Assessing jamming and spoofing impacts on GNSS receivers: Automatic gain control (AGC)

Emile Ghizzo, El-Mehdi Djelloul, Julien Lesouple, Carl Milner, Christophe Macabiau

Assessing jamming and spoofing impacts on GNSS receivers: Automatic gain control (AGC)

Emile GHIZZO[a,*], El-Mehdi DJELLOUL[a], Julien LESOUPLE[a], Carl MILNER[a], Christophe MACABIAU[a]

[a] *Fédération ENAC ISAE-SUPAERO ONERA, Université de Toulouse, 7 Avenue Édouard Belin, 31400, Toulouse, France*

Abstract

In modern GNSS receivers, the Automatic Gain Control (AGC) monitors the received signal level to optimize quantization and mitigate interference. This paper characterizes the jamming and spoofing impact on AGC and received signal. It first expresses the AGC gain as a function of the received signal level. Under nominal conditions, the AGC leverages the ergodic properties of the received signal to estimate its level over time. Two physical quantities, namely time-based power and signal distribution, are typically considered. However, in the presence of interference, these ergodic properties are no longer guaranteed, posing challenges in modeling the behavior of these quantities. This paper proposes a probabilistic framework for interpreting temporal estimation and computing time-based power and distribution in order to characterize AGC gain under jamming and spoofing. First, this study models the spoofing impact for both unique and multiple emitted spoofing signals as a function of the re-radiated noise power and the spoofing signals' characteristics (e.g., number of emitted signals, amplitudes, modulation). Furthermore, it reveals the non-uniformity of jamming chirp phase, which introduces distortions in power and signal distribution, consequently affecting AGC gain, and demonstrates the convergence of the jamming signal toward a continuous wave signal at high frequencies.

Keywords: AGC, spoofing, jamming, time-based estimation, signal distribution, ergodicity

1. Introduction

Global Navigation Satellite Systems (GNSS) have become indispensable for precise positioning and temporal synchronization. GNSS technology is utilized in terrestrial, aerial, and maritime navigation, as well as for timing in critical infrastructure and automated processes. However, this widespread dependence on GNSS introduces vulnerabilities that, if maliciously exploited, can lead to significant consequences. Among these threats, Radio Frequency Interference (RFI), including jamming and spoofing, are particularly insidious [1].

On one hand, GNSS jamming involves the deliberate or inadvertent transmission of radio-frequency signals within the GNSS band, capable of overpowering legitimate GNSS signals and degrading reception and accuracy. Extensive research has been conducted to address this issue and contribute to the understanding of jamming signals [2, 3]. This research has led to the following classification [3, 4, 5]:

1. Continuous Wave (CW): the jammer broadcasts a CW signal with a constant frequency.
2. Single chirp: the jammer transmits a frequency-modulated signal with a saw-tooth time-frequency (TF) evolution.
3. Multi-saw-tooth chirp signals: the device emits a frequency-modulated signal with a more complex TF evolution determined by the combination of several saw-tooth functions.
4. Pulsed signal: the jammer transmits a pulsed signal.
5. Narrow-band (NB): the device broadcasts narrow-band Gaussian noise.

On the other hand, a GNSS spoofer is a device capable of generating or re-radiating counterfeit GNSS signals, being able to deceive a receiver and to induce erroneous Position, Velocity, and Time (PVT) solutions. Spoofing signals are typically categorized based on their level of sophistication [6]. However, for the analysis of the impact of spoofers on the pre-correlation stage, a simpler classification can be used based on the number of transmitted signals:

1. Single PRN spoofer: a unique GNSS signal is transmitted.
2. Multiple PRN spoofer: at least two signals are broadcast simultaneously.

The Automatic Gain Control (AGC) is an essential component of modern GNSS receiver RF Front-Ends (RFFE), which monitors the amplitude of the received signal to maintain it at a fixed level at the input of the Analog-to-Digital Converter (ADC) and minimize quantization losses. The AGC typically comprises a feedback amplifier with a closed-loop architecture, as illustrated in Fig. 1, which includes a Variable Gain Amplifier (VGA), a detector, and a low-pass filter [7, p. 15]. The received signal is first amplified by the VGA. Subsequently, the detector measures the output signal level, which is compared with a reference level and filtered by the low-pass filter. The output of the filter is then utilized to adjust the gain of the VGA. To stabilize the signal envelope, the AGC is commonly implemented at Intermediate Frequency (IF). Various detector

*Corresponding author
Email address: emile.ghizzo@alumni.enac.fr (Emile GHIZZO)

methods are employed to measure the signal level, operating in both analog and digital domains [8, p.383].

The effectiveness of AGC in the presence of interference is a significant focus in the literature. Initially, the impact of RFI on AGC was primarily examined for CW interference [9, 10, 11]. The distribution of received CW was analyzed in [9], and its impact on signal distribution in an Additive White Gaussian Noise (AWGN) channel was studied in [10] to characterize AGC gain, ADC quantization losses, and induced Bit Error Rate (BER) degradation. Moreover, [11] investigated the behavior of distribution and power-based AGC in the presence of CW jamming interference, proposing an estimator for jamming signal power.

Furthermore, the impact of pulsed interference on receiver performance has been extensively studied, particularly in the context of the GPS L5 band in the presence of DME/TACAN interference [12, 13, 14, 15, 16]. ADC quantization losses and Signal-to-Noise Ratio (SNR) degradation in the presence of L5 pulsed interference were analyzed in [13]. Similarly, [14] examined the influence of the AGC on receiver BER and post-correlation Carrier-to-Noise density ratio (C/N_0) in the presence of pulsed interference. Additionally, both [15] and [16] investigated the impact of pulse blanking on receiver performance.

The distortion of the AGC directly impacts the quantification and subsequent signal processing stages [17, 18]. The impact of CW on the synchronization process is analyzed in [19]. Additionally, [20] studies the tracking performance under jamming or multipath, while [21] examines the impact of a spoofer on C/N_0 estimators.

Finally, AGC utilization has been widely applied in the context of jamming [22, 4, 11] and spoofing [23, 5, 24, 25] detection. These studies have investigated the impact of jamming and spoofing on AGC through data collection and experimental tests. For instance, [26] analyzed the AGC levels recorded at two different airports to monitor RFI attacks. Similarly, [25] examined the spoofing impact on AGC using aircraft receiver recordings of GNSS data. [27] proposes a method for mitigating chirp interference. Moreover, in studies such as [4, 28], an experimental benchmark was developed to assess the impact of jamming signals on GNSS receivers. This evaluation analyzed the effects on the RF front-end, acquisition, tracking loops, and position computation stages for both CW and chirp signals. Additionally, [5, 24] proposed a classification of combined AGC gain and C/N_0 behavior based on measurements for jamming and spoofing detection and characterization.

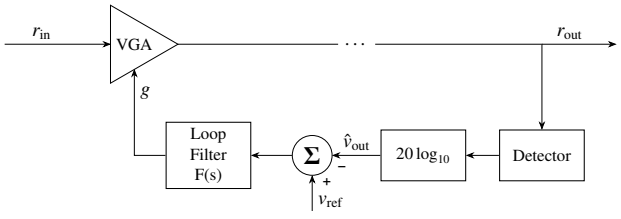


Figure 1: Typical architecture of an AGC (symbol '...' represents no block or a block that does not change the signal level).

To summarize, understanding the impact of jamming and spoofing on AGC is crucial for enhancing the resilience of GNSS receivers. Developing a model of AGC in the presence of RFI would enable the computation of induced quantification losses, dependent on the interference and its parameters, and pinpoint the most threatened AGC architectures. Furthermore, better predictions of VGA gain behaviors would facilitate the development of more sophisticated detection methods. While the impacts of CW and pulsed interference have been extensively studied in the literature, to the best of the authors' knowledge, existing models have not addressed the characterization of the impact of spoofing and chirp jamming on the AGC. Indeed, in the presence of jamming and spoofing, the received signal no longer exhibits ergodic properties, posing challenges in modeling the signal level estimated over time. Signal processing under non-ergodic conditions is discussed, for example, in [29, 30, 31].

This paper investigates the impact of jamming and spoofing on AGC and the received IF signal, and proposes a probabilistic framework for interpreting time-based estimation with non-ergodic signals, such as jamming and spoofing RFI. In that purpose, Sec. 2 introduces the received signal model at the AGC input, while Sec. 3 analyses the dynamic behavior of the AGC to model its gain in the steady state in the presence of RFI. To perform time-based estimation over ergodic and non-ergodic signals, Sec. 4 introduces mathematical definitions along with properties pertaining to time-based distribution and power, allowing the characterization of spoofing and jamming impacts on the AGC in Secs. 5 and 6 respectively.

2. Received signal

This section introduces the model of the received IF signal at the VGA input (see Fig. 1). The analog IF signal r_{in} can be expressed over one estimation interval I_t (typically $I_t = [\tau, \tau + T]$) as

$$r_{\text{in}}(t) = \Re\left\{x(t)\exp\left(j2\pi f_{\text{IF}}t + j\theta_{\text{IF}}\right)\right\}, \quad t \in I_t \tag{1}$$

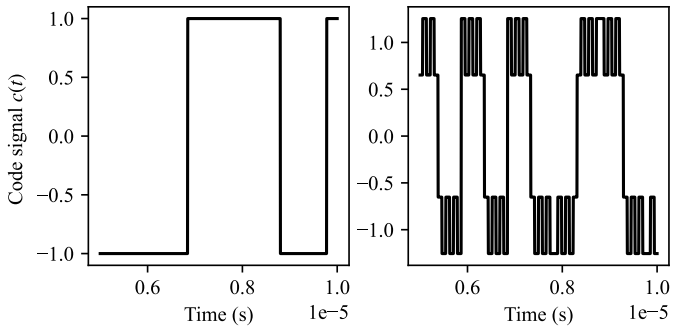
where $\Re\{\cdot\}$ is the real part operator, f_{IF} is the receiver IF, θ_{IF} the phase offset induced by down-conversion and filtering, and x represents the signal's complex representation after filtering. The baseband signal x is defined as

$$x(t) = x_{\text{a}}(t) + x_{\text{s}}(t) + \nu_{\text{a}}(t) + \nu_{\text{s}}(t) + x_{\text{j}}(t) \tag{2}$$

with x_{a} the nominal (authentic) GNSS signal, x_{s} the spoofing GNSS signal, ν_{a} the nominal AWGN, ν_{s} the additional AWGN re-radiated by the spoofer, and x_{j} the jamming signal (potentially containing AWGN). In the remainder of the paper, the nominal GNSS signal x_{a} is assumed to be negligible in comparison to AWGN ν_{a}. Thus, the received signal at the VGA input can be expressed as

$$r_{\text{in}}(t) = r_{\text{s}}(t) + n_{\text{a}}(t) + n_{\text{s}}(t) + r_{\text{j}}(t) \tag{3}$$

where $r_{\text{s}}(t) = \Re\left\{x_{\text{s}}(t)\exp\left(j2\pi f_{\text{IF}}t + j\theta_{\text{IF}}\right)\right\}$ represents the spoofing GNSS signal, $n_{\text{a}}(t) = \Re\left\{\nu_{\text{a}}(t)\exp\left(j2\pi f_{\text{IF}}t + j\theta_{\text{IF}}\right)\right\}$



(a) BPSK (b) BOC

Figure 2: PRN codes modulation.

the nominal AWGN, $n_s(t) = \Re\{\nu_s(t)\exp(j2\pi f_{IF}t + j\theta_{IF})\}$ the additional AWGN re-radiated by the spoofer, and $r_j(t) = \Re\left\{x_j(t)\exp(j2\pi f_{IF}t + j\theta_{IF})\right\}$ the jamming signal. These different terms are elaborated upon in the subsequent subsections.

2.1. AWGN signals

At the VGA input, the nominal AWGN n_a is defined as a centered normal random variable $n_a \sim \mathcal{N}(0, P_{n,a})$, and the re-radiated AWGN as $n_s \sim \mathcal{N}(0, P_{n,s})$, with $P_{n,a}$ and $P_{n,s}$ respectively representing the nominal and re-radiated noise powers. Both AWGN processes have ergodic properties and are assumed to be independent. Additionally, let P_n denote the total AWGN power, defined as

$$P_n = P_{n,a} + P_{n,s}. \tag{4}$$

2.2. Spoofing signal

While the power of the nominal GNSS signal is significantly lower than the noise level, the spoofing signal may be broadcast at a power level that affects the AGC gain. Such a scenario may arise when a non-sophisticated simulator broadcasts at excessively high power or when the receiver is in close proximity to a spoofer targeting another device farther away [32, 18].

Single PRN spoofer:

In the case of a single PRN spoofer, a unique GNSS signal $r_s : I_t \to I_s$ is emitted, where $I_s = r_s(I_t)$, defined as [8, chap.14]

$$r_s(t) = a_s\, d(t-\tau_s)\, c(t-\tau_s)\cos(2\pi f t + \theta_s) \tag{5}$$

with d representing the spoofing BPSK navigation signal, c the modulated Pseudo-Random Noise (PRN) signal, a_s the spoofing signal amplitude, τ_s the spoofing code delay, θ_s the initial phase offset such that $\theta_s \sim \mathcal{U}([0, 2\pi])$, and f the spoofing signal frequency given by $f = f_s + f_{IF}$, which includes the IF plus additional Doppler shift f_s. While the code, phase, and frequency τ_s, θ_s, and f_s may vary with time, it is reasonable to approximate these values as constant within the estimation time interval I_t involved in AGC processing. In this paper, two modulations, namely BPSK and CBOC [33], are considered for the PRN code c, as shown in Fig. 2.

Multiple PRN spoofer:

In the case of a multiple PRN spoofer, M spoofing signals are emitted, such that [8, chap.14]

$$r_s(t) = \sum_{m=1}^{M} a_{s,m}\, d_m(t-\tau_{s,m}) c_m(t-\tau_{s,m})\cos(2\pi f_m t + \theta_m) \tag{6}$$

with m indexing the m-th satellite for parameters defined in (5). The phases $(\theta_m)_{m\in[\![1;M]\!]}$ are assumed to be mutually independent and uniformly distributed over $[0, 2\pi]$.

2.3. Jamming signal

The jamming chirp signal can be expressed by its complex representation as [3]

$$x_j(t) = a_j \exp\left(j\theta_0 + j2\pi \int_0^{t-\tau_p} f_i(u)\,\mathrm{d}u\right) \tag{7}$$

where a_j is the jamming signal amplitude, τ_p the jammer to receiver propagation delay, θ_0 the jamming phase offset and f_i the instantaneous frequency with periodic patterns. In this paper, we consider a linear frequency as [3]

$$f_i(u) = \Delta f_c - \frac{B_j}{2} + \frac{B_j}{T_{sw}}\left(u - \left\lfloor \frac{u}{T_{sw}} \right\rfloor T_{sw}\right) \tag{8}$$

where $\lfloor\cdot\rfloor$ denotes the floor operator, B_j the chirp bandwidth, T_{sw} the chirp period, and Δf_c the jammer frequency offset compared to the GNSS carrier frequency f_{IF}. All these terms are represented in Fig. 3. This particular formulation leads

$$x_j(t) = a_j \exp\left\{j\theta_0 + j2\pi\left(\Delta f_c - \frac{B_j}{2}\right)\left(t - \tau_p - nT_{sw}\right) + j2\pi\Delta f_c nT_{sw} + j\pi\frac{B_j}{T_{sw}}(t-\tau_p-nT_{sw})^2\right\} \tag{9}$$

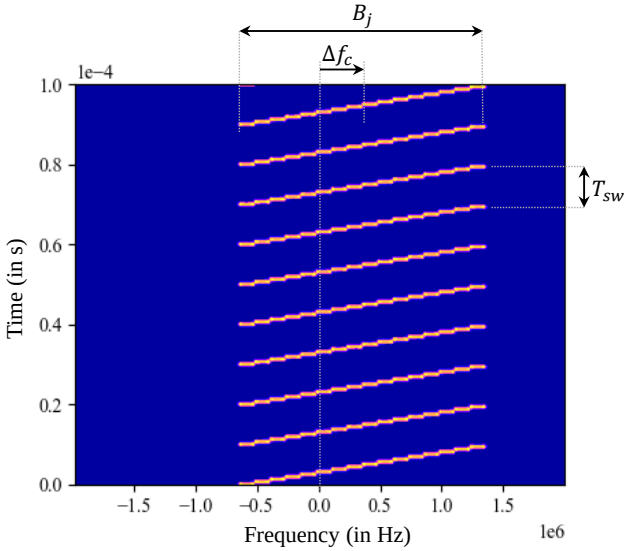


Figure 3: Spectral evolution of chirp jamming signal ($T_{sw} = 10\,\mu$s, $B = 2$ MHz, $\Delta f_c = 353$ kHz)

where n represents the index of the sweep period, such that

$$n = \left\lfloor \frac{t - \tau_\mathrm{p}}{T_\mathrm{sw}} \right\rfloor. \tag{10}$$

Therefore, the analog jamming signal $r_\mathrm{j} : I_t \to I_\mathrm{j}$ at the VGA input can be expressed as

$$r_\mathrm{j}(t) = \Re\left\{x_\mathrm{j}(t)\exp\left(j2\pi f_\mathrm{IF}t + j\theta_\mathrm{IF}\right)\right\} = a_\mathrm{j}\cos\left(\phi_\mathrm{j}(t)\right) \tag{11}$$

where $\phi_\mathrm{j} : I_t \to I_\phi$ is the jamming phase, with $I_\phi = \phi_\mathrm{j}(I_t)$, expressed as

$$\phi_\mathrm{j}(t) = \theta_\mathrm{j} + 2\pi\left(f_j - \frac{B_\mathrm{j}}{2}\right)\left(t - \tau_p - nT_\mathrm{sw}\right) \tag{12}$$

$$+ \pi\frac{B_\mathrm{j}}{T_\mathrm{sw}}(t - \tau_p - nT_\mathrm{sw})^2 + 2\pi f_\mathrm{j} nT_\mathrm{sw} \tag{13}$$

with $\theta_\mathrm{j} = \theta_\mathrm{IF} + 2\pi f_\mathrm{IF}\,\tau_p + \theta_0$ the resulting random phase offset and $f_\mathrm{j} = f_\mathrm{IF} + \Delta f_\mathrm{c}$ the jamming mean frequency. θ_j is considered uniform over $[0, 2\pi]$. The jamming phase ϕ_j can also be expressed as

$$\phi_\mathrm{j}(t) = \phi_\mathrm{sw}(t - nT_\mathrm{sw}) + \Delta\phi_m \tag{14}$$

where ϕ_sw is the periodic part defined for $t - \tau_\mathrm{p} \in I_\mathrm{sw} = [0, T_\mathrm{sw}]$ as

$$\phi_\mathrm{sw}(t) = \pi\frac{B_\mathrm{j}}{T_\mathrm{sw}}\left(t - \tau_\mathrm{p}\right)^2 + 2\pi\left(f_j - \frac{B_\mathrm{j}}{2}\right)\left(t - \tau_\mathrm{p}\right) + \theta_\mathrm{j} \tag{15}$$

and $\Delta\phi_n$ the phase shift at the n-th interval expressed as

$$\Delta\phi_n = 2\pi f_\mathrm{j}\, nT_\mathrm{sw}. \tag{16}$$

The periodic phase component ϕ_sw is plotted with $f_\mathrm{j} \in \{0.3, 2.5\}$ MHz in Fig. 4. In this paper, we consider the estimation duration T to be much larger than the sweep period T_sw, allowing to assume that an integer number of sweep periods spans I_t ($T \approx NT_\mathrm{sw}$). Additionally, as the signal is periodic, we can assume that ϕ_j and ϕ_sw are synchronized at the beginning of I_t, such that $\tau_\mathrm{p} = 0$. Under these approximations,

$$\phi_\mathrm{sw}(t) = \pi\frac{B_\mathrm{j}}{T_\mathrm{sw}}t^2 + 2\pi\left(f_\mathrm{j} - \frac{B_\mathrm{j}}{2}\right)t + \theta_\mathrm{j}. \tag{17}$$

3. AGC GAIN MODEL

As depicted in Fig. 1, the AGC employs a feedback structure to monitor the VGA gain g (in dB). This section models the dynamic behavior of the AGC as a function of the signal level (further defined in Sec. 3.1). Throughout the paper, we denote r_in (in V) as the input signal, r_out as the signal at the VGA output, $\hat{v}_\mathrm{out}$ as the estimated signal level at the detector output (in dBm), and v_ref as the reference level (in dBm). Additionally, v_out (resp. v_in) defines the true signal level of signal r_out (resp. r_in) (in dBm).

3.1. Signal level

The signal level v allows characterizing the occurrence of the values of the signal r within the interval $I_t = [\tau, \tau + T]$. In AGC, two physical quantities, namely time-based power and signal distribution, are typically estimated by the detector to represent the signal level.

- The power-based signal level measures the root average power within the time interval I_t and is defined as [8, chap.13]

$$v(\tau) = 10\log_{10}\left(P_t(\tau)\right) = 10\log_{10}\left(\int_{t\in I_t} r(t)^2\mathrm{d}t\right). \tag{18}$$

  with P_t the time-average power.

- The distribution-based signal level measures the proportion of signal distribution above a certain threshold $T_\mathrm{h} \in [0, 1]$, i.e. $\mathbb{P}_t\left(|r| > 10^{v(\tau)/20}\right) = T_\mathrm{h}$, with $\mathbb{P}_t(A)$ the proportion of time where A is satisfied within I_t (also referred to as time-based distribution) [8, chap.13]. The signal level can be expressed as a function of the time-based signal distribution p_r within the time interval I_t, such that

$$v(\tau) = 20\log_{10}\left(\eta^{-1}\left(T_\mathrm{h}\right)\right) \tag{19}$$

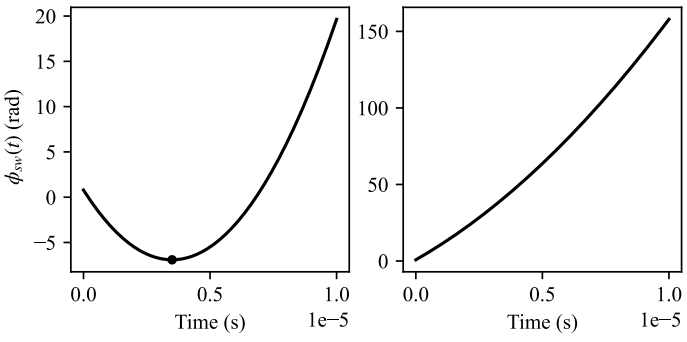
  with $\eta : \mathbb{R}^+ \to [0, 1]$ defined as

$$\eta(\kappa) = \mathbb{P}_t(|r| > \kappa) = 1 - \int_{-\kappa}^{\kappa} p_r(r)\,\mathrm{d}r. \tag{20}$$

3.2. Model assumptions

The AGC behavior is characterized under the following assumptions:

1. The detector perfectly estimates the real signal level v_out, such that
$$\hat{v}_\mathrm{out}(\tau) = v_\mathrm{out}(\tau). \tag{21}$$
2. The VGA operates in its linear mode, such that [34, p.254]
$$r_\mathrm{out}(\tau) = 10^{g(\tau)/20}\, r_\mathrm{in}(\tau) \tag{22}$$
or equivalently considering the signal level log-parameters
$$v_\mathrm{out}(\tau) = g(\tau) + v_\mathrm{in}(\tau). \tag{23}$$



(a) f_j = 0.3MHz (b) f_j = 2.5MHz

Figure 4: Periodic phase component ϕ_sw ($T_\mathrm{sw} = 10\,\mu$s, $B = 2$ MHz, $\theta_\mathrm{j} = \frac{\pi}{4}$).

3. The AGC time response is sufficiently fast compared to the signal level dynamics to allow the system to converge toward its steady state.

3.3. Gain closed-loop model

As depicted Fig. 1, the VGA gain can be expressed in the Laplace domain as

$$g(s) = F(s)\,(v_{\text{ref}}(s) - \hat{v}_{\text{out}}(s)) \tag{24}$$

where s is the variable of the Laplace Transform and $F(s)$ is the AGC low-pass filter transfer function. From the assumptions (21) and (23), the gain model (24) can be expressed as

$$g(s) = \frac{F(s)}{1 + F(s)}\,(v_{\text{ref}}(s) - v_{\text{in}}(s))\,. \tag{25}$$

Equivalently, defining the closed-loop error ε_g as

$$\varepsilon_g(s) \stackrel{\Delta}{=} v_{\text{ref}}(s) - v_{\text{in}}(s) - g(s), \tag{26}$$

the gain model (24) can be expressed as

$$\varepsilon_g(s) = v_{\text{ref}}(s) - v_{\text{in}}(s) - F(s)\,\varepsilon_g(s). \tag{27}$$

The model (27) is referred to as the gain closed-loop model and is illustrated in Fig. 5. In typical AGC systems, a first-order low-pass filter is commonly implemented, as described in [34, p.262], and expressed as

$$F(s) = \frac{\kappa_0}{s} \tag{28}$$

with κ_0 the filter coefficient (in s^{-1}). Considering the filter transfer function (28) in (27), the gain can be represented in the time domain by the differential equation

$$\frac{\text{d}\varepsilon_g}{\text{d}\tau} + \kappa_0\,\varepsilon_g = \frac{\text{d}v_{\text{ref}}}{\text{d}\tau} - \frac{\text{d}v_{\text{in}}}{\text{d}\tau}. \tag{29}$$

Under assumption 3, the system (29) has reached its steady state, such that the internal error ε_g remains constant, i.e.

$$\frac{d\varepsilon_g}{d\tau} = 0. \tag{30}$$

Moreover, considering that the time response is fast compared to the signal level dynamics,

$$\kappa_0 \gg \frac{\text{d}v_{\text{ref}}}{\text{d}\tau} - \frac{\text{d}v_{\text{in}}}{\text{d}\tau}, \tag{31}$$

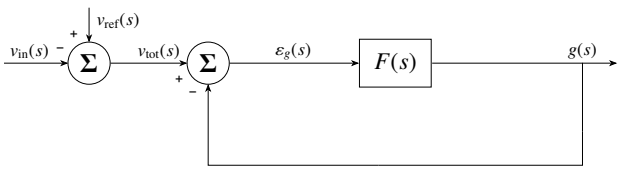


Figure 5: Equivalent model of the VGA gain.

the gain at steady state can be expressed as

$$v_{\text{out}}(\tau) = v_{\text{ref}}(\tau), \quad g(\tau) = v_{\text{ref}}(\tau) - v_{\text{in}}(\tau). \tag{32}$$

To conclude, at steady state, the VGA gain $g(\tau)$ can be obtained exclusively by computing the input signal level $v_{\text{in}}(\tau)$. The signal level is computed over interval I_t, considering the average power P_t or distribution p_r. In nominal conditions (without RFI), the received signal primarily comprises AWGN with ergodic properties; thus, the time-based distribution of the signal is represented by its random distribution [35] (with Gaussian properties). However, in the presence of RFI, these ergodic and Gaussian properties are no longer guaranteed, and the expression of P_t and p_r computed over I_t must be further defined.

4. Mathematical preliminaries on time-based estimation

This section introduces the mathematical definitions along with properties pertaining to time-based estimation under ergodic or non-ergodic signals. In particular, this section provides the definitions to compute and interpret the time-based average signal power and signal distribution introduced in the signal level (18) and (19).

Definition 1 (Time-event space). Let $(I_t, \mathcal{T}, \mathbb{P}_t)$ be a measure space on the bounded time-interval $I_t \subset \mathbb{R}^+$, with σ-algebra $\mathcal{T}$ and probability measure $\mathbb{P}_t : \mathcal{T} \to [0, 1]$ defined for all $F \in \mathcal{T}$ as

$$\mathbb{P}_t(F) = \frac{1}{T}\int_{t\in F} \text{d}t \;\text{ with } T = \int_{t\in I_t} \text{d}t. \tag{33}$$

The space $(I_t, \mathcal{T}, \mathbb{P}_t)$ is referred to as the time-event space.

Remark. *The time-event space $(I_t, \mathcal{T}, \mathbb{P}_t)$ satisfies all the probability axioms and can thus be seen as a probability space. Therefore, the principles and theorems established in probability theory can be directly applied to time-based estimation. Some of these properties are outlined below.*

Definition 2 (Time-dependent signal). Let $(I_t, \mathcal{T}, \mathbb{P}_t)$ be the time-event space and $(I_r, \mathcal{A}, \mu)$ be a measure space on the interval $I_r \subset \mathbb{R}$, with σ-algebra $\mathcal{A}$ and measure μ. The time-dependent signal $r : I_t \to I_r$ can be seen as a random variable from I_t to I_r. The time-based signal distribution, denoted p_r, is defined as the density of r with respect to the measure μ on $(I_r, \mathcal{A}, \mu)$ such that

$$\text{d}\mathbb{P}_{t,\,r} = p_r\,\text{d}\mu \tag{34}$$

with $\mathbb{P}_{t,\,r}(A) = \mathbb{P}_t\left(r^{-1}(A)\right), \;\; \forall A \in \mathcal{A}$ and r^{-1} the inverse image of r.

Definition 3 (Time-based moment). Let $r : I_t \to I_r$ be a time-dependent signal and φ be a measurable function. The moment of $\varphi(r)$ is defined as

$$\mathbb{E}_t\left[\varphi(r)\right] = \int_{I_t} \varphi(r)\,\text{d}\mathbb{P}_t = \frac{1}{T}\int_{I_t} \varphi(r)\,\text{d}t, \tag{35}$$

or equivalently as

$$\mathbb{E}_t\left[\varphi(r)\right] = \int_{I_r} \varphi(r)\,p_r(r)\,\text{d}r. \tag{36}$$

Remark. *The moment* (35) *is equivalent to the time-average typically denoted* $\langle\varphi(r)\rangle$.

Property 1 (Composition 1)**.** *[36, chap. 2] Let* $r : I_t \to I_r$ *be a time-dependent signal with signal distribution* p_r*, and let* $\varphi : I_r \to I_\varphi$ *be a continuous and monotonic function. Then,* φ *is a one-to-one mapping on* I_r*, and the signal distribution of* $\varphi \circ r$ *can be expressed as*

$$\forall \phi \in I_\varphi,\ \ p_\varphi(\phi) = p_r\left(\varphi^{-1}(\phi)\right)\left|\frac{\mathrm{d}}{\mathrm{d}\phi}\varphi^{-1}(\phi)\right|. \tag{37}$$

Property 2 (Composition 2)**.** *[36, chap. 2] Let* $r : I_t \to I_r$ *be a time-dependent signal with signal distribution* p_r *and* $\varphi : I_r \to I_\varphi$ *be a piecewise one-to-one mapping function, where each bijective restriction is denoted* $\varphi_n : I_n \to \varphi(I_n)$*. The distribution of* $\varphi \circ r$ *can therefore be expressed as*

$$\forall \phi \in I_\varphi,\ \ p_\varphi(\phi) = \sum_{n=1}^{N}\left\{p_u\left(\varphi_n^{-1}(\phi)\right)\left|\frac{\mathrm{d}}{\mathrm{d}\phi}\varphi_n^{-1}(\phi)\right|\mathbb{1}_{\varphi(I_n)}(\phi)\right\} \tag{38}$$

where $\mathbb{1}_I$ *is the characteristic function of the interval* I*.*

4.1. Independence of two time-dependent signals

Definition 4 (Independence). Let $r : I_t \to I_r$ and $u : I_t \to I_u$ be two time-dependent signals, with their respective time-based signal distributions p_r and p_u, and their joint time-based signal distribution $p_{r,u} : I_r \times I_u \to \mathbb{R}^+$. The signals r and u are said to be independent if

$$\forall (r,u) \in I_r \times I_u,\ \ p_{r,u}(r,u) = p_r(r)\, p_u(u). \tag{39}$$

Property 3 (Sum of independent signals)**.** *[36, chap. 2] Let* $u : I_t \to I_u$ *and* $r : I_t \to I_r$ *be two independent signals and* $y : I_t \to I_y$ *defined as* $y = u + r$*. The distribution of* y*, denoted* $p_y : I_y \to \mathbb{R}^+$ *is expressed as*

$$p_y(y) = \int_{-\infty}^{+\infty} p_u(x)\, p_r(y-x)\,\mathrm{d}x = (p_u * p_r)(y),\ \ \forall y \in I_y. \tag{40}$$

Property 4 (Product of independent signals)**.** *[36, chap. 2] Let* $u : I_t \to I_u$ *and* $r : I_t \to I_r$ *be two independent signals and* $w : I_t \to I_w$ *defined as* $w = u \cdot r$*. The distribution of* w*, denoted* $p_w : I_w \to \mathbb{R}^+$ *is expressed as*

$$p_w(w) = \int_{-\infty}^{+\infty}\left|\frac{1}{x}\right| p_u(x)\, p_r\left(\frac{w}{x}\right)\mathrm{d}x,\ \ \forall w \in I_w. \tag{41}$$

Remark. *In the case where the signal depends on random parameters defined on the probability space* $(I_\Omega, \mathcal{E}, \mathbb{P}_\Omega)$ *(referred to as the random sample space), the signal* $r : I_t \times I_\Omega \to I_r$ *is also a random variable taking values in the measure space* $(I_r, \mathcal{A}, \mu)$*.*

The time-based properties of the signal can be analyzed over a single random realization by considering the conditional random variable $r \mid \mathcal{E}'$*, where* $\mathcal{E}' \subseteq \mathcal{E}$ *is the smallest* σ*-algebra generated by* I_Ω*. The time-based distribution can thus be defined as*

$$\mathrm{d}\mathbb{P}_{t,r\mid\mathcal{E}'} = p_{r\mid\mathcal{E}'}\,\mathrm{d}\mu, \tag{42}$$

with $\mathbb{P}_{t,r\mid\mathcal{E}'}(A \mid \mathcal{E}') = \mathbb{P}_t\left(r^{-1}(A) \mid \mathcal{E}'\right),\ \ \forall A \in \mathcal{A}$*.*

Similarly, the random properties of the signal can be analyzed over a single time realization by considering the conditional random variable $r \mid \mathcal{T}'$*, where* $\mathcal{T}' \subseteq \mathcal{T}$ *is the smallest* σ*-algebra generated by* I_t*. The probability density function (pdf) is expressed as*

$$\mathrm{d}\mathbb{P}_{\Omega,r\mid\mathcal{T}'} = f_{r\mid\mathcal{T}'}\,\mathrm{d}\mu, \tag{43}$$

with $\mathbb{P}_{\Omega,r\mid\mathcal{T}'}(A \mid \mathcal{T}') = \mathbb{P}_\Omega\left(r^{-1}(A) \mid \mathcal{T}'\right),\ \ \forall A \in \mathcal{A}$*.*

4.2. Signal power

This subsection introduces the different definitions of the power of the time-dependent random signal $r : I_t \times I_\Omega \to I_r$.

Definition 5 (Random-average power). The random-average power represents the expected value of the instantaneous power over the random realizations of the signal, defined for any temporal realization $t \in \mathcal{T}'$ as

$$P_{r\mid\mathcal{T}'} = \mathbb{E}_\Omega\left[r^2 \mid \mathcal{T}'\right] = \int_{r\in I_\Omega} r^2\, f_{r\mid\mathcal{T}'}(r \mid \mathcal{T}')\,\mathrm{d}r. \tag{44}$$

with $\mathbb{E}_\Omega[\cdot] = \int_{I_\Omega} \cdot\, \mathrm{d}\mathbb{P}_\Omega$.

Definition 6 (Time-average power). The time-average power represents the expected value of the instantaneous power over the time realization of the signal, defined for any realization $\omega \in \mathcal{E}'$ as

$$P_{r\mid\mathcal{E}'} = \mathbb{E}_t\left[r^2 \mid \mathcal{E}'\right] = \frac{1}{T}\int_{t\in I_t} r(t)^2\,\mathrm{d}t = \int_{r\in I_r} r^2\, p_{r\mid\mathcal{E}'}(r \mid \mathcal{E}')\,\mathrm{d}r. \tag{45}$$

Definition 7 (Total-average power). The total-average power represents the expected value of the instantaneous power over both the time and random realizations, defined as

$$P_r = \mathbb{E}_t\left[\mathbb{E}_\Omega\left[r^2\right]\right] = \mathbb{E}_\Omega\left[\mathbb{E}_t\left[r^2\right]\right]. \tag{46}$$

4.3. CW signals

In this paper, a CW signal designates a random time-dependent signal $r : I_t \times I_\Omega \to I_r$ which can be expressed as

$$r(t) = a\cos(2\pi f t + \theta) \tag{47}$$

with frequency $f \in \mathbb{R}$, amplitude $a \in \mathbb{R}^+$, and phase $\theta \sim \mathcal{U}([0, 2\pi])$ constant over I_t. In addition, the weighted CW $r_\alpha : I_t \to I_\alpha$ (denoted as α-CW) is defined as

$$r_\alpha(t) = \alpha(t)\, r(t) \tag{48}$$

with $\alpha : I_t \to I_\alpha$ a continuous and finite (possibly random) time-dependent signal.

Property 5 (Time-based distribution of a CW)**.** *Let $r : I_t \to I_r$ be a CW signal, defined as* (47)*. In the case of a single period (i.e., $I_t = [t_0, t_0 + 1/f]$ with t_0 an arbitrary value), the signal distribution of r, denoted as $p_{r|\theta} : [-a, a] \to \mathbb{R}^+$ is given by*

$$p_{r|\theta}(r) = \frac{1}{\pi\sqrt{a^2 - r^2}}. \tag{49}$$

By periodicity, (49) *can be extended to any integer number of periods, and can be further extended to any I_t considering $1/f \ll T$ (i.e., $\frac{1}{Tf} \to 0$).*

Proof. Use Property 1 on $[0, \frac{1}{2f}]$ and extend to $[0, \frac{1}{f}]$ by parity.

Remark. *The time-based distribution* (49) *is independent of the random phase θ.*

Property 6 (Independence of two CW)**.** *Let r_1 and r_2 be two CW signals with frequencies f_1 and f_2, respectively. For $T \to \infty$, if f_2/f_1 is an irrational number, and if $1/f_1 \ll T$ or $1/f_2 \ll T$, then r_1 and r_2 are independent over time.*

Proof. See Appendix A.

Remark. *The independence can be extended to two α-CW signals if α_1 and α_2 are independent.*

Property 7 (Power of CW signal)**.** *Let $r : I_t \to I_r$ be a CW signal. If I_t spans an integer number of periods or if $1/f \ll T$, then*

$$\mathbb{E}_t[r] = \mathbb{E}_\Omega[r] = \mathbb{E}_\Omega[\mathbb{E}_t[r]] = 0. \tag{50}$$

and the random, time, and total-average powers of r are equal and expressed as

$$P_{CW} = \frac{a^2}{2}. \tag{51}$$

Remark. *The Property 7 can be extended to any α-CW as*

$$P_{\alpha-CW} = P_0\, P_{CW} = P_0\, \frac{a^2}{2} \tag{52}$$

with P_0 being the power of signal α (depending on the power definition).

Property 8 (Power of multiple α-CW signals)**.** *Let $S_M : I_t \to I_S$ be the sum of M pairwise α-CW signals $(r_m)_{m\in[\![1;M]\!]}$ defined as*

$$S_M(t) = \sum_{m=1}^{M} r_m(t) = \sum_{m=1}^{M} \alpha_m(t)\, a_m \cos(2\pi f_m t + \theta_m), \tag{53}$$

satisfying $\forall m \in [\![1; M]\!]$, $1/f_m \ll T$. If P_m defines the random, time, or total-average power of α_m, the corresponding average power P_S of S_M is expressed as

$$P_S = \frac{1}{2}\sum_{m=1}^{M} P_m\, {a_m}^2. \tag{54}$$

Proof. See (50) and (52).

Property 9 (Central Limit Theorem (CLT) for α-CW)**.** *Let $S_M : I_t \to I_S$ be the sum of M α-CW signals as defined in* (53) *such that $\forall m, f_{m+1} > f_m$. Let A_M and $\Sigma_M : I_t \to I_\Sigma$ be expressed as*

$$A_M = \left(\frac{1}{2}\sum_{m=1}^{M} P_m\, {a_m}^2\right)^{\frac{1}{2}}, \quad \Sigma_M = \left(\frac{1}{2}\sum_{m=1}^{M} {\alpha_m}^2\, {a_m}^2\right)^{\frac{1}{2}}. \tag{55}$$

If A_m satisfies the conditions

$$A_M \xrightarrow[M\to\infty]{} +\infty, \quad \forall m, \quad \frac{\sqrt{P_m m}\, a_m}{A_M} \xrightarrow[M\to\infty]{} 0, \quad \Sigma_M/{A_M}^2 \xrightarrow{\mathcal{L}} 1, \tag{56}$$

the signal S_M/A_M converges in distribution toward a Gaussian distribution, such that

$$S_M/A_M \xrightarrow{\mathcal{L}} \mathcal{N}(0, 1). \tag{57}$$

Proof. See Appendix B.

Remark. *A_M defines the mean root power of S_M and Σ_M is a random variable defining the instantaneous root power of S_M. The hypothesis* (56) *verifies that the power of S_M is not contained in a finite number of components. Notice that Property 9 does not require conditions on the time interval I_t nor the mutual independence of the signals $(r_m)_{m\in[\![1;M]\!]}$.*

Remark. *The properties 8 and 9 can be applied to CW signals by setting $\alpha_m(t) = 1$ and $P_m = 1$.*

4.4. AWGN signals

Property 10 (AWGN time-based power and distribution)**.** *Let $n : I_t \to \mathbb{R}$ be an AWGN with time-based distribution p_n and pdf f_n. Thus, n presents ergodic properties, such that*

$$P_n = P_{n|\mathcal{T}'} = P_{n|\mathcal{E}'} \tag{58}$$

and

$$p_{n|\mathcal{E}'}(r) = f_{n|\mathcal{T}'}(r) = \frac{1}{\sqrt{2\pi P_n}} \exp\left(-\frac{r^2}{2P_n}\right), \quad \forall r \in \mathbb{R}. \tag{59}$$

To conclude, this section presented several tools to compute the time-based distribution and power of both ergodic and non-ergodic signals. These properties will then be used to characterize the impacts of spoofing and jamming on the AGC.

5. Spoofing impact

This section characterizes the impact of spoofing on the VGA gain for both power-based (18) and distribution-based (19) methods. In this situation, the received signal $r_{\text{in}} : I_t \to I_r$, defined in the general case as (3), is reduced as

$$r_{\text{in}}(t) = r_{\text{s}}(t) + n_{\text{a}}(t) + n_{\text{s}}(t) \tag{60}$$

with n_{a} and n_{s} the nominal and re-radiated AWGN defined in Sec. 2.1 and r_{s} the spoofing GNSS signal defined for single PRN as (5) and for multiple PRN as (6). Each individual generated PRN in the spoofing signal exhibits α-CW properties, with $\alpha_m = c_m\, d_m$ as defined in (6) and mutually independent.

5.1. Signal power

In the presence of spoofing, all power definitions (Defs. 5, 6, and 7) are equal and expressed as

$$P_{\text{in}} = P_{\text{s}} + P_n \tag{61}$$

with P_{s} representing the spoofing signal power expressed for a single PRN as (52) and for multiple PRNs as (54) and P_n representing the total AWGN signal power as defined in (4). A straightforward computation of the power of α_m leads to $P_m = 1$ for all definitions. Additionally, we define the GNSS-spoofing-signal-to-total-noise ratio S/N defined as

$$S/N = \frac{P_{\text{s}}}{P_n} = \frac{P_{\text{s}}}{P_{n,\text{a}} + P_{n,\text{s}}}, \tag{62}$$

as well as the relative amplitudes $(\gamma_m)_{m\in[1,N]}$ as

$$\gamma_m = \frac{a_{\text{s},m}}{\sqrt{2P_{\text{s}}}}. \tag{63}$$

5.2. Single PRN signal distribution

In the case of an individually emitted PRN spoofing signal, as defined in (5), the signal distribution p_s can be determined by computing the distributions of the navigation message p_d, the PRN signal p_c, and the carrier signal $p_{\cos}$. Firstly, the navigation message d is uniformly distributed over $\{-1, 1\}$. Thus, for all r,

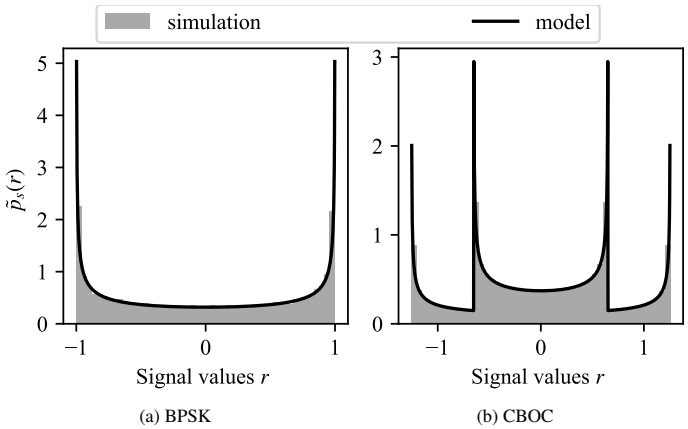
$$p_d(r) = \frac{1}{2}\left(\delta(r+1) + \delta(r-1)\right) \tag{64}$$

where $\delta(r)$ is the Dirac distribution. The distribution of the PRN code p_c depends on the modulation type. For BPSK modulation, the signal is uniformly distributed over $\{-1, 1\}$, while for CBOC modulation, the signal is uniformly distributed over $\{-\alpha_+, -\alpha_-, \alpha_+, \alpha_-\}$, with

$$\alpha_+ = \sqrt{\tfrac{10}{11}} + \sqrt{\tfrac{1}{11}},\quad \alpha_- = \sqrt{\tfrac{10}{11}} - \sqrt{\tfrac{1}{11}}. \tag{65}$$

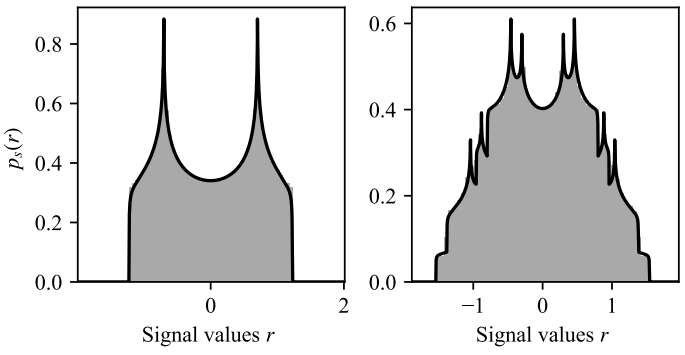
Therefore, the distribution of the modulated code c is expressed as

$$p_c(r)\begin{cases} = \frac{1}{2}\delta(r-1) + \frac{1}{2}\delta(r+1) & \text{(BPSK)} \\ = \frac{1}{4}\delta(r+\alpha_+) + \frac{1}{4}\delta(r+\alpha_-) & \\ \quad + \frac{1}{4}\delta(r-\alpha_+) + \frac{1}{4}\delta(r-\alpha_-) & \text{(CBOC)} \end{cases}. \tag{66}$$



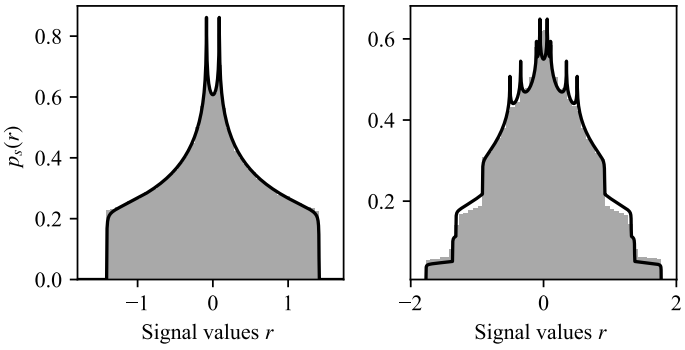
(a) BPSK (b) CBOC

Figure 6: Single PRN GNSS signal distribution.



(a) BPSK (b) CBOC

Figure 7: Dual PRN distribution ($P_{\text{s}} = 0.5$, $\gamma_1 = 0.96$, $\gamma_2 = 0.26$)



(a) BPSK (b) CBOC

Figure 8: Dual PRN distribution ($P_{\text{s}} = 0.5$, $\gamma_1 = 0.75$, $\gamma_2 = 0.66$)

Finally, assuming $T \gg 1/f$, the distribution $p_{\cos}$ can be expressed using (49) for $r \in \mathbb{R}$ as

$$p_{\cos}(r) = \frac{\mathbb{1}_{[-a,a]}(r)}{\pi\sqrt{a^2 - r^2}}. \tag{67}$$

The spoofing signal (5), being the product of the navigation message d, the PRN signal c and the carrier signal, and given that these terms can be considered mutually independent, the time-based distribution of the spoofing signal p_s can be expressed by applying Property 4 to (64), (66), and (67), leading to

$$p_s(r) = \frac{1}{a}\tilde{p}_s\left(\frac{r}{a}\right) \tag{68}$$

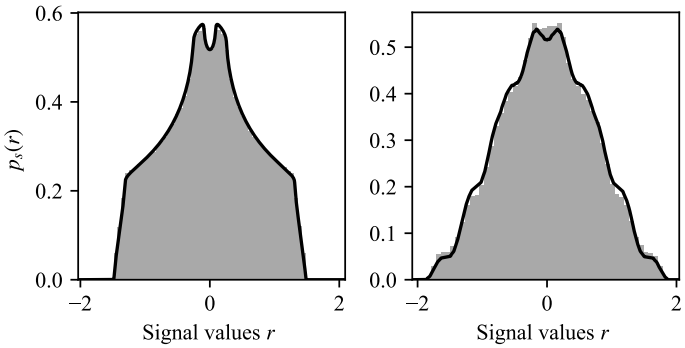
with $\tilde{p}_s$ the amplitude-normalized distribution defined as

$$\tilde{p}_s(r) = \begin{cases} \dfrac{\mathbb{1}_{[-1,1]}(r)}{\pi\sqrt{1-r^2}} & \text{(BPSK)} \\ \dfrac{1}{2\pi}\left(\dfrac{\mathbb{1}_{[-\alpha_-,\alpha_-]}(r)}{\sqrt{\alpha_-^2 - r^2}} + \dfrac{\mathbb{1}_{[-\alpha_+,\alpha_+]}(r)}{\sqrt{\alpha_+^2 - r^2}}\right) & \text{(CBOC)} \end{cases}. \tag{69}$$

The amplitude-normalized time-based distribution is plotted for both BPSK and CBOC modulation in Fig. 6. The model given by (69) is represented in black and compared with the histogram of a digital signal (in gray).

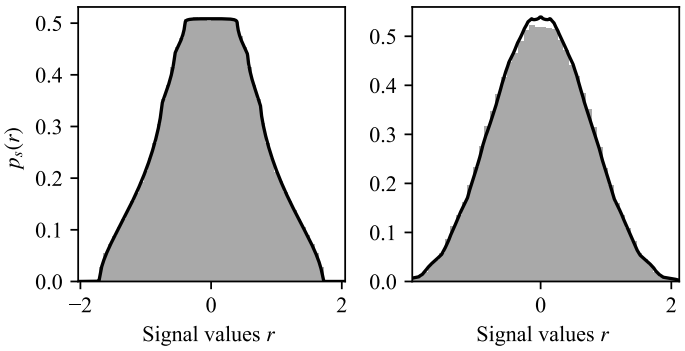
5.3. Multiple PRN signal distribution

In the case of multiple PRN spoofing signals, the received signal (6) is the combination of M individual signals $(r_m)_{m\in[\![1;M]\!]}$



(a) BPSK (b) CBOC

Figure 9: Multiple PRN distribution ($M = 3$, $P_s = 0.5$, $\gamma_1 = 0.09$, $\gamma_2 = 0.61$, $\gamma_3 = 0.78$)



(a) BPSK (b) CBOC

Figure 10: Multiple PRN distribution ($M = 3$, $P_s = 0.5$, $\gamma_1 = 0.48$, $\gamma_2 = 0.58$, $\gamma_3 = 0.66$)

with frequencies $(f_m)_{m\in[\![1;M]\!]}$ and amplitudes $(a_{s,m})_{m\in[\![1;M]\!]}$. The frequencies $(f_m)_{m\in[\![1;M]\!]}$ are physical parameters taking values in $\mathbb{R}$. Moreover, since $\mathbb{Q}$ has measure zero, for all distinct i and j, $\mathbb{P}(f_j/f_i \in \mathbb{Q}) = 0$ almost surely and, f_j/f_i is irrational. Assuming a sufficiently long time interval I_t, from Property 6, the signals $(r_m)_{m\in[\![1;M]\!]}$ can be considered mutually independent, and the distribution of the spoofing signal can be expressed for $r \in I_r$ as (considering the sum of M mutually independent signals, as presented in Property 3)

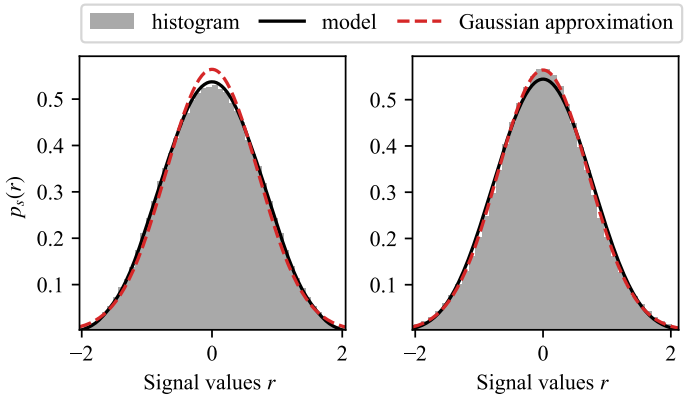
$$p_s(r) = \left(\circledast_{m=1}^{M} p_{s_m}\right)(r) \tag{70}$$

where $\circledast$ represents the convolution operator and p_{s_m} denotes the distribution of the m-th individual PRN signal as expressed in (68). Finally, as the number of emitted signals increases ($M \to +\infty$), the spoofing signal converges in distribution toward a normal variable, such that (see Property 9)

$$p_{s,\infty}(r) = \frac{1}{\sqrt{2\pi P_s}} \exp\left(-\frac{r^2}{2P_s}\right). \tag{71}$$

5.4. Received signal distribution

Finally, the distribution of the received signal in the presence of spoofing interference (60) can be expressed for $r \in I_r$ as



(a) BPSK (b) CBOC

Figure 11: Multiple PRN distribution ($M = 5$, $P_s = 0.5$, $\gamma_1 = 0.37$, $\gamma_2 = 0.49$, $\gamma_3 = 0.43$, $\gamma_4 = 0.64$, $\gamma_5 = 0.19$)

(Property 3)

$$p_r(r) = p_s * p_n(r) \tag{72}$$

with p_s the spoofing time-based distribution defined for single PRN in (68) or for multiple PRN in (70) and p_n the total AWGN distribution expressed as (59).

5.5. Time-based signal distribution results

This subsection analyzes the model of the spoofing signal time-based distribution obtained in (68) and (70). These results are compared with simulated distributions obtained by estimating the histogram of a digital signal generated from (5) or (6). The signal is generated with a sample frequency $F_s = 50$ MHz over an estimation time $T = 20$ ms. The model and simulation results are represented for both BPSK and CBOC modulations.

First, Figs. 7 and 8 plot the spoofing signal distribution for two emitted spoofing signals ($M = 2$) with two different sets of parameters $(\gamma_m)_{m\in[\![1;M]\!]}$ and $P_s = 0.5$. The simulated signals are generated with arbitrary frequencies ($f_1 = 1919.52$ Hz and $f_2 = -822.32$ Hz). The simulated signal histograms (gray) match the model curves (black). The results highlight the impact of the parameters $(\gamma_m)_{m\in[\![1;M]\!]}$ and the modulation on the shape of the signal distribution.

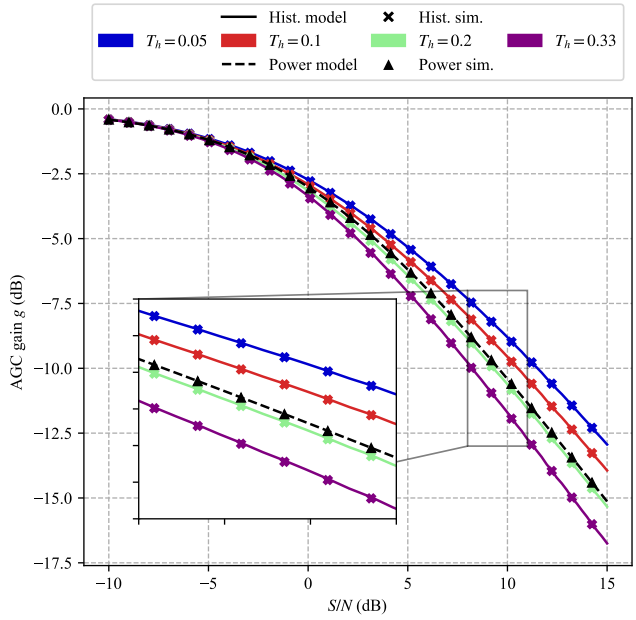
Similarly, Figs. 9 and 10 plot the spoofing signal distribution for three emitted spoofing signals ($M = 3$) with two different sets of parameters $(\gamma_m)_{m\in[\![1;M]\!]}$ and $P_s = 0.5$. While the parameters $(\gamma_m)_{m\in[\![1;M]\!]}$ and the modulation impact the shape of the distribution, the increase of M appears to smooth the distribution, as predicted by the convolution product in (70). Finally, Fig. 11 represents the signal distribution for $M = 5$ and shows the validity of the Gaussian approximation (59) for a large number of signals ($M > 5$).

5.6. VGA gain results

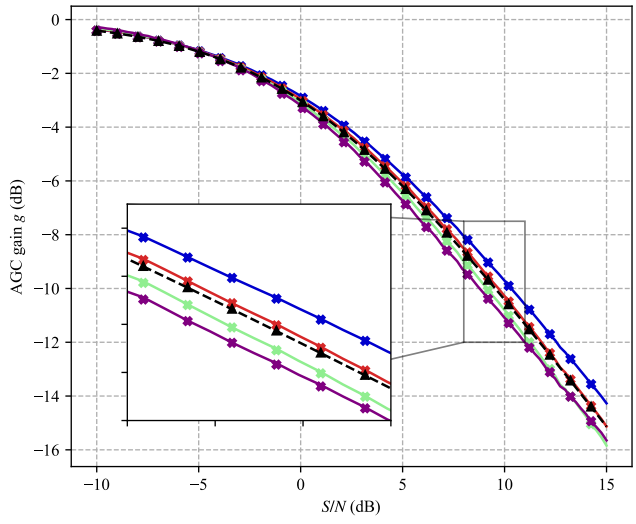
This subsection analyzes the VGA gain model for different parameters. The gain model is computed depending on the detector implementation: for the power-based detector, the time-average signal power (61) is injected into (18); for the histogram-based detector, the time-based signal distribution

(72) is used in (19). The theoretical gain is compared with simulated gain obtained by considering the AGC in steady state to estimate power-based and distribution-based signal levels on a digital signal generated from (60). The parameters of the generated signal are equal to those in Sec. 5.5. For both the model and simulation, the AGC reference v_{ref} is set to normalize the VGA gain (0 dB) in the presence of only nominal plus re-radiated noise ($P_s = 0$). In all figures, the gain is plotted for both BPSK and CBOC modulation as a function of S/N (62).

Fig. 12 presents the VGA gain in the presence of a single PRN spoofing signal. The model is represented by continuous lines with various colors for the histogram-based detectors, corresponding to different threshold values ($T_{\text{h}} \in \{0.05, 0.1, 0.2, 0.33\}$), and a dashed line for the power-based detector. Simulation results, on the other hand, are represented

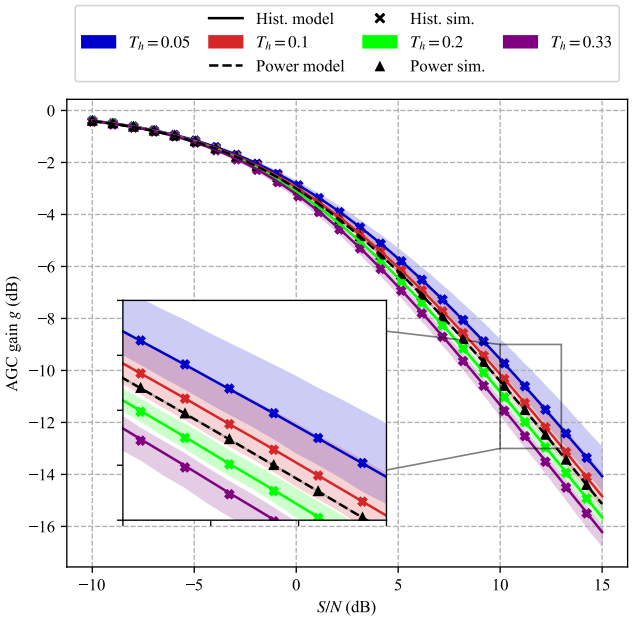


(a) BPSK modulation

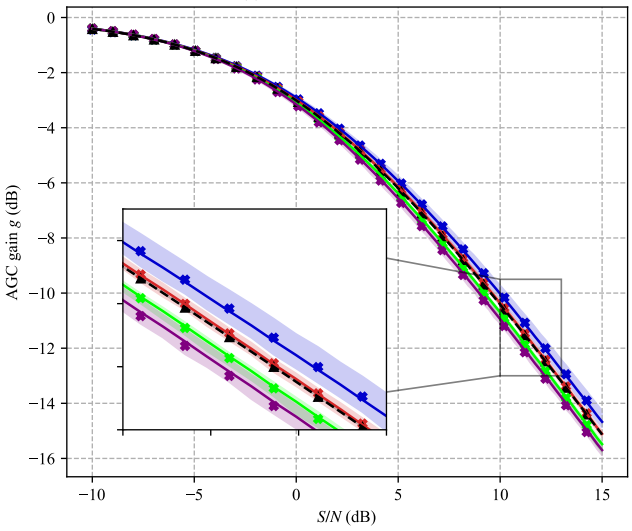


(b) CBOC modulation

Figure 12: VGA gain in the presence of single PRN spoofing signal



(a) BPSK modulation



(b) CBOC modulation

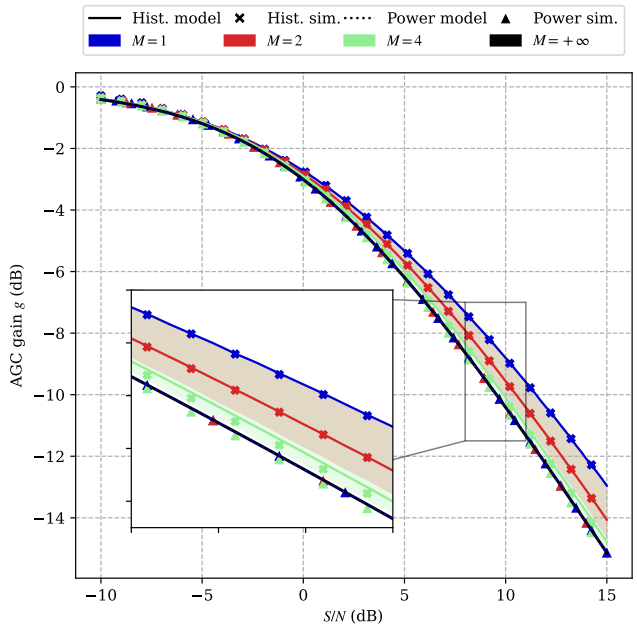
Figure 13: VGA gain in the presence of dual PRN spoofing signal

with markers without any connecting line (with corresponding colors). The model matches the simulation for both modulation and detector types. For the power-based detector, the modulation does not have any impact on the VGA gain (the power of the signal α, $P_m = 1$ in (54)). However, the histogram-based gain depends on the choice of T_{h}, inducing a gain difference of about 5 dB for BPSK and 2 dB for CBOC modulation (at $S/N = 15$ dB).

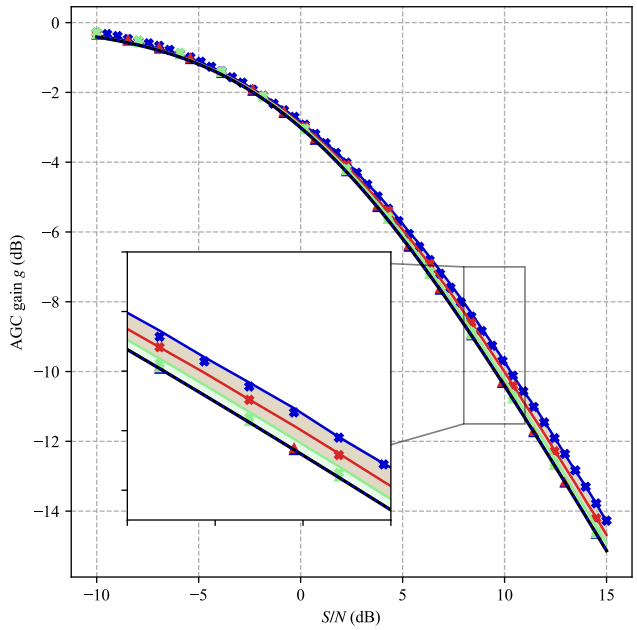
Similarly, Fig. 13 depicts the VGA gain in the presence of two spoofing signals. To consider the impact of the distribution shape, both the model and simulation are analyzed for all possible sets of $(\gamma_m)_{m\in\{1,2\}}$. For the model, the line represents the mean value of the gain, while the filled color represents the range of possible gain for all the values of $(\gamma_m)_{m\in\{1,2\}}$. For the simulation, the marker represents the mean value taken by

the VGA gain. For the power-based detector, neither modulation nor $(\gamma_m)_{m\in\{1,2\}}$ impacts the VGA gain, as predicted in (61). However, for the histogram-based gain, the shape of the distribution is shown to have more impact at lower thresholds and for BPSK modulation (from 1 dB for $T_\mathrm{h} = 0.05$ to 0.4 dB for $T_\mathrm{h} = 0.33$).

Lastly, Fig. 14 presents the impact of the number of spoofing signals on the VGA gain. For the model, the filled color represents the range of possible gain for all the values of $(\gamma_m)_{m\in[\![1;M]\!]}$, the continuous lines (histogram-based detector), and dotted lines (power-based detector) represent the model mean values, while the markers (crosses for histogram-based detector and triangles for power-based detector) represent the simulated mean gain values. The color represents the number of emitted signals ($M \in \{1, 2, 4\}$). Additionally, the Gaussian model in (71) is represented in black. The histogram-based method is plotted for $T_\mathrm{h} = 0.05$. For the power-based VGA gain, both modeled and simulated results match the Gaussian model for any M, as predicted in (61). For the histogram-based detector, the maximum range of the gain tends to increase as M increases, bounded by the single PRN case. However, the mean gain values tend to converge toward the Gaussian approximation (71).



(a) BPSK modulation



(b) CBOC modulation

Figure 14: VGA gain in the presence of multiple PRN spoofing signal ($T_\mathrm{h} = 0.05$)

5.7. Conclusion and discussion on spoofing impact

To conclude, this section proposes a model of the impact of spoofing on VGA gain for both power-based and histogram-based detectors. The model of the power-based gain is derived from the spoofing signal power (61) and the power-based signal level (18). Conversely, the histogram-based gain model is formulated using the spoofing signal distribution (72) and the distribution-based signal level (19).

The spoofing signal can be decomposed into two components: the re-radiated noise and the spoofing GNSS signal. The former can be modeled as AWGN, with its impact on gain reduced to the re-radiated noise power (as detailed in [10]). The impact of the spoofing GNSS signal is more complex as it depends on the S/N defined in (62), the AGC detector types, and the spoofing signal parameters (including the number of emitted signals, amplitudes, and modulation).

Firstly, to affect the AGC, the spoofing GNSS signal must be broadcast at a power similar to or higher than the nominal plus re-radiated noise, as shown in Figs. 12, 13, and 14 (no impact on VGA gain for $S/N < -10$ dB). Secondly, the impact of GNSS spoofing signals varies depending on the detector type: the power-based gain is independent of the input GNSS signal structure (number of emitted signals M or modulation) and depends only on the received power (61); the histogram-based gain depends on the signal distribution shape and therefore on the number of emitted signals M, parameters $(\gamma_m)_{m\in[\![1;M]\!]}$, modulation, and threshold T_h. These parameters can induce a difference of several decibels in the gain but tend to be negligible with the Gaussian approximation (71) as the number of emitted signals increases (see Fig. 14). The impact of Gaussian interference on AGC has been detailed in [10].

Finally, while the model is shown to be independent of the spoofing signal frequency $(f_m)_{m\in[\![1;M]\!]}$, the mutual dependence of each signal requires $T \gg 1/f_m$ (see Property 6). However, even if this dependence can disturb the signal distribution for a low number of signals M, the distortion of VGA gain will never exceed the single PRN bound as shown in Fig. 14, and tends to be negligible for a high number of signals (Property 9).

6. Jamming impact

This section characterizes the impact of jamming chirp signals on the VGA gain for both power-based (18) and distribution-based (19) methods. In this situation, the received

signal $r_{\text{in}} : I_t \to I_r$, defined in the general case as (3), is reduced as

$$r_{\text{in}}(t) = n_{\text{a}}(t) + r_{\text{j}}(t) \tag{73}$$

with $n_{\text{a}} : I_t \to \mathbb{R}$ the nominal AWGN defined in Sec. 2.1 and $r_{\text{j}} : I_t \to I_{\text{j}}$ the jamming chirp signal, defined in (11). Note that r_{j} is a non-ergodic signal depending on both time t and initial phase θ_{j}.

6.1. Signal power

This subsection characterizes the power of the received signal for all definitions 5, 7 and 6. For any definition, the signal power can be decomposed as

$$P_{\text{in}} = P_n + P_{\text{j}} \tag{74}$$

with P_n the AWGN power and P_{j} the jamming chirp signal power. The expression of jamming power varies across the power definitions.

First, the random-average power of the jamming signal is defined as the average power for one time realization, i.e., over the representation of the uniform phase $\theta_{\text{j}} \sim \mathcal{U}[0, 2\pi]$ and a fixed $t \in I_t$ and expressed as

$$P_{\text{j}\,|\,t} = \mathbb{E}_\Omega\left[r_{\text{j}}^2 \mid t\right] = \frac{{a_{\text{j}}}^2}{2}. \tag{75}$$

It is worth noting that the random-average power is independent of t, the total-average power P_{j}, defined as (46), is equal to (75). We define the jamming-signal-to-noise total-average power ratio J/N as

$$J/N = \frac{P_{\text{j}}}{P_n} = \frac{a_{\text{j}}^2}{2P_n}. \tag{76}$$

Finally, the time-average power (45) represents the average power for one random realization, i.e., over the time representation I_t and a fixed $\theta_{\text{j}} \in [0, 2\pi]$, such that

$$P_{\text{j}\,|\,\theta_{\text{j}}} = \mathbb{E}_t\left[r_{\text{j}}^2 \mid \theta_{\text{j}}\right] = \int_{r \in I_r} r^2\, p_{\text{j}\,|\,\theta_{\text{j}}}(r \mid \theta_{\text{j}})\,\mathrm{d}r. \tag{77}$$

with $p_{\text{j}\,|\,\theta_{\text{j}}} : I_{\text{j}} \to \mathbb{R}^+$ the jamming signal time-based distribution. Alternatively, considering the jamming phase wrapped on $[0, 2\pi]$, denoted $\phi^{(2\pi)} \mid \theta_{\text{j}} : I_t \to [0, 2\pi]$ and its distribution $p^{(2\pi)}_{\phi\,|\,\theta_{\text{j}}} : [0, 2\pi] \to \mathbb{R}^+$, the time-average power can be expressed as

$$P_{\text{j}\,|\,\theta_{\text{j}}} = \int_0^{2\pi} {a_{\text{j}}}^2 \cos(\theta)^2\, p^{(2\pi)}_{\phi\,|\,\theta_{\text{j}}}(\theta \mid \theta_{\text{j}})\,\mathrm{d}\theta. \tag{78}$$

6.2. Jamming signal time-based distribution

The jamming signal distribution $p_{\text{j}\,|\,\theta_{\text{j}}}$ is related to the wrapped jamming phase distribution $p^{(2\pi)}_{\phi\,|\,\theta_{\text{j}}}$ from (11) and Property 2 for all $r \in I_{\text{j}} = [-a_{\text{j}}, a_{\text{j}}]$ as

$$p_{\text{j}\,|\,\theta_{\text{j}}}(r) = \left[p^{(2\pi)}_{\phi\,|\,\theta_{\text{j}}}\left(\cos_1^{-1}\left(\frac{r}{a_{\text{j}}}\right)\right) + p^{(2\pi)}_{\phi\,|\,\theta_{\text{j}}}\left(\cos_2^{-1}\left(\frac{r}{a_{\text{j}}}\right)\right)\right] \frac{1}{2\sqrt{{a_{\text{j}}}^2 - r^2}} \tag{79}$$

with $\cos_1 : [0, \pi] \to [-1, 1]$, and $\cos_2 : [\pi, 2\pi] \to [-1, 1]$ the piece by piece one-to-one mapping restrictions of cos (Property 2).

6.3. Jamming phase time-based distribution

In the presence of chirp jamming, the signal time-average power (78) and time-based distribution (79) are expressed from $p^{(2\pi)}_{\phi\,|\,\theta_{\text{j}}}$. This section expresses $p^{(2\pi)}_{\phi\,|\,\theta_{\text{j}}}$ as a function of chirp parameters. First, as shown in (14), the jamming phase ϕ_{j} is the combination of a periodic component ϕ_{sw} and a phase offset $\Delta\phi_n$. Thus, the phase distribution can be expressed as a function of the ϕ_{sw} distribution, denoted as $p_{\text{sw}\,|\,\theta_{\text{j}}} : \phi_{\text{sw}}(I_{\text{sw}}) \to \mathbb{R}^+$, as

$$p_{\phi\,|\,\theta_{\text{j}}}(\phi) = \frac{1}{N}\sum_{n=0}^{N-1} p_{\text{sw}\,|\,\theta_{\text{j}}}(\phi - \Delta\phi_n) \tag{80}$$

$$= p_{\text{sw}\,|\,\theta_{\text{j}}}(\phi) * \left(\frac{1}{N}\sum_{n=0}^{N-1}\delta(\phi - \Delta\phi_n)\right). \tag{81}$$

The wrapped jamming phase distribution can be expressed for $\theta \in [0, 2\pi]$ as

$$p^{(2\pi)}_{\phi\,|\,\theta_{\text{j}}}(\theta) = \sum_{i=-\infty}^{+\infty} p_{\phi\,|\,\theta_{\text{j}}}(\theta + 2\pi i) \tag{82}$$

$$= \left(\frac{1}{N}\sum_{n=0}^{N-1} p_{\text{sw}\,|\,\theta_{\text{j}}}(\theta - \Delta\phi_n)\right) * \left(\sum_{i=-\infty}^{+\infty}\delta(\theta + 2\pi i)\right) \tag{83}$$

$$= \frac{1}{N}\sum_{n=0}^{N-1} p^{(2\pi)}_{\text{sw}\,|\,\theta_{\text{j}}}(\theta - \Delta\phi_n) \tag{84}$$

where $p^{(2\pi)}_{\text{sw}\,|\,\theta_{\text{j}}} : [0, 2\pi] \to \mathbb{R}^+$ is the distribution of the wrapped periodic component.

The expression of $p^{(2\pi)}_{\text{sw}\,|\,\theta_{\text{j}}}$ can be derived from ϕ_{sw} expressed as (17). ϕ_{sw} is a convex function, presenting a minimum in $t_{\min}$, such that

$$t_{\min} = \frac{-f_j T_{\text{sw}}}{B_{\text{j}}}, \quad \phi_{\text{sw}}(t_{\min}) = \theta_{\text{j}} + \pi f_j t_{\min}. \tag{85}$$

The monotony of ϕ_{sw} can be studied depending on $t_{\min}$, and as illustrated in Fig. 4, two possibilities appear:

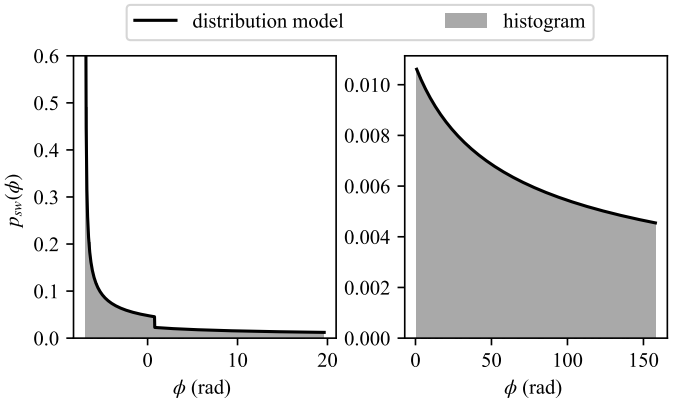
- If $t_{\min} \in I_{\text{sw}}$ the function is convex and symmetric around $t_{\min}$, and presents a one-to-one mapping on the intervals $I^{(\text{l})}_{\text{sw}} = [0, t_{\min}]$ and $I^{(\text{r})}_{\text{sw}} = [t_{\min}, T_{\text{sw}}]$. Therefore the function ϕ_{sw} can be decomposed into the two monotonic functions $\phi^{(\text{l})}_{\text{sw}} : I^{(\text{l})}_{\text{sw}} \to \phi_{\text{sw}}(I^{(\text{l})}_{\text{sw}})$ and $\phi^{(r)}_{\text{sw}} : I^{(\text{r})}_{\text{sw}} \to \phi_{\text{sw}}(I^{(\text{r})}_{\text{sw}})$.
- If $t_{\min} \notin I_{\text{sw}}$, the function is monotonic on I_{sw}.

The distribution p_{sw} can thus be expressed, using Property 2 for $\phi \in \phi_{\text{sw}}(I_{\text{sw}})$ as

$$p_{\text{sw}\,|\,\theta_{\text{j}}}(\phi) = p_{t\,|\,\theta_{\text{j}}}(\phi)\sqrt{\frac{T_{\text{sw}}}{\pi B_{\text{j}}}}\frac{1}{2\sqrt{\phi - \phi_{\text{sw}}(t_{\min})}} \tag{86}$$

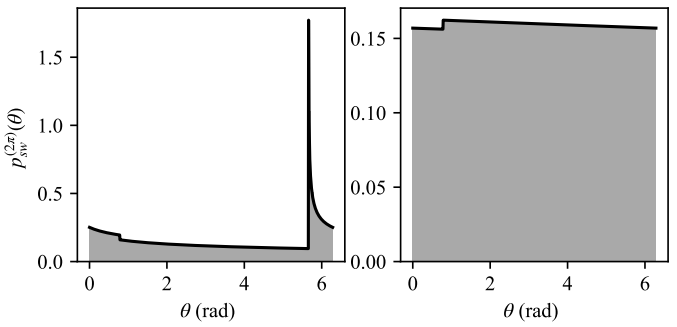
with

$$p_{t\,|\,\theta_{\text{j}}}(\phi) = \begin{cases} \dfrac{1}{T_{\text{sw}}}\left(\mathbb{1}_{\phi_{\text{sw}}(I^{(\text{l})}_{\text{sw}})}(\phi) + \mathbb{1}_{\phi_{\text{sw}}(I^{(\text{r})}_{\text{sw}})}(\phi)\right) & t_{\min} \in I_{\text{sw}} \\ \dfrac{1}{T_{\text{sw}}}\mathbb{1}_{\phi_{\text{sw}}(I_{\text{sw}})}(\phi) & t_{\min} \notin I_{\text{sw}} \end{cases}. \tag{87}$$



(a) f_j = 0.3MHz (b) f_j = 2.5MHz

Figure 15: Periodic phase component distribution (T_{sw} = 10 μs, B = 2 MHz, $\theta_j = \frac{\pi}{4}$).



(a) f_j = 0.3MHz (b) f_j = 2.5MHz

Figure 16: Periodic wrapped phase component distribution (T_{sw} = 10 μs, B = 2 MHz, $\theta_j = \frac{\pi}{4}$).

Similarly, the distribution of the wrapped periodic phase, $p^{(2\pi)}_{sw\,|\,\theta_j}$ can be expressed for $\theta \in [0, 2\pi]$ as

$$p^{(2\pi)}_{sw\,|\,\theta_j}(\theta) = \sum_{i=-\infty}^{+\infty} p_{sw\,|\,\theta_j}(\theta + 2\pi i). \tag{88}$$

6.4. Received signal distribution

Finally, the distribution of the received signal in the presence of jamming interference (73) can be expressed for $r \in I_r$ as (Property 3)

$$p_r(r) = p_j * p_n(r) \tag{89}$$

with p_j the jamming signal time-based distribution on I_t, expressed as (79) and p_n the AWGN timed-based distribution expressed as (59).

6.5. Time-based signal and phase distribution results

This subsection analyzes the model of the jamming phase and signal time-based distributions. These results are compared with simulated distributions obtained by estimating the histogram of a digital signal generated from (14) and (11). The signal is generated with a sample frequency F_s = 50 MHz over an estimation time T = 20 ms.

First, Figs. 15 and 16 present the impact of the jamming frequency f_j on p_{sw} and $p^{(2\pi)}_{sw}$; the time-based distributions (86) and (88) are plotted for two frequencies f_j of 0.3 MHz and 2.5 MHz. For $f_j < B_j$, the phase differentiation crosses its zero and the distribution p_{sw} presents a sharp peak (Fig. 16a). As the frequency increases, the phase distribution becomes smoother, resulting in a nearly constant wrapped phase distribution (Fig. 16b). The location of the peak depends on the jamming phase θ_j.

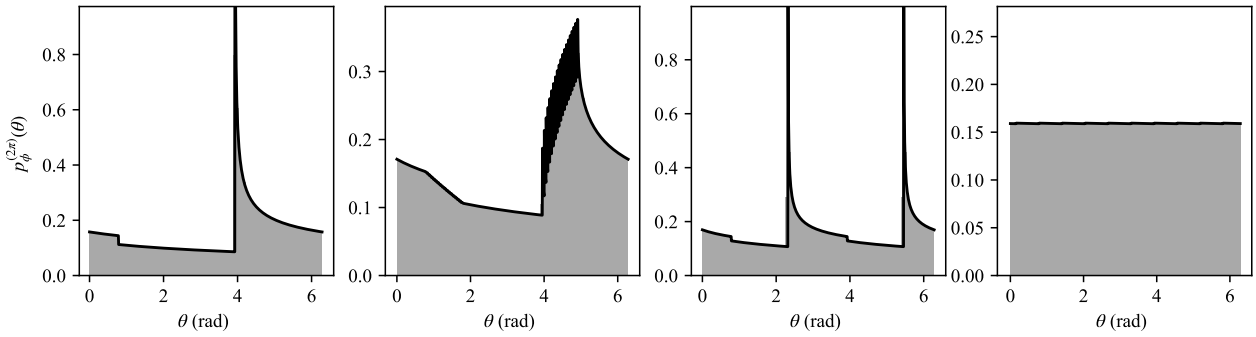
Then, Fig. 17 presents the distribution $p^{(2\pi)}_{\phi}$, expressed in (84), for different normalized frequencies $\tilde{f_j} = f_j T_{sw}$. The peak in $p^{(2\pi)}_{sw}$ is averaged depending on the number of periodic patterns N and shift $\Delta\phi_n = 2\pi\tilde{f_j}$. For example, with $\tilde{f_j} = 0$, the periodic phase is not shifted and $p^{(2\pi)}_{\phi} = p^{(2\pi)}_{sw}$ (Fig. 17a). Then, with a relatively low $\tilde{f_j}$ (such that $N\tilde{f_j} < 1$), the averaging operation in (84) smooths the phase over a partial part of $[0, 2\pi]$ (Fig. 17b). Fig. 17c illustrates a case where $\tilde{f_j}$ induces a periodic pattern on $\phi^{(2\pi)}_j$ reducing the phase smoothing. Lastly, for high frequencies, $p^{(2\pi)}_{\phi}$ shapes a uniform distribution over $[0, 2\pi]$ (Fig. 17d).

Finally, Fig. 18 presents the jamming signal distribution $p_{j\,|\,\theta_j}$, modeled in (79). The shape of $p_{j\,|\,\theta_j}$ is impacted by the peaks in $p^{(2\pi)}_{\phi\,|\,\theta_j}$. The degree of distortion in the signal distribution is weighted depending on the phase peak position (fixed by θ_j). Moreover, the smoothing of $p^{(2\pi)}_{\phi\,|\,\theta_j}$ also smooths the signal distribution $p_{j\,|\,\theta_j}$, converging to a CW distribution when the wrapped phase is uniform (Fig. 18d).

6.6. VGA gain results

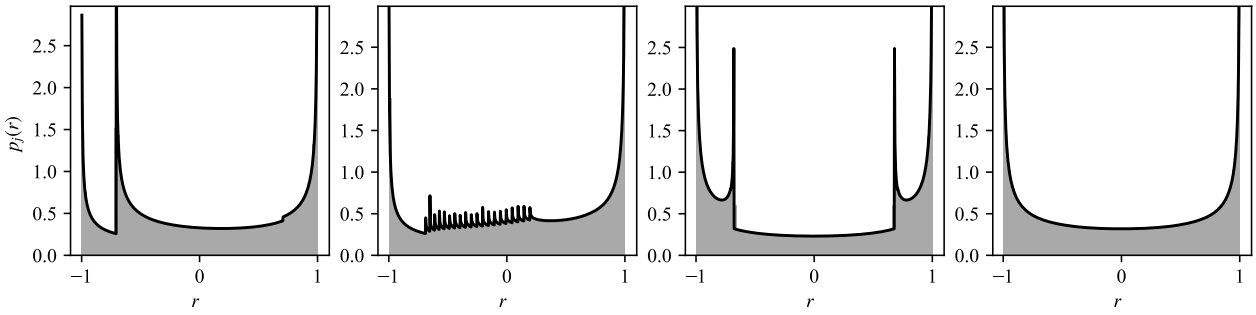
This subsection analyzes the VGA gain model for different parameters. The gain model is computed depending on the detector implementation: for the power-based detector, the time-average signal power (73) is injected into (18); for the histogram-based detector, the time-based signal distribution (79) is used in (19). The theoretical gain is compared with simulated gain obtained by considering the AGC in steady state to estimate power-based and distribution-based signal levels on a digital signal generated from (73). The parameters of the generated signal are equal to those in Sec. 6.5. For both the model and simulation, the AGC reference v_{ref} is set to normalize the VGA gain (0 dB) in the absence of jamming (P_j = 0). In the figures, the gain is plotted as a function of the J/N ratio, defined in (76).

Fig. 19 presents the VGA gain in the presence of a chirp jamming signal with a frequency of f_j = 50 kHz. The corresponding phase and signal distributions are plotted in Figs. 17c and 18c, respectively. In the figure, the lines represent the mean values of the gain, while the filled colors represent the set of possible values for θ_j ranging $[0, 2\pi]$. Additionally, markers without any line (crosses for histogram-based detector and triangles for power-based detector) indicate the simulated mean gain values (for θ_j ranging $[0, 2\pi]$). For both the model and simulation, the histogram-based gain is plotted for four different thresholds ($T_h \in \{0.05, 0.2, 0.33, 0.5\}$) and the power-based gain is plotted in black. The model matches the simulation for



(a) f_j = 0Hz, $\tilde{f}_\mathrm{j}$ = 0 (b) f_j = 800Hz, $\tilde{f}_\mathrm{j}$ = 0.008 (c) f_j = 50kHz, $\tilde{f}_\mathrm{j}$ = 0.5 (d) f_j = 2.51MHz, $\tilde{f}_\mathrm{j}$ = 25.1

Figure 17: Wrapped phase distribution (T_sw = 0.1us, B = 2MHz, $\theta_\mathrm{j} = \frac{\pi}{4}$).



(a) f_j = 0Hz, $\tilde{f}_\mathrm{j}$ = 0 (b) f_j = 800Hz, $\tilde{f}_\mathrm{j}$ = 0.008 (c) f_j = 50kHz, $\tilde{f}_\mathrm{j}$ = 0.5 (d) f_j = 2.51MHz, $\tilde{f}_\mathrm{j}$ = 25.1

Figure 18: Jamming signal distribution (T_sw = 0.1us, B = 2MHz, $\theta_\mathrm{j} = \frac{\pi}{4}$).

both modulation and detector types. Fig. 19 highlights the impact of the initial phase θ_j on the VGA gain for both the power-based and histogram-based detectors, resulting in variations between 0.2 dB (for T_h = 0.05) to 5 dB (for T_h = 0.5) for the histogram-based method and 1 dB for the power-based detector (at J/N = 25 dB).

Lastly, Fig. 20 presents the VGA gain in the presence of a chirp jamming signal with a frequency of f_j = 2.5 MHz. The legend of the figure is the same as in Fig. 19. As shown in Figs. 17d and 18d, at high frequencies, the phase is smoothed

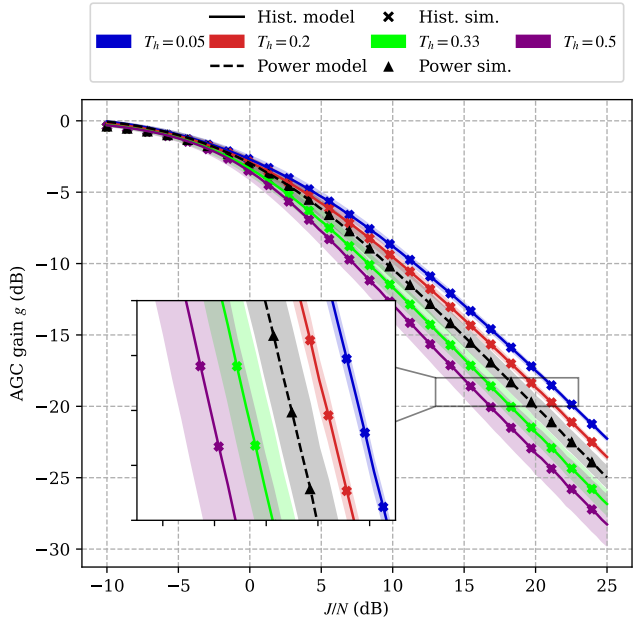


Figure 19: VGA gain in the presence of jamming chirp signal (f_j = 50kHz, $\tilde{f}_\mathrm{j}$ = 0.5)

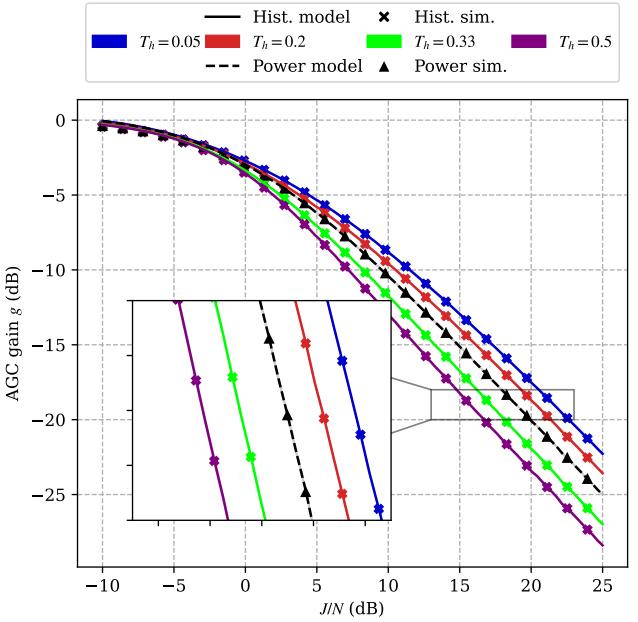


Figure 20: VGA gain in the presence of jamming chirp signal (f_j = 2.5MHz, $\tilde{f}_\mathrm{j}$ = 25.0)

and converges towards a uniform distribution. The VGA gain g is then independent of θ_j (no filled color region) and its behavior converges toward the result of a CW interference.

6.7. Conclusion and discussion on jamming impact

This section proposes a model of the impact of a chirp jamming signal on VGA gain for both power-based and histogram-based detectors. On the one hand, the model of the time-average power is presented in (74) and (78). On the other hand, the signal distribution is described by (89), both of which depend on the jamming signal distribution expressed in (79).

Due to the non-ergodicity of the jamming signal, characterized by the non-uniformity of the jamming phase over the estimation time I_t, both the signal distribution and the VGA gain exhibit differences compared to CW interference. The distribution depends on parameters such as the number of chirp periods N, the jamming frequency f_j, and the jamming initial phase θ_j. The discrepancy between chirp and CW interference is bounded by 1 dB (at $J/N = 20$ dB) for the power-based detector and ranges from 5 dB ($T_h = 0.5$) to 0 dB ($T_h = 0$) for the histogram-based detector (see Fig. 19). This difference is most pronounced for $f_j = 0$ or $N = 1$ and tends to converge to CW behavior as f_j increases. Consequently, for IF signals ($f_{IF} > 1$MHz, commonly implemented in GNSS receivers), the chirp signal can be effectively assimilated as CW interference by the AGC and ADC. Therefore, models for quantization degradation and BER in the presence of CW interference, such as those derived in [9], can be applied to chirp signals at IF.

7. Conclusion

This paper characterizes the jamming and spoofing impact on AGC and IF received signal. It first expresses the AGC behavior as a function of the received signal level, i.e., based on time-based signal power or distribution, and proposes a new probabilistic framework for time-based estimation to characterize these quantities under jamming and spoofing.

On one hand, the spoofing signal can be decomposed into two components: the re-radiated noise and the GNSS spoofing signal. The former can be modeled as AWGN, thus the VGA gain depends solely on the nominal and re-radiated noise power. The impact of the latter is much more complex. It depends on the AGC detector types, the S/N, as well as the spoofing signal parameters (including the number of emitted signals, amplitudes, and modulation). These spoofing parameters can lead to several decibels of difference but tend to be negligible with the Gaussian approximation of the spoofing signal as the number of emitted signals increases. The impact of Gaussian interference on AGC has been detailed in [10].

On the other hand, the chirp jamming signal presents non-ergodic properties and cannot be considered as CW (due to the non-uniformity of the phase). This paper proposes a model of the jamming signal time-based distribution and power based on the chirp phase distribution. The model is expressed as a function of the AGC detector type, J/N, and signal parameters (including the number of chirp periods N, the frequency f_j, and the initial phase θ_j). The jamming distribution is shown to shape a CW distribution as f_j increases. Consequently, for IF signals ($f_{IF} > 1$ MHz, commonly implemented in GNSS receivers), the chirp signal can be assimilated as CW interference (characterized in [9]) by the AGC and ADC.

In future works, the AGC gain and IF signal models developed in this paper, under jamming and spoofing interference, will be applied to characterize the potential threats to the GNSS receiver's RF front-end, such as VGA saturation or quantization losses [8, Chap.13] [37], and their impact on other signal processing blocks and the Position, Velocity and Time (PVT) solution.

Additionally, the results on AGC and IF signals, linked to specific geometries between the receiver and the jammer/spoofer, may facilitate the development of new robust detection and mitigation techniques, based on AGC and IF signal monitoring, before correlation [24, 38].

Finally, the theoretical framework introduced in this paper can be further explored to establish formal definitions for time-based estimation, power, and ergodicity of stochastic processes in signal processing, or coupled with other approaches such as random matrix theory (RMT), which allows capturing the system's statistical properties to characterize complex stochastic dynamic systems, similar to the AGC [39, 40]. Additionally, future research applying the probabilistic framework could improve the characterization of time-based estimation under non-ergodic conditions, such as the C/N_0 estimators under spoofing interference [21].

Appendix A. Proof independence of two CW (Property 6)

Let r_1 and r_2 be two CW signals defined by their phases $\theta_1 : I_t \to \mathbb{R}$ and $\theta_2 : I_t \to \mathbb{R}$, respectively, as

$$\theta_1(t) = 2\pi f_1 t, \quad \theta_2(t) = 2\pi f_2 t, \tag{A.1}$$

such that $f_2/f_1 \in \mathbb{R}\setminus\mathbb{Q}$, $1/f_2 \ll T$, and $1/f_1 \ll T$. Additionally, we define their wrapped phases $\tilde{\theta}_1 : I_t \to [0, 2\pi]$ and $\tilde{\theta}_2 : I_t \to [0, 2\pi]$, as

$$\tilde{\theta}_1 = \mathrm{mod}_{2\pi}\{\theta_1(t)\}, \;\; \tilde{\theta}_1 = \mathrm{mod}_{2\pi}\{\theta_1(t)\}. \tag{A.2}$$

The independence of r_1 and r_2 can be shown by demonstrating the independence of $\tilde{\theta}_1$ and $\tilde{\theta}_2$, by establishing the equality of the conditional distribution $p_{\tilde{\theta}_1|\tilde{\theta}_2}$ and the marginal distribution $p_{\tilde{\theta}_1}$, such that

$$\forall \tilde{\theta} \in [0, 2\pi], \;\; p_{\tilde{\theta}_1}(\tilde{\theta}) = p_{\tilde{\theta}_1|\tilde{\theta}_2}(\tilde{\theta}). \tag{A.3}$$

On one hand, considering $1/f_1 \ll T$, the variable $\tilde{\theta}_1$ is uniformly distributed on $[0, 2\pi]$, such that for all $\tilde{\theta} \in [0, 2\pi]$,

$$p_{\tilde{\theta}_1}(\tilde{\theta}) = \frac{1}{2\pi}. \tag{A.4}$$

On the other hand, the conditional wrapped phase $\tilde{\theta}_1|\tilde{\theta}_2$ can be expressed from the unwrapped conditional variable $\theta_1|\theta_2$. The unwrapped phase variable is expressed as

$$\theta_1|(\theta_2 = \theta) = \frac{f_2}{f_1}\theta, \tag{A.5}$$

thus

$$\theta_1|(\tilde{\theta}_2 = \tilde{\theta}) = \left\{\theta_1|(\theta_2 = \tilde{\theta} + 2\pi i)\right\}_{i\in\mathbb{N}} \tag{A.6}$$

$$= \left\{\frac{f_2}{f_1}\left(\tilde{\theta} + 2\pi i\right)\right\}_{i\in\mathbb{N}} \tag{A.7}$$

and

$$\tilde{\theta}_1|(\tilde{\theta}_2 = \tilde{\theta}) = \left\{\mathrm{mod}_{2\pi}\left[\frac{f_2}{f_1}\left(\tilde{\theta} + 2\pi i\right)\right]\right\}_{i\in\mathbb{N}} \tag{A.8}$$

Using the hypotheses $f_2/f_1 \in \mathbb{R}\setminus\mathbb{Q}$, $1/f_1 \ll T$, and $1/f_2 \ll T$, we deduce from the Weyl equidistribution theorem [41, Theorem 2], the variable $(\tilde{\theta}_1|\tilde{\theta}_2)/2\pi$ is uniformly distributed on the circle $\mathbb{R}/\mathbb{Z}$. Therefore, for all $\tilde{\theta} \in [0, 2\pi]$,

$$p_{\tilde{\theta}_1|\tilde{\theta}_2}(\tilde{\theta}) = \frac{1}{2\pi} = p_{\tilde{\theta}_1}(\tilde{\theta}). \tag{A.9}$$

The two distributions are equal for all $\tilde{\theta}$ in $[0, 2\pi]$, indicating that the variables $\tilde{\theta}_1$ and $\tilde{\theta}_2$ are independent, and by extension, so are r_1 and r_2.

Appendix B. Proof CLT for α-CW (Property 9)

Let S_M and A_M be defined as (53) and Σ_M as (55) and let the normalized random variables $\tilde{S}_M : I_t \to I_{\tilde{S}}$ and $\tilde{\Sigma}_M : I_t \to I_{\tilde{\Sigma}}$ be defined as

$$\tilde{S}_M = \frac{S_M}{A_M} \quad \text{and} \quad \tilde{\Sigma}_M = \frac{\Sigma_M}{{A_M}^2}. \tag{B.1}$$

Let $\boldsymbol{\alpha}_M = (\alpha_1, \ldots, \alpha_M)$ be a vector of real random variables converging in distribution toward $\boldsymbol{\alpha}$. This appendix studies the convergence in distribution of $\tilde{S}_M$. To do so, let us first study the convergence of $\tilde{S}_M|\tilde{\Sigma}_M$ expressed for all $s \in I_{\tilde{S}}$ and $\sigma \in I_{\tilde{\Sigma}}$ as

$$p_{\tilde{S}\,|\,\tilde{\Sigma}}(s \mid \sigma) = \lim_{M\to+\infty} p_{\tilde{S}_M\,|\,\tilde{\Sigma}_M}(s \mid \sigma) \tag{B.2}$$

$$= \lim_{M\to+\infty} \mathbb{E}_t\left[p_{\tilde{S}_M|\boldsymbol{\alpha}_M}(s \mid \alpha) \mid \tilde{\Sigma}_M = \sigma\right] \tag{B.3}$$

using expectation definition (35). If A_M verifies the conditions (56), $\tilde{S}_M \mid \boldsymbol{\alpha}_M$ converges in distribution toward a Gaussian distribution [42, p.263] such that, from dominated convergence theorem,

$$p_{\tilde{S}\,|\,\tilde{\Sigma}}(s \mid \sigma) = \mathbb{E}_t\left[\lim_{M\to+\infty} p_{\tilde{S}_M\,|\,\boldsymbol{\alpha}_M}(s \mid \alpha) \mid \tilde{\Sigma}_M = \sigma\right] \tag{B.4}$$

$$= \mathbb{E}_t\left[\frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{s^2}{2\sigma^2}}\right] = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{s^2}{2\sigma^2}}. \tag{B.5}$$

Therefore the random variable $\tilde{S}_M \mid (\tilde{\Sigma}_M = \sigma) \xrightarrow{\mathcal{L}} \mathcal{N}(0, \sigma)$. Moreover $\tilde{S}_M$ can be expressed as

$$p_{\tilde{S}_M}(s) = \mathbb{E}_t\left[p_{\tilde{S}_M}(s \mid \tilde{\Sigma}_M)\, \mathbb{1}_{I_{\tilde{\Sigma}}}\right]. \tag{B.6}$$

As $\tilde{\Sigma}_M \xrightarrow{\mathcal{L}} 1$, and from dominated convergence theorem,

$$p_{\tilde{S}}(s) = \lim_{M\to+\infty} p_{\tilde{S}_M}(s) = \lim_{M\to+\infty} \mathbb{E}_t\left[p_{\tilde{S}_M}(s \mid \tilde{\Sigma}_M)\, \mathbb{1}_{I_{\tilde{\Sigma}}}\right] \tag{B.7}$$

$$= \mathbb{E}_t\left[p_{\tilde{S}}(s \mid \tilde{\Sigma})\, \mathbb{1}_{\{\tilde{\Sigma}=1\}}\right] = \frac{1}{\sqrt{2\pi}} e^{-\frac{s^2}{2}}. \tag{B.8}$$

References

[1] M. L. Psiaki, T. E. Humphreys, GNSS Spoofing and Detection, Proc. IEEE 104 (6) (2016) 1258–1270.

[2] R. H. Mitch, R. C. Dougherty, M. L. Psiaki, S. P. Powell, B. W. O'Hanlon, J. A. Bhatti, T. E. Humphreys, Signal Characteristics of Civil GPS Jammers, in: Proc. ION GNSS 2011, 2011, pp. 1907–1919.

[3] T. Kraus, R. Bauernfeind, B. Eissfeller, Survey of In-Car Jammers-Analysis and Modeling of the RF Signals and IF Samples (Suitable for Active Signal Cancelation), in: Proc. ION GNSS 2011, 2011, pp. 430–435.

[4] D. Borio, F. Dovis, H. Kuusniemi, L. L. Presti, Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers, Proc. IEEE 104 (6) (2016) 1233–1245.

[5] D. Miralles, N. Levigne, D. M. Akos, J. Blanch, S. Lo, Android Raw GNSS Measurements as the New Anti-spoofing and Anti-jamming Solution, in: Proc. ION GNSS+ 2018, 2018, pp. 334–344.

[6] I. Fernández-Hernández, T. Walter, K. Alexander, B. Clark, E. Châtre, C. Hegarty, M. Appel, M. Meurer, Increasing International Civil Aviation Resilience: a Proposal for Nomenclature, Categorization and Treatment of new Interference Threats, in: Proc. ION ITM 2019, 2019, pp. 389–407.

[7] J. P. A. Pérez, S. C. Pueyo, B. C. López, Automatic Gain Control, Springer, 2011.

[8] P. J. Teunissen, O. Montenbruck, Springer Handbook of Global Navigation Satellite Systems, Vol. 10, Springer, 2017.

[9] F. Amoroso, Adaptive A/D Converter to Suppress CW Interference in DSPN Spread-Spectrum Communications, IEEE Trans. Commun. COM-31 (10) (1983) 1117–1123.

[10] F. Amoroso, J. Bricker, Performance of the Adaptive A/D Converter in Combined CW and Gaussian Onterference, IEEE Trans. Commun. COM-34 (3) (1986) 209–213.

[11] R. J. R. Thompson, E. Cetin, A. G. Dempster, Detection and Jammer-to-Noise Ratio Estimation of Interferers using the Automatic Gain Control, in: Proc. IGNSS Symp., 2011, pp. 1–14.

[12] N. Gault, A. Garcia-Pena, A. Chabory, C. Macabiau, Impact of DME/TACAN on GNSS L5/E5a Receivers at Low Altitude Considering Multipath, in: Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022), 2022, pp. 276–303.

[13] F. Bastide, D. Akos, C. Macabiau, B. Roturier, Automatic Gain Control (AGC) as an Interference Assessment Tool, in: Proc. ION GPS/GNSS 2003, 2003, pp. 2042–2053.

[14] X. Dai, J. Nie, B. Li, Z. Lu, G. Ou, Performance of GNSS Receivers with AGC in Noise Pulse Interference, in: Proc. ICCSNT 2016, 2016, pp. 735–740.

[15] C. Hegarty, A. Van Dierendonck, D. Bobyn, M. Tran, J. Grabowski, Suppression of pulsed interference through blanking, in: Proc. 56th ION AM, 2000, pp. 399–408.

[16] C. J. Hegarty, Analytical Model for GNSS Receiver Implementation Losses, Navigation 58 (1) (2011) 29–44.

[17] H. Issa, G. Stienne, S. Reboul, M. Semmling, M. Raad, G. Faour, J. Wickert, A Probabilistic Model for On-line Estimation of the GNSS Carrier-to-noise Ratio, Signal Processing 183 (2021) 107992.

[18] M. Hussong, E. Ghizzo, C. Milner, A. Garcia-Pena, J. Lesouple, C. Macabiau, Impact of Meaconers on Aircraft GNSS Receivers During Approaches, in: Proc. ION GNSS+ 2023, 2023, pp. 856–880.

[19] Y. Liu, Y. Ran, T. Ke, X. Hu, Code Tracking Performance Analysis of GNSS Signal in the Presence of CW Interference, Signal Processing 91 (4) (2011) 970–987.

[20] M. Sahmoudi, M. G. Amin, Robust Tracking of Weak GPS Signals in Multipath and Jamming Environments, Signal Processing 89 (7) (2009) 1320–1333.

[21] E. Ghizzo, A. G. Pena, J. Lesouple, C. Milner, C. Macabiau, Assessing GNSS Carrier-to-Noise-Density Ratio Estimation in The Presence of Meaconer Interference, in: Proc. ICASSP 2024, 2024, pp. 8971–8975.

[22] E. Axell, F. M. Eklöf, P. Johansson, M. Alexandersson, D. M. Akos, Jamming Detection in GNSS Receivers: Performance Evaluation of Field Trials, Navigation 62 (1) (2015) 73–82.

[23] D. M. Akos, Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via automatic Gain Control (AGC), Navigation 59 (4) (2012) 281–290.

[24] S. Lo, F. Rothmaier, D. Miralles, D. Akos, T. Walter, Developing a Practical GNSS Spoofing Detection Thresholds for Receiver Power Monitoring, in: Proc. ION GNSS+ 2021, 2021, pp. 803–815.
[25] C. Hegarty, A. Odeh, K. Shallberg, K. Wesson, T. Walter, K. Alexander, Spoofing Detection for Airborne GNSS Equipment, in: Proc. ION GNSS+ 2018, 2018, pp. 1350–1368.
[26] O. Isoz, D. Akos, T. Lindgren, C.-C. Sun, S.-S. Jan, Assessment of GPS L1/Galileo E1 Interference Monitoring System for the Airport Environment, in: Proc. ION GNSS 2011, 2011, pp. 1920–1930.
[27] Y. Wang, Y. Li, G. Yu, Y. Li, Z. Zhou, X. Geng, Interference mitigation for FMCW radar via chirp rate estimation and signal separation, Signal Processing 222 (2024) 109537.
[28] D. Borio, C. O'Driscoll, J. Fortuny, GNSS Jammers: Effects and Countermeasures, in: Proc. Navitec 2012, IEEE, 2012, pp. 1–7.
[29] F. Gianfelici, C. Turchetti, P. Crippa, A non-probabilistic recognizer of stochastic signals based on KLT, Signal Processing 89 (4) (2009) 422–437.
[30] Z.-X. Guo, X.-H. Bai, J.-Y. Li, P.-L. Shui, J. Su, L. Wang, Small target detection in sea clutter using dominant clutter tree based on anomaly detection framework, Signal Processing 219 (2024) 109399.
[31] C. Chen, K. Sun, S. He, An improved image encryption algorithm with finite computing precision, Signal Processing 168 (2020) 107340.
[32] M. Coulon, A. Chabory, A. Garcia Peña, J. Vezinet, C. Macabiau, P. Estival, P. Ladoux, B. Roturier, Characterization of Meaconing and its Impact on GNSS Receivers, in: Proc. ION GNSS+ 2020, St. Louis, MO, USA, 2020, pp. 3713–3737.
[33] E. Rebeyrol, C. Macabiau, L. Lestarquit, L. Ries, J.-L. Issler, M.-L. Boucheret, M. Bousquet, BOC Power Spectrum Densities, in: Proc. ION NTM 2005, 2005, pp. 769–778.
[34] U. L. Rohde, J. C. Whitaker, H. Zahnd., Communications Receivers: Principles and Design. 2th ed, New York : McGraw-Hill Education, 1997.
[35] P. Walters, An Introduction to Ergodic Theory, Vol. 79, Springer Science & Business Media, 2000.
[36] P. Billingsley, Probability and Measure, John Wiley & Sons, 2017.
[37] M. Abdizadeh, J. T. Curran, G. Lachapelle, Quantization Effects in GNSS Receivers in the Presence of Interference, in: Proceedings of the 2012 International Technical Meeting of The Institute of Navigation, 2012, pp. 742–779.
[38] F. D. Nunes, F. M. Sousa, GNSS Blind Interference Detection Based on Fourth-Order Autocumulants, IEEE Transactions on Aerospace and Electronic Systems 52 (5) (2016) 2574–2586.
[39] R. Couillet, M. Debbah, Random matrix methods for wireless communications, Cambridge University Press, 2011.
[40] Y. Takahashi, Markov Chains with Random Transition Matrices, in: Kodai Mathematical Seminar Reports, Vol. 21, Department of Mathematics, Tokyo Institute of Technology, 1969, pp. 426–447.
[41] H. Weyl, Über die Gleichverteilung von Zahlen Mod. Eins, Mathematische Annalen 77 (3) (1916) 313–352.
[42] A. Zygmund, Trigonometric Series, Vol. 2, Cambridge University Press, 2002.