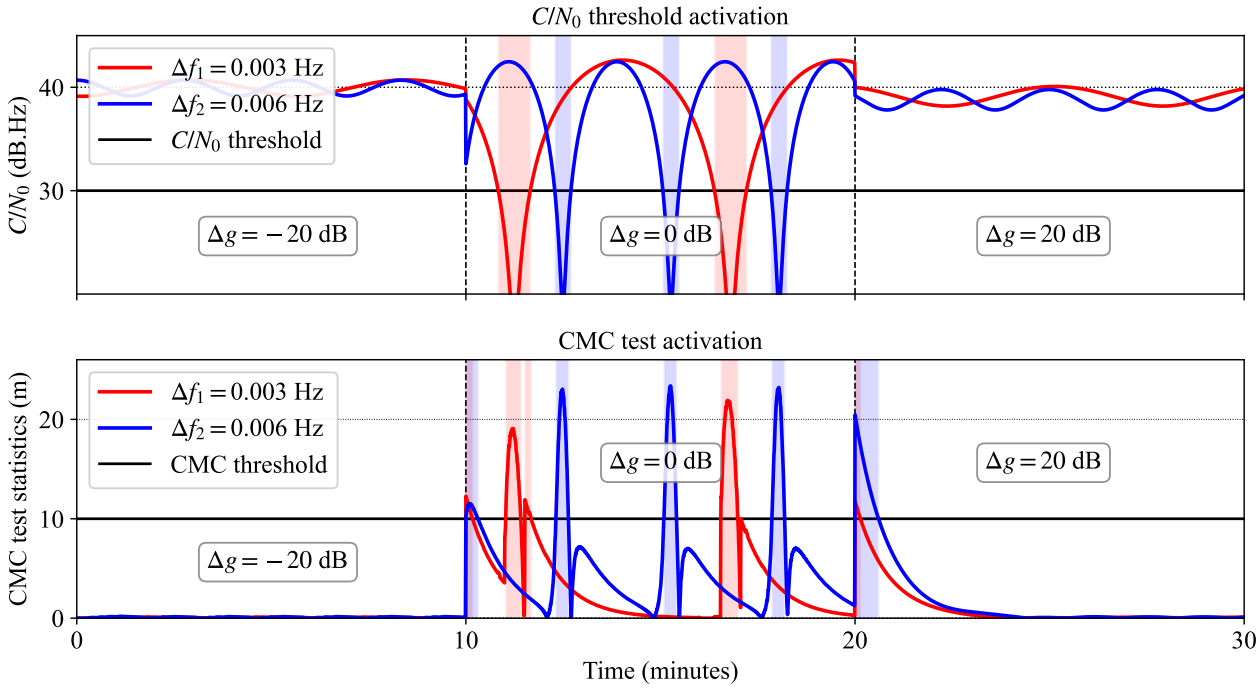

Figure 7: Pseudorange approval test statistics for the two pedagogic scenarios.

Fig. 7 exhibits that both the C/N_0 threshold and the CMC test activates in the presence of onboard meaconing when $\Delta g = 0$ dB. Some pseudoranges can therefore be declared as unusable and not used for positioning due to the meaconing interference. The two tests appear to be correlated, as they are likely to be activated at the same epoch under meaconing interference. They also activate quite often when $\Delta g = 0$ dB, with an activation rate of about 17% for the C/N_0 threshold, and of about 10% for the CMC test. When $\Delta g = -20$ dB and $\Delta g = 20$ dB, the tests never activate (except during the convergence phase at $t = 20$ minutes, due to the past-persisting bias inside the smoothed tracking estimation term $\tilde{\varepsilon}_{\text{smo}}$).

f) Example of the onboard meaconing interference on the position estimation, PL computation and FD test statistics

For this paragraph, 6 other relative parameter profiles similar to (38) and (39) have been designed for pedagogic purpose. These 6 additional profiles only differ from their relative delay $\Delta\tau$, relative Doppler Δf, and initial relative phase $\theta_{0,f}$. They complete the 2 already given profiles to form a coherent constellation of 8 satellites representative of an onboard meaconing scenario. The DLL and PLL SE have been computed for the remaining 6 profiles, as well as the smoothed pseudorange neglecting the tracking loop estimation error and the post-SBAS correction residual errors (i.e., assuming $\tilde{n} = 0$ and $\tilde{\omega}_i = 0$ in Eq. 24), and the approval tests have been carried out. The theoretical position can then be estimated from the usable smoothed pseudoranges with Eq. (33), along with the PL computation (35) and the FD test statistics (34). The results are shown in Fig. 8 and explained hereafter.

Fig. 8a represents the horizontal position errors and the horizontal protection levels during the flight. Fig. 8b shows the vertical position error and the corresponding vertical protection level. Fig. 8c details the number of tracked and usable satellites. Finally, Fig. 8d highlights the FD threshold along with the FD test statistics computed during the flight.

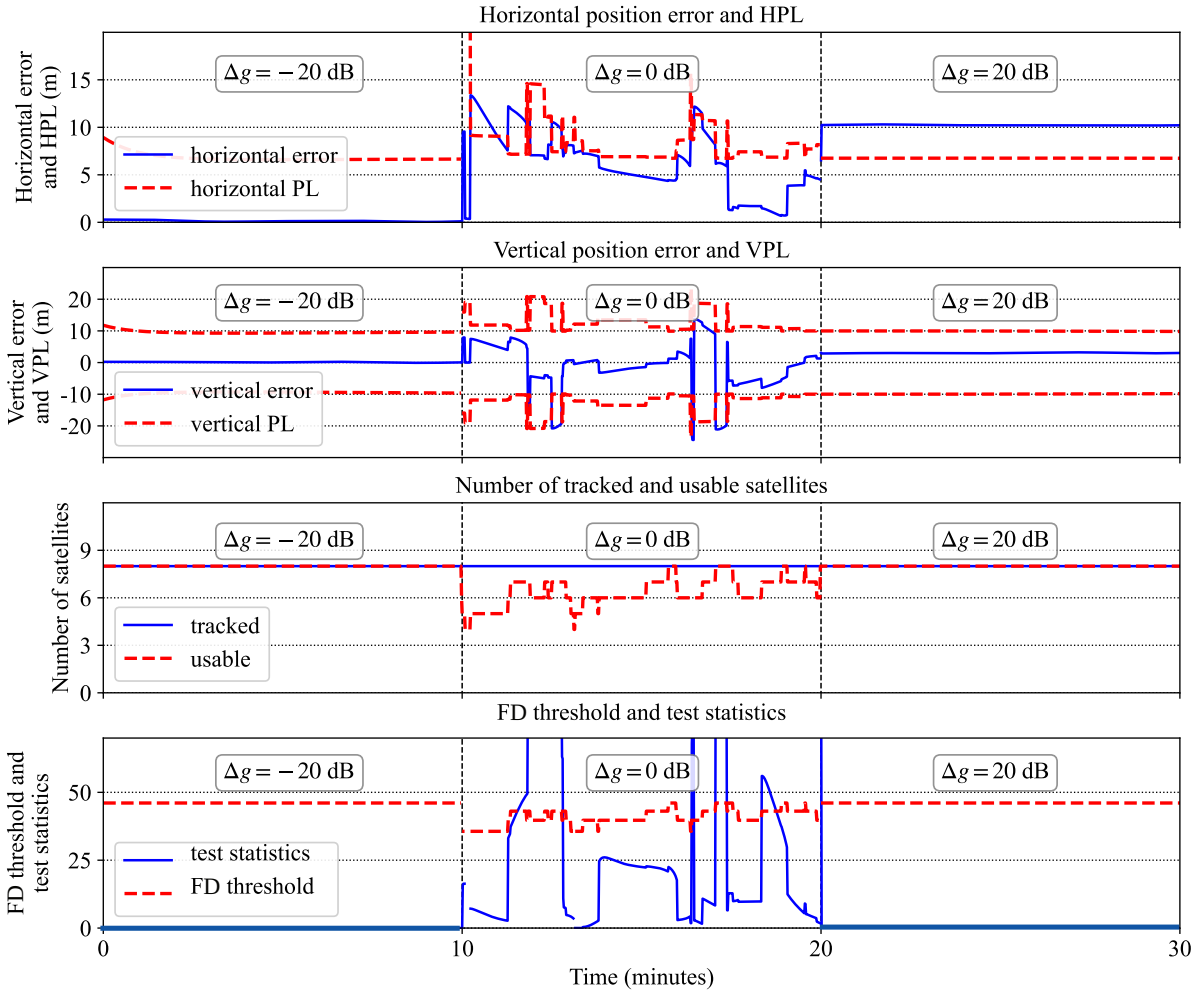

Figure 8: Theoretical position errors, PL, number of usable satellites, and FD test statistics during the flight.

When $\Delta g = -20$ dB, both the horizontal and vertical position errors are close to 0 m. As the post-SBAS correction noise has been neglected, only the distortions caused by the meaconing interference on the DLL and PLL outputs can deteriorate the position estimation. Since the meaconer has a marginal impact on the DLL and PLL outputs (and thus on the smoothed pseudorange) in this configuration, the position error induced by the meaconer is negligible. All the tracked satellites are usable, because the meaconing interference are not sufficiently high to cause any of the pseudorange approval test to activate. The FD threshold is therefore constant, as the number of usable pseudorange is always 8. The FD test statistics stays also extremely close to 0.

When $\Delta g = 0$ dB, the smoothed pseudoranges corrupted by the smoothed SE deflections feed the WLSE position algorithm, creating errors up to 20 m. The protection levels are also changing because the set of usable satellites is often modified due to the C/N_0 threshold and CMC tests activations. The number of usable pseudoranges varies between 8 (full set) and 4 (minimal number to estimate a position). At some epochs, the position error exceeds the corresponding protection level. The FD procedure raises alarms at some epochs, however, it can be observed that an alarm is not always raised when the position error exceeds the protection level (for instance around 11 minutes of flight for the horizontal position). Additionally, when exactly 4 pseudoranges are usable, the FD test is deemed non-operational and no FD test statistics can be computed.

When $\Delta g = 20$ dB, the DLL and PLL tracking loops follow the meaconer signals, inducing errors of $-c\Delta\tau$ in all the smoothed pseudoranges. The position is therefore estimated around the meaconer location (about 10.2 m behind the aircraft's antenna horizontally, and 3 m below the aircraft's antenna vertically). In that configuration, the horizontal position error exceeds the HPL, and the FD procedures does not raise any error because the 8 smoothed pseudoranges are corrupted with coherent errors (coherently pinning the meaconer location).

The same figure integrating post-SBAS correction pseudorange errors is given in Appendix VII.1 for the curious reader.

IV. THEORETICAL GNSS PERFORMANCE DEGRADATION UNDER ONBOARD MEACONING

This section presents a methodology to quantify the GNSS performance degradations induced by the meaconer onboard the aircraft. The methodology begins with the definition of three metrics, which are introduced in the first subsection. The metrics are then computed for different configurations of onboard meaconing in the subsequent subsections, along with explanations of their causes and consequences, to theoretically assess the GNSS performance under onboard meaconing.

1. Definition of the metrics of interest

This paper focuses on three metrics to evaluate the degradations caused by onboard meaconing interference: the *position availability*, the *position accuracy*, and the *position integrity*. These metrics are designed to explicitly represent and illustrate the impact of the meaconer on the aircraft's GNSS receiver performance. They do not directly correspond to the standardized notions of GNSS availability, accuracy, and integrity known in civil aviation (hence their distinct names). The definitions of these metrics are provided in the following paragraphs.

a) Position availability

In this study, the *position availability* is defined as the proportion of time a GNSS position can be estimated and used for positioning during a flight. Alternatively, the *position availability* can also be defined as the probability of being able to compute and use a GNSS position at any given time during the flight (this equivalence is based on the ergodic properties of the GPS signals in this configuration, as discussed in (Ghizzo, 2024, Chap. II, 1.1.3)).

Mathematically, the *position availability* $\mathcal{P}_{\text{ava}}$ is computed as the probability of having at least four usable pseudoranges (necessary for position computation), without triggering an FD alarm, and with protection levels below the alert limits. To compute this probability, the condition for the smoothed pseudorange i to be usable must, first, be determined. A smoothed pseudorange is declared usable if both the C/N_0 threshold and the CMC test are not activated. Denoting $\mathcal{T}_i^{\text{use}}$ the flag equal to 1 only if the pseudorange of PRN i is usable, it follows

$$\mathcal{T}_i^{\text{use}}[\boldsymbol{\Delta}\eta_i] \;=\; \left(1-\mathcal{T}_i^{\text{CN0}}[\boldsymbol{\Delta}\eta_i]\right) \;\times\; \left(1-\mathcal{T}_i^{\text{CMC}}[\boldsymbol{\Delta}\eta_i]\right). \tag{41}$$

In Eq. (41), the dependencies of the different pseudorange approval tests are expressed with respect to the relative parameters $\boldsymbol{\Delta}\eta = [\Delta g, \Delta N, \Delta\tau, \Delta f, \Delta\theta]$ at epoch κ, instead of epoch κ directly. This approach, while lengthening the expressions, provides a clearer understanding of the factors influencing the results. Hereafter, only the relative parameters affecting the equations' results are given in arguments.

A position can be estimated if at least four smoothed pseudoranges are available. Denoting $\mathcal{T}^{\text{pos}}$ the flag equal to 1 if a position can be estimated, it follows

$$\mathcal{T}^{\text{pos}}[\boldsymbol{\Delta}\mathbf{H}] = \begin{cases} 1 & \text{if} \quad \sum_{i=1}^{N_{\text{sat}}} \mathcal{T}_i^{\text{use}}[\boldsymbol{\Delta}\eta_i] \geq 4 \\ 0 & \text{otherwise.} \end{cases} \tag{42}$$

In Eq. (42), N_{sat} is the number of visible satellites, and the matrix $\boldsymbol{\Delta}\mathbf{H} = [\boldsymbol{\Delta}\eta_1\,,\,\boldsymbol{\Delta}\eta_2\,,\,\ldots\,,\,\boldsymbol{\Delta}\eta_{N_{\text{sat}}}]$ contains the relative parameters of all the visible satellites at epoch κ. A position is considered available if it can be computed, no FD error is raised, and the protection levels are below the alert limits. Denoting $\mathcal{T}^{\text{ava}}$ the flag equal to 1 only if the position is available, it follows

$$\mathcal{T}^{\text{ava}}[\boldsymbol{\Delta}\mathbf{H}] = \mathcal{T}^{\text{pos}}[\boldsymbol{\Delta}\mathbf{H}] \;\times\; \left(1-\mathcal{T}^{\text{FD}}[\boldsymbol{\Delta}\mathbf{H}]\right) \;\times\; \left(1-\mathcal{T}^{\text{PL}}[\boldsymbol{\Delta}\mathbf{H}]\right). \tag{43}$$

Finally, *position availability* $\mathcal{P}_{\text{ava}}$ is derived as the probability of $\mathcal{T}^{\text{ava}} = 1$. The value of $\mathcal{T}^{\text{ava}}$ at epoch κ is a deterministic function of the relative parameters $\boldsymbol{\Delta}\mathbf{H}$ at epoch κ. For onboard meaconing during straight-line flight, the relative parameters Δg, ΔN, $\Delta\tau$, and Δf are considered constant for each satellite signal. The relative phases $\boldsymbol{\Delta}\theta$ of the signals are assumed to be uniformly distributed between 0 and 2π. The ergodic properties of the GPS signals allow for the computation of $\mathcal{P}_{\text{ava}}$ in the temporal (44) or statistical (45) domains, resulting in

$$\mathcal{P}_{\text{ava}}[\boldsymbol{\Delta}\mathbf{g}, \boldsymbol{\Delta}\mathbf{N}, \boldsymbol{\Delta}\tau, \boldsymbol{\Delta}\mathbf{f}] = \lim_{\kappa\to\infty} \frac{1}{\kappa} \sum_{j=1}^{\kappa} \mathcal{T}^{\text{ava}}[\boldsymbol{\Delta}\mathbf{g}, \boldsymbol{\Delta}\mathbf{N}, \boldsymbol{\Delta}\tau, \boldsymbol{\Delta}\mathbf{f}, \boldsymbol{\Delta}\theta(j)] \tag{44}$$

$$= \frac{1}{(2\pi)^{N_{sat}}} \int_{\Omega} \mathcal{T}^{\text{ava}}[\boldsymbol{\Delta}\mathbf{g}, \boldsymbol{\Delta}\mathbf{N}, \boldsymbol{\Delta}\tau, \boldsymbol{\Delta}\mathbf{f}, \boldsymbol{\Delta}\theta] \, \mathrm{d}\boldsymbol{\Delta}\theta. \tag{45}$$

Where $\Omega = [0\,;\, 2\pi]^{N_{\text{sat}}}$ is the definition space of the vector $\boldsymbol{\Delta}\theta$. Although Eqs. (44) and (45) yield the same result, they offer different interpretations of the *position availability*. In Eq. (44), the *position availability* denotes the proportion of time a position can be estimated and used for positioning during a flight. In Eq. (45), the *position availability* denotes the probability of being able to compute and use a position at a given time during the flight.

b) Position accuracy

The *position accuracy* is defined in this study as the 99%-quantile of the estimated position error distribution at a given epoch κ during the flight for which the position is available (i.e., when $\mathcal{T}^{\text{ava}}[\kappa] = 1$). By ergodicity of the position error, the *position accuracy* gives, for specific values of $\boldsymbol{\Delta}\mathbf{g}$, $\boldsymbol{\Delta}\mathbf{N}$, $\boldsymbol{\Delta}\tau$ and $\boldsymbol{\Delta}\mathbf{f}$, the distance that bounds 99% of the availiable position errors during the flight.

Mathematically, the *position accuracy* is defined with respect to the position error $\delta\mathbf{x}$, given for all relative parameters $\boldsymbol{\Delta}\mathbf{H}$ by

$$\delta\mathbf{x}[\boldsymbol{\Delta}\mathbf{H}] = \| \, \mathbf{x} - \hat{\mathbf{x}}[\boldsymbol{\Delta}\mathbf{H}] \, \| \tag{46}$$

where $\mathbf{x}$ is the true aircraft 3D position, and $\| \, \|$ denotes the Euclidean norm. The error flag $\mathcal{T}^{\text{err}}$ is then defined as being equal to 1 only if the position error is smaller than a given distance ϵ:

$$\mathcal{T}^{\text{err}}[\boldsymbol{\Delta}\mathbf{H}, \epsilon] = \begin{cases} 1 & \text{if} \quad \delta\mathbf{x}[\boldsymbol{\Delta}\mathbf{H}] \leq \epsilon \\ 0 & \text{otherwise.} \end{cases} \tag{47}$$

The *position accuracy* $\mathcal{P}_{\text{acc}}$ can finally be defined in the temporal (48) and in the statistical (49) domain, as

$$\mathcal{P}_{\text{acc}}[\boldsymbol{\Delta}\mathbf{g}, \boldsymbol{\Delta}\mathbf{N}, \boldsymbol{\Delta}\tau, \boldsymbol{\Delta}\mathbf{f}] = \min \left[\quad \epsilon \quad \middle| \quad \lim_{\kappa\to\infty} \left(\frac{\sum_{j=1}^{\kappa} \mathcal{T}^{\text{err}}[\boldsymbol{\Delta}\mathbf{g}, \boldsymbol{\Delta}\mathbf{N}, \boldsymbol{\Delta}\tau, \boldsymbol{\Delta}\mathbf{f}, \boldsymbol{\Delta}\theta(j), \epsilon]}{\sum_{j=1}^{\kappa} \mathcal{T}^{\text{ava}}[\boldsymbol{\Delta}\mathbf{g}, \boldsymbol{\Delta}\mathbf{N}, \boldsymbol{\Delta}\tau, \boldsymbol{\Delta}\mathbf{f}, \boldsymbol{\Delta}\theta(j)]} \right) \geq 0.99 \right] \tag{48}$$

$$= \min \left[\quad \epsilon \quad \middle| \quad \frac{\int_{\Omega} \mathcal{T}^{\text{err}}[\boldsymbol{\Delta}\mathbf{g}, \boldsymbol{\Delta}\mathbf{N}, \boldsymbol{\Delta}\tau, \boldsymbol{\Delta}\mathbf{f}, \boldsymbol{\Delta}\theta, \epsilon] \mathrm{d}\boldsymbol{\Delta}\theta}{\int_{\Omega} \mathcal{T}^{\text{ava}}[\boldsymbol{\Delta}\mathbf{g}, \boldsymbol{\Delta}\mathbf{N}, \boldsymbol{\Delta}\tau, \boldsymbol{\Delta}\mathbf{f}, \boldsymbol{\Delta}\theta] \, \mathrm{d}\boldsymbol{\Delta}\theta} \geq 0.99 \right]. \tag{49}$$

Although Eqs. (48) and (49) give the same result, they propose a different interpretation of the *position accuracy*. In Eq. (48), the *position accuracy* denotes the distance that bounds 99% of the position errors during the flight. In Eq. (49), the *position accuracy* denotes the 99%-quantile of the estimated position error distribution at a given epoch during the flight.

c) Position integrity

The *position integrity* is defined in this study as the proportion of estimated positions that are available during the flight, while having a position error greater than the protection level. By ergodicity, the *position integrity* can also be defined as the probability of estimating a position at a given time during the flight, that is available while having a position error greater than the protection level.

To derive the *position integrity*, the horizontal and vertical position errors ($\delta^H\mathbf{x}$ and $\delta^V\mathbf{x}$), as well as their corresponding flags ($\mathcal{T}^{\text{err},H}$ and $\mathcal{T}^{\text{err},V}$) are defined similarly to Eqs. (46) and (47).

$$\delta^H\mathbf{x}[\boldsymbol{\Delta}\mathbf{H}] = \left\| \, \mathbf{x}^H - \hat{\mathbf{x}}^H[\boldsymbol{\Delta}\mathbf{H}] \, \right\| \tag{50}$$

$$\delta^V\mathbf{x}[\boldsymbol{\Delta}\mathbf{H}] = \left\| \, \mathbf{x}^V - \hat{\mathbf{x}}^V[\boldsymbol{\Delta}\mathbf{H}] \, \right\|. \tag{51}$$

where $\mathbf{x}^H$ and $\mathbf{x}^V$ are respectively the horizontal and vertical projections of the true aircraft position. $\hat{\mathbf{x}}^H$ and $\hat{\mathbf{x}}^V$ denote their corresponding estimations by the aircraft receiver. The error flags $\mathcal{T}^{\text{err},H}$ and $\mathcal{T}^{\text{err},V}$ are then defined as being equal to 1 only if the corresponding projected position error is smaller than a given distance ϵ:

$$\mathcal{T}^{\text{err},H}[\mathbf{\Delta H}, \epsilon] = \begin{cases} 1 & \text{if} \quad \delta\mathbf{x}^H[\mathbf{\Delta H}] \leq \epsilon \\ 0 & \text{otherwise} \end{cases} \tag{52}$$

$$\mathcal{T}^{\text{err},V}[\mathbf{\Delta H}, \epsilon] = \begin{cases} 1 & \text{if} \quad \delta\mathbf{x}^V[\mathbf{\Delta H}] \leq \epsilon \\ 0 & \text{otherwise.} \end{cases} \tag{53}$$

A flag of misleading information $\mathcal{T}^{\text{mi}}$ can be defined, equal to 1 only if at least one projected position error exceeds its corresponding protection level:

$$\mathcal{T}^{\text{mi}}[\mathbf{\Delta H}] = 1 - \mathcal{T}^{\text{err},H}[\mathbf{\Delta H}, HPL[\mathbf{\Delta H}]] \times \mathcal{T}^{\text{err},V}[\mathbf{\Delta H}, VPL[\mathbf{\Delta H}]]. \tag{54}$$

Finally, the *position integrity* $\mathcal{P}_{\text{int}}$ can be defined in the temporal (55) or in the statistical (56) domain as

$$\mathcal{P}_{\text{int}}[\mathbf{\Delta g}, \mathbf{\Delta N}, \mathbf{\Delta}\tau, \mathbf{\Delta f}] = \lim_{\kappa\to\infty} \left(\frac{\sum_{j=1}^{\kappa} \mathcal{T}^{\text{mi}}[\mathbf{\Delta g}, \mathbf{\Delta N}, \mathbf{\Delta}\tau, \mathbf{\Delta f}, \mathbf{\Delta}\theta(j)]}{\sum_{j=1}^{\kappa} \mathcal{T}^{\text{ava}}[\mathbf{\Delta g}, \mathbf{\Delta N}, \mathbf{\Delta}\tau, \mathbf{\Delta f}, \mathbf{\Delta}\theta(j)]} \right) \tag{55}$$

$$= \left(\frac{\int_{\Omega} \mathcal{T}^{\text{mi}}[\mathbf{\Delta g}, \mathbf{\Delta N}, \mathbf{\Delta}\tau, \mathbf{\Delta f}, \mathbf{\Delta}\theta] \, \mathrm{d}\mathbf{\Delta}\theta}{\int_{\Omega} \mathcal{T}^{\text{ava}}[\mathbf{\Delta g}, \mathbf{\Delta N}, \mathbf{\Delta}\tau, \mathbf{\Delta f}, \mathbf{\Delta}\theta] \, \mathrm{d}\mathbf{\Delta}\theta} \right). \tag{56}$$

Although Eqs. (55) and (56) give the same result, they propose a different interpretation of the *position integrity*. In Eq. (55), the *position integrity* denotes the percentage of time during the flight in which the estimated position has an error greater than the protection level. In Eq. (56), the *position integrity* denotes the probability that, at a given epoch during the flight where a position is estimated, the estimated position has an error greater than the protection level.

2. Evaluation of the theoretical position availability under onboard meaconing

This subsection provides the theoretical *position availability* $\mathcal{P}_{\text{ava}}$ for different relative parameter values. This section also analyzes and identifies the causes of the *position availability* degradation. First, the probability of activation of the different checks (C/N_0 threshold, CMC test, FD procedure, and PL integrity check) that play a role in the *position availability* are computed. Second, the *position availability* is plotted for different relative parameters representative of onboard meaconing interference.

The probability of activation of the standalone C/N_0 threshold and CMC test can be obtained by calculating the mean value of the checks (Eqs. (31) and (32)) for a given PRN i in the statistical domain, averaged over its relative phase $\Delta\theta_i$. The pseudorange approval checks are still considered deterministic as a function of the relative parameters $\mathbf{\Delta}\eta_i$ in this subsection.

$$\mathbb{P}\left(\mathcal{T}_i^{\text{CN0}}[\Delta g_i, \Delta N_i, \Delta\tau_i, \Delta f_i]\right) = \frac{1}{2\pi} \int_0^{2\pi} \mathcal{T}_i^{\text{CN0}}[\Delta g_i, \Delta N_i, \Delta\tau_i, \Delta f_i, \Delta\theta] \, \mathrm{d}\Delta\theta \tag{57}$$

$$\mathbb{P}\left(\mathcal{T}_i^{\text{CMC}}[\Delta g_i, \Delta N_i, \Delta\tau_i, \Delta f_i]\right) = \frac{1}{2\pi} \int_0^{2\pi} \mathcal{T}_i^{\text{CMC}}[\Delta g_i, \Delta N_i, \Delta\tau_i, \Delta f_i, \Delta\theta] \, \mathrm{d}\Delta\theta \tag{58}$$

The results of Eqs. (57) and (58) are plotted for a GPS signal with a nominal $C/N_0 = 40$ dB.Hz, and a relative frequency $\Delta f = 0.003$ Hz (representative of an average onboard meaconing scenario). Due to the lack of actual data for a generic meaconer noise factor, an ideal meaconer with $NF_m = 0$ dB has been chosen, resulting in the equality $\Delta g = \Delta N$. The probability of activation of the C/N_0 threshold and the CMC test (Eqs. (57) and (58)) is computed for any values of Δg and $\Delta\tau$, and the results are shown in Fig. 9.

In Fig. 9a, the C/N_0 threshold can be activated around $\Delta g = 0$ dB when the relative delay $\Delta\tau$ is smaller than 0.5 chip. The probability of C/N_0 threshold activation does not exceed 15%, because the estimated C/N_0 oscillates with the relative phase

value $\Delta\theta$, as demonstrated in (Hussong et al., 2024c, Fig. 15a). The C/N_0 threshold alone is unlikely to cause a loss of availability. Indeed, the probability $\mathbb{P}_{\text{unav}}^{CN0}$ of being unavailable solely due to the C/N_0 threshold is majored by:

$$\mathbb{P}_{\text{unav}}^{CN0}[N_{\text{sat}}] \leq \mathbb{P}\left(n < 4\right) \qquad \text{with} \qquad n \sim \mathbb{B}\left(N_{\text{sat}}\,;\, 0.15\right) \tag{59}$$

$$\begin{aligned} &\text{When } N_{\text{sat}} = 8\,, \quad \mathbb{P}_{\text{unav}}^{CN0}[8] \leq 0.3\% && \text{When } N_{\text{sat}} = 9\,, \quad \mathbb{P}_{\text{unav}}^{CN0}[9] \leq 0.07\% \\ &\text{When } N_{\text{sat}} = 10\,, \quad \mathbb{P}_{\text{unav}}^{CN0}[10] \leq 0.02\% && \text{When } N_{\text{sat}} = 11\,, \quad \mathbb{P}_{\text{unav}}^{CN0}[11] \leq 0.003\% \end{aligned} \tag{60}$$

The C/N_0 threshold is triggered when $\Delta\tau > 1$ chip, for $10 < \Delta g < 15$ dB. At these relative delays, the jamming situation is observed, resulting in a deterministic degradation of the effective C/N_0 by a factor of $1 + \Delta N = 1 + \Delta g$ as described in Eq. (26). This degradation continues until Δg reaches approximately 15 dB, causing the receiver to lose lock on the authentic signal. Upon losing lock, the receiver reacquires the meaconer signal, leading to a spoofing scenario where the effective C/N_0 increases again, as indicated by Eq. (27). It is important to note that the activation of the C/N_0 threshold is highly influenced by the nominal $C/N_{0,\text{a}} = 40$ dB.Hz in this region of the plots. Different signals with different nominal C/N_0 would activate the C/N_0 threshold in different regions in the plot. Therefore, not all GPS signals may be discarded by this threshold alone at the same time when $\Delta\tau > 1$ chip.

As illustrated in Fig. 9b, the CMC test is triggered when $\Delta g \approx 0$ dB and $\Delta\tau < 1$ chip. However, the FD procedure tends to raise an alert with a significantly higher probability when the CMC test is activated (as explained in the next paragraphs). Consequently, the *position availability* is not notably impacted by the activation of the CMC test on its own.

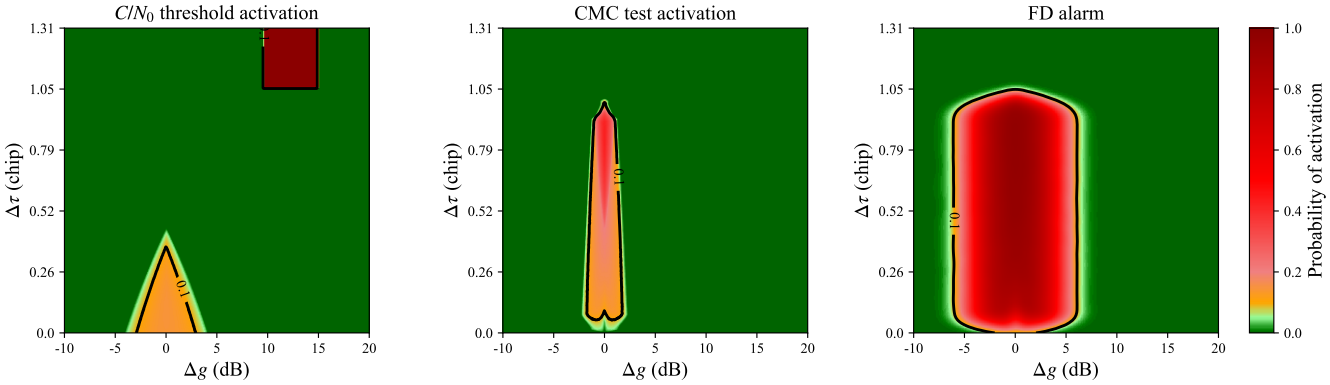

Figure 9: Theoretical probability of activation of the different tests, depending on Δg and $\Delta\tau$.

The probability of activation of the standalone FD procedure can be obtained by calculating the mean value of Eq. (34) in the statistical domain, averaged over the relative phases of the visible satellites $\boldsymbol{\Delta}\theta$:

$$\mathbb{P}\left(\mathcal{T}^{\text{FD}}[\boldsymbol{\Delta}\mathbf{g}, \boldsymbol{\Delta}\mathbf{N}, \boldsymbol{\Delta}\tau, \boldsymbol{\Delta}\mathbf{f}]\right) = \frac{1}{(2\pi)^{N_{sat}}} \int_{\Omega} \mathcal{T}^{\text{FD}}[\boldsymbol{\Delta}\mathbf{g}, \boldsymbol{\Delta}\mathbf{N}, \boldsymbol{\Delta}\tau, \boldsymbol{\Delta}\mathbf{f}, \boldsymbol{\Delta}\theta]\, \mathrm{d}\boldsymbol{\Delta}\theta \tag{61}$$

To perform this computation, 8 visible satellites are assumed, the nominal C/N_0 of the satellites is set to 40 dB, and the relative frequencies $\boldsymbol{\Delta}\mathbf{f}$ are uniformly chosen over $[-0.006\,;\, 0.006]$ Hz, to represent a generic onboard meaconing scenario. The results of (61) are plotted in Fig. 9c. The FD procedure activates when $|\Delta g| < 8$ dB, and the probability of activation increases to 50% or more when $|\Delta g| < 4$ dB. Therefore, the FD procedure is the main cause of the *position availability* reduction when $\Delta\tau < 1$ chip.

The probability of availability loss due to the PL integrity check (54) has been computed similarly to the probability of activation of the FD procedure. The PL check activates in rare occasions and never before the FD procedure in the context of onboard meaconing. Therefore, the reduction in *position availability* due to the PL check alone can be neglected in this study.

The *position availability* is calculated in the statistical domain using Eq. (45), and the results are presented in Fig. 10. This analysis is performed under the same assumptions as those used in the computation of the FD procedure probability of activation. The figure is plotted as a function of the meaconer gain G_m and meaconer delay τ_m, which are more practical parameters to handle compared to Δg and $\Delta\tau$ at the position level, as they are consistent across the different PRNs (unlike Δg and $\Delta\tau$ that differ from one signal to another). The conversion from relative parameters to G_m and τ_m is achieved using Eqs. (1) and (3), with the assumptions $\Delta\tau_{\text{ant}} = 0$ s, $\Delta g_{\text{ant}} = 0$ dB, and $\Delta g_{\text{env}} = -9$ dB. The value of $\Delta g_{\text{env}} = -9$ dB is chosen to match the maximum measured GNSS coupling of -65 dB between the aircraft's GNSS antenna and an onboard GNSS antenna DO235 (2022). Under these assumptions, the relationships between a relative gain Δg_i and the meaconer gain G_m is $\Delta g_i + 65 = G_m$ in dB.

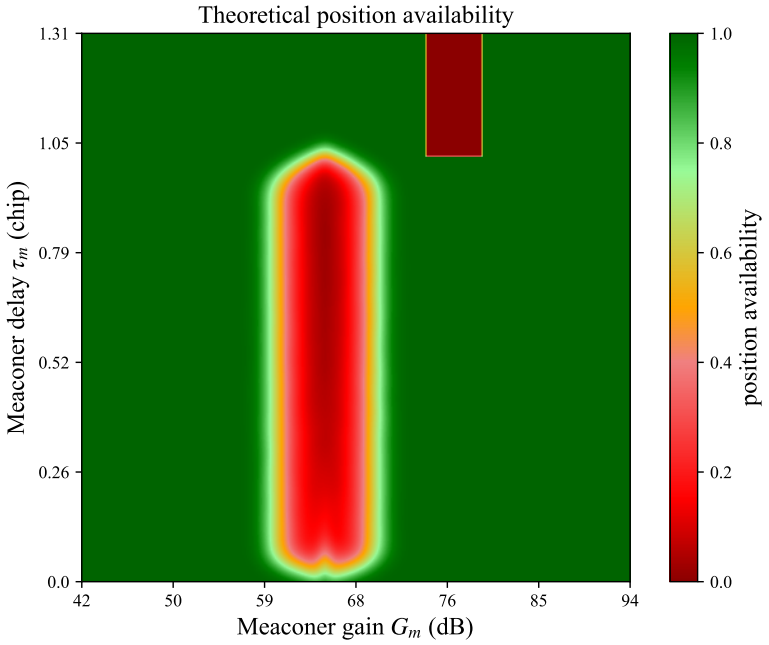

Figure 10: Theoretical *position availability* under onboard meaconing, depending on G_m and τ_m.

Fig. 10 demonstrates significant degradations in availability, primarily caused by the FD procedure when $\Delta\tau < T_{\text{max}} = 1.05$ chip, and by the C/N_0 threshold when $\Delta\tau \geq T_{\text{max}}$. In regions where $\Delta\tau \geq T_{\text{max}}$, the nominal/jamming/spoofing situation is observed, rendering the relative delay irrelevant to GNSS performance and explaining the perfect vertical consistency of the *position availability* in this part of the plot. Fig. 10 indicates that the presence of a meaconer onboard the aircraft could degrade GNSS availability beyond the requirements set by civil aviation standards.

It is important to note that this theoretical computation does not account for the post-SBAS correction pseudorange errors (as it has been calculated with $\tilde{\omega}_i = 0$ in Eq. (24)) and assumes the same C/N_0 across all visible PRNs. These simplifications may lead to discrepancies between the theoretical *position availability* and the simulation results discussed in section V.

3. Theoretical position accuracy under onboard meaconing

To analyze the impact of meaconing on the *position accuracy*, the DLL and PLL SE are computed for various values of Δg and $\Delta\tau$ using Eq. (9). The smoothed SE can then be derived from the DLL and PLL SE using Eq. (21). For these computations, this paper assumes $\Delta g = \Delta N$ and $\Delta f = 0.003$ Hz, which are representative of typical onboard meaconing scenarios. The maximum absolute DLL, PLL, and smoothed SE are calculated with Eqs. (62), (63), and (64), respectively, and are illustrated in Fig. 11.

$$\epsilon_{\tau,\text{max}} = \max_{\Delta\theta\in[0;2\pi]} |\epsilon_\tau[\Delta g, \Delta N, \Delta\tau, \Delta f, \Delta\theta]| \tag{62}$$

$$\epsilon_{\theta,\text{max}} = \max_{\Delta\theta\in[0;2\pi]} |\epsilon_\theta[\Delta g, \Delta N, \Delta\tau, \Delta f, \Delta\theta]| \tag{63}$$

$$\tilde{\epsilon}_{\text{max}} = \max_{\kappa\in\mathbb{R}^+} \left[\; |\tilde{\epsilon}[\kappa]| \;\middle|\; \tilde{\epsilon}[\kappa] = \begin{cases} \frac{1}{\Gamma}\epsilon_\tau[\kappa] + \frac{\Gamma-1}{\Gamma}\left(\tilde{\epsilon}[\kappa-1] + \epsilon_\theta[\kappa] - \epsilon_\theta[\kappa-1]\right) & \text{if available} \\ \epsilon_\tau[\kappa] & \text{otherwise} \end{cases} \right] \tag{64}$$

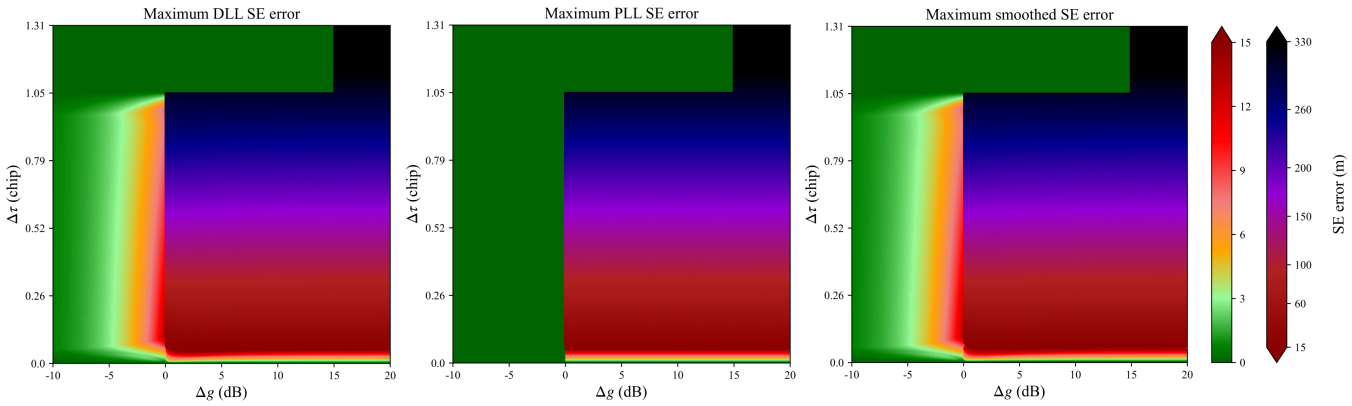

Figure 11: Theoretical DLL, PLL and smoothed absolute SE as functions of Δg and $\Delta\tau$.

In Fig. 11, two distinct behaviors of the SE values are evidenced depending on Δg and $\Delta\tau$. When $\Delta g < 0$ dB and $\Delta\tau < T_{\text{max}}$, the meaconer and authentic signals overlap at the correlator output, and the strongest signal at the receiver antenna is the authentic one, causing the tracking loops to converge close to its characteristics. The tracking loops are considered to start locked on the authentic signal in this figure. The DLL and smoothed SE values reach up to 15 m in this region, while the PLL SE values remain relatively close to 0 m. Conversely, when $\Delta g > 0$ dB and $\Delta\tau < T_{\text{max}}$, the meaconer signal dominates at the correlator output. Consequently, the tracking loops converge around the characteristics of the meaconer signal, leading to SE absolute values of approximately $c\Delta\tau$ meters. Here, the presence of the authentic signal can contribute to additional estimation errors up to 15 m, which are less noticeable compared to the shifted SE values of up to $cT_{\text{max}} \approx 308$ m. When $\Delta\tau \geq T_{\text{max}}$, either a nominal, jamming or spoofing scenario is observed. In these cases, the authentic (in nominal/jamming) or the meaconer (in spoofing) signal is tracked independently, leading to SE absolute values of 0 meter (jamming) or $c\Delta\tau$ meters (spoofing).

The distribution of the smoothed SE can be estimated for each tracked PRN i by accumulating the values $\tilde{\epsilon}_i[\kappa]$ over a sufficiently long time period. From the smoothed SE distributions, the position errors are estimated through a Monte Carlo method. The 99% quantile of the position error distribution (i.e., the *position accuracy*) is plotted in Fig. 12.

Fig. 12 shows that the *position accuracy* generally mirrors the smoothed SE variations from Fig. 11c, except in the region where $G_m > 65$ dB. In this region, the smoothed SE values for all PRNs i are high but consistent with each other, as the signals are all offset by $c\Delta\tau_i$. Thus, the estimated position aligns with the meaconer position, and the additional bias in the smoothed SE is absorbed by the time bias term of the WLSE. Consequently, the mean position error is approximately 10.2 m (the Euclidean distance between the aircraft's antenna and the meaconer), resulting in a *position accuracy* of a similar magnitude.

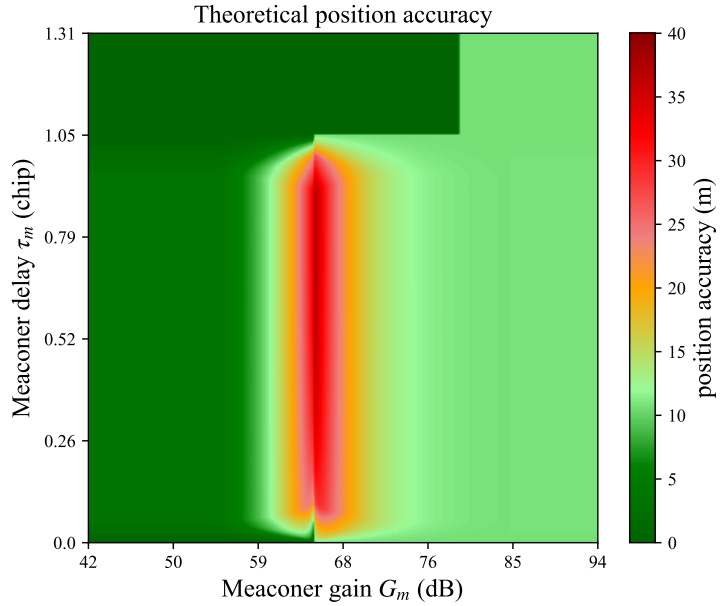

Figure 12: Theoretical *position accuracy* under onboard meaconing, depending on G_m and τ_m.

The position error is also larger when $\Delta g \approx 0$ dB due to the increased and uncorrelated smoothed SE errors. The theoretical *position accuracy* (excluding post-SBAS residual noise and tracking loop estimation noise) can be up to 35 m when $\Delta g \approx 0$ dB. Such position errors are significant for civil aviation safety, as they could exceed protection levels (discussed in the next section). Furthermore, the simulated *position accuracy* might show even larger errors since it incorporates post-SBAS corrections noise and tracking estimation errors in the smoothed pseudorange used for WLSE.

4. Theoretical position integrity under onboard meaconing

The *position integrity* can be estimated like the *position accuracy*, by estimating the distribution of the position errors for every values of Δg and $\Delta\tau$ with a Monte-Carlo method. Then, the *position integrity* is determined by calculating the proportion of the Horizontal Position Error (HPE =$\delta^H \mathbf{x}$) exceeding the HPL, or the Vertical Position Error (VPE $= \delta^V \mathbf{x}$) exceeding the VPL for each couple $(\Delta g; \Delta\tau)$. The results are presented in Fig. 13 and explained below.

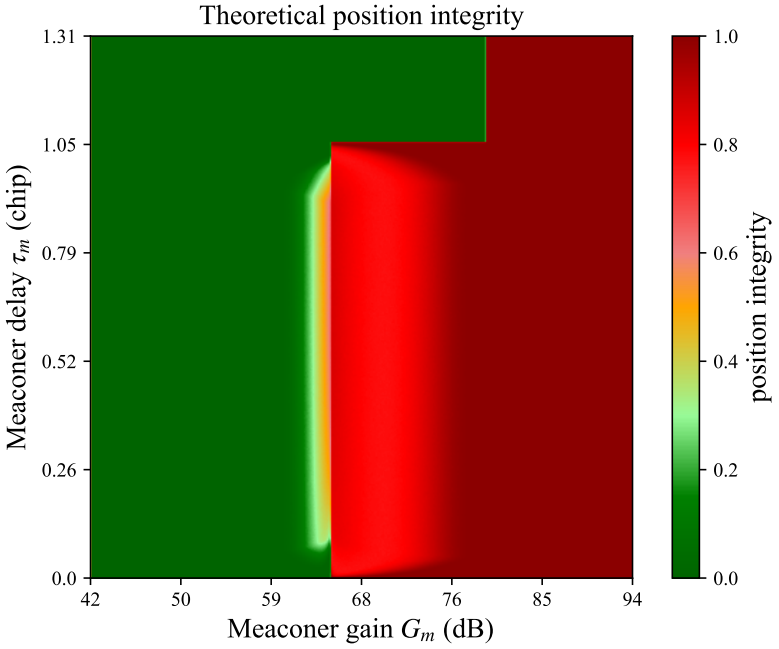

Figure 13: Theoretical *position integrity* under onboard meaconing, depending on G_m and τ_m.

In Fig. 13, the *position integrity* almost equals 1 where $G_m > 76$ dB and $\Delta\tau < T_{\text{max}}$. Indeed, in this region of the plot, the estimated position is centered around the meaconer, located more than 10 m away in the horizontal plane. The horizontal position error (distributed around this distance of 10 m) is likely to exceed the HPL which is around 7 m in this configuration (as it can be observed in Fig. 8). When $G_m \approx 65$ dB, some position errors also exceed the corresponding protection levels. and the *position integrity* is above 0 when $G_m > 62$ dB. A meaconer onboard the aircraft can therefore significantly degrade the integrity of the flight.

When the meaconer gain is smaller than $G_m = 59$ dB, no integrity hazard is detected when neglecting the post-SBAS correction noise in the smoothed pseudoranges, and the estimation errors of the tracking loops. These two additional error sources may increase the *position integrity* once considered, as shown in the next section.

V. SIMULATED GNSS PERFORMANCE DEGRADATION UNDER ONBOARD MEACONING

This section presents the simulation results of the onboard meaconer impact on the *position availability*, *position accuracy*, and *position integrity*. The results are used to validate the theoretical models of section IV by comparing the theoretical GPS degradations to highly-realistic simulation results, obtained from a self-implemented GNSS simulator (including a GNSS receiver). The simulation results consider the values of the implemented tracking loops to estimate the GNSS metrics, including the random deflections of the tracking loops from the SE (not modeled in section IV), and the random post-SBAS correction pseudorange noise affecting the position estimation (also not included in section IV). First, the simulation software and the scenario under scrutiny are presented. Second, the impact of onboard meaconing on this scenario is highlighted with respect to the *position availability*, the *position accuracy*, and the *position integrity*.

1. Simulation software and definition of the simulated scenario

a) Simulation software description

The simulations are performed using a highly-realistic GNSS software named FIVES (for "Simulation Software for Spoofing Scenario Studies"). FIVES generates 7D flight profiles (3D position, 3D orientation, and time) compliant with aircraft dynamics and civil aviation standards. It also computes the satellite positions, velocities, and orientations observed during the flight, using the SPS 24-satellite almanac from U.S. Government (2024). Actual signal processing functions (correlators, acquisition, tracking) are implemented to generate the pseudoranges from the mathematical models of the GNSS signals reaching the user's GNSS antenna. The C/N_0 is estimated using the moment method from the generated correlator outputs. Standardized measurement processing procedures (pseudorange approval checks, WLSE, FD, PL computations) are used to obtain the estimated position at any point during the flight. The series of estimated positions, combined with the corresponding protection

levels, permit the evaluation of GPS performance through the *position availability*, *position accuracy*, and *position integrity* metrics. Additional details on the receiver's architecture and processing logic of FIVES are provided in Hussong et al. (2023).

b) Definition of the scenario under scrutiny

The simulations analyze the *position availability*, *position accuracy*, and *position integrity* metrics for different values of meaconer gain G_m ranging from 42 dB to 94 dB (with a step of 0.1 dB), and different values of the meaconer intrinsic delay τ_m ranging from 0 ns to 1350 ns $\approx$ 1.3 chip (with a step of 2.7 ns). For each combination of G_m and τ_m, FIVES runs 24 different flights of 1 hour, compiling 24 hours of data to estimate the *position availability*, the *position accuracy*, and the *position integrity*.

The 24 flight profiles last 1 hour at $FL300$ with a ground speed of 540 kt. The flights start over Toulouse, France, and proceed eastward in a straight line. Each flight starts 1 hour after the previous one to ensure coverage of all satellite constellations observable over Toulouse, thereby collecting a full day's worth of data.

The aircraft's antenna gain pattern adheres to the standardized model of DO235 (2022), while the meaconer's antennas are omnidirectional. The meaconer noise factor NF_m is set to 0 dB, and both the meaconer frequency and phase offsets f_m and θ_m are set to 0 Hz and 0 rad, respectively.

With a measurement sampling frequency of 1 Hz, 84600 position estimations are attempted over the 24 hours for each (G_m, τ_m) pair. The *position availability*, *position accuracy*, and *position integrity* metrics are computed in the temporal domain according to Eqs. (44), (48), and (55) from this dataset.

2. Simulated position availability under onboard meaconing

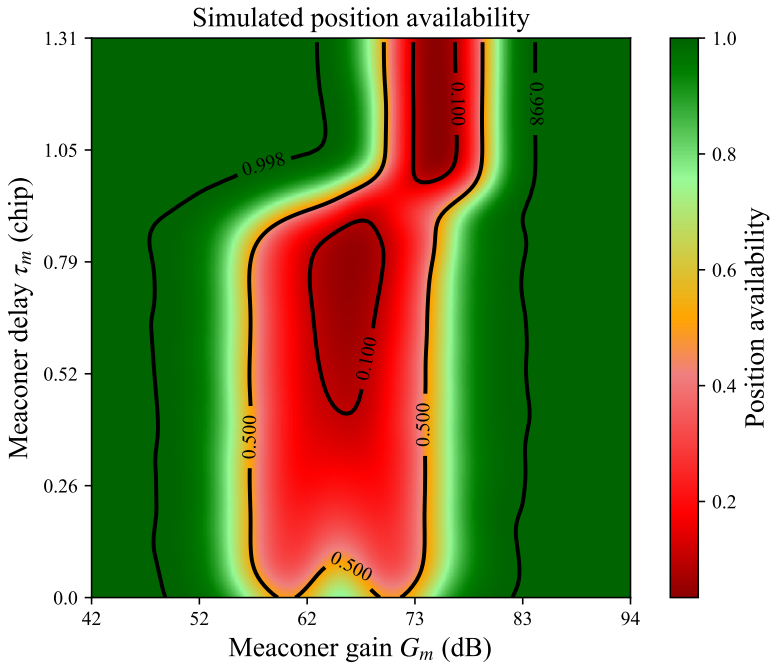

Figure 14: Simulated *position availability* under onboard meaconing, depending on G_m and τ_m.

The simulated *position availability* is shown in Fig. 14. The simulation results align with the theoretical ones of Fig. 10, showing a degradation of the *position availability* around $G_m = 65$ dB when $\tau_m < T_{\text{max}}$ and around $G_m = 75$ dB when $\tau_m \geq T_{\text{max}}$. The *position availability* decreases by up to 90% or more in these regions. The simulated results indicate lower *position availability* than the theoretical results. Particularly, around $G_m \approx 65$ dB, the simulated *position availability* is significantly reduced, exacerbating the severe GNSS availability issue for civil aviation. The discrepancy between theoretical and simulated models is due to three main factors given hereafter.

First, the theoretical results do not account for post-SBAS correction noise in the smoothed pseudorange, which increases the residuals $\mathbf{r}$ and thus the test statistics q of the FD procedure (34), leading to more FD alarms and reduced *position availability*. Second, the theoretical models use the theoretical C/N_0, whereas the simulations use the estimated C/N_0, which includes estimation errors that can reduce the estimated C/N_0 below the threshold (31), thereby reducing the number of usable pseudoranges and decreasing the availability. Third, the theoretical results use deterministic models of the SE to emulate tracking loop outputs, while the simulations use actual tracking loop outputs, which can deviate from the SE with a standard deviation reaching 5 meters (Hussong et al., 2024c, Fig. 15b). This additional error is reflected (after smoothing) in the smoothed pseudoranges, increasing the probability of FD activation and further reducing *position availability*.

3. Simulated position accuracy under onboard meaconing

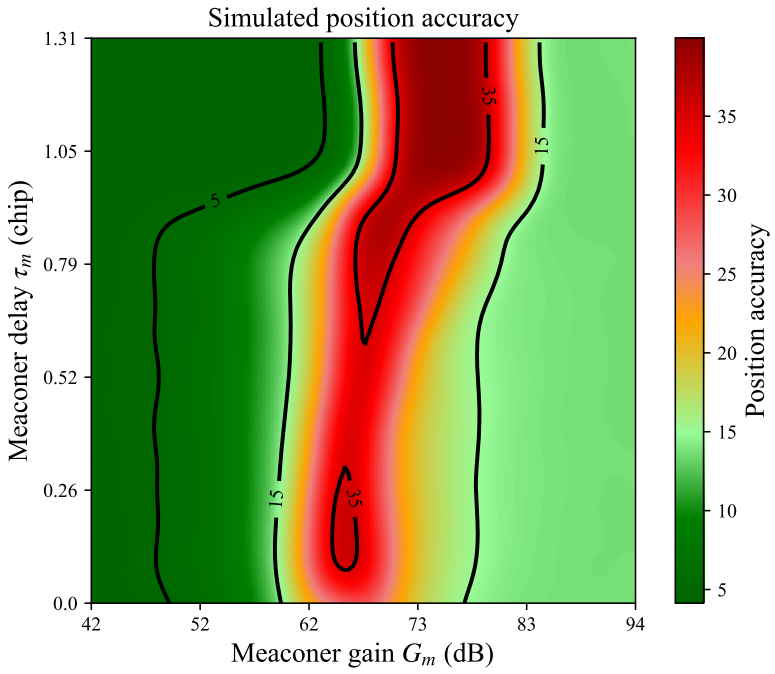

Figure 15: Simulated *position accuracy* under onboard meaconing, depending on G_m and τ_m.

The simulated *position accuracy* is shown in Fig. 15. The simulated *position accuracy* aligns with the theoretical one (Fig. 12) in many aspects. First, the order of magnitude of the theoretical and simulated metrics is identical, with the highest values of the *position accuracy* around 40 meters. Second, the *position accuracy* is approximately 15 meters in both figures when $\Delta g > 75$ dB and $\tau_m < T_{\text{max}}$, and when $\Delta g > 83$ dB and $\tau_m \geq T_{\text{max}}$. Finally, when $\Delta g < 55$ dB, the position error is nearly nominal in both theoretical and simulated cases.

However, some notable differences exist. First, the simulated *position accuracy* is larger than the theoretical one when $G_m < 75$ dB, likely because the simulation accounts for post-SBAS correction errors and tracking estimation errors that increase the smoothed pseudorange noise, resulting in larger position errors after WLSE. Second, in the region where $70 < G_m < 80$ dB and $\tau_m > T_{\text{max}}$, the simulated *position accuracy* is about 40 meters, whereas the theoretical metric is still 0 meters. This difference can be explained because pseudoranges are in the jamming situation in this region, and the meaconer gain is high enough to significantly drop the effective C/N_0 of the measurements. While the effective C/N_0 of some satellites drops below 30 dB.Hz, activating the C/N_0 threshold, the other PRNs (with an effective C/N_0 close but above 30 dB.Hz) suffer huge tracking errors, as modeled by Hussong et al. (2024b). As the number of usable satellites decreases, the Dilution of Precision (DOP) factor increases (Tahsin et al. (2015)). Meanwhile, the remaining usable satellites exhibit greater pseudorange errors. These combined effects increase the position error and the *position accuracy*.

Overall, both simulated and theoretical results indicate that an onboard meaconer can significantly deteriorate the GNSS estimation accuracy, potentially exceeding civil aviation requirements. A small meaconer gain of 60 dB can also impact GNSS availability when the meaconer delay is smaller than T_{max}.

4. Simulated position integrity under onboard meaconing

The simulated *position integrity* is shown in Fig. 16, displaying similarities with the theoretical results of Fig. 13. Both figures indicate a drastic reduction of the *position integrity* when $G_m > 80$ dB, because the estimated position shifts around the meaconer location, exceeding the horizontal protection level. Some differences are also notable between the theoretical and simulated results.

First, the *position integrity* for $55 < G_m < 65$ dB is higher in simulations, because tracking loops estimation errors and post-SBAS correction noise increase the simulated position errors. Second, around $G_m \approx 65$ dB, the simulated *position integrity* is close to 0, whereas the theoretical one is close to 1. This is because, in this region, maximum position errors are around 30 meters (Fig. 15),but the corresponding protection levels are even higher, because the pseudoranges are not getting tracked for long (as the meaconing interferences often degrade the C/N_0 under the tracking threshold, as illustrated by Fig. 6). The smoothed pseudorange errors are therefore higher in this region, as the carrier smoothing filter needs uninterrupted and coherent code and phase measurements to smooth the noise inside the pseudoranges. This larger noise is considered in the protection level computation, as the receiver excepts higher pseudorange noises, and the values of the protection levels increase.

Although the position errors are larger than expected, they are likely to be smaller than the protection levels, reducing the *position integrity*. This increase of the PL is not considered in the theoretical model, explaining the difference between the two results.

Overall, onboard meaconing significantly compromises position integrity, potentially creating integrity threats during critical phases flight. A small meaconer gain of 60 dB can also impact the flight integrity when the meaconer delay is smaller than T_{max}.

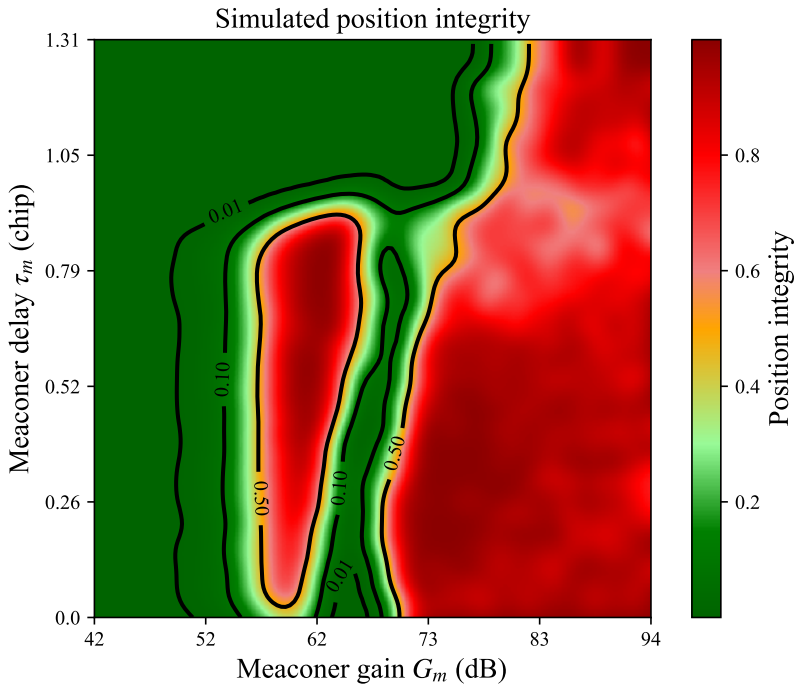

Figure 16: Simulated *position integrity* under onboard meaconing, depending on G_m and τ_m.

VI. CONCLUSION

This paper investigated the impact of meaconing interference on a standardized aircraft GNSS receiver when the meaconer is onboard the aircraft. Onboard meaconing interference are substantially different than meaconing interference from the ground, for four major reasons. First, a smaller meaconer gain is required to reach the aircraft's antenna with sufficient power to corrupt the receiver due to the reduced distance between the meaconer and the aircraft's antenna. Second, the multipath situation can be continuously observed for all the PRNs when the meaconer is onboard, leading to more significant distortions of the estimated tracking loop outputs and C/N_0 compared to the jamming situation mostly observed with a ground meaconer. Third, an onboard meaconer can induce uninterrupted distortions of the GNSS observables that may be less likely identifiable than sporadic distortions caused by ground meaconers. Fourth, if the aircraft's estimated position shifts to the meaconer position, the small but critical position error when the meaconer is inside the aircraft is hardly detectable and could jeopardize the safety of the flight.

Mathematical models, validated by highly realistic simulations, highlighted a significant GNSS performance degradation endured by the aircraft receiver during onboard meaconing scenarios. The ability to estimate a position that can be used for navigation is drastically reduced under onboard meaconing. Both theoretical models and simulation results showed a 90% drop in *position availability* for specific meaconer characteristics, potentially jeopardizing civil aviation availability requirements. The accuracy of the estimated position is also seriously degraded, with position errors of up to 40 meters observed even with SBAS corrections. Some meaconer characteristics lead to a shift of the aircraft's estimated position around the meaconer location. Finally, the integrity of the flight is compromised, exceeding civil aviation integrity requirements. The estimated position can exceed the protection levels in some situations while not being detected by the receiver. All the GNSS performance degradations are observed with a relatively small gain of the meaconer. When the meaconer intrinsic delay is smaller than 1 chip, degradations of the GNSS performances begin from 50 dB of meaconer gain, and large accuracy errors occur around 65 dB of gain. Above this gain, the integrity of the flight is drastically impaired. When the meaconer intrinsic delay is larger than 1 chip, the same degradations are observed, but each time with a meaconer gain about 10 dB higher.

However, some limitations exist in this study. First, only one constellation has been modeled. GNSS performance under onboard meaconing could be improved if the aircraft uses Dual-Frequency Multi-Constellations (DFMC) to estimate its position. Second, this paper assumes that the meaconer is rebroadcasting all the visible GPS signals with the same attenuation, which may not be true if the meaconer is placed closer to a window of the plane that will receive more GPS signal from the satellites in line of sight. Third, the flight was assumed to be a straight line at constant speed without autopilot corrections. The results might be slightly different under other conditions. Finally, the meaconer was assumed to have a noise factor of 0 dB. This value would be larger in a real case, potentially modifying the GNSS performances or changing the conditions to observe the evidenced results.

For these reasons, this paper would benefit from a real experiment of onboard meaconing to compare the results of the study to the actual behavior of a standardized aircraft GNSS receiver. Additionally, extensive investigations could be conducted on the limiting factors exposed in the previous paragraph to quantify the impact of the assumptions made for this study. Even though these limiting factors reduce the trustworthiness of the paper, it highlights the problems raised by meaconers onboard aircrafts, proving their danger in civil aviation and exposing their effects on aircraft receivers.

VII. APPENDICES

1. Example of the onboard meaconing interference on the position estimation, PL computation and FD test statistics, with post-SBAS noise

The equivalent of fig. 8 with the post-SBAS correction noise taken into account is plotted in Fig. 17. The effect of the residual SBAS error on the smoothed pseudoranges is transcribed as Gaussian variations of the estimated terms around the mean values of fig. 8.

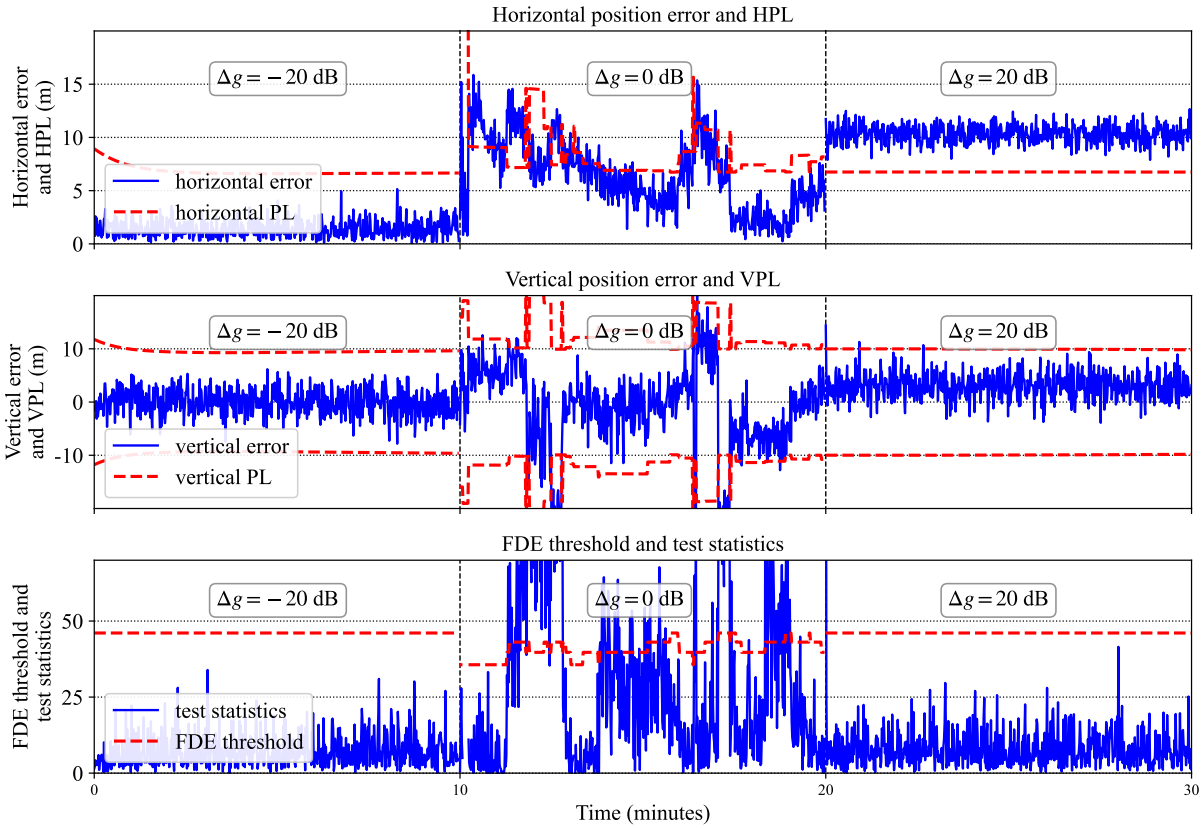

Figure 17: Position errors, PL, number of usable satellites, and FD test statistics during the flight with post-SBAS noise.

2. GPS simulated performances with FDE

For the curious reader, the *position availability*, as well as two new metrics representative of the GNSS accuracy and integrity of the flight are provided when the FD procedure is modified to also exclude the erroneous measurement, when possible. The Fault Detection and Exclusion (FDE) procedure is presented in Hussong et al. (2023), the results when activating FDE are plotted in Figs. 18 to 20 and explained hereafter.

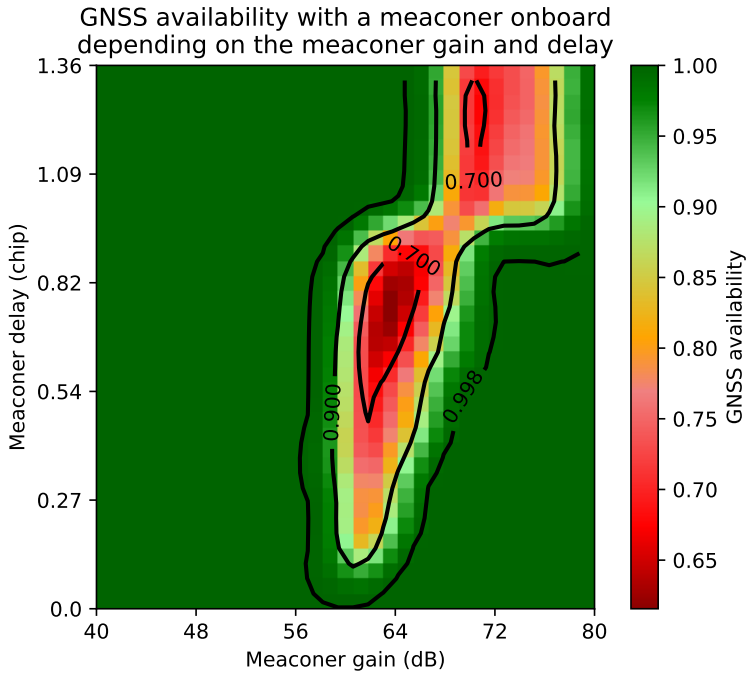

Figure 18: Simulated *position availability* during onboard meaconing with FDE

The *position availability* can be compromised due to several factors with FDE, including:

- The multipath situation degrades the C/N_0 estimations, potentially activating the C/N_0 threshold that removes the low C/N_0 pseudoranges from the position estimation, or even causing losses of lock of the corresponding PRNs that might take time to reacquire.
- The multipath situation causes code pseudorange errors of ± 15 m, that can activate the CMC test and remove the corresponding pseudoranges from the position estimation.
- The multipath situation increases the pseudoranges errors, that can trigger the FDE procedure, producing unusable position estimations.

The *position availability* depicted in Fig. 18 show strong reductions of the ability to compute a position that can be used for positioning under certain gain and delay conditions. Below 56 dB of gain, the meaconer has no significant impact on the availability. Above 74 dB, the availability is also preserved, because the tracking loops follow the meaconer signals instead of the authentic ones. The meaconer needs a smaller gain to affect the GNSS availability when the meaconer delay is smaller than $\tau_m = T_{\text{max}}$, because the correlation peaks of the authentic signal and of the meaconer signal overlap, more easily distorting the tracking loops. If a PRN is spoofed, the greater the delay, the larger the pseudorange error, so a greater delay is more likely to activate the FDE procedure and then to reduce GNSS availability. When the meaconer delay is higher than $\tau_m = T_{\text{max}}$, the delay has no more influence on the GNSS performance, because the correlation peaks of the authentic signal and of the meaconer signal don't overlap anymore. In the worst-case observed scenario, the GNSS availability is only of about 62%, far from the civil aviation requirements. In comparison with the same metric using FD instead of FDE, the *position availability* is higher with FDE than with FD. This is because, when an alarm is raised by the FD test statistics of Eq. (34), the position is not used for positioning with FD. However with FDE, the procedure has a chance to spot the faulty pseudoranges and to remove them from the position estimation before calculating a new position that will be used for positioning. Nevertheless, the same variations of the *position availability* are observed with FDE and with FD.

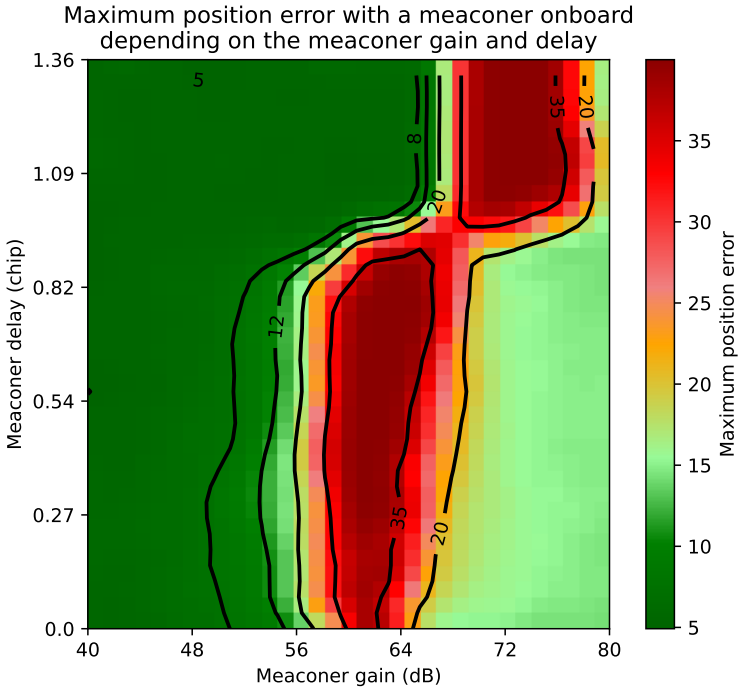

Figure 19: Observed maximum position error during onboard meaconing with FDE

The GNSS accuracy can be degraded due to several factors, including:

- The multipath situation can potentially cause code pseudorange errors of ± 15 m when $\Delta g < 0$, and of $c\Delta\tau$ when $\Delta g > 0$.
- The thermal noise increases during meaconer interference, generating higher pseudorange errors.

The accuracy metric presented in Fig. 18 represents the maximum position error between the actual aircraft position and the estimated position, with FDE. For every meaconer gain and delay, 500 seconds of flight have been simulated and the maximum observed position error is represented. The nominal maximum position errors are about 5 meters and are observed when the meaconer gain is below 40 dB. Above 74 dB, the meaconer might spoof the aircraft receiver, causing a mean error of about 10 meters (the distance between the aircraft antenna and the meaconer receiving antenna around which the position is estimated). Higher position errors can be observed when $G_m \approx 60$ dB and $\tau_m < T_{\text{max}}$, because the smoothed pseudoranges are corrupted by errors of ± 15 m. If the meaconer delay $\tau_m > T_{\text{max}}$ the multipath situation is not observed, and the pseudoranges are either in the nominal, jamming or spoofing situations, which consequences do not longer depend on the meaconer delay. Large positioning errors may be undetected by the FDE procedure when the meaconer causes all but 4 PRNs to be lost or unusable, because the FDE procedure can not detect faulty measurements when only 4 usable pseudoranges are received. The results with FDE in terms of accuracy are similar to the *position accuracy* with FD.

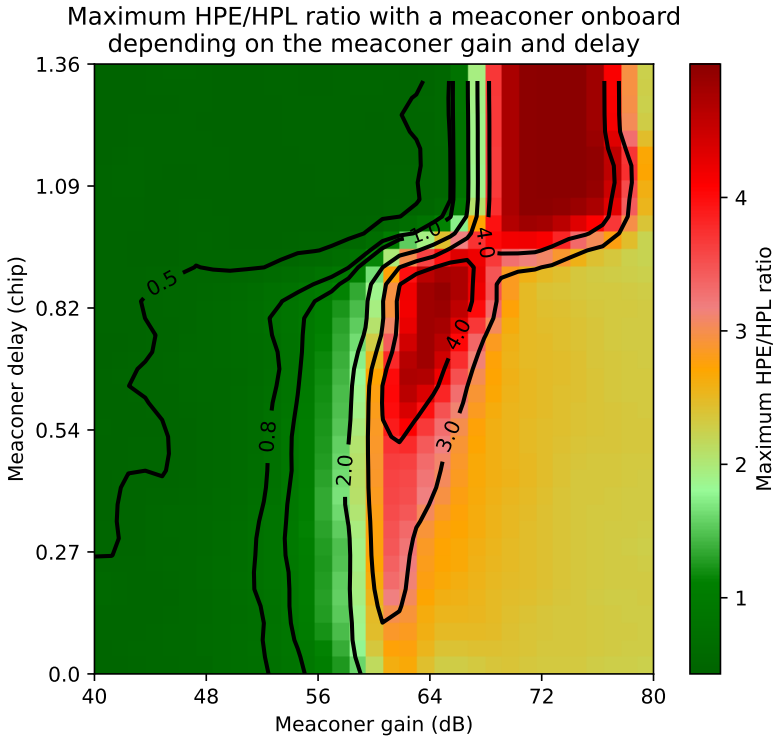

Figure 20: Observed max HPE over HPL ratio during onboard meaconing with FDE

The GNSS integrity can be degraded because the position errors might be larger when exposed to meaconing interference, while the corresponding protection levels may not consider the meaconer induced biases. The integrity metric under scrutiny (here, the maximal observed ratio between the horizontal position errors and the horizontal protection levels, during a 500 second flight) is depicted in Fig. 20. The mean value of this ratio is expected to be around 0.5 in a nominal situation. The ratio exceeds the value 1 for many different meaconer characteristics, causing integrity hazards and demonstrating the potential threat of onboard meaconers, even with FDE.

3. Actual relative parameters variations during a flight in straight line

The actual values of $\Delta g = \Delta N$, $\Delta\tau$, and Δf are provided in Figs. 21 to 23 for a flight of 1 hour in straight line at 540 kt under onboard meaconing. They confirm that $\Delta g = \Delta N$, $\Delta\tau$, and Δf can be considered as constant for simplifications of the models.

The figures have been computed with $\tau_m = 0$ s and $f_m = 0$ Hz, to only represent the impact of the geometrical terms in the calculations of the relative parameters. Different values of τ_m or f_m would have just offset the curves by a constant term, keeping the same variations of the relative parameters.

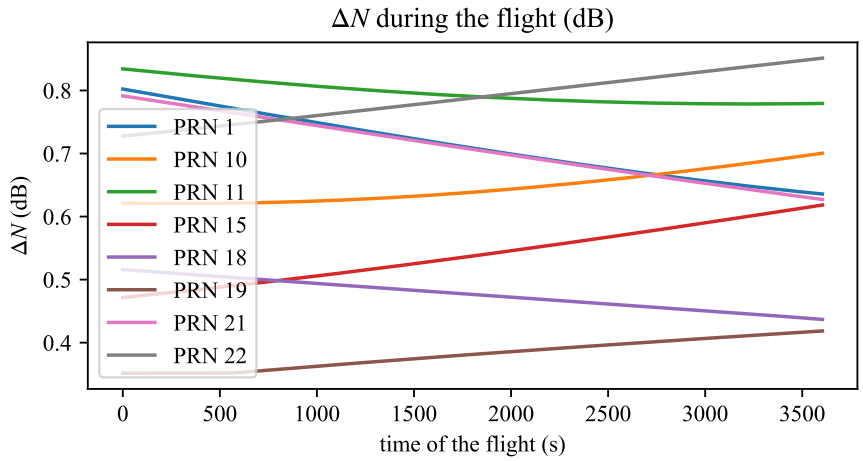

Figure 21: Relative noise ΔN of the visible satellites during a 1-hour flight.

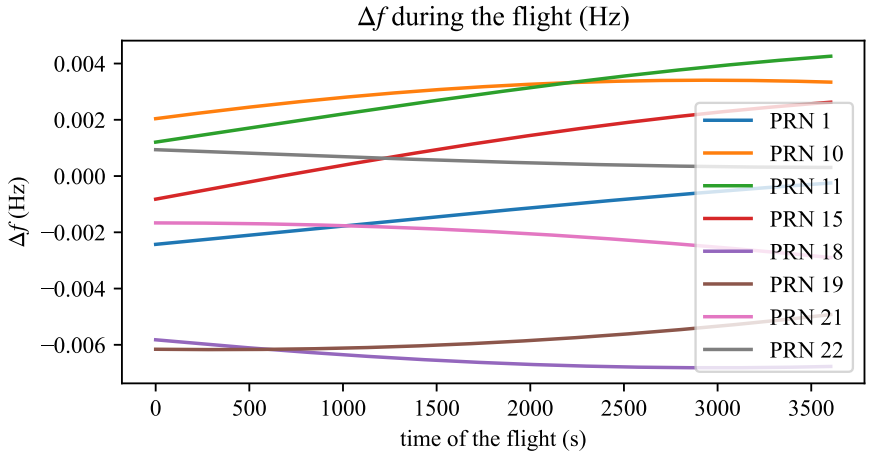

Figure 22: Relative Doppler Δf of the visible satellites during a 1-hour flight.

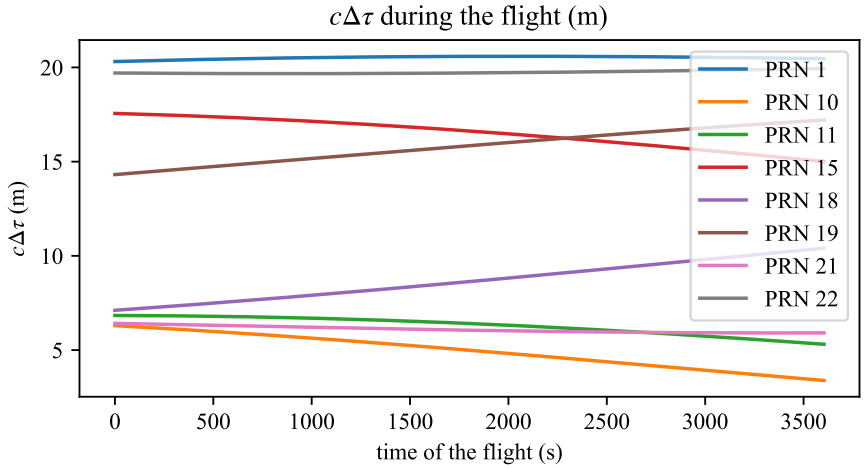

Figure 23: Relative distance $c\Delta\tau$ of the visible satellites during a 1-hour flight.

4. Dependencies of the DLL and PLL SE with respect to the relative phase

The relative phase $\Delta\theta$ that gives the maximum DLL and PLL SE values are plotted in Fig. 24. In this figure, it can be observed that the maximum DLL SE value around $\Delta f = 0$ Hz (corresponding of onboard meaconing scenarios) is obtained at $\Delta\theta = \pi \mod [2\pi]$, whatever the value of $\Delta\tau$.

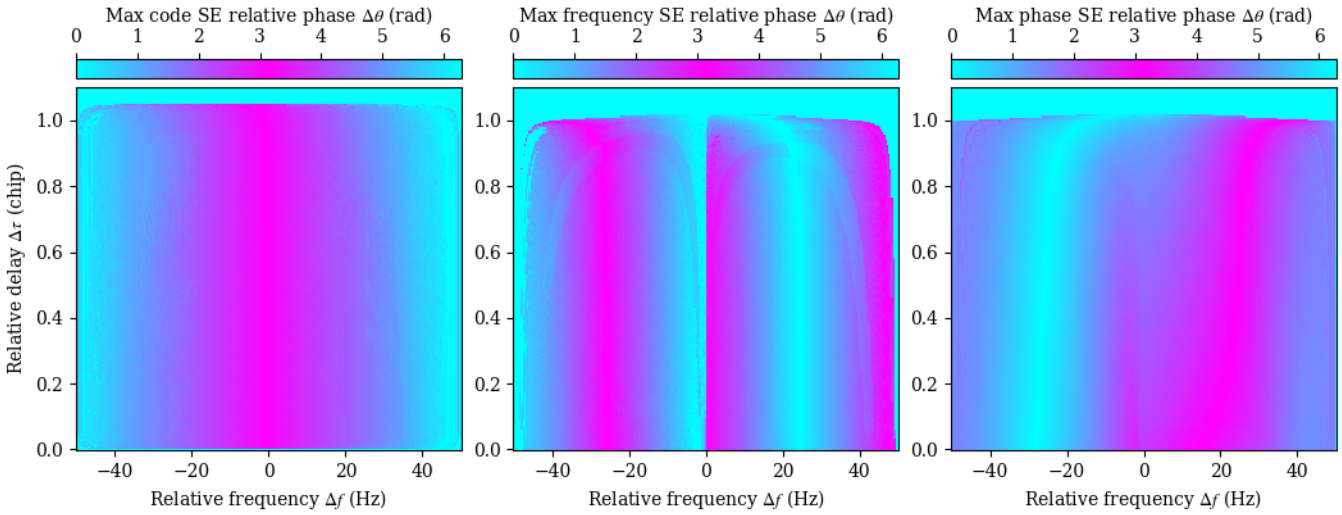

Figure 24: Relative phase $\Delta\theta$ corresponding to the maximum DLL, frequency, and PLL SE.

REFERENCES

Bamberg, T., Appel, M. M., and Meurer, M. (2018). Which GNSS Tracking Loop Configuration is Most Robust Against Spoofing? In *Proc. ION 31st Int. Tech. Meet. Satellite Division (ION GNSS+ 2018)*, pages 3587–3595, Miami, FL, USA.

Coulon, M., Chabory, A., Garcia-Pena, 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 33rd Int. Tech. Meet. Satellite Division (ION GNSS+ 2020)*, pages 3713–3737.

DO229E (2016). *DO 229E - Minimum Operational Performance Standards for Global Positioning System/Satellite-Based Augmentation System Airborne Equipment - 2.5.10.3.1*. RTCA Inc.

DO235 (2022). *DO 235C - Assessment of Radio Frequency Interference Relevant to the GNSS L1 Frequency Band - 2.5.2.1*. RTCA Inc.

Dobryakova, L. and Ochin, E. (2014). On the application of gnss signal repeater as a spoofer. *Zeszyty Naukowe/Akademia Morska w Szczecinie*.

Dovis, F. (2015). *GNSS interference threats and countermeasures*. Artech House.

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

Garcia-Pena, A., Macabiau, C., Novella, G., Julien, O., Mabilleau, M., and Durel, P. (2020). RFI GNSS L5/E5a Mask Derivation. In *Proc. ION 33rd Int. Tech. Meet. Satellite Division (ION GNSS+ 2020)*, pages 188–205.

Ghizzo, E. (2024). Insert here the name of the thesis of Emile. Thesis manuscript, ENAC, Toulouse, France.

Ghizzo, E., Hussong, M., Garcia-Pena, A., Lesouple, J., Milner, C., and Macabiau, C. (2024a). Assessing Spoofer Impact on GNSS Receivers : Tracking Loops. *Signal Processing*.

Ghizzo, E., Pena, A. G., Lesouple, J., Milner, C., and Macabiau, C. (2024b). Assessing GNSS Carrier-to-Noise-Density Ratio Estimation in The Presence of Meaconer Interference. In *Proc. Int. Conf. Acoust., Speech, Signal Process. (ICASSP)*, pages 8971–8975, Seoul, Republic of Korea. IEEE.

Hussong, M., Ghizzo, E., Milner, C., and Garcia-Pena, A. (2024a). GNSS Performance under Meaconing in Civil Aviation: Ground Zones of Impact. *GPS Solutions - **pending***.

Hussong, M., Ghizzo, E., Milner, C., and Garcia-Pena, A. (2024b). GNSS Performance under Meaconing in Civil Aviation: Methodology, Pseudorange and Position Models. *GPS Solutions - **pending***.

Hussong, M., Ghizzo, E., Milner, C., Garcia-Pena, A., and Lesouple, J. (2024c). Characterization of the multipath situation under meaconing interference. In *Proc. ION 37th Int. Tech. Meet. Satellite Division (ION GNSS+ 2023)*, Baltimore, MA, USA.

Hussong, M., Ghizzo, E., Milner, C., Garcia-Pena, A., Lesouple, J., and Macabiau, C. (2023). Impact of Meaconers on Aircraft GNSS Receivers During Approaches. In *Proc. ION 36th Int. Tech. Meet. Satellite Division (ION GNSS+ 2023)*, pages 856–880, Denver, CO, USA.

International Civil Aviation Organization (2022). *Global Aviation Safety Plan 2023–2025*. International Civil Aviation Organization. Doc 10004, Order Number: 10004.

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

Lohan, E. S., Ferre, R. M., Richter, P., Falletti, E., Falco, G., and De La Fuente, A. (2019). Gnss navigation threats management on-board of aircraft. *INCAS Bulletin*, 11(03/2019):111–125.

Peng, C., Li, H., and Lu, M. (2019). Research on the Responses of GNSS Tracking Loop to Intermediate Spoofing. In *Proc. ION 32nd Int. Tech. Meet. Satellite Division (ION GNSS+ 2019)*, pages 943–952, Miami, FL,USA.

Skorupski, J. and Uchroński, P. (2018). Evaluation of the effectiveness of an airport passenger and baggage security screening system. *Journal of Air Transport Management*, 66:53–64.

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 *Proc. Eur. Navigat. Conf. (ENC 2013)*, Wien, Österreich.

Tahsin, M., Sultana, S., Reza, T., and Hossam-E-Haider, M. (2015). Analysis of dop and its preciseness in gnss position estimation. In *2015 International conference on electrical engineering and information communication technology (ICEEICT)*, pages 1–6. IEEE.

U.S. Government (2024). Official u.s. government information about the global positioning system (gps) and related topics. Accessed: 2024-07-29.