GNSS Receiver Signal Processing Under Spoofing

Emile GHIZZO

ENAC Telecom, Toulouse

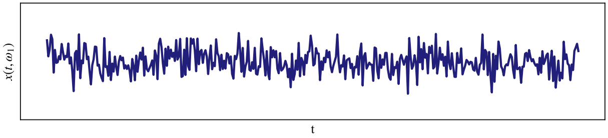
Seminar Presentation

October 17, 2025

A Probabilistic Framework for Non-ergodic Signals

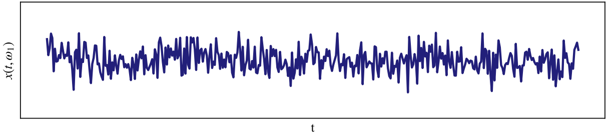
Time-based estimation under non-ergodicity

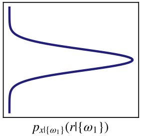
$$y(t, \omega_1) = x(t, \omega_1)$$



Time-based estimation under non-ergodicity

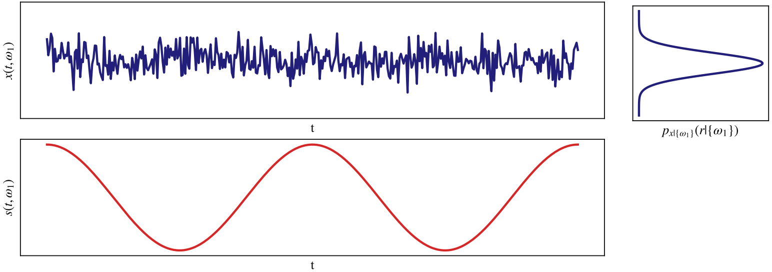
$$y(t,\omega_1) = \underbrace{x(t,\omega_1)}_{\text{Gaussian}}$$





Time-based estimation under non-ergodicity

$$y(t,\omega_1) = \underbrace{x(t,\omega_1)}_{\text{Gaussian}} + \overbrace{s(t,\omega_1)}^{\text{Continuous wave (CW)}}$$

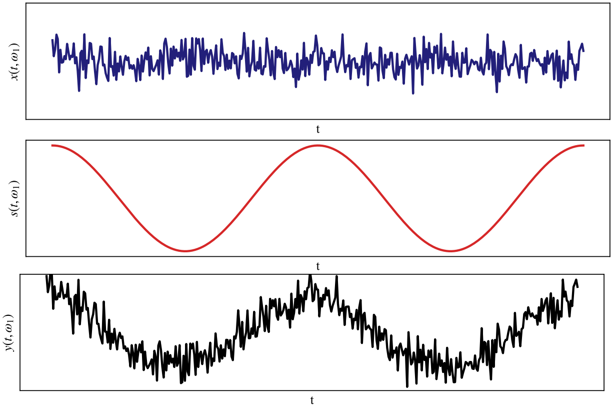


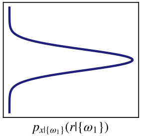
Time-based estimation under non-ergodicity

Continuous wave (CW)

$$y(t,\omega_1) = x(t,\omega_1) + s(t,\omega_1)$$

Gaussian





Ergodicity

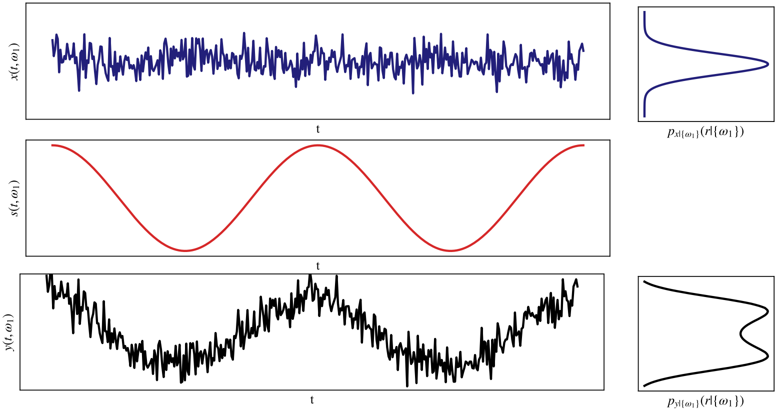
Ergodicity allows the statistical properties of a signal to be inferred from a single realization, ω_1, observed over a time interval I_t.

Time-based estimation under non-ergodicity

Continuous wave (CW)

$$y(t,\omega_1) = x(t,\omega_1) + s(t,\omega_1)$$

Gaussian



Ergodicity

Ergodicity allows the statistical properties of a signal to be inferred from a single realization, ω_1, observed over a time interval I_t.

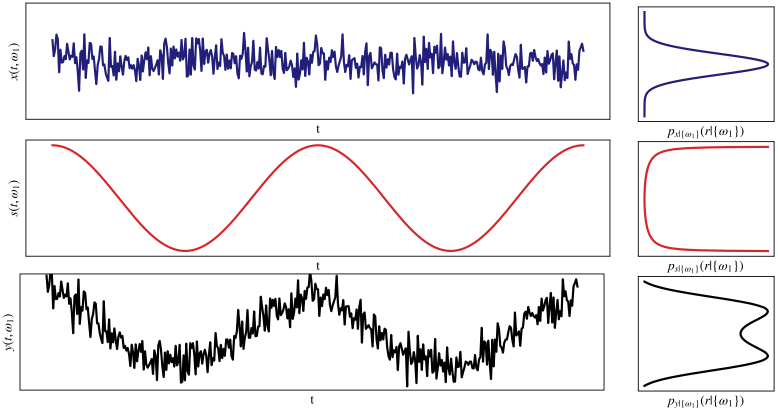
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Time-based estimation under non-ergodicity

Continuous wave (CW)

$$y(t,\omega_1) = x(t,\omega_1) + s(t,\omega_1)$$

Gaussian

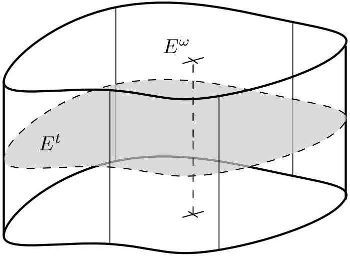


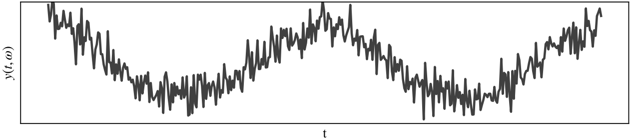
Ergodicity

Ergodicity allows the statistical properties of a signal to be inferred from a single realization, ω_1, observed over a time interval I_t.

Proposed framework (1/2)

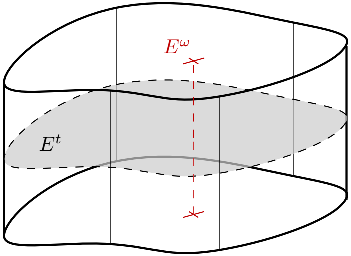
$$\left(I_t \times I_\Omega \,,\, \mathcal{E}_\Omega \otimes \mathcal{E}_t \,,\, \mathbb{P}_{t\times\Omega} \right)$$

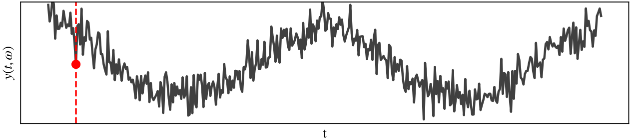


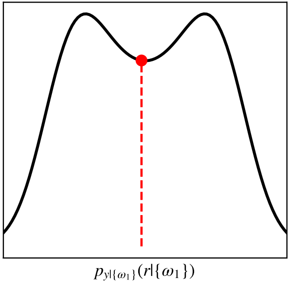


Proposed framework (1/2)

$$\left(\boxed{I_t} \times I_\Omega \;, \boxed{\mathcal{E}_\Omega} \otimes \mathcal{E}_t \;, \mathbb{P}_{\boxed{t}\times\Omega} \right)$$





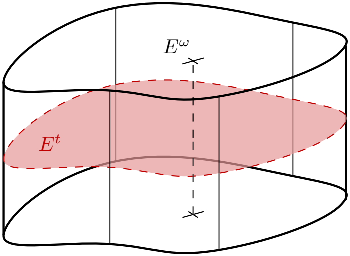


Time probability space:

$$(I_t, \mathcal{E}_t, \mathbb{P}_t)$$

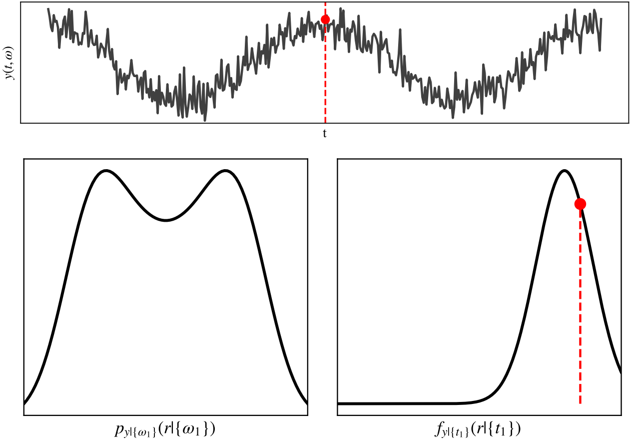
Proposed framework (1/2)

$$(I_t \times I_\Omega ,\ \mathcal{E}_\Omega \otimes \mathcal{E}_t ,\mathbb{P}_{t\times \Omega})$$



Random probability space:

$$(I_\Omega, \mathcal{E}_\Omega, \mathbb{P}_\Omega)$$



Proposed framework (2/2)

Measure Theory Framework: Consider the time interval as a probability space, with the observed signal represented as a random variable over the total event space:

- **Time Probability Space:** Captures the signal realization over time
- **Random Probability Space:** Captures the randomness of the observed signal.
- **Total Probability Space:** Combines the time and random realizations of the signal.

Measure Theory Framework

Proposed framework (2/2)

Measure Theory Framework: Consider the time interval as a probability space, with the observed signal represented as a random variable over the total event space:

- **Time Probability Space:** Captures the signal realization over time
- **Random Probability Space:** Captures the randomness of the observed signal.
- **Total Probability Space:** Combines the time and random realizations of the signal.

Measure Theory Framework

✓ Probability theory enables formal definitions of power, distribution, and independence within each probability space.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Proposed framework (2/2)

Measure Theory Framework: Consider the time interval as a probability space, with the observed signal represented as a random variable over the total event space:

- **Time Probability Space:** Captures the signal realization over time
- **Random Probability Space:** Captures the randomness of the observed signal.
- **Total Probability Space:** Combines the time and random realizations of the signal.

Measure Theory Framework

- ✓ Probability theory enables formal definitions of power, distribution, and independence within each probability space.
- ✓ Provides a basis for defining properties such as ergodicity and stationarity.

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Proposed framework (2/2)

Measure Theory Framework: Consider the time interval as a probability space, with the observed signal represented as a random variable over the total event space:

- **Time Probability Space:** Captures the signal realization over time
- **Random Probability Space:** Captures the randomness of the observed signal.
- **Total Probability Space:** Combines the time and random realizations of the signal.

Measure Theory Framework

- ✓ Probability theory enables formal definitions of power, distribution, and independence within each probability space.
- ✓ Provides a basis for defining properties such as ergodicity and stationarity.
- ✓ Facilitates the analysis of classical signals (e.g., Markov processes, CW, multiple CWs).

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

What is GNSS spoofing?

What is GNSS spoofing?

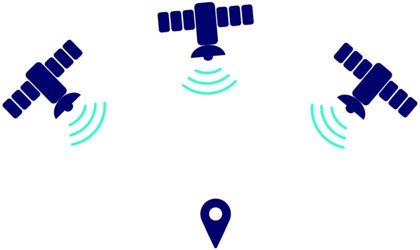
Definition

GNSS like signal capable of deceiving a receiver and inducing erroneous Position, Velocity, and Time (PVT) solutions.

What is GNSS spoofing?

Definition

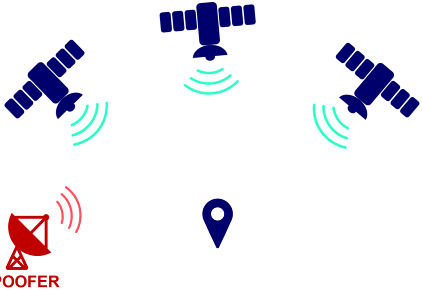
GNSS like signal capable of deceiving a receiver and inducing erroneous Position, Velocity, and Time (PVT) solutions.



What is GNSS spoofing?

Definition

GNSS like signal capable of deceiving a receiver and inducing erroneous Position, Velocity, and Time (PVT) solutions.



What is GNSS spoofing?

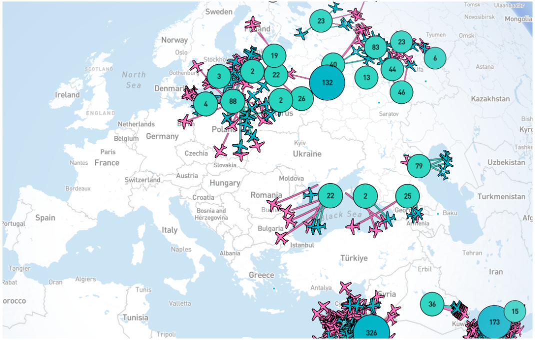
Definition

GNSS like signal capable of deceiving a receiver and inducing erroneous Position, Velocity, and Time (PVT) solutions.

What is GNSS spoofing?

Definition

GNSS like signal capable of deceiving a receiver and inducing erroneous Position, Velocity, and Time (PVT) solutions.

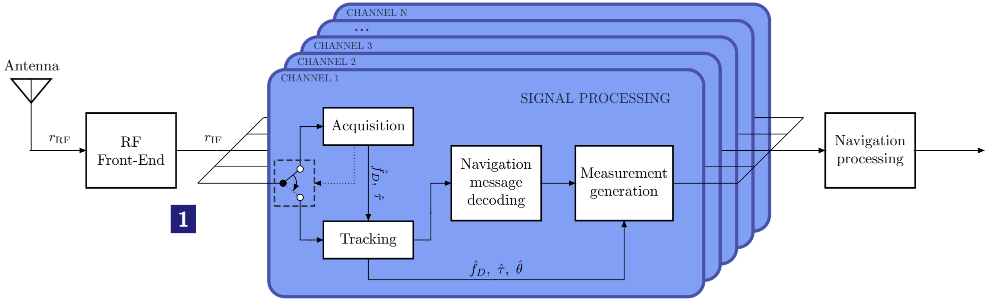


Recorded spoofing events on aircraft receivers (06/11/2025)

https://spoofing.skai-data-services.com/

Which stages of GNSS receivers are affected by spoofing?

Which stages of GNSS receivers are affected by spoofing?

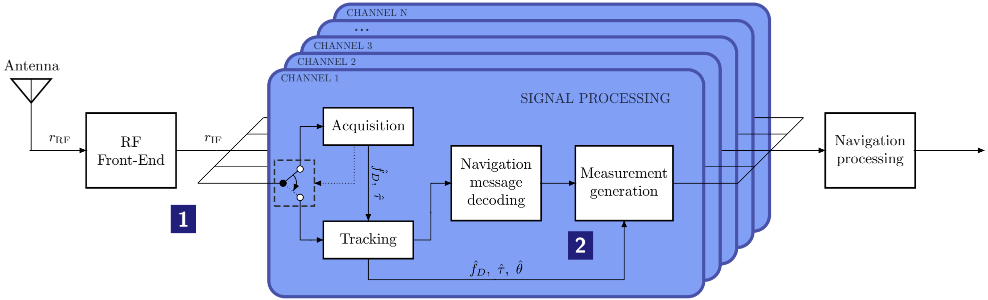


1

- Automatic Gain Control (AGC) [1]
- Signal prior to correlation (power, distribution) [1]

[1] Emile Ghizzo et al. "Assessing jamming and spoofing impacts on GNSS receivers: Automatic gain control (AGC)". In: *Signal Processing* 228 (2025), p. 109762

Which stages of GNSS receivers are affected by spoofing?

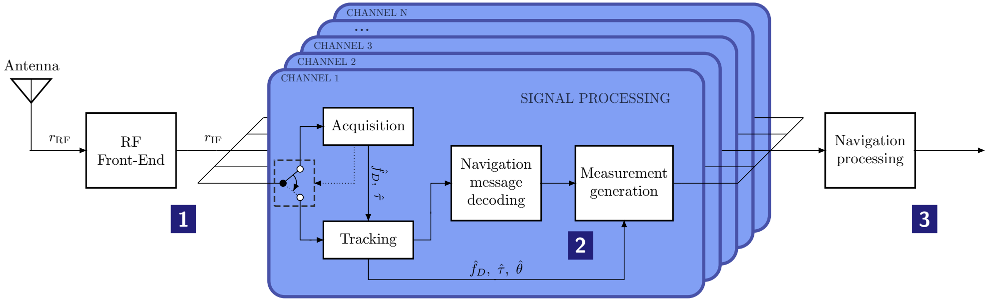


1
- Automatic Gain Control (AGC)
- Signal prior to correlation (power, distribution)

2
- Signal post-correlation [2] [4]
- Synchronization estimates [3]
- C/N_0, power [4]

[2] Mathieu Hussong et al. "Impact of Meaconers on Aircraft GNSS Receivers During Approaches". In: *Proc. ION GNSS+ 2023*. Sept. 2023, pp. 856–880
[3] Emile Ghizzo et al. "Assessing Spoofer Impact on GNSS Receivers: Tracking Loops". In: *NAVIGATION: Journal of the Institute of Navigation* 72.4 (2025)
[4] Emile Ghizzo, Julien Lesouple, and Carl Milner. "Assessing jamming and spoofing impacts on GNSS receivers: Carrier-to-Noise density Ratio". In: *Signal Processing* (2025)

Which stages of GNSS receivers are affected by spoofing?



1
- Automatic Gain Control (AGC)
- Signal prior to correlation (power, distribution)

2
- Signal post-correlation
- Synchronization estimates
- C/N_0, power

3
- Pseudoranges [5]
- Position [5]
- Residuals

[5] Mathieu Hussong et al. "GNSS performance degradation under meaconing in civil aviation: pseudorange and position models". In: *GPS Solutions* 29.3 (2025), p. 93

Objectives

Objectives

Characterize the impact of spoofing on GNSS receiver signal processing, both before and after correlation.

Objectives

Objectives

Characterize the impact of spoofing on GNSS receiver signal processing, both before and after correlation.

Contributions

Objectives

Objectives

Characterize the impact of spoofing on GNSS receiver signal processing, both before and after correlation.

Contributions

- Introduced a measure-theoretic framework to **study time-based estimation under non-ergodic conditions.**

Objectives

Objectives

Characterize the impact of spoofing on GNSS receiver signal processing, both before and after correlation.

Contributions

- Introduced a measure-theoretic framework to **study time-based estimation under non-ergodic conditions.**
- Derived theoretical models to **predict spoofing impact both before correlation and after correlation**.

Objectives

Objectives

Characterize the impact of spoofing on GNSS receiver signal processing, both before and after correlation.

Contributions

- Introduced a measure-theoretic framework to **study time-based estimation under non-ergodic conditions.**
- Derived theoretical models to **predict spoofing impact both before correlation and after correlation**.
- Identified specific spoofing situations where GNSS receivers **exhibit harmful distortions**, including tracking loop chaotic behaviors (e.g., high oscillations, bifurcations) and significant C/N_0 degradation.

REPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Outline

Outline

Outline

Received signal model

$$r_{\mathrm{RF}}(t) = \Re\left\{ \left[\sum_{i \in \mathcal{M}_{\mathrm{a}}(t)} \sqrt{C_{\mathrm{a}}^{i}(t)}\; s_i(t - \tau_{\mathrm{a}}^{i}(t))e^{j\,\theta_{\mathrm{a}}^{i}(t)} + \sum_{i \in \mathcal{M}_{\mathrm{s}}(t)} \sqrt{C_{\mathrm{s}}^{i}(t)}\; s_i(t - \tau_{\mathrm{s}}^{i}(t))e^{j\,\theta_{\mathrm{s}}^{i}(t)} \right] \exp(2j\pi f_0 + j\theta_0) + n_{\mathrm{a}}(t) + n_{\mathrm{s}}(t) \right\}$$

$s_i(t)$: GNSS signal of the i^{th} satellite (Navigation message and spreading signal)

Received signal model

Authentic dynamic

$$r_{\mathrm{RF}}(t) = \Re\left\{\left[\sum_{i\in\mathcal{M}_{\mathrm{a}}(t)} \sqrt{\boxed{C_{\mathrm{a}}^i(t)}}\, s_i(t - \boxed{\tau_{\mathrm{a}}^i(t)})e^{j\,\boxed{\theta_{\mathrm{a}}^i(t)}} + \sum_{i\in\mathcal{M}_{\mathrm{s}}(t)} \sqrt{C_{\mathrm{s}}^i(t)}\, s_i(t - \tau_{\mathrm{s}}^i(t))e^{j\,\theta_{\mathrm{s}}^i(t)}\right]\exp\left(2j\pi f_0 + j\theta_0\right) + n_{\mathrm{a}}(t) + n_{\mathrm{s}}(t)\right\}$$

$s_i(t)$: GNSS signal of the i^{th} satellite (Navigation message and spreading signal)

τ_{a}^i, θ_{a}^i: Authentic signal code and carrier delay (Doppler modeled by their variation)

Received signal model

Authentic dynamic

$$r_{\mathrm{RF}}(t) = \Re\left\{\left[\sum_{i\in\mathcal{M}_{\mathrm{a}}(t)} \sqrt{C_{\mathrm{a}}^{i}(t)}\, s_i(t - \tau_{\mathrm{a}}^{i}(t))e^{j\,\theta_{\mathrm{a}}^{i}(t)} + \sum_{i\in\mathcal{M}_{\mathrm{s}}(t)} \sqrt{C_{\mathrm{s}}^{i}(t)}\, s_i(t - \tau_{\mathrm{s}}^{i}(t))e^{j\,\theta_{\mathrm{s}}^{i}(t)}\right]\exp(2j\pi f_0 + j\theta_0) + n_{\mathrm{a}}(t) + n_{\mathrm{s}}(t)\right\}$$

$s_i(t)$: GNSS signal of the i^{th} satellite (Navigation message and spreading signal)

τ_{a}^{i}, θ_{a}^{i}: Authentic signal code and carrier delay (Doppler modeled by their variation)

Received signal model

Authentic dynamic

$$r_{\mathrm{RF}}(t) = \Re\left\{ \left[\sum_{i \in \mathcal{M}_{\mathrm{a}}(t)} \sqrt{C_{\mathrm{a}}^{i}(t)}\, s_i(t - \tau_{\mathrm{a}}^{i}(t))\, e^{j\,\theta_{\mathrm{a}}^{i}(t)} + \sum_{i \in \mathcal{M}_{\mathrm{s}}(t)} \sqrt{C_{\mathrm{s}}^{i}(t)}\, s_i(t - \tau_{\mathrm{s}}^{i}(t))\, e^{j\,\theta_{\mathrm{s}}^{i}(t)} \right] \exp\left(2j\pi f_0 + j\theta_0\right) + n_{\mathrm{a}}(t) + n_{\mathrm{s}}(t) \right\}$$

Spoofing dynamic

$s_i(t)$: GNSS signal of the i^{th} satellite (Navigation message and spreading signal)

τ_{a}^{i}, θ_{a}^{i}: Authentic signal code and carrier delay (Doppler modeled by their variation)

τ_{s}^{i}, θ_{s}^{i}: Spoofing signal code and carrier delay (Doppler modeled by their variation)

Received signal model

Authentic dynamic

$$r_{\mathrm{RF}}(t) = \Re\left\{ \left[\sum_{i \in \mathcal{M}_{\mathrm{a}}(t)} \sqrt{\boxed{C_{\mathrm{a}}^{i}(t)}}\, s_i(t - \boxed{\tau_{\mathrm{a}}^{i}(t)})e^{j\boxed{\theta_{\mathrm{a}}^{i}(t)}} + \sum_{i \in \mathcal{M}_{\mathrm{s}}(t)} \sqrt{\boxed{C_{\mathrm{s}}^{i}(t)}}\, s_i(t - \boxed{\tau_{\mathrm{s}}^{i}(t)})e^{j\boxed{\theta_{\mathrm{s}}^{i}(t)}} \right] \exp\left(2j\pi f_0 + j\theta_0\right) + n_{\mathrm{a}}(t) + n_{\mathrm{s}}(t) \right\}$$

Spoofing dynamic

$s_i(t)$: GNSS signal of the i^{th} satellite (Navigation message and spreading signal)

τ_{a}^{i}, θ_{a}^{i}: Authentic signal code and carrier delay (Doppler modeled by their variation)

τ_{s}^{i}, θ_{s}^{i}: Spoofing signal code and carrier delay (Doppler modeled by their variation)

Received signal model

$$r_{\mathrm{RF}}(t) = \Re\left\{\left[\sum_{i\in\mathcal{M}_{\mathrm{a}}(t)} \sqrt{C_{\mathrm{a}}^{i}(t)}\, s_i(t - \tau_{\mathrm{a}}^{i}(t))e^{j\,\theta_{\mathrm{a}}^{i}(t)} + \sum_{i\in\mathcal{M}_{\mathrm{s}}(t)} \sqrt{C_{\mathrm{s}}^{i}(t)}\, s_i(t - \tau_{\mathrm{s}}^{i}(t))e^{j\,\theta_{\mathrm{s}}^{i}(t)}\right]\exp\left(2j\pi f_0 + j\theta_0\right) + n_{\mathrm{a}}(t) + n_{\mathrm{s}}(t)\right\}$$

Authentic dynamic

Spoofing dynamic

$s_i(t)$: GNSS signal of the i^{th} satellite (Navigation message and spreading signal)

τ_{a}^{i}, θ_{a}^{i}: Authentic signal code and carrier delay (Doppler modeled by their variation)

τ_{s}^{i}, θ_{s}^{i}: Spoofing signal code and carrier delay (Doppler modeled by their variation)

Received signal model

$$r_{\mathrm{RF}}(t) = \Re\left\{\left[\sum_{i\in\mathcal{M}_a(t)} \sqrt{\underbrace{C_a^i(t)}_{\text{Authentic dynamic}}}\, s_i(t - \tau_a^i(t))e^{j\theta_a^i(t)} + \sum_{i\in\mathcal{M}_s(t)} \sqrt{C_s^i(t)}\, s_i(t - \underbrace{\tau_s^i(t)}_{\text{Spoofing dynamic}})e^{j\theta_s^i(t)}\right]\exp\left(2j\pi f_0 + j\theta_0\right) + \underbrace{n_a(t)}_{\text{Nominal AWGN}} + n_s(t)\right\}$$

$s_i(t)$: GNSS signal of the i^{th} satellite (Navigation message and spreading signal)

τ_a^i, θ_a^i: Authentic signal code and carrier delay (Doppler modeled by their variation)

τ_s^i, θ_s^i: Spoofing signal code and carrier delay (Doppler modeled by their variation)

Received signal model

$$r_{\mathrm{RF}}(t) = \Re\left\{\left[\sum_{i\in\mathcal{M}_a(t)} \sqrt{\overbrace{C_a^i(t)}^{}}\, s_i(t - \overbrace{\tau_a^i(t)}^{\text{Authentic dynamic}})e^{j\,\theta_a^i(t)} + \sum_{i\in\mathcal{M}_s(t)} \sqrt{C_s^i(t)}\, s_i(t - \underbrace{\tau_s^i(t)}_{\text{Spoofing dynamic}})e^{j\,\theta_s^i(t)}\right]\exp\left(2j\pi f_0 + j\theta_0\right) + \underbrace{n_a(t)}_{\text{Nominal AWGN}} + \overbrace{n_s(t)}^{\text{Re-radiated AWGN}}\right\}$$

$s_i(t)$: GNSS signal of the i^{th} satellite (Navigation message and spreading signal)

τ_a^i, θ_a^i: Authentic signal code and carrier delay (Doppler modeled by their variation)

τ_s^i, θ_s^i: Spoofing signal code and carrier delay (Doppler modeled by their variation)

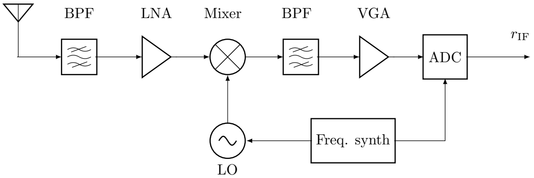
Outline

Impact of spoofing on the RFFE

Objectives

- Characterize the signal at RFFE output
- Characterize the AGC dynamic response

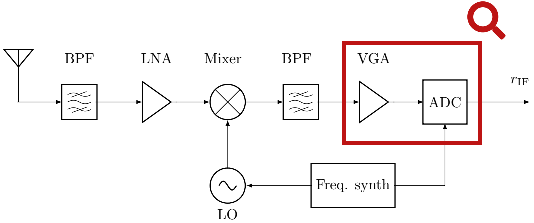
Impact of spoofing on the RFFE



Objectives

- Characterize the signal at RFFE output
- Characterize the AGC dynamic response

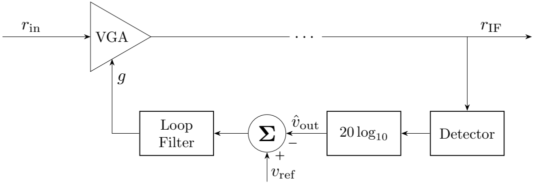
Impact of spoofing on the RFFE



Objectives

- Characterize the signal at RFFE output
- Characterize the AGC dynamic response

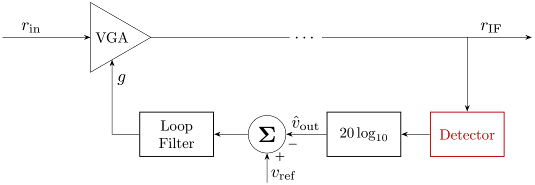
Impact of spoofing on the RFFE



Objectives

- Characterize the signal at RFFE output
- Characterize the AGC dynamic response

Impact of spoofing on the RFFE



Objectives

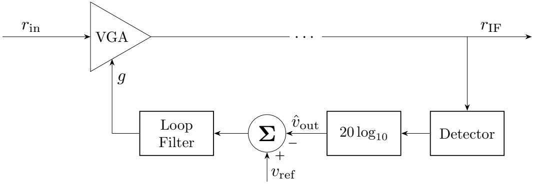
- Characterize the signal at RFFE output
- Characterize the AGC dynamic response

Two Types of Detectors:[1]

- **Power-based:** Computed from the time-domain power over the estimation time I_t.
- **Distribution-based:** Computed from the time-domain distribution over I_t.

[1] Juan Pablo Alegre Pérez, Santiago Celma Pueyo, and Belén Calvo López. *Automatic Gain Control.* Springer, 2011

Impact of spoofing on the RFFE



Objectives

- Characterize the signal at RFFE output
- Characterize the AGC dynamic response

AGC dynamic model:

$$\overset{\text{VGA gain}}{g(s)} = \frac{F(s)}{1 + F(s)} \left(v_{\text{ref}}(s) - v_{\text{in}}(s) \right)$$

$$v_{\text{out}}(s) = g(s) + v_{\text{in}}(s)$$

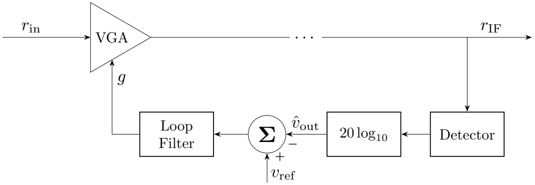
Two Types of Detectors:[1]

- **Power-based:** Computed from the time-domain power over the estimation time I_t.
- **Distribution-based:** Computed from the time-domain distribution over I_t.

[1] Juan Pablo Alegre Pérez, Santiago Celma Pueyo, and Belén Calvo López. *Automatic Gain Control*. Springer, 2011

RÉPUBLIQUE FRANÇAISE Liberté Égalité Fraternité

Impact of spoofing on the RFFE



Objectives

- Characterize the signal at RFFE output
- Characterize the AGC dynamic response

AGC dynamic model:

$$\overbrace{g(s)}^{\text{VGA gain}} = \frac{F(s)}{1 + \underbrace{F(s)}_{\text{Low-pass filter}}} \left(v_{\mathrm{ref}}(s) - v_{\mathrm{in}}(s) \right)$$

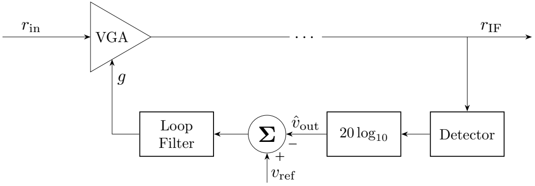
$$v_{\mathrm{out}}(s) = g(s) + v_{\mathrm{in}}(s)$$

Two Types of Detectors:[1]

- **Power-based:** Computed from the time-domain power over the estimation time I_t.
- **Distribution-based:** Computed from the time-domain distribution over I_t.

[1] Juan Pablo Alegre Pérez, Santiago Celma Pueyo, and Belén Calvo López. *Automatic Gain Control.* Springer, 2011

Impact of spoofing on the RFFE



Objectives

- Characterize the signal at RFFE output
- Characterize the AGC dynamic response

AGC dynamic model:

$$\overbrace{g(s)}^{\text{VGA gain}} = \frac{F(s)}{1+\underbrace{F(s)}_{\text{Low-pass filter}}}\left(v_{\text{ref}}(s) - v_{\text{in}}(s)\right)$$

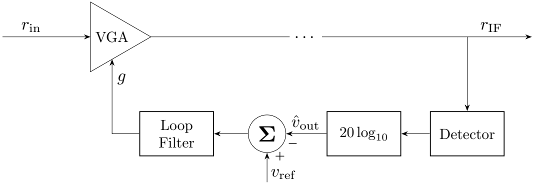
$$v_{\text{out}}(s) = g(s) + v_{\text{in}}(s)$$

Two Types of Detectors:[1]

- **Power-based:** Computed from the time-domain power over the estimation time I_t.
- **Distribution-based:** Computed from the time-domain distribution over I_t.

[1] Juan Pablo Alegre Pérez, Santiago Celma Pueyo, and Belén Calvo López. *Automatic Gain Control.* Springer, 2011

Impact of spoofing on the RFFE



Objectives

- Characterize the signal at RFFE output
- Characterize the AGC dynamic response

AGC dynamic model:

$$\overbrace{g(s)}^{\text{VGA gain}} = \frac{F(s)}{1 + \underbrace{F(s)}_{\text{Low-pass filter}}} \left(v_{\text{ref}}(s) - \overbrace{v_{\text{in}}(s)}^{\text{Input signal level}} \right)$$

$$v_{\text{out}}(s) = g(s) + v_{\text{in}}(s)$$

Two Types of Detectors:[1]

- **Power-based:** Computed from the time-domain power over the estimation time I_t.
- **Distribution-based:** Computed from the time-domain distribution over I_t.

[1] Juan Pablo Alegre Pérez, Santiago Celma Pueyo, and Belén Calvo López. *Automatic Gain Control.* Springer, 2011

Spoofing impact on signal level

Signal Level v

Describes the strength of the signal r. It can be defined through the signal power or its distribution within the estimation interval I_t, depending on the type of detector.

Spoofing impact on signal level

Signal Level v

Describes the strength of the signal r. It can be defined through the signal power or its distribution within the estimation interval I_t, depending on the type of detector.

Spoofing signal model:

$$r_{\mathrm{s}}(t) = \sum_{m=1}^{M} a_{\mathrm{s},m} \; s_m \left(t - \tau_{\mathrm{s},m}\right) \cos\left(2\pi \, f_m \, t + \theta_m\right)$$

Spoofing impact on signal level

Signal Level v

Describes the strength of the signal r. It can be defined through the signal power or its distribution within the estimation interval I_t, depending on the type of detector.

Spoofing signal model:

Signal parameters (constant over I_t)

$$r_s(t) = \sum_{m=1}^{M} \boxed{a_{s,m}}\; s_m \left(t - \boxed{\tau_{s,m}}\right) \cos\left(2\pi \boxed{f_m}\, t + \boxed{\theta_m}\right)$$

Spoofing impact on signal level

Signal Level v

Describes the strength of the signal r. It can be defined through the signal power or its distribution within the estimation interval I_t, depending on the type of detector.

Spoofing signal model:

Signal parameters (constant over I_t)

$$r_s(t) = \sum_{m=1}^{M} a_{s,m} \, s_m \left(t - \tau_{s,m}\right) \cos\left(2\pi f_m t + \theta_m\right)$$

Spoofing impact on signal level

Signal Level v

Describes the strength of the signal r. It can be defined through the signal power or its distribution within the estimation interval I_t, depending on the type of detector.

Spoofing signal model:

Number of GNSS signals

Signal parameters (constant over I_t)

$$r_s(t) = \sum_{m=1}^{M} a_{s,m} \, s_m \left(t - \tau_{s,m}\right) \cos\left(2\pi f_m t + \theta_m\right)$$

Spoofing impact on signal level

Signal Level v

Describes the strength of the signal r. It can be defined through the signal power or its distribution within the estimation interval I_t, depending on the type of detector.

Spoofing signal model:

$$r_s(t) = \sum_{m=1}^{\overbrace{M}^{\text{Number of GNSS signals}}} a_{s,m} \, s_m \left(t - \tau_{s,m}\right) \cos\left(2\pi f_m t + \theta_m\right)$$

Signal parameters (constant over I_t): $a_{s,m}$, $\tau_{s,m}$, f_m, θ_m

Results

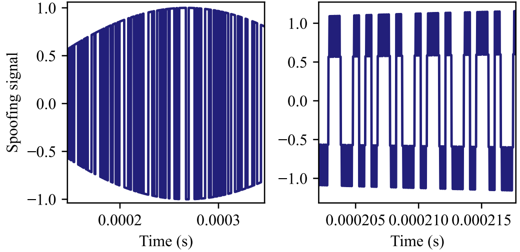
The input signal level v_{in} (and, consequently, the AGC) can be determined by computing its power and distribution.

Individual PRN spoofing signal ($M = 1$)

Results

The individual PRN signal is shown to be equivalent to a weighted **continuous wave (CW)**, modeled through the proposed **measure theory framework**.

Signal time evolution:



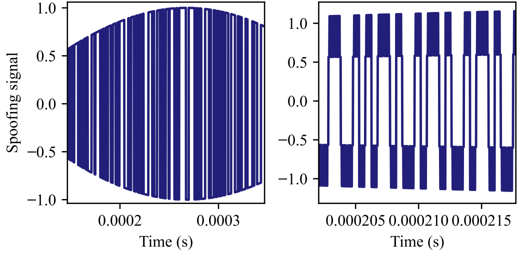
(a) BPSK (b) CBOC

Individual PRN spoofing signal ($M = 1$)

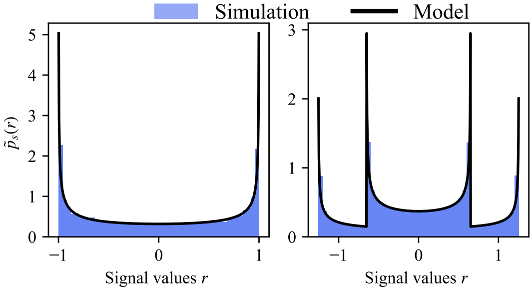
Results

The individual PRN signal is shown to be equivalent to a weighted **continuous wave (CW)**, modeled through the proposed **measure theory framework**.

Signal time evolution:



(a) BPSK (b) CBOC

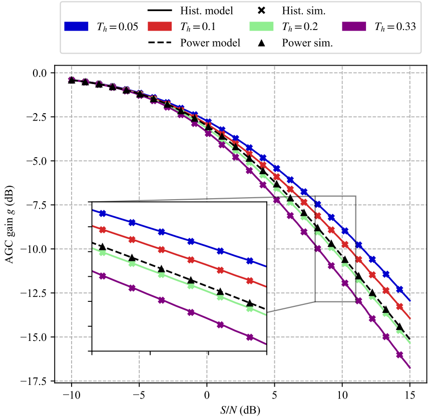


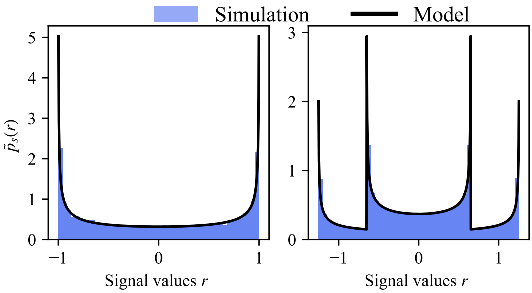
(a) BPSK (b) CBOC

Individual PRN spoofing signal ($M = 1$)

Results

The individual PRN signal is shown to be equivalent to a weighted **continuous wave (CW)**, modeled through the proposed **measure theory framework**.





(a) BPSK (b) CBOC

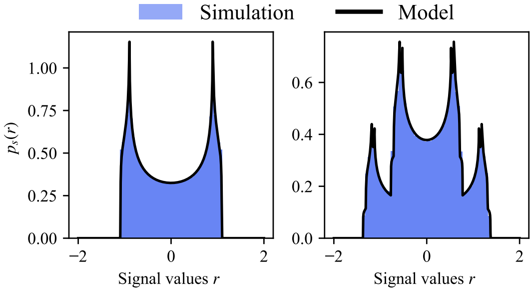
S/N: Spoofing-to-Noise power ratio

Multiple PRN Spoofing Signal ($M > 1$)

Results

- Equivalent to multiple weighted CWs.

Signal distribution (M=2):



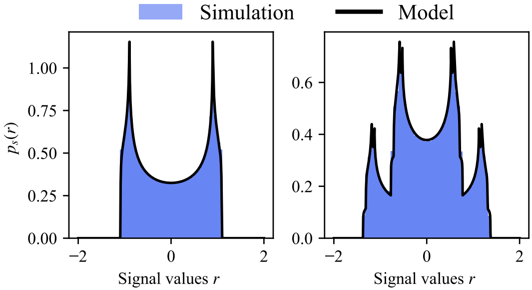
(a) BPSK (b) CBOC

Multiple PRN Spoofing Signal ($M > 1$)

Results

- Equivalent to multiple weighted CWs.
- Distribution depends on the relative amplitudes between CWs.

Signal distribution (M=2):

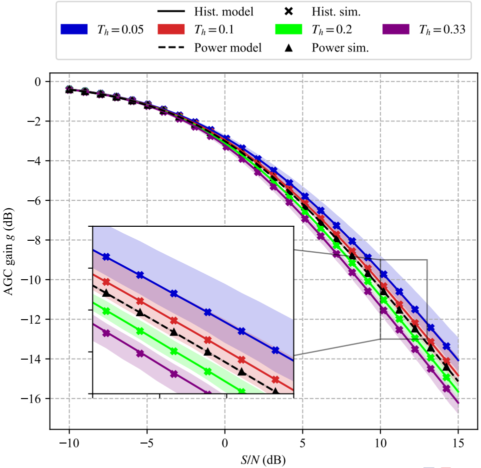


(a) BPSK (b) CBOC

Multiple PRN Spoofing Signal ($M > 1$)

Results

- Equivalent to multiple weighted CWs.
- Distribution depends on the relative amplitudes between CWs.

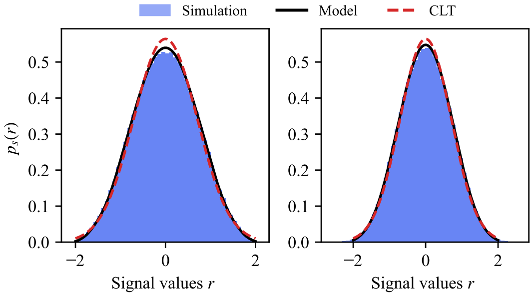


Multiple PRN Spoofing Signal ($M > 1$)

Results

- Equivalent to multiple weighted CWs.
- Distribution depends on the relative amplitudes between CWs.
- The signal converges toward a normal distribution as $M \to +\infty$ (Central Limit Theorem, CLT).

Signal distribution (M=5):



(a) BPSK (b) CBOC

Conclusion on spoofing impact before correlation

Spoofing Impact Before Correlation

The AGC dynamic response can be characterized through the input signal level (and thus signal power and distribution).

The spoofing impact can be modeled as weighted continuous waves (CWs), analyzed similarly to a jammer:

- $M = 1$**:** Equivalent to a single weighted CW.
- $M > 1$**:** Equivalent to multiple weighted CWs.
- $M \to \infty$**:** Converges toward a normal distribution.

Spoofing acts as a multiple weighted CW jammer for the AGC, starting to impact AGC values for $S/N > -5\,\mathrm{dB}$.

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

[1] Emile Ghizzo et al. "Assessing jamming and spoofing impacts on GNSS receivers: Automatic gain control (AGC)". In: *Signal Processing* 228 (2025), p. 109762

Outline

1. Context
2. Received signal model under spoofing
3. Impact of spoofing before correlation
4. Impact of spoofing after correlation
   - Correlator output
   - Tracking loops
   - C/N_0
5. Experimentation
6. Conclusion

Outline

Correlator model under spoofing (1/2)

$$\Lambda(\boldsymbol{\eta}) = \frac{1}{T_\mathrm{i}} \int_{k\,T_\mathrm{i}}^{(k+1)\,T_\mathrm{i}} r_\mathrm{IF}(t)\, c^*(t-\tau) \exp\left(-2j\pi t(f_\mathrm{IF} + f) - j(\theta - \pi T_\mathrm{i}\, f)\right) \mathrm{d}t, \quad \forall \boldsymbol{\eta} = [\tau, \theta, f]^\mathsf{T}$$

Correlator model under spoofing (1/2)

$$\Lambda(\boldsymbol{\eta}) = \frac{1}{T_{\text{i}}} \int_{k\,T_{\text{i}}}^{(k+1)\,T_{\text{i}}} r_{\text{IF}}(t)\; c^{*}(t-\tau)\exp\left(-2j\pi t(f_{\text{IF}}+f) - j(\theta - \pi T_{\text{i}} f)\right)\mathrm{d}t, \quad \forall \boldsymbol{\eta} = [\tau, \theta, f]^{\mathsf{T}}$$

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Correlator model under spoofing (1/2)

$$\Lambda(\boldsymbol{\eta}) = \frac{1}{\underbrace{T_\text{i}}_{\text{Integration time}}} \int_{k\,T_\text{i}}^{(k+1)\,T_\text{i}} r_\text{IF}(t)\; c^*(t-\tau)\exp\left(-2j\pi t(f_\text{IF} + f) - j(\theta - \pi T_\text{i} f)\right)\mathrm{d}t, \quad \forall \boldsymbol{\eta} = [\tau, \theta, f]^\intercal$$

Correlator model under spoofing (1/2)

$$\Lambda(\boldsymbol{\eta}) = \underbrace{\frac{1}{T_\mathrm{i}}}_{\text{Integration time}} \int_{k\,T_\mathrm{i}}^{(k+1)\,T_\mathrm{i}} \underbrace{r_\mathrm{IF}(t)}_{\text{Received signal}}\, c^*(t-\tau)\exp\left(-2j\pi t(f_\mathrm{IF}+f)-j(\theta-\pi T_\mathrm{i} f)\right)\mathrm{d}t, \quad \forall\boldsymbol{\eta}=[\tau,\theta,f]^\mathsf{T}$$

Correlator model under spoofing (1/2)

$$\Lambda(\boldsymbol{\eta}) = \frac{1}{\underbrace{T_\mathrm{i}}_{\text{Integration time}}} \int_{k\,T_\mathrm{i}}^{(k+1)\,T_\mathrm{i}} \underbrace{r_\mathrm{IF}(t)}_{\text{Received signal}}\, c^*(t-\tau) \exp\left(-2j\pi t(f_\mathrm{IF}+f) - j(\theta - \pi T_\mathrm{i} f)\right) \mathrm{d}t, \quad \forall \boldsymbol{\eta} = [\tau, \theta, f]^\mathsf{T}$$

$$r_\mathrm{IF}(t) = \left[\sum_{i \in \mathcal{M}_\mathrm{a}} r_\mathrm{a}^i(t, \boldsymbol{\eta}_\mathrm{a}^i) + \sum_{i \in \mathcal{M}_\mathrm{s}} r_\mathrm{s}^i(t, \boldsymbol{\eta}_\mathrm{s}^i)\right] \exp\left(2j\pi f_\mathrm{IF} + j\theta_\mathrm{IF}\right) + n_\mathrm{a}(t) + n_\mathrm{s}(t)$$

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Correlator model under spoofing (1/2)

$$\Lambda(\boldsymbol{\eta}) = \frac{1}{\underbrace{T_\mathrm{i}}_{\text{Integration time}}} \int_{k\,T_\mathrm{i}}^{(k+1)\,T_\mathrm{i}} \underbrace{r_\mathrm{IF}(t)}_{\text{Received signal}}\, c^*(t-\tau) \exp\left(-2j\pi t(f_\mathrm{IF} + f) - j(\theta - \pi T_\mathrm{i} f)\right) \mathrm{d}t, \quad \forall \boldsymbol{\eta} = [\tau, \theta, f]^\intercal$$

$$r_\mathrm{IF}(t) = \left[\sum_{i \in \underbrace{\mathcal{M}_\mathrm{a}}_{\text{Set of authentic PRNs}}} \overbrace{r^i_\mathrm{a}(t, \boldsymbol{\eta}^i_\mathrm{a})}^{\text{Authentic signals}} + \sum_{i \in \mathcal{M}_\mathrm{s}} r^i_\mathrm{s}(t, \boldsymbol{\eta}^i_\mathrm{s})\right] \exp\left(2j\pi f_\mathrm{IF} + j\theta_\mathrm{IF}\right) + n_\mathrm{a}(t) + n_\mathrm{s}(t)$$

Correlator model under spoofing (1/2)

$$\Lambda(\boldsymbol{\eta}) = \frac{1}{\underbrace{T_\mathrm{i}}_{\text{Integration time}}} \int_{k\,T_\mathrm{i}}^{(k+1)\,T_\mathrm{i}} \underbrace{r_{\mathrm{IF}}(t)}_{\text{Received signal}}\, c^*(t-\tau)\exp\left(-2j\pi t(f_{\mathrm{IF}}+f) - j(\theta - \pi T_\mathrm{i} f)\right)\mathrm{d}t, \quad \forall \boldsymbol{\eta} = [\tau, \theta, f]^\mathsf{T}$$

$$r_{\mathrm{IF}}(t) = \left[\sum_{i \in \underbrace{\mathcal{M}_\mathrm{a}}_{\text{Set of authentic PRNs}}} \overbrace{r_\mathrm{a}^i(t, \boldsymbol{\eta}_\mathrm{a}^i)}^{\text{Authentic signals}} + \sum_{i \in \underbrace{\mathcal{M}_\mathrm{s}}_{\text{Set of spoofing PRNs}}} \overbrace{r_\mathrm{s}^i(t, \boldsymbol{\eta}_\mathrm{s}^i)}^{\text{Spoofing signals}}\right] \exp(2j\pi f_{\mathrm{IF}} + j\theta_{\mathrm{IF}}) + n_\mathrm{a}(t) + n_\mathrm{s}(t)$$

Correlator model under spoofing (1/2)

$$\Lambda(\boldsymbol{\eta}) = \underbrace{\frac{1}{T_\mathrm{i}}}_{\text{Integration time}} \int_{k\,T_\mathrm{i}}^{(k+1)\,T_\mathrm{i}} \underbrace{r_\mathrm{IF}(t)}_{\text{Received signal}}\, c^*(t-\tau) \exp\left(-2j\pi t(f_\mathrm{IF} + f) - j(\theta - \pi T_\mathrm{i} f)\right) \mathrm{d}t, \quad \forall \boldsymbol{\eta} = [\tau, \theta, f]^\mathsf{T}$$

$$r_\mathrm{IF}(t) = \left[\sum_{\underbrace{i \in \mathcal{M}_\mathrm{a}}_{\text{Set of authentic PRNs}}} \overbrace{r_\mathrm{a}^i(t, \boldsymbol{\eta}_\mathrm{a}^i)}^{\text{Authentic signals}} + \sum_{\underbrace{i \in \mathcal{M}_\mathrm{s}}_{\text{Set of spoofing PRNs}}} \overbrace{r_\mathrm{s}^i(t, \boldsymbol{\eta}_\mathrm{s}^i)}^{\text{Spoofing signals}} \right] \exp(2j\pi f_\mathrm{IF} + j\theta_\mathrm{IF}) + \underbrace{n_\mathrm{a}(t)}_{\text{Nominal AWGN}} + n_\mathrm{s}(t)$$

Correlator model under spoofing (1/2)

$$\Lambda(\boldsymbol{\eta}) = \underbrace{\frac{1}{T_\mathrm{i}}}_{\text{Integration time}} \int_{k\,T_\mathrm{i}}^{(k+1)\,T_\mathrm{i}} \underbrace{r_\mathrm{IF}(t)}_{\text{Received signal}}\, c^*(t-\tau) \exp\left(-2j\pi t(f_\mathrm{IF}+f) - j(\theta - \pi T_\mathrm{i} f)\right) \mathrm{d}t, \quad \forall \boldsymbol{\eta} = [\tau, \theta, f]^\mathsf{T}$$

$$r_\mathrm{IF}(t) = \left[\sum_{i \in \underbrace{\mathcal{M}_\mathrm{a}}_{\text{Set of authentic PRNs}}} \overbrace{r_\mathrm{a}^i(t, \boldsymbol{\eta}_\mathrm{a}^i)}^{\text{Authentic signals}} + \sum_{i \in \underbrace{\mathcal{M}_\mathrm{s}}_{\text{Set of spoofing PRNs}}} \overbrace{r_\mathrm{s}^i(t, \boldsymbol{\eta}_\mathrm{s}^i)}^{\text{Spoofing signals}} \right] \exp\left(2j\pi f_\mathrm{IF} + j\theta_\mathrm{IF}\right) + \underbrace{n_\mathrm{a}(t)}_{\text{Nominal AWGN}} + \overbrace{n_\mathrm{s}(t)}^{\text{Re-radiated AWGN}}$$

Correlator model under spoofing (1/2)

$$\Lambda(\boldsymbol{\eta}) = \underbrace{\frac{1}{T_\mathrm{i}}}_{\text{Integration time}} \int_{k\,T_\mathrm{i}}^{(k+1)\,T_\mathrm{i}} \underbrace{r_\mathrm{IF}(t)}_{\text{Received signal}}\, c^*(t-\tau)\exp\left(-2j\pi t(f_\mathrm{IF}+f)-j(\theta-\pi T_\mathrm{i} f)\right)\mathrm{d}t, \quad \forall\boldsymbol{\eta}=[\tau,\theta,f]^\mathsf{T}$$

$$r_\mathrm{IF}(t) = \left[\sum_{i\in\underbrace{\mathcal{M}_\mathrm{a}}_{\text{Set of authentic PRNs}}} \overbrace{r_\mathrm{a}^i(t,\boldsymbol{\eta}_\mathrm{a}^i)}^{\text{Authentic signals}} + \sum_{i\in\underbrace{\mathcal{M}_\mathrm{s}}_{\text{Set of spoofing PRNs}}} \overbrace{r_\mathrm{s}^i(t,\boldsymbol{\eta}_\mathrm{s}^i)}^{\text{Spoofing signals}}\right]\exp\left(2j\pi f_\mathrm{IF}+j\theta_\mathrm{IF}\right) + \overbrace{n(t)}^{\text{Total AWGN}}$$

Correlator model under spoofing (1/2)

$$\Lambda(\boldsymbol{\eta}) = \underbrace{\frac{1}{T_i}}_{\text{Integration time}} \int_{k\,T_i}^{(k+1)\,T_i} \underbrace{r_{IF}(t)}_{\text{Received signal}}\, c^*(t-\tau)\exp\left(-2j\pi t(f_{IF}+f) - j(\theta - \pi T_i f)\right)\mathrm{d}t, \quad \forall \boldsymbol{\eta} = [\tau, \theta, f]^{\mathsf{T}}$$

$$r_{IF}(t) = \left[\underbrace{r_a(t, \boldsymbol{\eta}_a)}_{\text{Authentic signal}} + \underbrace{r_s(t, \boldsymbol{\eta}_s)}_{\text{Spoofing signal}} + \sum_{i \in \underbrace{\mathcal{X}_a}_{\text{Authentic inter-signal set}}} r_a^i(t) + \sum_{i \in \underbrace{\mathcal{X}_s}_{\text{Spoofing inter-signal set}}} r_s^i(t)\right] \exp\left(2j\pi f_{IF} + j\theta_{IF}\right) + \underbrace{n(t)}_{\text{Total AWGN}}$$

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Correlator model under spoofing (1/2)

$$\Lambda(\boldsymbol{\eta}) = \underbrace{\frac{1}{T_\mathrm{i}}}_{\text{Integration time}} \int_{k\,T_\mathrm{i}}^{(k+1)\,T_\mathrm{i}} \underbrace{r_\mathrm{IF}(t)}_{\text{Received signal}}\, c^*(t-\tau)\exp\left(-2j\pi t(f_\mathrm{IF}+f) - j(\theta - \pi T_\mathrm{i} f)\right)\mathrm{d}t, \quad \forall \boldsymbol{\eta} = [\tau, \theta, f]^\intercal$$

$$r_\mathrm{IF}(t) = \Big[\overbrace{r_\mathrm{a}(t, \boldsymbol{\eta}_\mathrm{a})}^{\text{Authentic signal}} + \overbrace{r_\mathrm{s}(t, \boldsymbol{\eta}_\mathrm{s})}^{\text{Spoofing signal}} + \underbrace{\chi(t)}_{\text{Total inter-signal interference}}\Big]\exp\left(2j\pi f_\mathrm{IF} + j\theta_\mathrm{IF}\right) + \overbrace{n(t)}^{\text{Total AWGN}}$$

$\chi(t)$ is shown as a **Gaussian random variable** (CLT)

Correlator model under spoofing (2/2)

$$\Lambda(\boldsymbol{\eta}, \boldsymbol{\eta}_{\mathrm{a}}, \boldsymbol{\eta}_{\mathrm{s}}) = \Lambda_{\mathrm{a}}(\boldsymbol{\eta}_{\mathrm{a}} - \boldsymbol{\eta}) + \Lambda_{\mathrm{s}}(\boldsymbol{\eta}_{\mathrm{s}} - \boldsymbol{\eta}) + \Lambda_{\chi} + \Lambda_{n}$$

Correlator model under spoofing (2/2)

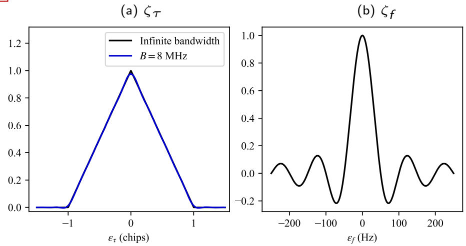
$$\Lambda(\boldsymbol{\eta}, \boldsymbol{\eta}_\mathrm{a}, \boldsymbol{\eta}_\mathrm{s}) = \overbrace{\Lambda_\mathrm{a}(\boldsymbol{\eta}_\mathrm{a} - \boldsymbol{\eta})}^{\text{Authentic peak}} + \Lambda_\mathrm{s}(\boldsymbol{\eta}_\mathrm{s} - \boldsymbol{\eta}) + \Lambda_\chi + \Lambda_n$$

- Authentic peak:
  $\Lambda_\mathrm{a}(\boldsymbol{\eta}_\mathrm{a} - \boldsymbol{\eta}) = \sqrt{C_\mathrm{a}}\, d_k\, \zeta_\tau(\tau_\mathrm{a} - \tau)\, \zeta_f(f_\mathrm{a} - f)\, e^{j(\theta_\mathrm{a} - \theta)}$

Correlator model under spoofing (2/2)

$$\Lambda(\boldsymbol{\eta}, \boldsymbol{\eta}_\mathrm{a}, \boldsymbol{\eta}_\mathrm{s}) = \overbrace{\Lambda_\mathrm{a}(\boldsymbol{\eta}_\mathrm{a} - \boldsymbol{\eta})}^{\text{Authentic peak}} + \underbrace{\Lambda_\mathrm{s}(\boldsymbol{\eta}_\mathrm{s} - \boldsymbol{\eta})}_{\text{Spoofing peak}} + \Lambda_\chi + \Lambda_n$$

- Authentic peak:
  $$\Lambda_\mathrm{a}(\boldsymbol{\eta}_\mathrm{a} - \boldsymbol{\eta}) = \sqrt{C_\mathrm{a}}\, d_k\, \zeta_\tau(\tau_\mathrm{a} - \tau)\, \zeta_f(f_\mathrm{a} - f)\, e^{j(\theta_\mathrm{a} - \theta)}$$
- Spoofing peak:
  $$\Lambda_\mathrm{s}(\boldsymbol{\eta}_\mathrm{s} - \boldsymbol{\eta}) = \sqrt{C_\mathrm{s}}\, d_k\, \zeta_\tau(\tau_\mathrm{s} - \tau)\, \zeta_f(f_\mathrm{s} - f)\, e^{j(\theta_\mathrm{s} - \theta)}$$



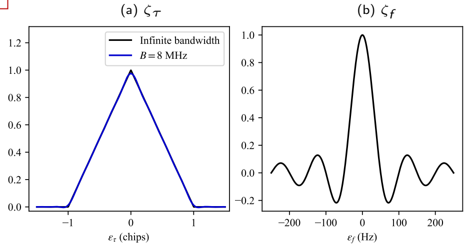
Correlator model under spoofing (2/2)

Authentic peak

$$\Lambda(\eta, \eta_a, \eta_s) = \Lambda_a(\eta_a - \eta) + \Lambda_s(\eta_s - \eta) + \Lambda_\chi + \Lambda_n$$

Spoofing peak

- Authentic peak:
  $\Lambda_a(\eta_a - \eta) = \sqrt{C_a}\, d_k\, \zeta_\tau(\tau_a - \tau)\, \zeta_f(f_a - f)\, e^{j(\theta_a - \theta)}$
- Spoofing peak:
  $\Lambda_s(\eta_s - \eta) = \sqrt{C_s}\, d_k\, \zeta_\tau(\tau_s - \tau)\, \zeta_f(f_s - f)\, e^{j(\theta_s - \theta)}$



Authentic and spoofing dynamics:

$$\eta_a = \left[\ \tau_a\ ,\ \theta_a\ ,\ f_a\ \right]^\mathsf{T} \text{ and } \eta_s = \left[\ \tau_s\ ,\ \theta_s\ ,\ f_s\ \right]^\mathsf{T}$$

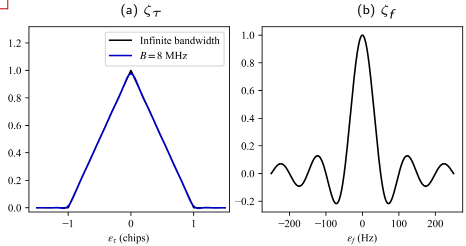
Correlator model under spoofing (2/2)

$$\Lambda(\eta, \eta_a, \eta_s) = \underbrace{\Lambda_a(\eta_a - \eta)}_{\text{Authentic peak}} + \underbrace{\Lambda_s(\eta_s - \eta)}_{\text{Spoofing peak}} + \Lambda_\chi + \Lambda_n$$

- Authentic peak:

  $\Lambda_a(\eta_a - \eta) = \sqrt{C_a}\, d_k\, \zeta_\tau(\tau_a - \tau)\, \zeta_f(f_a - f)\, e^{j(\theta_a - \theta)}$
- Spoofing peak:

  $\Lambda_s(\eta_s - \eta) = \sqrt{C_s}\, d_k\, \zeta_\tau(\tau_s - \tau)\, \zeta_f(f_s - f)\, e^{j(\theta_s - \theta)}$



Authentic and spoofing dynamics:

$$\eta_a = [\underbrace{\tau_a}_{\text{Authentic delay}}, \underbrace{\theta_a}_{\text{Authentic phase}}, \underbrace{f_a}_{\text{Authentic frequency}}]^T \text{ and } \eta_s = [\underbrace{\tau_s}_{\text{Spoofing delay}}, \underbrace{\theta_s}_{\text{Spoofing phase}}, \underbrace{f_s}_{\text{Spoofing frequency}}]^T$$

Correlator model under spoofing (2/2)

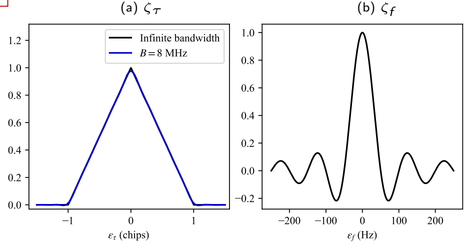
$$\Lambda(\boldsymbol{\eta}, \boldsymbol{\eta}_a, \boldsymbol{\eta}_s) = \underbrace{\Lambda_a(\boldsymbol{\eta}_a - \boldsymbol{\eta})}_{\text{Authentic peak}} + \underbrace{\Lambda_s(\boldsymbol{\eta}_s - \boldsymbol{\eta})}_{\text{Spoofing peak}} + \underbrace{\Lambda_\chi}_{\text{Inter-signal contribution}} + \underbrace{\Lambda_n}_{\text{AWGN contribution}}$$

- Authentic peak:

  $$\Lambda_a(\boldsymbol{\eta}_a - \boldsymbol{\eta}) = \sqrt{C_a}\, d_k\, \zeta_\tau(\tau_a - \tau)\, \zeta_f(f_a - f)\, e^{j(\theta_a - \theta)}$$

- Spoofing peak:

  $$\Lambda_s(\boldsymbol{\eta}_s - \boldsymbol{\eta}) = \sqrt{C_s}\, d_k\, \zeta_\tau(\tau_s - \tau)\, \zeta_f(f_s - f)\, e^{j(\theta_s - \theta)}$$



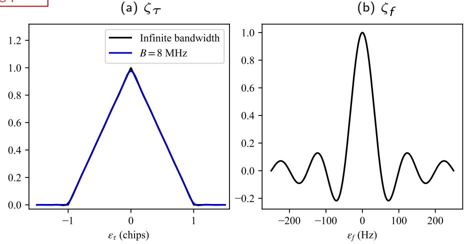
Authentic and spoofing dynamics:

$$\boldsymbol{\eta}_a = [\underbrace{\tau_a}_{\text{Authentic delay}}, \underbrace{\theta_a}_{\text{Authentic phase}}, \underbrace{f_a}_{\text{Authentic frequency}}]^T \text{ and } \boldsymbol{\eta}_s = [\underbrace{\tau_s}_{\text{Spoofing delay}}, \underbrace{\theta_s}_{\text{Spoofing phase}}, \underbrace{f_s}_{\text{Spoofing frequency}}]^T$$

Correlator model under spoofing (2/2)

$$\Lambda(\boldsymbol{\eta},\boldsymbol{\eta}_{\mathrm{a}},\boldsymbol{\eta}_{\mathrm{s}}) = \underbrace{\Lambda_{\mathrm{a}}(\boldsymbol{\eta}_{\mathrm{a}}-\boldsymbol{\eta})}_{\text{Authentic peak}} + \underbrace{\Lambda_{\mathrm{s}}(\boldsymbol{\eta}_{\mathrm{s}}-\boldsymbol{\eta})}_{\text{Spoofing peak}} + \underbrace{\Lambda_{\varsigma}}_{\text{Random contribution}}$$

- Authentic peak:
  $\Lambda_{\mathrm{a}}(\boldsymbol{\eta}_{\mathrm{a}}-\boldsymbol{\eta}) = \sqrt{C_{\mathrm{a}}}\, d_k\, \zeta_\tau(\tau_{\mathrm{a}}-\tau)\,\zeta_f(f_{\mathrm{a}}-f)\, e^{j(\theta_{\mathrm{a}}-\theta)}$
- Spoofing peak:
  $\Lambda_{\mathrm{s}}(\boldsymbol{\eta}_{\mathrm{s}}-\boldsymbol{\eta}) = \sqrt{C_{\mathrm{s}}}\, d_k\, \zeta_\tau(\tau_{\mathrm{s}}-\tau)\,\zeta_f(f_{\mathrm{s}}-f)\, e^{j(\theta_{\mathrm{s}}-\theta)}$
- Random contribution:
  $\Lambda_{\varsigma} = \Lambda_{\chi} + \Lambda_n \;(\Lambda_{\varsigma} \sim \mathcal{CN}(0, P_{\chi}+P_n))$



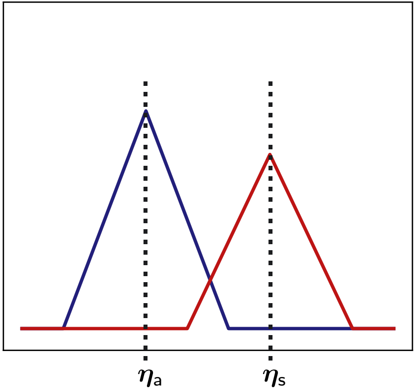
Authentic and spoofing dynamics:

$$\boldsymbol{\eta}_{\mathrm{a}} = [\underbrace{\tau_{\mathrm{a}}}_{\text{Authentic delay}}, \underbrace{\theta_{\mathrm{a}}}_{\text{Authentic phase}}, \underbrace{f_{\mathrm{a}}}_{\text{Authentic frequency}}]^{\mathsf{T}} \text{ and } \boldsymbol{\eta}_{\mathrm{s}} = [\underbrace{\tau_{\mathrm{s}}}_{\text{Spoofing delay}}, \underbrace{\theta_{\mathrm{s}}}_{\text{Spoofing phase}}, \underbrace{f_{\mathrm{s}}}_{\text{Spoofing frequency}}]^{\mathsf{T}}$$

RÉPUBLIQUE FRANÇAISE Liberté Égalité Fraternité ENAC

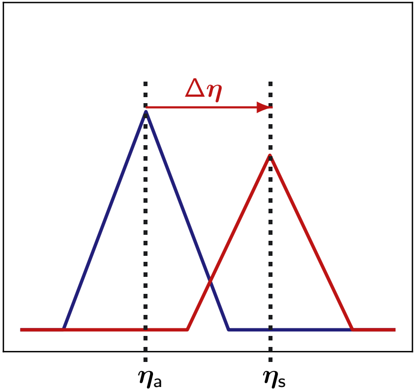
Relative dynamic

$$\Lambda(\eta, \eta_a, \eta_s) = \Lambda_a(\overset{\text{Authentic dynamic}}{\eta_a} - \eta) + \Lambda_s(\underset{\text{Spoofing dynamic}}{\eta_s} - \eta) + \Lambda_\varsigma$$



Relative dynamic

$$\Lambda(\eta, \underbrace{\eta_a}_{}, \Delta\nu) = \Lambda_a(\overset{\text{Authentic dynamic}}{\eta_a} - \eta) + \sqrt{\Delta g}\,\Lambda_a(\eta_a - \eta + \overset{\text{Relative dynamic}}{\Delta\eta}) + \Lambda_\varsigma$$

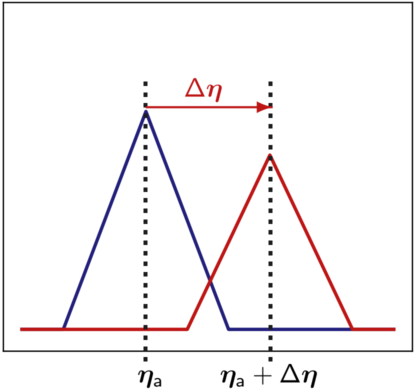


Relative dynamic:

$$\Delta\eta = \eta_s - \eta_a = \left[\overset{\text{Relative delay}}{\Delta\tau}, \overset{\text{Relative phase}}{\Delta\theta}, \underset{\text{Relative frequency}}{\Delta f}\right]^\mathsf{T}$$

Relative dynamic

$$\Lambda(\eta, \overbrace{\eta_a}^{\text{Authentic dynamic}}, \Delta\nu) = \Lambda_a(\overbrace{\eta_a}^{\text{Authentic dynamic}} - \eta) + \sqrt{\Delta g}\,\Lambda_a(\eta_a - \eta + \overbrace{\Delta\eta}^{\text{Relative dynamic}}) + \Lambda_\varsigma$$

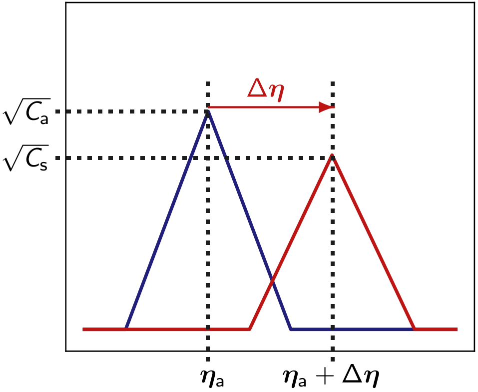


Relative dynamic:

$$\Delta\eta = \eta_s - \eta_a = \left[\overbrace{\Delta\tau}^{\text{Relative delay}}, \overbrace{\Delta\theta}^{\text{Relative phase}}, \underbrace{\Delta f}_{\text{Relative frequency}}\right]^T$$

Relative dynamic

$$\Lambda(\eta, \eta_a, \Delta\nu) = \Lambda_a(\overset{\text{Authentic dynamic}}{\eta_a} - \eta) + \sqrt{\Delta g}\,\Lambda_a(\eta_a - \eta + \overset{\text{Relative dynamic}}{\Delta\eta}) + \Lambda_\varsigma$$

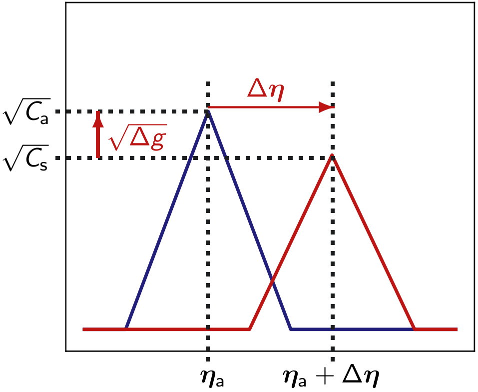


Relative dynamic:

$$\Delta\eta = \eta_s - \eta_a = \left[\overset{\text{Relative delay}}{\Delta\tau}, \overset{\text{Relative phase}}{\Delta\theta}, \underset{\text{Relative frequency}}{\Delta f}\right]^\intercal$$

Relative dynamic

$$\Lambda(\eta, \boxed{\eta_a}, \boxed{\Delta\nu}) = \Lambda_a(\overset{\text{Authentic dynamic}}{\boxed{\eta_a}} - \eta) + \underset{\text{Relative power}}{\boxed{\sqrt{\Delta g}}}\,\Lambda_a(\boxed{\eta_a} - \eta + \overset{\text{Relative dynamic}}{\boxed{\Delta\eta}}) + \Lambda_\varsigma$$



Relative dynamic:

$$\Delta\eta = \eta_s - \eta_a = \left[\overset{\text{Relative delay}}{\boxed{\Delta\tau}}, \overset{\text{Relative phase}}{\boxed{\Delta\theta}}, \underset{\text{Relative frequency}}{\boxed{\Delta f}}\right]^\mathsf{T}$$

Relative parameters:

$$\Delta\nu = \left[\Delta\eta^\mathsf{T}, \overset{\text{Relative power}}{\boxed{\Delta g}}\right]^\mathsf{T} \text{ with } \Delta g = C_s / C_a$$

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Classification

$$\Lambda(\eta, \eta_a, \Delta\nu) = \underbrace{\Lambda_a(\eta_a - \eta)}_{\text{Authentic peak}} + \underbrace{\Lambda_s(\eta_a - \eta, \Delta\nu)}_{\text{Spoofing peak}} + \underbrace{\Lambda_\varsigma}_{\text{Random contribution}}$$

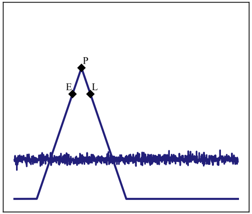
Classification

Authentic peak

Spoofing peak

Random contribution

$$\Lambda(\eta, \eta_a, \Delta\nu) = \Lambda_a(\eta_a - \eta) + \Lambda_s(\eta_a - \eta, \Delta\nu) + \Lambda_\varsigma$$



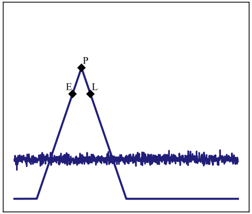
Nominal

$$\Lambda^{(N)} = \Lambda_a + \Lambda_\varsigma$$

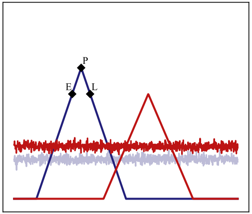
Classification

Authentic peak — Spoofing peak — Random contribution

$$\Lambda(\eta, \eta_a, \Delta\nu) = \Lambda_a(\eta_a - \eta) + \Lambda_s(\eta_a - \eta, \Delta\nu) + \Lambda_\varsigma$$



Nominal

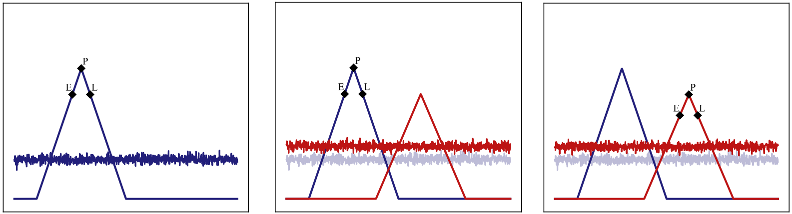


Induced-jamming

$$\Lambda^{(N)} = \Lambda_a + \Lambda_\varsigma \qquad \Lambda^{(J)} = \Lambda_a + \Lambda_\varsigma$$

Classification

$$\Lambda(\eta, \eta_a, \Delta\nu) = \underbrace{\Lambda_a(\eta_a - \eta)}_{\text{Authentic peak}} + \underbrace{\Lambda_s(\eta_a - \eta, \Delta\nu)}_{\text{Spoofing peak}} + \underbrace{\Lambda_\varsigma}_{\text{Random contribution}}$$



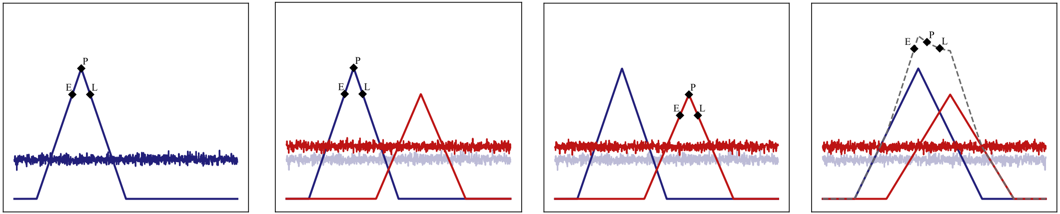
Nominal Induced-jamming Induced-spoofing

$$\Lambda^{(N)} = \Lambda_a + \Lambda_\varsigma \qquad \Lambda^{(J)} = \Lambda_a + \Lambda_\varsigma \qquad \Lambda^{(S)} = \Lambda_s + \Lambda_\varsigma$$

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Classification

$$\Lambda(\eta, \eta_a, \Delta\nu) = \overbrace{\Lambda_a(\eta_a - \eta)}^{\text{Authentic peak}} + \overbrace{\Lambda_s(\eta_a - \eta, \Delta\nu)}^{\text{Spoofing peak}} + \overbrace{\Lambda_\varsigma}^{\text{Random contribution}}$$

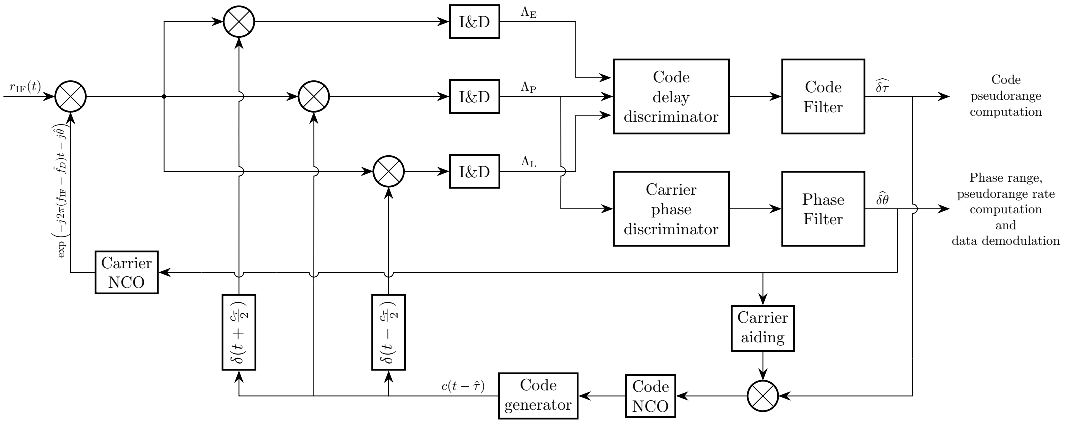


Nominal | Induced-jamming | Induced-spoofing | Induced-multipath

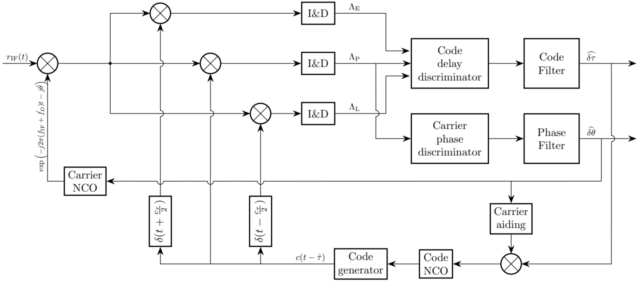
$$\Lambda^{(N)} = \Lambda_a + \Lambda_\varsigma \qquad \Lambda^{(J)} = \Lambda_a + \Lambda_\varsigma \qquad \Lambda^{(S)} = \Lambda_s + \Lambda_\varsigma \qquad \Lambda^{(M)} = \Lambda_a + \Lambda_s + \Lambda_\varsigma$$

Outline

Tracking loops model

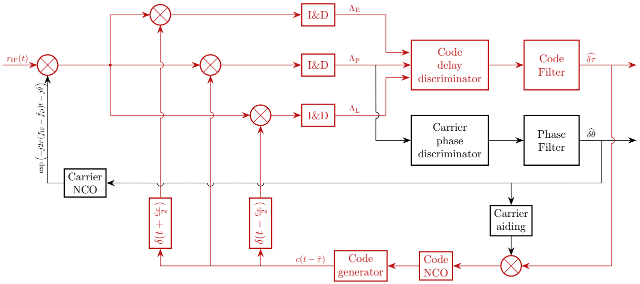


Tracking loops model



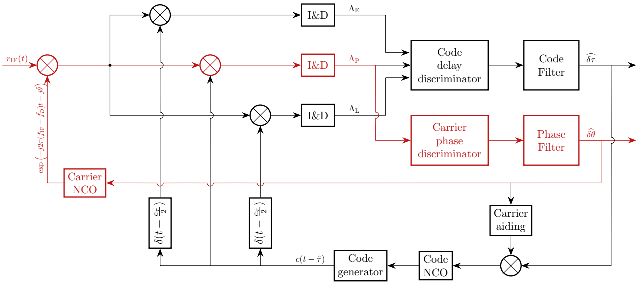
Tracking loops model

$$\begin{cases} \hat{\tau}(z) = \dfrac{z^{-1}}{1 - z^{-1}} T_\mathrm{i}\, F_\tau(z)\, D_\tau\left(\boldsymbol{\eta}_\mathrm{a}(z) - \hat{\boldsymbol{\eta}}(z), \Delta\boldsymbol{\nu}(z)\right) & \text{(DLL)} \end{cases}$$



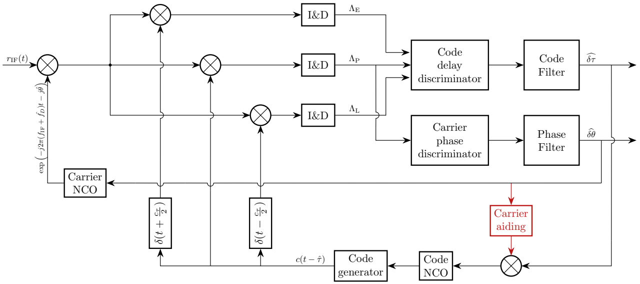
Tracking loops model

$$\begin{cases} \hat{\tau}(z) = \dfrac{z^{-1}}{1-z^{-1}} T_i\, F_\tau(z)\, D_\tau\left(\boldsymbol{\eta}_a(z) - \hat{\boldsymbol{\eta}}(z), \Delta\boldsymbol{\nu}(z)\right) & \text{(DLL)} \\ \hat{\theta}(z) = \dfrac{z^{-1}}{1-z^{-1}} T_i\, F_\theta(z)\, D_\theta\left(\boldsymbol{\eta}_a(z) - \hat{\boldsymbol{\eta}}(z), \Delta\boldsymbol{\nu}(z)\right) & \text{(PLL)} \end{cases}$$



Tracking loops model

$$\begin{cases} \hat{\tau}(z) + \beta\,\hat{\theta}(z) = \dfrac{z^{-1}}{1-z^{-1}}\, T_\mathrm{i}\, F_\tau(z)\, D_\tau\left(\boldsymbol{\eta}_\mathrm{a}(z) - \hat{\boldsymbol{\eta}}(z), \Delta\boldsymbol{\nu}(z)\right) & \text{(DLL)} \\ \hat{\theta}(z) = \dfrac{z^{-1}}{1-z^{-1}}\, T_\mathrm{i}\, F_\theta(z)\, D_\theta\left(\boldsymbol{\eta}_\mathrm{a}(z) - \hat{\boldsymbol{\eta}}(z), \Delta\boldsymbol{\nu}(z)\right) & \text{(PLL)} \end{cases}$$



Tracking loops model

$$\begin{cases} \hat{\tau}(z) + \beta\ \hat{\theta}(z) = \dfrac{z^{-1}}{1-z^{-1}} T_{\mathrm{i}}\ F_{\tau}(z)\ D_{\tau}\left(\boldsymbol{\eta}_{\mathrm{a}}(z) - \hat{\boldsymbol{\eta}}(z)\ ,\ \Delta\boldsymbol{\nu}(z)\right) & \text{(DLL)} \\ \hat{\theta}(z) = \dfrac{z^{-1}}{1-z^{-1}} T_{\mathrm{i}}\ F_{\theta}(z)\ D_{\theta}\left(\boldsymbol{\eta}_{\mathrm{a}}(z) - \hat{\boldsymbol{\eta}}(z)\ ,\ \Delta\boldsymbol{\nu}(z)\right) & \text{(PLL)} \end{cases}$$

Tracking loops model

State vector

$$\begin{cases} \hat{\tau}(z) + \beta\, \hat{\theta}(z) = \dfrac{z^{-1}}{1 - z^{-1}} T_{\mathrm{i}}\, F_{\tau}(z)\;\; D_{\tau}\left(\boldsymbol{\eta}_{\mathrm{a}}(z) - \hat{\boldsymbol{\eta}}(z),\; \Delta\boldsymbol{\nu}(z)\right) & \text{(DLL)} \\ \hat{\theta}(z) = \dfrac{z^{-1}}{1 - z^{-1}} T_{\mathrm{i}}\, F_{\theta}(z)\;\; D_{\theta}\left(\boldsymbol{\eta}_{\mathrm{a}}(z) - \hat{\boldsymbol{\eta}}(z),\; \Delta\boldsymbol{\nu}(z)\right) & \text{(PLL)} \end{cases}$$

Tracking loops model

State vector

$$
\begin{cases}
\hat{\tau}(z) + \beta\,\hat{\theta}(z) = \dfrac{z^{-1}}{1-z^{-1}}\, T_{\mathrm{i}}\, F_{\tau}(z)\;\; D_{\tau}\left(\boldsymbol{\eta}_{\mathrm{a}}(z) - \hat{\boldsymbol{\eta}}(z),\; \Delta\boldsymbol{\nu}(z)\right) & \text{(DLL)} \\
\hat{\theta}(z) = \dfrac{z^{-1}}{1-z^{-1}}\, T_{\mathrm{i}}\, F_{\theta}(z)\;\; D_{\theta}\left(\boldsymbol{\eta}_{\mathrm{a}}(z) - \hat{\boldsymbol{\eta}}(z),\; \Delta\boldsymbol{\nu}(z)\right) & \text{(PLL)}
\end{cases}
$$

Loop filter

Tracking loops model

State vector

$$\begin{cases} \boxed{\hat{\tau}(z)} + \beta\, \boxed{\hat{\theta}(z)} = \dfrac{z^{-1}}{1 - z^{-1}} T_\mathrm{i}\, F_\tau(z)\;\; D_\tau \left(\eta_\mathrm{a}(z) - \boxed{\hat{\eta}(z)},\; \Delta\nu(z)\right) & \text{(DLL)} \\ \boxed{\hat{\theta}(z)} = \dfrac{z^{-1}}{1 - z^{-1}} T_\mathrm{i}\, \underbrace{F_\theta(z)}_{\text{Low-pass filter}}\;\; \underbrace{D_\theta}_{\text{Discriminator}} \left(\eta_\mathrm{a}(z) - \boxed{\hat{\eta}(z)},\; \Delta\nu(z)\right) & \text{(PLL)} \end{cases}$$

Tracking loops model

$$\begin{cases} \underbrace{\hat{\tau}(z)}_{\text{State vector}} + \beta\, \hat{\theta}(z) = \dfrac{z^{-1}}{1 - z^{-1}} T_\mathrm{i}\, F_\tau(z)\ D_\tau \left(\eta_\mathrm{a}(z) - \hat{\eta}(z), \overbrace{\Delta\nu(z)}^{\text{Relative dynamic}}\right) & \text{(DLL)} \\ \hat{\theta}(z) = \dfrac{z^{-1}}{1 - z^{-1}} T_\mathrm{i}\, \underbrace{F_\theta(z)}_{\text{Low-pass filter}}\ \underbrace{D_\theta}_{\text{Discriminator}} \left(\eta_\mathrm{a}(z) - \hat{\eta}(z), \Delta\nu(z)\right) & \text{(PLL)} \end{cases}$$

Tracking loops model

State vector

Relative dynamic

$$\begin{cases} \hat{\tau}(z) + \beta\,\hat{\theta}(z) = \dfrac{z^{-1}}{1-z^{-1}} T_i\, F_\tau(z)\ D_\tau\left(\eta_a(z) - \hat{\eta}(z), \Delta\nu(z)\right) & \text{(DLL)} \\ \hat{\theta}(z) = \dfrac{z^{-1}}{1-z^{-1}} T_i\, F_\theta(z)\ D_\theta\left(\eta_a(z) - \hat{\eta}(z), \Delta\nu(z)\right) & \text{(PLL)} \end{cases}$$

Low-pass filter

Discriminator

Dynamic approach:

- Characterize the dynamic behavior under spoofing through the analysis of the closed-loop model.
- Account for the interconnection between DLL and PLL, incorporating all dynamic aspects (e.g., filter and feedback architecture).
- Propose an analysis of linearity, Stable Equilibria (SE), and stochastic behavior for each spoofing-induced situation.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Linearity

Definition: State variable $\hat{\phi}$ and its derivatives appear linearly. A linear system satisfies **additivity** and **homogeneity** and can be analyzed though **tranfer function tools**.[1]

[1] Floyd M Gardner. *Phaselock Techniques*. John Wiley & Sons, 2005

Linearity

Definition: State variable $\hat{\phi}$ and its derivatives appear linearly. A linear system satisfies **additivity** and **homogeneity** and can be analyzed though **tranfer function tools**.[1]

State vector

$$\begin{cases} \hat{\tau}(z) + \beta\, \hat{\theta}(z) = \dfrac{z^{-1}}{1-z^{-1}} T_{\mathrm{i}}\, F_{\tau}(z)\ \ D_{\tau}\left(\eta_{\mathrm{a}}(z) - \hat{\eta}(z), \Delta\nu(z)\right) & \text{(DLL)} \\ \hat{\theta}(z) = \dfrac{z^{-1}}{1-z^{-1}} T_{\mathrm{i}}\, \underbrace{F_{\theta}(z)}_{\text{Low-pass filter}}\ \ \underbrace{D_{\theta}}_{\text{Discriminator}}\left(\eta_{\mathrm{a}}(z) - \hat{\eta}(z), \Delta\nu(z)\right) & \text{(PLL)} \end{cases}$$

[1] Floyd M Gardner. *Phaseload Techniques*. John Wiley & Sons, 2005

Linearity

Definition: State variable $\hat{\phi}$ and its derivatives appear linearly. A linear system satisfies **additivity** and **homogeneity** and can be analyzed though **tranfer function tools**.[1]

State vector

$$\begin{cases} \hat{\tau}(z) + \beta\,\hat{\theta}(z) = \dfrac{z^{-1}}{1 - z^{-1}} T_{\text{i}}\, F_{\tau}(z)\ \ D_{\tau}\left(\eta_{\text{a}}(z) - \hat{\eta}(z), \Delta\nu(z)\right) & \text{(DLL)} \\ \hat{\theta}(z) = \dfrac{z^{-1}}{1 - z^{-1}} T_{\text{i}}\, F_{\theta}(z)\ \ D_{\theta}\left(\eta_{\text{a}}(z) - \hat{\eta}(z), \Delta\nu(z)\right) & \text{(PLL)} \end{cases}$$

Low-pass filter

Discriminator

Results

- ✓ Maintains its linearity assumption under induced jamming and spoofing situations (near SE).
- × Exhibits non-linearity in both DLL and PLL under induced multipath situation.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

[1] Floyd M Gardner. *Phaselock Techniques*. John Wiley & Sons, 2005

Stable Equilibria (SE) (1/3)

Stable Equilibrium: State where the system has **successfully converged** and **returns to this state after a small perturbation**.[1]

[1] Gennady A. Leonov et al. "Hold-In, Pull-In, and Lock-In Ranges of PLL Circuits: Rigorous Mathematical Definitions and Limitations of Classical Theory". In: *IEEE Trans. Circuits Syst. I, Reg. Papers* 62.10 (2015), pp. 2454–2464

Stable Equilibria (SE) (1/3)

Stable Equilibrium: State where the system has **successfully converged** and **returns to this state after a small perturbation**.[1]

Objective

- Enable the analysis of **system convergence** (identifying the different **points of convergence** and **potential bifurcations**).
- Facilitate the analysis of the **system's dynamic behavior**, including transient response, tracking error at lock, and stress error.

[1] Gennady A. Leonov et al. "Hold-In, Pull-In, and Lock-In Ranges of PLL Circuits: Rigorous Mathematical Definitions and Limitations of Classical Theory". In: *IEEE Trans. Circuits Syst. I, Reg. Papers* 62.10 (2015), pp. 2454–2464

Stable Equilibria (SE) (1/3)

Stable Equilibrium: State where the system has **successfully converged** and **returns to this state after a small perturbation.**[1]

Objective

- Enable the analysis of **system convergence** (identifying the different **points of convergence** and **potential bifurcations**).
- Facilitate the analysis of the **system's dynamic behavior**, including transient response, tracking error at lock, and stress error.

Closed-loop model SE:

$$\begin{cases} d_\tau\left(\varepsilon_\eta^l, \Delta\boldsymbol{\nu}\right) = 0, \quad d_\theta\left(\varepsilon_\eta^l, \Delta\boldsymbol{\nu}\right) = 0, \quad \chi_f\left(\varepsilon_\eta^l, \Delta\boldsymbol{\nu}\right) = 0 & \text{(Equilibrium)} \\ \dfrac{\partial\, d_\tau\left(\varepsilon_\eta^l, \Delta\boldsymbol{\nu}\right)}{\partial\varepsilon_\tau} > 0, \quad \dfrac{\partial\, d_\theta\left(\varepsilon_\eta^l, \Delta\boldsymbol{\nu}\right)}{\partial\varepsilon_\theta} > 0, \quad \dfrac{\partial\, \chi_f\left(\varepsilon_\eta^l, \Delta\boldsymbol{\nu}\right)}{\partial\varepsilon_f} > 0 & \text{(Stability)} \end{cases}$$

[1] Gennady A. Leonov et al. "Hold-In, Pull-In, and Lock-In Ranges of PLL Circuits: Rigorous Mathematical Definitions and Limitations of Classical Theory". In: *IEEE Trans. Circuits Syst. I, Reg. Papers* 62.10 (2015), pp. 2454–2464

RÉPUBLIQUE FRANÇAISE

Stable Equilibria (SE) (1/3)

Stable Equilibrium: State where the system has **successfully converged** and **returns to this state after a small perturbation.**[1]

Objective

- Enable the analysis of **system convergence** (identifying the different **points of convergence** and **potential bifurcations**).
- Facilitate the analysis of the **system's dynamic behavior**, including transient response, tracking error at lock, and stress error.

Closed-loop model SE:

$$\begin{cases} \overset{\text{DLL disc.}}{d_\tau}\left(\varepsilon_\eta^I, \Delta\boldsymbol{\nu}\right) = 0, & \overset{\text{PLL disc.}}{d_\theta}\left(\varepsilon_\eta^I, \Delta\boldsymbol{\nu}\right) = 0, & \overset{\text{PLL derivative disc.}}{\chi_f}\left(\varepsilon_\eta^I, \Delta\boldsymbol{\nu}\right) = 0 & \text{(Equilibrium)} \\ \dfrac{\partial\, d_\tau\left(\varepsilon_\eta^I, \Delta\boldsymbol{\nu}\right)}{\partial \varepsilon_\tau} > 0, & \dfrac{\partial\, d_\theta\left(\varepsilon_\eta^I, \Delta\boldsymbol{\nu}\right)}{\partial \varepsilon_\theta} > 0, & \dfrac{\partial\, \chi_f\left(\varepsilon_\eta^I, \Delta\boldsymbol{\nu}\right)}{\partial \varepsilon_f} > 0 & \text{(Stability)} \end{cases}$$

[1] Gennady A. Leonov et al. "Hold-In, Pull-In, and Lock-In Ranges of PLL Circuits: Rigorous Mathematical Definitions and Limitations of Classical Theory". In: *IEEE Trans. Circuits Syst. I, Reg. Papers* 62.10 (2015), pp. 2454–2464

Stable Equilibria (SE) (1/3)

Stable Equilibrium: State where the system has **successfully converged** and **returns to this state after a small perturbation.**[1]

Objective

- Enable the analysis of **system convergence** (identifying the different **points of convergence** and **potential bifurcations**).
- Facilitate the analysis of the **system's dynamic behavior**, including transient response, tracking error at lock, and stress error.

Closed-loop model SE:

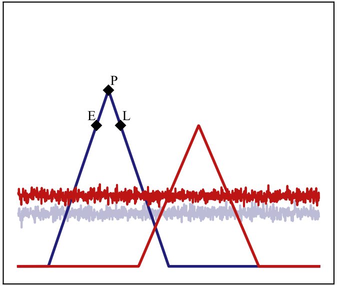
SE solutions

$$\begin{cases} d_\tau\left(\varepsilon_\eta^l, \Delta\boldsymbol{\nu}\right) = 0, \quad d_\theta\left(\varepsilon_\eta^l, \Delta\boldsymbol{\nu}\right) = 0, \quad \chi_f\left(\varepsilon_\eta^l, \Delta\boldsymbol{\nu}\right) = 0 & \text{(Equilibrium)} \\ \dfrac{\partial\, d_\tau\left(\varepsilon_\eta^l, \Delta\boldsymbol{\nu}\right)}{\partial\varepsilon_\tau} > 0, \quad \dfrac{\partial\, d_\theta\left(\varepsilon_\eta^l, \Delta\boldsymbol{\nu}\right)}{\partial\varepsilon_\theta} > 0, \quad \dfrac{\partial\, \chi_f\left(\varepsilon_\eta^l, \Delta\boldsymbol{\nu}\right)}{\partial\varepsilon_f} > 0 & \text{(Stability)} \end{cases}$$

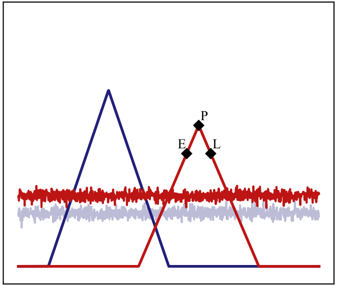
[1] Gennady A. Leonov et al. "Hold-In, Pull-In, and Lock-In Ranges of PLL Circuits: Rigorous Mathematical Definitions and Limitations of Classical Theory". In: *IEEE Trans. Circuits Syst. I, Reg. Papers* 62.10 (2015), pp. 2454–2464

Stable Equilibria (SE) (2/3)

Induced-jamming



Induced-spoofing



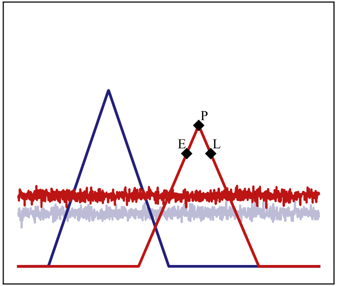
LINEAR ASSUMPTION

Stable Equilibria (SE) (2/3)

Induced-jamming

Tracked dynamic: Authentic dynamic η_{a} or frequency-mismatched version $(1/2T_{\text{i}})$

Induced-spoofing



Stable Equilibria (SE) (2/3)

Induced-jamming

Tracked dynamic: Authentic dynamic η_a or frequency-mismatched version $(1/2T_i)$

Induced-spoofing

Tracked dynamic: Spoofing dynamic η_s or a frequency-mismatched version $(1/2T_i)$

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Stable Equilibria (SE) (2/3)

Induced-jamming

Tracked dynamic: Authentic dynamic η_{a} or frequency-mismatched version $(1/2T_{\mathrm{i}})$

Induced-spoofing

Tracked dynamic: Spoofing dynamic η_{s} or a frequency-mismatched version $(1/2T_{\mathrm{i}})$

Stable Equilibria (SE) (3/3)

System SE under induced-multipath:

$$\begin{cases} d_\tau\left(\boxed{\boldsymbol{\varepsilon}_\eta^l}, \Delta\boldsymbol{\nu}\right) = 0, & d_\theta\left(\boxed{\boldsymbol{\varepsilon}_\eta^l}, \Delta\boldsymbol{\nu}\right) = 0, & \chi_f\left(\boxed{\boldsymbol{\varepsilon}_\eta^l}, \Delta\boldsymbol{\nu}\right) = 0 \\ \dfrac{\partial d_\tau\left(\boxed{\boldsymbol{\varepsilon}_\eta^l}, \Delta\boldsymbol{\nu}\right)}{\partial \varepsilon_\tau} > 0, & \dfrac{\partial d_\theta\left(\boxed{\boldsymbol{\varepsilon}_\eta^l}, \Delta\boldsymbol{\nu}\right)}{\partial \varepsilon_\theta} > 0, & \dfrac{\partial \chi_f\left(\boxed{\boldsymbol{\varepsilon}_\eta^l}, \Delta\boldsymbol{\nu}\right)}{\partial \varepsilon_f} > 0 \end{cases}$$

$$\overbrace{\boxed{\boldsymbol{\varepsilon}_\eta^l}}^{\text{System SE}} = \left[\underbrace{\boxed{{\varepsilon_\tau}^l}}_{\text{Code SE}}, \underbrace{\boxed{{\varepsilon_f}^l}}_{\text{Frequency SE}}, \overbrace{\boxed{{\varepsilon_\theta}^l}}^{\text{Phase SE}}\right]^{\mathsf{T}}$$

⚠ NON-LINEAR AND INTERDEPENDENT ⚠

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Stable Equilibria (SE) (3/3)

System SE under induced-multipath:

Independent of ε_θ

$$\begin{cases} d_\tau\left(\varepsilon_\tau^l, \varepsilon_f^l, \Delta\boldsymbol{\nu}\right) = 0, & d_\theta\left(\boldsymbol{\varepsilon}_\eta^l, \Delta\boldsymbol{\nu}\right) = 0, & \chi_f\left(\varepsilon_\tau^l, \varepsilon_f^l, \Delta\boldsymbol{\nu}\right) = 0 \\ \dfrac{\partial d_\tau\left(\varepsilon_\tau^l, \varepsilon_f^l, \Delta\boldsymbol{\nu}\right)}{\partial \varepsilon_\tau} > 0, & \dfrac{\partial d_\theta\left(\boldsymbol{\varepsilon}_\eta^l, \Delta\boldsymbol{\nu}\right)}{\partial \varepsilon_\theta} > 0, & \dfrac{\partial \chi_f\left(\varepsilon_\tau^l, \varepsilon_f^l, \Delta\boldsymbol{\nu}\right)}{\partial \varepsilon_f} > 0 \end{cases}$$

$$\underbrace{\boldsymbol{\varepsilon}_\eta^l}_{\text{System SE}} = \left[\underbrace{{\varepsilon_\tau}^l}_{\text{Code SE}}, \underbrace{{\varepsilon_f}^l}_{\text{Frequency SE}}, {\varepsilon_\theta}^l\right]^\mathsf{T}$$

⚠ d_τ and χ_f INDEPENDENT OF PHASE ERROR ⚠

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Stable Equilibria (SE) (3/3)

System SE under induced-multipath:

$$\begin{cases} d_\tau\left(\varepsilon_\tau^I, \varepsilon_f^I, \Delta\boldsymbol{\nu}\right) = 0, & d_\theta\left(\boldsymbol{\varepsilon}_\eta^I, \Delta\boldsymbol{\nu}\right) = 0, & \chi_f\left(\varepsilon_\tau^I, \varepsilon_f^I, \Delta\boldsymbol{\nu}\right) = 0 \\ \dfrac{\partial d_\tau\left(\varepsilon_\tau^I, \varepsilon_f^I, \Delta\boldsymbol{\nu}\right)}{\partial \varepsilon_\tau} > 0, & \dfrac{\partial d_\theta\left(\boldsymbol{\varepsilon}_\eta^I, \Delta\boldsymbol{\nu}\right)}{\partial \varepsilon_\theta} > 0, & \dfrac{\partial \chi_f\left(\varepsilon_\tau^I, \varepsilon_f^I, \Delta\boldsymbol{\nu}\right)}{\partial \varepsilon_f} > 0 \end{cases}$$

$$\underbrace{\boldsymbol{\varepsilon}_\eta^I}_{\text{System SE}} = \left[\underbrace{{\varepsilon_\tau}^I}_{\text{Code SE}}, \underbrace{{\varepsilon_f}^I}_{\text{Frequency SE}}, {\varepsilon_\theta}^I\right]^\mathsf{T}$$

⚠ d_τ and χ_f INDEPENDENT OF PHASE ERROR ⚠

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Stable Equilibria (SE) (3/3)

System SE under induced-multipath:

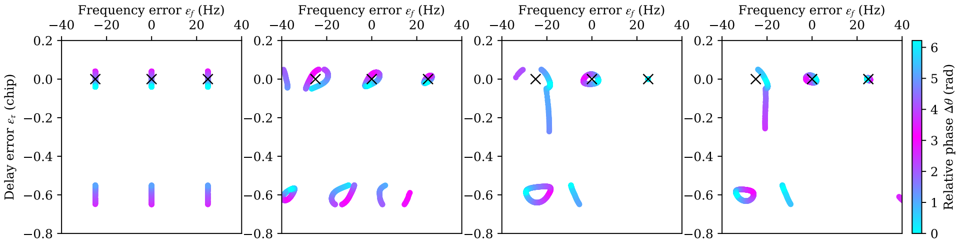
$$\begin{cases} d_\tau\left(\varepsilon^I_\tau, \varepsilon^I_f, \Delta\boldsymbol{\nu}\right) = 0, & d_\theta\left(\boldsymbol{\varepsilon}^I_\eta, \Delta\boldsymbol{\nu}\right) = 0, & \chi_f\left(\varepsilon^I_\tau, \varepsilon^I_f, \Delta\boldsymbol{\nu}\right) = 0 \\ \dfrac{\partial d_\tau\left(\varepsilon^I_\tau, \varepsilon^I_f, \Delta\boldsymbol{\nu}\right)}{\partial \varepsilon_\tau} > 0, & \dfrac{\partial d_\theta\left(\boldsymbol{\varepsilon}^I_\eta, \Delta\boldsymbol{\nu}\right)}{\partial \varepsilon_\theta} > 0, & \dfrac{\partial \chi_f\left(\varepsilon^I_\tau, \varepsilon^I_f, \Delta\boldsymbol{\nu}\right)}{\partial \varepsilon_f} > 0. \end{cases}$$

$$\overset{\text{System SE}}{\boldsymbol{\varepsilon}^I_\eta} = \left[\underset{\text{Code SE}}{{\varepsilon_\tau}^I},\ \underset{\text{Frequency SE}}{{\varepsilon_f}^I},\ {\varepsilon_\theta}^I\right]^{\mathsf{T}}$$

⚠ d_τ and χ_f INDEPENDENT OF PHASE ERROR ⚠

Stable Equilibria (SE) (3/3)

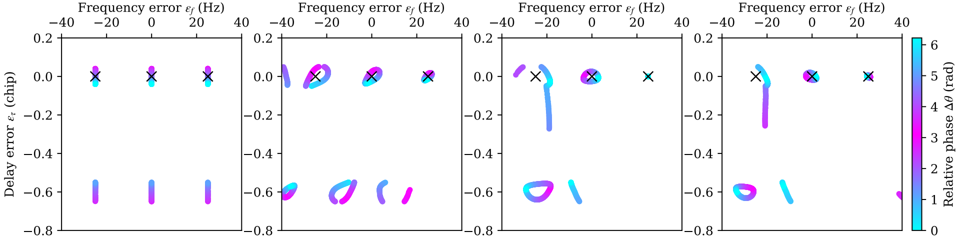
System SE under induced-multipath:



$\Delta f = 0$ Hz $\Delta f = 12$ Hz $\Delta f = 25$ Hz $\Delta f = 31$ Hz

Stable Equilibria (SE) (3/3)

System SE under induced-multipath:

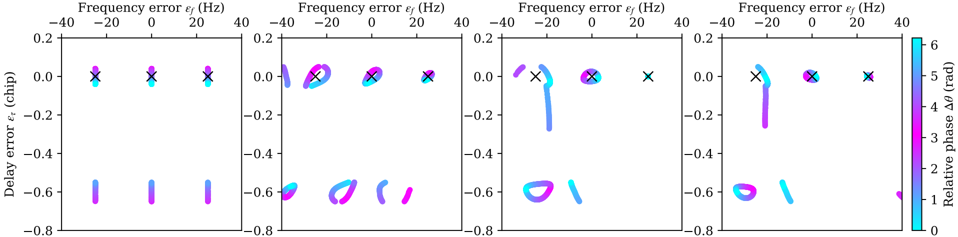


$\Delta f = 0$ Hz $\Delta f = 12$ Hz $\Delta f = 25$ Hz $\Delta f = 31$ Hz

Induced-Multipath Results (Asynchronous Frequency Spoofer)

Stable Equilibria (SE) (3/3)

System SE under induced-multipath:



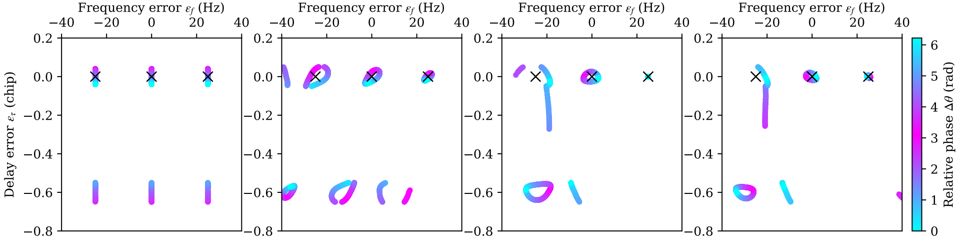
$\Delta f = 0$ Hz $\quad \Delta f = 12$ Hz $\quad \Delta f = 25$ Hz $\quad \Delta f = 31$ Hz

Induced-Multipath Results (Asynchronous Frequency Spoofer)

Emergence of **multiple possible points of convergence** (chaotic behavior and bifurcations).

Stable Equilibria (SE) (3/3)

System SE under induced-multipath:



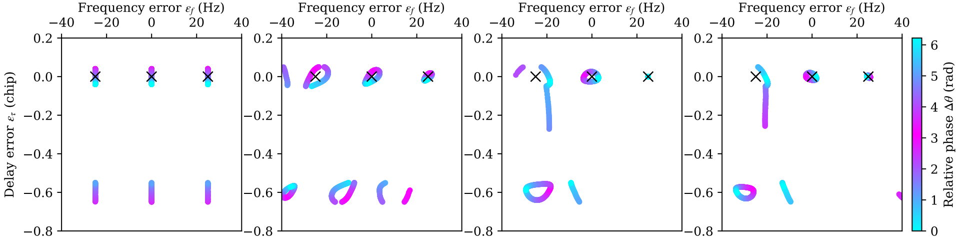
$\Delta f = 0$ Hz $\Delta f = 12$ Hz $\Delta f = 25$ Hz $\Delta f = 31$ Hz

Induced-Multipath Results (Asynchronous Frequency Spoofer)

- Emergence of **multiple possible points of convergence** (chaotic behavior and bifurcations).
- **Interdependence** between the DLL and PLL.

Stable Equilibria (SE) (3/3)

System SE under induced-multipath:



$\Delta f = 0$ Hz $\Delta f = 12$ Hz $\Delta f = 25$ Hz $\Delta f = 31$ Hz

Induced-Multipath Results (Asynchronous Frequency Spoofer)

- Emergence of **multiple possible points of convergence** (chaotic behavior and bifurcations).
- **Interdependence** between the DLL and PLL.
- **Oscillating patterns** over the relative phase $\Delta\theta \in [0, 2\pi]$.

Dynamic and stochastic response (1/5)

Objective

- **Characterize the dynamic response** of the loops, including transient behavior and all dynamic aspects (feedback and filtering).

[1] Someshwar C Gupta. "Phase-Locked loops". In: *Proc. IEEE* 63.2 (1975), pp. 291–306

Dynamic and stochastic response (1/5)

Objective

- **Characterize the dynamic response** of the loops, including transient behavior and all dynamic aspects (feedback and filtering).
- Evaluate the **impact of noise** on the dynamic response.[1]

[1] Someshwar C Gupta. "Phase-Locked loops". In: *Proc. IEEE* 63.2 (1975), pp. 291–306

Dynamic and stochastic response (1/5)

Objective

- **Characterize the dynamic response** of the loops, including transient behavior and all dynamic aspects (feedback and filtering).
- Evaluate the **impact of noise** on the dynamic response.[1]

Closed-loop model:

$$\begin{cases} \hat{\tau}(z) + \beta\, \hat{\theta}(z) = \dfrac{z^{-1}}{1 - z^{-1}} T_{\mathrm{i}}\, F_{\tau}(z)\, D_{\tau}\left(\boldsymbol{\eta}_{\mathrm{a}}(z) - \hat{\boldsymbol{\eta}}(z), \Delta\boldsymbol{\nu}(z)\right) & \text{(DLL)} \\ \hat{\theta}(z) = \dfrac{z^{-1}}{1 - z^{-1}} T_{\mathrm{i}}\, F_{\theta}(z)\, D_{\theta}\left(\boldsymbol{\eta}_{\mathrm{a}}(z) - \hat{\boldsymbol{\eta}}(z), \Delta\boldsymbol{\nu}(z)\right) & \text{(PLL)} \end{cases}$$

[1] Someshwar C Gupta. "Phase-Locked loops". In: *Proc. IEEE* 63.2 (1975), pp. 291–306

Dynamic and stochastic response (2/5)

Induced-Jamming and Induced-Spoofing Results

Linear Assumption:

LINEAR ASSUMPTION

[1] John W Betz and Kevin R Kolodziejski. "Generalized theory of code tracking with an early-late discriminator part II: Noncoherent processing and numerical results". In: *IEEE Transactions on Aerospace and Electronic Systems* 45.4 (2009), pp. 1557–1564.

Dynamic and stochastic response (2/5)

Induced-Jamming and Induced-Spoofing Results

Linear Assumption:

✓ The dynamic response can be analyzed through the **transfer function** of the equivalent linear closed-loop model $H_\phi(z)$:

$$\hat{\phi}^{(\mathrm{J})}(z) = H_\phi(z)\,\phi_{\mathrm{a}}, \qquad \hat{\phi}^{(\mathrm{S})}(z) = H_\phi(z)\,\phi_{\mathrm{s}}.$$

LINEAR ASSUMPTION

[1] John W Betz and Kevin R Kolodziejski. "Generalized theory of code tracking with an early-late discriminator part II: Noncoherent processing and numerical results". In: *IEEE Transactions on Aerospace and Electronic Systems* 45.4 (2009), pp. 1557–1564.

Dynamic and stochastic response (2/5)

Induced-Jamming and Induced-Spoofing Results

Linear Assumption:

- ✓ The dynamic response can be analyzed through the **transfer function** of the equivalent linear closed-loop model $H_\phi(z)$:

$$\hat{\phi}^{(\mathrm{J})}(z) = H_\phi(z)\,\phi_\mathrm{a}, \qquad \hat{\phi}^{(\mathrm{S})}(z) = H_\phi(z)\,\phi_\mathrm{s}.$$

- ✓ The noise is considered **additive and homogeneous** and can be modeled as presented for the nominal situation in the literature[1].

LINEAR ASSUMPTION

[1] John W Betz and Kevin R Kolodziejski. "Generalized theory of code tracking with an early-late discriminator part II: Noncoherent processing and numerical results". In: *IEEE Transactions on Aerospace and Electronic Systems* 45.4 (2009), pp. 1557–1564.

Dynamic and stochastic response (3/5)

Resolution Under Induced-Multipath Situation

Non-linear:

- × The system **cannot be modeled using a transfer function**.

$$\begin{cases} \hat{\tau}(z) + \beta\, \hat{\theta}(z) = \dfrac{z^{-1}}{1 - z^{-1}} T_\mathrm{i}\, F_\tau(z)\, D_\tau\Big(\boldsymbol{\eta}_\mathrm{a}(z) - \hat{\boldsymbol{\eta}}(z)\, , \boxed{\Delta\boldsymbol{\nu}(z)}\Big) & \text{(DLL)} \\ \hat{\theta}(z) = \dfrac{z^{-1}}{1 - z^{-1}} T_\mathrm{i}\, F_\theta(z)\, D_\theta\Big(\boldsymbol{\eta}_\mathrm{a}(z) - \hat{\boldsymbol{\eta}}(z)\, , \boxed{\Delta\boldsymbol{\nu}(z)}\Big) & \text{(PLL)} \end{cases}$$

⚠ NON-LINEAR AND INTERDEPENDENT ⚠

RÉPUBLIQUE FRANÇAISE Liberté Égalité Fraternité ENAC

Dynamic and stochastic response (3/5)

Resolution Under Induced-Multipath Situation

Non-linear:

- × The system **cannot be modeled using a transfer function**.

Random state vector $\hat{\phi}$ (p_ϕ)

$$\begin{cases} \hat{\tau}(z) + \beta\,\hat{\theta}(z) = \dfrac{z^{-1}}{1-z^{-1}} T_\mathrm{i}\, F_\tau(z)\, D_\tau\Big(\boldsymbol{\eta}_\mathrm{a}(z) - \hat{\boldsymbol{\eta}}(z), \Delta\boldsymbol{\nu}(z)\Big) & \text{(DLL)} \\ \hat{\theta}(z) = \dfrac{z^{-1}}{1-z^{-1}} T_\mathrm{i}\, F_\theta(z)\, D_\theta\Big(\boldsymbol{\eta}_\mathrm{a}(z) - \hat{\boldsymbol{\eta}}(z), \Delta\boldsymbol{\nu}(z)\Big) & \text{(PLL)} \end{cases}$$

⚠ NON-LINEAR AND INTERDEPENDENT ⚠

Dynamic and stochastic response (3/5)

Resolution Under Induced-Multipath Situation

Non-linear:

- × The system **cannot be modeled using a transfer function**.
- × **Non-additivity:** Input dynamics and noise response cannot be separated.

Random state vector $\hat{\phi}$ (p_{ϕ})

$$
\begin{cases}
\hat{\tau}(z) + \beta\, \hat{\theta}(z) = \dfrac{z^{-1}}{1 - z^{-1}}\, T_{\mathrm{i}}\, F_{\tau}(z)\, D_{\tau}\left(\boldsymbol{\eta}_{\mathrm{a}}(z) - \hat{\boldsymbol{\eta}}(z), \Delta\boldsymbol{\nu}(z)\right) & \text{(DLL)} \\
\hat{\theta}(z) = \dfrac{z^{-1}}{1 - z^{-1}}\, T_{\mathrm{i}}\, F_{\theta}(z)\, D_{\theta}\left(\boldsymbol{\eta}_{\mathrm{a}}(z) - \hat{\boldsymbol{\eta}}(z), \Delta\boldsymbol{\nu}(z)\right) & \text{(PLL)}
\end{cases}
$$

⚠ NON-LINEAR AND INTERDEPENDENT ⚠

Dynamic and stochastic response (3/5)

Resolution Under Induced-Multipath Situation

Non-linear:

- × The system **cannot be modeled using a transfer function**.
- × **Non-additivity:** Input dynamics and noise response cannot be separated.
- × **Heterogeneity:** Noise variance depends on the system's actual state.

Random state vector $\hat{\phi}$ (p_{ϕ})

$$\begin{cases} \hat{\tau}(z) + \beta\, \hat{\theta}(z) = \dfrac{z^{-1}}{1 - z^{-1}} T_{\mathrm{i}}\, F_{\tau}(z)\, D_{\tau}\Big(\boldsymbol{\eta}_{\mathrm{a}}(z) - \hat{\boldsymbol{\eta}}(z), \Delta\boldsymbol{\nu}(z)\Big) & \text{(DLL)} \\ \hat{\theta}(z) = \dfrac{z^{-1}}{1 - z^{-1}} T_{\mathrm{i}}\, F_{\theta}(z)\, D_{\theta}\Big(\boldsymbol{\eta}_{\mathrm{a}}(z) - \hat{\boldsymbol{\eta}}(z), \Delta\boldsymbol{\nu}(z)\Big) & \text{(PLL)} \end{cases}$$

⚠ NON-LINEAR AND INTERDEPENDENT ⚠

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Dynamic and stochastic response (3/5)

Resolution Strategy

Quasi-Harmonic Behavior:

Random state vector $\hat{\phi}$ (p_ϕ)

$$\begin{cases} \hat{\tau}(z) + \beta\, \hat{\theta}(z) = \dfrac{z^{-1}}{1-z^{-1}}\, T_{\mathrm{i}}\, F_\tau(z)\, D_\tau\Big(\boldsymbol{\eta}_{\mathrm{a}}(z) - \hat{\boldsymbol{\eta}}(z),\, \Delta\boldsymbol{\nu}(z)\Big) & \text{(DLL)} \\ \hat{\theta}(z) = \dfrac{z^{-1}}{1-z^{-1}}\, T_{\mathrm{i}}\, F_\theta(z)\, D_\theta\Big(\boldsymbol{\eta}_{\mathrm{a}}(z) - \hat{\boldsymbol{\eta}}(z),\, \Delta\boldsymbol{\nu}(z)\Big) & \text{(PLL)} \end{cases}$$

⚠ NON-LINEAR AND INTERDEPENDENT ⚠

Dynamic and stochastic response (3/5)

Resolution Strategy

Quasi-Harmonic Behavior:

- The system's SE exhibit oscillations along the relative phase $\Delta\theta$.

Random state vector $\hat{\phi}$ (p_{ϕ})

$$
\begin{cases}
\hat{\tau}(z) + \beta\,\hat{\theta}(z) = \dfrac{z^{-1}}{1 - z^{-1}}\, T_{\text{i}}\, F_{\tau}(z)\, D_{\tau}\Big(\boldsymbol{\eta}_{\text{a}}(z) - \hat{\boldsymbol{\eta}}(z), \Delta\boldsymbol{\nu}(z)\Big) & \text{(DLL)} \\
\hat{\theta}(z) = \dfrac{z^{-1}}{1 - z^{-1}}\, T_{\text{i}}\, F_{\theta}(z)\, D_{\theta}\Big(\boldsymbol{\eta}_{\text{a}}(z) - \hat{\boldsymbol{\eta}}(z), \Delta\boldsymbol{\nu}(z)\Big) & \text{(PLL)}
\end{cases}
$$

⚠ NON-LINEAR AND INTERDEPENDENT ⚠

Dynamic and stochastic response (3/5)

Resolution Strategy

Quasi-Harmonic Behavior:

- The system's SE exhibit oscillations along the relative phase $\Delta\theta$.
- Other relative parameters, $\Delta\boldsymbol{\nu}$, can be assumed constant over $\Delta\theta \in [0, 2\pi]$.

Random state vector $\hat{\phi}$ (p_{ϕ})

$$\begin{cases} \hat{\tau}(z) + \beta\, \hat{\theta}(z) = \dfrac{z^{-1}}{1 - z^{-1}}\, T_{\mathrm{i}}\, F_{\tau}(z)\, D_{\tau}\Big(\boldsymbol{\eta}_{\mathrm{a}}(z) - \hat{\boldsymbol{\eta}}(z), \Delta\boldsymbol{\nu}(z)\Big) & \text{(DLL)} \\ \hat{\theta}(z) = \dfrac{z^{-1}}{1 - z^{-1}}\, T_{\mathrm{i}}\, F_{\theta}(z)\, D_{\theta}\Big(\boldsymbol{\eta}_{\mathrm{a}}(z) - \hat{\boldsymbol{\eta}}(z), \Delta\boldsymbol{\nu}(z)\Big) & \text{(PLL)} \end{cases}$$

⚠ NON-LINEAR AND INTERDEPENDENT ⚠

Dynamic and stochastic response (3/5)

Resolution Strategy

Quasi-Harmonic Behavior:

- The system's SE exhibit oscillations along the relative phase $\Delta\theta$.
- Other relative parameters, $\Delta\boldsymbol{\nu}$, can be assumed constant over $\Delta\theta \in [0, 2\pi]$.
- The system behavior can be characterized by its quasi-harmonic response for any $\Delta\boldsymbol{\nu}$.

Random state vector $\hat{\phi}$ (p_ϕ)

Constant except $\Delta\theta \in [0, 2\pi]$

$$\begin{cases} \hat{\tau}(z) + \beta\,\hat{\theta}(z) = \dfrac{z^{-1}}{1 - z^{-1}}\, T_{\mathrm{i}}\, F_\tau(z)\, D_\tau\Big(\boldsymbol{\eta}_{\mathrm{a}}(z) - \hat{\boldsymbol{\eta}}(z), \Delta\boldsymbol{\nu}\Big) & \text{(DLL)} \\ \hat{\theta}(z) = \dfrac{z^{-1}}{1 - z^{-1}}\, T_{\mathrm{i}}\, F_\theta(z)\, D_\theta\Big(\boldsymbol{\eta}_{\mathrm{a}}(z) - \hat{\boldsymbol{\eta}}(z), \Delta\boldsymbol{\nu}\Big) & \text{(PLL)} \end{cases}$$

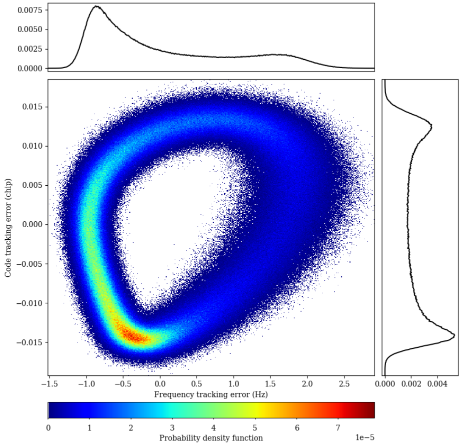
⚠ NON-LINEAR AND INTERDEPENDENT ⚠

Dynamic and stochastic response (4/5)

Induced-Multipath Results

Quasi-harmonic behavior:

Dynamic and stochastic response (4/5)



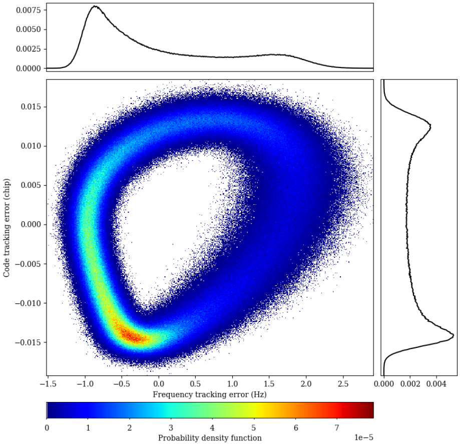
Tracking error PDF p_ϕ ($\Delta\tau = 0.5$ chip, $\Delta f = 2$ Hz, $\Delta g = 0.64$ and $C/N_0 = 50$ dB.Hz).

Induced-Multipath Results

Quasi-harmonic behavior:

- ✓ Enable the characterization of the tracking error under induced multipath as a function of the relative dynamics $\Delta\nu$ and receiver parameters.

Dynamic and stochastic response (4/5)



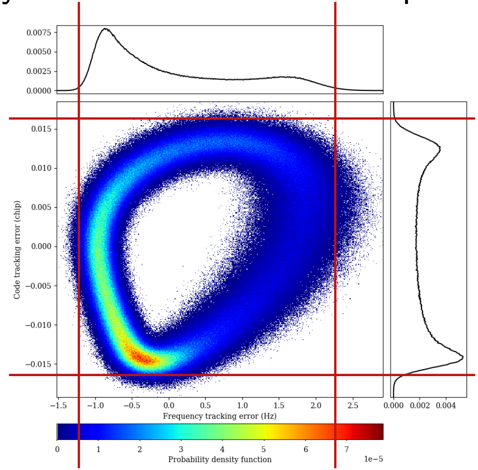
Tracking error PDF p_ϕ ($\Delta\tau = 0.5$ chip, $\Delta f = 2$ Hz, $\Delta g = 0.64$ and $C/N_0 = 50$ dB.Hz).

Induced-Multipath Results

Quasi-harmonic behavior:

- ✓ Enable the characterization of the tracking error under induced multipath as a function of the relative dynamics $\Delta\nu$ and receiver parameters.
- ✓ Accounts for the **system's non-linearity, filtering, and stochastic aspects**.

Dynamic and stochastic response (4/5)



Tracking error PDF p_ϕ ($\Delta\tau = 0.5$ chip, $\Delta f = 2$ Hz, $\Delta g = 0.64$ and $C/N_0 = 50$ dB.Hz).

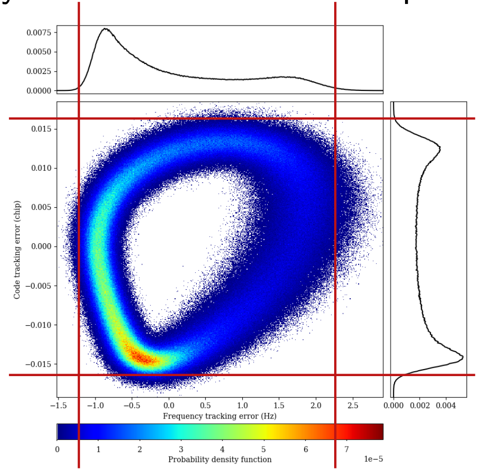
Induced-Multipath Results

Quasi-harmonic behavior:

- ✓ Enable the characterization of the tracking error under induced multipath as a function of the relative dynamics $\Delta\nu$ and receiver parameters.
- ✓ Accounts for the **system's non-linearity, filtering, and stochastic aspects**.
- ✓ Enables the derivation of a more accurate **Spoofing Error Envelope (SEE)**.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Dynamic and stochastic response (4/5)



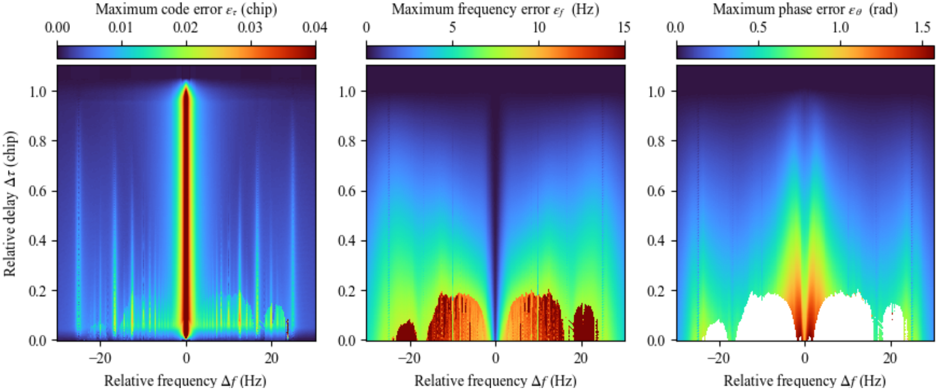
Tracking error PDF p_ϕ ($\Delta\tau = 0.5$ chip, $\Delta f = 2$ Hz, $\Delta g = 0.64$ and $C/N_0 = 50$ dB.Hz).

Induced-Multipath Results

Quasi-harmonic behavior:

- ✓ Enable the characterization of the tracking error under induced multipath as a function of the relative dynamics $\Delta\boldsymbol{\nu}$ and receiver parameters.
- ✓ Accounts for the **system's non-linearity, filtering, and stochastic aspects**.
- ✓ Enables the derivation of a more accurate **Spoofing Error Envelope (SEE)**.
- × Does not model **bifurcation or transient response**.

Dynamic and stochastic response (5/5)



Code Frequency Phase

Absolute Spoofing Error Envelope ($\Delta g = 0.64$ and authentic C/N_0 of 55 dB.Hz).

Outline

C/N_0 definition

Objective

Characterize the true and estimated C/N_0 under each induced-spoofing situation.

C/N_0 definition

Objective

Characterize the true and estimated C/N_0 under each induced-spoofing situation.

True C/N_0 (over $\Omega \times I_t$):

$$\left(\frac{C}{N_0}\right)_{\text{true}} \triangleq \frac{1}{T_\mathrm{i}} \frac{P_\mathrm{d}}{P_\varsigma}$$

C/N_0 definition

Objective

Characterize the true and estimated C/N_0 under each induced-spoofing situation.

True C/N_0 (over $\Omega \times I_t$):

$$\left(\frac{C}{N_0}\right)_{\text{true}} \triangleq \underbrace{\frac{1}{T_\text{i}}}_{\text{Normalization factor}} \frac{\overbrace{P_\text{d}}^{\text{Useful signal power}}}{\underbrace{P_\varsigma}_{\text{Random signal power}}}$$

C/N_0 definition

Objective

Characterize the true and estimated C/N_0 under each induced-spoofing situation.

True C/N_0 (over $\Omega \times I_t$):

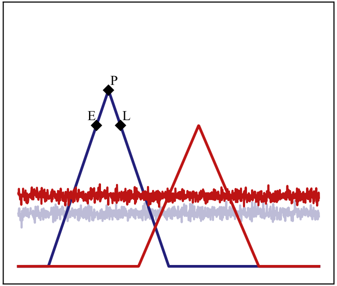
$$\left(\frac{C}{N_0}\right)_{\text{true}} \triangleq \underbrace{\frac{1}{T_\mathrm{i}}}_{\text{Normalization factor}} \frac{\overbrace{P_\mathrm{d}}^{\text{Useful signal power}}}{\underbrace{P_\varsigma}_{\text{Random signal power}}}$$

Estimated C/N_0 (measured on the prompt correlator outputs over I_t):
Three algorithms:

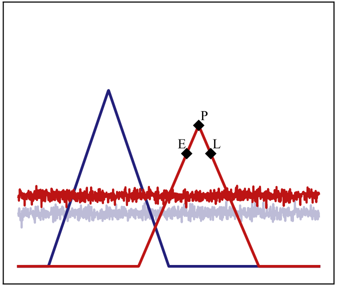
- Moment Method (MM) (equivalent to Variance Summing Method (VSM),
- Narrow Wideband Power Ratio (NWPR),
- Beaulieu method.

C/N_0 under spoofing (1/4)

Induced-jamming



Induced-spoofing



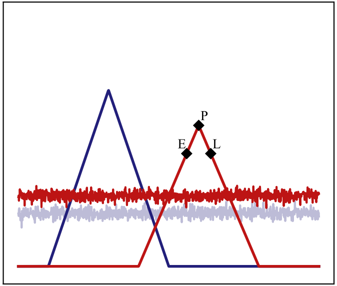
C/N_0 under spoofing (1/4)

Induced-jamming

True C/N_0:

$$\left(\frac{C}{N_0}\right)^{(\mathrm{J})}_{\mathrm{true}} = \frac{1}{T_\mathrm{i}}\frac{P_\mathrm{d}}{P_\varsigma} = \frac{\zeta(\varepsilon_\eta)^2}{T_\mathrm{i}}\frac{C_\mathrm{a}}{P_n + P_\chi}$$

Induced-spoofing



C/N_0 under spoofing (1/4)

Induced-jamming

True C/N_0:

$$\left(\frac{C}{N_0}\right)^{(\mathrm{J})}_{\mathrm{true}} = \frac{1}{T_\mathrm{i}}\frac{P_\mathrm{d}}{P_\varsigma} = \frac{\zeta(\varepsilon_\eta)^2}{T_\mathrm{i}}\frac{C_\mathrm{a}}{P_n + P_\chi}$$

Induced-spoofing

True C/N_0:

$$\left(\frac{C}{N_0}\right)^{(\mathrm{S})}_{\mathrm{true}} = \frac{1}{T_\mathrm{i}}\frac{P_\mathrm{d}}{P_\varsigma} = \frac{\zeta(\varepsilon_\eta + \Delta\boldsymbol{\eta})^2}{T_\mathrm{i}}\frac{\Delta g\, C_\mathrm{a}}{P_n + P_\chi}$$

C/N_0 under spoofing (1/4)

Induced-jamming

True C/N_0:

$$\left(\frac{C}{N_0}\right)^{(\mathrm{J})}_{\mathrm{true}} = \frac{1}{T_\mathrm{i}} \frac{\overbrace{P_\mathrm{d}}^{\text{Authentic power}}}{\underbrace{P_\varsigma}_{\text{Random contribution power}}} = \frac{\zeta(\varepsilon_\eta)^2}{T_\mathrm{i}} \frac{\overbrace{C_\mathrm{a}}^{\text{Authentic power}}}{\underbrace{P_n + P_\chi}_{\text{Random contribution power}}}$$

Induced-spoofing

True C/N_0:

$$\left(\frac{C}{N_0}\right)^{(\mathrm{S})}_{\mathrm{true}} = \frac{1}{T_\mathrm{i}} \frac{\overbrace{P_\mathrm{d}}^{\text{Spoofing power}}}{\underbrace{P_\varsigma}_{\text{Random contribution power}}} = \frac{\zeta(\varepsilon_\eta + \Delta\eta)^2}{T_\mathrm{i}} \frac{\overbrace{\Delta g\, C_\mathrm{a}}^{\text{Spoofing power}}}{\underbrace{P_n + P_\chi}_{\text{Random contribution power}}}$$

C/N_0 under spoofing (1/4)

Induced-jamming

True C/N_0:

$$\left(\frac{C}{N_0}\right)^{(\mathrm{J})}_{\text{true}} = \frac{1}{T_\mathrm{i}} \frac{\overbrace{P_\mathrm{d}}^{\text{Authentic power}}}{\underbrace{P_\varsigma}_{\text{Random contribution power}}} = \frac{\zeta(\varepsilon_\eta)^2}{T_\mathrm{i}} \frac{\overbrace{C_\mathrm{a}}^{\text{Authentic power}}}{\underbrace{P_n + P_\chi}_{\text{Random contribution power}}}$$

Induced-spoofing

True C/N_0:

$$\left(\frac{C}{N_0}\right)^{(\mathrm{S})}_{\text{true}} = \frac{1}{T_\mathrm{i}} \frac{\overbrace{P_\mathrm{d}}^{\text{Spoofing power}}}{\underbrace{P_\varsigma}_{\text{Random contribution power}}} = \frac{\zeta(\varepsilon_\eta + \Delta\eta)^2}{T_\mathrm{i}} \frac{\overbrace{\Delta g \; C_\mathrm{a}}^{\text{Spoofing power}}}{\underbrace{P_n + P_\chi}_{\text{Random contribution power}}}$$

Induced-Jamming and Induced-Spoofing Results

The estimators are unbiased and converge to the true C/N_0 value.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

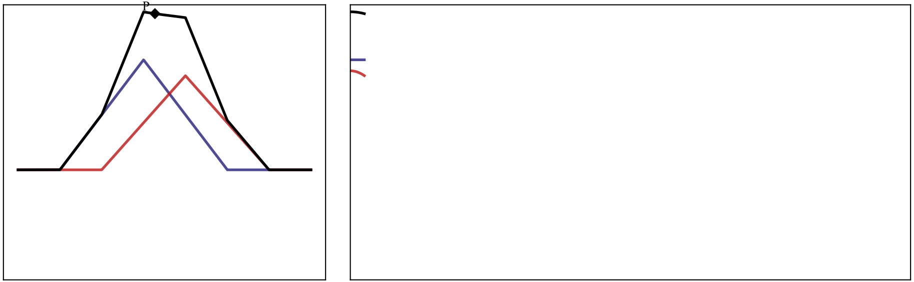
C/N_0 under spoofing (2/4)

Induced-multipath:

$$\Lambda(\eta, \eta_a, \Delta\eta) = \underbrace{\Lambda_a(\eta_a - \eta)}_{\text{Authentic peak}} + \underbrace{\Lambda_s(\eta_a - \eta + \Delta\eta)}_{\text{Spoofing peak}} + \underbrace{\Lambda_\varsigma}_{\text{Random contribution}}$$

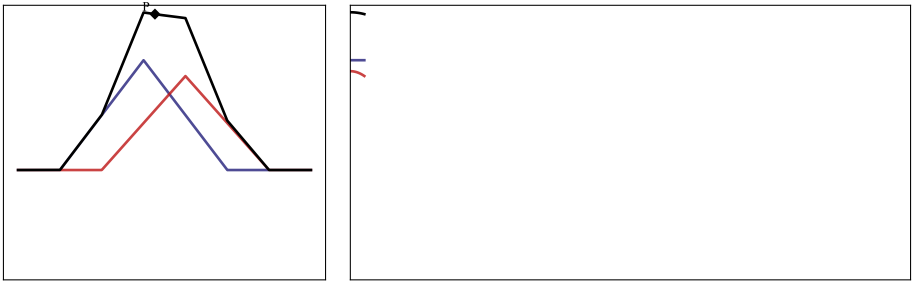
C/N_0 under spoofing (2/4)

Prompt correlator evolution:



C/N_0 under spoofing (2/4)

Prompt correlator evolution:



True C/N_0:

Individual power Interaction power

$$\left(\frac{C}{N_0}\right)^{(\mathrm{M})}_{\mathrm{true}} = \frac{1}{T_\mathrm{i}}\frac{P_\mathrm{d}}{P_\varsigma} = \frac{1}{T_\mathrm{i}}\frac{\left(\mu_d + \omega_d\right) C_\mathrm{a}}{P_n + P_\chi}.$$

Random contribution power

C/N_0 under spoofing (3/4)

Induced-Multipath Results

C/N_0 under spoofing (3/4)

Induced-Multipath Results

- Derivation of **analytic expressions** as a function of $\Delta\eta$.

MM:

$$\mathbb{E}_\Omega\left[\frac{\widehat{C}}{N_0}\right]^{(\mathrm{M})}_{\mathrm{MM}} \approx \frac{1}{T_\mathrm{i}}\frac{\sqrt{{P_\mathrm{d}}^2 - {C_\mathrm{a}}^2 \overbrace{\sigma_\mathrm{d}^2}^{\text{Interaction random power variance}}}}{P_\varsigma + P_\mathrm{d} - \sqrt{{P_\mathrm{d}}^2 - {C_\mathrm{a}}^2 \sigma_\mathrm{d}^2}}$$

Beaulieu:

$$\mathbb{E}_\Omega\left[\frac{\widehat{C}}{N_0}\right]^{(\mathrm{M})}_{\mathrm{B}} = \left[\frac{P_\varsigma + \overbrace{\delta_B}^{\text{Correlator difference power}}}{P_\mathrm{d}} - \underbrace{\varepsilon_B}_{\text{Beaulieu Non-ergodic error}}\right]^{-1}$$

NWPR:

$$\mathbb{E}_\Omega\left[\frac{\widehat{C}}{N_0}\right]^{(\mathrm{M})}_{\mathrm{NWPR}} \approx \frac{1}{T_\mathrm{i}}\frac{P_\mathrm{d} + \sigma_{\mathrm{WB}} - \varepsilon_{\mathrm{PR}}}{P_\varsigma - \underbrace{\sigma_{\mathrm{WB}}}_{\text{NW band error}} + \underbrace{\varepsilon_{\mathrm{PR}}}_{\text{PR non-ergodic error}} / L}$$

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

C/N_0 under spoofing (3/4)

Induced-Multipath Results

- Derivation of **analytic expressions** as a function of $\Delta\eta$.
- The MM, Beaulieu, and NWPR estimators are **biased** and do not reflect the true C/N_0.

MM:

$$\mathbb{E}_\Omega\left[\frac{\widehat{C}}{N_0}\right]_{\mathrm{MM}}^{(\mathrm{M})} \approx \frac{1}{T_\mathrm{i}} \frac{\sqrt{{P_\mathrm{d}}^2 - {C_\mathrm{a}}^2 \overbrace{\sigma_\mathrm{d}^2}^{\text{Interaction random power variance}}}}{P_\varsigma + P_\mathrm{d} - \sqrt{{P_\mathrm{d}}^2 - {C_\mathrm{a}}^2 \sigma_\mathrm{d}^2}}$$

Beaulieu:

$$\mathbb{E}_\Omega\left[\frac{\widehat{C}}{N_0}\right]_{\mathrm{B}}^{(\mathrm{M})} = \left[\frac{P_\varsigma + \overbrace{\delta_B}^{\text{Correlator difference power}}}{P_\mathrm{d}} - \underbrace{\varepsilon_B}_{\text{Beaulieu Non-ergodic error}}\right]^{-1}$$

NWPR:

$$\mathbb{E}_\Omega\left[\frac{\widehat{C}}{N_0}\right]_{\mathrm{NWPR}}^{(\mathrm{M})} \approx \frac{1}{T_\mathrm{i}} \frac{P_\mathrm{d} + \sigma_{\mathrm{WB}} - \varepsilon_{\mathrm{PR}}}{P_\varsigma - \underbrace{\sigma_{\mathrm{WB}}}_{\text{NW band error}} + \underbrace{\varepsilon_{\mathrm{PR}}}_{\text{PR non-ergodic error}} / L}$$

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

C/N_0 under spoofing (3/4)

Induced-Multipath Results

- Derivation of **analytic expressions** as a function of $\Delta\eta$.
- The MM, Beaulieu, and NWPR estimators are **biased** and do not reflect the true C/N_0.
- Spoofing distortion **varies depending on the type of estimator**.

MM:

$$\mathbb{E}_\Omega\left[\frac{\widehat{C}}{N_0}\right]^{(\mathrm{M})}_{\mathrm{MM}} \approx \frac{1}{T_\mathrm{i}} \frac{\sqrt{{P_\mathrm{d}}^2 - {C_\mathrm{a}}^2 \overbrace{\sigma_\mathrm{d}^2}^{\text{Interaction random power variance}}}}{P_\varsigma + P_\mathrm{d} - \sqrt{{P_\mathrm{d}}^2 - {C_\mathrm{a}}^2 \sigma_\mathrm{d}^2}}$$

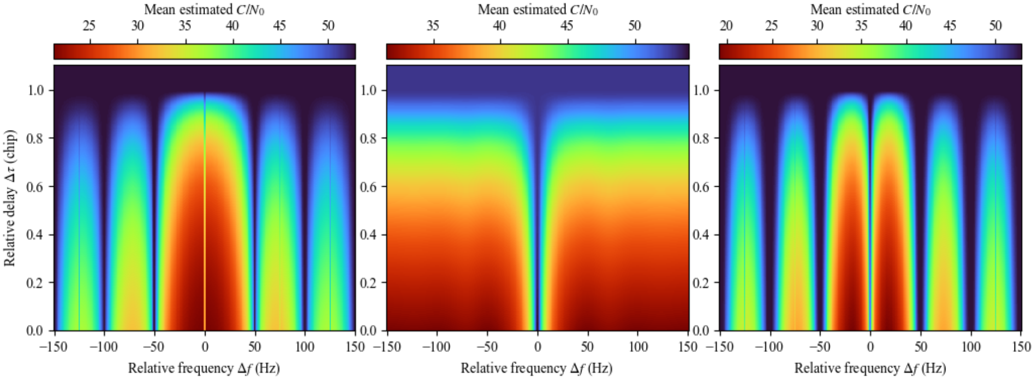
Beaulieu:

$$\mathbb{E}_\Omega\left[\frac{\widehat{C}}{N_0}\right]^{(\mathrm{M})}_{\mathrm{B}} = \left[\frac{P_\varsigma + \overbrace{\delta_B}^{\text{Correlator difference power}}}{P_\mathrm{d}} - \underbrace{\varepsilon_B}_{\text{Beaulieu Non-ergodic error}}\right]^{-1}$$

NWPR:

$$\mathbb{E}_\Omega\left[\frac{\widehat{C}}{N_0}\right]^{(\mathrm{M})}_{\mathrm{NWPR}} \approx \frac{1}{T_\mathrm{i}} \frac{P_\mathrm{d} + \sigma_{\mathrm{WB}} - \varepsilon_{\mathrm{PR}}}{P_\varsigma - \underbrace{\sigma_{\mathrm{WB}}}_{\text{NW band error}} + \underbrace{\varepsilon_{\mathrm{PR}}}_{\text{PR non-ergodic error}} / L}$$

C/N_0 under spoofing (4/4)



MM NWPR Beaulieu

Mean estimated C/N_0 in dB.Hz ($\Delta g = 0.64$ and authentic C/N_0 of 55 dB.Hz).

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Conclusion

Spoofing Impact After Correlation

The impact of spoofing on post-correlation stages can be classified into four situations:

- **Nominal:** The reference scenario with no spoofing impact.
- **Induced-Jamming:** The receiver tracks the authentic dynamics, and the spoofing impact is **reduced to re-radiated noise**.
- **Induced-Spoofing:** The receiver tracks the spoofing dynamics and **adapts to the characteristics of the spoofing signal**.
- **Induced-Multipath:** The receiver tracks a composite of both signals:
  - ⚠ The tracking loops exhibit **chaotic behavior**, including multiple SE and non-linear effects, inducing varying tracking errors and possible bifurcations.
  - ⚠ The C/N_0 estimators **suffer significant degradation**, potentially leading to **loss-of-lock**.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Outline

Experiment presentation

Objectives

Experiment presentation

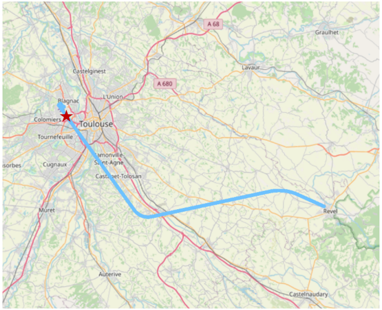
Objectives

- Observe the distortions predicted by the theoretical model in a **realistic spoofing environment** using **real GNSS receivers**.

Experiment presentation

Objectives

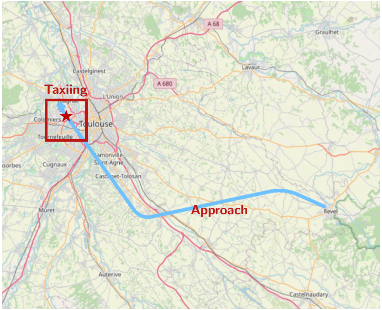
- Observe the distortions predicted by the theoretical model in a **realistic spoofing environment** using **real GNSS receivers**.



Experiment presentation

Objectives

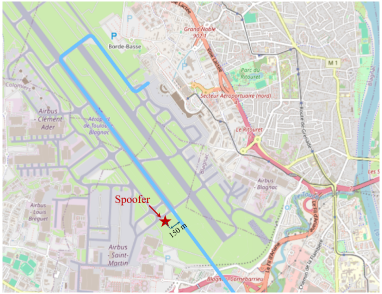
- Observe the distortions predicted by the theoretical model in a **realistic spoofing environment** using **real GNSS receivers**.



Experiment presentation

Objectives

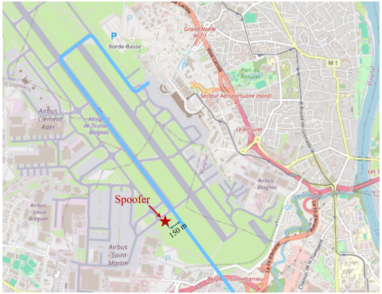
- Observe the distortions predicted by the theoretical model in a **realistic spoofing environment** using **real GNSS receivers**.



Experiment presentation

Objectives

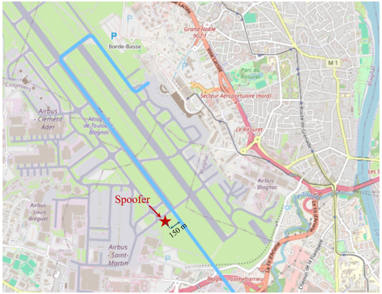
- Observe the distortions predicted by the theoretical model in a **realistic spoofing environment** using **real GNSS receivers**.
- **Evaluate** the theoretical predictions against experimental results and **compare** different receiver architectures.



Experiment presentation

Objectives

- Observe the distortions predicted by the theoretical model in a **realistic spoofing environment** using **real GNSS receivers**.
- **Evaluate** the theoretical predictions against experimental results and **compare** different receiver architectures.

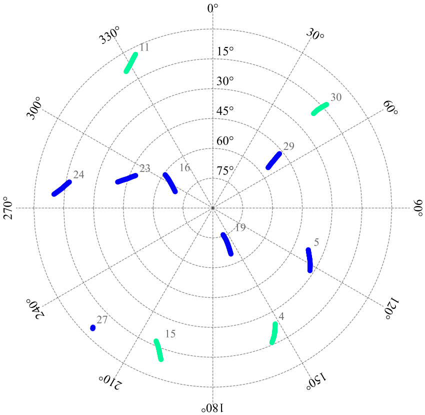


Examined Observables:

- **Theoretical Models**
- **Simulator:** Implements correlator, C/N_0 estimator, and tracking loops.
- **Real Receivers:**
  - GNSS SDR
  - Ifen SX3

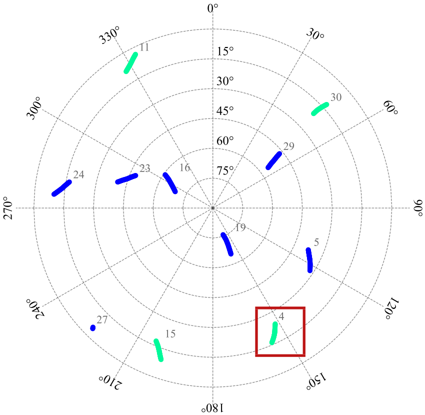
RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité
ENAC

Experiment scenario (1/2)



Experiment scenario (1/2)

PRN 4 analyzed (PRN 11, 15 and 30 in the manuscript)

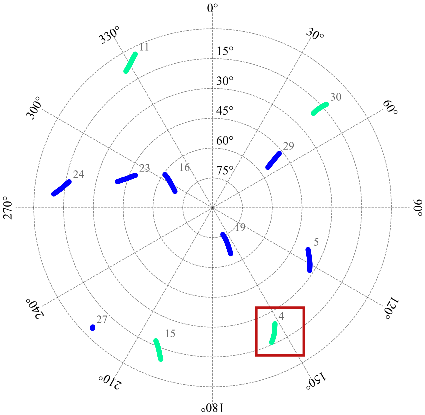


Experiment scenario (1/2)

PRN 4 analyzed (PRN 11, 15 and 30 in the manuscript)

Experiment Scenarios:

- **Scenario 1:** Nominal scenario (no spoofing).
- **Scenario 2:** Low-power sophisticated repeater without re-radiated noise.
- **Scenario 3:** High-power sophisticated repeater without re-radiated noise.



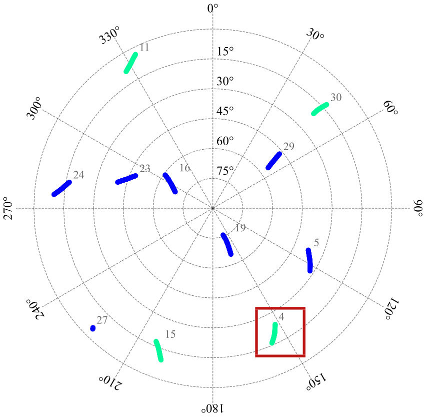
Experiment scenario (1/2)

PRN 4 analyzed (PRN 11, 15 and 30 in the manuscript)

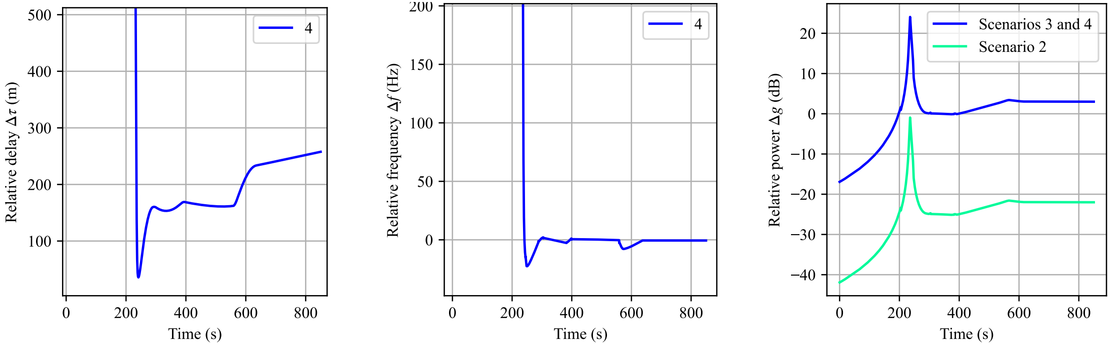
Experiment Scenarios:

- **Scenario 1:** Nominal scenario (no spoofing).
- **Scenario 2:** Low-power sophisticated repeater without re-radiated noise.
- **Scenario 3:** High-power sophisticated repeater without re-radiated noise.

Same authentic dynamics: $\tau_a(t)$, $\theta_a(t)$, and **same spoofing dynamics:** $\tau_s(t)$, $\theta_s(t)$ across each scenario.

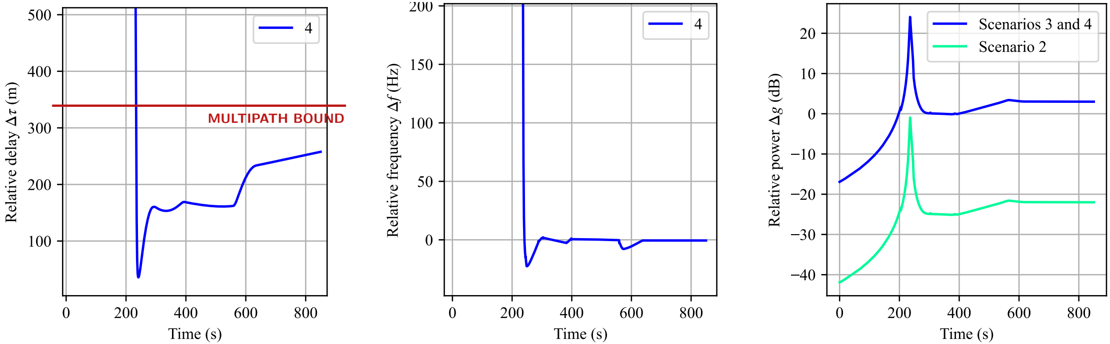


Experiment scenario (2/2)



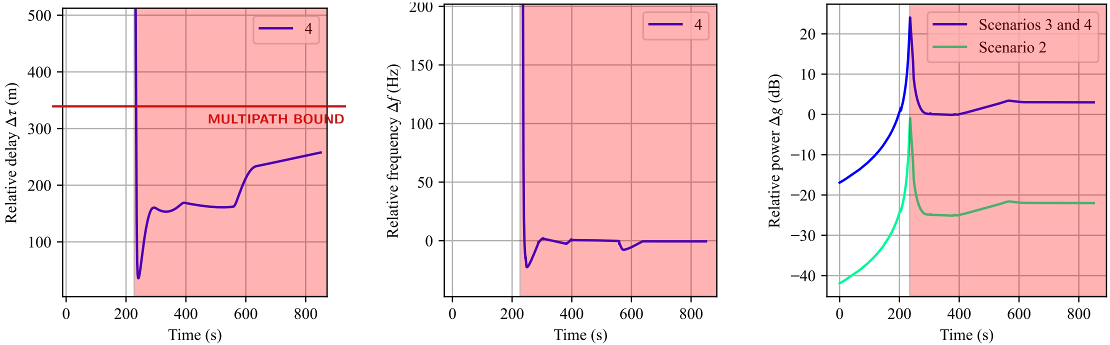
Relative parameters (code, frequency, power) for PRN 4.

Experiment scenario (2/2)



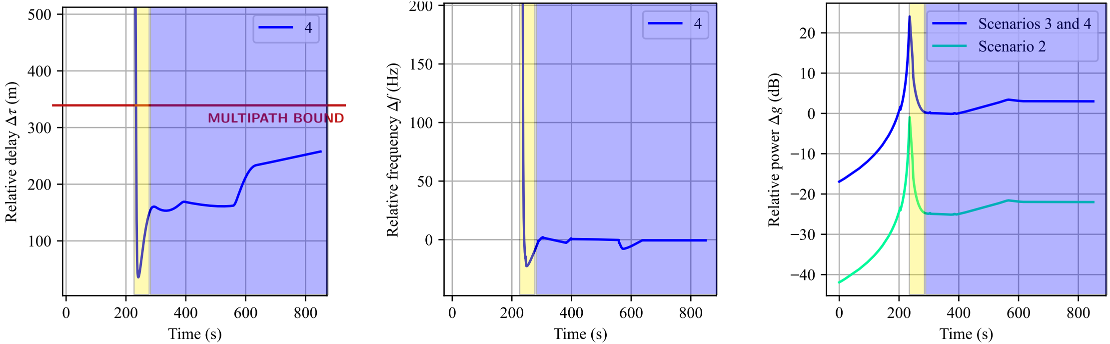
Relative parameters (code, frequency, power) for PRN 4.

Experiment scenario (2/2)



Relative parameters (code, frequency, power) for PRN 4.

Experiment scenario (2/2)



Relative parameters (code, frequency, power) for PRN 4.

: Flying over the spoofer / Landing (high dynamics)

: Taxiing (low dynamics)

Experiment setup

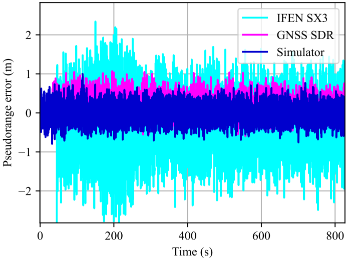
<table>
<tr><th colspan="2"></th><th>SX3</th><th>GNSS-SDR</th><th>Simulator</th></tr>
<tr><td colspan="2" rowspan="2">Acquisition</td><td colspan="2">Doppler $= \pm 5000$ Hz</td><td>Doppler $= \pm 3500$ Hz</td></tr>
<tr><td colspan="3">Coherent time $= 1$ ms, Incoherent number $= 10$, $P_{\mathrm{Fa}} = 10^{-3}$</td></tr>
<tr><td colspan="2">Tracking correlator</td><td colspan="3">Integration time $T_{\mathrm{i}} = 10$ ms</td></tr>
<tr><td rowspan="4">DLL</td><td rowspan="2">Discriminator</td><td>EMLP</td><td>EMLE</td><td>EMLP</td></tr>
<tr><td colspan="3">$c_\tau = 0.1$ chip</td></tr>
<tr><td>Low-pass filter</td><td colspan="3">1st order, $B_\tau = 1$ Hz</td></tr>
<tr><td>Loss indicator</td><td colspan="3">Duration: 1 s, Type: C/N_0, Threshold $\gamma_\tau = 25$ dB·Hz</td></tr>
<tr><td rowspan="4">PLL</td><td>Discriminator</td><td>Costas loop (unknown)</td><td colspan="2">Costas loop (atan)</td></tr>
<tr><td rowspan="2">Low-pass filter</td><td>$B_\theta = 20$ Hz</td><td>$B_\theta = 30$ Hz</td><td>$B_\theta = 20$ Hz</td></tr>
<tr><td colspan="3">3rd order</td></tr>
<tr><td>Loss indicator</td><td>Not used</td><td>NECT, Duration: 1 s,
Threshold $\gamma_\theta = 0.85$</td><td>Not used</td></tr>
<tr><td colspan="2" rowspan="2">C/N_0 estimation</td><td>Signal power/Noise power</td><td colspan="2">Type: MM</td></tr>
<tr><td colspan="3">Estimation period: 1 s</td></tr>
</table>

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

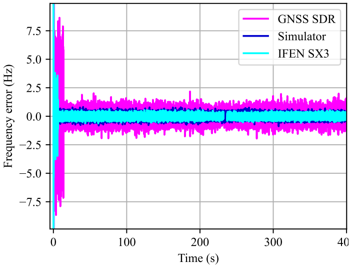
Experiment setup

<table>
<tr><th colspan="2"></th><th>SX3</th><th>GNSS-SDR</th><th>Simulator</th></tr>
<tr><td colspan="2" rowspan="2">Acquisition</td><td colspan="2">Doppler $= \pm 5000$ Hz</td><td>Doppler $= \pm 3500$ Hz</td></tr>
<tr><td colspan="3">Coherent time $= 1$ ms, Incoherent number $= 10$, $P_{\mathrm{Fa}} = 10^{-3}$</td></tr>
<tr><td colspan="2">Tracking correlator</td><td colspan="3">Integration time $T_{\mathrm{i}} = 10$ ms</td></tr>
<tr><td rowspan="4">DLL</td><td rowspan="2">Discriminator</td><td>EMLP</td><td>EMLE</td><td>EMLP</td></tr>
<tr><td colspan="3">$c_{\tau} = 0.1$ chip</td></tr>
<tr><td>Low-pass filter</td><td colspan="3">1st order, $B_{\tau} = 1$ Hz</td></tr>
<tr><td>Loss indicator</td><td colspan="3">Duration: 1 s, Type: C/N_0, Threshold $\gamma_{\tau} = 25$ dB·Hz</td></tr>
<tr><td rowspan="4">PLL</td><td>Discriminator</td><td>Costas loop (unknown)</td><td colspan="2">Costas loop (atan)</td></tr>
<tr><td rowspan="2">Low-pass filter</td><td>$B_{\theta} = 20$ Hz</td><td>$B_{\theta} = 30$ Hz</td><td>$B_{\theta} = 20$ Hz</td></tr>
<tr><td colspan="3">3rd order</td></tr>
<tr><td>Loss indicator</td><td>Not used</td><td>NECT, Duration: 1 s,
Threshold $\gamma_{\theta} = 0.85$</td><td>Not used</td></tr>
<tr><td colspan="2" rowspan="2">C/N_0 estimation</td><td>Signal power/Noise power</td><td colspan="2">Type: MM</td></tr>
<tr><td colspan="3">Estimation period: 1 s</td></tr>
</table>

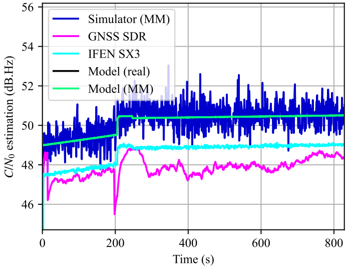
Nominal scenario



Code error

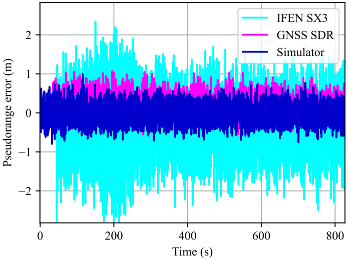


Frequency error

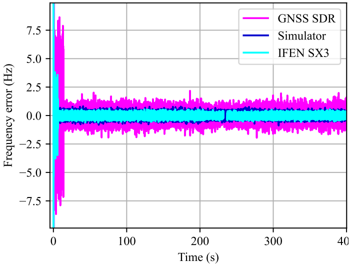


C/N_0

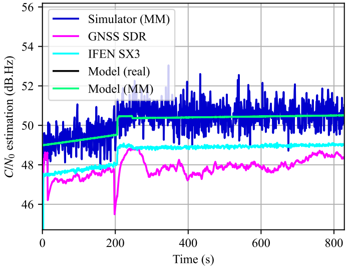
Nominal scenario



Code error



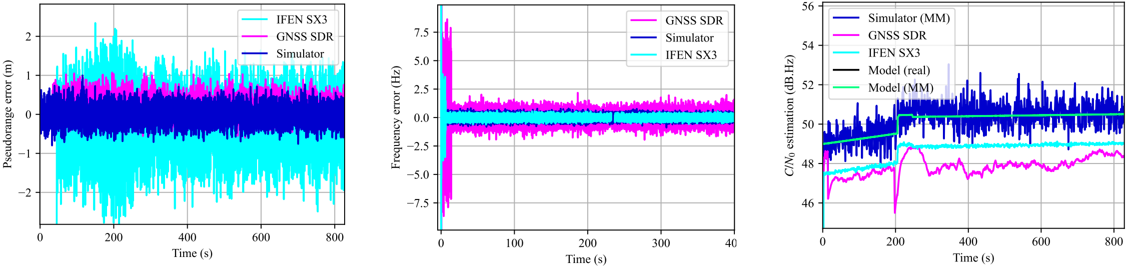
Frequency error



C/N_0

Experimental Errors:

Nominal scenario

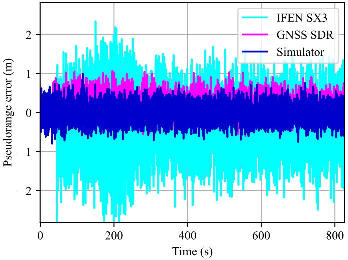


Code error Frequency error C/N_0

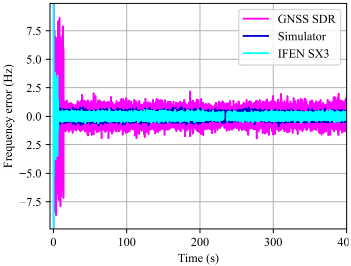
Experimental Errors:

- **Additional noise in the SX3 code tracking error** (possibly due to clock correction of the pseudorange).

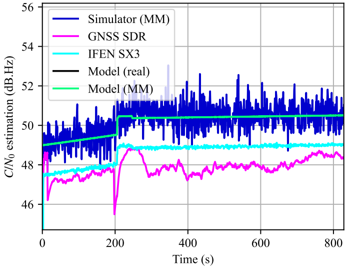
Nominal scenario



Code error



Frequency error

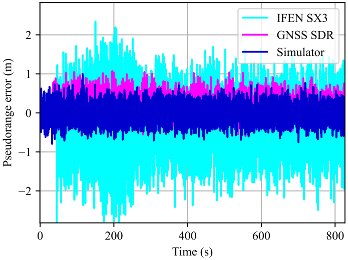


C/N_0

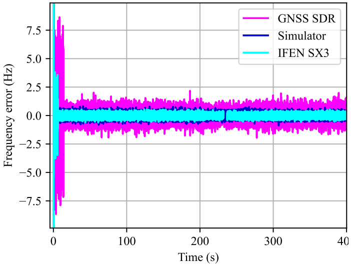
Experimental Errors:

- **Additional noise in the SX3 code tracking error** (possibly due to clock correction of the pseudorange).
- The SX3 and GNSS-SDR C/N_0 estimators **are biased** (constant bias but show the same trend as the expected C/N_0).

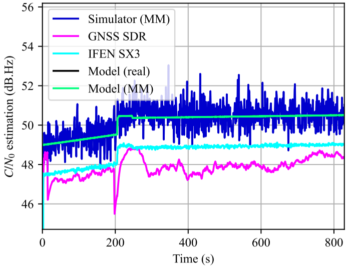
Nominal scenario



Code error



Frequency error

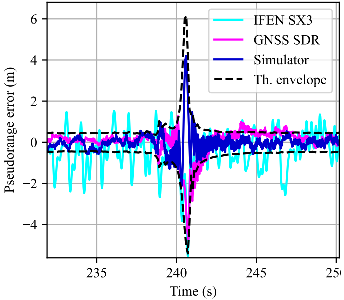


C/N_0

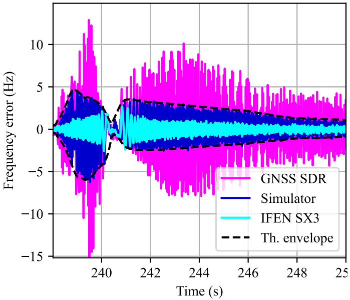
Experimental Errors:

- **Additional noise in the SX3 code tracking error** (possibly due to clock correction of the pseudorange).
- The SX3 and GNSS-SDR C/N_0 estimators **are biased** (constant bias but show the same trend as the expected C/N_0).
- The GNSS-SDR C/N_0 estimators **appear to be low-pass filtered**.

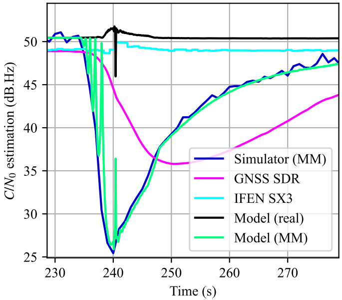
Low-power repeater scenario - Landing phase



Code error

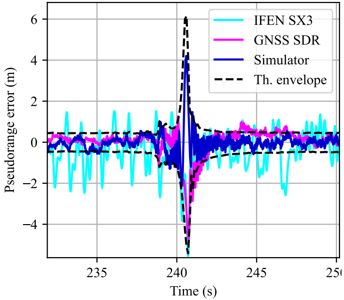


Frequency error

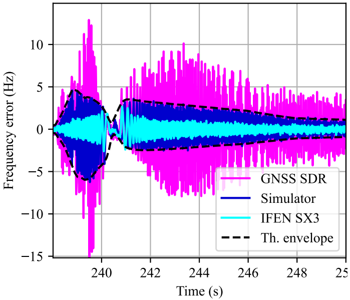


C/N_0

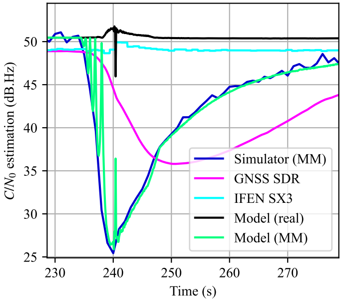
Low-power repeater scenario - Landing phase



Code error



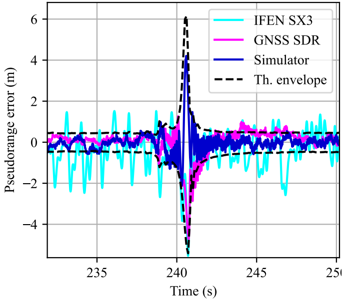
Frequency error



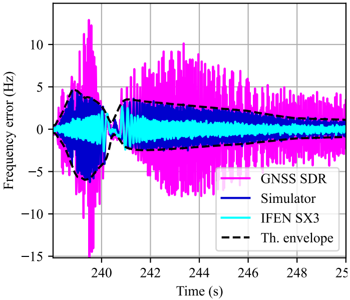
C/N_0

Observations:

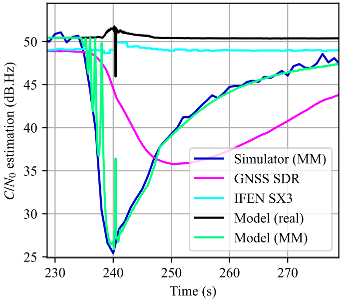
Low-power repeater scenario - Landing phase



Code error



Frequency error

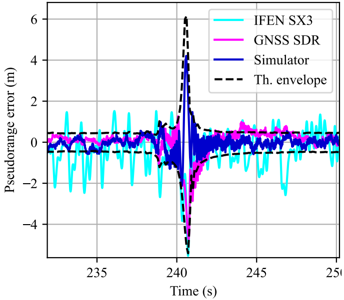


C/N_0

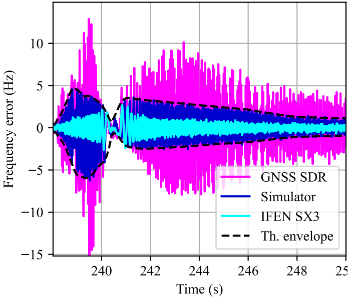
Observations:

- Tracking Errors: **oscillations** observed (dependence on the **receiver architecture**).

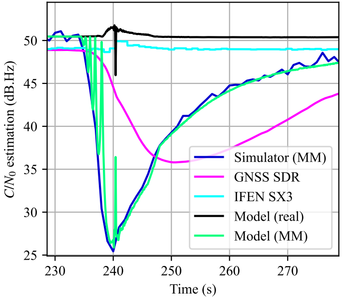
Low-power repeater scenario - Landing phase



Code error



Frequency error

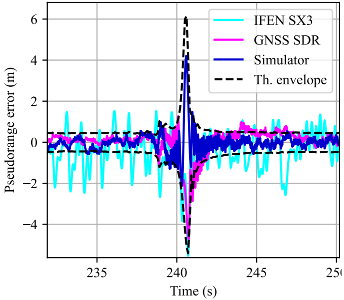


C/N_0

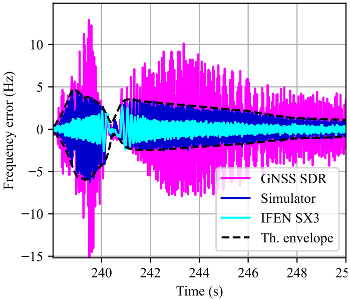
Observations:

- Tracking Errors: **oscillations** observed (dependence on the **receiver architecture**).
- C/N_0 Degradation: **Significant degradation** observed (strong **dependence** on the estimator method).

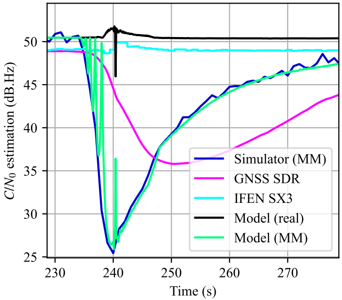
Low-power repeater scenario - Landing phase



Code error



Frequency error

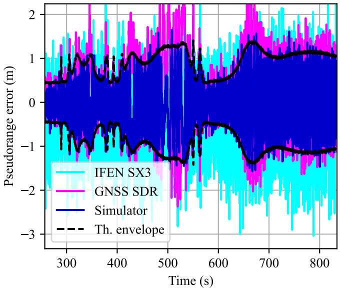


C/N_0

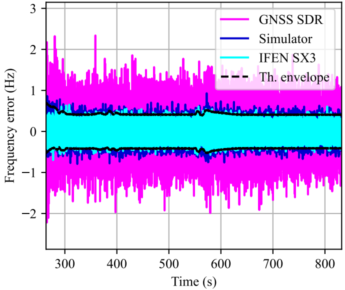
Observations:

- Tracking Errors: **oscillations** observed (dependence on the **receiver architecture**).
- C/N_0 Degradation: **Significant degradation** observed (strong **dependence** on the estimator method).
- The theoretical models **accurately predict receiver behavior under spoofing conditions**.

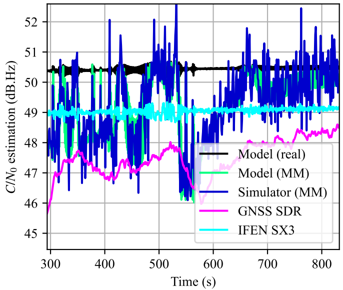
Low-power repeater scenario - Taxiing phase



Code error

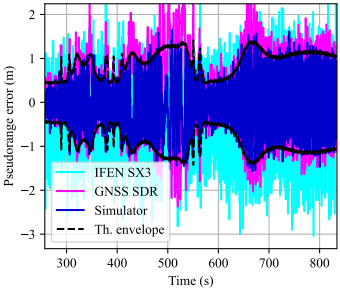


Frequency error

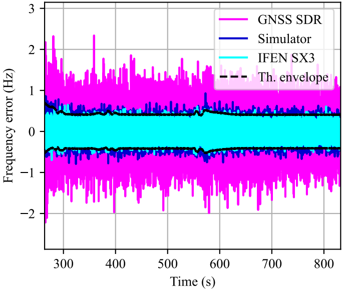


C/N_0

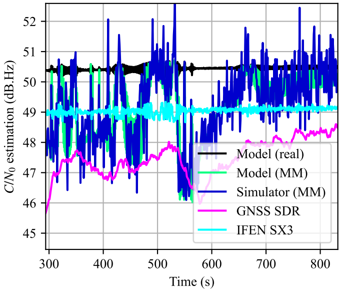
Low-power repeater scenario - Taxiing phase



Code error



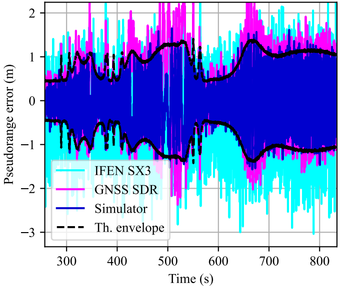
Frequency error



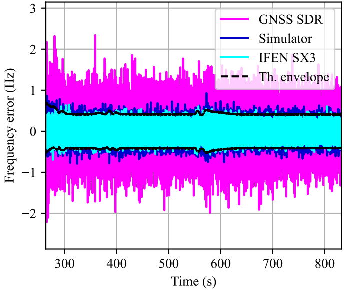
C/N_0

Observations:

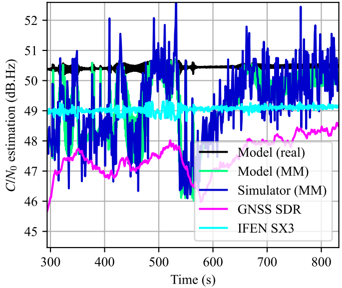
Low-power repeater scenario - Taxiing phase



Code error



Frequency error

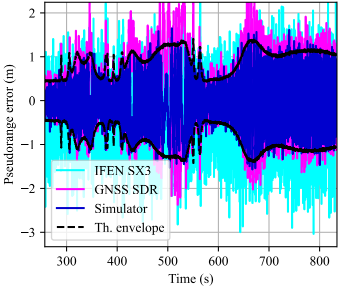


C/N_0

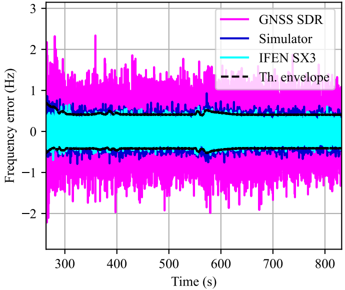
Observations:

- Low oscillations in tracking errors and C/N_0 degradation ranging from 0.5 to 2 dB (dependence on the **receiver architecture**).

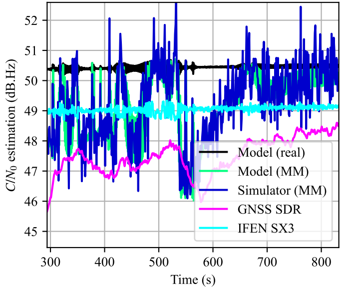
Low-power repeater scenario - Taxiing phase



Code error



Frequency error

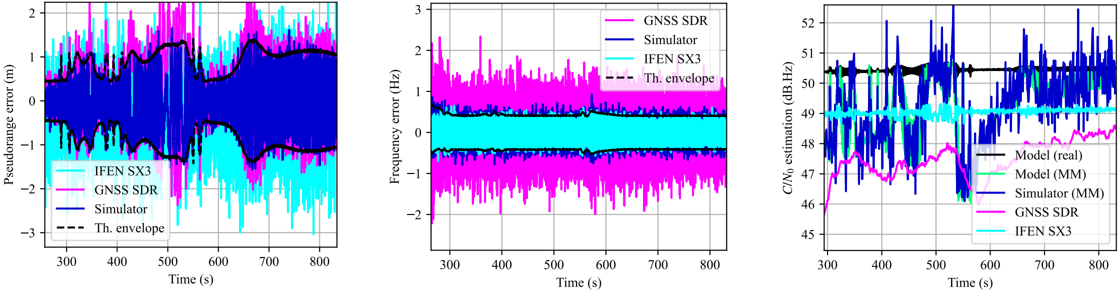


C/N_0

Observations:

- Low oscillations in tracking errors and C/N_0 degradation ranging from 0.5 to 2 dB (dependence on the **receiver architecture**).
- Observed distortion even at **very low spoofing received power**, $\Delta g < -20$ dB.

Low-power repeater scenario - Taxiing phase

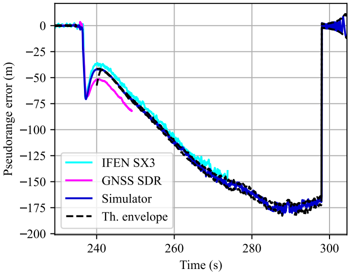


Code error | Frequency error | C/N_0

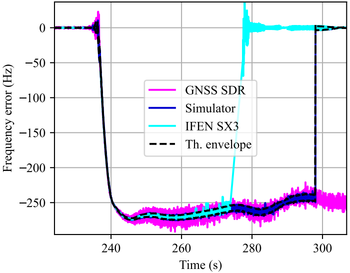
Observations:

- Low oscillations in tracking errors and C/N_0 degradation ranging from 0.5 to 2 dB (dependence on the **receiver architecture**).
- Observed distortion even at **very low spoofing received power**, $\Delta g < -20$ dB.
- The theoretical models **accurately predict receiver behavior under spoofing conditions**.

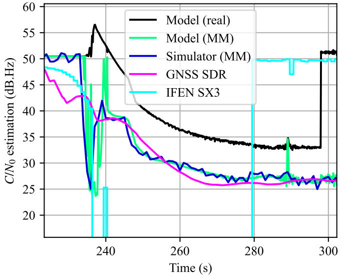
High-power repeater scenario - Landing phase



Code error



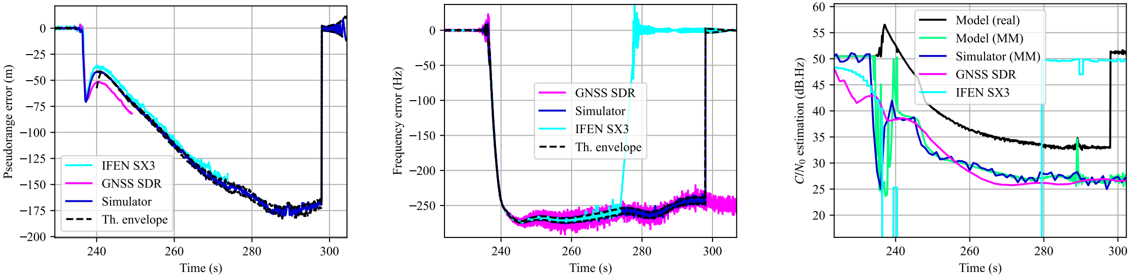
Frequency error



C/N_0

Observations:

High-power repeater scenario - Landing phase

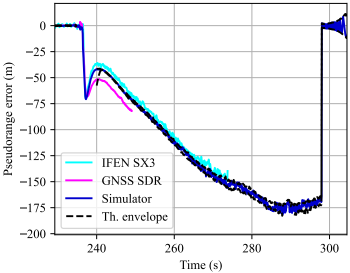


Code error | Frequency error | C/N_0

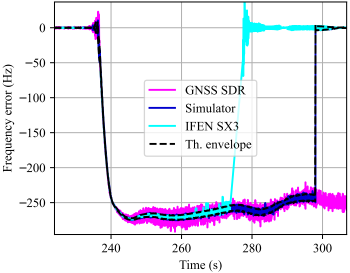
Observations:

- **Bifurcation** toward the 250 Hz-mismatched spoofing SE.

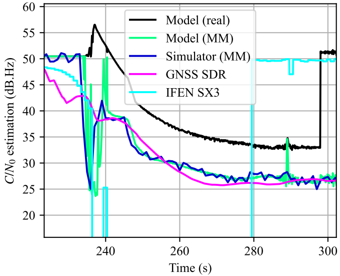
High-power repeater scenario - Landing phase



Code error



Frequency error



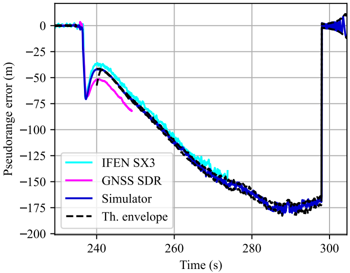
C/N_0

Observations:

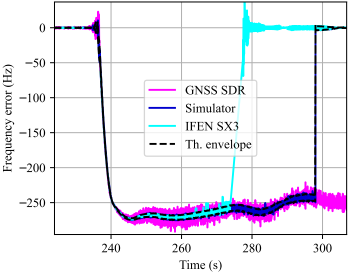
- **Bifurcation** toward the 250 Hz-mismatched spoofing SE.
- **Loss-of-lock** as the received spoofing power decreases, followed by **re-acquisition** on the authentic SE.

RÉPUBLIQUE FRANÇAISE Liberté Égalité Fraternité ENAC

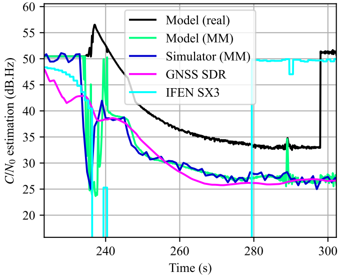
High-power repeater scenario - Landing phase



Code error



Frequency error

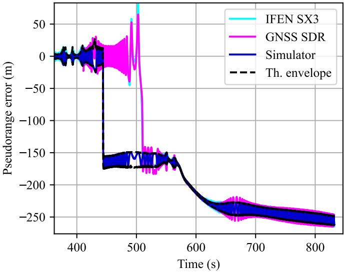


C/N_0

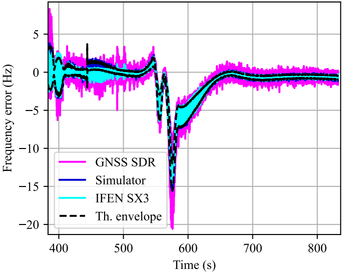
Observations:

- **Bifurcation** toward the 250 Hz-mismatched spoofing SE.
- **Loss-of-lock** as the received spoofing power decreases, followed by **re-acquisition** on the authentic SE.
- The model predicts the possible SE to which the system converges, as well as the C/N_0 behavior.

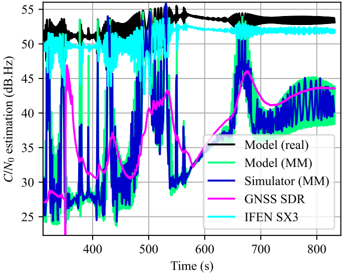
High-power repeater scenario - Taxiing phase



Code error



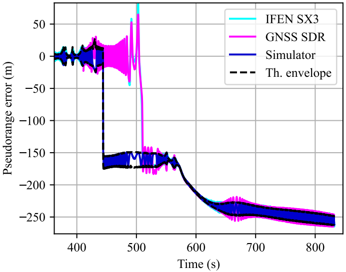
Frequency error



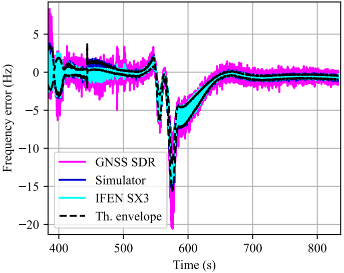
C/N_0

Observations:

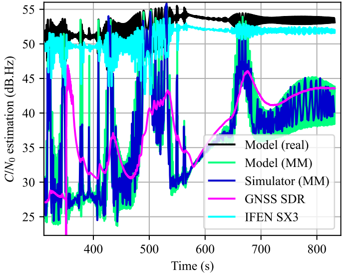
High-power repeater scenario - Taxiing phase



Code error



Frequency error



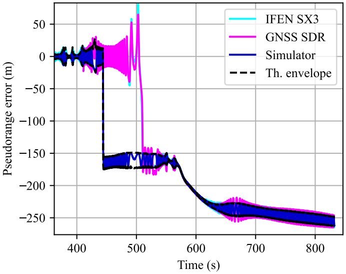
C/N_0

Observations:

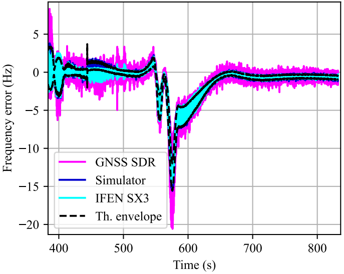
- Tracking errors: **Strong oscillations** and **bifurcation** toward the spoofing SE (**chaotic behavior** with high dependence on the receiver architecture and environment).

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

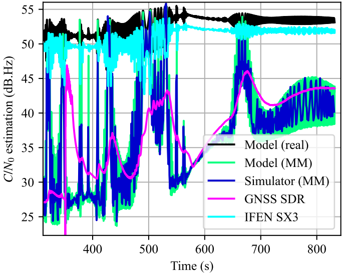
High-power repeater scenario - Taxiing phase



Code error



Frequency error

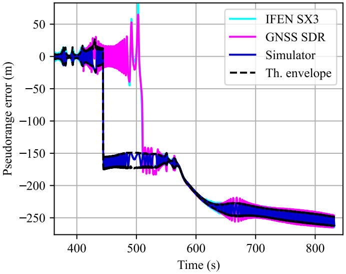


C/N_0

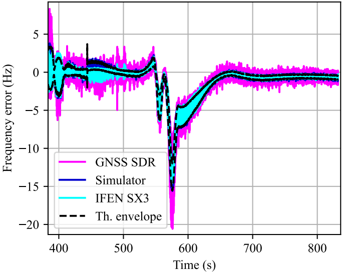
Observations:

- Tracking errors: **Strong oscillations** and **bifurcation** toward the spoofing SE (**chaotic behavior** with high dependence on the receiver architecture and environment).
- C/N_0 degradation: **Significant degradation** with method dependence and possible **loss-of-locks** (e.g., simulator at $t = 450$ s, followed by re-acquisition on the spoofing SE).

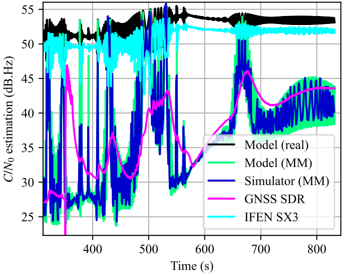
High-power repeater scenario - Taxiing phase



Code error



Frequency error



C/N_0

Observations:

- Tracking errors: **Strong oscillations** and **bifurcation** toward the spoofing SE (**chaotic behavior** with high dependence on the receiver architecture and environment).
- C/N_0 degradation: **Significant degradation** with method dependence and possible **loss-of-locks** (e.g., simulator at $t = 450$ s, followed by re-acquisition on the spoofing SE).
- The model accurately predicts the **possible SE** to which the system converges, as well as the C/N_0 behavior (and potential loss-of-locks).

Conclusion

Experiment observations

Conclusion

Experiment observations

⚠ The harmful distortion observed under induced-multipath situation, as exhibited in the theoretical models, **is also observed in realistic spoofing environments**.

Conclusion

Experiment observations

- ⚠ The harmful distortion observed under induced-multipath situation, as exhibited in the theoretical models, **is also observed in realistic spoofing environments**.
- ⚠ The experiments highlight the **strong chaotic behavior** of the GNSS receiver under such distortion, including tracking loop bifurcations, loss-of-lock, and a strong dependence on both the receiver architecture and the spoofing environment.

Conclusion

Experiment observations

- ⚠ The harmful distortion observed under induced-multipath situation, as exhibited in the theoretical models, **is also observed in realistic spoofing environments**.
- ⚠ The experiments highlight the **strong chaotic behavior** of the GNSS receiver under such distortion, including tracking loop bifurcations, loss-of-lock, and a strong dependence on both the receiver architecture and the spoofing environment.
- ✓ However, the models proposed in this thesis **provide accurate predictions** of the possible loop SE and C/N_0 degradation, **offering a means to understand and quantify the impact of spoofing**.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Outline

General Conclusions

Measure-Theory Framework

Introduction of a measure-theoretic framework for estimation under non-ergodic conditions:

General Conclusions

Measure-Theory Framework

Introduction of a measure-theoretic framework for estimation under non-ergodic conditions:

- Provide formal definitions for **signal power, independence, and expectation**.

General Conclusions

Measure-Theory Framework

Introduction of a measure-theoretic framework for estimation under non-ergodic conditions:

- Provide formal definitions for **signal power, independence, and expectation**.
- Derive properties related to **stationarity** and **ergodicity**.

General Conclusions

Measure-Theory Framework

Introduction of a measure-theoretic framework for estimation under non-ergodic conditions:

- Provide formal definitions for **signal power, independence, and expectation**.
- Derive properties related to **stationarity** and **ergodicity**.

Receiver Behavior Under Spoofing

Derivation of the theoretical model for the impact of spoofing before correlation (AGC, IF signal) and after correlation (Correlator outputs, tracking loops, and C/N_0):

General Conclusions

Measure-Theory Framework

Introduction of a measure-theoretic framework for estimation under non-ergodic conditions:

- Provide formal definitions for **signal power, independence, and expectation**.
- Derive properties related to **stationarity** and **ergodicity**.

Receiver Behavior Under Spoofing

Derivation of the theoretical model for the impact of spoofing before correlation (AGC, IF signal) and after correlation (Correlator outputs, tracking loops, and C/N_0):

- **Pre-Correlation:** Spoofing acts as a multiple **weighted CW jammer** for the AGC, starting to impact AGC values when $S/N > -5\,\text{dB}$.

General Conclusions

Measure-Theory Framework

Introduction of a measure-theoretic framework for estimation under non-ergodic conditions:

- Provide formal definitions for **signal power, independence, and expectation**.
- Derive properties related to **stationarity** and **ergodicity**.

Receiver Behavior Under Spoofing

Derivation of the theoretical model for the impact of spoofing before correlation (AGC, IF signal) and after correlation (Correlator outputs, tracking loops, and C/N_0):

- **Pre-Correlation:** Spoofing acts as a multiple **weighted CW jammer** for the AGC, starting to impact AGC values when $S/N > -5\,\text{dB}$.
- **Post-Correlation:** The impact of spoofing is categorized into four situations, including a harmful case where the receiver exhibits chaotic behavior, inducing **high tracking errors** and **significant C/N_0 degradation**, as well as, possible **tracking bifurcations** and **loss-of-locks**.

Thank You!

emile.ghizzo@alumni.enac.fr