Results and Lessons Learned from the NAVITEC 2024 Resilient GNSS Challenge

Lotfi Massarweh, *Delft University of Technology (TUD)*
Chengyu Yin, *Delft University of Technology (TUD)*
Daniele Borio, *European Commission, Joint Research Centre (JRC)*
Melania Susi, *Topcon Positioning Systems*
Hakan Uyanik, *German Aerospace Center (DLR)*
Daniel Medina, *German Aerospace Center (DLR)*
Andrea Bellés Ferreres, *German Aerospace Center (DLR)*
Filippo Giacomo Rizzi, *German Aerospace Center (DLR)*
Christoph Lass, *German Aerospace Center (DLR)*
Tao Lin, *Correlation Semiconductor Co. LTD*
Tao Li, *Correlation Semiconductor Co. LTD*
Wei Gao, *Correlation Semiconductor Co. LTD*
Gerarda De Pasquale, *HE Space for ESA*
Noori Bni Lam, *Telespazio Belgium SRL for ESA*
Ruediger Matthias Weiler, *European Space Agency (ESA)*
Paolo Crosta, *European Space Agency (ESA)*

ABSTRACT

At the end of 2024, the 'Resilient GNSS Challenge' was organized by the European Space Agency (ESA) and hosted during the 11th ESA Workshop on Satellite Navigation Technologies (NAVITEC 2024). This competition focused on real world challenges, based on a dataset collected in September 2024 during the Norwegian Jammertest campaign. In this contribution, we present the challenge results, thus describing the scenarios and providing details on the solutions developed by the teams ranked in the top three positions of the competition. Different spoofing conditions were considered in two scenarios, with a total of three problems to be solved with static and/or moving receivers tracking spoofed signals. All in all, the analysis of Carrier-To-Noise Power Spectral Density Ratio (C/N_0) values turned out to be an essential element for a proper characterization of the different problems, along with providing a correct identification of genuine GNSS signals that could safely be used by the teams.

I. INTRODUCTION

The Global Navigation Satellite System (GNSS) is vulnerable to multiple forms of Radio Frequency (RF) interference. These include unintentional phenomena, such as spurious emissions from faulty electronics, and intentional threats, such as jamming and spoofing events (Borio et al., 2016; Psiaki and Humphreys, 2016), which have significantly increased in the last few years. For instance, jamming is primarily used as a deception tactic in several conflict zones, resulting in the GNSS Denial of Service (DoS) across extensive geographical regions. Spoofing incidents have also risen notably, as documented by different GNSS stakeholders including aviation operators and monitoring systems (Lo et al., 2025).

Jamming and spoofing can cause DoS or, even worse, provide misleading information with severe impacts on society, especially for Positioning, Navigation and Timing (PNT) applications. To reduce the risks associated with these threats, GNSS receiver manufacturers are introducing security features in their devices, which are now able to detect and potentially mitigate the effects of these types of interference (Heijnen et al., 2025). In this respect, the Norwegian Jammertest campaign (https://jammertest.no) has become the largest open annual GNSS resilience test event enabling industry, academia, and the public sector to test GNSS resilience solutions in open-air scenarios under different live jamming and/or spoofing conditions. In September 2024, the event lasted five days and it featured multiple jamming and spoofing scenarios. The European Space Agency (ESA) participated to the 2024 Norwegian Jammertest and collected more than 100 terabytes of In-phase/Quadrature (IQ) samples and several hours of GNSS raw measurements from receivers of various grades. The data collected cover a large part of the GNSS spectrum under different jamming and spoofing conditions. Additionally, several dynamic user conditions were considered. Events such as the Jammertest (Jammertest Consortium, 2024) aim to promote international collaboration, share best practices, and develop common solutions that can help mitigate the impact of emerging GNSS threats.

In this spirit, ESA launched the 'Resilient GNSS Challenge' where some of the raw measurements (i.e. GNSS observables) collected during the 2024 Norwegian Jammertest were shared openly with the research community. The challenge was organized as part of the 11th ESA Workshop on Satellite Navigation Technologies (NAVITEC), held at the European Space Research and Technology Centre (ESTEC) at the end of 2024. Participants were encouraged to collaborate, analyze the data, and propose solutions to different problems focusing on spoofing events. In the first scenario, the position of a static user under spoofing was considered, while the second scenario consisted of two problems: the accurate positioning of a spoofed dynamic user and the determination of the Angle-of-Arrival (AoA) of the spoofing source.

The goal of this contribution is to describe the challenges and technical solutions identified by the teams ranked in the first three positions of the ESA's 'Resilient GNSS Challenge'. This work shares the experiences gained by the teams and provides a comprehensive overview of the results obtained, including limitations and recommendations for effective spoofing mitigation. Note that in all challenges, only raw observations based on the Receiver INdependent EXchange (RINEX) format were provided, without additional information at receiver level, such as IQ samples, and with relatively limited information as further described in the next section.

This paper is divided into three parts: first, it describes the two scenarios with three associated problems, detailing the raw GNSS data and additional information made available for each problem. Next, it explains the methodologies and results obtained by the teams when solving each problem. Finally, a discussion on the main outcomes of the challenge is provided, thus offering recommendations for future work.

II. RESILIENT GNSS CHALLENGE DESCRIPTION

The ESA 'Resilient GNSS Challenge', held in conjunction with NAVITEC 2024[1], was designed to evaluate the robustness of GNSS-based positioning solutions under realistic spoofing conditions. The challenge was based on real-world data collected during the Norwegian Jammertest campaign in September 2024. This section briefly describes the two scenarios and the three problems constituting the challenge.

Scenario 1: Static Receiver Under Coherent Spoofing

In this scenario, a stationary spoofer transmitted GPS L1 Coarse Acquisition (C/A) signals using true broadcast ephemerides to simulate a coherent spoofing attack. The spoofed signals were intended to align (to within a few 100 ns) with those received from actual satellites at the target location (coherent). The spoofed signals were transmitted at a power level of 0.316 W and designed to emulate drone-like dynamics, misleading the receiver and inducing it to believe that it was in motion. This was part of flying (route 4) "drone scenario" for GPS L1-only discussed in (Jammertest Consortium, 2024, Section 2.3.12). The victim receiver was static and located near Bleik Stadion in Norway. The problem associated to Scenario 1 involved the estimation of the true receiver position using only the provided RINEX observation files, which spanned from GPS Time 15:13:30 to 15:23:00 on September 11, 2024. Observations from the reference station ANDE00NOR, i.e. located in Andøya island approximately 9 km away from the victim receiver, were also made available to support differential processing.

The spoofed signals introduced significant errors in both pseudorange and carrier-phase observations. These distortions rendered conventional positioning techniques ineffective. Participants were challenged to identify and mitigate the spoofing effects using alternative positioning strategies, like Doppler-based navigation. The RINEX file for the victim receiver included multi-frequency, multi-constellation observations, as summarized in Table 1.

Table 1: GNSS signals available for the victim receiver of Scenario 1, including RINEX codes.

Constellation	Band (Code)	Frequency (MHz)
G: GPS	L1 (1C)	1575.42
	L5 (5Q)	1176.45
E: Galileo	E6 (6C)	1278.75
	E5a (5Q)	1176.45
	E5b (7Q)	1207.14
	E5 (8Q)	1191.795
C: BeiDou	B2a (5P)	1176.45
	B3 (7I)	1207.14

[1]More information at `https://atpi.eventsair.com/navitec-2024/call-for-competitors`

Scenario 2: Mobile Spoofer and AoA Estimation

The second scenario introduced a more complex spoofing environment involving both a static and a dynamic phase. The mobile spoofer, mounted on the roof of a vehicle, initially stationary, began moving along Stavedalsveien (FV7702) at approximately 40 km/h after ten minutes while continuously transmitting a fixed spoofed position. The spoofing signal was transmitted for GPS L1 at a lower power level of 0.01 W, as described in (Jammertest Consortium, 2024, Section 2.6.2).

This scenario was divided into two distinct problems:

Problem A – Spoofer AoA Estimation

Teams were provided with RINEX data derived from a 2×2 patch antenna array, with elements spaced 10 cm apart as illustrated in Figure 1. Spoofing affected only the GPS L1 C/A band, with the remaining signals unavailable. The goal here was to estimate the azimuth of the spoofing source relative to the local antenna frame at a 1 Hz sampling rate. Teams were expected to apply direction-finding techniques, such as carrier-phase differencing and weighted least squares in order to determine the AoA of the spoofed signals. It is worth noting that typically raw IQ samples should be used in order to estimate the AoA of the received signals (BniLam et al., 2023; BniLam and Crosta, 2024). However, in this challenge, only the GNSS observables have been exploited to estimate the AoA of the spoofed signals.

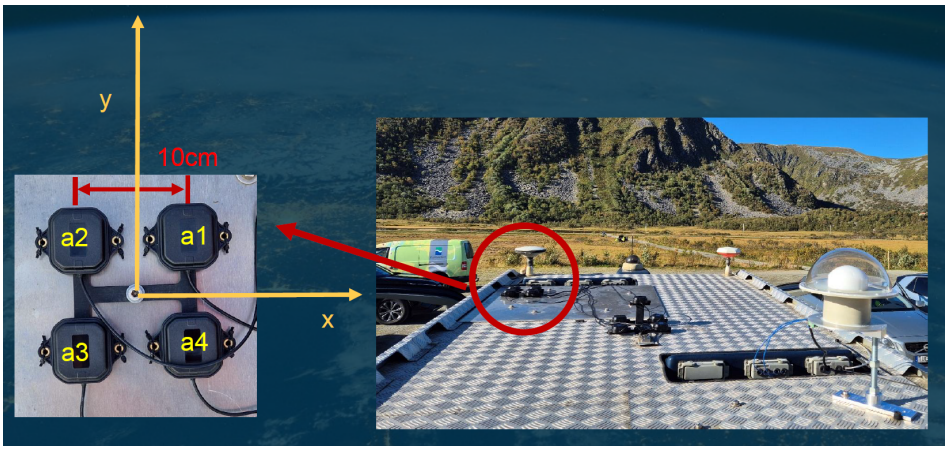


Figure 1: Illustration of the 2×2 patch antenna array on the roof of a vehicle and tracking GPS L1 C/A signals, used for Scenario 2A. Note that the x-y axes refer to a local (horizontal) coordinate system.

Problem B – Dynamic Receiver Positioning

In this task, participants were asked to estimate the true trajectory of a moving receiver affected by spoofing. As for the previous problem, the receiver was initially static and then moved along a known route. Only raw GNSS observations were provided between GPS Time 8:46:00 till 8:59:59 on September 12, 2024. Teams had to identify usable signals and apply advanced positioning techniques (Odijk, 2017), such as Precise Point Positioning (PPP) and Real-Time Kinematic (RTK), to recover the true path of the receiver with the highest possible precision. The signals available for the Scenario 2B are listed, per constellation, in the following Table 2.

Table 2: GNSS signals available for the victim receiver of the Scenario 2B, including RINEX codes.

Constellation	Band Name (Code)	Frequency (MHz)
G: GPS	L1 (1C)	1575.42
	L2 (2W/2L)	1227.60
	L5 (5Q)	1176.45
E: Galileo	E1 (1C)	1575.42
	E6 (6C)	1278.75
	E5a (5Q)	1176.45
	E5b (7Q)	1207.14
	E5 (8Q)	1191.795

Throughout the challenge, no prior information was given about the spoofing conditions. Therefore, teams had to independently detect spoofed signals, assess measurement quality, and infer the dynamics of both the spoofer and the receiver. The C/N_0 and Doppler measurements proved particularly useful in identifying spoofed signals and understanding the underlying motion patterns. An illustration of the two scenarios is shown in Figure 2.

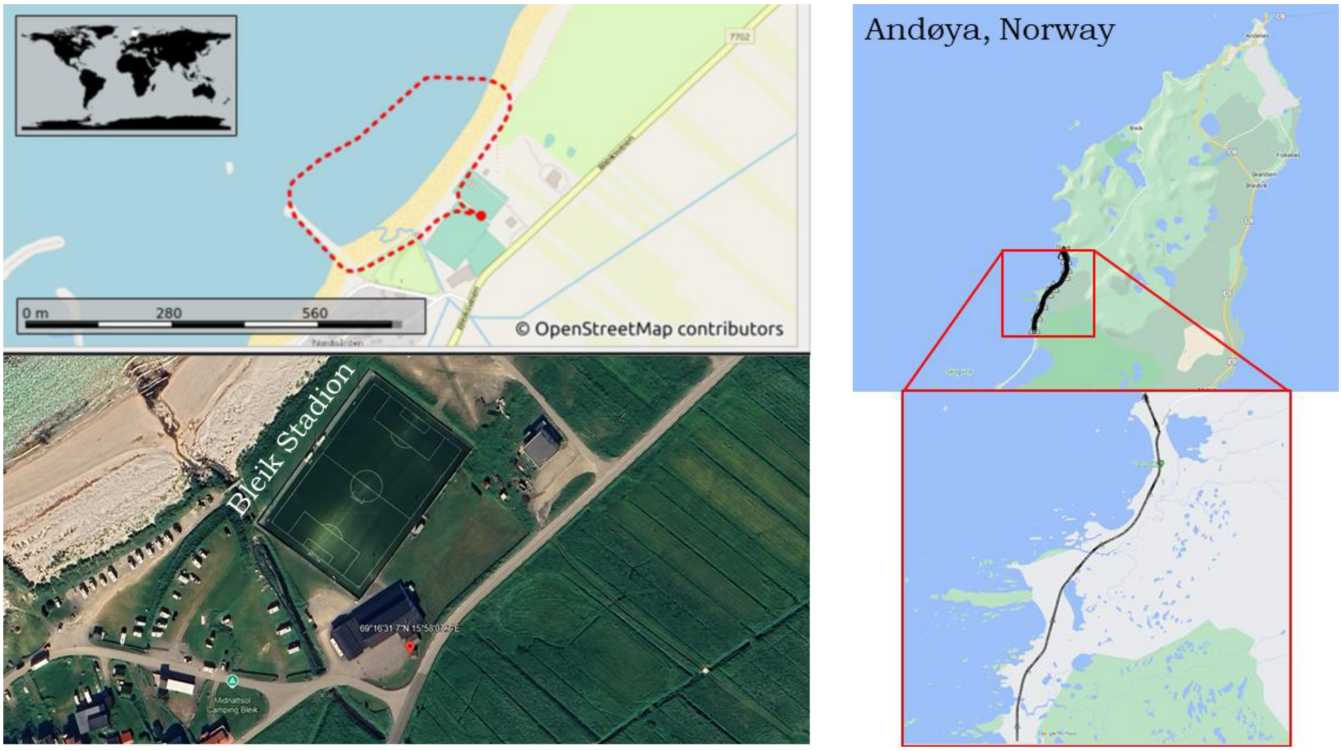


Figure 2: Graphical illustration of the two scenarios considered for the ESA's 'Resilient GNSS Challenge'. On the left: the static user location near Bleik Stadion used for Scenario 1 (including the spoofed trajectory in red dashed line). On the right: the dynamical user trajectory along Stavedalsveien considered for both problems of Scenario 2.

III. RESULTS AND SOLUTIONS

We present a summary of the main solutions developed by the three teams for the different problems. A very first step was to understand which type of attack was implemented in each case. This understanding included:

- **spoofing conditions**, concerning portions of the datasets that were actually affected by spoofing, distinguish between signals that were genuine or counterfeited;
- **dynamic conditions**, understanding if either the receiver or the spoofer were moving or kept static during the event;
- **measurement quality**, assessing which measurements could be trusted and which distortions were caused by spoofing.

Preliminary analyses and considerations

In all problems, the C/N_0 revealed to be effective in discriminating different dynamic conditions and indicating whether a set of signals was genuine or not. For instance, when both receiver and spoofer are kept static, the C/N_0 of the different signals changes gradually and is affected only by minor fades and variations. In contrast, larger and faster variations occur under fast dynamic conditions. Based on these preliminary considerations, it was possible to determine that the affected receiver was kept static for the entire duration of Scenario 1. On the other hand, the C/N_0 analysis for Scenario 2 revealed static conditions only during the first part. This is clearly visible in Figure 3, which shows the C/N_0 values of GPS L1 C/A signals tracked by the four antennas in the array system previously illustrated by Figure 1.

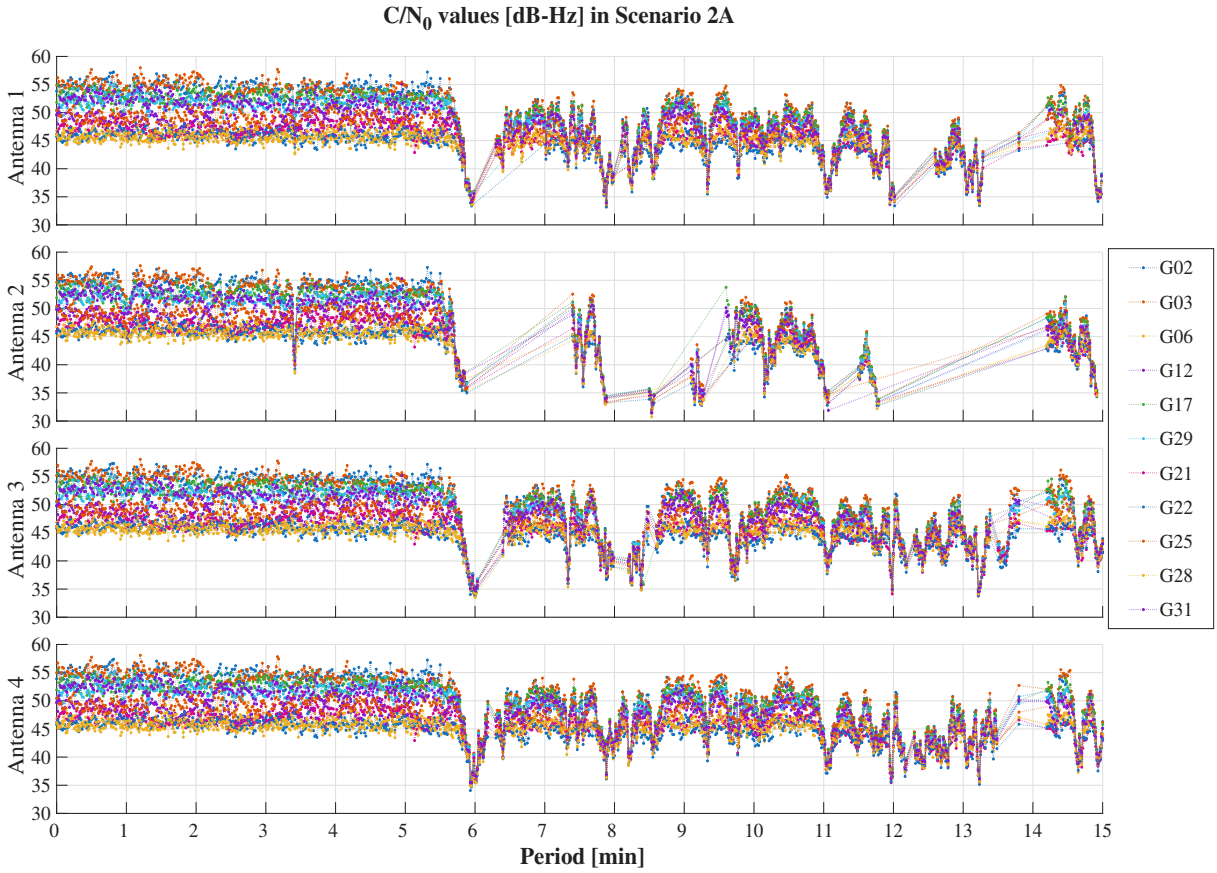


Figure 3: C/N_0 values of the GPS L1 C/A signals tracked by the four antennas in the 2×2 patch array system used in Scenario 2A.

The C/N_0 values characterizing the first part of the test are stable and affected only by reduced variations, which indicate the lack of relative dynamics between the receiver and the spoofer. After about 350 seconds from the start of the dataset, C/N_0 time series are affected by deep fades, often causing loss of signal lock, and larger oscillations. This indicates the presence of relative dynamics between spoofer and receiver. Signals generated by a spoofer equipped with a single antenna cross the same communication channel when they reach the victim receiver. Thus, they are affected by the same impairments and suffer correlated power changes. In this respect, C/N_0 values can be used for spoofing detection (Dehghanian et al., 2012). This fact also clearly emerges from Figure 3. During the dynamic portion of the test, the C/N_0 values of all the signals are affected by very similar fades confirming that all the received signals are actually counterfeited.
Although this method is effective in dynamic conditions, its reliability diminishes under static conditions, e.g., when both the receivers and the spoofer consistently occupy the same location. Therefore, the C/N_0 time series show fewer variations, as clearly visible in the first five minutes of Figure 3. While spoofing detection methods based on the C/N_0 can be generally adopted, more specific approaches can be selected depending on the problem. At this point, in the following sections we will further discuss results and solutions specific to each scenario.

Results for Scenario 1

As mentioned, the Scenario 1 was characterized by static conditions with measurements available from different constellations and frequencies (see Table 1). While only the GPS L1 C/A signals were spoofed, periodic jumps and noisy variations, in the order of kilometers, affected carrier phases and pseudoranges from all frequencies, making it unfeasible to obtain a valid position solution via standard techniques. These variations and jumps were likely due to the way receiver computed its local time. The GPS L1 C/A signals were likely used for clock steering and thus for the computation of the receiver time, so this scenario shows that a receiver time steered to spoofed signals can compromise pseudoranges and carrier phases from all frequencies. While receivers should ideally cross-check timing information coming from the different frequencies and signals (Kirkko-Jaakkola et al., 2017), this was not the case for the victim receiver in Scenario 1.

The only measurements not corrupted by spoofing were Doppler observations. This is due to that fact that the actual computation of such observable does not generally depend on the receiver time, which can be potentially steered to a spoofed signal. Through the analysis of Doppler data, it was therefore possible to identify which signals were completely spoofed. The principle adopted is shown in Figure 4, which shows the Doppler differences between rover and reference receivers.

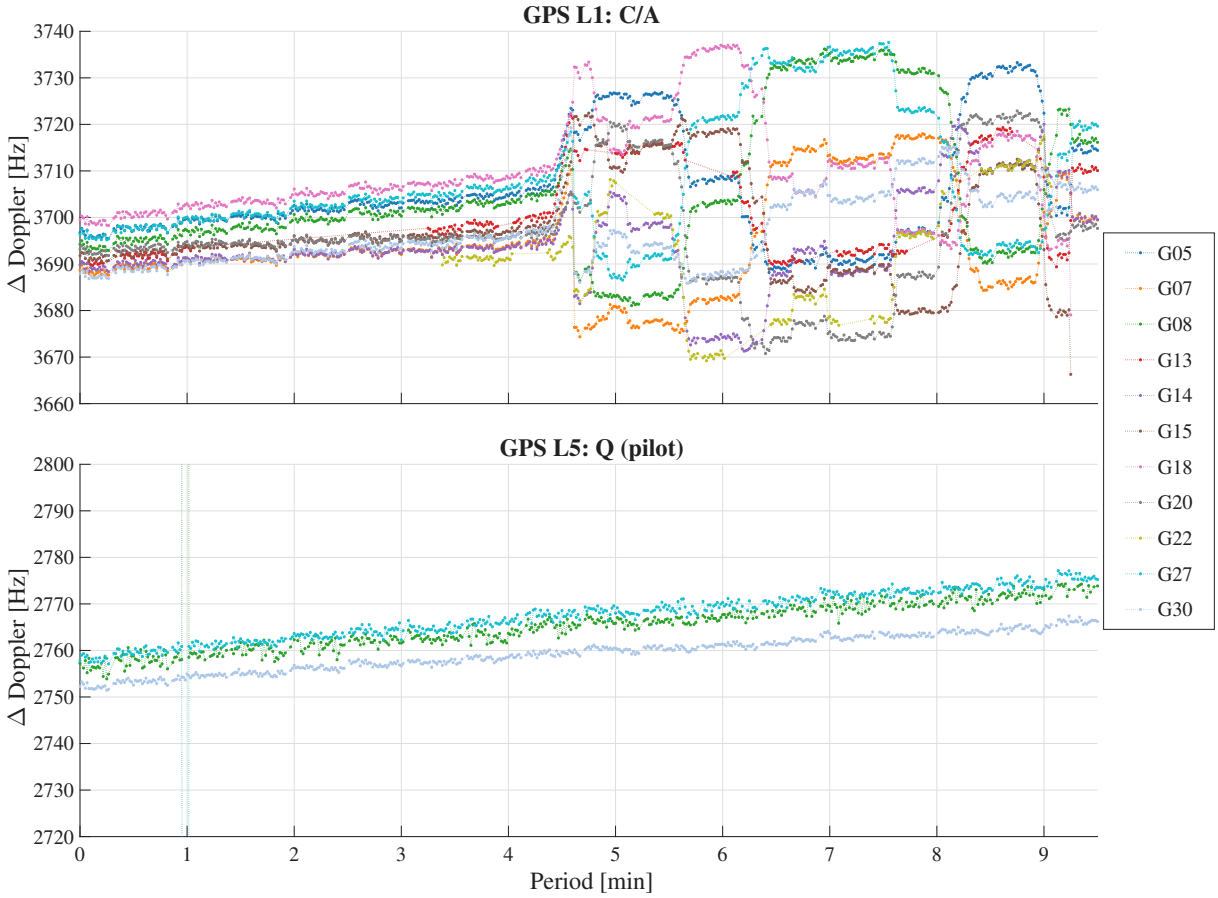


Figure 4: Doppler differences computed between measurements from the rover and reference receiver in Scenario 1. Top and bottom panels refer to GPS L1 C/A and L5 measurements, respectively.

For nearby receivers, Doppler differences should reflect the relative motion between receivers plus the difference between receiver clock drifts. Doppler components from GPS L1 C/A signals indicate that the user should be moving during the second part of the test while the C/N_0 time series of Scenario 1 suggested a static receiver. Therefore, the spoofer was trying to make the receiver believe to be a drone performing periodic loops: the oscillations in the Doppler differences clearly visible in the upper part of Figure 4 are the direct consequence of the spoofing attack. All other Doppler differences, such as those shown in the bottom part of Figure 4, are characterized by parallel linear trends, which are driven by the receiver clock drifts. These results confirm the potential of Doppler measurements for spoofing detection (Zhou et al., 2022). Ultimately, both Doppler and C/N_0 measurements should be used jointly to determine inconsistent dynamic conditions (Wei et al., 2024).

Following the previous considerations, GPS L1 C/A measurements were discarded, and the remaining Doppler observations – not affected by spoofing – were used to compute a Doppler-based navigation solution. The algorithm originally developed for Low Earth Orbit (LEO) satellites by Psiaki (2021) was adapted here to the specific scenario and it allowed the computation of the static position solution. The time series of positioning errors based on this Doppler positioning is shown in Figure 5, for ENU and 3D components. Even if errors up to 200 meters were found, this Doppler-based positioning was - in the best of our knowledge - the only approach able to overcome the challenging spoofing conditions given for Scenario 1. The position solution in Figure 5 was obtained using the Kalman filter-based approach from Psiaki (2021), but more complex approaches might be adopted. For instance, the knowledge of a static receiver allows the implementation of multi-epoch batch solutions, nonetheless such advanced strategies were not explored in the time frame of the ESA challenge.

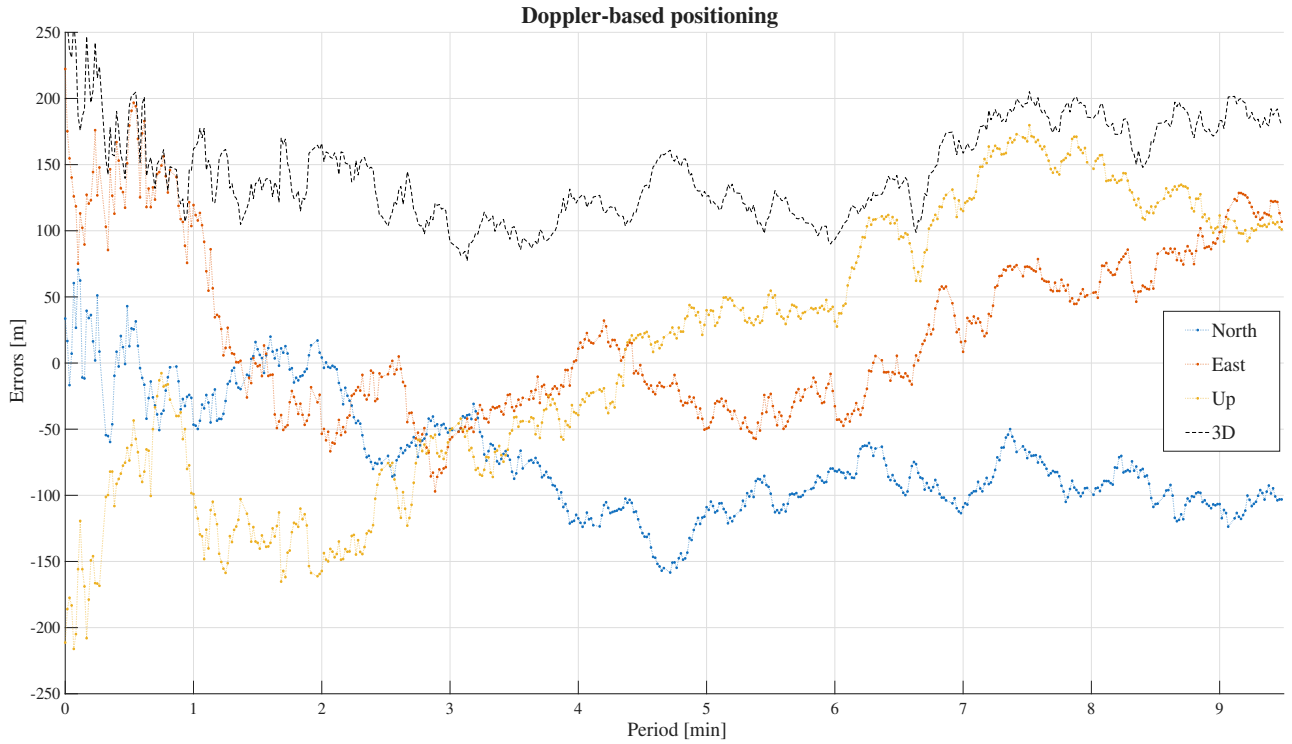


Figure 5: Positioning errors in East-North-Up and 3D components using Doppler measurements in Scenario 1.

Results for Scenario 2

In the Scenario 2, we have two separate problems.

Problem 2A: Spoofer Azimuth Estimation

This problem involves the estimation of the spoofer AoA (azimuth), with respect to the local frame of a 2×2 patch antenna array. As discussed in Section III, a first analysis phase was conducted to determine the actual conditions and quality of the measurements. The C/N_0 analysis revealed that all the measurements available for the first problem of Scenario 2 were actually spoofed and that no genuine observation was present in the dataset. This fact was also confirmed by the analysis of the carrier phase measurements. A simple approach based on carrier-phase double differences (Borio and Gioia, 2016) allowed the teams to clearly confirm that all the signals were spoofed for the whole duration of the experiment. Indeed, carrier-phase double differences showed that all the signals were coming from the same direction, i.e. the spoofer AoA. Moreover, this analysis also revealed that measurements could be potentially affected by half-cycle ambiguities. In order to obtain a reliable AoA estimation algorithm, this effect needed to be accounted for.

While different approaches were tested by the different teams only the most performing one is described here. This approach adopted a between-receiver single-difference model relying on carrier-phase differencing. It allowed the mitigation of common mode errors across the four antennas of the array system. In this case, C/N_0 values were also incorporated as a weighting factor for the contributions to the AoA estimation from the different spoofed signals. C/N_0 data contain useful information regarding the measurement quality and the weighting scheme adopted ensures that higher quality signals carried proportionally greater influence on the estimated AoA. This method proved to reliably detect suspicious AoA patterns, enhancing situational awareness under such spoofing scenarios.

For each satellite s, the single-differenced (SD) carrier-phase L1 observation between receivers a and b at time k is

$$\Delta\phi^s_{ab}(k) \;=\; \phi^s_a(k) - \phi^s_b(k) \;=\; \frac{2\pi}{\lambda}\, b^T_{ab}\, u^s(k) + B^s_{ab}(k) \;+\; \varepsilon^s_{ab}(k), \tag{1}$$

with baseline vector b_{ab}, and $u^s(k)$ is the unit direction vector to the signal source, B^s_{ab} is the SD phase ambiguity together with the bias terms (e.g., between-receiver hardware delays) assumed constant over a continuous arc and λ is the wavelength related to GPS L1 signal. The direction is identical for every PRN when the signals are spoofed by a single transmitter.

To simplify the model for linear estimation, the bias terms are assumed to be constant across the measured baselines, such that $B^s_{12}(k) = B^s_{13}(k) = B^s_{14}(k) = B^s(k)$. Note that, unlike conventional GNSS processing, the line-of-sight vectors do not relate each observation to the corresponding satellite, but rather to the spoofer. Also, the four receivers worked under the same clock, for which the clock offset disappear after the differencing.

At each epoch, we stack the SD phase observations with respect to a reference antenna (#1), such that

$$\boldsymbol{y}(k) \;=\; \begin{bmatrix} \Delta\phi^s_{12}(k) \\ \Delta\phi^s_{13}(k) \\ \Delta\phi^s_{14}(k) \end{bmatrix}, \qquad \boldsymbol{A} \;=\; \begin{bmatrix} b^T_{12} & 1 \\ b^T_{13} & 1 \\ b^T_{14} & 1 \end{bmatrix}, \qquad \boldsymbol{W}(k) = \begin{bmatrix} w_{12}(k) & 0 & 0 \\ 0 & w_{13}(k) & 0 \\ 0 & 0 & w_{14}(k) \end{bmatrix}, \tag{2}$$

with

$$w_{1j}(k) \;=\; \frac{\bar{S}_{1j}(k)}{\max\limits_{j\in\{2,3,4\}} \bar{S}_{1j}(k)}, \qquad \bar{S}_{1j}(k) \;=\; \frac{S^s_1(k) + S^s_j(k)}{2},$$

where $S^s_j(k)$ is the C/N_0 observed for satellite s and antenna j at each epoch k. With this choice, each diagonal element is the average C/N_0 of the two antennas normalized by the largest average. The (weighted) least-squares solution follows as

$$\hat{u}^s(k) \;=\; \left(\mathbf{A}^T\mathbf{W}(k)\mathbf{A}\right)^{-1}\mathbf{A}^T\mathbf{W}(k)\mathbf{y}(k), \tag{3}$$

and we repeat the process per each epoch, thus computing

$$\alpha^s(k) \;=\; \text{atan2}\big(\hat{u}^s_y(k),\, \hat{u}^s_x(k)\big), \tag{4}$$

where α^s refers to the time-varying azimuth angle.

The results from the AoA estimation process are presented in Figure 6, focusing on each GPS satellite (left panel) and on the combined estimation (right panel). Despite the varying geometry of the GPS satellites, all the estimates converge to very similar azimuth values $\hat{u}^s(k), \forall s$, which is a good indication of a common bearing source. The individual satellite directions were combined by leveraging the signal quality of each satellite in the final estimated solution, thereby minimizing the impact of possible outliers from any single satellite. C/N_0 values are leveraged twice in the computation. Initially, C/N_0 values are used at each epoch and satellite as described in Eq.(2) – weighting matrix $\mathbf{W}$ is normalized by the maximum values – and later in the aggregation phase to compute the final heading. Once individual azimuth angles are obtained, the same C/N_0 values are reused as scalar weights in a simple weighted mean that combines all satellites' azimuth into one array-based heading.

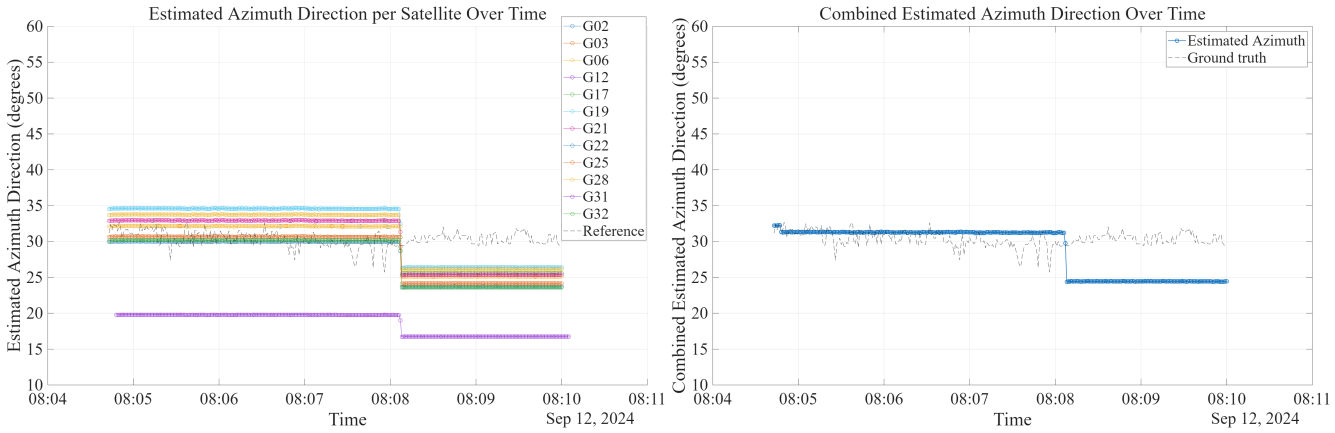


Figure 6: Results of the Angle-of-Arrival (AoA) estimation process in Scenario 2A using the different satellites separately (left panel) and using a joint estimation process (right panel). See text for more details.

Problem 2B: Dynamic Receiver Positioning

In the last problem of the competition, relative to Scenario 2B, the objective was again to estimate an accurate positioning for a dynamic user. The preliminary analysis of C/N_0 values revealed that authentic Galileo E5Q, E7Q and E6C signals were received. On the contrary, GPS L1 C/A and Galileo E1 signals were characterized by highly correlated C/N_0 values, thus resulting in the precise positioning algorithms failing to converge when utilizing these measurements. Instead, by using Galileo triple-frequency signals (E5Q, E7Q and E6C), it was possible to roughly determine the user position.

A few different approaches were attempted, for instance using:

1. **Single Point Positioning (SPP)**, where only code data and broadcast ephemerides are adopted in epoch-wise estimation;
2. **Precise Point Positioning (PPP)**, where precise satellite products are used together with code-phase measurements;
3. **Real-Time Kinematics (RTK)**, where DD observations with a nearby ground station are used for the baseline solution.

However, the SPP solution was less likely suitable for high-accuracy kinematic user positioning. Consequently, only PPP and RTK methods were utilized, whereas in both cases no integer ambiguity resolution (IAR) was attempted.

Precise Point Positioning (PPP) Solution

All processing steps of PPP follow the classic formulation (Odijk, 2017), with code-phase observations given as

$$p^s_{r,j} = \rho^s_r + \left(dt_r - dt^s\right) + m^s_T\tau_r + I^s_{r,j} + \left(d_{r,j} - d^s_{,j}\right) + e^s_{r,j}, \tag{5}$$

$$\phi^s_{r,j} = \rho^s_r + \left(dt_r - dt^s\right) + m^s_T\tau_r - I^s_{r,j} + \left(\delta_{r,j} - \delta^s_{,j}\right) + \epsilon^s_{r,j} + \lambda_j N^s_j, \tag{6}$$

where ρ^s_r is the geometric range from $r$eceiver to $s$atellite, then $\left(dt_r - dt^s\right)$ is the receiver–satellite clock offset, τ_r is the vertical tropospheric delay mapped into slant by the elevation-dependent mapping function $m^s_T = m^s_T(el^\circ)$, $I^s_{r,j}$ is the ionospheric slant delay on the j-th frequency, $\left(d_r - d^s\right)$ and $\left(\delta_r - \delta^s\right)$ are respectively code and phase hardware delays, and N^s_j is the integer ambiguity with the wavelength λ_j.

The measurement noises, here assumed zero-mean Gaussian distributed, are given by $e^s_{r,j}$ for code and $\epsilon^s_{r,j}$ for phase, and are further scaled by an elevation weighting scheme so that low-elevation observations contribute less. The Kalman filter is driven by a Galileo-only solution, based on a triple-frequency (E6C, E5Q and E7Q) dataset. The carrier-phase ambiguities are not fixed here and therefore remain float values.

Real-Time Kinematic (RTK) Solution

RTK is a differential positioning technique that can provide millimeter to centimeter-level positioning once the phase ambiguities are resolved to their correct integer number of cycles. In the data processing for this problem, we used the single-baseline double-differenced (DD) observation model as described in (Odijk, 2017). The reference station we used is AND100NOR, and is co-located with a tide gauge for sea level monitoring, and its observations can be downloaded from SONEL (Système d'Observation du Niveau des Eaux Littorales, https://www.sonel.org). Due to its functionality, AND100NOR is installed next to the sea and thus suffers from strong multipath errors caused by signals reflected from the sea.

While, this is ideal for sea level monitoring by GNSS interferometric reflectometry, or GNSS-IR, it is not well-suited for user positioning applications. Nevertheless, by differencing the observations from the reference station and the receiver, the satellite clock offset and hardware delays can be eliminated, and atmospheric delays can also be reduced, benefiting from the short baseline length of around 17.5 km between the ground station and the moving receiver (under spoofing). The DD observation equations for pseudorange and carrier-phase are given by

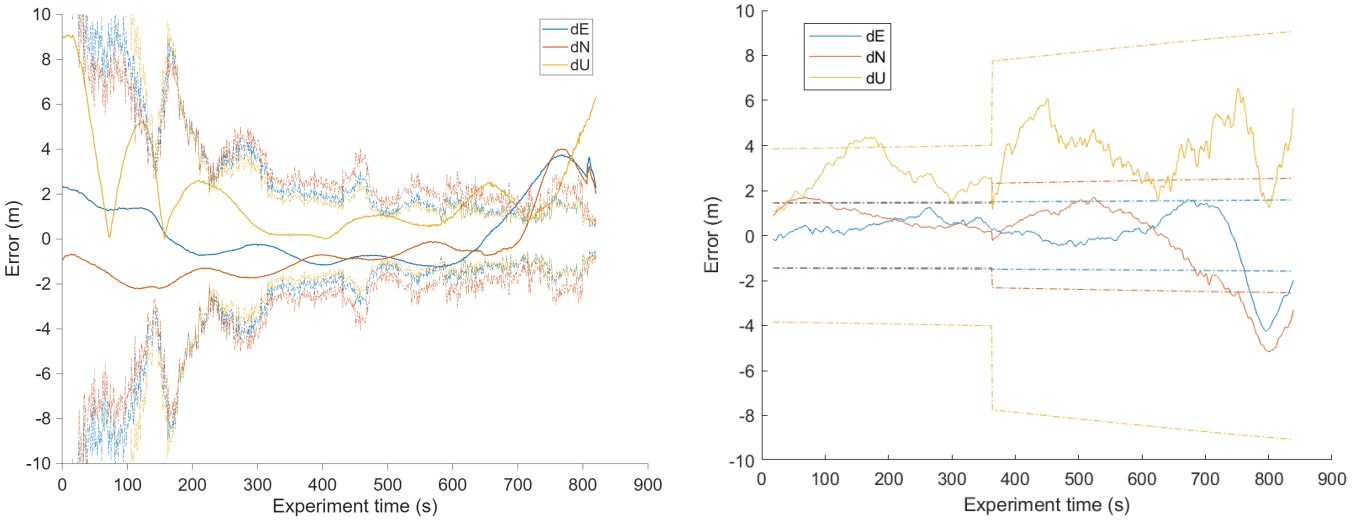
$$p^{1s}_{1r,j} = \rho^{1s}_{1r} + e^{1s}_{1r,j}, \tag{7}$$

$$\phi^{1s}_{1r,j} = \rho^{1s}_{1r} + \epsilon^{1s}_{1r,j} + \lambda_j N^{1s}_{1j}, \tag{8}$$

where satellite 1 (in superscript) is selected as the reference satellite and 1 in subscript denotes the reference station. The ρ^{1s}_{1r} and N^{1s}_{1j} denote the DD geometric range and ambiguity, respectively. The atmosphere delays are assumed to be canceled out. In the stochastic model, the zenith-referenced undifferenced pseudorange and carrier phase standard deviations are set to be 30 cm and 3 mm, and elevation-dependent weight is applied (Eueler and Goad, 1991). As for the PPP case, triple-frequency Galileo measurements (E6C, E5Q, E7Q) are used in data processing.

Positioning Results

The positioning errors in the local East North Up (ENU) frame are shown in Figure 7 for both the PPP and RTK solutions, respectively in the left and right panels. Errors are at meter level, potentially due to the lower quality of measurements assumed not to be spoofed during the experimentation period. Still, such results were not investigated in the context of the challenge (due to time limitations) and should further be examined in future work.



(a) PPP solution

(b) RTK solution

Figure 7: Errors and 3-sigma curves in East-North-Up (ENU) local frame are shown for PPP (left panel) and RTK (right panel) solutions adopted in Scenario 2B, both based on Galileo-only triple-frequency data with E6C, E5Q, and E7Q signals.

IV. SUMMARY

Initiatives such as the Norwegian Jammertest campaign and ESA's 'Resilient GNSS Challenge' are of paramount importance to create awareness among the scientific community, better understand threats such as jamming and spoofing events, along with fostering collaboration among research institutions. Their positive impact can also be amplified through the publication of open data and problem solutions, while a larger involvement of GNSS/PNT communities is surely beneficial in the definition of new methodologies, along with potential novel technologies in response to such threats expected to become more and more common in the next years.

In this work we presented the results from the NAVITEC 2024 competition, which took place at the end of 2024 and it was organized by the European Space Agency (ESA). The competition consisted of two scenarios with a total of three problems, which have been discussed in this contribution, where we described the datasets made available and methodologies adopted by the top three teams.

A summary of results follows:

- In **Scenario 1**, a static receiver was spoofed on GPS L1 consequently affecting all code and phase data. Therefore, only a Doppler-based positioning was possible, based on methodologies developed by Psiaki (2021), however here with errors at the level of hundreds of meters.
- In **Scenario 2A**, four antennas in a 2×2 patch array system were considered, this time limited to single-frequency data. The analysis of C/N_0 in Figure 3 revealed that receiver was most likely static over the first 5-6 minutes, and consistency among all satellites demonstrated how all signals were actually spoofed. By means of single-differenced between-receiver phase data, it was possible to determine the AoA of the spoofer, even if some issues were introduced by half-ambiguity problems in single or multiple receiver antennas.
- In **Scenario 2B**, multi-GNSS and multi-frequency data was available from a receiver initially static, then moving along Stavedalsveien (Norway) at approximately 40 km/h. After excluding GPS L1 and Galileo E1 signals, both spoofed with highly correlated C/N_0 values, it was possible to compute a positioning solution at meter level with PPP and RTK methodologies, unfortunately not further investigated during the competition.

Overall, one key element in the approach adopted by all teams was to consider the analysis of C/N_0 values for all frequencies, and in this way it was possible to infer which signals were spoofed, and also if receiver was likely static or moving. Ultimately, for a resilient solution under spoofing conditions, this preliminary analysis proved to be fundamental for many of the teams and therefore it should further be investigated, e.g., in the context of real-time strategies, thus supporting future safety-critical positioning applications.

ACKNOWLEDGEMENTS

We would like to thank Xurxo Otero Villamide, Luciano Musumeci, and Cecilia Kalmeijer for their valuable contributions to the organization of the ESA's 'Resilient GNSS Challenge', as well as all other participating teams.

DISCLAIMER

The content of the present article reflects solely the authors' view and by no means represents the official ESA view.

REFERENCES

BniLam, N. and Crosta, P. (2024). Resilient GNSS coarse positioning based of angle of arrival estimates. In *2024 11th Workshop on Satellite Navigation Technology (NAVITEC)*, pages 1–5. IEEE.

BniLam, N., Principe, F., and Crosta, P. (2023). Large array antenna aperture for GNSS applications. *IEEE Transactions on Aerospace and Electronic Systems*, 60(1):675–684.

Borio, D., Dovis, F., Kuusniemi, H., and Lo Presti, L. (2016). Impact and detection of GNSS jammers on consumer grade satellite navigation receivers. *Proceedings of the IEEE*, 104(6):1233–1245.

Borio, D. and Gioia, C. (2016). A sum-of-squares approach to GNSS spoofing detection. *IEEE Transactions on Aerospace and Electronic Systems*, 52(4):1756–1768.

Dehghanian, V., Nielsen, J., and Lachapelle, G. (2012). GNSS spoofing detection based on receiver C/N_0 estimates. In *Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS)*, pages 2878–2884, Nashville, TN, USA.

Eueler, H.-J. and Goad, C. C. (1991). On optimal filtering of GPS dual frequency observations without using orbit information. *Bulletin Géodésique*, 65:130–143.

Heijnen, S., Sleewaegen, J., and Heijnen, S. (2025). Jamming mitigation performance analysis of a state-of-the-art multi-band receiver module. In *Proceedings of the European Navigation Conference ENC*, Wroclaw, Poland.

Jammertest Consortium (2024). Jammertest 2024 Test Catalogue. `https://jammertest.no/content/files/2025/02/Testcatalog.pdf`. Accessed: 2024-10-14.

Kirkko-Jaakkola, M., Thombre, S., Honkala, S., Soderholm, S., Kaasalainen, S., Kuusniemi, H., Zelle, H., Veerman, H., Wallin, A., Aarmo, K. A., and Boyero, J. P. (2017). Receiver-level robustness concepts for EGNSS timing services. In *Proceedings of the 30th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+)*, pages 3353–3367, Portland, OR, USA.

Lo, S., Liu, Z., Ibrahim, L., Chen, Y. H., and Walter, T. (2025). Observations of GNSS spoofing in Russia in 2023-2024. In *Proceedings of the International Technical Meeting ITM of The Institute of Navigation*, pages 425–442, Long Beach, CA, USA.

Odijk, D. (2017). Positioning model. In *Springer Handbook of Global Navigation Satellite Systems*, pages 605–638. Springer.

Psiaki, M. L. (2021). Navigation using carrier Doppler shift from a LEO constellation: Transit on steroids. *NAVIGATION*, 68(3):621–641.

Psiaki, M. L. and Humphreys, T. E. (2016). GNSS spoofing and detection. *Proceedings of the IEEE*, 104(6):1258–1270.

Wei, X., Sun, C., Li, X., and Ma, J. (2024). GNSS spoofing detection for UAVs using Doppler frequency and carrier-to-noise density ratio. *Journal of Systems Architecture*, 153:1–11.

Zhou, Z., Li, H., Chen, Z., Zhong, M., and Lu, M. (2022). GNSS spoofing discrimination based on Doppler residual monitoring. In *Proceedings of the International Technical Meeting (ITM) of The Institute of Navigation*, pages 168–181, Long Beach, California, USA.