

1

# Descriptor: *Tuni2025 GNSS - Galileo and GPS Spoofing Datasets (TG-GGSD)*

S.M.U. RAHMAN<sup>1</sup>, M. Zahidul H. BHUIYAN<sup>2</sup> (MEMBER, IEEE), J. NURMI<sup>1</sup> (SENIOR MEMBER, IEEE), AND E.S. LOHAN<sup>1</sup>, (SENIOR MEMBER, IEEE)

<sup>1</sup>Tampere Wireless Research Center, Electrical Engineering Unit, Tampere University, Finland

<sup>2</sup>Finnish Geospatial Research Institute, National Land Survey, Finland

CORRESPONDING AUTHOR: S.M.U Rahman (e-mail: syed.urrhman@tuni.fi).

**ABSTRACT** The Tuni2025 GNSS spoofing datasets provide raw in-phase and quadrature (I/Q) measurement data from Global Navigation Satellite System (GNSS) signals to support research in spoofing detection and signal authentication. It includes a total of 17 scenarios: eight for Galileo signals and nine for GPS signals, featuring static spoofing attacks, both with and without multipath. One GPS scenario includes also a delayed spoofer activation with all PRNs spoofed, allowing for a time-segmented analysis. The spoofer signals are generated in-lab with a Spectracom signal generator, while the genuine GNSS signals are collected from the sky, via a roof-top GNSS antenna.

The data was collected using a USRP NI-2954 software-defined radio (SDR) and a NovAtel GNSS-703 antenna, with a high sampling rate of 50 MHz, to allow high-resolution studies. The spoofing signal was generated with a Spectracom GSG-6 signal generator targeting the GPS L1 and Galileo E1 signals. The pseudorandom codes (PRNs) for the spoofed signals were intentionally generated to be distinct from the genuine PRNs visible at the time of the data collection, in order to enable further investigations of hardware-induced impairments and spoofing signal behavior via Radio Frequency Fingerprinting Identification (RFFI) approaches. Our datasets are unique in this aspect, as they include up to five spoofed PRNs co-existing with genuine PRNs and therefore allowing for a ground truth in spoofing PRN detection, unlike few other existing datasets in the literature that superpose fake and genuine signals with the same PRNs.

Each scenario is provided as a standalone raw binary file, accompanied by a detailed README file that describes its structure, its PRN configuration, the sampling parameters (sampling frequency and number of quantization bits), and some file interpretation guidelines. No scenario control files or software scripts are included. The dataset is intended for reproducibility in spoofing-detection algorithm testing, RFFI studies, and data-driven modeling of spoofing environments in GNSS systems.

**IEEE SOCIETIES/COUNCILS** Aerospace and Electronic Systems Society (AESS); Communications Society (ComSoc) and Signal Processing Society (SPS)

**DATA DOI/PID** 10.5281/zenodo.15470142, 10.5281/zenodo.15572975

**DATA TYPE/LOCATION** Binary I/Q raw data (readable with the open-access FGI-GSRx Open Source multi-GNSS software receiver) / Tampere University Campus and neighborhoods, Tampere, Finland

**INDEX TERMS** Authentication, Asynchronous Spoofing, Galileo, GNSS, GPS, open-source, Positioning, Velocity and Timing (PVT), Radio Frequency Fingerprinting Identification (RFFI), satellite raw I/Q data, signal processing

## BACKGROUND AND MOTIVATION

Spoofing attacks in Global Navigation Satellite Systems (GNSS) have increased over the past few years [1]–[3]. Spoofing in GNSS refers to the situation when a malicious player tries to impersonate a genuine GNSS signal with the aim of deceiving the receiver about its position, velocity, or time. In order to detect and possibly mitigate spoofing, recent research work has focused on identifying unique and intrinsic physical-layer features of the transmitted signals, and in particular those caused by hardware imperfections on the transmitter side [3], [4]. Such hardware imperfections, called Radio Frequency Fingerprints (RFF) can be caused, for example, by the power-amplifiers non-linearities, the I/Q imbalances in the front-end mixers, the phase noises in the local oscillators, or distortions introduced by the Digital-to-Analog-Converters (DAC) and other analogue filters [5].

Despite several recent advancements, the research community in Radio Frequency Fingerprinting Identification (RFFI) for GNSS spoofing detection and mitigation faces a significant bottleneck: the lack of high-fidelity, publicly accessible datasets that capture GNSS spoofing under realistic and varied conditions. Existing repositories like TEXBAT [6] and OAKBAT [7] have provided valuable early foundations, but have low sampling rate, synchronous spoofing of all PRNs, and no multipath addition to spoofer signals. Moreover, OAKBAT datasets have now been restricted to private use and are no longer available in full open access as of July 2025. As shown in Table 1, our Tuni2025 GNSS spoofing datasets [8], [9] address these limitations by offering 17 controlled scenarios across GPS and Galileo signals, captured at 50 MHz sampling rate, with a static receiver, both in single-path and multipath conditions, as well as using a variable number of PRN spoofed signals (i.e., selective PRN spoofing) and delayed injection conditions. We are proving in our data 17 carefully controlled spoofing scenarios targeting both Galileo E1 and GPS L1 bands. This makes our datasets particularly valuable for developing and benchmarking advanced spoofing detection methods based on statistical signal modeling, machine learning, or RF fingerprinting.

Ultimately, the motivation behind Tuni2025 GNSS spoofing datasets is to promote reproducible research, enable rigorous testing of spoofing detection algorithms, and encourage the development of more robust GNSS receivers capable of distinguishing between authentic and malicious signals. By sharing detailed documentation along with the raw data, our datasets may also serve as a reference point for future spoofing measurement campaigns which can be helpful in applications related to critical infrastructures like grid stations, telecommunications network which are stationary and also help us understand the limit of RFF fingerprinting in dynamic cases.

The main novelty of our paper stems from the data itself, as its added value compared to other existing I/Q raw datasets in the literature is provided in Table 1. An additional novel point lies in the well-documented measurement

methodology. It is to be noted in the last row of Table 1 that no research papers have used our data yet, because it is still very new.

## COLLECTION METHODS AND DESIGN

The Tuni2025 GNSS spoofing datasets were generated through a carefully designed in-lab measurement setup at Tampere University, producing asynchronous spoofing scenarios with a high sampling rate, incremental spoofing PRNs, and multipath spoofer signals. The primary objective was to capture raw in-phase and quadrature (I/Q) GNSS signal samples for both spoofed and authentic signals in laboratory settings.

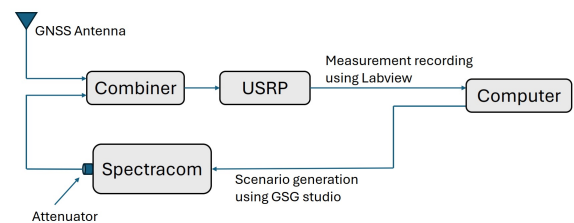


FIGURE 1. Block diagram of hardware setup

The comprehensive setup used for signal acquisition is illustrated in Figure 1, which shows a block diagram of the hardware components. The setup integrates a live-sky GNSS antenna (NovAtel GPS-703-GGG) with a Spectracom GSG-6 GNSS signal generator. The live signal from the rooftop antenna travels through a 91-meter coaxial cable having an attenuation of 0.33 dB/m and is amplified using a Low-Noise Amplifier (LNA) to compensate for signal attenuation. Simultaneously, the Spectracom signal generator generates spoofed signals for GPS L1 and Galileo E1 bands. These two signals are then merged using a Mini-Circuits ZN2PD2-63-S+ RF splitter and recorded using a USRP NI2954R.

An important consideration in this setup was the difference in signal powers between the simulated and real signals. The Spectracom signal generator outputs the spoofed signals at approximately  $-100$  dBm per satellite, while the authentic GNSS signals received via the antenna typically arrive at  $-130$  dBm or weaker. To prevent the spoofed signals from overpowering the authentic signals in order to replicate realistic scenarios, a 20 dB attenuator was installed at the Spectracom signal generator output. This ensured a balanced and realistic signal power mix at the input of the recording device, allowing both genuine and spoofing signals to be captured by the receiver without saturation of the spoofed component.

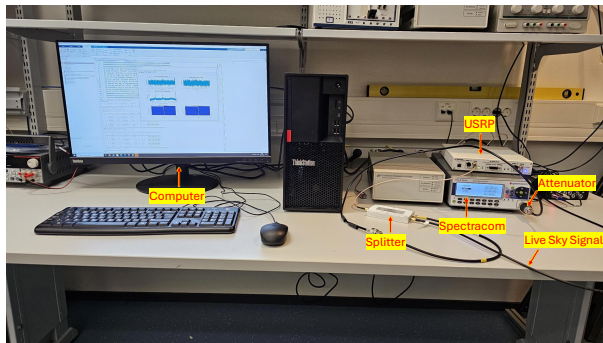
Figure 2 presents the actual physical implementation of the test bench in the lab, highlighting the connections between the Spectracom signal generator, USRP, RF splitter, and the controlling PC. The PC runs the LabVIEW software which was used to configure the USRP-2945R device for capturing raw I/Q data. Each dataset was recorded at a

**TABLE 1.** Comparison of Tuni2025 GNSS spoofing datasets with other open-access GNSS spoofing datasets available in the current literature.

Characteristics	Textbat [6]	Oakbat* [7]	ESA EWF [10]	FGI1 [11]	FGI2 [12]	Tuni2025 GNSS (this paper) [8], [9]
Spoofed Constellation	GPS	GPS, GAL	GPS, GAL	GPS, GAL	GPS, GAL	GPS, GAL
Frequency Bands	L1	L1/E1	L1/E1, L5	L1/E1, L5/E5a	L1/E1	L1/E1
Sampling Frequency	25 MHz	5 MHz	90 MHz	26 MHz	30.69 MHz	50 MHz
Complex Quantization Level	32 (I+Q)	32 (I+Q)	32 (I+Q)	8 (I only) for L1/E1 and 16 (I+Q) for E5a/L5	16 (I+Q)	32 (I+Q)
Duration per dataset	468 s	468 s	100 ms	370 s	400 s and 896 s	150 s
Spoofed PRNs	All PRNs	All PRNs	1 PRN	All PRNs	All PRNs	1-5 and All PRNs
Number of Scenarios	6	12	39	4	2	17
Multipath	No	No	No	No	No	Yes, limited
Receiver Mobility	Static, Dynamic	Static, Dynamic	Static	Static	Static, Dynamic	Static
Year of measurements	2012	2020	2022	2023	2023	2025
Location	Texas, USA	Tennessee, USA	Noordwijk, Netherlands	Espoo, Finland	Andøya, Norway	Tampere, Finland
Examples of spoofing-related research based on this data	[13]	[14]	[15]	[16]	[17]	N/A

\*It is to be noted that Oakbat is no longer available in open-access as of July 2025.

sampling frequency of 50 MHz with a 32-complex-bit resolution (namely 16-bit for I and 16-bit for Q components). The recordings were stored as binary files, accompanied by detailed metadata files describing scenario ID, spoofed PRNs, receiver position, and signal parameters, and our recordings are fully compatible with the open-source FGI-GSRx software-defined GNSS receiver processing [18].



**FIGURE 2.** Complete hardware setup

The spoofing scenarios were created using the GSG StudioView software. These scenarios include a static receiver location at the true position of the GNSS antenna at the same place and spoofing in the presence or absence of simulated multipath reflections. The simulated Spectracom signals are generated at the exact same location of the receiving GNSS

antenna. Real navigation data are included in the spoofing signals in all the scenarios. The navigation data are taken from the NASA repositories and the position of the satellites is driven from that navigation data. In terms of spoofing PRNs, they were artificially and intentionally chosen to be distinct PRNs from those visible the sky. While this would make a position fix impossible in the spoofing case, this would ensure that spoofing and clean PRNs are never the same and it will enable accurate studies of RF fingerprinting in pre-correlation and post-correlation domains. This is a unique characteristic that no other available datasets in the open access has, and it is a strong enabler of the possibility to develop RFF mechanisms with clear labels: spoofed versus non-spoofed PRNs. For example, in Textbat and Oakbat datasets, when spoofers are present, they are spoofing exactly the same PRNs from the sky, therefore, one cannot put a PRN-level accurate label whether a PRN is coming from a spoofer or a clean signal, as exactly the same PRN identifies both the clean and the spoofed signals. In our approach and datasets (with the exception of SS-33 scenarios), each PRN has a clear label: it is either coming from a spoofing signal or from a clean signal. The dataset SS-33 (GPS delayed spoofing, all PRNs) is the only case where exactly the same PRNs from the clear sky were also spoofed, through a meaconing approach, and this case was also added as the reference the closest to other datasets available in open access, such as

Texbat and Oakbat. Therefore, the spoofed PRN indices were carefully selected to allow per-PRN analysis, in such a way that we have a unique label per PRN code (i.e., either clean signal or spoofed signal) in all cases except the last case (SS-33) of GPS delayed spoofing, where spoofing signals were also generated by the Spectracom, and then injected into the receiver by physically adding the Spectracom output cable to the Mini-Circuits ZN2PD2-63-S+ RF splitter after a certain duration while recording the scenario. A total of 17 scenarios were captured—eight for Galileo and nine for GPS—each with a duration of 150 seconds per scenario. The Spectracom signal parameters and antenna parameters are provided in Table 2 and further details about each scenario are provided later, in Table 3.

**TABLE 2. Spectracom signal parameters and antenna parameters**

Parameter	Value
Transmit Power per Satellite	-100 dBm
Carrier-to-Noise density ratio	40 dB-Hz
Sky Elevation Limit	10 Degree
Propagation Model	Open Sky
Ionospheric Model	Klobuchar
Tropospheric Model	Saastamoinen
Antenna model	GPS-703-GGG
Simulated Receiver Movement	Static
Receiver Position	Real
Multipath	0 or 1 Multipath per Satellite
Noise Channel	Yes
Noise Figure	2 dB
Out of Band Rejection in L1	≥ 45 dB
Antenna Size	185 mm diameter × 69 mm
LNA Gain	29 dB

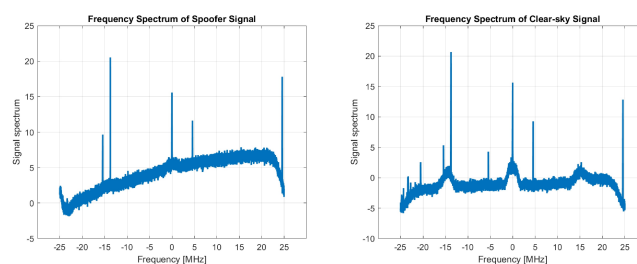
As seen in Table 2, the key signal and antenna parameters include: the signal transmission power from the simulator, the sky elevation limit for the spoofed satellites, the propagation models (Klobuchar for ionosphere and Saastamoinen for troposphere) for the spoofed satellites, the roof antenna dimensions, and the noise settings. The LNA noise figure value listed in the Table 2 is of the NovAtel GNSS-703 antenna mounted at the rooftop of the one university building at Tampere University for capturing real GNSS satellite signals. The configurations were designed to emulate open-sky conditions while incorporating realistic impairments and environmental factors to ensure signal fidelity and diversity across scenarios.

The use of a high sampling rate, PRN-based asynchronous spoofing scenario diversity, and addition of multipath in spoofed signals makes the Tuni2025 GNSS spoofing datasets unique in the existing literature and highly suitable for spoofing detection algorithm development, statistical feature analysis, and radio frequency fingerprinting under controlled yet realistic laboratory conditions. This latter part is feasible because all-but-last scenarios have distinct labels per PRN

codes, and therefore each PRN code can be uniquely identified as spoofer or as a genuine signal.

### VALIDATION AND QUALITY

The technical validity of the Tuni2025 GNSS spoofing datasets was assessed using the open-source FGI-GSRx software-defined GNSS receiver [18], [19], developed by the Finnish Geospatial Research Institute (FGI). This FGI-GSRx receiver is capable of multi-GNSS signal acquisition and analysis in both pre-correlation and post-correlation domains, making it suitable for evaluating raw I/Q datasets collected under spoofed and authentic conditions. Each recorded scenario (which was approximately 30 GB) was successfully processed by the FGI-GSRx receiver, confirming the structural integrity and usability of the data.

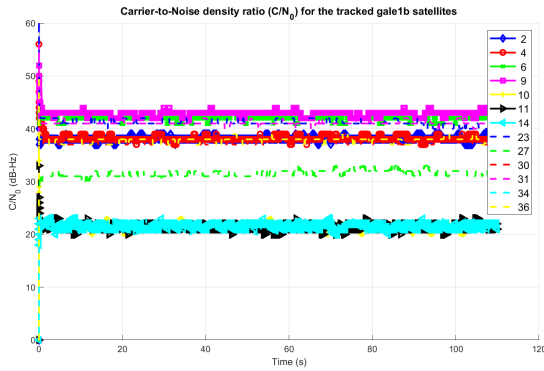


**FIGURE 3. Frequency Spectrum of SS-5 (left side, spoofed Galileo signal) and C-1 (right side, clean Galileo signal) Scenarios (see Table 3 for additional details)**

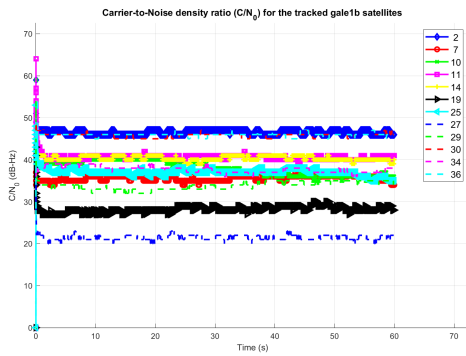
For example, in order to examine the spectral quality of the collected signals, Figure 3 compares the power spectrum of a spoofed Galileo PRN code with that of a clear-sky Galileo PRN code, both sampled at 50 MHz. The spectrum of the authentic clear-sky signal exhibits a smooth and symmetric signal profile, consistent with expectations from an open-sky GNSS reception. In contrast, the spoofed signal demonstrates minor spectral irregularities and amplitude fluctuations across the frequency bins. These deviations can be attributed to the digitally generated and overlaid nature of the spoofed signals that confirm the presence of distinct signal features introduced by the simulation process.

Further validation is provided through the carrier-to-noise density ratio ( $C/N_0$ ) analysis of the SS-5 and C-1 scenarios (referred to in table 3) as shown in Figures 4 and 5, respectively. In the spoofed Galileo SS-5 scenario, the  $C/N_0$  values associated with the spoofed PRNs are generally higher and exhibit less fluctuation compared to the genuine PRNs. This consistency stems from the controlled conditions in which the spoofed signals are generated. In contrast, the clear-sky scenario C-1 presents natural variation in  $C/N_0$  across PRNs, reflecting environmental influences such as multipath, atmospheric fading, and line-of-sight obstructions typical of real GNSS reception.

A notable observation in the spoofed SS-5 scenario is an initial drop in  $C/N_0$  of approximately 5–10 dB for

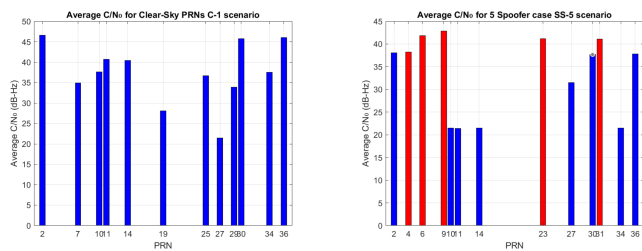


**FIGURE 4.** Carrier-to-Noise density ratio of all the PRNs present in SS-5 scenario, Spoofed PRNs {4, 6, 9, 23, 31}, Clear-Sky PRNs {2, 10, 11, 14, 27, 30, 34, 36}



**FIGURE 5.** Carrier-to-Noise density ratio of all the PRNs present in C-1 scenario, namely PRNs {2, 7, 10, 11, 14, 19, 25, 27, 29, 30, 34, 36}

the spoofed PRNs during the early segment of the signal acquisition. This reduction is likely due to cross-correlation interference between time-asynchronous spoofed and authentic signals, leading to partial signal degradation in early tracking phases. These effects are consistent with asynchronous spoofing conditions where the alignment between the genuine and spoofed signals is not exact, resulting in a decrease in the correlator output strength at the receiver.



**FIGURE 6.** Average Carrier to Noise ratio of all the PRNs present in clear-sky C-1 scenario and Spoofed SS-5 scenario (see Table 3 for details on scenarios)

This  $C/N_0$  behavior is further illustrated in Figure 6, which presents the average  $C/N_0$  per PRN for both C-1 and SS-5 scenarios. The SS-5 plot uses color coding to distinguish between genuine and spoofed PRNs, with spoofed PRNs generally exhibiting high average  $C/N_0$  levels. The scenario C-1 was recorded at 14:23 UTC whereas SS-5 was recorded 20 minutes later and therefore the change of satellite position and also the atmospheric conditions resulted in different values of  $C/N_0$  ratio for the clear-sky PRNs in both cases. Also, in SS-5 the clear-sky and spoofer PRNs are merged using a Mini-Circuits ZN2PD2-63-S+ RF splitter which further reduces the  $C/N_0$  values in this case. This supports the effectiveness of the spoofing setup and confirms that the datasets capture distinguishable signal characteristics suitable for spoofing detection, classification, and RF fingerprinting analysis.

### RECORDS AND STORAGE

The Tuni2025 GNSS datasets include 17 independent GNSS signal scenarios: eight for Galileo E1 and nine for GPS L1, each provided as a raw binary file containing interleaved 32-bit I/Q samples. These .bin files are accompanied by scenario-specific .pdf README documents that describe the spoofing configuration, sampling frequency, PRN numbers, time and date of collection, scenario duration, and environmental conditions. All files follow a uniform naming convention (e.g., SS-5.bin, C-1.bin) and are directly usable without the need for external dependencies or preprocessing pipelines.

The dataset is organized into two publicly accessible repositories hosted on Zenodo:

- **Galileo scenarios:** <https://doi.org/10.5281/zenodo.15470142>
- **GPS scenarios:** <https://doi.org/10.5281/zenodo.15572975>

Each scenario is stored as a standalone unit and contains approximately 30 GB of raw data sampled at 50 MSps. The consistent file structure across scenarios allows for a scalable analysis using custom or existing GNSS signal processing tools. The README files contain all necessary metadata for interpretation, including sampling parameters, spoofer count, PRN numbers, and notes on multipath inclusion.

A compact summary of the scenario configurations is presented in Table 3, which categorizes each case by signal type (GPS or Galileo), scenario number, scenario type, number of spoofers, and the presence or absence of multipath. For example C-1 and C-3 scenarios are both corresponding to clear-sky genuine signals, SS-3 corresponds to a situation with three Galileo PRN spoofing codes and no multipath, SS-27 corresponds to a situation with one GPS PRN spoofing code with multipath, etc. In the case of multipath it is important to note that the simulated multipath for each PRN is different and the range offset ranges from 200m to 500m and power offset from -2 dB to -5 dB. All scenarios

**TABLE 3. Summary of Tuni2025 GNSS Clean and Spoofing Scenarios**

ID	Scenario no. ( $n$ )	Scenario Type	Number of spoofed PRNs ( $s$ )	Multipath
C- $n$	$n = 1$	Galileo Static Clear-sky (clean)	0	No
SS- $n$	$n = 1, 3, 5$	Galileo Static True Pos. (spoof)	$s = 1, 3, 5$	No
C- $n$	$n = 3$	Galileo Static Clear-sky (clean)	0	No
SS- $n$	$n = 11, 12, 13$	Galileo Static True Pos. (spoof)	$s = 1, 2, 4$	Yes*
C- $n$	$n = 5$	GPS Static Clear-sky (clean)	0	No
SS- $n$	$n = 17, 18, 20$	GPS Static True Pos. (spoof)	$s = 1, 3, 5$	No
C- $n$	$n = 7$	GPS Static Clear-sky (clean)	0	No
SS- $n$	$n = 27, 28, 29$	GPS Static True Pos. (spoof)	$s = 1, 2, 4$	Yes*
SS- $n$	$n = 33$	GPS Delayed Spoofing, All PRNs (spoof)	All	No

\*Multipath profiles vary with number of spoofed PRN codes; details found in the text in this section describing this table.

were collected during two days, 25th of January (all Galileo scenarios) and 30th of January (all GPS scenarios). We remark that the only difference between C-1 and C-3 scenarios is that they were collected one hour apart (C-1 starting at 14:23 UTC on 25.01.2025 C-3 starting at 15:23 UTC on 25.01.2025) and that the clean-sky scenarios C- $n$  contain all GNSS signals (GPS, Galileo, Beidou and Glonass) available on the sky at the time of measurements; the overlapping information between C-1 and C-3 can be in fact used as a further validation point in the data analysis. Table 3 serves as a quick reference to the contents and conditions of each scenario file, supporting the reproducibility and the selective use in research workflows. The scenarios starting with letter C denote the clear sky scenarios, while those starting with letter S denote the spoofer scenarios. We remark that additional details are included in each 'Readme' file at the Zenodo repositories with our datasets.

### FURTHER INSIGHTS AND NOTES

As one potential limitation of our work, we mention that the datasets were collected using a measurement setup that did not implement precise time synchronization between the spoofed and authentic signals. As a result, fully time-synchronous spoofing scenarios are not available in our datasets, but this fact does not reduce the usefulness of our datasets by any means, since one of the main purposes of our datasets is to enable RFFI studies relying on hardware impairments of the transmitters and these studies are not

affected by the time stamps. However, the time-synchronous spoofing aspect should be considered if one wants to analyze the features that depend on the relative timing between the spoofed and the genuine signals, such as those derived from pseudorange-level processing. A time-synchronous spoofer, unlike a non-synchronous one, acts as additional multipath components, and therefore time-synchronous spoofing detection can rely also on multipath detection methods, by expanding them to identify whether the first arriving paths are due to a spoofer or to a genuine signal. Nevertheless, many spoofing detection algorithms, such as those based on machine learning, are working with both synchronous and non-synchronous spoofers.

Additionally, the latency introduced by the Spectracom signal generator caused a consistent delay in the injection of spoofed signals. This delay may influence the observed signal dynamics and the behavior of tracking loops in the receiver, potentially creating some differences with the effects encountered in real-world spoofing attacks. These limitations reflect the characteristics of the controlled lab environment and should be kept in mind when interpreting the datasets, but they are by no means reducing the viability of the provided datasets or their usefulness in future RFFI studies.

An important direction for future work involves expanding the dataset to incorporate greater spatial and temporal diversity. Specifically, conducting measurements across multiple receiver locations and at different times, introducing receiver mobility into the measurement setup could provide valuable insights into the real-world applicability of the proposed methods. To facilitate this, we recently acquired an I/Q grabber capable of supporting dynamic and outdoor measurements, which will enable us to systematically explore these aspects in subsequent phases of the research.

### ANALYSIS, SOURCE CODE, AND SCRIPTS

The datasets described in here can be processed and analyzed by using the open-source multi-GNSS software receiver developed by the FGI, specifically versions 2.0.1 and 2.0.2 of the MATLAB-based FGI-GSRx tool available in open-access on Github at and described in [18]. This GNSS receiver was instrumental in processing the raw I/Q measurement files and extracting relevant signal features for both GPS and Galileo systems. To support reproducibility and facilitate further research, we have included the configuration files used for both GPS and Galileo signal processing in a publicly accessible Zenodo repository. Additionally, two Spectracom scenario files, one corresponding to GPS and the other to Galileo, were provided in Zenodo to enable the research community to replicate the Spectracom-based measurement setup and validate the results. The goal of this data descriptor paper was to focus on the structural integrity and detailed data description of the provided datasets rather than on the development of algorithms based on these datasets. Nevertheless, for interested readers, our prior work in the

MSc thesis at Tampere University published as open access at [20] includes several examples of  $C/N_0$  analyses and other pre- and post-correlation analyses achieved with some of the datasets presented here.

### ACKNOWLEDGMENTS AND INTERESTS

S.M.U.R curated and analyzed the data, and wrote the main parts of the manuscript. M.Z.H.B, J.N, and E.S.L reviewed the curation and wrote parts of the manuscript. All authors reviewed the manuscript.

This work was funded by the by the National Science Foundation (NSF) and by the Research Council of Finland (RCF) grant 359846 under RESILIENT project. This work has also been partially supported by the LEDSOL project funded within the LEAP-RE programme by the European Union's Horizon 2020 Research and Innovation Program under Grant Agreement 963530 and the RCF grant 352364.

The article authors have declared no conflicts of interest.

### REFERENCES

- [1] F. Rothmaier, Y.-H. Chen, S. Lo, and T. Walter, "A framework for GNSS spoofing detection through combinations of metrics," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 57, no. 6, pp. 3633–3647, 2021.
- [2] X. Li, H. Zhang, X. Yu, and W. Liu, "A robust reliability-centric method for swift spoofing signal detection in advanced gnss security," *Chinese Journal of Electronics*, vol. 34, no. 3, pp. 774–786, 2025.
- [3] S. Bertram, L. Eisentraut, and R. Buettner, "A systematic literature review of current machine learning approaches for detecting gnss spoofing attacks," *IEEE Access*, vol. 13, pp. 108 898–108 917, 2025.
- [4] W. Wang, E. S. Lohan, I. A. Sanchez, and G. Caparra, "Pre-correlation and post-correlation rf fingerprinting methods for gnss spoofer identification with real-field measurement data," in *2022 10th Workshop on Satellite Navigation Technology (NAVITEC)*, 2022, pp. 1–10.
- [5] H. Wang, S. Guo, Z. Liu, Y. Zhang, Y. Shen, and X. Jiang, "Gnss signal spoofing detection based on satellite oscillator stability," in *2024 International Conference on Satellite Internet (SAT-NET)*, 2024, pp. 44–51.
- [6] Radionavigation Laboratory, The University of Texas at Austin. (2025) Texas spoofing test battery (textbat) dataset repository. Accessed: 2025-06-09. [Online]. Available: <https://rnl-data.ae.utexas.edu/datastore/textbat/>
- [7] Oak Ridge National Laboratory. (2025) Oakbat: Oak ridge spoofing and interference test battery dataset. Accessed: 2025-06-09. [Online]. Available: <https://doi.ccs.ornl.gov/dataset/d21dfe58-3af9-5ed8-9c97-693c12045aee>
- [8] S. M. U. Rahman, "Tuni2025 datasets for gnss - galileo spoofing," May 2025. [Online]. Available: <https://doi.org/10.5281/zenodo.15470142>
- [9] —, "Tuni2025 datasets for gnss - gps spoofing," May 2025. [Online]. Available: <https://doi.org/10.5281/zenodo.15572975>
- [10] European Space Agency (ESA). (2025) Evil waveform (ewf) – esa gnss vulnerability testing initiative. Accessed: 2025-06-09. [Online]. Available: [https://www.esa.int/Enabling\\_Support/Space\\_Engineering\\_Technology/Radio\\_Frequency\\_Systems/Evil\\_WaveForm](https://www.esa.int/Enabling_Support/Space_Engineering_Technology/Radio_Frequency_Systems/Evil_WaveForm)
- [11] S. Islam, M. Z. H. Bhuiyan, M. Liaquat, I. Pääkkönen, and S. Kaasalainen, "Fgi's gnss spoofing dataset repository (fgi-spoofrepo)," Feb. 2024, national Land Survey of Finland, FGI Dept. of Navigation and Positioning. [Online]. Available: <https://doi.org/10.23729/7a648509-2ca8-4a7d-8223-0b429182f857>
- [12] M. Liaquat, M. Z. H. Bhuiyan, and S. Islam, "Fgi jammer test 2025 repository," May 2025, national Land Survey of Finland, FGI Dept. of Navigation and Positioning. [Online]. Available: <https://doi.org/10.23729/fd-06d27736-45cb-3ca2-aff8-725d42c6caeb>
- [13] A. Lemmenes, P. Corbell, and S. Gunawardena, "Detailed analysis of the textbat datasets using a high fidelity software gps receiver," in *Proceedings of the 29th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2016)*, Portland, Oregon, Sep 2016, pp. 3027–3032. [Online]. Available: <https://doi.org/10.33012/2016.14668>
- [14] G. Marchand, A. Toumi, G. Seco-Granados, and J. A. López-Salcedo, "Machine learning assessment of anti-spoofing techniques for gnss receivers," in *Work-in-Progress in Hardware and Software for Location Computation (WIHAL 2023)*, Castellon, Spain, jun 2023, hAL Id: hal-04184075. [Online]. Available: <https://hal.science/hal-04184075>
- [15] P. Thevenon, O. Julien, Q. Tessier, D. Maillard, M. Cabantous, F. Amarillo-Fernández, and F. D. Oliveira-Salgueiro, "Detection performances of evil waveform monitors for the gps l5 signal," in *Proceedings of the 27th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2014)*, Tampa, Florida, sep 2014, pp. 3312–3322.
- [16] S. Islam, M. Z. H. Bhuiyan, M. Liaquat, I. Pääkkönen, and S. Kaasalainen, "An open gnss spoofing data repository: characterization and impact analysis with fgi-gsrx open-source software-defined receiver," *GPS Solutions*, vol. 28, no. 4, 8 2024. [Online]. Available: <http://dx.doi.org/10.1007/s10291-024-01719-2>
- [17] M. Z. H. Bhuiyan, M. Liaquat, S. Islam *et al.* (2025, jun) Implementation and performance analysis of a chi-square test based gnss signal anomaly detection. Preprint, Version 1. [Online]. Available: <https://doi.org/10.21203/rs.3.rs-6750861/v1>
- [18] M. Liaquat, M. Z. H. Bhuiyan, S. Islam, I. Pääkkönen, and S. Kaasalainen, "An enhanced fgi-gsrx software-defined receiver for the execution of long datasets," *Sensors*, vol. 24, p. 4015, 2024. [Online]. Available: <https://doi.org/10.3390/s24124015>
- [19] B. Kai, F.-H. Ignacio, L.-S. José A., and M. Z. H. Bhuiyan, *GNSS Software Receivers*. Cambridge University Press, 2022.
- [20] S. M. U. Rahman, "In-lab measurement campaigns and measurement-based analysis for gnss spoofing models and countermeasures: Gnss spoofing dataset generation," Master's Thesis, Tampere University, Tampere, Finland, 2025. [Online]. Available: <https://urn.fi/URN:NBN:fi:tuni-202505306401>