Characterization of Meaconing and its Impact on GNSS Receivers

Maxandre Coulon, Alexandre Chabory, Axel Javier Garcia Peña, Jérémy Vezinet, Christophe Macabiau, Philippe Estival, Pierre Ladoux, Benoit Roturier

Characterization of meaconing and its impact on GNSS receivers

Maxandre Coulon, Alexandre Chabory, Axel Garcia-Pena, Jeremy Vezinet, Christophe Macabiau, *ENAC, Universite de Toulouse, France*
Philippe Estival, Pierre Ladoux, Benoit Roturier, *DGAC/DSNA, Direction Generale de l'Aviation Civile, France*

BIOGRAPHY

Maxandre Coulon received the M.Sc. degree in electrical engineering from the French Civil Aviation University, Toulouse, France, in 2018. He is currently preparing his Ph.D. degree in telecommunications within Institut National Polytechnique de Toulouse. His thesis title is "Characterization of the threats and reinforcement of Civil Aviation to GNSS meaconing".

Alexandre Chabory received the M.Sc. degree in electrical engineering from the French Civil Aviation University, Toulouse, France, in 2001, and the Ph.D. degree in electromagnetics from Paul Sabatier University, Toulouse, in 2004. Since 2007, he has been an Assistant Professor with the Electromagnetics and Antennas Research Group, Telecom Team, ENAC, Toulouse, where he has been the Head since 2012. His current research interests include electromagnetic theory and modeling, mainly for aeronautical applications.

Axel Garcia-Pena is a researcher/lecturer with the SIGnal processing and NAVigation (SIGNAV) research axis of the TELECOM research group of ENAC (French Civil Aviation University) lab, Toulouse, France. His research interests are GNSS navigation message demodulation, optimization and design, GNSS receiver design and GNSS satellite payload. He received his double engineer degree in 2006 in digital communications from SUPAERO and UPC, and his PhD in 2010 from the Department of Mathematics, Computer Science and Telecommunications of the INPT (Polytechnic National Institute of Toulouse), France.

Jeremy Vezinet holds a Ph.D. in multi-sensors hybridization. He is a Research Associate in the TELECOM team of ENAC in Toulouse (France) since 2014. He has been involved in several projects on multi-antenna GNSS receivers, GNSS/INS integration techniques and integrity monitoring. His research interests are GNSS, Inertial Navigation, Multi-sensor Hybridization, Integrity Monitoring and Video-Based Navigation.

Christophe Macabiau graduated as an electronics engineer in 1992 from the French Civil Aviation University, Toulouse, France. He received his Ph.D. in 1997. Since 1994 he has been working on the application of satellite navigation techniques to civil aviation and has been in charge of the signal processing lab of the ENAC since 2000. He is currently the head of the TELECOM team of ENAC, that includes research groups on signal processing and navigation, electromagnetics, and data communication networks.

Philippe Estival is a GNSS expert at the French civil aviation service provider (DGAC/DSNA/DTI) currently involved in EGNOS mission requirements and standardization activities on future multi-constellation GNSS receivers Eurocae WG62 and within EU/US cooperation agreement Working Group C. He has been in charge of CCF (EGNOS Central Control Facility) operational support and evolutions for PACF department until 2009 and then for ESSP SAS System Operation Unit up to 2015. He graduated in 2005 as an electronics engineer from French Civil Aviation University, Toulouse, France

Pierre Ladoux started his career as maintenance engineer on conventional radionavigation aids and then was involved at DSNA/DTI, the French Air Navigation Provider Technical Directorate, in activities related to satellite navigation systems and more specifically on the ICAO standardized Ground Based Augmentation System (GBAS). He is now the head of the Spectrum and Frequency management unit at DSNA.

Benoit Roturier graduated as a CNS systems engineer from French Civil Aviation University, Toulouse, France, in 1985 and obtained a PhD in Electronics from Institut National Polytechnique de Toulouse in 1995. He was in charge of operational implementation of civil aviation navigation systems at DGAC, then of research activities on CNS systems at ENAC. He is now head of GNSS Navigation programs at DGAC/DSNA and is involved in the development of civil aviation applications based on GPS/ABAS, EGNOS and Galileo.

DISCLAIMER

ABSTRACT

This article offers a new characterization of GNSS meaconing and its impact on GNSS receivers through mathematical models and simulations.

First, general mathematical models of the received signal at a receiver's correlators input and output in nominal conditions then in presence of a GNSS repeater are derivated. Then, the impact of a GNSS repeater is mathematically determined through simulations on a virtual GNSS receiver having various trajectories (static, pedestrian, car and airborne) for both realistic and degraded satellites and repeater configurations.

In this article, the received meaconing power, code delay and phase shift are computed with reason to the authentic signal's parameters. A 3D multipath error envelope is introduced to obtain maximal and minimal code delay estimation error according to multipath's delay and Doppler difference. A model of the new $\frac{C}{N_0}$ cause by the meaconer is also given in this article.

Simulations in nominal and degraded satellites configurations for various trajectories allow to emphasize the impact of the meaconer's Doppler difference on the pseudorange and positioning errors. The impact of meaconing also is also proven to greatly depends on the GNSS receiver's trajectory and velocity.

I. INTRODUCTION

Even though the use of GNSS navigation has experienced a major growth in the last years, indoor GNSS positioning remains still a challenge due to the physical propagation channel constraints: blockage of loss of Line-Of-Sight (LOS) signal and strong presence of multipath can result in a loss of GNSS positioning availability and/or a degradation of its performance. However, several solutions to overcome these propagation channel constraints and to allow indoor positioning have been developed, where most of them include re-radiated signals. One adopted solution is to use repeaters or meaconers: these devices are able to receive signals with an antenna outside a building and to re-radiate them with another antenna inside it. In this case, a user inside the building would estimate its position to be the repeater's reception antenna as all his estimated pseudo-ranges would be the same as the repeater's reception antenna's with an additional delay in the receiver clock.

However, the adoption of this solution to provide indoor GNSS positioning presents some risks. Indeed, since the building/space is never perfectly electromagnetically confined, re-radiated spurious signals can reach outdoor users such as pedestrians, cars or receiver with a possible significant impact on their position estimation. This type of situation is considered as a meaconing scenario where these outdoor users become the victims and the repeaters/meaconers signals are denoted as meaconing signals. The overall authentic and meaconing received signal is called spoofed received signal. Therefore, to accurately mathematically model the impact of these re-radiated GNSS signals on the signal processing stages and positioning performance of the outdoor receivers among authentic signals is of great interest.

Several efforts have been done on this modeling, especially on the signal processing part, resulting on a good characterization of the correlator outputs of a spoofed signal ([1], [2], [3], [4]). However, most of the time, the impact of spoofed signals has only been characterized while tracking the spoofing signal and the authentic signal is therefore not always considered. Moreover, the mathematical model of the received signal could benefit from the consideration of the antennas and propagation channel as their impact on the amplitude, code and phase delays can be important, especially when the direction of arrival of the repeated signal is different from that of the authentic signal.

The content of this paper is organized as follows. In Section II, general mathematical models of the received signal at a receiver's correlators input and output in nominal conditions then in presence of a GNSS repeater are derivated. In Section III, the impact of a GNSS repeater is mathematically determined through simulations on a virtual GNSS receiver ([5]) having various trajectories (static, pedestrian, car and airborne) for both realistic and degraded satellites and repeater configurations.

II. MATHEMATICAL MODEL OF A SPOOFED GNSS SIGNAL

1. General mathematical model of a received spoofed GNSS signal

For a specific GNSS signal (for instance GPS L1C/A or Galileo E5a), the received signal at the receiver's correlators input can be first modeled as

$$S_R = \sum_{i}^{I} S_{R_i} + \sum_{j}^{J} S_{R_j} + n_m + n \tag{1}$$

with

- S_{R_i} the received signal from the i^{th} satellite (or i^{th} received signal) among the I satellites in view;
- S_{R_j} the received re-radiated j^{th} satellite (or j^{th} received signal from the meaconer) among the J re-radiated received signals;
- n_m the additional noise resulting from the meaconer;
- n the White Gaussian noise.

2. GNSS signals fundamentals

To define the basic model of a GNSS satellite-to-receiver communication, the position vector of the receiver (more precisely its receiving antenna's reference point) will be denoted as $\boldsymbol{x} = (x, y, z)$ expressed in the ECEF coordinate system and its orientation angles vector $\boldsymbol{\alpha} = (\alpha, \beta, \gamma)$ also expressed in the ECEF coordinate system. Similarly, the position vector of the i^{th} received signal's satellite is $\boldsymbol{x_i} = (x_i, y_i, z_i)$ and its orientation vector $\boldsymbol{\alpha_i} = (\alpha_i, \beta_i, \gamma_i)$.

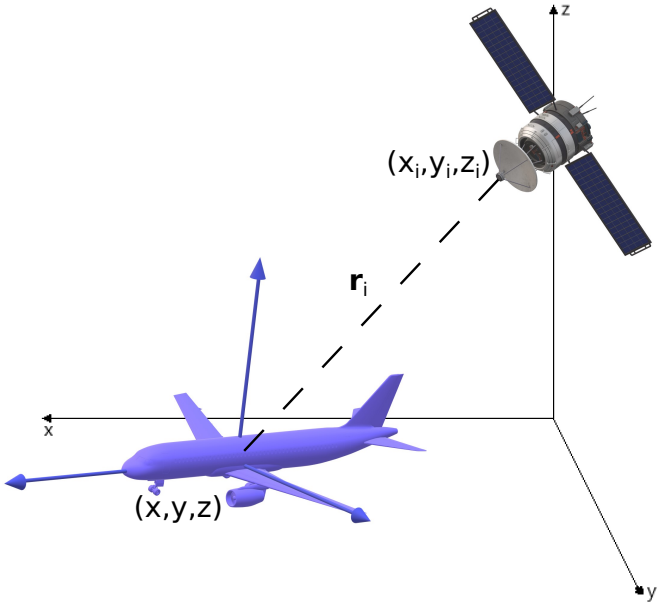


Figure 1: Coordinates and orientations of a receiver and a satellite

Introducing $\boldsymbol{r_i} = \boldsymbol{x_i} - \boldsymbol{x} = r_i \boldsymbol{u_{r_i}}$ the vector between the two antennas' reference points (ARP), with r_i the distance and $\boldsymbol{u_{r_i}}$ the vector between $\boldsymbol{x_i}$ and $\boldsymbol{x}$, the received signal from the i^{th} satellite without multipath depends on the distance between the two antennas and there orientations and can be expressed as ([6])

$$\begin{aligned} S_{R_i}(t, \boldsymbol{r_i}, \boldsymbol{\alpha_i}, \boldsymbol{\alpha}) = \sqrt{2P_{R_i}(\boldsymbol{r_i}, \boldsymbol{\alpha_i}, \boldsymbol{\alpha})} d_i(t - \tau_i(\boldsymbol{r_i}, \boldsymbol{\alpha_i}, \boldsymbol{\alpha})) c_{1,i}(t - \tau_i(\boldsymbol{r_i}, \boldsymbol{\alpha_i}, \boldsymbol{\alpha})) \\ c_{2,i}(t - \tau_i(\boldsymbol{r_i}, \boldsymbol{\alpha_i}, \boldsymbol{\alpha})) sc(t - \tau_i(\boldsymbol{r_i}, \boldsymbol{\alpha_i}, \boldsymbol{\alpha})) \cos(2\pi f_L t + \phi_i(t, \boldsymbol{r_i}, \boldsymbol{\alpha_i}, \boldsymbol{\alpha})), \end{aligned} \tag{2}$$

with

- P_{R_i} the power of the i^{th} received signal;
- d_i the navigation message of the i^{th} received signal;
- τ_i the time delay of the i^{th} received signal between the satellite and the receiver;
- c_i the PRN code of the i^{th} received signal;
- $c_{2,i}$ the secondary PRN code of the i^{th} received signal;
- sc the subcarrier;
- f_L the carrier frequency;
- ϕ_i the received phase of the i^{th} received signal.

When considering multipath, the mathematical model of the received signal becomes

$$S_{R_i}(t, \boldsymbol{X}) = \sum_{l=0}^{L-1} \Big(A_l(\boldsymbol{X}) \sqrt{2P_{R_i}(\boldsymbol{r_i}, \boldsymbol{\alpha_i}, \boldsymbol{\alpha})} d_i\big(t - \tau_i(t, \boldsymbol{r_i}, \boldsymbol{\alpha_i}, \boldsymbol{\alpha}) - \delta\tau_{il}(\boldsymbol{X})\big) c_i\big(t - \tau_i(t, \boldsymbol{r_i}, \boldsymbol{\alpha_i}, \boldsymbol{\alpha}) - \delta\tau_{il}(\boldsymbol{X})\big) \\ c_{2,i}\big(t - \tau_i(t, \boldsymbol{r_i}, \boldsymbol{\alpha_i}, \boldsymbol{\alpha}) - \delta\tau_{il}(\boldsymbol{X})\big) sc\big(t - \tau_i(t, \boldsymbol{r_i}, \boldsymbol{\alpha_i}, \boldsymbol{\alpha}) - \delta\tau_{il}(\boldsymbol{X})\big) \cos\big(2\pi f_L t + \phi_i(t, \boldsymbol{r_i}, \boldsymbol{\alpha_i}, \boldsymbol{\alpha}) + \delta\phi_{il}(\boldsymbol{X})\big) \Big), \tag{3}$$

where

- $\boldsymbol{X}$ is a simplified notation refering the global system's geometry, including coordinates and orientations of the satellite ($\boldsymbol{x_i}$, $\boldsymbol{\alpha_i}$), receiver ($\boldsymbol{x}$, $\boldsymbol{\alpha}$) and the multipath bouncing points;
- L is the number of paths including the LOS ($l = 0$);
- A_l is the relative amplitude attenuation induced by the l^{th} multipath with respect to the LOS transmission channel's amplitude in the highest gain's direction ($A_0 = 1$);
- $\delta\tau_{il}$ is the additional delay induced by the l^{th} multipath with respect to the LOS transmission channel's delay τ_i ($\delta\tau_{i0} = 0$s);
- $\delta\phi_{il}$ is the additional phase shift induced by the l^{th} multipath with respect to the LOS transmission channel's phase shift ϕ_i ($\delta\phi_{i0} = 0$).

a) Received power

For a non-spoofed signal, the power of the i^{th} received signal P_{R_i} at the correlator's input can be expressed within a given observation interval as ([7], [8])

$$P_{R_i}(\boldsymbol{r_i}, \boldsymbol{\alpha_i}, \boldsymbol{\alpha}) = L_{RF_R} G_R(\boldsymbol{u_{r_i}}, \boldsymbol{\alpha}) L_{fs_i}(r_i) L_{p_i}(\boldsymbol{u_{r_i}}, \boldsymbol{\alpha_i}, \boldsymbol{\alpha}) L_{\Gamma_i} L_{m_i}(\boldsymbol{r_i}) G_{T_i}(\boldsymbol{u_{r_i}}, \boldsymbol{\alpha_i}) P_{T_i} \tag{4}$$

with

- L_{RF_R} the losses due to the RF front-end gain;
- G_R the receiving antenna's gain;
- L_{fs_i} the free-space loss;
- L_{p_i} the polarization mismatch losses;
- L_{Γ_i} the losses due to antenna mismatch;
- L_{m_i} the miscellaneous losses including the ones from the ionosphere and troposphere;
- G_{T_i} the transmitting antenna's gain for the i^{th} signal;

- P_{T_i} the transmitted power of the i^{th} signal at the antenna's input.

We can express the losses as

$$L_{fs} = \left(\frac{\lambda}{4\pi r_i}\right)^2, \tag{5}$$

$$L_{p_i} = |\boldsymbol{p_R}.\boldsymbol{p_{T_i}}|^2, \tag{6}$$

with $\boldsymbol{p_R}$ and $\boldsymbol{p_{T_i}}$ the polarization vectors of the two antennas,

$$L_{\Gamma_i} = \left(1 - |\Gamma_R|^2\right)\left(1 - |\Gamma_{T_i}|^2\right), \tag{7}$$

where Γ_R and Γ_{T_i} are the reflection coefficients of the antennas.

As a result, the power of the i^{th} received signal P_{R_i} can be expressed as

$$P_{R_i}(\boldsymbol{r_i}, \boldsymbol{\alpha_i}, \boldsymbol{\alpha}) = L_{RF_R} G_R(\boldsymbol{u_{r_i}}, \boldsymbol{\alpha}) \left(\frac{\lambda}{4\pi r_i}\right)^2 |\boldsymbol{p_R}.\boldsymbol{p_{T_i}}|^2 \left(1 - |\Gamma_R|^2\right)\left(1 - |\Gamma_{T_i}|^2\right) L_{m_i}(\boldsymbol{r_i}) G_{T_i}(\boldsymbol{u_{r_i}}, \boldsymbol{\alpha_i}) P_{T_i}. \tag{8}$$

b) Code delay

For a satellite-to-receiver propagation, the code delay depends on the propagation delay and the delay induced by the antennas. It can be expressed as

$$\tau_i(\boldsymbol{X}) = \tau_{T_{RF,i}} + \tau_{T_i}(\boldsymbol{u_{r_i}}, \boldsymbol{\alpha_i}) + \tau_{r_i}(\boldsymbol{x_i}, \boldsymbol{x}) + \tau_R(\boldsymbol{u_{r_i}}, \boldsymbol{\alpha}) + \tau_{R_{RF}}, \tag{9}$$

with

- $\tau_{T_{RF,i}}$ the delay induced by the RF components of the i^{th} satellite;
- τ_{T_i} the delay induced by the transmitting antenna of the i^{th} satellite;
- τ_{r_i} the propagation delay between $\boldsymbol{x_i}$ and $\boldsymbol{x}$;
- τ_R the delay induced by the receiving antenna of the receiver;
- $\tau_{R_{RF}}$ the delay induced by the RF front-end;

The propagation delay can be modeled as

$$\tau_{r_i}(\boldsymbol{x_i}, \boldsymbol{x}) = \frac{1}{c}\Big(r_i + d_I^i(\boldsymbol{x_i}, \boldsymbol{x}) + d_T^i(\boldsymbol{x_i}, \boldsymbol{x})\Big), \tag{10}$$

with

- d_I^i the ionospheric excess delay ($\simeq \frac{STEC}{f^2}$ where $STEC$ is Slant Total Electron Content $i.e.$ the integrated electron density along the slant path)
- d_T^i the tropospheric excess delay.

c) Phase delay

Similarly to the code delay, for a satellite-to-receiver propagation, the phase shift depends on the propagation delay and the delay induced by the antennas. It can be expressed as

$$\phi_i(\boldsymbol{X}) = \phi_{T_{RF,i}} + \phi_{T_i}(\boldsymbol{u_{r_i}}, \boldsymbol{\alpha_i}) + \phi_{r_i}(\boldsymbol{x_i}, \boldsymbol{x}) + \phi_R(\boldsymbol{u_{r_i}}, \boldsymbol{\alpha}) + \phi_{R_{RF}} + \phi_n, \tag{11}$$

with

- $\phi_{T_{RF,i}}$ the phase shift induced by the RF components of the i^{th} satellite;
- ϕ_{T_i} the phase shift induced by the transmitting antenna of the i^{th} satellite;
- ϕ_{r_i} the propagation phase shift between $\boldsymbol{x_i}$ and $\boldsymbol{x}$;
- ϕ_R the phase shift induced by the receiving antenna of the receiver;
- $\phi_{R_{RF}}$ the phase shift induced by the RF front-end;
- ϕ_n the phase's noise, including the ionospheric scintillation's phase shift.

The propagation phase shift can be modeled as

$$\phi_{r_i}(\boldsymbol{x_i}, \boldsymbol{x}) = \frac{2\pi}{\lambda}\Big(r_i + d_I^i(\boldsymbol{x_i}, \boldsymbol{x}) + d_T^i(\boldsymbol{x_i}, \boldsymbol{x})\Big), \tag{12}$$

with

- λ is the signal's wavelength;
- d_I^i the ionospheric delay;
- d_T^i the tropospheric delay.

3. Mathematical model of a received meaconing signal

In this mathematical model, the meaconer is receiving a GNSS signal from the satellite (in blue in Figure 2) and re-radiates the signal to an indoor GNSS receiver and possibly to other receivers on the outside (in red in Figure 2).

The j^{th} satellite position and orientation angle vectors are denoted $\boldsymbol{x_j}$ and $\boldsymbol{\alpha_j}$ in the ECEF reference system, the meaconer's receiving and transmitting antenna position and orientation angles vectors are respectively $\boldsymbol{x_R}$, $\boldsymbol{\alpha_R}$, $\boldsymbol{x_T}$ and $\boldsymbol{\alpha_T}$ and the receiver's position and orientation angles vectors are still denote $\boldsymbol{x}$ and $\boldsymbol{\alpha}$.

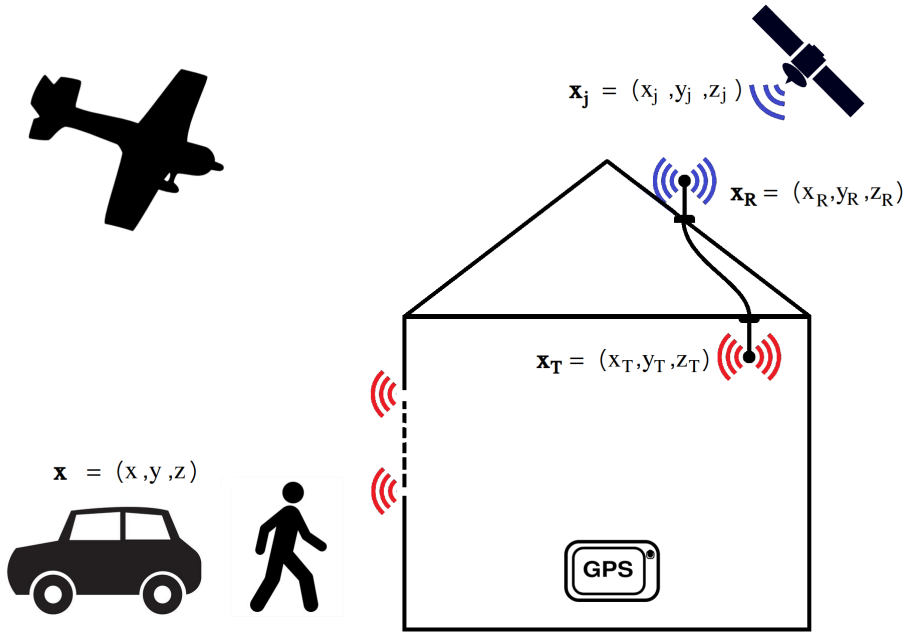


Figure 2: Considered meaconing geometry

By analogy to the satellite-to-receiver's section and by using the notations used in the previous sections, we can express the j^{th} received signal from the meaconer without multipath as

$$S_{R_j}(t, \boldsymbol{X_m}) = \sqrt{2P_{R_j}(\boldsymbol{X_m})} d_j(t - \tau_j(t, \boldsymbol{X_m})) c_j(t - \tau_j(t, \boldsymbol{X_m})) c_{2,j}(t - \tau_j(t, \boldsymbol{X_m})) sc(t - \tau_j(t, \boldsymbol{X_m})) \cos(2\pi f_L t + \phi_j(t, \boldsymbol{X})), \tag{13}$$

with

- $\boldsymbol{X_m}$ a term which refers the global system's geometry, including the meaconer's position and orientation;
- P_{R_j} the power of the j^{th} received signal from the meaconer at the receiver's correlator input;
- d_j the navigation message of the j^{th} received signal transmitted by the meaconer;
- τ_j the time delay of the j^{th} received signal between the satellite and the receiver induced by the meaconer;
- c_j the PRN code of the j^{th} received signal transmitted by the meaconer;
- $c_{2,j}$ the secondary PRN code of the j^{th} received signal transmitted by the meaconer;
- sc the subcarrier;
- f_L the carrier frequency;
- ϕ_j the received phase of the j^{th} received signal induced by the meaconer.

When considering multipath, the received meaconing signal becomes

$$\begin{aligned} S_{R_j}(t, \boldsymbol{X_m}) = \sum_{l_1=0}^{L_1-1} \sum_{l_2=0}^{L_2-1} & A_{l_1}^{sm}(\boldsymbol{X_m}) A_{l_2}^{mr}(\boldsymbol{X_m}) \sqrt{2P_{R_j}(\boldsymbol{X_m})} d_j\big(t - \tau_j(t, \boldsymbol{X_m}) - \delta\tau_{jl_1}^{sm}(\boldsymbol{X_m}) - \delta\tau_{jl_2}^{mr}(\boldsymbol{X_m})\big) \\ & c_j\big(t - \tau_j(t, \boldsymbol{X_m}) - \delta\tau_{jl_1}^{sm}(\boldsymbol{X_m}) - \delta\tau_{jl_2}^{mr}(\boldsymbol{X_m})\big) c_{2,j}\big(t - \tau_j(t, \boldsymbol{X_m}) - \delta\tau_{jl_1}^{sm}(\boldsymbol{X_m}) - \delta\tau_{jl_2}^{mr}(\boldsymbol{X_m})\big) \\ & sc\big(t - \tau_j(t, \boldsymbol{X_m}) - \delta\tau_{jl_1}^{sm}(\boldsymbol{X_m}) - \delta\tau_{jl_2}^{mr}(\boldsymbol{X_m})\big) \cos\big(2\pi f_L t + \phi_j(t, \boldsymbol{X_m}) - \delta\phi_{jl_1}^{sm}(\boldsymbol{X_m}) - \delta\phi_{jl_2}^{mr}(\boldsymbol{X_m})\big), \end{aligned} \tag{14}$$

where

- L_1 is the number of paths between the satellite and the meaconer including the LOS ($l_1 = 0$);
- L_2 is the number of paths between the meaconer and the receiver including the LOS ($l_2 = 0$);
- $A_{l_1}^{sm}$ is the amplitude attenuation induced by the l_1^{th} multipath with respect to the LOS transmission channel's power between the satellite and the meaconer and similarly $A_{l_2}^{mr}$ between the meaconer and the receiver;
- $\delta\tau_{jl_1}^{sm}$ is the additional delay induced by the l_1^{th} multipath with respect to the LOS transmission channel's delay between the satellite and the meaconer and similarly $\delta\tau_{jl_2}^{mr}$ between the meaconer and the receiver;
- $\delta\phi_{jl_1}^{sm}$ is the additional phase shift induced by the l_1^{th} multipath with respect to the LOS transmission channel's phase shift between the satellite and the meaconer and similarly $\delta\phi_{jl_2}^{mr}$ between the meaconer and the receiver.

a) Identification of alterable variables

When ignoring additional multipath, some variables within (13) can be altered when the signal is re-radiated by a meaconer.

- P_{R_j} is altered by the propagation range and can be modified by changing the meaconer's gain;
- τ_j also depends on the propagation distance and an additional set delay can be added by the meaconer;
- ϕ_j can also be modified by the meaconer in addition to its propagation distance dependence.

b) Received power of a meaconing signal

By analogy to (8), we can deduce the expression of the power of the j^{th} received signal P_{R_j} at the receiver's correlator input within a given observation interval as

$$P_{R_j} = L_{RF_R} G_R(\boldsymbol{u_{r_T}}, \boldsymbol{\alpha}) \Big(\frac{\lambda}{4\pi r_T}\Big)^2 |\boldsymbol{p_R}.\boldsymbol{p_{T_T}}|^2 \big(1 - |\Gamma_R|^2\big)\big(1 - |\Gamma_{T_T}|^2\big) L_{m_i}(\boldsymbol{r_T}) G_{T_T}(\boldsymbol{u_{r_T}}, \boldsymbol{\alpha_T}) P_{T_T}, \tag{15}$$

where

- $\boldsymbol{u_{r_T}}$ is the unit vector between the meaconer's transmitting antenna and the receiver;
- $\boldsymbol{p_{T_T}}$ is the polarization vector of the meaconer's transmitting antenna;
- Γ_{T_T} is the reflection coefficient of the meaconer's transmitting antenna;
- G_{T_T} is the gain of the meaconer's transmitting antenna;
- P_{T_T} is the transmitted power of the meaconer at its antenna's output.

For a meaconer, it is possible to deduce, by analogy to (8), the expression of the received power $P_{R_{s_j}}$ of the j^{th} signal at the meaconer's antenna input within a given observation interval as

$$P_{R_{s_j}} = G_{R_R}(\boldsymbol{u_{r_{jR}}}, \boldsymbol{\alpha_R}) \Big(\frac{\lambda}{4\pi r_{jR}}\Big)^2 |\boldsymbol{p_{R_R}}.\boldsymbol{p_{T_j}}|^2 \big(1 - |\Gamma_{R_R}|^2\big)\big(1 - |\Gamma_{T_j}|^2\big) L_{m_i}(\boldsymbol{r_{jR}}) G_{T_j}(\boldsymbol{u_{r_{jR}}}, \boldsymbol{\alpha_j}) P_{T_j}. \tag{16}$$

where

- $\boldsymbol{u_{r_{j_R}}}$ is the unit vector between the j^{th} satellite and the meaconer's receiving antenna;
- $\boldsymbol{p_{R_R}}$ is the polarization vector of the meaconer's receiving antenna;
- Γ_{R_R} is the reflection coefficient of the meaconer's receiving antenna;
- G_{R_R} is the gain of the meaconer's receiving antenna.

We can therefore express the power of the j^{th} received signal from the meaconer P_{R_j} as a fonction of the j^{th} transmitted signal's power P_{T_j} :

$$\begin{aligned} P_{R_j} = {} & L_{RF_R} G_R(\boldsymbol{u_{r_T}}, \boldsymbol{\alpha}) \Big(\frac{\lambda}{4\pi r_T}\Big)^2 |\boldsymbol{p_R}.\boldsymbol{p_{T_T}}|^2 \big(1 - |\Gamma_R|^2\big)\big(1 - |\Gamma_{T_T}|^2\big) L_{m_i}(\boldsymbol{r_T}) G_{T_T}(\boldsymbol{u_{r_T}}, \boldsymbol{\alpha_T}) G_{s_j} \\ & G_{R_R}(\boldsymbol{u_{r_{jR}}}, \boldsymbol{\alpha_R}) \Big(\frac{\lambda}{4\pi r_{jR}}\Big)^2 |\boldsymbol{p_{R_R}}.\boldsymbol{p_{T_j}}|^2 \big(1 - |\Gamma_{R_R}|^2\big)\big(1 - |\Gamma_{T_j}|^2\big) L_{m_i}(\boldsymbol{r_{jR}}) G_{T_j}(\boldsymbol{u_{r_{jR}}}, \boldsymbol{\alpha_j}) P_{T_j}, \end{aligned} \tag{17}$$

with

$$G_{s_j} = \frac{P_{T_T}}{P_{R_R}} \tag{18}$$

the internal meaconer's gain.

It should be noted that while the spurious received signal is not necessarily tracked by the receiver, its re-radiated noise is added to the already existing one. The resulting $\frac{C}{N_0}$ observed by the receiver is

$$\frac{C}{N_0} = \frac{C_{tracked}}{N_{0_{authentic}} + N_{0_{re-radiated}}} \simeq \frac{C_{tracked}}{N_{0_{authentic}}(1 + FSPL * G_{s_j})} \tag{19}$$

where $FSPL$ are the linear Free Space Path Losses between the meaconer's transmitting antenna and the receiver.

c) Code delay of a meaconing signal

We can deduce from (9) that the code delay of a meaconing signal will be

$$\tau_j(\boldsymbol{X}) = \tau_{s_j} + \tau_{r_T}(\boldsymbol{x}, \boldsymbol{x_T}) + \tau_R(\boldsymbol{u_{r_T}}, \boldsymbol{\alpha}) + \tau_{R_{RF}}, \tag{20}$$

with

- τ_{s_j} the time delay between the GPS time and the j^{th} signal at the meaconer's antenna output;
- τ_{r_T} the propagation delay between $\boldsymbol{x_T}$ and $\boldsymbol{x}$;
- τ_R the delay induced by the receiving antenna of the receiver;
- $\tau_{R_{RF}}$ the delay induced by the RF front-end.

For a meaconing signal, the signal is transmitted from a satellite to a meaconer and then from a meaconer to a receiver. We can deduce from (20) that the time delay between the GPS time and the j^{th} signal at the meaconer's antenna output is

$$\tau_{s_j} = \tau_{T_{j_{RF}}} + \tau_{T_j}(\boldsymbol{u_{r_{jR}}}, \boldsymbol{\alpha_j}) + \tau_{r_{jR}}(\boldsymbol{x_j}, \boldsymbol{x_R}) + \tau_{R_R}(\boldsymbol{u_{r_{jR}}}, \boldsymbol{\alpha_{s_R}}) + \tau_{R_{s_{RF}}} + \tau_{sp_{s_j}} + \tau_{T_{s_{RF}}} + \tau_{T_T}(\boldsymbol{u_{r_T}}, \boldsymbol{\alpha_T}), \tag{21}$$

with

- $\tau_{T_{j_{RF}}}$ the delay induced by the RF components of the j^{th} satellite;
- τ_{T_j} the delay induced by the transmitting antenna of the j^{th} satellite;
- $\tau_{r_{jR}}$ the propagation delay between $\boldsymbol{x_j}$ and $\boldsymbol{x_R}$;
- τ_{R_R} the delay induced by the receiving antenna of the meaconer;
- $\tau_{R_{s_{RF}}}$ the delay induced by the RF components of the meaconer's input;
- $\tau_{sp_{s_j}}$ the signal processing delay of the meaconer for the j^{th} signal;
- $\tau_{T_{s_{RF}}}$ the delay induced by the RF components of the meaconer's output;
- τ_{T_s} the delay induced by the transmitting antenna of the meaconer.

d) Phase delay of a meaconing signal

We can deduce from (11) that the phase shift of a meaconing signal will be

$$\phi_j(\boldsymbol{X}) = \phi_{s_j} + \phi_{r_T}(\boldsymbol{x}, \boldsymbol{x_s}) + \phi_R(\boldsymbol{u_{r_T}}, \boldsymbol{\alpha}) + \phi_{R_{RF}}, \tag{22}$$

with

- ϕ_{s_j} the phase shift between the GPS time and the j^{th} signal at the meaconer's antenna output;
- ϕ_{r_T} the propagation phase shift between $\boldsymbol{x_T}$ and $\boldsymbol{x}$;
- ϕ_R the phase shift induced by the receiving antenna of the receiver;
- $\phi_{R_{RF}}$ the phase shift induced by the RF components of the receiver.

For a meaconing signal, the signal is transmitted from a satellite to a meaconer and then from a meaconer to a receiver. We can deduce from (22) that the phase shift between the satellite and the j^{th} signal at the meaconer's antenna output is

$$\begin{aligned}\phi_{s_j} = \phi_{T_{j_{RF}}} + \phi_{T_j}(\boldsymbol{u_{r_{jR}}}, \boldsymbol{\alpha_j}) + \phi_{r_{jR}}(\boldsymbol{x_j}, \boldsymbol{x_R}) + \phi_{R_R}(\boldsymbol{u_{r_{jR}}}, \boldsymbol{\alpha_{s_R}}) \\ + \phi_{R_{s_{RF}}} + \phi_{sp_{s_j}} + \phi_{add_{s_j}} + \phi_{T_{s_{RF}}} + \phi_{T_T}(\boldsymbol{u_{r_T}}, \boldsymbol{\alpha_T}) + \phi_n,\end{aligned} \tag{23}$$

with

- $\phi_{T_{j_{RF}}}$ the phase shift induced by the RF components of the j^{th} satellite;
- ϕ_{T_j} the phase shift induced by the transmitting antenna of the j^{th} satellite;
- $\phi_{r_{jR}}$ the propagation phase shift between $\boldsymbol{x_j}$ and $\boldsymbol{x_R}$;
- ϕ_{R_R} the phase shift induced by the receiving antenna of the meaconer;
- $\phi_{R_{s_{RF}}}$ the phase shift induced by the RF components of the meaconer's input;
- $\phi_{sp_{s_j}}$ the signal processing phase shift of the meaconer for the j^{th} signal;
- $\phi_{add_{s_j}}$ the additional phase shift induced by the meaconer for the j^{th} signal;
- $\phi_{T_{s_{RF}}}$ the phase shift induced by the RF components of the meaconer's output;
- ϕ_{T_s} the phase shift induced by the transmitting antenna of the meaconer.

4. Impact of a meaconer on a receiver's correlator outputs

As seen previously, a meaconer re-radiates a GNSS signal with a different amplitude, code delay and phase shift, similarly to multipath. As the satellites are in movement, there may be a Doppler difference between the authentic received signal (LOS) and the re-radiated received signal (NLOS). As an example, the late in-phase correlator output I_L would be

$$\begin{aligned} I_L(k) = &\frac{A_0}{2} d(q) \text{sinc}\big(\pi \epsilon_{f_{LOS}}(k) T_i\big) Rc\big(\epsilon_{\tau_{LOS}}(k) + \frac{C_s}{2}\big) \cos\big(\epsilon_{\theta_{LOS}}(k) + \pi T_i \epsilon_{f_{LOS}}(k)\big) + n_I(q) \\ &+ \frac{A_1}{2} d(q) \text{sinc}\big(\pi T_i \epsilon_{f_{NLOS}}(k)\big) Rc\big(\epsilon_{\tau_{NLOS}}(k) + \frac{C_s}{2}\big) \cos\big(\epsilon_{\theta_{NLOS}}(k) + \pi T_i \epsilon_{f_{NLOS}}(k)\big), \end{aligned} \tag{24}$$

where C_s is the chip spacing, T_I is the integration time, ϵ_τ is the code delay estimation error, ϵ_θ is the phase estimation error at the beginning of the interval and ϵ_f is the frequency estimation error.

It should be noted that the difference in the code delay estimation errors is the same as the delay between the authentic signal and the repeated one, as stated in the following equation,

$$\epsilon_{\tau_{LOS}} - \epsilon_{\tau_{NLOS}} = \tau_{LOS} - \tau_{NLOS} = \Delta\tau \tag{25}$$

and the same equations can be observed for the phase shift and Doppler difference with $\Delta\tau$ the code delay difference between the authentic signal and the multipath one, $\Delta\theta$ the phase difference between the authentic signal and the multipath one and Δf the frequency difference between the authentic signal and the multipath one.

When observing the code delay estimation error for the authentic signal $\epsilon_{\tau_{LOS}}$ through the output of the tracking loop, a multipath (or spoofed) error envelope can be drawn as a function of $\Delta\tau$, $\Delta\theta$ and Δf. For instance, for GPS L1C/A, with a BPSK modulation, a chip spacing $C_s = \frac{T_c}{2}$ of half a chip, a RF bandwidth B_{RF} of 40MHz, an integration time T_i of 20ms, a multipath amplitude ratio $\alpha = \frac{A_1}{A_0}$ equal to 0.5 and for a Early-Minus-Late Power (EMLP) discriminator, the 3D multipath error envelope is given in Figure 3.

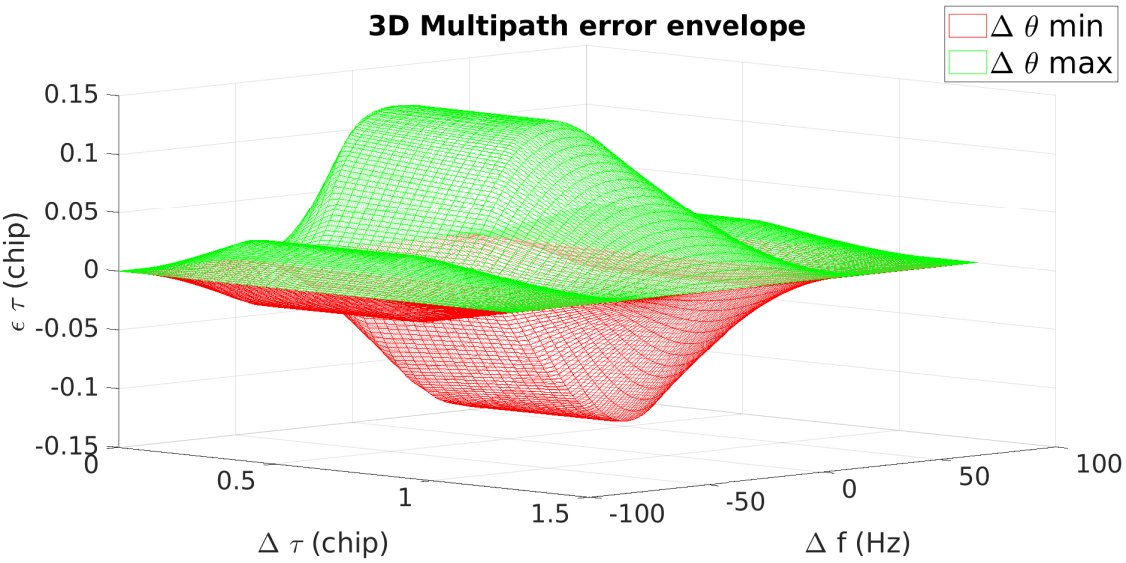


Figure 3: 3D multipath error envelope

In this Figure, the code delay estimation error for the authentic signal $\epsilon_{\tau_{LOS}}$ for a specific $\Delta\tau$ and Δf is bounded between two values even though the phase shift Δf is evolving through time. The 2D error envelope ($\epsilon_{\tau_{LOS}}$,$\Delta\tau$) is a known figure but the study on meaconing also requires to consider the third dimension Δf which modulates the error envelope with a sinc function with zeros on $\Delta f = \frac{1}{T_i}$.

III. APPLICATIONS

In this section, the mathematical model of the received repeated signal will be injected into ENAC's simulated receiver GeneIQ ([5]). The outputs will be compared to theory and will be computed for several scenarios and configurations to match the various cases a GNSS receiver can be used for.

1. Presentation of GeneIQ

GeneIQ is an ENAC's software developped in the 2000's to emulate GNSS receivers' $I\&Q$ correlator outputs. The fundamental principle of GeneIQ is to emulate the correlator outputs of a virtual GNSS receiver by using associated mathematical formulas for base-band processing and RF processing and without considering the authentic signal. From those correlator outputs, almost all the receiver's functions, such as tracking and positioning, are emulated. GeneIQ does not emulate the signal's acquisition yet. For the moment, the acquisition is considered already done on the signal with the highest power when the signal is in visibility and the acquisition is supposed to be perfect (the first estimated values are the real values). The tracking is considered lost when the estimated $\frac{C}{N_0}$ drops below 20dB or if the mean value of $\frac{I_P^2-Q_P^2}{I_P^2+Q_P^2}$ drops below 0.4. In this case, a reacquisition is tried 1s later if both thresholds are met again.

In the current version of GeneIQ, it is possible to configure the receiver by modifying the signal processing parameters for each of GPS and Galileo's bandwidths, to set a trajectory as well as attitude data, inertial data, antennas radiation pattern for the receiver. The satellites constellations are directly located from almanacs and dates. The software is able to run a simulation epoch by epoch by computing the position of the user and the satellites, testing the visibility, then computing the true pseudo-ranges, the link budget and $\frac{C}{N_0}$ for both authentic and spurious signal. The correlator outputs are calculated, then the phase and code delay to finally get the pseudo-ranges estimated by the receiver. GeneIQ also computes the navigation solution using Least Square Method or a Kalman Filter hybridized with or without inertial data. The overall strucutre of GeneIQ is summarized in Figure 4.

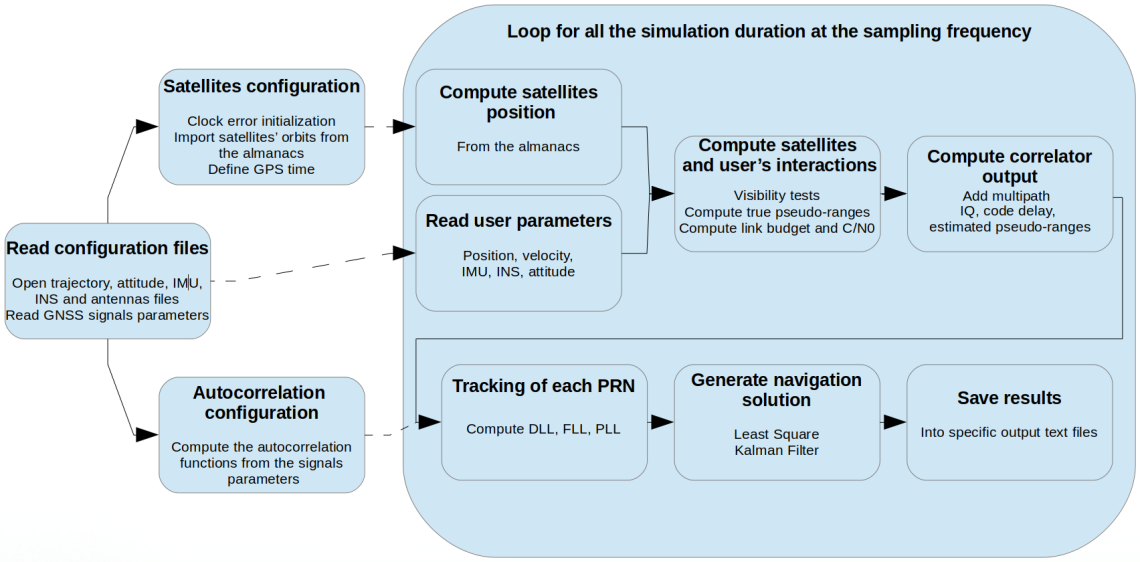


Figure 4: Structure of GeneIQ

2. Simulation's parameters

The overall simulation takes place in Toulouse, France (43.6043N, 1.4437E). The simulation does not consider additional multipath.

a) Satellites parameters

The satellites position generated in these simulations are based on the real position of GPS L1C/A satellites, based on the almanacs as show in Figure 5 where an elevation of 90° means the satellite is at zenith.

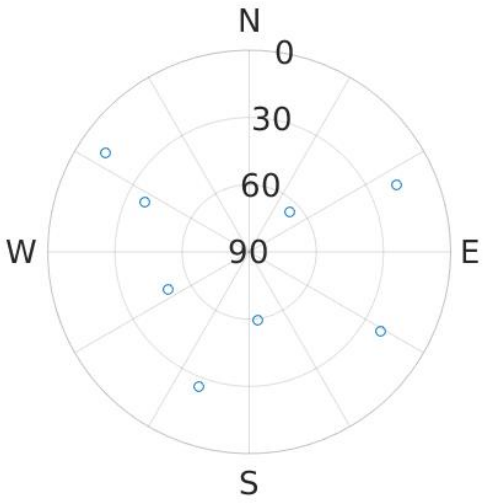


Figure 5: Skyplot of the 8 GPS L1C/A satellites with their azimuth and elevation angles

b) Meaconer parameters

The simulated meaconer has an isotropic transmitting antenna with an overall receiving-to-transmitting gain of 60dB for the nominal configuration and 80dB for the degraded. It is assumed as a simplification that it induces no additional code delay due to its antennas or RF components.

c) Receiver's parameters

The simulated receiver has a receiving antenna with a 0dB isotropic gain. It uses a first order DLL and a third order PLL to track the signal. Both the tracking loops present an integration time T_i of 20ms. The DLL chip spacing is $C_s = \frac{T_c}{2}$ with a chiping period $T_c = \frac{1}{1.023e^6}$ seconds. The bandwidth of the RF filter $B_{RF} = 2$MHz.

In these simulations, the tracking is considered lost when the estimated $\frac{C}{N_0}$ drops below 20dB or if the mean value of $\frac{I_P^2 - Q_P^2}{I_P^2 + Q_P^2}$ drops below 0.4. In this case, a reacquisition is tried 1s later if both thresholds are met again.

3. Scenarios and configurations

In this article, the simulated receiver will be put in 2 different configurations. The first one is a nominal satellite configuration, where the receiver is seeing 8 GPS L1C/A satellites which positions come from almanacs. The meaconer present in this configuration has a 60dB isotropic gain. The second configuration is a degraded satellite configuration, imagined with a higher meaconing gain and a lower visibility on satellites. In this configuration, the receiver is only seeing 4 GPS L1C/A satellites as a mask covering the southern azimutal hemisphere has been set to simulate a building or over kind of satellites occultation. In this configuration, the meaconer's gain is of 80dB. The configurations are summarized in Table 1.

	Nominal configuration	Worse configuration
Meaconer's gain	60dB	80dB
Number of satellites in view	8	4
Azimuth	All	Only northern hemisphere

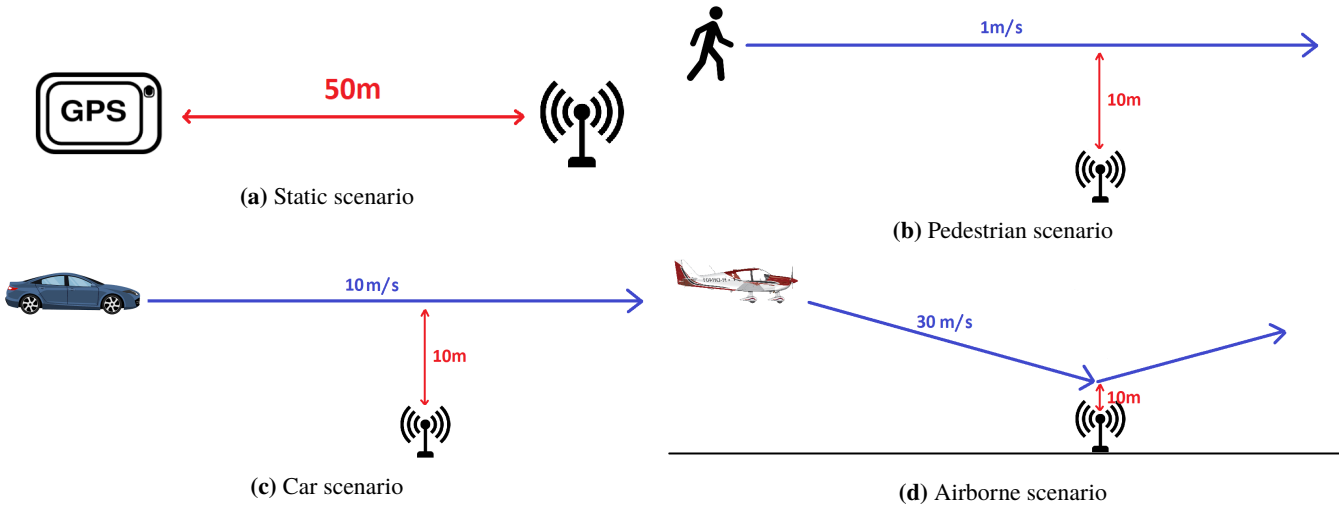
Table 1: Configurations summary

For both configurations, the receiver is tested in 4 different scenarios :

1. a static scenario where the meaconer is located 50m afar;
2. a pedestrian scenario where the receiver moves toward the meaconer at 1m/s from west to east and reaches a point 10m north from the meaconer before continuing its linear path;

3. a car scenario where the receiver moves toward the meaconer at 10m/s from west to east and reaches a point 10m north from the meaconer before continuing its linear path;
4. an airborne scenario where the receiver lands toward the meaconer at 30m/s from west to east with a 3° slope and reaches a point 10m above the meaconer before going around and taking off at the same speed and slope.

These 4 scenarios are illustrated in Figure 6.



(a) Static scenario

(b) Pedestrian scenario

(c) Car scenario

(d) Airborne scenario

Figure 6: Meaconing scenarios

4. Results

During this simulation, the meaconer is activated after 60s to let the Least Square algorithm accumulate enough values as it requires 20s to converge.

In order to remain easy to read, the results only give the most important receiver's outputs.

First result of interest is the meaconer-to-authentic power ratio J/S computed from the link budget. A positive value in dB means that the received meaconing power is greater than the received authentic power.

Another important parameter computed from the link budget is the Doppler difference between the meaconing signal and the authentic one.

The estimated $\frac{C}{N_0} = \frac{E[I_P]^2}{\sigma^2(Q_P)}$ (with I_P and Q_P the prompt in-phase and quadrature correlator outputs) is a crucial indicator of the tracking loop status as the tracking is lost if the estimated $\frac{C}{N_0}$ goes below 20dB.

Finally, pseudorange errors and positioning errors are observed. While pseudorange errors are directly obtained through the correlator ouputs, the positioning error comes from a standard Least Square algorithm.

a) Static scenario in a nominal configuration

Figure 7 shows the meaconer-to-authentic received power ratio of each satellite, their respective pseudorange errors, the overall positioning error as well as the Doppler difference between the meaconing signal and each of the satellites' authentic signal while the receiver is static with a nominal satellites configuration with a 60dB meaconer's gain.

It should be noted that this first simulation does not consider any noise in order to clearly see the impact of the meaconer on the receiver's outputs.

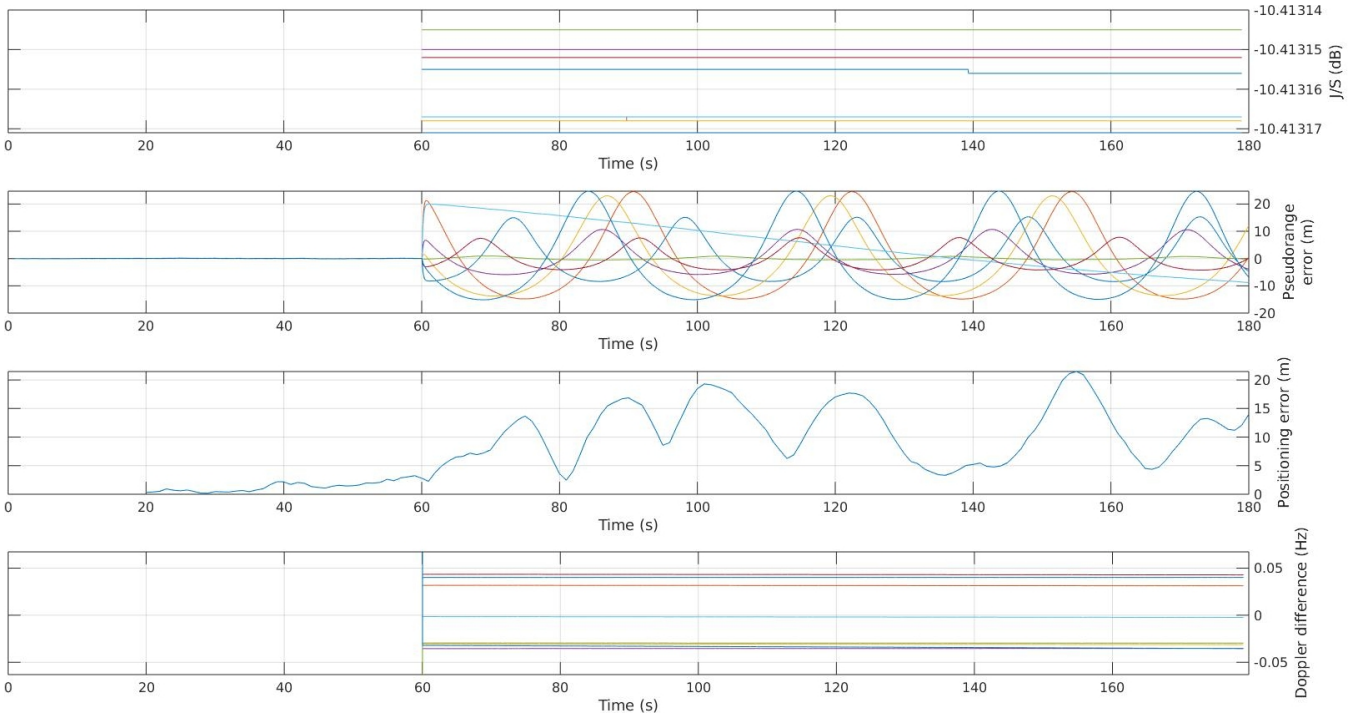


Figure 7: Static scenario in a nominal configuration without noise

As seen on the first plot, the meaconer-to-authentic received power ratio J/S is almost the same for each PRN and is equal to -10.413dB and remains almost constant as a result of the link budget and the low satellite-meaconer distance variation.

The fourth plot gives the Doppler difference Δf between the received authentic signal and the received meaconing signal for each satellite. They remain almost constant as the distance satellite-meaconer-receiver and satellite-receiver remain almost constant during the whole simulation. The maximal Doppler difference is lower than 0.05Hz.

In the second plot, pseudorange errors are oscillating with a $\frac{1}{\Delta f}$ periodicity as most of the PRNs have a period between 20s (1/0.05Hz) and 40s(1/0.025Hz). The only PRN with a much longer period is the light blue one which Doppler difference is almost equal to zero as the satellite is moving in a direction perpendicular to the meaconer-receiver direction. The observed pseudorange errors are bounded by the values set by the 3D multipath error envelope at the given Δf and $\Delta\tau$ resulting from the satellite/meaconer/receiver geometry. It should be noted that the maximal theoretical pseudorange error of the 3D error envelope is $c\frac{\alpha C_s}{2} \simeq 24$m where c is the speed of light, $\alpha = \frac{A_1}{A_0} = 10^{(J/S)/10}$ is the meaconing-to-authentic signal power's ratio and $C_s = \frac{T_c}{2}$ is the chip spacing used by the DLL. The maximal observed pseudorange error is 24m and respects the theoretical maximum value.

Finally, the third plot shows the Least Square positioning error after 20s of value accumulation. The maximal positioning error is of 22m for the noiseless static scenario in a nominal satellite configuration and with a 60dB meaconer.

To be more realistic and in order to consider possible tracking loss due to poor estimated $\frac{C}{N_0}$, the noise should be added to the simulations. Figure 8 shows the meaconer-to-authentic received power ratio of each satellite, their respective pseudorange errors, the overall positioning error as well as the estimated $\frac{C}{N_0}$ of each PRN while the receiver is static with a degraded satellites configuration with a 60dB meaconer's gain when considering noise.

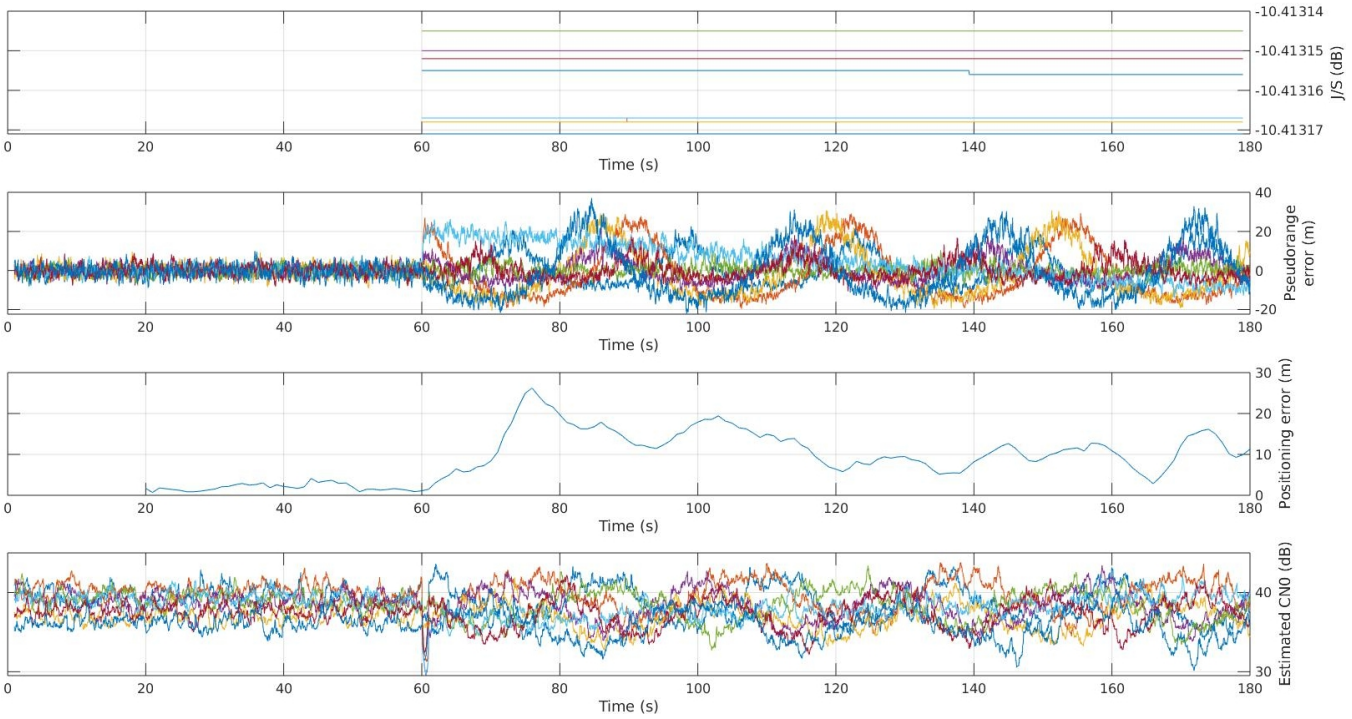


Figure 8: Static scenario in a nominal configuration

It can be seen that the overall behaviour of the pseudorange error in the second plot and positioning error in the third plot is the same with or without noise. The resulting positioning error is therefore a bit higher, with a slightly higher maximal value of 26m. For this simulation, the estimated $\frac{C}{N_0}$ in the fourth plot doesn't go below 30dB and therefore there is no tracking loss after appearance of the meaconer under a nominal configuration for the static scenario. When introducing meaconing, the amplitude of the oscillations slightly increases with variations between 30dB and 43dB while it was only between 35dB and 43dB before meaconing.

b) Static scenario in a degraded configuration

Figure 9 shows the meaconer-to-authentic received power ratio of each satellite, their respective pseudorange errors, the overall positioning error as well as the estimated $\frac{C}{N_0}$ of each PRN while the receiver is static with a degraded satellites configuration with a 80dB meaconer's gain.

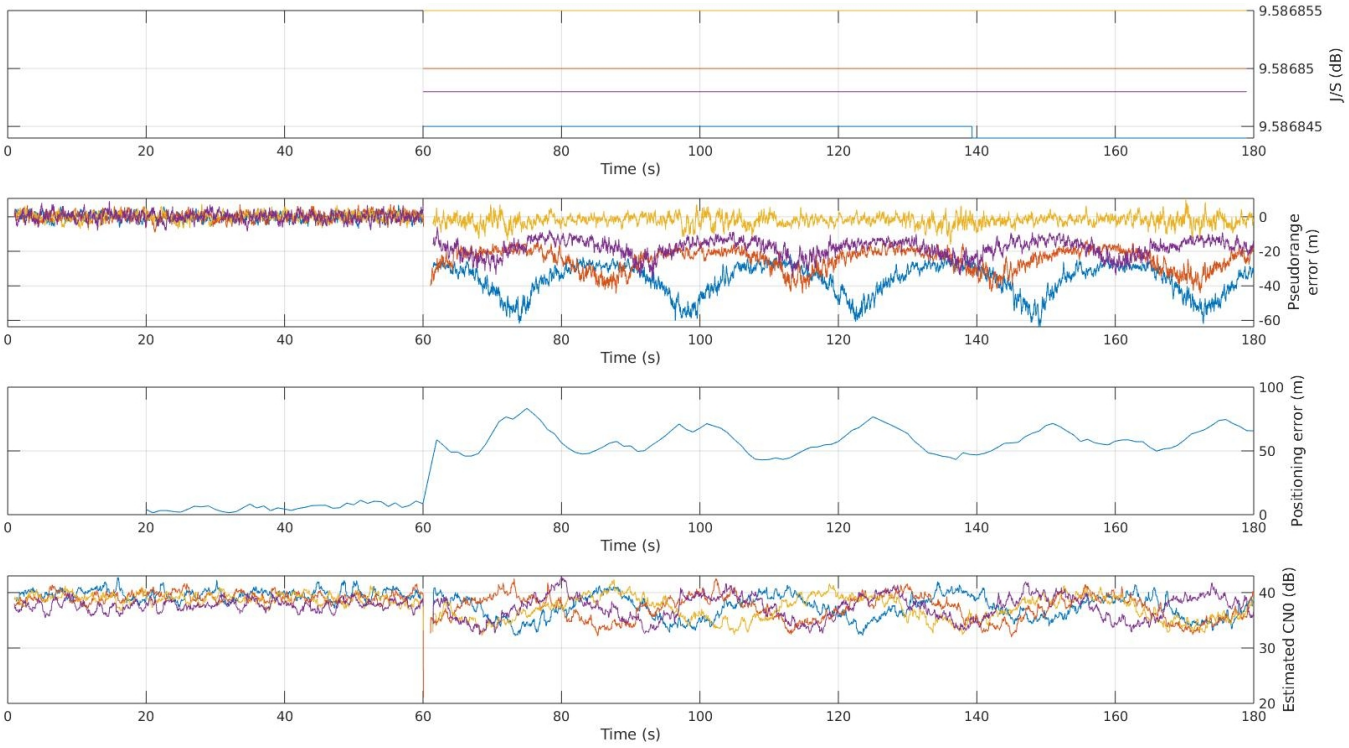


Figure 9: Static scenario in a degraded configuration

This time, it can be observed in the fourth plot that tracking is lost when meaconing appears as the estimated $\frac{C}{N_0}$ goes below the 20dB threshold. The meaconing signal is reacquired after 1s as it is the signal with the highest power (J/S = 9.587dB > 0dB).

In this configuration, the tracked signal is the meaconer's and the authentic signal becomes multipath. Therefore, the 3D error envelope boundaries can still be observed in the second plot (pseudorange errors) but with the LOS signal being the meaconer's. As the meaconer's signal is received after the authentic signal, the estimatd code delay error is negative as the authentic signal, acting as multipath, is received first.

In the third plot, the mean positioning error is 50m as the position is estimated around the meaconer's position. The mean pseudorange error depends on the satellite/meaconer/receiver geometry. If the meaconer is on the path between the satellite and the receiver, the code delay of the meaconing signal will almost be the same as the authentic code delay, while if the signal has to go through longer distances, the meaconing signal will have a higher code delay and therefore will lead to greater pseudorange errors. The pseudorange error periodicity is still linked to the Doppler difference between the authentic and the meaconing signal, which is not shown for visibility purpose but is the same as in Figure 7.

c) Pedestrian scenario in a nominal configuration

As for the previous scenario, the pedestrian scenario simulations will first be observed in a noiseless environment then with noise. Noiseless simulations allow to see subtle variations in the pseudorange errors due to the Doppler difference but to remain more realistic and to consider tracking loss, noise should be added at the end.

Figure 10 shows the meaconer-to-authentic received power ratio of a single satellite, its pseudorange error, the overall positioning error as well as the Doppler difference between the meaconing signal and the satellite's authentic signal while the receiver is tested on a pedestrian scenario with a nominal satellites configuration and a 60dB meaconer's gain.

The plots are shown for a single satellite for visibility purpose but the simulation have been conducted for the 8 satellites and the Least Square positioning solution comes from all the 8 pseudoranges.

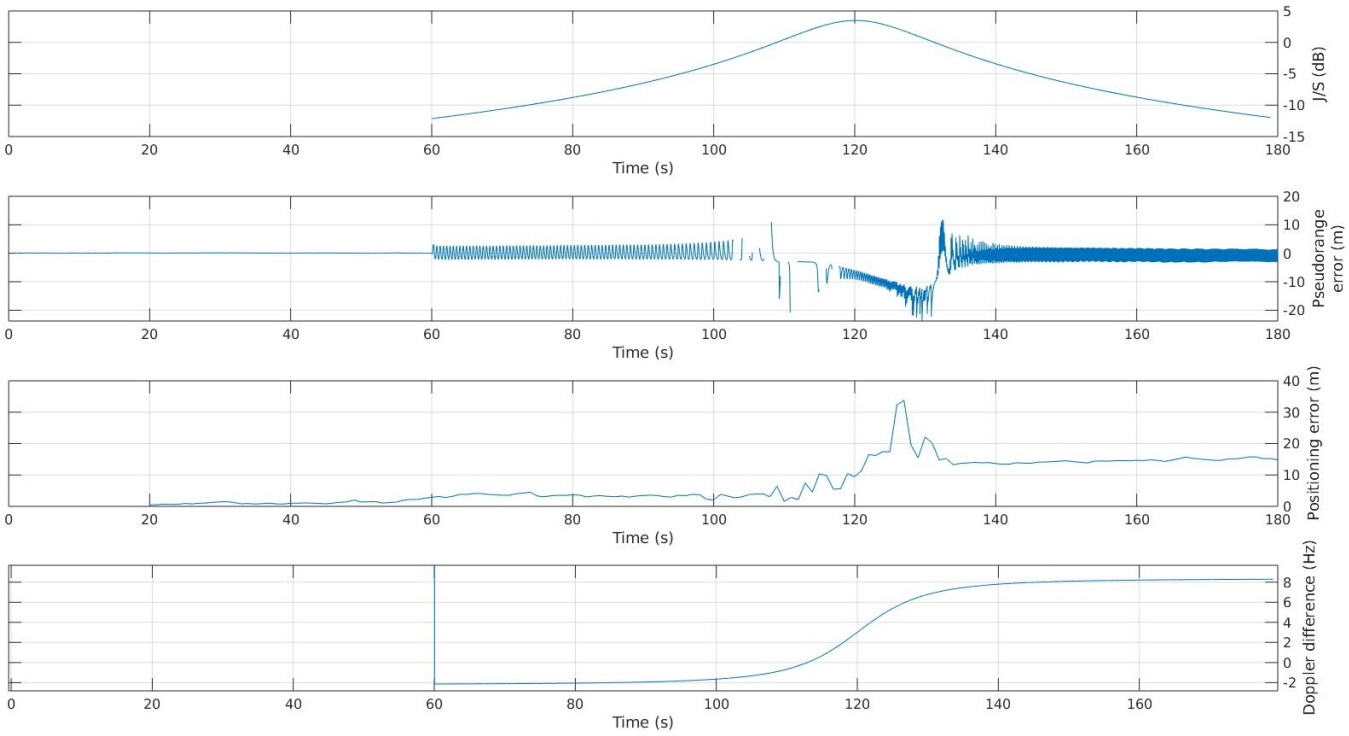


Figure 10: Pedestrian scenario in a nominal configuration without noise

As the receiver is moving, the meaconer-to-signal ratio J/S in the first plot is evolving with time. The J/S gets higher when the receiver is getting closer to the meaconer. It reaches positive values which reveals that the meaconer's received signal is higher than the authentic one. The J/S finally decreases when the receiver is getting away from the meaconer.

In the second plot, the pseudorange error is centered on 0 and oscillates with a periodicity of 0.5s = $\frac{1}{|\Delta f|}$ between 60s and 110s of simulation. Then when the J/S reaches 0dB, the mean pseudorange error is almost equal to the receiver-meaconer distance as it is 10m at 120s and 14m (10 meters north, 10 meters east) at 130s. When the J/S drops below 0dB at 130s, the mean pseudorange error is once again null. The oscillation periodicity is then of 0.12s $\simeq \frac{1}{\Delta f}$ as Δf can be observed in the fourth plot.

Once again, to be more realistic and in order to consider possible tracking loss due to poor estimated $\frac{C}{N_0}$, the noise should be added to the simulations. Figure 11 shows the meaconer-to-authentic received power ratio of each satellite, their respective pseudorange errors, the overall positioning error as well as the estimated $\frac{C}{N_0}$ of each PRN while the receiver is tested on a pedestrian scenario with a nominal satellites configuration and a 60dB meaconer's gain.

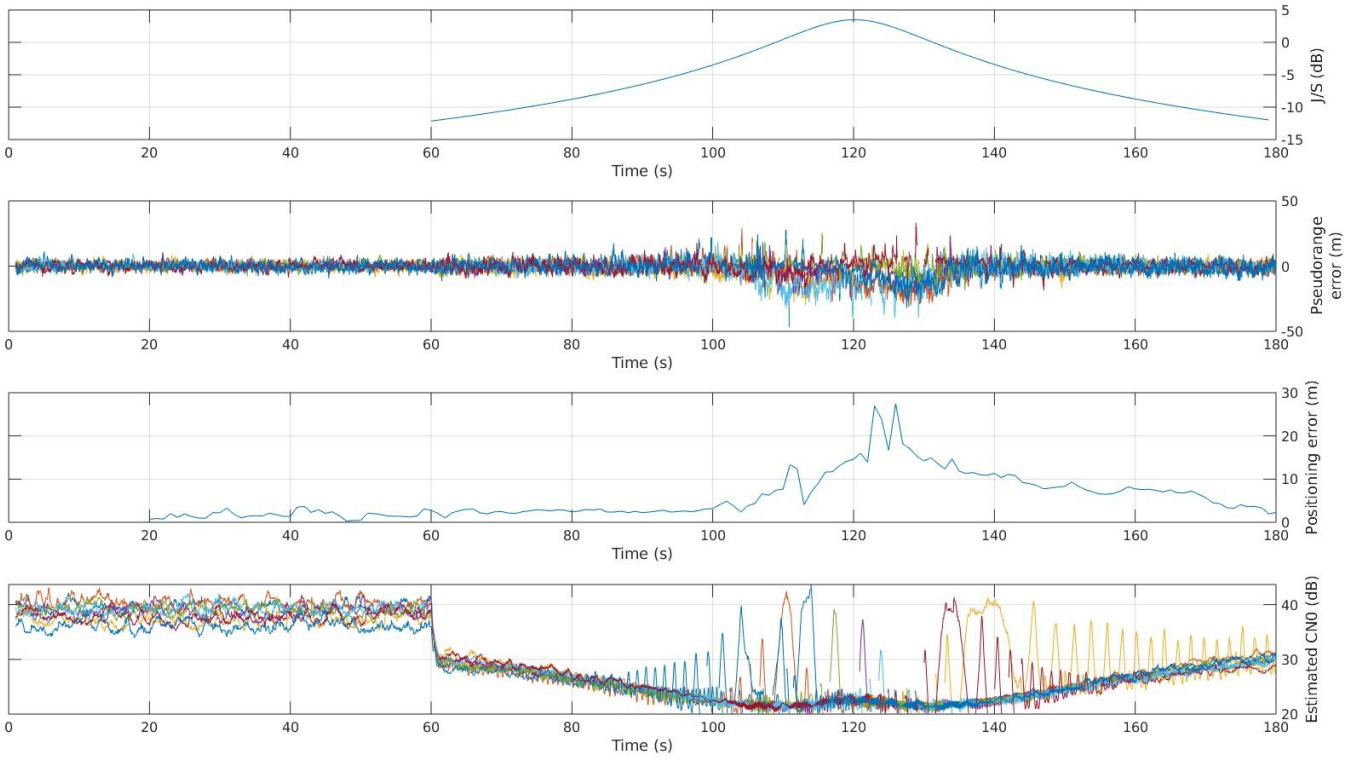


Figure 11: Pedestrian scenario in a nominal configuration

In the fourth plot, it can be seen that the activation of the meaconer, while in a 60m range from the receiver, leads to a drop in the mean estimated $\frac{C}{N_0}$ as the meaconer re-radiates noise as well and the received noise power depends on the meaconer-receiver distance.

When the receiver is at its closest to the meaconer, around 120s, the mean estimated $\frac{C}{N_0}$ drops near to 20dB. The oscillations that can be seen for some PRN are attempts of our simulator to track the signal while the $\frac{C}{N_0}$ is really bad and should not be considered for the estimation of $\frac{C}{N_0}$ as the re-acquisition process of our simulator is still to be enhanced.

The second plot reveals an impact of the meaconer on the pseudorange errors as they reach a maximal value of 48m and the maximal positioning error in the third plot is of 28m.

d) Pedestrian scenario in a degraded configuration

Figure 12 shows the meaconer-to-authentic received power ratio of each satellite, their respective pseudorange errors, the overall positioning error as well as the estimated $\frac{C}{N_0}$ of each PRN while the receiver is tested on a pedestrian scenario with a degraded satellites configuration and a 80dB meaconer's gain.

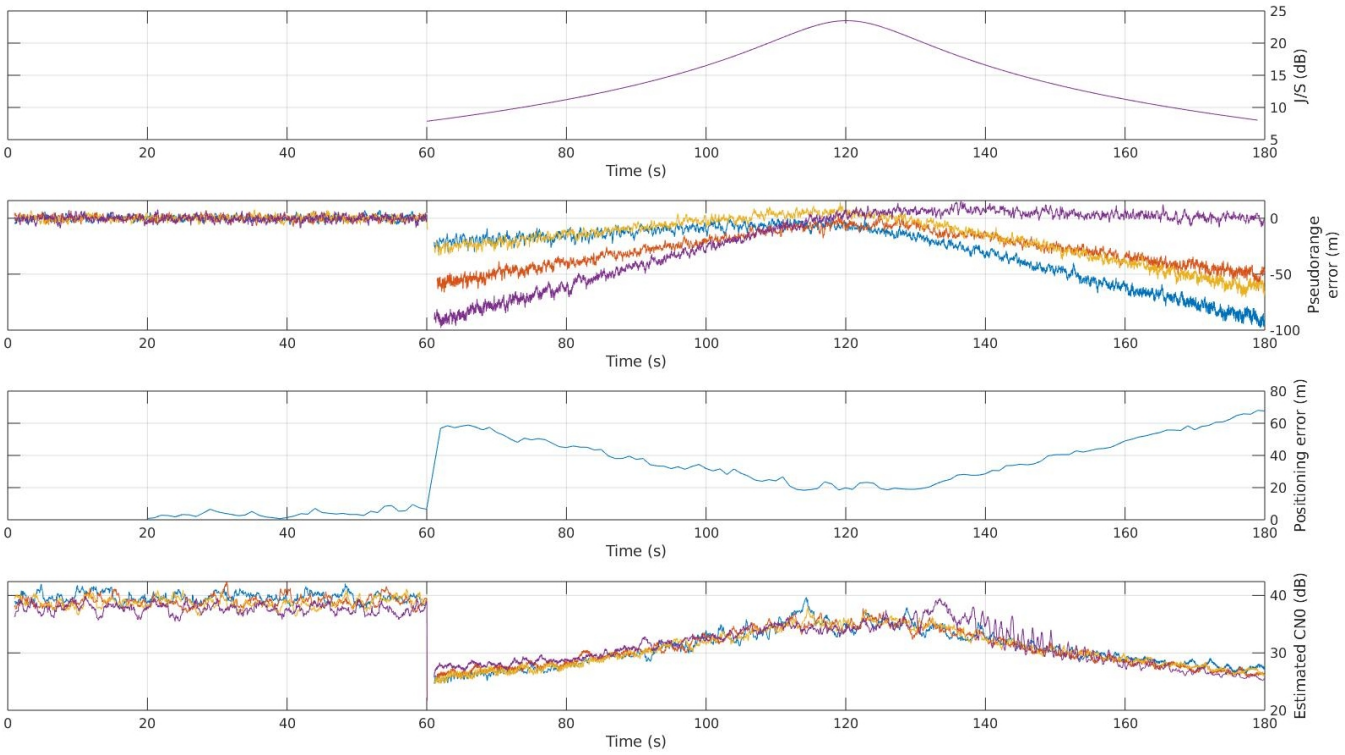


Figure 12: Pedestrian scenario in a degraded configuration

The J/S, visible in the first plot, is higher than 0 during the whole meaconing period.

In the fourth plot, the estimated $\frac{C}{N_0}$ goes below the threshold. This suddent drop can be explained as the $\frac{C}{N_0}$ estimator accumulates the correlator outputs values over 1 second to compute the mean value of I_P and the variance of Q_P. The estimated $\frac{C}{N_0}$ is therefore biaised during the first second of the meaconer's apparition and it leads to a tracking loss. As J/S > 0dB, the meaconer's signal is tracked and the estimated $\frac{C}{N_0}$ increases with the J/S as the tracked signal's power and the meaconer's noise are increasing while the authentic noise remains constant ($\frac{C}{N_0} = \frac{C_{tracked}}{N_{authentic}+N_{meaconer}}$).

The interpretation of the positioning error and pseudorange errors plots is the same as for the degraded configuration of the static scenario. The meaconer's position is tracked and therefore the positioning error is approximately equal to the meaconer-receiver distance. As the meaconer's signal is tracked and the authentic signal is considered as multipath, the differences between the received code delay of the meaconer and of the authentic signal are negative and so are the pseudorange errors.

e) Car scenario in a nominal configuration

Figure 13 shows the meaconer-to-authentic received power ratio of each satellite, their respective pseudorange errors, the overall positioning error as well as the estimated $\frac{C}{N_0}$ of each PRN while the receiver is tested on a car scenario with a nominal satellites configuration and a 60dB meaconer's gain.

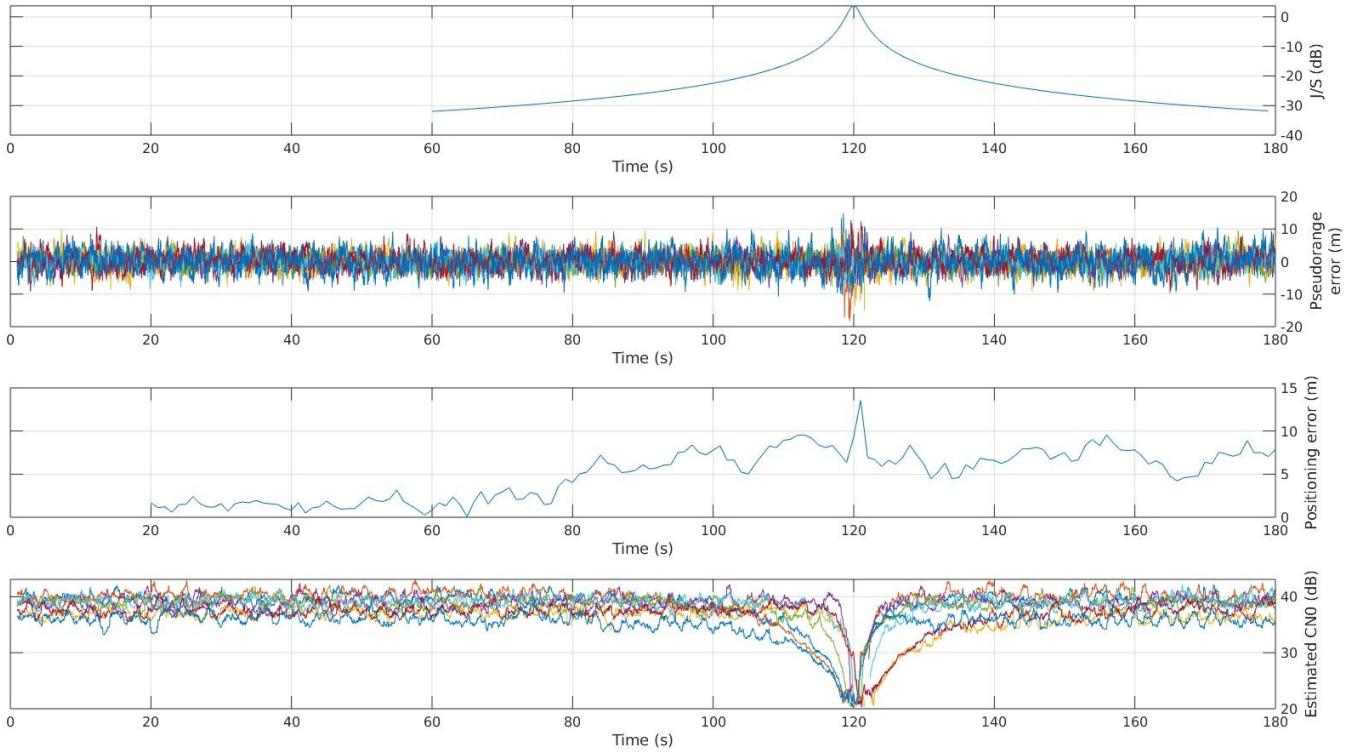


Figure 13: Car scenario in a nominal configuration

As the receiver is moving faster, the J/S evolves faster too in the first plot. It is only higher than 0dB for a few seconds around 120s.

The overall behaviour of the receiver is the same as for the pedestrian scenario but the time of impact of the meaconer is shorter as the receiver starts at a longer distance and is in the range of the pedestrian scenario for only 12s.

In the fourth plot, the impact of the meaconer on the estimated $\frac{C}{N_0}$ can be observed around 120s for a J/S>-15dB. The tracking is lost for some PRNs but the re-acquisition is succesfully achieved a few seconds later when the $\frac{C}{N_0}$ as gained a few dB.

The impact of the meaconer on the pseudorange errors and positioning errors is quite low, as the maximal positioning error only reaches 13m the iteration after the maximal J/S value and does not exceed 10m otherwise.

f) Car scenario in a degraded configuration

Figure 14 shows the meaconer-to-authentic received power ratio of each satellite, their respective pseudorange errors, the overall positioning error as well as the estimated $\frac{C}{N_0}$ of each PRN while the receiver is tested on a car scenario with a degraded satellites configuration and a 80dB meaconer's gain.

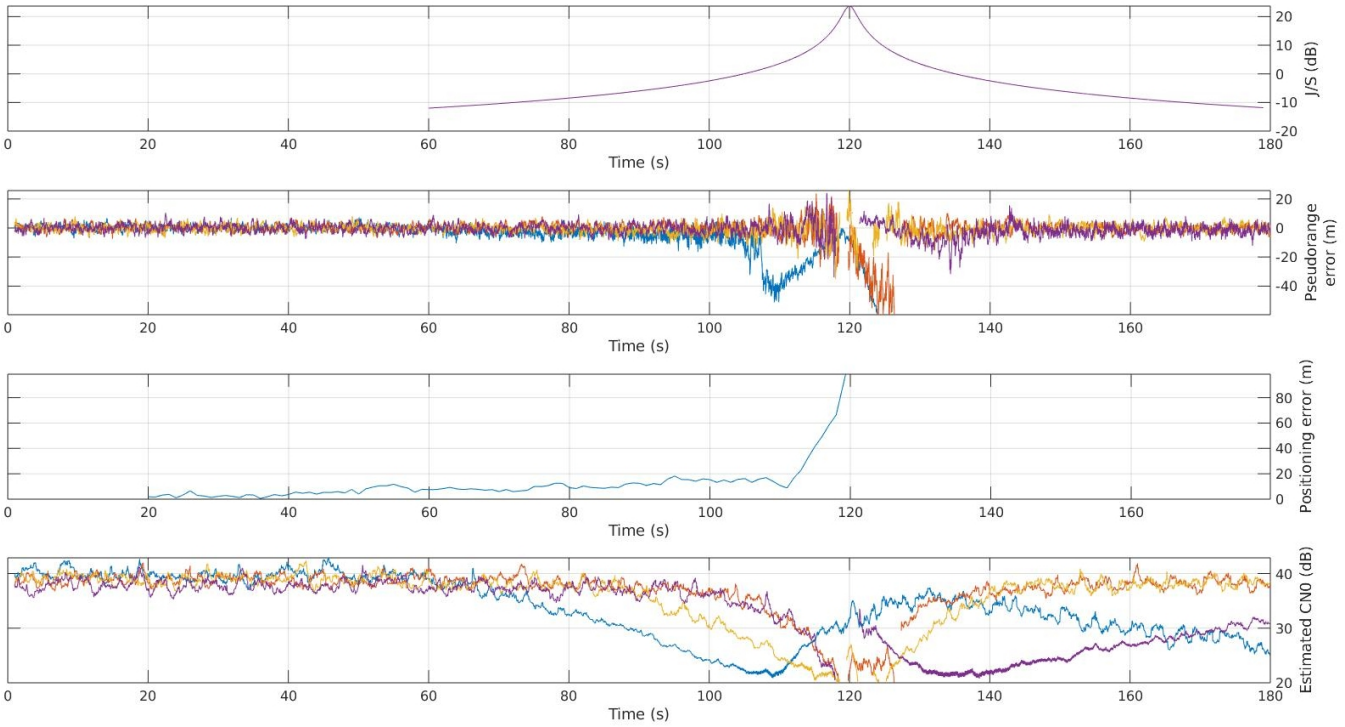


Figure 14: Car scenario in a degraded configuration

In the fourth plot, the impact of the meaconer on the estimated $\frac{C}{N_0}$ can be observed as soon as the meaconer is activated. The tracking is lost for 3 PRNs around 120s but the blue PRN does not seem to be considered lost. However, it seems that the meaconer's signal has been tracked slowly around 110s as the estimated $\frac{C}{N_0}$ increases and decreases with the J/S after that moment.

This behaviour can also be observed in the second plot as only 3 pseudorange errors are visible after 130s.

In the third plot, there are no longer 4 pseudoranges after 118s so there is no more Least Square positioning available. While 3 of the authentic signals are normally tracked after 130s, the Least Square's position keep increasing as the last tracking loop channel is still locked on the meaconer's signal. The plot as been cropped so that the behaviour before 120s can be better seen.

g) Airborne scenario in a nominal configuration

Figure 15 shows the meaconer-to-authentic received power ratio of each satellite, their respective pseudorange errors, the overall positioning error as well as the estimated $\frac{C}{N_0}$ of each PRN while the receiver is tested on an airborne scenario with a nominal satellites configuration and a 60dB meaconer's gain.

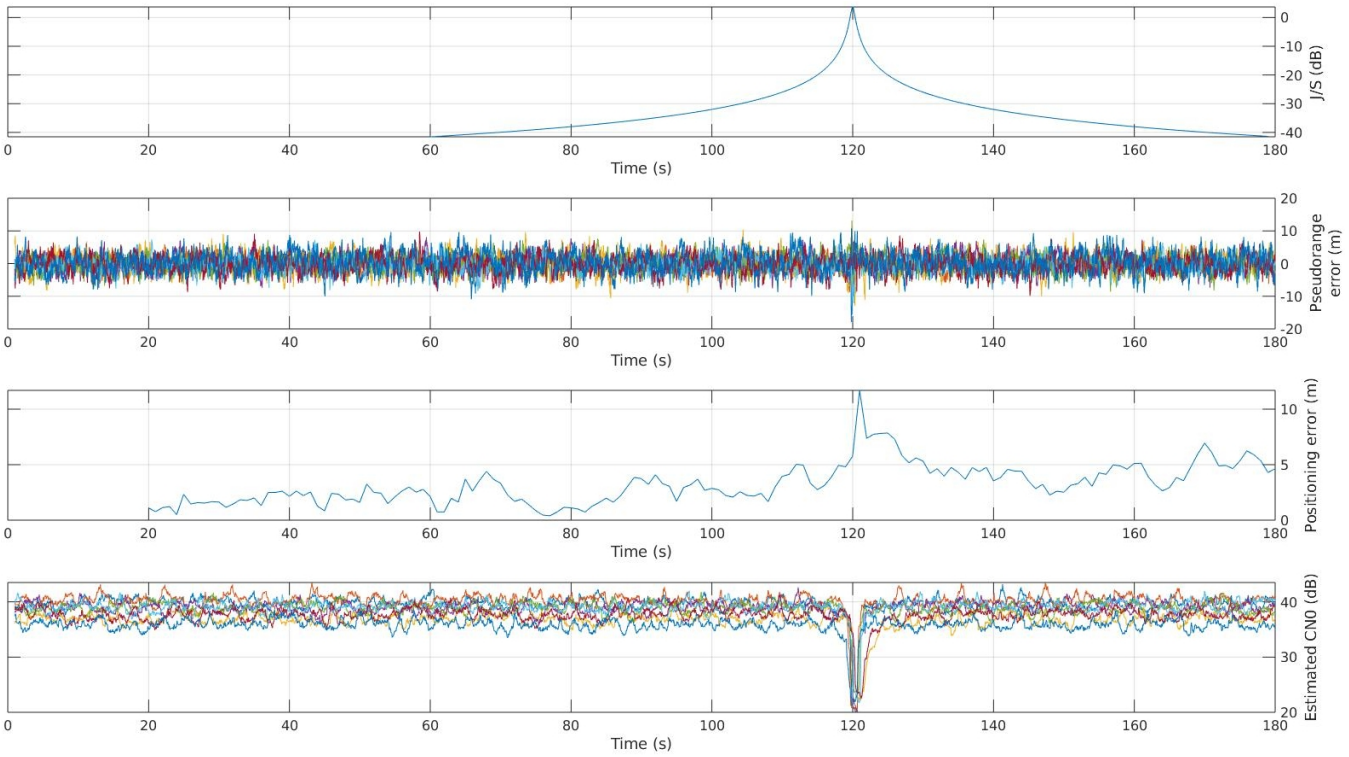


Figure 15: Airborne scenario in a nominal configuration

As the receiver is moving faster, the J/S evolves faster too in the first plot. It is only higher than 0dB for a few seconds around 120s.

The overall behaviour of the receiver is the same as for the pedestrian scenario but the time of impact of the meaconer is shorter as the receiver starts at a longer distance and is in the range of the pedestrian scenario for only 4s.

In the fourth plot, the impact of the meaconer on the estimated $\frac{C}{N_0}$ can be observed around 120s. For a J/S>-15dB. The tracking is lost for some PRNs but the re-acquisition is succesfully achieved a few seconds later when the $\frac{C}{N_0}$ as gained a few dB.

The impact of the meaconer on the pseudorange errors and positioning errors is quite low, as the maximal positioning error only reaches 12m the iteration after the maximal J/S value and does not exceed 8m otherwise.

h) Airborne scenario in a degraded configuration

Figure 16 shows the meaconer-to-authentic received power ratio of each satellite, their respective pseudorange errors, the overall positioning error as well as the estimated $\frac{C}{N_0}$ of each PRN while the receiver is tested on an airborne scenario with a degraded satellites configuration and a 80dB meaconer's gain.

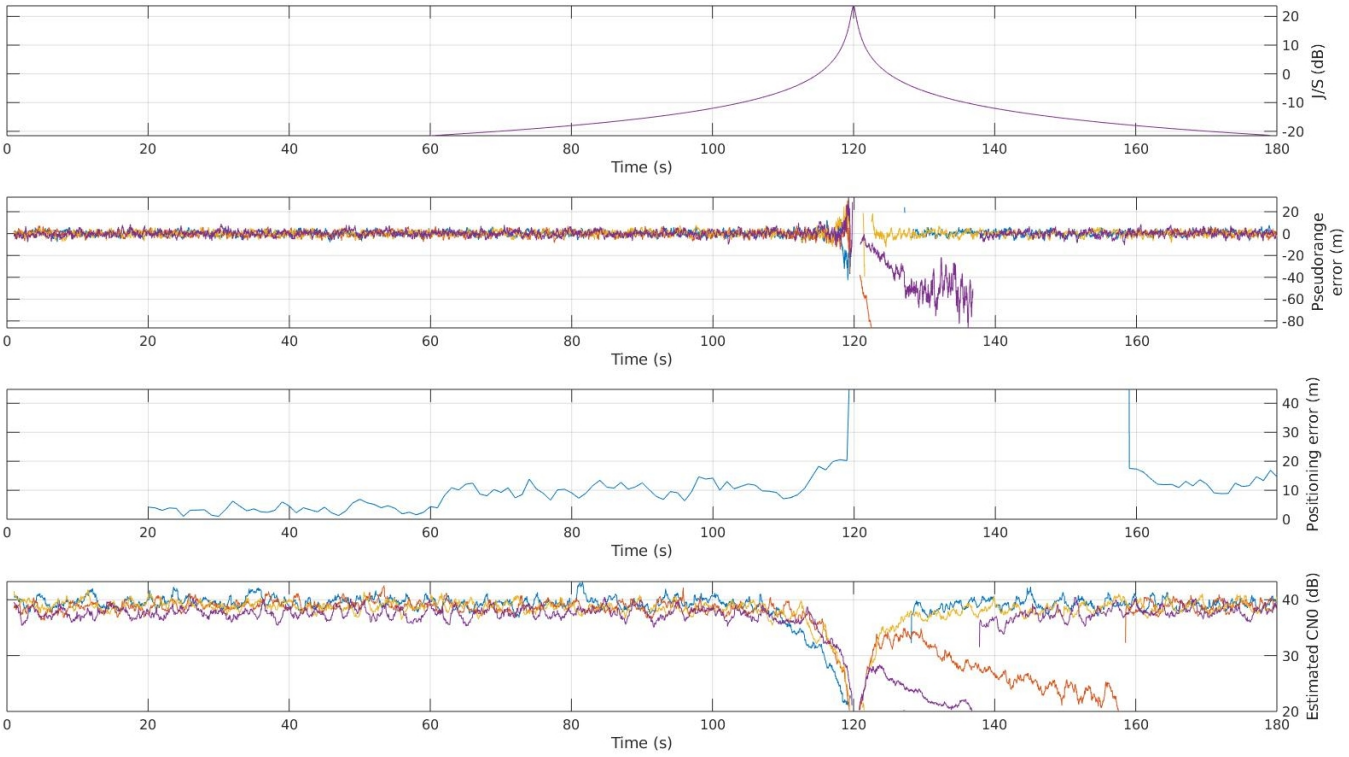


Figure 16: Airborne scenario in a degraded configuration

In the fourth plot, the estimated $\frac{C}{N_0}$ goes below the tracking threshold for all of the 4 PRNs this time. As there are no longer 4 pseudoranges after 119s, there is no more Least Square positioning available. The reacquired signals are the meaconing signals for the purple and orange PRN but is also tracking the authentic signal of the blue and yellow PRNs it reacquired a few seconds later.

The estimated position, in the third plot, after the reacquisition is out of range and isn't shown in the Figure 16 as the scale wouldn't allow to see the previous behaviour before 119s. However, the tracking of the meaconer's signal is definetively lost at 158s and therefore the 4 authentic signals are tracked after 159s of simulation, allowing the receiver to compute an approximatively accurate position through the LS algorithm at the end of the simulation when J/S < -15dB.

This behaviour can also be observed in the second plot as all the 4 pseudorange errors are centered on 0 after 159s.

IV. CONCLUSION

In this article, it has been seen that the received meaconing signal is added to the received authentic signal at the receiver's correlator inputs. The power, code delay and phase shift of the received meaconing signal come from a combination of two link budgets, one from the satellite to the meaconer and one from the meaconer to the receiver. It has also been seen that a meaconer can act like a jammer as it amplifies noise. A multipath error envelope can be modeled to characterize the impact of meaconing on correlator outputs. This model can be extended to a 3D model including the code delay, phase shift and Doppler difference between the authentic signal and the meaconing one.

Some simulations have been conducted on an ENAC simulated receiver called GeneIQ. These simulations included various configurations and scenarios to reflect the various situations a GNSS receiver can be faced with. During nominal configuration scenarios, the meaconing-to-signal ratio J/S was negative in dB and therefore the tracking process wasn't really affected, only additional pseudorange errors could be detected. For scenarios with a higher velocity such as the car scenario or the airborne scenario, the impact of the meaconer was of really short duration and of a weak amplitude. However, during degraded configuration scenarios, the meaconing-to-signal ratio was sometimes positive, and in case of tracking losses, the meaconer's signal was acquired. For low velocity scenarios such as the static or the pedestrian ones, the receiver was estimating the meaconer position. On the other hand, for higher velocities, only some of the PRN were acquired and the estimated position was neither the authentic position, nor the meaconer's position. Noiseless simulations revealed that Doppler frequency and overall scenario's geometry were of a great impact on pseudorange and positioning errors.

Meaconing as been shown to be of a considerable impact on low velocity receivers, especially when only few satellites are available. However, all these simulations have been done without authentic multipath and meaconing often comes with environment multipath as the meaconer is often located inside buildings, and the outdoor radiation comes from apertures (doors, windows, ...) that are not shielded. This study was led with simplistic propagation parameters but the receiver's antenna gain toward the meaconer should be considered as it may degradedn or ease the impact of the meaconer while moving around.

REFERENCES

[1] E. Steindl, W. R. Dunkel, A. Hornbostel, C. Hättich, and P. Rémi, "The impact of interference caused by gps repeaters on gnss receivers and services," 2013.

[2] C. GÃijnther, "A survey of spoofing and counter-measures," *Navigation*, vol. 61, 09 2014.

[3] A. Iliopoulos, C. Enneking, T. Jost, O. Garcia Crespillo, M. Appel, and F. Antreich, "Robust ranging in the presence of repeater signals," 09 2017.

[4] T. . B. W. . W. J. . M. L. . A.-R. J.-A. . I. R. Dampf, J. ; Pany, "Real world spoofing trials and mitigation via direction of arrival discrimination," *Inside GNSS*, 2017.

[5] P. Brocard, D. Salos, O. Julien, and M. Mabilleau, "Performance evaluation of multipath mitigation techniques for critical urban applications based on a land mobile satellite channel model," in *2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014*, 2014, pp. 612–625.

[6] E. D. Kaplan and C. J. Hegarty, *Understanding GPS : Principles and Applications, 2nd Edition*, A. House, Ed. Artech House, 2006.

[7] C. Chabory, A. ; Morlass, "Antennes," ENAC courses, 2017.

[8] C. Julien, O. ; Macabiau, "Gnss advanced concepts," ENAC courses, 2018.