GPS Solutions (2024) 28:176
https://doi.org/10.1007/s10291-024-01719-2

ORIGINAL ARTICLE

An open GNSS spoofing data repository: characterization and impact analysis with FGI-GSRx open-source software-defined receiver

Saiful Islam[1] · Mohammad Zahidul H. Bhuiyan[1] · Muwahida Liaquat[1] · Into Pääkkönen[1] · Sanna Kaasalainen[1]

Received: 6 March 2024 / Accepted: 27 July 2024

Abstract

Spoofing is becoming a prevalent threat to the users of Global Navigation Satellite Systems (GNSS). It is important to deepen our understanding of spoofing attacks and develop resilient techniques to effectively combat this threat. Detecting and mitigating these attacks requires thorough testing, typically conducted in a laboratory environment through the establishment of a spoofing test-bed. The complexity, cost and resource demands of creating such a test-bed underscore the necessity of utilizing openly available datasets. To address this need, this paper introduces a new GNSS spoofing data repository from Finnish Geospatial Research Institute (FGI) named hereafter as 'FGI-SpoofRepo'. This data repository consists of raw In-phase and Quadrature (I/Q) data of live recordings of GPS L1 C/A, Galileo E1, GPS L5, and Galileo E5a signals. These datasets encompass three distinct types of spoofing characteristics (synchronous, asynchronous, and meaconing), making them very useful example candidates of open data for testing the performance of any anti-spoofing techniques (be it detection or mitigation). The inclusion of live signals in multiple GNSS frequencies and the presence of cryptographic signatures in Galileo E1 signal make these datasets potential benchmarks for assessing the resilience performance of multi-frequency multi-constellation receivers. The analysis of the datasets is carried out with an open-source MATLAB-based software-defined receiver, FGI-GSRx. An updated version of FGI-GSRx, equipped with the necessary modifications for processing and analyzing the new datasets, is released alongside the datasets. Therefore, the GNSS research community can utilize the open-source FGI-GSRx or any third-party SDR to process the publicly available raw I/Q data for implementation, testing and validation of any new anti-spoofing technique. The results show that time-synchronous spoofing seamlessly takes over positioning solution, while time-asynchronous spoofing acts as noise or in some cases, completely prevent the receiver from providing a positioning solution. Signal re-acquisition during an ongoing spoofing attack (cold start), the receiver tends to lock onto the spoofing signal with the highest peak, posing a potential threat to GNSS receivers without assisted information. Overall, this research aims to advance the understanding of complex spoofing attacks on GNSS signals, providing insight into enhancing resilience in navigation systems.

Keywords GNSS · GPS · Galileo spoofing · Software-defined receiver

Introduction

Spoofing poses an increasingly common threat to users of Global Navigation and Satellite Systems (GNSS), impacting safety and mission-critical applications across terrestrial, maritime and aerial domains. As a result, unprotected GNSS receivers and other GNSS dependent systems are becoming increasingly vulnerable to attack, regardless of whether they are intended targets or accidental victims. Understanding various spoofing attacks and their operational impacts on any receivers is vital. This understanding includes the ability to identify various methods of attacks, evaluate failure patterns, grasp how a device reacts to a given threat, as well as understanding of recovery procedures (Homeland 2022). Addressing these challenges involves the development of anti-spoofing techniques by the end users or more particularly, receiver manufacturers.

The introduction of civilian GPS spoofing, as documented in Humphreys et al. (2008), marked a significant shift in the threat landscape. Unlike previous spoofing attempts that relied on initial jamming, this new approach deceives

✉ Saiful Islam
saiful.islam@nls.fi

[1] Department of Navigation and Positioning, Finnish Geospatial Research Institute, FGI-NLS, Espoo, Finland

Published online: 12 August 2024

target receivers at the tracking stage without significantly compromising the tracking characteristics (i.e., in terms of variation in phase or code tracking loops). Following this, the landscape for commercial GNSS users underwent a notable change with the emergence of affordable GPS spoofers, as discussed in Lin and Qing (2015). The affordability of basic spoofing afterwards led to an upsurge in spoofing incidents (EUSPA 2023b; GPSWorld 2023). In response to these growing threats, research on spoofing detection and mitigation techniques has been ongoing since the introduction of civilian GPS spoofers (Montgomery et al. 2009; Cavaleri et al. 2010; Broumandan et al. 2015; Magiera and Katulski 2015; Orouji and Mosavi 2021; Shang et al. 2022). A comprehensive exploration of various spoofing generation techniques, receiver vulnerabilities on spoofing, and approaches for detection and mitigation are presented in Jafarnia-Jahromi et al. (2012), including example spoofing scenarios for real-world receiver testing.

The spoofing detection can be preliminary categorized into four groups: signal power monitoring, multi-correlator tracking (Jafarnia-Jahromi et al. 2012; Guo et al. 2018; Turner et al. 2020), signal quality monitoring (Phelts 2001), and cryptographic signature validation (Anderson et al. 2017; Motella et al. 2021). Numerous other approaches have been proposed, such as spatial processing, time of arrival discriminator, consistency checks with other navigation systems, code and phase rate consistency check, and received ephemeris consistency check, among others.

As the way of spoofing attacks and their characteristics continuously evolve alongside the modernization of GNSS signals, continuous research is vital for the development of effective detection and mitigation techniques. For instance, monitoring correlation peaks is one such technique, as multipath and spoofing both distort the peaks in the composite signal. If the code and carrier phase of the spoofing signal closely align with the authentic signal, the correlation peak monitoring based technique may erroneously detect the spoofing signal as multipath (Magiera and Katulski 2015). Therefore, thorough evaluation and testing of each spoofing detection or mitigation technique is essential to address the evolving and growing nature of spoofing threats.

Evaluating the effectiveness of these techniques requires commonly used datasets resembling real-world situations. This is often accomplished by establishing a spoofing test-bed consisting of one or more software/hardware simulator and other complex setups. One such test-bed is essential for performing various vulnerability assessments, providing fine-grained control over crucial parameters. These tests aim to evaluate the resilience of Position Navigation and Timing (PNT) systems by determining how GNSS receivers react to potential spoofing attacks, applying mitigation techniques, re-testing the improved system and adjusting parameters as needed (Perdue et al. 2016). However, establishing such a complex test-bed typically requires significant budget, specialized software and hardware, expert professionals and time. Furthermore, achieving a code and carrier phase-aligned coherent spoofing attack is extremely difficult and often requires repeated attempts.

Therefore, a set of well-known open datasets emerges as a pragmatic solution to save money and time and to ease complexity. The Texas Spoofing Test Battery (TEXBAT) is one such dataset introduced by the University of Texas (Humphreys et al. 2012). For many years, researchers and professionals have been driven to the TEXBAT datasets to assess the spoofing vulnerability of GPS receivers. Various statistical spoofing detection and mitigation techniques are proposed by using TEXBAT datasets including (Gamba et al. 2017; Kuusniemi et al. 2017; Khan et al. 2020). The Oak Ridge Spoofing and Interference Test Battery (OAKBAT) was introduced following the framework of the TEXBAT datasets (Albright et al. 2020). OAKBAT datasets contain GPS L1 C/A and Galileo E1 signals while TEXBAT datasets contain only GPS L1 C/A signals. These datasets and studies have primarily focused on legacy GNSS signals and have demonstrated various approaches to identify and mitigate spoofing. The current state of the art however reveals several limitations, most existing spoofing datasets are limited in scope, often focusing on simple spoofing scenarios and lacking representation of modernized GNSS signals. Additionally, the available software tools for processing GNSS signals are limited, do not fully support the multi frequency diversity in the event of single frequency or constellation spoofing. It is also crucial to test the spoofing vulnerability of other GNSS signals from lower L-band such as GPS L5 and Galileo E5a. Both datasets, on the other hand, are lacking lower L-band signals. The authenticity testing of GNSS navigation messages is another key part of any resilient navigation system. Galileo Open Service Navigation Message Authentication (OSNMA) is an authentication technique allowing a receiver to verify that the navigation message is coming from a trusted source and has not been modified in the way (ESA 2021). Galileo OSNMA data bits, broadcast on the E1-B data channel since late 2020, are absent from existing datasets, highlighting a key gap in the current landscape. Our research aims to fill these gaps by creating a completely new set of digitized GNSS In-phase and Quadrature (I/Q) data that includes both legacy and modernized signals in sophisticated and realistic spoofing scenarios.

This paper is inspired by the authors' recent work (Islam et al. 2023) where details of spoofing signal generation under a simulated environment and their impact on the different-grade GNSS receivers are presented. Motivated by the limitations of previously available datasets and the importance of assessing modernized GNSS signals and contemporary spoofing events, this paper introduces a new GNSS spoofing data repository from Finnish Geospatial Research Institute

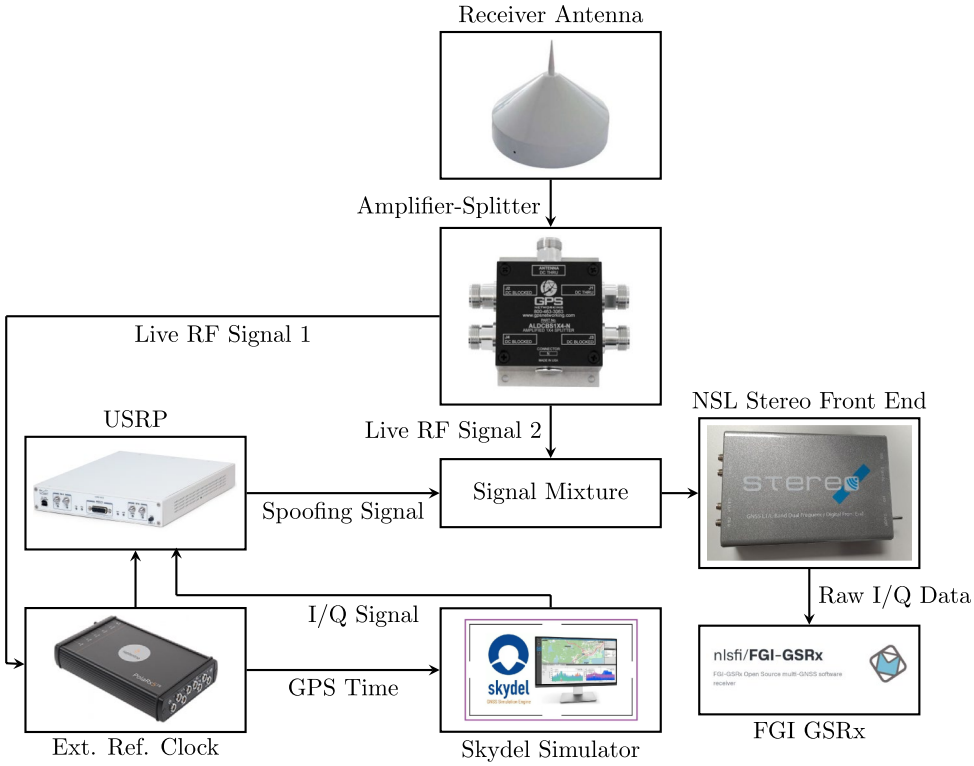


Fig. 1 Experimental setup diagram of spoofing test-bed

(FGI) named as 'FGI-SpoofRepo'. This repository consist of a set of raw I/Q data with live GNSS signals. GNSS spoofing attacks can be carried out in many ways depending on the expertise of the spoofers and available resources. FGI-SpoofRepo comprise a set of four digitized recordings of live static datasets of GPS L1 C/A, Galileo E1, GPS L5 and Galileo E5a signals. The new datasets contain three types of spoofing scenarios: Targeted Spoofing (time and position synchronous), Untargeted Spoofing (time and or position asynchronous), and Meaconing (re-radiator). These datasets integrate real-world live signals with simulated spoofing signals, admitting the inherent challenges of spoofing the live signal in a controlled environment. The real-world nature of the datasets incorporates environmental effects and cryptographic signatures, such as OSNMA, portraying them as very good example candidates of open data for testing performance of spoofing detection and mitigation techniques with multi-frequency multi-constellation receivers.

This paper provides a thorough overview of the spoofing dataset generation, accompanied by an in-depth analysis of each dataset. Processing of the datasets has been carried out by an open-source software-defined receiver named 'FGI-GSRx', released as open-source in 2022 (Kai et al. 2022). An updated open-source version of FGI-GSRx is released along with the datasets and software features including necessary modifications for processing and analyzing the new datasets. The novel contribution of this paper lies in the generation of a completely new set of digitized GNSS I/Q data involving both legacy and modernized signals in sophisticated spoofing scenarios. Adding real-world multi-frequency, multi-constellation signals, inherently including cryptographic signatures in the Galileo E1 signal and updated version of the software receiver has further empowered the novelty. By utilizing these advancements in new datasets and software, researchers can develop and verify new techniques to detect and counteract GNSS spoofing, ultimately strengthening the resilience and reliability of GNSS-based systems. The remainder of the paper progresses as follows. The experimental setup reveals the spoofing generation procedure and an overview of the used equipment. Following that, the spoofing scenario definition section details the spoofing scenarios and their characteristics. Afterwards, the data analysis section thoroughly assesses the characteristics of each scenario by the FGI-GSRx software receiver. Finally, the paper summarizes the results and outlines potential directions for future research activities.

Experimental setup

This section encompasses several key components, each contributing to the comprehensive datasets preparation process. These components include a Software-Defined GNSS simulator, an external reference clock for precise timing, a receiving antenna for live signal reception, an amplifier to compensate cable losses, an RF front-end for capturing I/Q

data, and an open-source software-defined receiver for in-depth analysis. The composition of these equipment ensures a controlled environment for the experiments. The experimental setup of spoofing datasets generation is presented in Fig. 1.

- **Spoofing Signal Generation** All the spoofing signals in the datasets are generated using the Safran Skydel software-defined GNSS simulator (Safran 2023) in conjunction with external hardware. Skydel is an advanced GNSS signal simulator known for its customizability and scalability, with integrated interference generation capabilities across multiple frequencies and constellations. Most simulation parameters are controllable on the fly while the simulation is running, a feature of particular relevance in the context of jamming and spoofing experiments.

  It is crucial to initialize the simulator with the most up-to-date broadcast GNSS ephemeris data for an accurate spoofing signal generation. Using outdated ephemeris information may result in unsuccessful spoofing attempt. Within the simulator, there is a provision to import Receiver Independent Exchange (RINEX) compatible files, which are used to update the orbits of GPS and Galileo satellites. When a RINEX file is imported, it overrides the existing information on orbits, perturbations, clock, group delay, and health status. The broadcast ephemeris data in RINEX format can be sourced from NASA's Crustal Dynamics Data Information System (CDDIS)(Noll 2010).

  The simulation time is carefully synchronized with GPS time for targeted time synchronous scenarios, which is obtained from a reference GNSS timing receiver. The timing receiver generates a 1 Pulse Per Second (1 PPS) signal and a 10 MHz reference signal to the Universal Software Radio Peripheral (USRP) X310. This effectively ensures that the USRP maintains timing synchronization with the reference receiver.

  The connectivity between Skydel and the USRP is facilitated through a high-speed 10 Gigabit Ethernet link, ensuring real-time data transmission. Within the USRP, the I/Q data is up-converted into an RF signal, operating at a rate of 60 MS/s (mega samples per seconds) with both the L1/E1 and L5/E5a frequency. Subsequently, the RF signal is then combined with an authentic live-sky GNSS signal using a signal-mixer.
- **External Clock** Septentrio's PolaRX5T is utilized as an external reference clock to discipline the USRP X310. The PolaRx5TR is designed to achieve precise time synchronization in applications involving time and frequency transfer. In such applications, the device receives a 10 MHz reference signal and a 1 PPS signal from an external clock source, which, in our case, is the PolaRX5T.
- **Receiver Antenna** A reference antenna is used to fetch live GNSS signals. The same antenna is also used to connect a reference receiver that provides a clock source to USRP. The live signal is obtained using Septentrio's PolaNt Choke Ring antenna, which is a high-precision antenna that supports various GNSS signals (Septrentio 2023).

Table 1 RF recording configuration of the NSL Stereo dual-band GNSS front-end

Parameters	Frequency bands (L1/E1)	Frequency bands (L5/E5a)
Center frequency (MHz)	1569.03	1176.45
Sampling rate (MHz)	26	26
Data type	Real	Complex
Sample bit width	8 bit (I)	8 bit + 8 bit (I + Q)
Bandwidth (MHz)	4.2	10.09

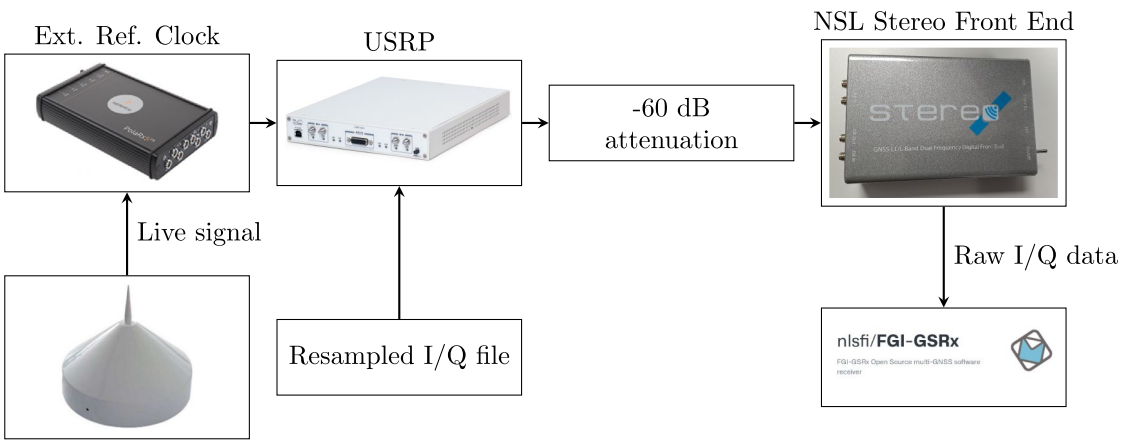


Fig. 2 Setup used for replaying and re-recording FGI-SpoofRepo dataset

- **Amplifier-Splitter** A Low Noise Amplifier (LNA) plays a crucial role in signal amplification and compensating for cable losses between the rooftop antenna and the receiver port. An Amplified Loaded DC Blocked Splitter (ALDCBS1X4) is employed featuring one active input and four RF outputs. In the context of data collection, one of the output port is connected to a reference receiver, denoted as the PolarRx5TR. An additional output port from the amplifier is connected to a mixer. This mixer is responsible for combining spoofing signals with authentic live-sky GNSS signals.
- **FGI-GSRx Multi-Frequency, Multi-Constellation Receiver** The FGI-GSRx is a MATLAB-based Software-Defined Receiver (SDR) developed by the Finnish Geospatial Research Institute (FGI). The software receiver plays a vital role in many national and international projects, serving as a key tool for testing and validating innovative receiver processing algorithms (Söderholm et al. 2016; Kai et al. 2022; Pany et al. 2024). In recent times, the GNSS community has been granted access to the FGI-GSRx as an open-source software under the General Public License (FGI-NLS 2022). The architecture of this software allows the development and testing of new algorithms at any stage within the receiver processing chain, with minimal modifications to the original structure.

  The current open-source version of FGI-GSRx can process GPS L1 C/A, Galileo E1, BeiDou B1, GLONASS G1, and NavIC L5 signals. However, all the datasets in this manuscript also contain GPS L5 and Galileo E5a signals. FGI has not yet made the GPS L5 and Galileo E5a signals based receiver implementation open to the public. Therefore, the authors utilize two separate versions of FGI-GSRx for processing the datasets: i) The open-source FGI-GSRx, and ii) The in-house FGI-GSRx. The users of FGI-GSRx open-source version will be able to reproduce the results with the shared datasets for GPS L1 and Galileo E1 signals. The users will need to utilize any other third party open-source SDR tool, for example, GNSS-SDR (Pany et al. 2024) in order to process GPS L5 and Galileo E5a datasets. However, the processing results for GPS L5 and Galileo E5a signals are anyway presented here with the in-house FGI-GSRx.

Table 3 Summary of spoofing data repository

Folder name	File name	Size (KB)	Duration (s)
Targeted_SFMC	TGS_L1_E1.dat	9878528	373
	TGS_L5_E5a.dat	19757056	373
Targeted_DFMC	TGD_L1_E1.dat	9728448	373
	TGD_L5_E5a.dat	19456896	373
Untargeted_DFMC	UTD_L1_E1.dat	9595136	377
	UTD_L5_E5a.dat	19190272	377
Meaconing_DFMC	MCD_L1_E1.dat	12216512	478
	MCD_L5_E5a.dat	24433024	478

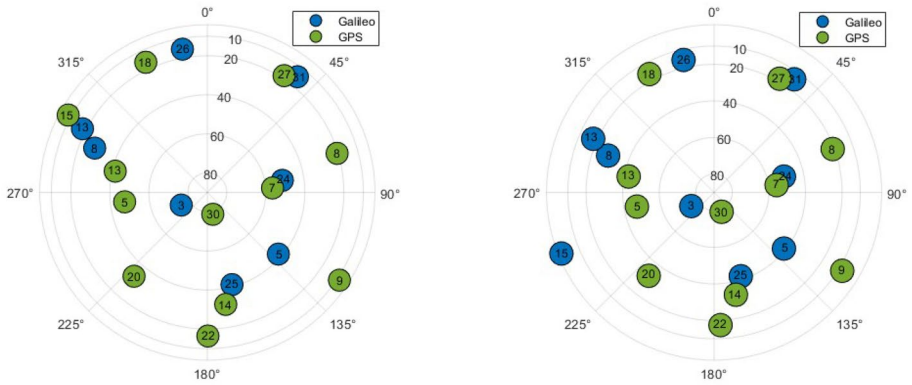
- **RF Recording Device** The raw I/Q data samples are captured using the stereo dual-band GNSS front-end developed by Nottingham Scientific Limited (NSL). The front-end comprises two distinct Radio Frequency (RF) chains: the MAX2769B, responsible for covering the upper L-band, also known as the L1 chain, and the MAX2112, which encompasses both upper and lower L-bands, collectively referred to as the L-band chain. The Local Oscillator (LO) associated with the L1 chain is tunable within the frequency range of 1550 MHz to 1610 MHz, allowing for precise adjustment to GNSS signals within this spectrum. Similarly, the LO for the L-band chain can be adjusted within the range of 900 MHz to 2400 MHz, enabling the capture of any signals within the L-band. The configuration detailed in Table 1 is used for capturing the raw I/Q data.
- **Dataset Replay Validation Setup** The recording setup was validated by transmitting and recording again a scenario using USRP X310 and NSL Stereo front-end. Usable sample rates for the USRP were calculated by dividing the device's 200 MHz master clock rate with an integer. The dataset had to therefore re-sampled from 26 MHz to 25 MHz which was done during pre-processing using Scipy's Signal package. The L1 band signals were also down-converted from IF (Intermediate Frequency) $1575.42 - 1569.03 = 6.39$ MHz to baseband. The developed Python script is also made available alongside the datasets allowing the users to replay the datasets for their own test and validation.

Table 2 Summary of spoofing scenarios

Name	Initial position Synch	Initial time synch	Position switch	Time shift	Latest ephemeris injected	Spoofing signal(s)
Targeted SFMC	Yes	Yes	Dynamic	No	Yes	L1, E1
Targeted DFMC	Yes	Yes	Dynamic	No	Yes	L1, E1, L5, E5a
Untargeted DFMC	No	No	Static	Advance	N/A	L1, E1, L5, E5a
Meaconing DFMC	No	No	Static	Delay	N/A	L1, E1, L5, E5a

(a) Live sky (b) Spoofing signal

Fig. 3 Skyplots of Targeted SFMC scenario



(a) Live sky (b) Spoofing signal

Fig. 4 Skyplots of Targeted DFMC scenario

GNU Radio companion was used to program the USRP to transmit the re-sampled FGI-SpoofRepo dataset. 60 dB attenuation was used between the USRP and the Stereo front-end to approximately match the transmitted RF power to live-sky. The recorded dataset was processed in FGI-GSRx using the same configurations as was used with the original dataset. A constant frequency offset of around 1.2 kHz was observed between the original and replayed-recorded dataset, but this effect was compensated automatically by the acquisition module and the carrier tracking loop of FGI-GSRx.

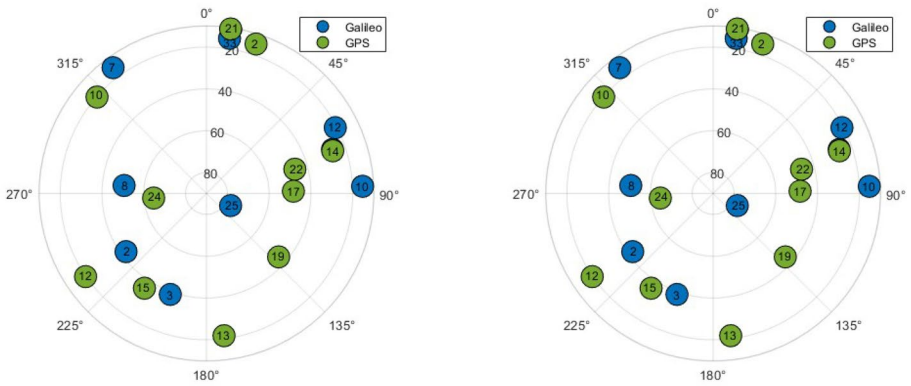
The setup used for the replay validation is illustrated in Fig. 2. The re-recorded FGI-SpoofRepo dataset was processed in FGI-GSRx to verify that the replayed and then re-recorded file could be useful without a significant drop in signal-tracking performance. A similar validation process was also attempted using a USRP X310 and commercial receivers i.e; u-blox M8T and F9P. The u-blox receivers (M8T) were able to receive both L1 C/A and E1 signals but not the L5 and E5a as the receivers do not support the use of L5-only solution.

Spoofing scenario definition

The true receiver is stationary in all four scenarios. It's position estimated by a geodetic-grade receiver is 60.182°N, 24.828°E with an altitude of 47.248 m. The true receiver is connected with a rooftop antenna at the Otaniemi premises of the Finnish Geospatial Research Institute (FGI). As the recordings are made on live signals, the starting date and time are always unique for each dataset. The initial 130 s across all datasets are free from intentional interference, making a clean baseline before the injection of the spoofing signals. It is worth noting that all live skyplots are generated based on information from the navigation engine of FGI-GSRx, with only those satellites utilized in the final Position, Velocity, and Timing (PVT) computation. On the other hand, skyplots for the spoofing signals are generated using log information provided by the simulator. The uniform replication of satellites, along with their corresponding elevation and azimuth concerning live signals, holds significant importance, particularly in scenarios involving targeted or synchronous spoofing attacks.

(a) Live sky (b) Spoofing signal

Fig. 5 Skyplots of Untargeted DFMC scenario



(a) Live sky (b) Replayed signal

Fig. 6 Skyplots of Meaconing DFMC scenario

Table 2 offers a detailed insight into the spoofing datasets and the associated techniques used to generate those datasets. The Targeted Single-Frequency Multi-Constellation (SFMC) scenario is generated by synchronizing the initial time and position with the true receiver, along with the injection of the latest available ephemeris. The intended spoofed location follows a circular trajectory. A similar process is followed for the Targeted Dual-Frequency Multi-Constellation (DFMC) scenario. On the contrary, both Untargeted DFMC and Meaconing DFMC scenarios do not maintain initial time and position synchronization with the true signal. In both scenarios, the intended spoof location remains static. However, in the Untargeted case, the spoofed time is advanced by hours, while in Meaconing, the spoofed time is delayed by minutes. Above all, the injection of the latest ephemeris is not applicable in both Untargeted and Meaconing cases.

A summary of the spoofing dataset repository is presented in Table 3. The repository contains several folders, each of which represents a different scenario. By accessing the folders, users will have access to two files that are specific to each signal. The table also includes the approximate size and duration of each file. It is to be noted that the duration provided in the table is truncated, and the actual files may contain a couple of seconds of extra data.

- **Targeted SFMC**

  Both GPS L1 and Galileo E1 signals are spoofed in this scenario. The other RF chain comprising GPS L5 and Galileo E5a signals are not spoofed throughout the test. This test is intended to assess the potential fallback behaviour of modern GNSS receivers equipped with multiple frequencies and constellations. The simulated spoofing signals are generated using the most recent ephemeris data available from NASA's CDDIS. The recordings are made on 2023-10-03 at 14:19:00 UTC over a 370 s duration. Figure 3 illustrates the skyplot for both spoofing and live signals on 2023-10-03 at 14:19:06 UTC. Eleven

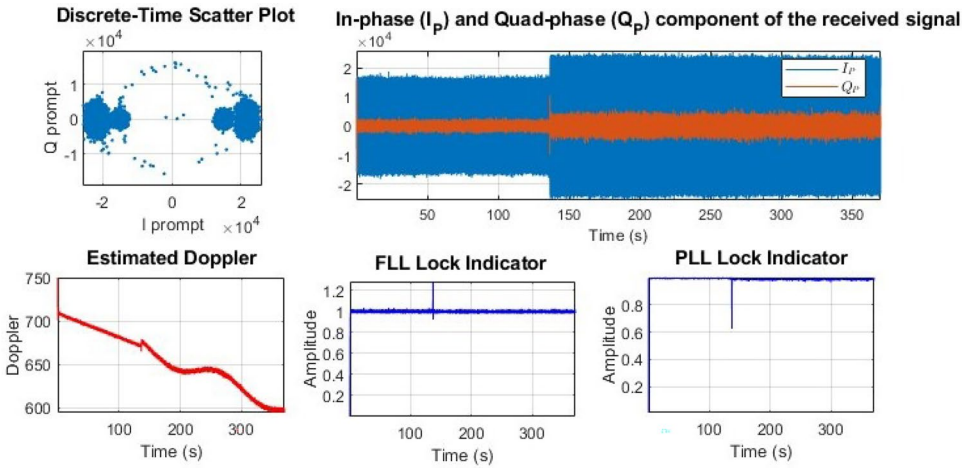


Fig. 7 Tracking of a GPS L1 satellite

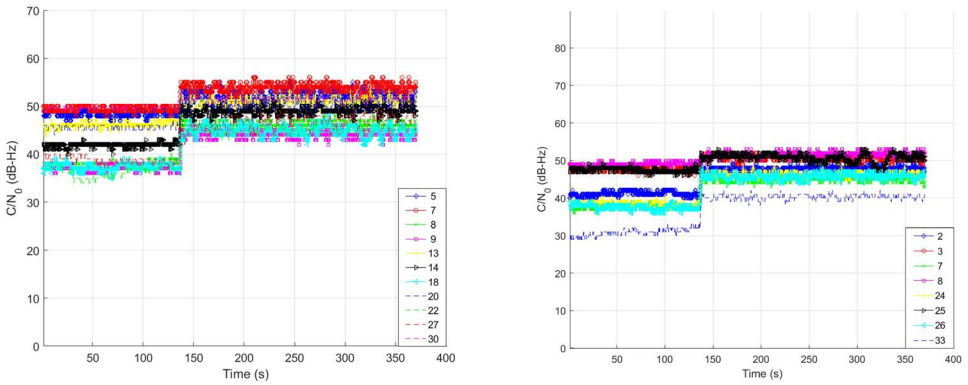


Fig. 8 C/N_0 of Targeted SFMC scenario

(a) C/N_0 of GPS L1

(b) C/N_0 of Galileo E1

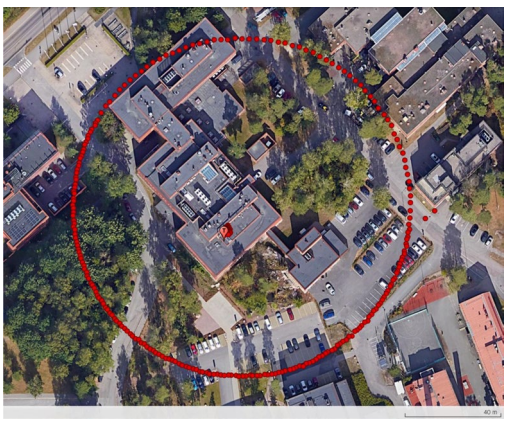


Fig. 9 Position estimated by the device under test

GPS satellites are simulated to match with live constellations. As for Galileo, the spoofing simulation replicates the live signal based on the ephemeris available during the recording. Notably, Galileo system's PRN 14 and 18 have been temporarily excluded from active service, as documented in (EUSPA 2023a), which explains their disappearance from the live signal skyplot. Additionally, Galileo PRN 13 failed to meet the signal power threshold, consequently absent from the skyplot.

- **Targeted DFMC**

  This scenario shares similar characteristics with the previous dataset with the main distinction being the inclusion of GPS L5 and Galileo E5a signals alongside GPS L1 and Galileo E1 signals in the spoofing. The recordings are made on 2023-10-20 at 13:20:02 UTC over a 370 s duration.

  Figure 4 illustrates the skyplot for both spoofing and live signals on 2023-10-20 at 13:20:13 UTC. In this scenario, similar to the previous one, eleven GPS satellites are simulated. However, the live signal exhibits an additional satellite, PRN 15 near the 10-degree cut-off threshold. The spoofing signal is missing the same satellite, as the signal generation has a cut-off threshold of 10 degrees. As for Galileo, nine satellites are simulated, yet the receiver acquire eight satellites from the live signal.

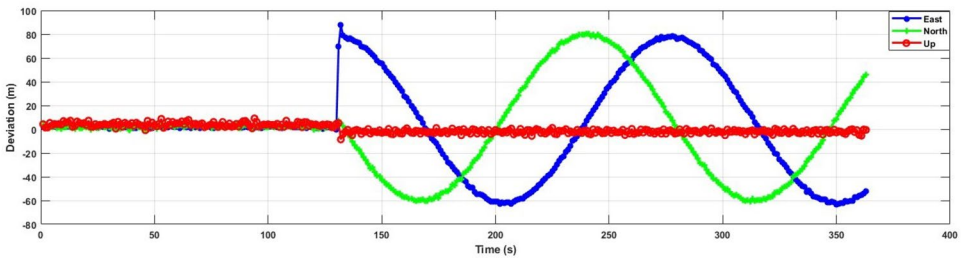
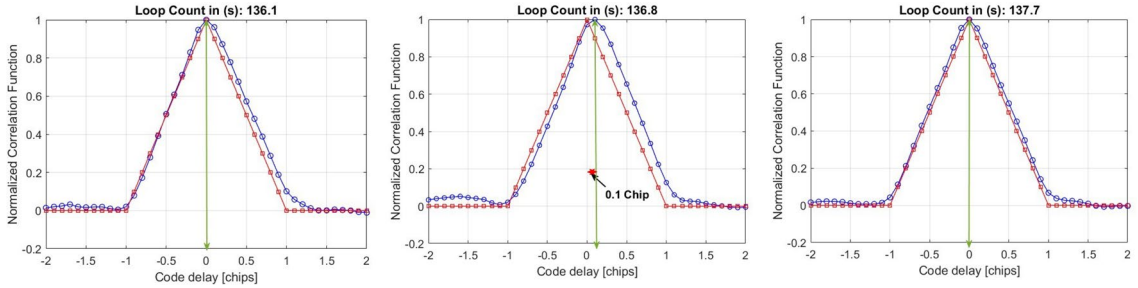


Fig. 10 Position deviation with respect to true location



(a) Before capture (b) During capture (c) After capture

Fig. 11 Multi-correlator monitoring of GPS L1 signal's PRN 7 to demonstrate the impact of spoofing on the receiver tracking

- **Untargeted DFMC**

  This scenario differs significantly from the previous targeted scenarios, forming an untargeted attack characterized by asynchronous positioning and timing of the spoofer with respect to the true location. In this case, the spoofer's intended position is simulated to be static at a distance of approximately 15 km from the actual location, with the spoofing time advanced by around 10 h. Recordings for this scenario are conducted on 2023-11-10 at 14:05:00 UTC, extending over a 377-second duration. The chosen target location for the spoofer is 60.16675899°N, 24.56664248°E, with an altitude of 2.00 m, and the spoofing start time is simulated on 2023-11-10 23:55:00 UTC.

  Figure 5 illustrates both the spoofing and live signals at specific epochs. Given the untargeted nature of this attack, the spatial distribution of live and simulated satellites does not aligned. The receiver is expected to view a new set of satellite constellations because of the considerable distance and the temporal divergence of nearly 10 h.
- **Meaconing DFMC**

  The LabSat 3 Wideband record and replay device (LabSat 2023) is used in the meaconing test. The scenario is recorded outside of the FGI premises, about 60 m away from the rooftop antenna. After the recording, the replayed signal is introduced alongside the live signal with an approximately 15-minute delay. The re-transmitted signal is introduced after 155 s of clean recordings, marking an exception in comparison to other datasets. There is a lack of synchronization in time, but it includes all the characteristics of live sky signals. The signals that are spoofed in this scenario belong to GPS L1, L5, and Galileo E1, E5a. The recordings are made on 2023-11-16 at 15:04:36 UTC. The dataset lasts around 478 s which is longer than other datasets. This prolonged duration renders it useful for applications that require extended initialization periods, such as cryptographic signature validation. Figure 6 illustrates the skyplots for both spoofed and live signals on 2023-11-16 at 15:04:42.

Data analysis

This section provides a detailed analysis of each dataset, focusing on how it affects the receiver's signal tracking and positioning performance. The open-source and in-house version of FGI-GSRx is utilized to perform the analysis. The open-source version is used to process the GPS L1 and Galileo E1 signals, whereas the in-house version is used to process the GPS L5 and Galileo E5a signals. In all scenarios, the position solution is computed using a 5-degree elevation mask and a 30 dB-Hz Carrier-to-Noise Density (C/N_0) threshold. In each scenario, there is a 1–5 s window of flexibility due to the manual

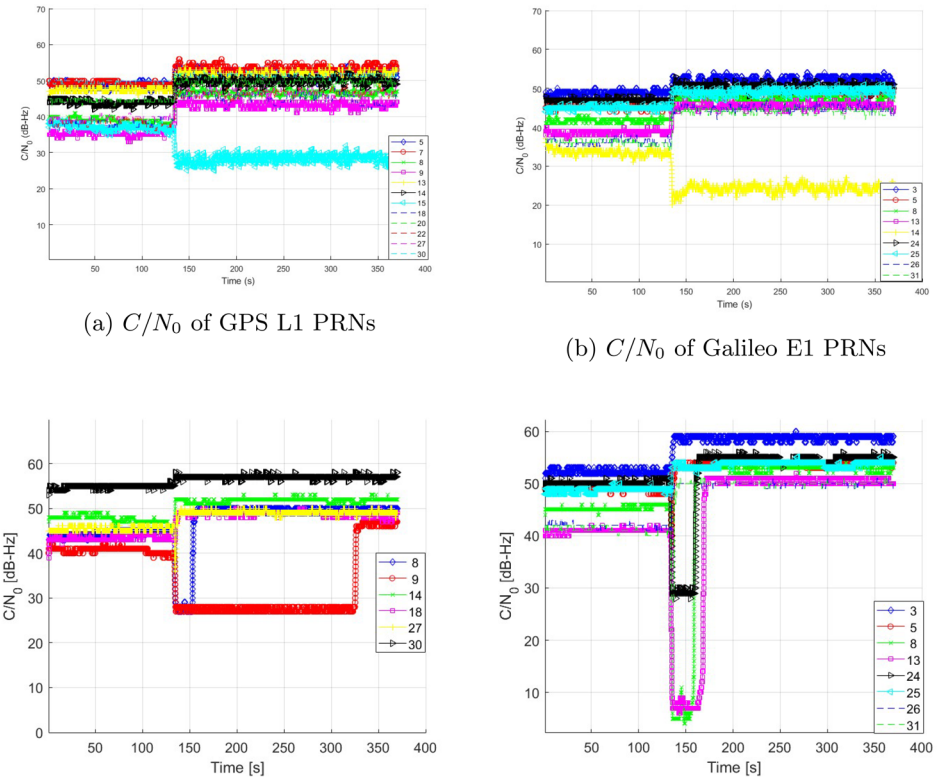


Fig. 12 C/N_0 of Targeted DFMC scenario

(a) C/N_0 of GPS L1 PRNs

(b) C/N_0 of Galileo E1 PRNs

(c) C/N_0 of GPS L5 PRNs

(d) C/N_0 of Galileo E5a PRNs

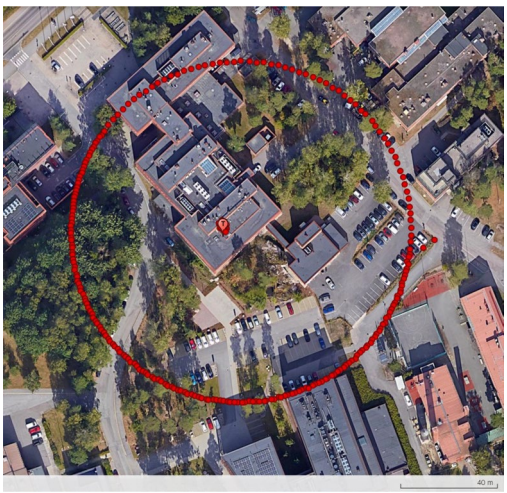


Fig. 13 Position estimated by the device under test

execution of the spoofing attack. Moreover, a brief period is required for the synchronization between signal generation by Skydel simulator and the streaming of RF signals by the USRP. It is important to note that the impacts of a spoofing signal may not be immediately noticeable in the analysis upon injection due to the delay mentioned above.

- **Targeted SFMC** Figure 7 illustrates the tracking results of PRN 03 of GPS L1 signal. The figure indicates smooth takeover of the receiver tracking loop by the spoofer. Following the injection of the spoofing signal at approximately 131 s, no loss of lock is observed. However, significant jumps in the amplitude of both the real and imaginary components of the prompt correlator are observed since both noise and signal power increase. The estimated Doppler exhibited the expected behaviour, and the Phase-Locked Loop (PLL) and Frequency-Locked Loop (FLL) maintained consistent lock throughout the duration. Although there are clear changes in FLL and PLL and the corresponding Doppler, these are well within the anticipated range.

  The analysis of targeted spoofing attack is further supported by the results presented in Fig. 8a, b. Both GPS and Galileo PRN experienced harmonious jumps in their C/N_0 values, averaging 5 dB-Hz. The intended location of the spoofing signal is also distinctly portrayed in Figs. 9 and 10. A circle with a 70-m diameter represents the spoofer's intended location. Figure 10 depicts deviation of East, North and Up components with respect to ground truth.

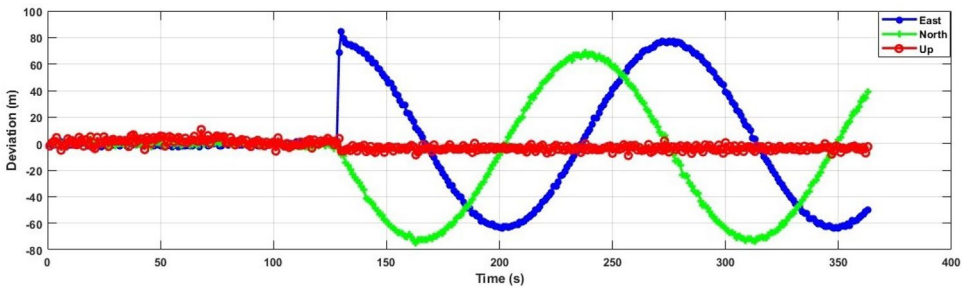


Fig. 14 Position deviation with respect to time

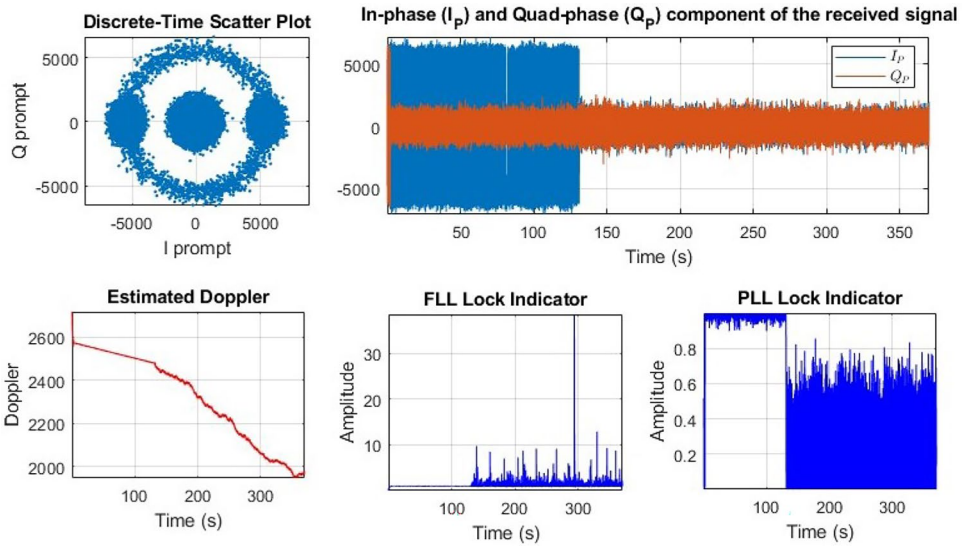


Fig. 15 Tracking result of GPS L1 signal's PRN 15

– **Time synchronous spoofing with multi-correlator monitoring**

Multi-correlator monitoring is used to further assess the alignment of the spoofing signal with the authentic signal. In this process, 41 complex correlators are utilized with a code delay window of ± 2 chips and a 0.1 chips correlator spacing. Figure 11 illustrates the normalized correlation function at various stages of tracking of GPS PRN 7. Before the capture at around 136100^{th} millisecond (ms), the shape of the correlator output resembles a triangle that overlaps with the expected theoretically-generated triangle centered at zero. During the pull-off stage, for example at 136800^{th} ms depicted in Fig. 11b, the spoofing signal coexists with the authentic signal introducing a 0.1 chips delay. Figure 11c then shows an instance at around 137700^{th} ms, indicating successful locking onto the spoofing signal. It is noteworthy that this entire process unfolds rapidly, completing almost within a few seconds. The tight time synchronization between the spoofing signal and the authentic signal presents a substantial challenge for the receiver to successfully detect an ongoing spoofing (Hegarty et al. 2019).

- **Targeted DFMC**

In this scenario targeted spoofing is applied to GPS L5 and Galileo E5a signals in addition to L1 and E1. Figure 12a, b depict the seamless take over of both GPS L1 and Galileo E1 signals that evident in their C/N_0 values. GPS L5 (PRN 8 and 9) and Galileo E5a (PRN 8, 13, and 24) satellites, on the other hand, exhibited a minor delay before locking onto the spoofing signal as seen in Fig. 12c, d. The inherited characteristics of GPS L5 and Galileo E5a, which is designed to provide better resilience against interferences, can be attributable to this delay. These characteristics include longer codes, better modulations, and higher chipping rates.

The positioning performance of GPS L1 and Galileo E1 as illustrated in Figs. 13 and 14, is similar to the previous scenario since both scenarios are characterized by a targeted spoofing attack.

- **Untargeted DFMC**

Figure 15 illustrates the tracking result of GPS L1 signal's PRN 15. After the injection of spoofing signal, the noise takes over, effectively appearing as jamming for the receiver for the rest of the duration. Two primary reasons contributed to this incident. Firstly, the receiver is already at the fine-tracking stage, and secondly, the

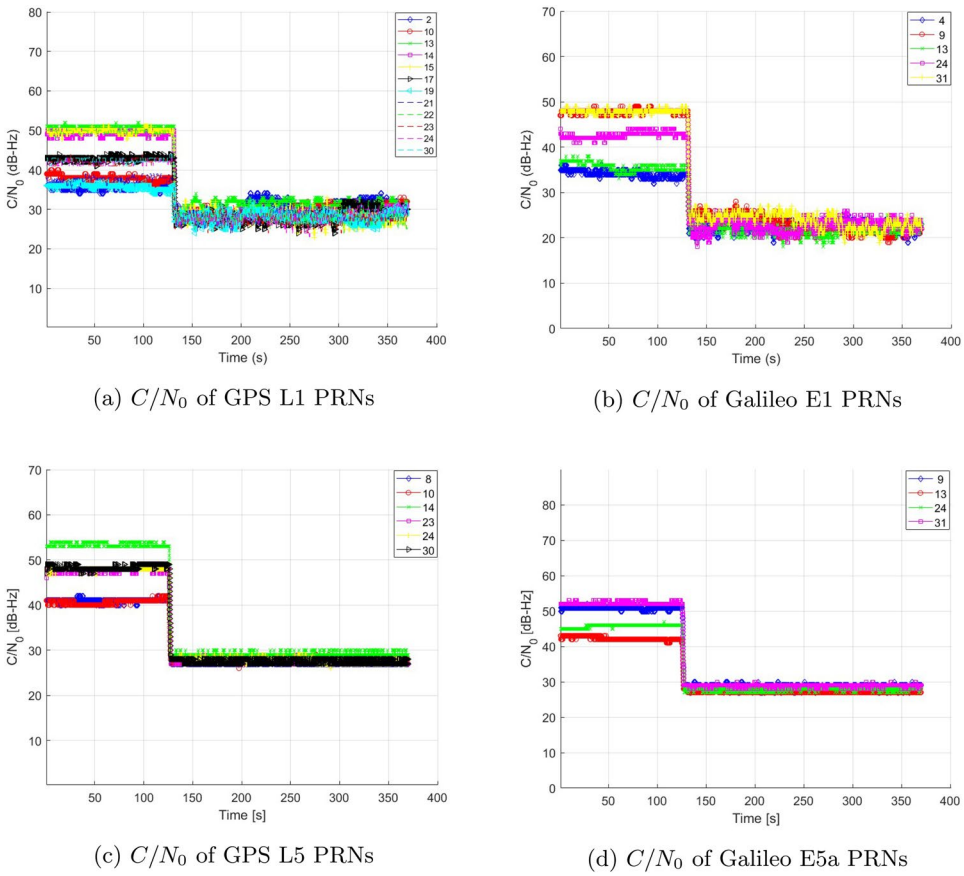


Fig. 16 C/N_0 of Untargeted DFMC scenario

(a) C/N_0 of GPS L1 PRNs

(b) C/N_0 of Galileo E1 PRNs

(c) C/N_0 of GPS L5 PRNs

(d) C/N_0 of Galileo E5a PRNs

Fig. 17 Position estimated by the device under test

spoofing signal is not aligned within the fraction of a code chip.

Once the receiver enters the tracking stage, it has already locked onto the authentic signal, given the assumption that spoofing occurs after a specific initialization period. Unlike the acquisition stage, the receiver would not perform any exhaustive search at the tracking stage. If the carrier frequency and code phase of the spoofing signal are not closely aligned or are far from the authentic signal, the spoofing signal does not attract the receiver. Instead, due to this misalignment, the spoofing signal appears as noise for the receiver. As described in the previous section, the intended spoofed location is simulated 15 kms away from the actual location and 10 h ahead of the actual time, making it asynchronous in both time and position. This particular scenario is designed to reflect a situation where the spoofer possesses no prior information about the target receiver.

If a receiver attempts to re-acquire a signal during an ongoing spoofing attack, it is likely to acquire the signal with the highest peak unless it has access to other assisted information. FGI-GSRx on the other hand is a post-processing receiver, and it does not attempt re-acquisition within the same dataset. Further discussion on this situation is provided in the meaconing section. The impact of the asynchronous attack is illustrated in Fig. 16. Following the injection of the spoofing signal, the estimated C/N_0 of all satellites exhibit a sharp decline for all the analyzed GPS and Galileo signals.

Figures 17 and 18 demonstrate that the receiver is not spoofed to the intended location, but a denial of service appears after the injection of the spoofing signal. The navigation solution is computed based on the predefined criteria described earlier that incorporate elevation and

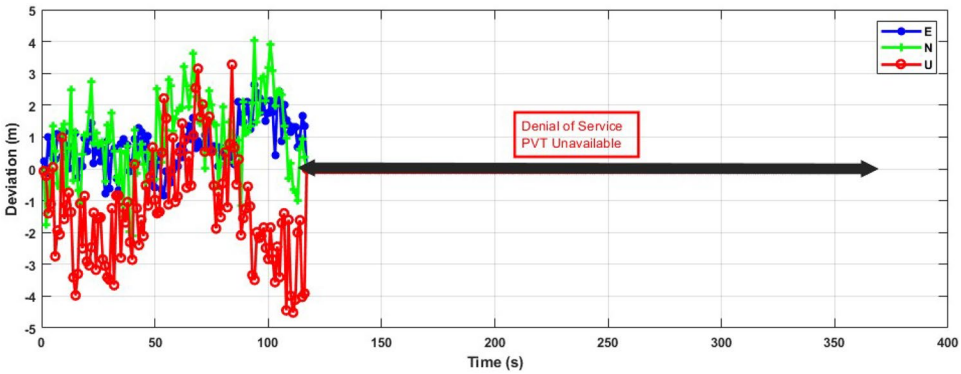


Fig. 18 Position deviation with respect to true position

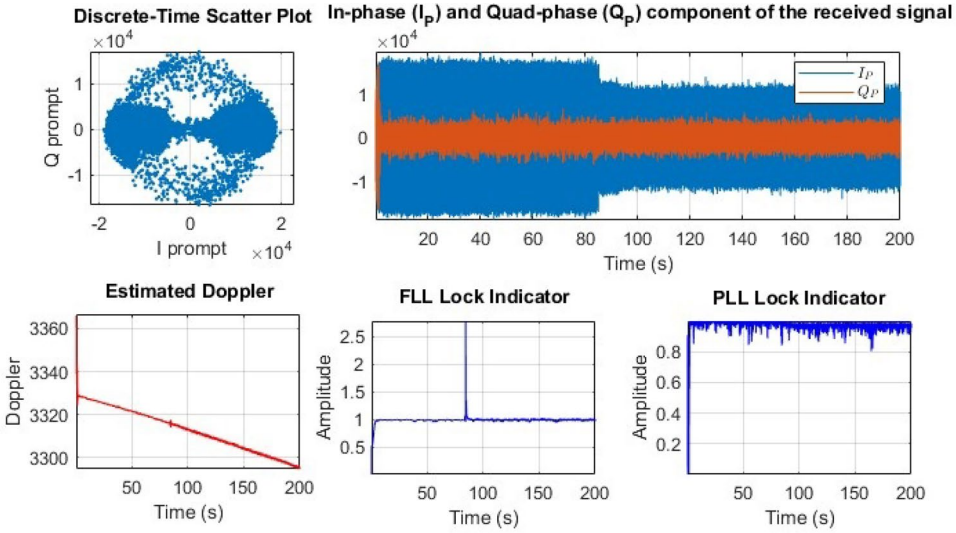


Fig. 19 Tracking loop of Galileo PRN 2

C/N_0 thresholds. Following the injection of the spoofing signal, the initially set thresholds no longer meets the criteria, thereby preventing the receiver from offering any PVT solution.

In summary, the FGI-GSRx successfully resisted spoofing attempts. It is also pertinent to mention here that although these non-coherent attacks result in an unsuccessful spoofing attempt, they can still pose a threat by mimicking jamming. This is inline with the other intention of the spoofer otherwise referred to as *denial of service*.

- **Meaconing DFMC**

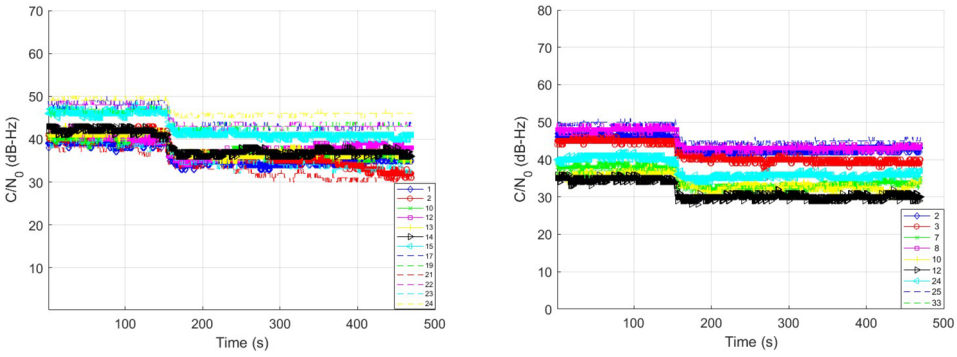
  Re-transmission of authentic signals often represents an asynchronous attack, wherein, in the worst-case scenario, there might be a complete misalignment in position and time. The code and carrier mismatch in the meaconing signal, resulting in a noise signal that essentially appears as a jamming signal. The impact of this phenomenon can be observed in Fig. 20a–d, where the injection of meaconing leads to a drop in C/N_0 values for all satellites.

The tracking loop performance of a Galileo E5a satellite is illustrated in Fig. 19. After the injection of the meaconing signal, a slight degradation in signal power becomes visible. Despite this, the Doppler, Frequency-Locked Loop (FLL), and Phase-Locked Loop (PLL) maintained their locks.

The effect of meaconing attack may not be uniform across all GNSS receivers; those with re-acquisition capabilities may respond differently compared to receivers like FGI-GSRx. For instance, when re-transmission occurs with significantly high power, it can introduce additional noise and eventually saturate the receivers. Afterwards, the affected receiver might attempt a re-acquisition, potentially locking onto the spoofing signal. This phenomenon is of particular interest for observation with Commercial off-the-shelf (COTS) receivers (Islam et al. 2023).

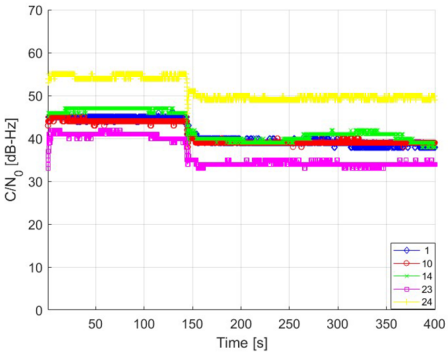
Figures 21 and 22 shows the positioning performance of FGI-GSRx during the meaconing attack. Contrary to expectations, the receiver did not lock onto the spoofing signal, indicating that it remained unspoofed.

Fig. 20 C/N_0 of Meaconing DFMC scenario

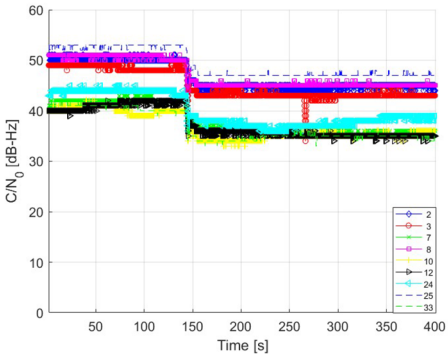


(a) C/N_0 of GPS L1 PRNs

(b) C/N_0 of Galileo E1 PRNs



(c) C/N_0 of GPS L5 PRNs



(d) C/N_0 of Galileo E5a PRNs

Fig. 21 Position estimated by the device under test

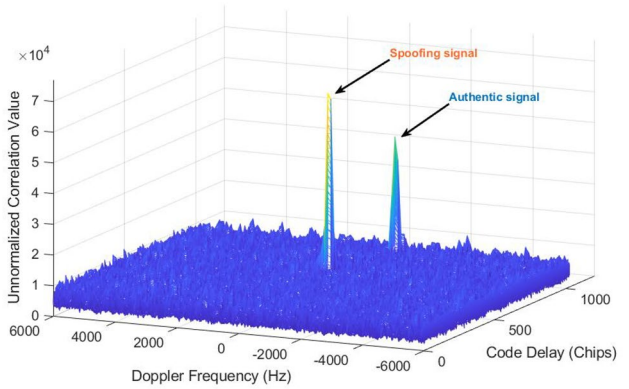


Fig. 23 Code-Doppler search result at 165^{th} second by FGI-GSRx acquisition block

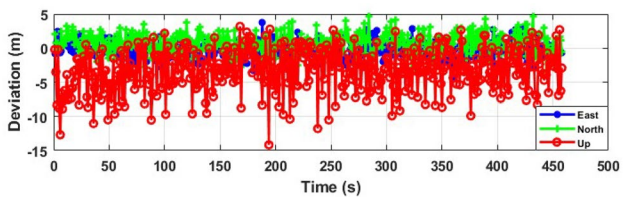


Fig. 22 Position deviation with respect to time

– **Cold start during ongoing spoofing event**

The conventional assumption is that a receiver is operational before a spoofer injects the spoofing signals. However, what if the receiver starts operation during an ongoing spoofing event? An analysis is conducted using the meaconing scenario to explore this hypothesis. The receiver is switched-on in cold-start mode and it begins the acquisition

Table 4 Summary of positioning performance

Scenario	Signal subdivision	Duration (s)	ε_{3D}	ε_H	σ_H	ε_V	σ_V
TG SFMC	L1+E1	370	55.58	51.95	32.68	19.76	5.57
	L5+E5a	370	6.93	4.23	0.24	5.49	0.45
	L1+E1+L5+E5a	370	34.46	32.15	19.52	12.34	7.2
TG DFMC	L1+E1	370	56.69	53.07	33.40	19.93	2.00
	L5+E5a	370	55.84	55.17	31.69	8.64	5.38
	L1+E1+L5+E5a	370	56.05	55.84	32.43	4.85	2.14
UT DFMC	L1+E1	370	2.86	1.92	0.93	2.11	1.12
	L5+E5a	370	8.49	2.24	0.13	8.19	0.35
	L1+E1+L5+E5a	370	4.79	2.38	0.46	4.15	1.05
Meconing DFMC	L1+E1	470	4.83	2.93	0.96	3.84	2.64
	L5+E5a	470	4.23	1.32	0.32	4.01	0.45
	L1+E1+L5+E5a	470	2.58	1.50	0.50	2.09	0.89

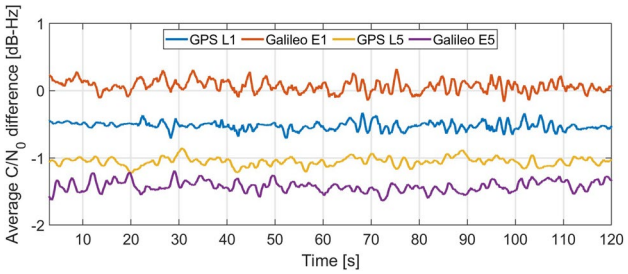


Fig. 24 Average C/N_0 difference between a replayed-recorded and the originally recorded targeted DFMC data

process at around 165^{th} second, when both authentic and spoofing signals are present. Under such a situation, a receiver is likely to pick up the signal with the highest peak, unless any other assisted information is available. Figure 23 illustrates the acquisition search space for the PRN 15 of the GPS L1 signal. As both authentic and spoofing signals coexist during the acquisition, the receiver picks up the spoofing signal with the highest peak. This susceptibility is particularly significant in untargeted and meaconing attacks given their untargeted nature, assuming a substantial offset in the code phase between the spoofing and the authentic signals (Li et al. 2020).

Although, as illustrated in Fig. 20a–d, the receiver is not spoofed during the tracking stage, acquisition or re-acquisition during ongoing spoofing events may expose the GNSS receiver to potential threats from meaconing and untargeted attacks. Therefore, the identification of multi-peaks during the acquisition stage (Humphreys et al. 2008) is vital, especially when the receiver lacks additional assisted information.

- **Summary Results**

  Table 4 provides a comprehensive overview of the positioning solution acquired across various scenarios and signal combinations by using both open-source and in-house versions of FGI-GSRx. In this table, symbols ε_{3D}, ε_H, and ε_V represent 3-Dimensional Root-Mean-Square (RMS), horizontal RMS, and vertical RMS in meters respectively, while σ_H and σ_V denote horizontal and vertical standard deviation in meters. In the Targeted SFMC scenario, GPS L5 and Galileo E5a signals are not simulated to be spoofed. Therefore, the L1+E1 solution is seen to be much deviated compared to the L5+E5a solution. It is vital to analyze the positioning performance under the combination of signals including both spoofing and unspoofing ones. Processing all signals together yields superior results compared to processing only spoofing signals, as evident in the Targeted SFMC scenario. In the Targeted DFMC scenario, all four signals are spoofed, and the estimated positioning solution by FGI-GSRx reflects the spoofer's intended location in all the three combinations. For the Untargeted DFMC and Meaconing DFMC scenarios, FGI-GSRx remains unspoofed across all combinations. However, in the Untargeted DFMC scenario, a denial of service is observed after 120 s due to the impact of the spoofing signal on the receiver that appeared as jamming for the receiver. With a C/N_0 threshold of 30 dB-Hz, there are not enough satellite measurements available for position computation. Consequently, it can be said that in case of Untargeted DFMC, the receiver is not compromised to the spoofer's desired location, but it indeed experiences the denial of offering positioning service right after the injection of spoofing signal.
- **Validation Results for Replayed I/Q data**

  Figure 24 shows average observed loss in tracking C/N_0 for a replayed-recorded targeted DFMC scenario. The I/Q data was recorded using the setup defined in

Sect. 2. The Galileo E5a signal showed a loss of around 1.5 dB-Hz compared to the original DFMC dataset, while no significant loss in C/N_0 was observed for Galileo E1. The observed loss can be caused by a few reasons like added thermal noise and clock jitter from the process of transmitting and receiving the signal, or other inaccuracies in reproducing the digitized baseband signal back to RF. Different outcomes could be observed if parameters, like signal bandwidth and sample rate, or different transmitter and GNSS front-end were used.

Conclusion and future work

This paper presents raw GNSS spoofing datasets across four scenarios, analyzed with an updated version of FGI-GSRx software receiver. The new set of raw I/Q spoofing data, comprising live-sky GNSS signals, fills a notable gap in existing datasets, enhancing the available resources to the GNSS community. Notably, these datasets cover multiple GNSS frequencies and incorporate cryptographic signatures (OSNMA) in Galileo E1-B data channel, positioning them as potential benchmarks for evaluating the resilience performance of multi-frequency multi-constellation receivers. An updated open-source version of FGI-GSRx is provided alongside the datasets with the necessary features for processing and analyzing the new data. This research aims to deepen our understanding of complex spoofing attacks on GNSS signals, offering insights into the challenges and opportunities for improving resilience in navigation systems. The datasets and analyses presented here provide a foundation for future research on GNSS technologies against evolving spoofing threats, thus contributing to the ongoing effort to safeguard satellite navigation systems worldwide.

The authors are currently working towards implementation of Galileo's OSNMA-based spoofing detection in FGI-GSRx. In addition, the authors plan to implement a robust GNSS anomaly detection technique based on a combination of different receiver parameters. These include Automatic Gain Control (AGC) variation at the front-end level, phase and Doppler change rate detection at the tracking level, and the authentication status flag based on navigation message authentication at the navigation level.

Acknowledgements Special acknowledgement goes to the Safran MINERVA academic programme for donating the Skydel simulator.

Author Contributions Conceptualization: SI and ZB; Methodology: SI and ZB; Data curation: SI, IP, ML; Formal analysis and investigation: SI, ZB, ML, IP; Software: SI, ZB, ML, IP; Writing - original draft preparation: SI; Writing - review and editing: SI, ZB, ML, IP, SK; Funding acquisition: ZB, SK; Resources: SI, ZB, ML, IP, SK; Supervision: ZB. All authors commented on previous versions of the manuscript.

Funding Open Access funding provided by National Land Survey of Finland. This work has been supported by the Academy of Finland's special funding for research into crisis preparedness and security of supply (project REASON - Resilience and Security of Geospatial Data for Critical Infrastructures) and the National Emergency Supply Agency of Finland programme Digital Security 2030.

Availability of data and materials The four datasets, including the updated version of the FGI-GSRx and auxiliary scripts for potential replay, can be accessed at the following webpage (https://www.maanmittauslaitos.fi/en/research/research/gnss-specialists/fgi-gnss-jamming-and-spoofing-dataset-repository-fgi-jsdr). Table 3 contains detailed information about scenarios, folder names, and dataset sizes. The Finnish Geospatial Research Institute (FGI) has made these datasets and related scripts available to researchers and other interested stakeholders. This initiative aims to enhance the robustness and effectiveness of receiver-based spoofing detection and mitigation techniques, thereby strengthening overall security measures in satellite-based navigation systems. All updates of the open-source FGI-GSRx receiver will be available along with the corresponding release notes. If there are any further inquiries, please feel free to contact FGI.

Declarations

Consent for publication All authors reviewed and approved the final manuscript.

Conflict of interest The authors declare no conflict of interest.

References

Albright A, Powers S, Bonior J, Combs F (2020) Oak ridge spoofing and interference test battery (OAKBAT) - GPS. In: Proceedings of the 33rd international technical meeting of the satellite division of the institute of navigation (ION GNSS+ 2020), pp 3697–3712. https://doi.org/10.13139/ORNLNCCS/1664429

Anderson JM, Carroll KL, DeVilbiss NP, Gillis JT, Hinks JC, O'Hanlon BW, Rushanan JJ, Scott L, Yazdi RA (2017) Chips-message robust authentication (chimera) for GPS civilian signals. In: Proceedings of the 30th international technical meeting of the satellite division of the institute of navigation (ION GNSS+ 2017), pp 2388–2416

Broumandan A, Jafarnia-Jahromi A, Lachapelle G (2015) Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver. GPS Solut 19:475–487

Cavaleri A, Motella B, Pini M, Fantino M (2010) Detection of spoofed GPS signals at code and carrier tracking level. In: 2010 5th ESA workshop on satellite navigation technologies and European workshop on GNSS signals and signal processing (NAVITEC), pp 1–6

ESA (2021) Galileo Open Service Navigation Message Authentication (OSNMA)

EUSPA (2023a) European GNSS (Galileo) Services Open Service Quarterly Performance Report October–December 2022 [Accessed on 12 03, 2023]. https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo-OS-Quarterly-Performance_Report-Q4-2022.pdf

EUSPA (2023b) The ultimate response to maritime spoofing attacks [Accessed on 11 27, 2023]. https://www.euspa.europa.eu/newsroom/news/asgard-ultimate-response-maritime-spoofing-attacks

FGI-NLS (2022) FGI-GSRx software receiver [Accessed on 12 10, 2023]. https://www.maanmittauslaitos.fi/en/fgi-gsrx-os

Gamba MT, Truong MD, Motella B, Falletti E, Ta TH (2017) Hypothesis testing methods to detect spoofing attacks: a test against the TEXBAT datasets. GPS Solut 21:577–589

GPSWorld (2023) Increasing GNSS interference: UK and EU warn aviation [Accessed on 11 27, 2023]. https://www.gpsworld.com/increasing-gnss-interference-uk-and-eu-warn-aviation/

Guo Y, Miao L, Zhang X (2018) Spoofing detection and mitigation in a multi-correlator GPS receiver based on the maximum likelihood principle. Sensors 19(1):37

Hegarty C, O'Hanlon B, Odeh A, Shallberg K, Flake J (2019) Spoofing detection in GNSs receivers through cross-ambiguity function monitoring. In: Proceedings of the 32nd international technical meeting of the satellite division of The Institute of Navigation (ION GNSS+ 2019), pp 920–942

Homeland S (2022) Resilient Positioning, Navigation, and Timing (PNT) Conformance Framework

Humphreys TE, Bhatti JA, Shepard DP, Wesson KD (2012) The Texas spoofing test battery: toward a standard for evaluating GPS signal authentication techniques. https://api.semanticscholar.org/CorpusID:113952187

Humphreys TE, Ledvina BM, Psiaki ML, O'Hanlon BW, Kintner PM et al (2008) Assessing the spoofing threat: development of a portable GPS civilian spoofer. In: Proceedings of the 21st International technical meeting of the satellite division of the institute of navigation (ION GNSS 2008), pp 2314–2325

Islam S, Bhuiyan MZH, Pääkkönen I, Saajasto M, Mäkelä M, Kaasalainen S (2023) Impact analysis of spoofing on different-grade GNSS receivers. (2023) IEEE/ION Position. Location and Navigation Symposium (PLANS), pp 492–499. https://doi.org/10.1109/PLANS53410.2023.10139934

Jafarnia-Jahromi A, Broumandan A, Nielsen J, Lachapelle G (2012) GPS vulnerability to spoofing threats and a review of antispoofing techniques. Int J Navig Observ

Kai B, Ignacio F-H, José A, L-S, Bhuiyan MZH (2022) GNSS software receivers. Cambridge University Press. https://doi.org/10.1017/9781108934176

Khan AM, Iqbal N, Khan AA, Khan MF, Ahmad A (2020) Detection of intermediate spoofing attack on global navigation satellite system receiver through slope based metrics. J Navig 73:1052–1068

Kuusniemi H, Blanch J, Chen Y-H, Lo SC, Innac A, Ferrara GN, Honkala S, Bhuiyan MZH, Thombre S, Söderholm S, Walter T, Phelts RE, Enge PK (2017) Feasibility of fault exclusion related to advanced RAIM for GNSS Spoofing detection. https://api.semanticscholar.org/CorpusID:67182166

LabSat (2023) LabSat 3 Wideband Record and Replay Device [Accessed on 12 03, 2023]. https://www.labsat.co.uk/index.php/en/products/labsat-3-wideband

Li J, Zhu X, Ouyang M, Li W, Chen Z, Dai Z (2020) Research on multi-peak detection of small delay spoofing signal. IEEE Access 8:151777–151787. https://doi.org/10.1109/ACCESS.2020.3016971

Lin H, Qing Y (2015) GPS spoofing low-cost GPS simulator. In: Proceedings of the DEF CON, 23

Magiera J, Katulski R (2015) Detection and mitigation of GPS spoofing based on antenna array processing. J Appl Res Technol 13(1):45–57

Montgomery PY, Humphreys TE, Ledvina BM (2009) Receiver-autonomous spoofing detection: experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer. In: Proceedings of the 2009 international technical meeting of the institute of navigation, pp 124–130

Motella B, Nicola M, Damy S (2021) Enhanced gnss authentication based on the joint chimera/osnma scheme. IEEE Access 9:121570–121582

Noll CE (2010) The crustal dynamics data information system: a resource to support scientific analysis using space geodesy. Adv Space Res 45(12):1421–1440

Orouji N, Mosavi M (2021) A multi-layer perceptron neural network to mitigate the interference of time synchronization attacks in stationary GPS receivers. GPS Solut 25:1–15

Pany T, Akos D, Arribas J, Bhuiyan MZH, Closas P, Dovis F, Fernandez-Hernandez I, Fernández–Prades C, Gunawardena S, Humphreys T et al (2024) Gnss software-defined radio: history, current developments, and standardization efforts. NAVIGATION J Inst Navig 71(1)

Perdue L, Sasaki H, Boime G, Sicsik-Paré E (2016) 1.4 - Testing GNSS receivers robustness against spoofing attempts, pp 33–39. https://doi.org/10.5162/etc2016/1.4

Phelts RE (2001) Multicorrelator techniques for robust mitigation of threats to GPS signal quality. Stanford University

Safran (2023) Safran Skydel GNSS Software Simulator [Accessed on 12 10, 2023]. https://www.safran-group.com/products-services/skydel-gnss-simulation-software

Septrentio (2023) High-precision geodetic full GNSS spectrum choke ring antenna [Accessed on 12 10, 2023]. https://www.septentrio.com/en/products/antennas/polant-chokering

Shang X, Sun F, Zhang L, Cui J, Zhang Y (2022) Detection and mitigation of GNSS spoofing via the pseudorange difference between epochs in a multicorrelator receiver. GPS Solut 26:1–14

Söderholm S, Bhuiyan MZH, Thombre S, Ruotsalainen L, Kuusniemi H (2016) A multi-GNSS software-defined receiver: design, implementation, and performance benefits. Ann Telecommun. https://doi.org/10.1007/s12243-016-0518-7

Turner M, Wimbush S, Enneking C, Konovaltsev A (2020) Spoofing detection by distortion of the correlation function. In: 2020 IEEE/ION position, location and navigation symposium (PLANS), pp 566–574

Saiful Islam received the M.Sc. (Tech.) degree (Hons.) from Tampere University (TAU), Finland, in 2019, where he is currently pursuing the Ph.D. degree. He is also a Research Scientist at the Finnish Geospatial Research Institute (FGI-NLS). He is a member of the Navigation and Sensing Technologies Group, Department of Navigation and Positioning, FGI-NLS. He is involved in research projects on GNSS receiver development and validation, timing algorithms, maritime navigation, LEO-PNT, GNSS jamming, and spoofing. He is one of the key people in the implementation of the GPS L5 solution in FGI-GSRx. His research interests include GNSS signal processing, resilient software-defined radio (SDR) development, satellite-based augmentation systems (SBAS), and 5G new radio (NR).

Mohammad Zahidul H. Bhuiyan is a Research Professor at the Department of Navigation and Positioning in Finnish Geospatial Research Institute. He is also serving as an Adjunct Professor in Tampere University. His main research interests include multi-GNSS receiver development, PNT robustness and resilience, seamless positioning, LEO-PNT user receiver development, etc. He has been also working as a Technical Expert for the EU Agency for the Space Program (EUSPA) in H2020/Horizon Europe project reviewing and proposal evaluation.

Muwahida Liaquat received her BE Computer Engineering, ME Electrical Engineering in 2004 and 2006 respectively. She received Ph.D Electrical Engineering degree with specialization in signal processing and control systems from National University of Sciences and Technology, Pakistan in 2013. She is working as a senior research scientist at the Department of Navigation and Positioning, Finish Geospatial Research Institute, National Land Survey of Finland, and is also affiliated with NUST, Pakistan. Her research focuses on various aspects of multi-tier GNSS and LEO-PNT receiver design, GNSS vulnerabilities identification and mitigation and sensor fusion algorithms.

Into Pääkkönen is an assistant research scientist at the Department of Navigation and Positioning at Finnish Geospatial Research Institute (FGI). He holds a B.Sc. (Tech.) degree and M.Sc. (Tech.) degree from Aalto University, Finland, with a major in engineering physics and M.Sc (Tech.) degree. Into's interests include signal processing, applied physics, and navigation and communication technologies. His current research at FGI focuses on GNSS and LEO-PNT simulation and receiver development, and varying topics related to resilient PNT such as IMU-GNSS fusion. He has also contributed to the development of FGI-GSRx GNSS software receiver with GPS L1C and Galileo HAS processing capabilities.

Sanna Kaasalainen is a professor and head of the Department of Navigation and Positioning at the National Land Survey of Finland. She has a long-term research career in positioning, remote sensing, optics, and space sciences. She is a member of the European Commission Space Program Committee for Galileo EGNOS Configuration and the navigation Program Board at the European Space Agency.