NAVISP-EL1-064

BREGO

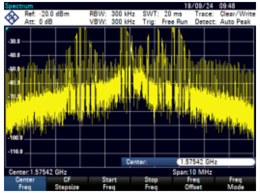
Block-box for an optimised GNSS spectrum monitoring network using artificial intelligence

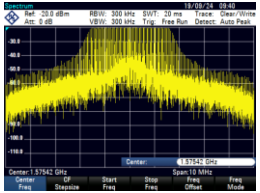
FINAL PRESENTATION
13/12/2024

Contract No. 4000139928/22/NL/WC

BREGO Project: Introduction, objectives and rationale

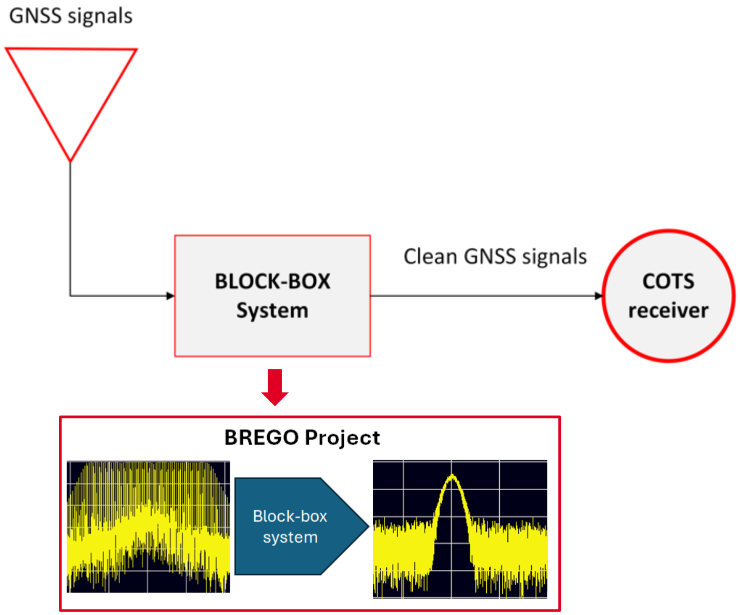
- GNSS provides the ability to determine the position, velocity and time of a receiver globally.
- GNSS has been used in different domains covering safety critical applications, liability critical and commercial applications and others.
- However, relatively low-power signal (sensitive to jamming) that can nullified GNSS signals and the openness of the signal structures, specifically GPS L1 and E1 (sensitive to spoofing).





The rationale:

- Motivates the development towards solutions aiming at providing resilient navigation in environments dominated by GNSS threats, such as Radio Frequency Interference or Spoofing.
- Develops a signal cleaner system that is receiver-agnostic, flexible, configurable, and can be implemented without changing an existing infrastructure.



Objectives:

- The BREGO project aims at Developing and demonstrating algorithms for jamming and spoofing detection, characterisation and mitigation of GNSS signals.
- providing a real-time jamming and spoofing detection, classification and mitigation by means of optimised signal processing techniques driven by AI and machine learning algorithms.

BREGO Project: development and implementation steps

Phase 1: Software and algorithm development (MATLAB software)

- Review of State of the Art for GNSS Threats, Detection and Mitigation techniques.
- Trade-Off and Technical Specification Consolidation.
- AI/ML and DSP based Interference Detection and Mitigation Algorithms Modelling and Preliminary Testing
  - SW modelling and testing to test all the candidate algorithms .
  - The usage of in-house dataset for training purposes across all the testing phases to support AI/ML design and testing for jamming and spoofing detection and classification.

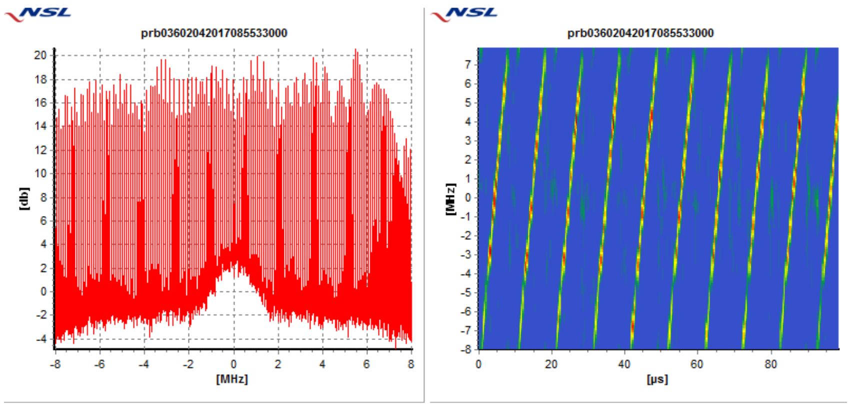
Phase 2: Hardware implementation (Hardware and C/C++ software)

- Block-box Software Experimentation and System Design Consolidation.
- Block-Box System Procurement, Development and Integration.
- Block-box System Testing and E2E Validation.
  - Validation activities and experimentation at GMV premises.
- Block-Box System Experimentation
  - Test at GMV UK laboratory with simulated and public TEXBAT dataset.
  - Test Campaign in ESTEC using **JammerTest** data (used for project acceptance test)
  - Jammer test 2024: The event, the Island of Andøya, in Northwestern, features both simple and sophisticated, staged spoofing and jamming attacks, allowing participants to identify potential strengths and weaknesses in their GNSS-based system.

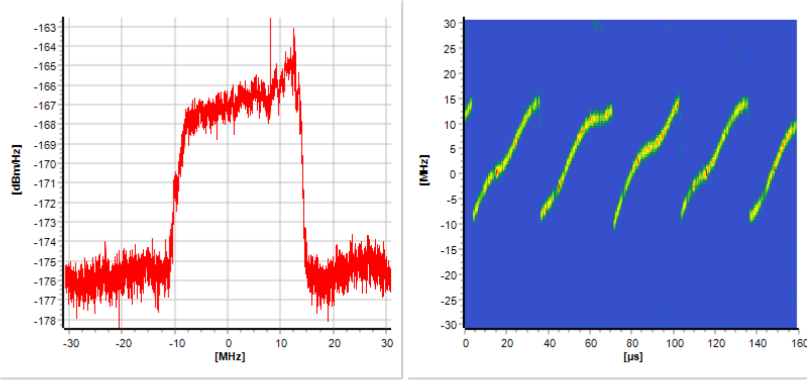
Jamming: Detection and mitigation

Real-life jamming examples:

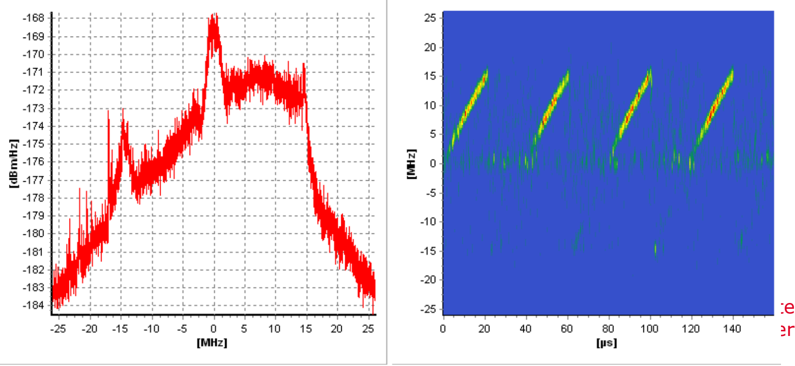
Linear Frequency Modulated



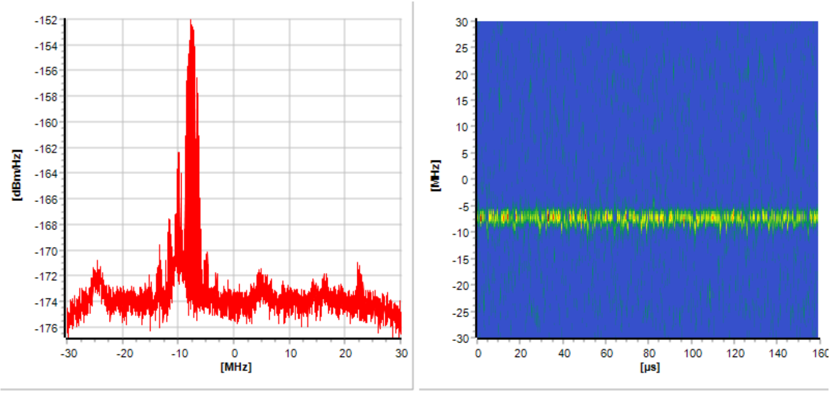
Non-Linear Frequency Modulated



Pulsed Frequency Modulated

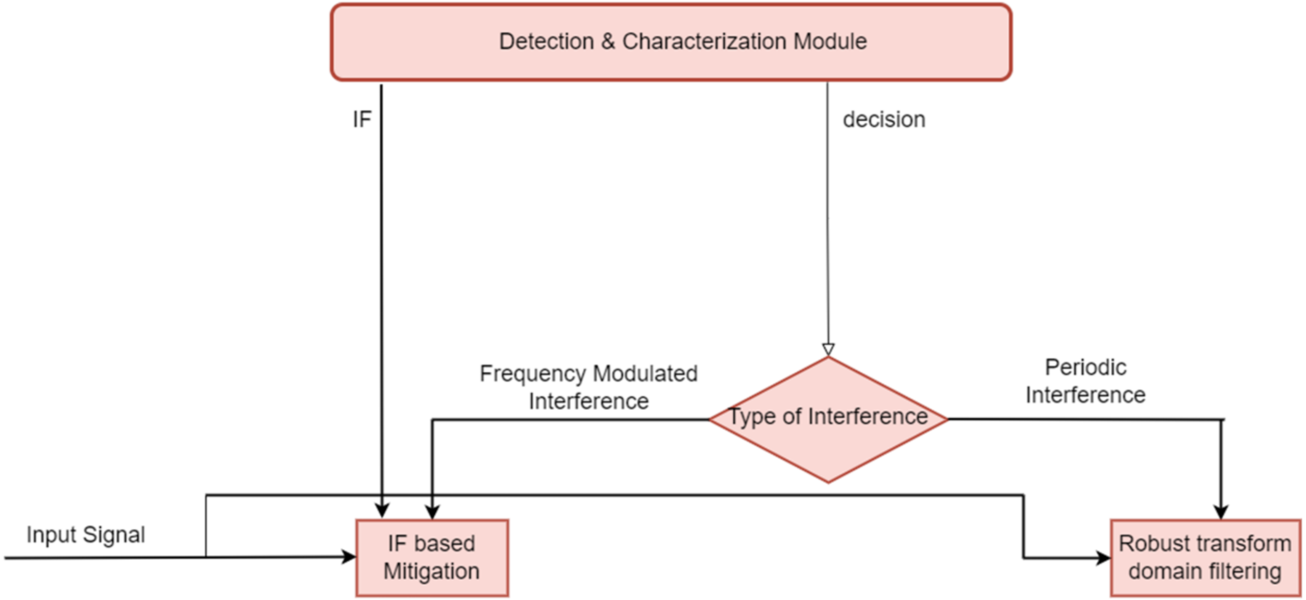


CDMA Interference



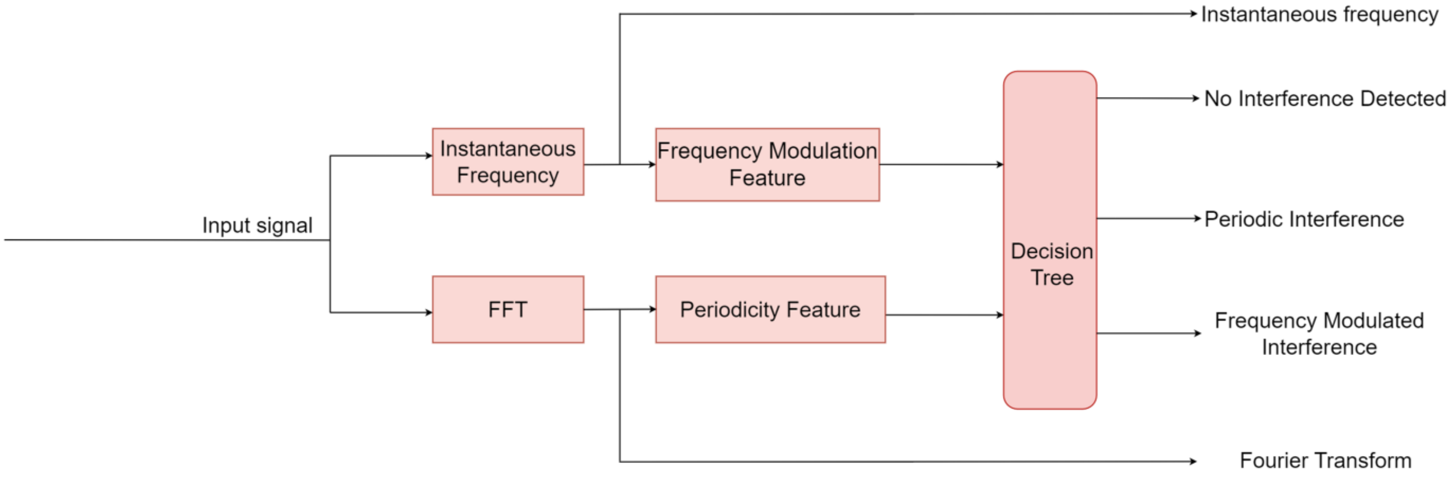
Jamming: Detection and mitigation

Overall Jamming Mitigation System


Detection & Characterization Module
IF
decision
Frequency Modulated Interference
Type of Interference
Periodic Interference
Input Signal
IF based Mitigation
Robust transform domain filtering

Jamming: Detection and mitigation cont’d

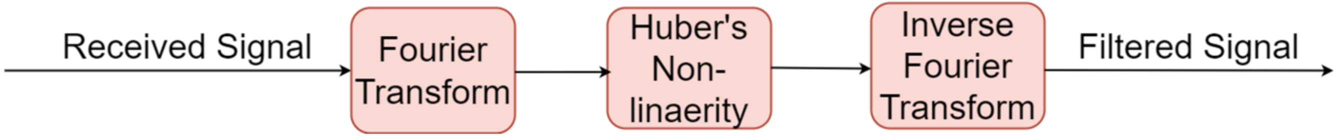
Interference Characterization



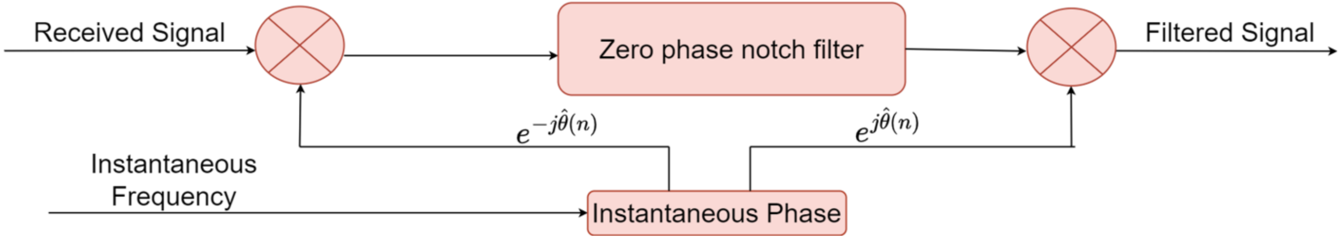
Jamming: Detection and mitigation cont'd

Interference Mitigation

Periodic/CDMA Interference Mitigation

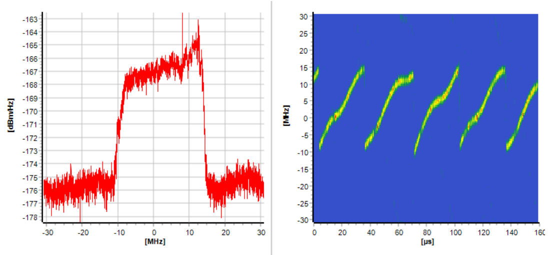


Chirp/Frequency modulated interference mitigation



Jamming: Detection and mitigation cont’d

- Non-periodic non-stationary interferences cannot be mitigated in frequency domain. We need instantaneous frequency-based methods for such signals



- Conventional adaptive notch filter based instantaneous frequency estimation is performed as

$$f_0[n] = f_0[n-1] + 2\mu \angle\left(x[n]x_r^*[n-1]e^{-2j\pi f_0[n-1]}\right)$$

- where, $\mathrm{x_r}[n]$ is obtained through a bandpass filter centered at $f_0[n]$ to reduce the impact of noise:

$$\mathrm{x_r}[n] = (1-\alpha)e^{jf_0[n]}x_r[n-1] + \alpha x[n-1]$$

- We further refine Instantaneous frequency estimate through additional post-processing step:

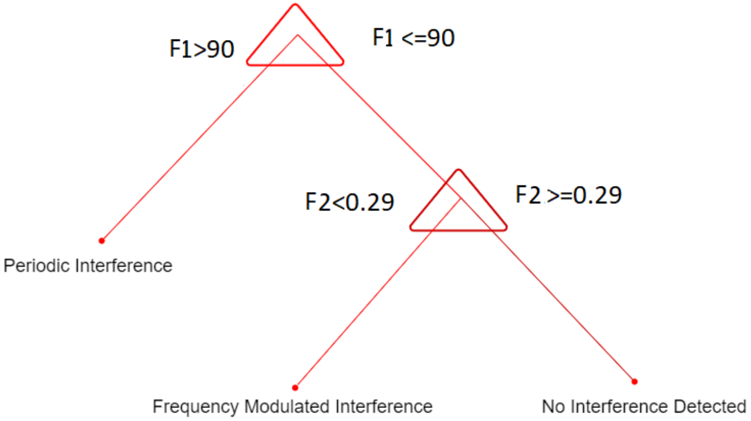
$$\mathrm{f[n]} = \mathrm{f_0[n]} + \frac{\alpha}{2\mathrm{M}+1}\sum_{k=-M}^{M}\left(x[n+k]x_r^*[n+k-1]e^{-jf_0[n+k]}\right)$$

Jamming: Interference Characterization

Training of classifier

- Training Dataset: A roof top clean signal of bandwidth 12 MHz is recorded. Training data is generated by adding both frequencies modulated interferences and periodic interferences to the signal.
- Features Extraction
  - Periodicity Detection Feature (F1): based on the ratio of the peak of FFT and the mean of FFT.
  - Frequency modulation detection Feature (F2): sum of diagonal elements of the covariance matrix of a de-chirped signal normalized by the sum of all elements of the covariance matrix.
- Classification: A decision tree classifier is then trained using MATLAB.

Decision Tree Classifier

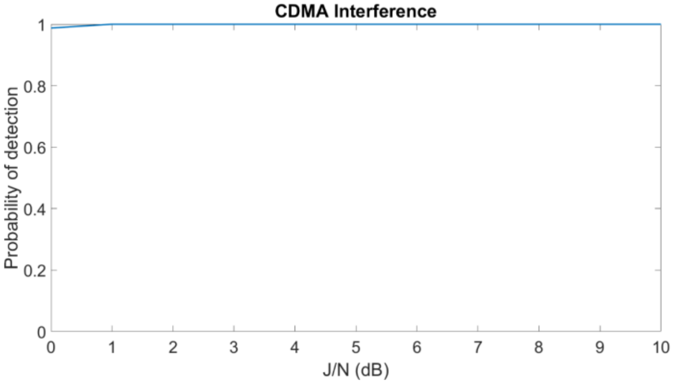


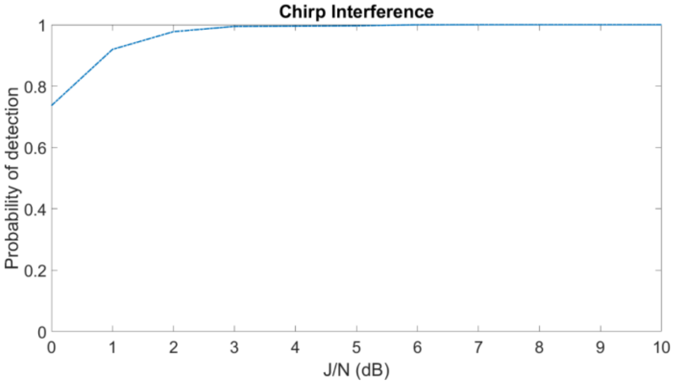
Jamming: characterisation and performance analysis

Probability of detection and probability of false alarm:

Performance evaluation:

1) A clean real-life GNSS signal is corrupted with ramp up interference with J/N levels ranging 0 dB to 10 dB.
2) Each interference level was maintained for 60 second.
3) First 180 second of data are kept free from interference for computing probability of false alarm.
4) The BREGO system is employed to generate the interference characterization results as output for each sample. The stored characterization results are then read by MATLAB file to generate probability of detection and false alarm.

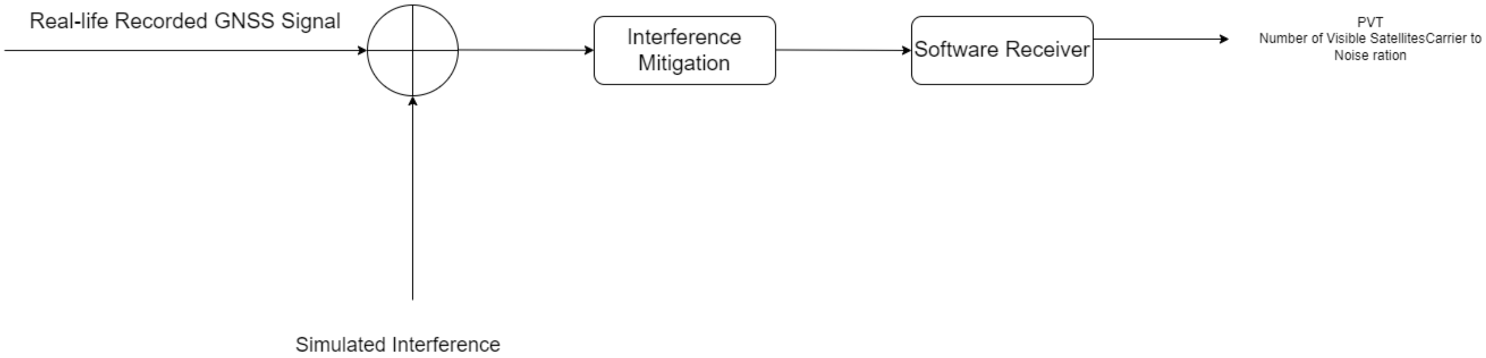




Type of Interference	Probability of false alarm
Chirp	0.0013
CDMA	$<10^{-7}$

Jamming: characterisation and performance analysis cont’d

Simulated results using a snapshot receiver:



Real-life Recorded GNSS Signal

Interference Mitigation

Software Receiver

PVT
Number of Visible SatellitesCarrier to
Noise ration

Simulated Interference

Sampling Frequency: 15 MHz

Criteria for evaluation: Average degradation in $\frac{C}{N_0}$

Performance Comparison:

Adaptive notch filter (ANF)

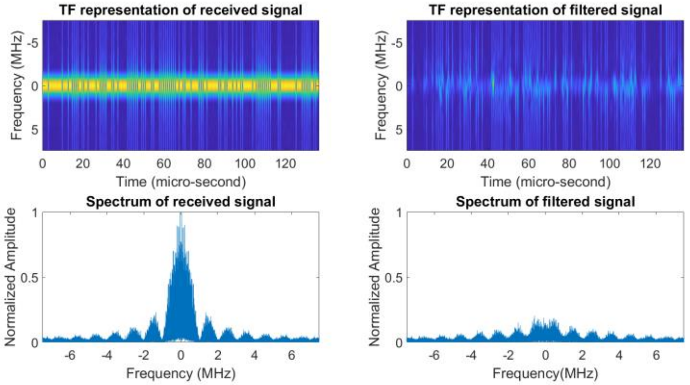
Frequency domain Mitigation (FDM)

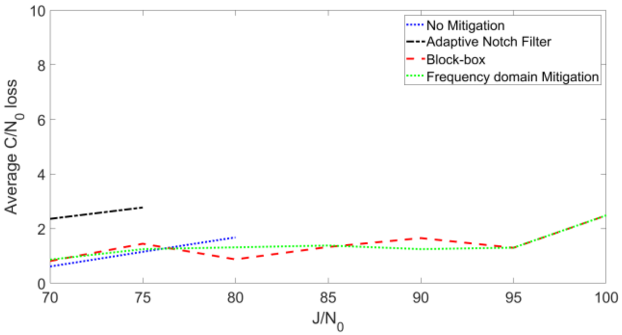
Block-Box (Proposed interference characterization and mitigation system)

Jamming: characterisation and performance analysis cont’d

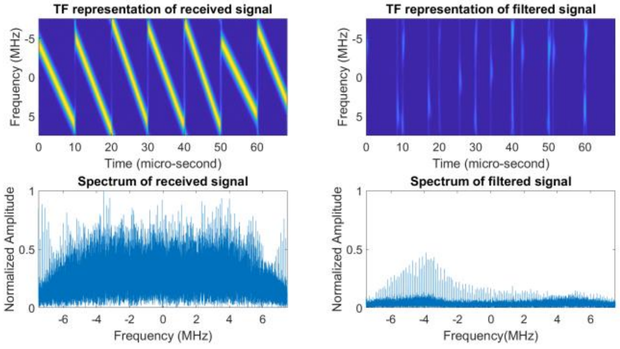
Simulated results using a snapshot receiver

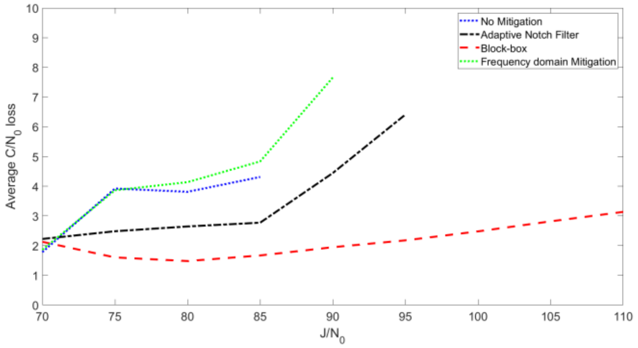
- **CDMA** interference with 1.024 Mega chips per second





- **Chirp** interference with :
  1) Sweep rate: 10 micro-seconds
  2) $f_{\text{min}} = (-4 + 2a_1)MHz$ $f_{max} = (4 + 2a_1)MHz$ where a_1 is uniformly distribution between 0 to1

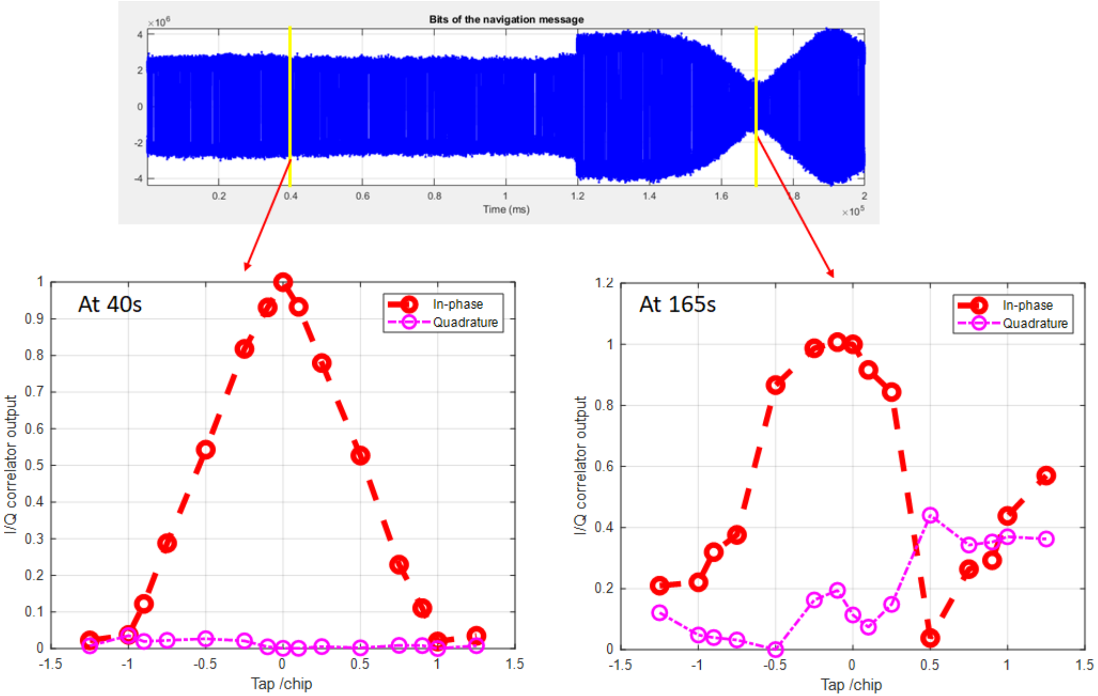




Conclusion: Block-box can mitigate CDMA attack up to 100 dB-Hz and chirp attack up to 110 dB-Hz for snapshot receiver. Frequency domain mitigation is good for CDMA mitigation but not for chirp attacks.

Spoofing: Correlator shapes

- Implementation focus on coherent (overlapping) spoofing on GPS L1



Correlator taps:

E7	E6	E5	E4	E3	E2	E1	P	L1	L2	L3	L4	L5	L6	L7
-1.25	-1	-0.9	-0.75	-0.5	-0.25	-0.1	0	0.1	0.25	0.5	0.75	0.9	1	1.25

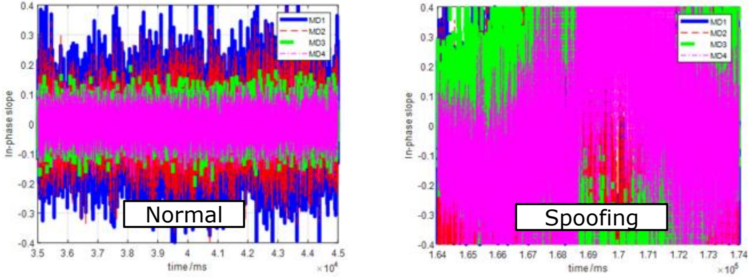
Spoofing: Detection

- List of features for spoofing detection by ML:

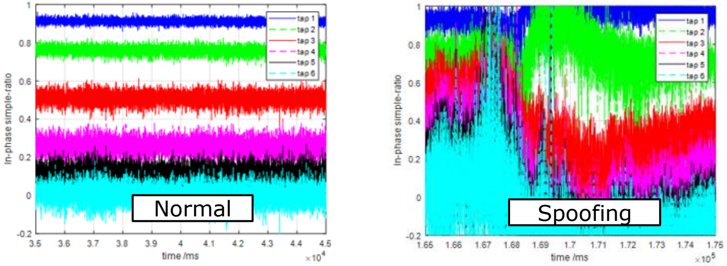
Features	Description
The ratio of partial data bits (beg_end_ratio)	Only on channel I (for DNN and SVM) and for both I and Q channel (for ConvNN)
Slope-based features (MD1, MD2, MD3, MD4)	At four different taps for both I and Q channel
Six Simple ratio	At six different taps (±0.1, ±0.25, ±0.5, ±0.75, ±0.9, ±1) for both I and Q channel
Six Sum ratio	At six different taps (±0.1, ±0.25, ±0.5, ±0.75, ±0.9, ±1) for both I and Q channel
Six Difference ratio	At six different taps (±0.1, ±0.25, ±0.5, ±0.75, ±0.9, ±1) for both I and Q channel
Residual of correlation functions	For both I and Q channel
Skewness of the correlator point	Within a coherent integration cycle (one tracking epoch) for both I and Q channel

- Feature extractions:

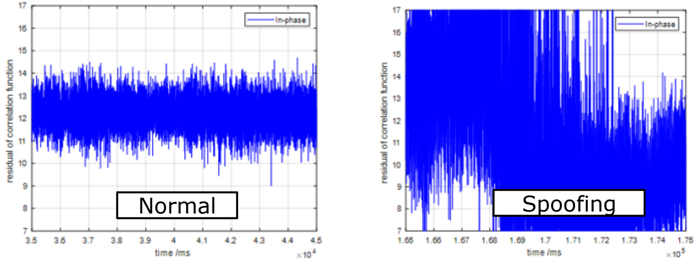
Slope-based feature



SQM ratio: simple, diff, sum

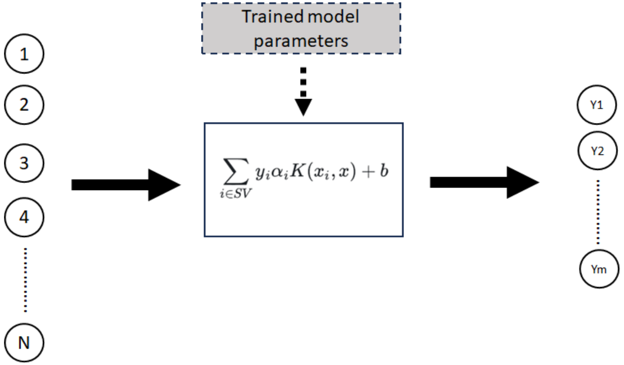


Residual of correlation functions

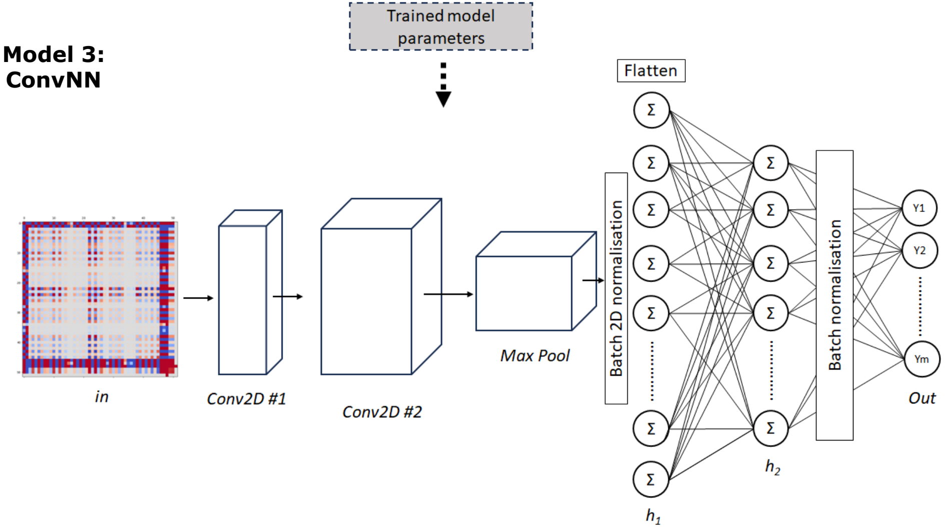


Spoofing: Detection cont'd

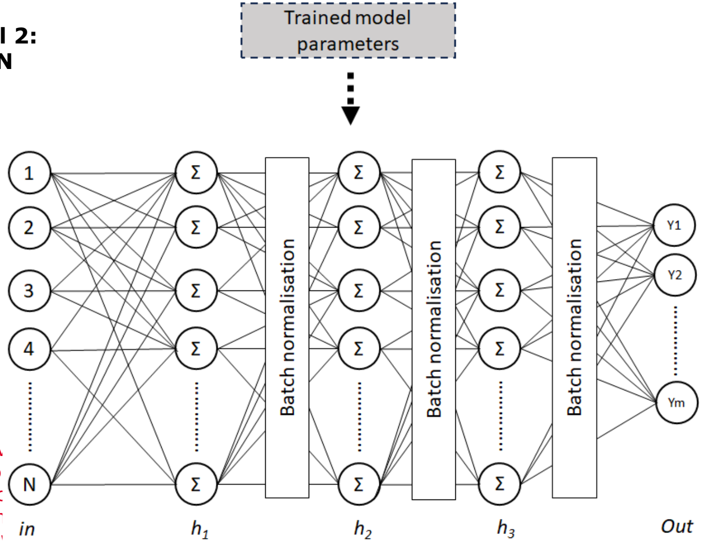
Model 1: Classical SVM



Model 3: ConvNN



Model 2: DNN

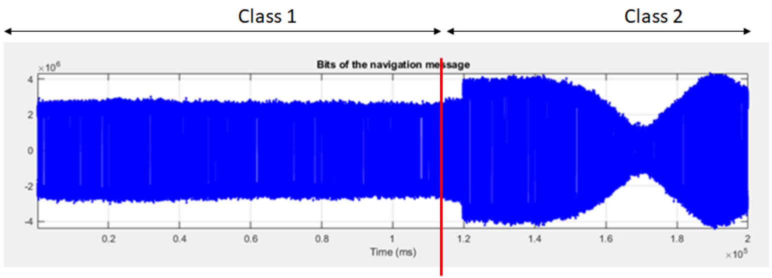


Model number	Model size
Model 1: SVM	52
Model 2: DNN	8418
Model 3: ConvNN	211437

DATASET (Reference)	Description	Total data	Total data points
TEXBAT	• Sampling rate: 25 MHz • Duration: 550-600s per dataset • Format: int16 per sample	10 dataset GPS L1= 2 clean dataset (static & dynamic) + 8 spoofed dataset	±1.4 millions of data points. ±40% for authentic signal class, ±30% for overlapping at prompt spoofing and ±30% for overlapping at NON-prompt.

Spoofing: Detection performance analysis

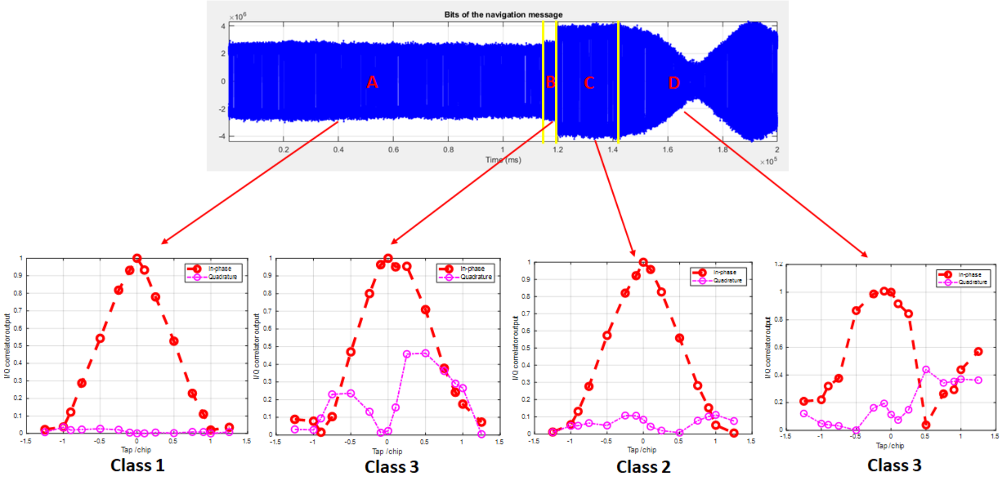
- 2-class detection and classification:



ML types	SVM (Polynomial kernel)	DNN deep neural network (tanh activation function)	ConvNN deep neural network (ReLU and sigmoid activation function)
Number of model parameters	**53**	**8418**	**211437**
Training accuracy /%	99.6	99.8	97.6
Testing accuracy /%	99	99.2	97

probability of false alarm of the spoofing detection is around 0.009

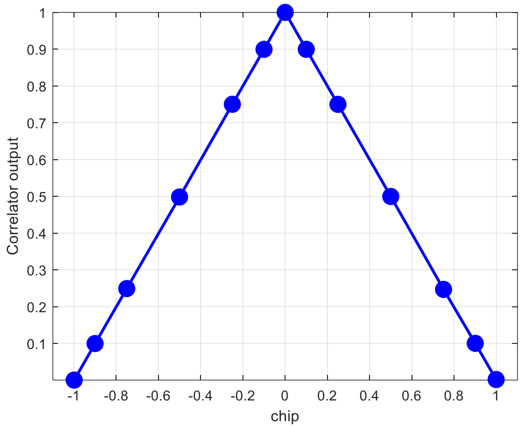
- 3-class detection and classification:



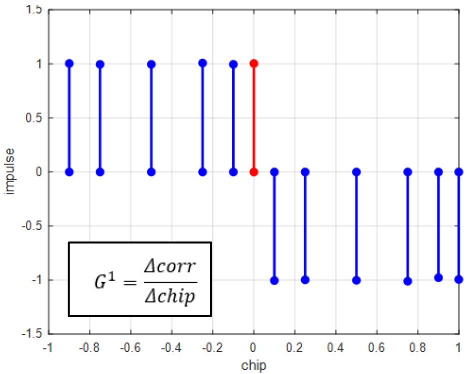
ML types	SVM (Polynomial kernel)	DNN deep neural network (tanh activation function)	ConvNN deep neural network (ReLU and sigmoid activation function)
Number of model parameters	**53**	**8418**	**211437**
Training accuracy /%	98	99.4	67.4
Testing accuracy /%	97	98.8	67.7

Spoofing: Mitigation

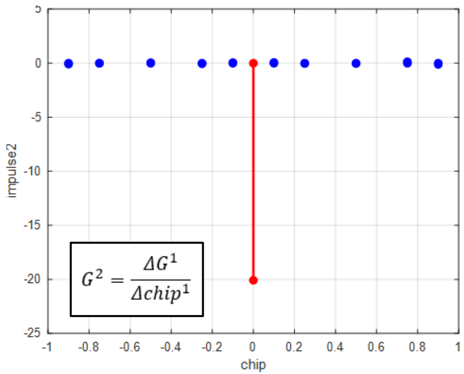
- Spoofing mitigation using 2nd gradient approach



1st gradient



2nd gradient



- 1st gradient impulse calculation:

$$G^1 = \frac{\Delta corr}{\Delta chip}$$

- 2nd gradient impulse calculation:

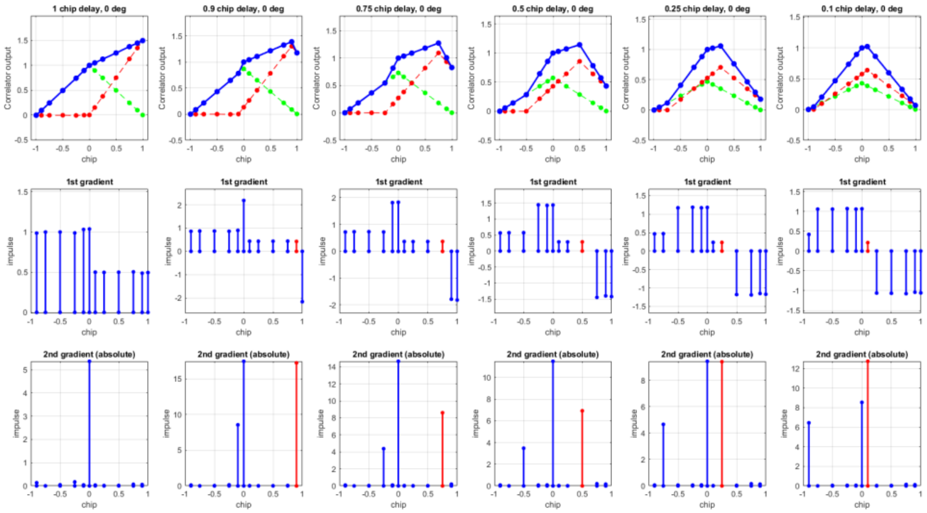
$$G^2 = \frac{\Delta G^1}{\Delta chip^1}$$

- Chip delay of the 2nd gradient impulse location is refined by weighted average:

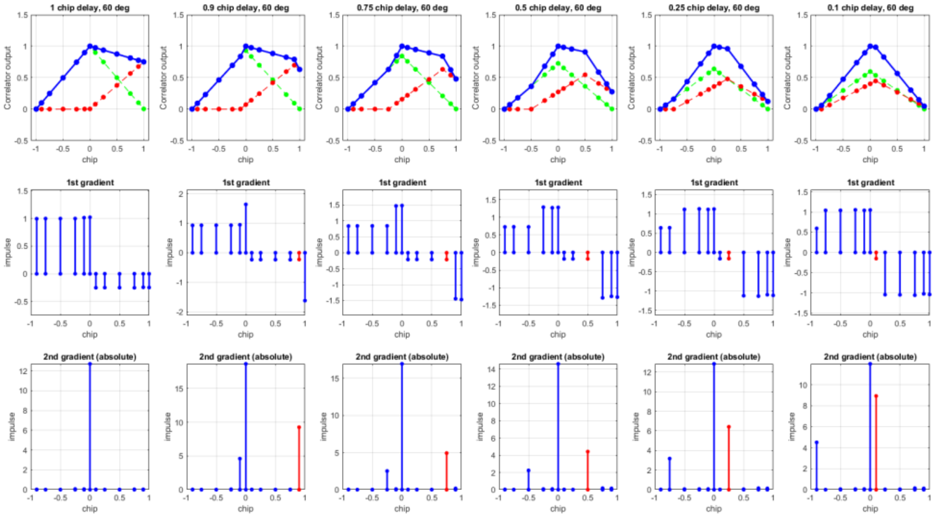
$$Code\ delay\ (Tap\ location)\ estimate_i = \frac{(I_{i-1} \times tap_{i-1} + I_i \times tap_i + I_{i+1} \times tap_{i+1})}{(I_{i-1} + I_i + I_{i+1})}$$

Spoofing: Mitigation cont’d

- correlator shape distortion, 1st gradient and 2nd gradient (impulse) of GPS L1 signal with a spoofer at different code delay. The spoofer power = 1.5 × the authentic signal’s power and the spoofer carrier phase = the authentic signal’s carrier phase.

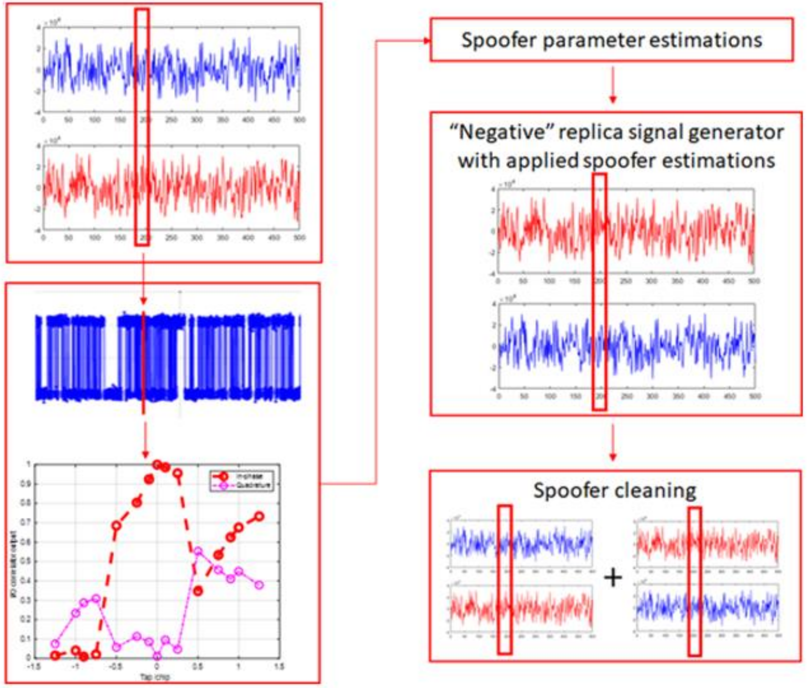


- correlator shape distortion, 1st gradient and 2nd gradient (impulse) of GPS L1 signal with a spoofer at different code delay. The spoofer power = 1.5 × the authentic signal’s power and the spoofer carrier phase 60^0 diff to the authentic signal’s carrier phase.



Spoofing: Mitigation cont’d

- GPS L1 spoofing mitigation procedure

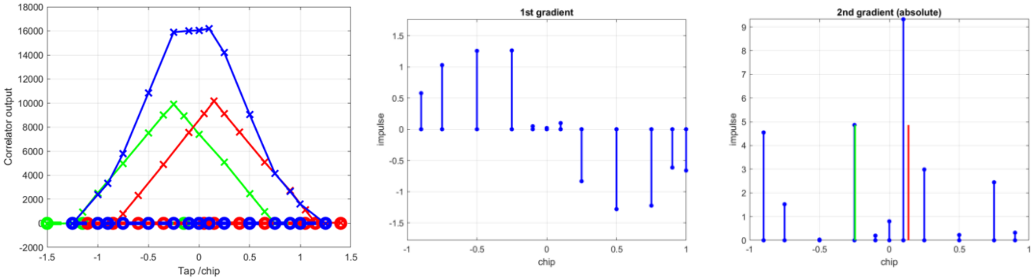


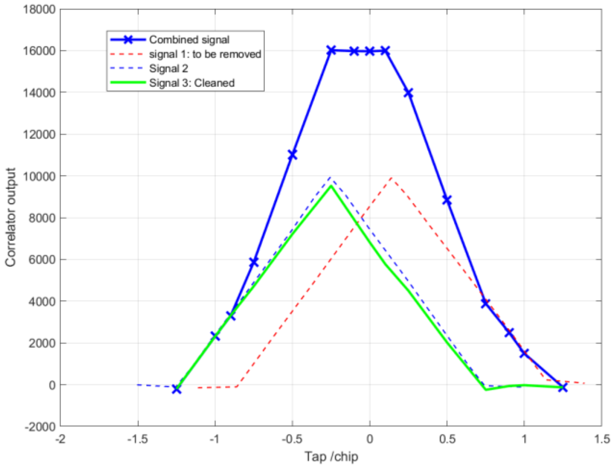
Spoofer parameter estimations

“Negative” replica signal generator with applied spoofer estimations

Spoofer cleaning

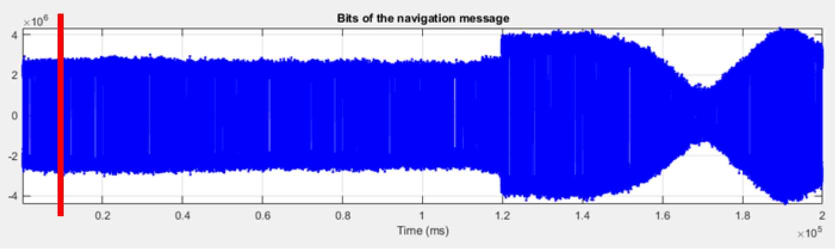
- Simulated individual signals. 10MHz sampling rate, amplitude 1 and carrier phase rotation of 0 radian. The simulated code delay for signal 1 and signal 2 are 0.15chip and -0.25chip. Gaussian noises with 5dB power. The power difference between signal 1 and signal 2 is 2.5dB.

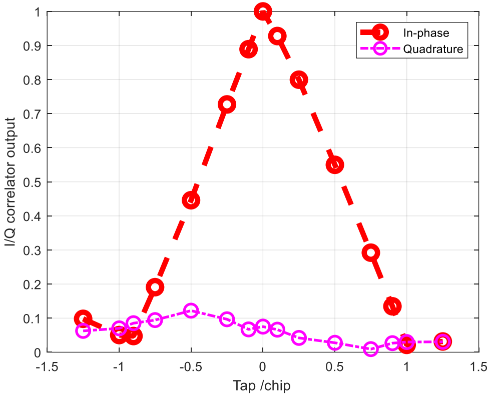


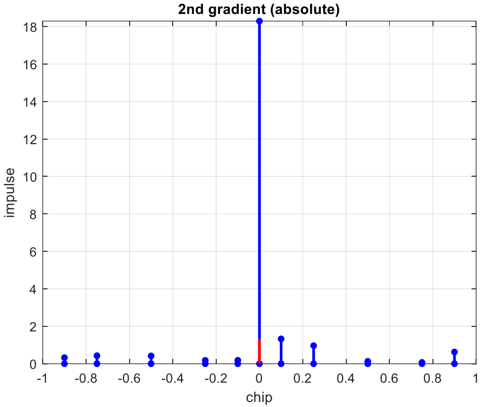


Spoofing: Mitigation performance analysis

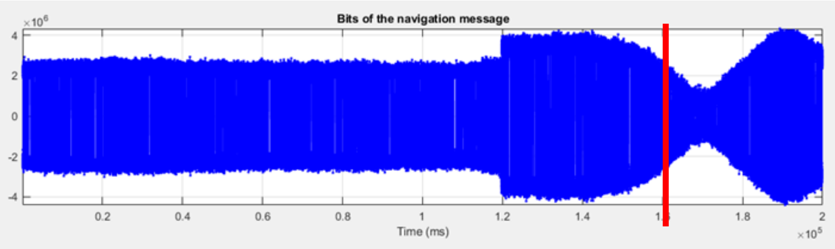
1. Authentic signal

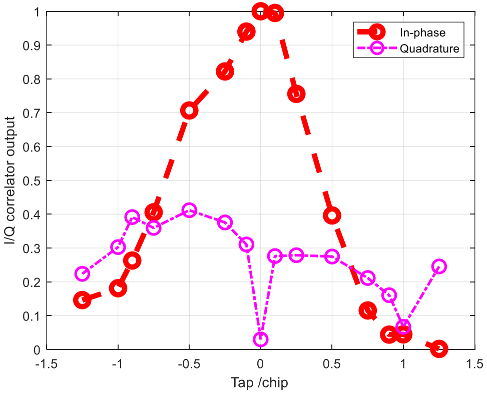


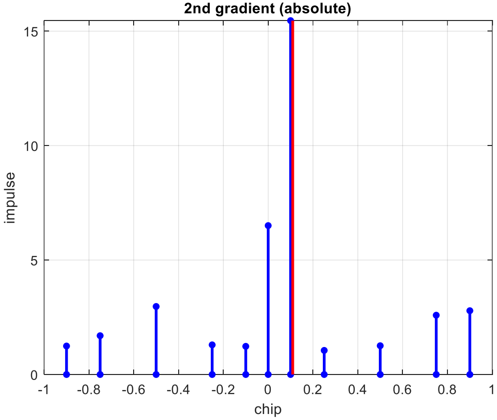




2. Spoofed signal





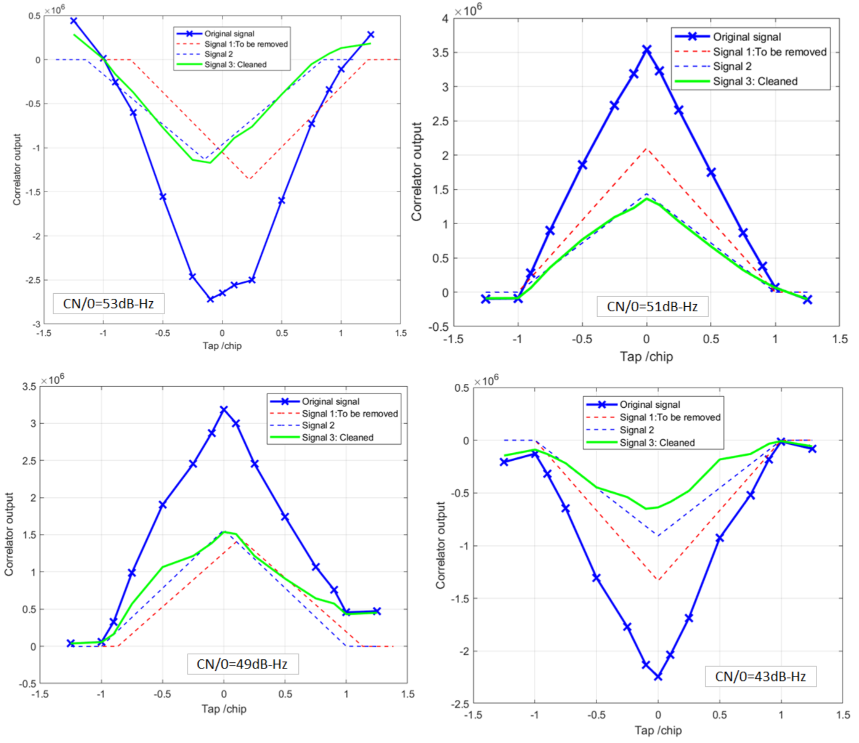


Spoofing: Mitigation performance analysis

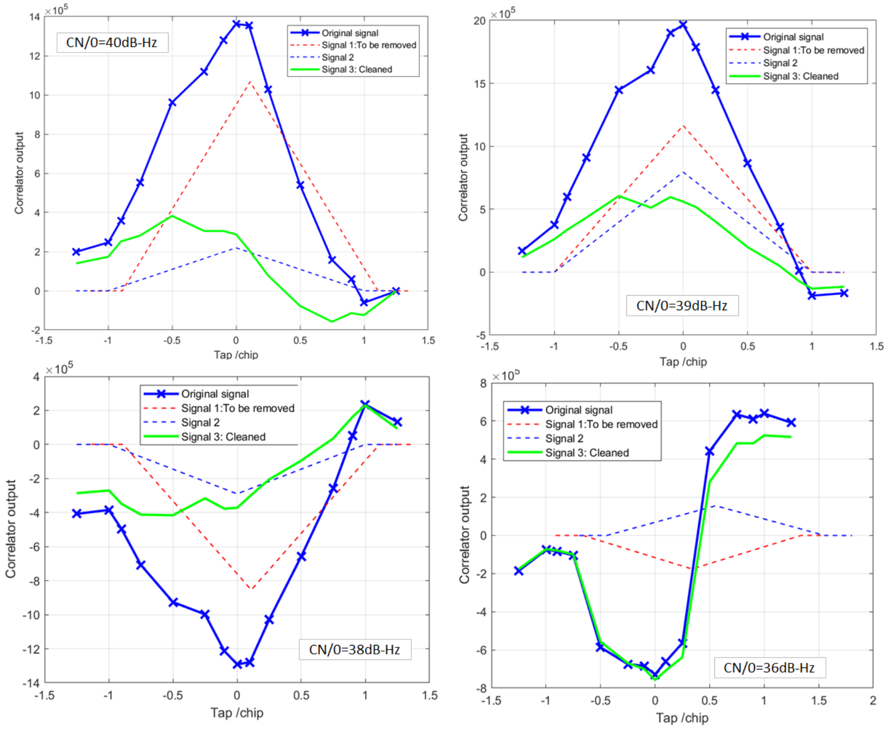
Note:

- The C/N0 is the tracked spoofed signal.
- The spoofer is ±1.3dB higher than the authentic signal

Spoofing mitigation effective working condition limit:



CN/0 > 40dB-Hz

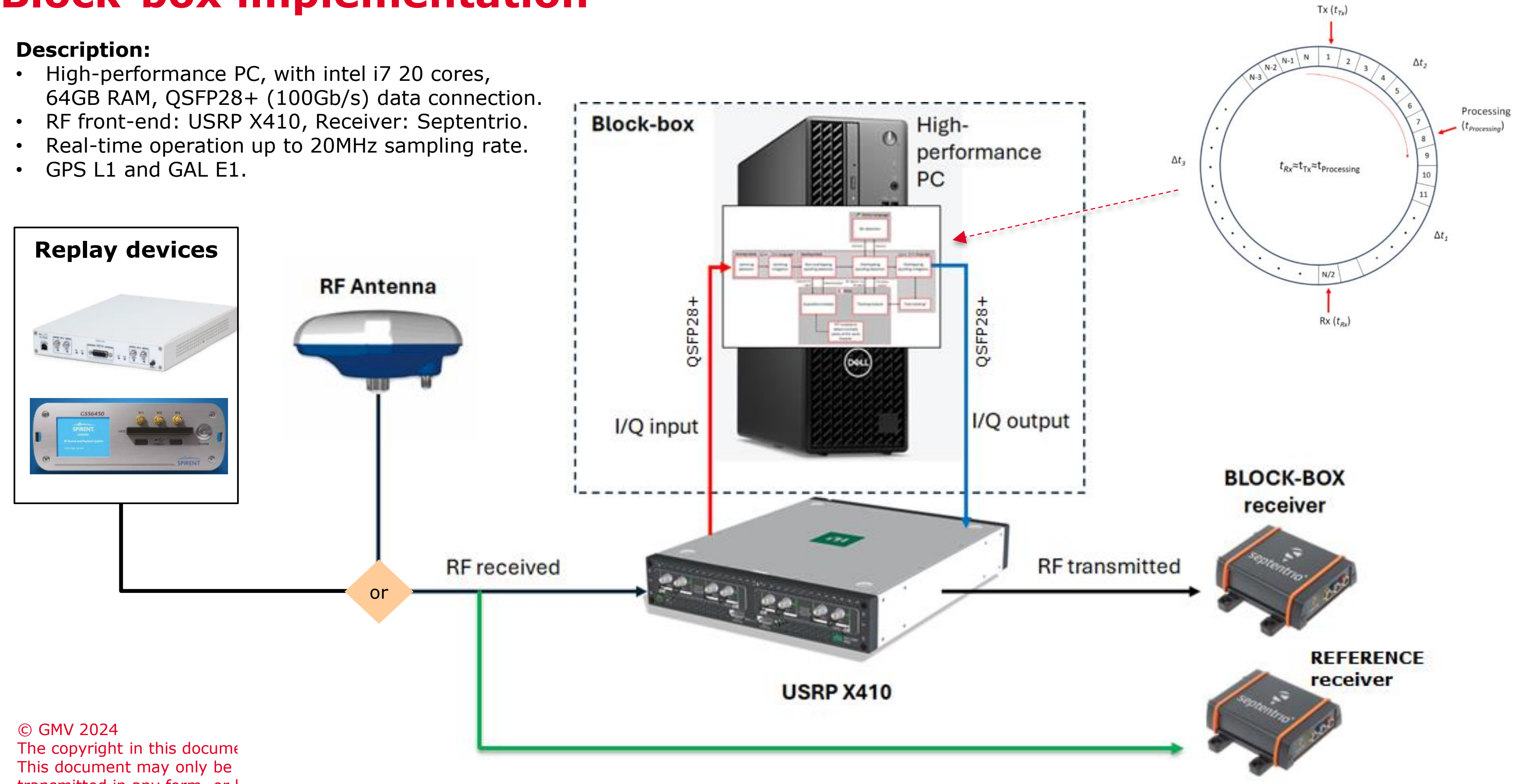


CN/0 ≤ 40dB-Hz

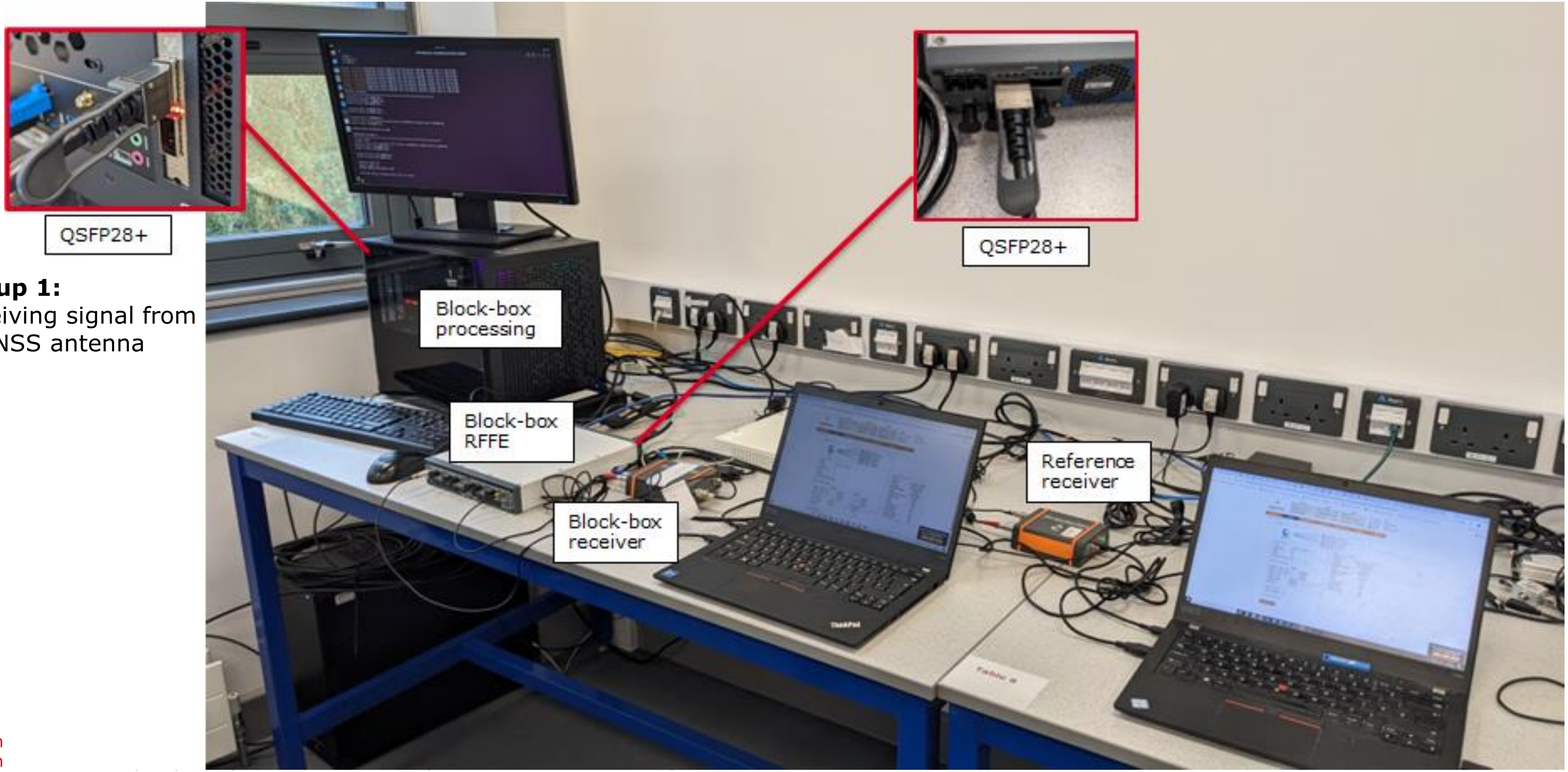
Block-box implementation

Description:

- High-performance PC, with intel i7 20 cores, 64GB RAM, QSFP28+ (100Gb/s) data connection.
- RF front-end: USRP X410, Receiver: Septentrio.
- Real-time operation up to 20MHz sampling rate.
- GPS L1 and GAL E1.



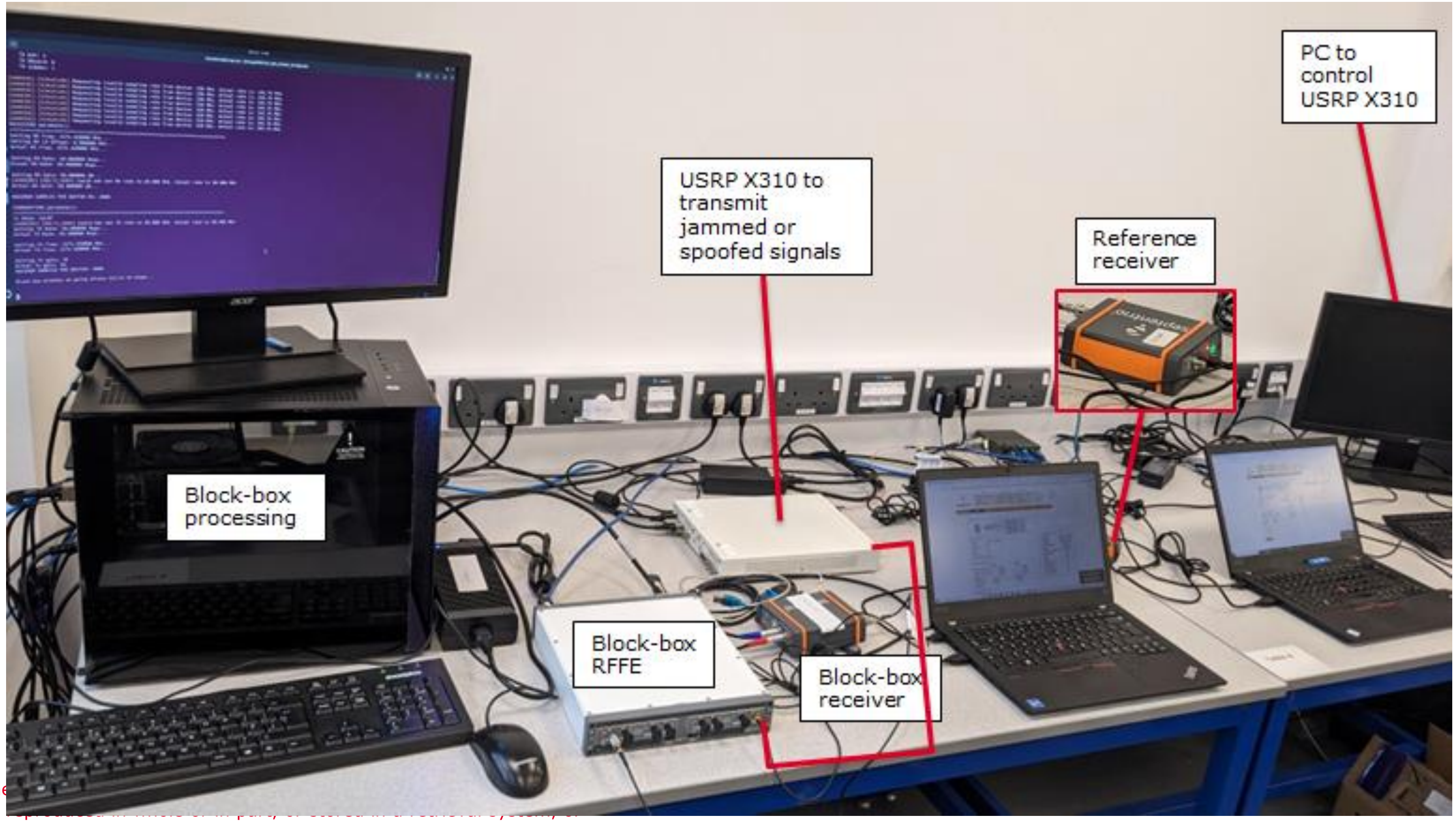
Block-box implementation cont’d



Setup 1:
receiving signal from a GNSS antenna

Block-box implementation cont’d

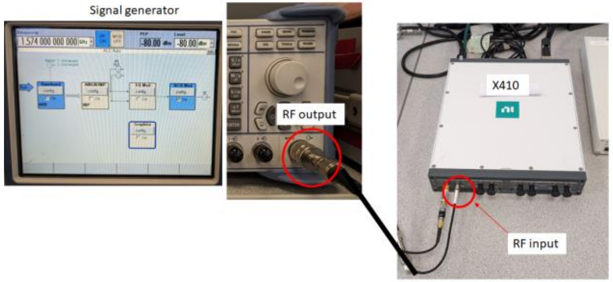
Setup 2:
receiving signal from a RF replay device



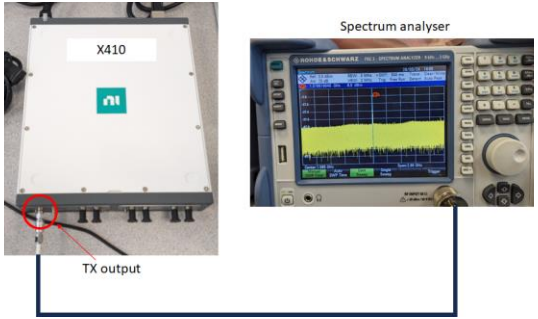
Block-box implementation cont'd

RFFE characterisation of USRP X410:

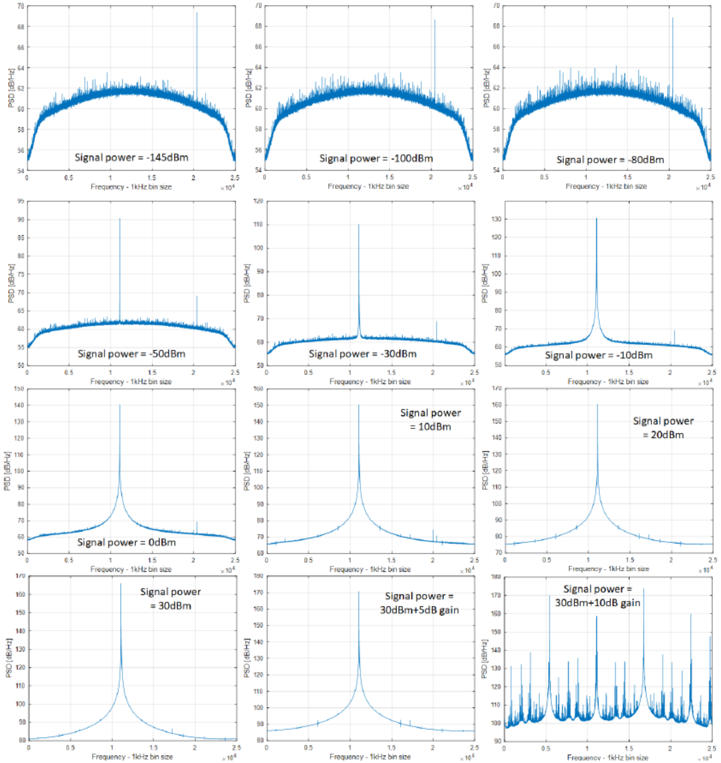
- X410 Dynamic range and input power operational range:



- X410 Power output measurement:



A consistent spurious artefact, from the RFFE device, of 10MHz offset from the centre frequency is observed.



The spurious artefact is confirmed by adding a 30dB attenuator. With this attenuator, the sinuous signal's power is reduced while the artefact's power remains the same.

Results:

- RFFE noise=-144.8dBm/Hz,

- Dynamic range = 65-75dB-Hz

- The input power dynamic range of the RF front-end is around 85dBm = -50dBm to 135dBm.

- The transmitter power output is around 17dBm (at 50dB gain) and, by assuming linearity, the power output is -23dBm (at 10dB gain) and at -33dBm (at 0 dB gain).

- The X410 maximum power output specification = <23dBm

Jamming interference mitigation test

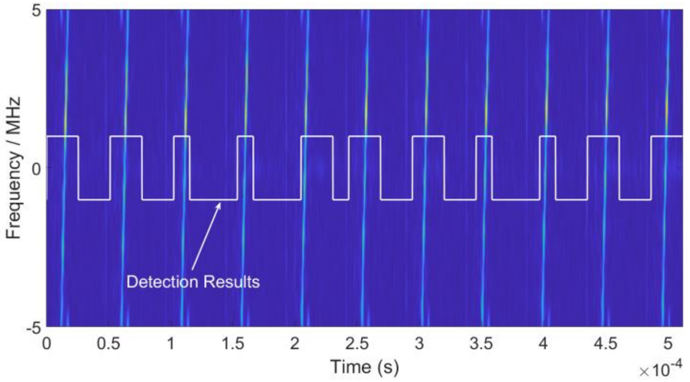
- Three jamming scenarios gathered from jammertest2024 data were replayed to the block-box and reference receiver in real-time at **ESA-ESTEC** Radio Navigation Laboratory.
- Objective: To evaluate the potential benefit of BREGO system in a realistic scenario for unknown signals.
- Replayed signals are:
    - Low powered chirp jammer
        - Time-duration: 14:16 – 14:28
        - Power: 0.1 W
        - Type: Chirp
    - Ramp-up Ramp-down jammer
        - Time duration: 16:00 to 16:14
        - Power: -37 dBm to 47 dBm with 2 dB increment
        - Type: CDMA
    - Narrow band jammer with slow varying centre frequency
        - Time duration: 16:10 – 16:25
        - Centre frequency: 1545 – 1620 MHz
        - Type: Continuous Wave

Results: Interference Characterization Results

1) Low Powered Chirp Jammer:
   - Ground truth is obtained using the signal energy.
   - Probability of detection =0.98
   - Probability of false alarm for interference free region is 0.004 (i.e., first 90 seconds)

2) Tone with time-varying frequency:
   1) The tone appears in the 10 MHz band for approximately 2.5 minutes.
   2) The probability of detection is 0.99 and probability of false alarm is 0.0023.

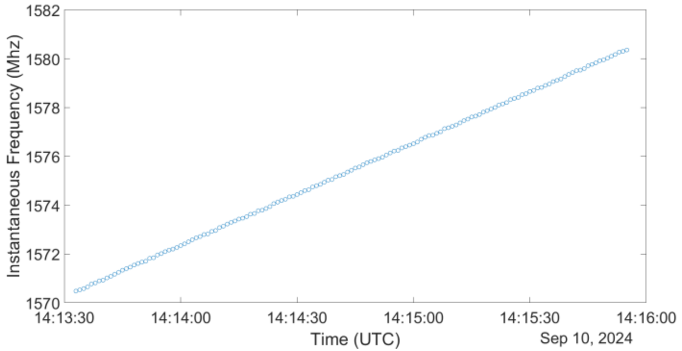
Spectrogram of (J1.3)



Confusion matrix J1.2 (complete signal)

	Chirp	No Interference	Periodic Interference
Chirp	5439688	1844020	0
No Interference	81289	8209375	0
Periodic Interference	0	0	0

Instantaneous frequency of interference (J1.5)

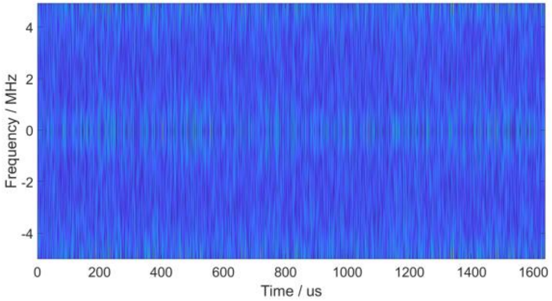


Confusion matrix J1.5 (complete signal)

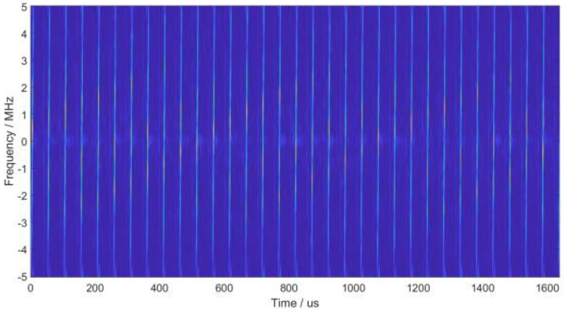
	Periodic Interference	No Interference	Chirp
Periodic Interference	10973184	9728	0
No Interference	42441	72616934	0
Chirp	0	185838	0

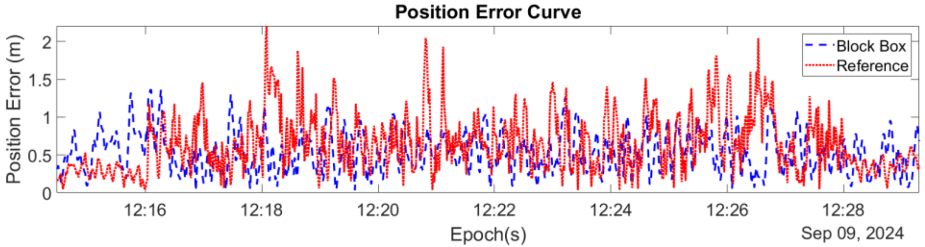
Mitigation Results: Low Powered Jammer (0.2 W)

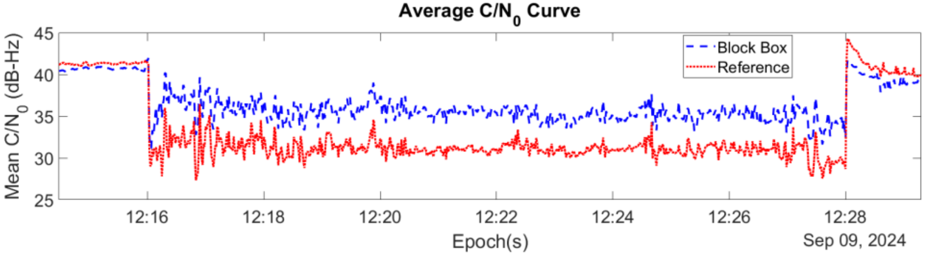
Spectrogram of interference free part



Spectrogram of corrupted signal





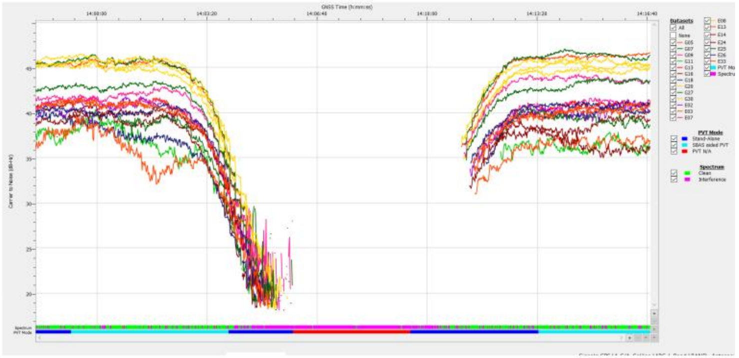


Average C/No with and without mitigation

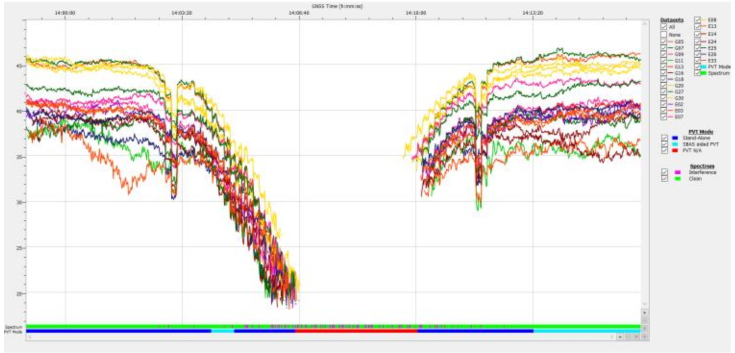
	BREGO	Reference Receiver
Interference Free	40.15	41.39
With Interference	35.30	31.2

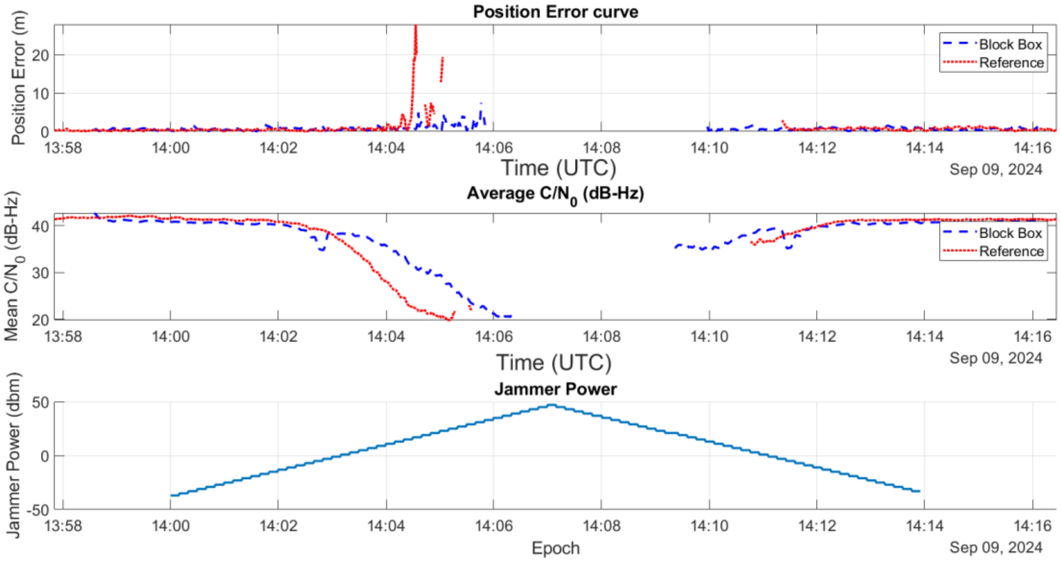
Mitigation Results: Ramp Up CDMA Jammer (-37 dBm to 47 dBm)

Reference



BREGO



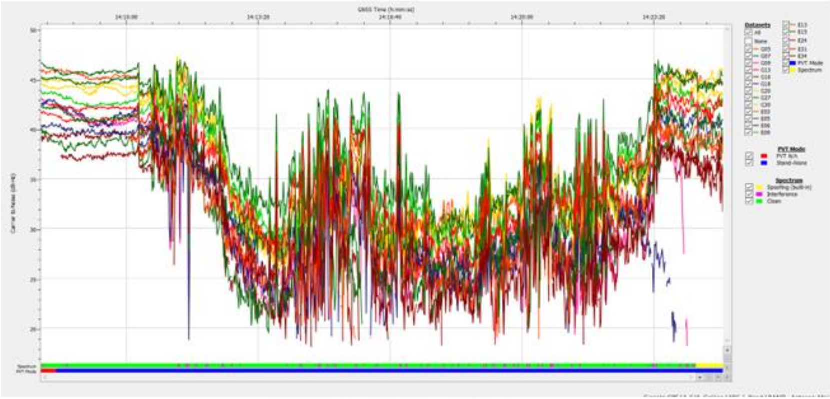


Conclusion:

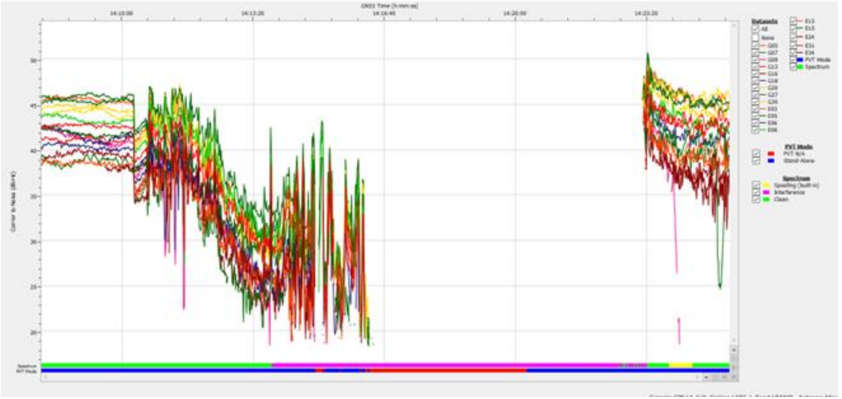
1) With mitigation, the receiver can track up to power levels of 31 dBm. It starts tracking again at 13 dBm.
2) Without mitigation, the receiver can track up to 19 dBm and regain tracking at -3 dBm.

Results: Narrowband Interference(1545 MHz –1620 MHz)

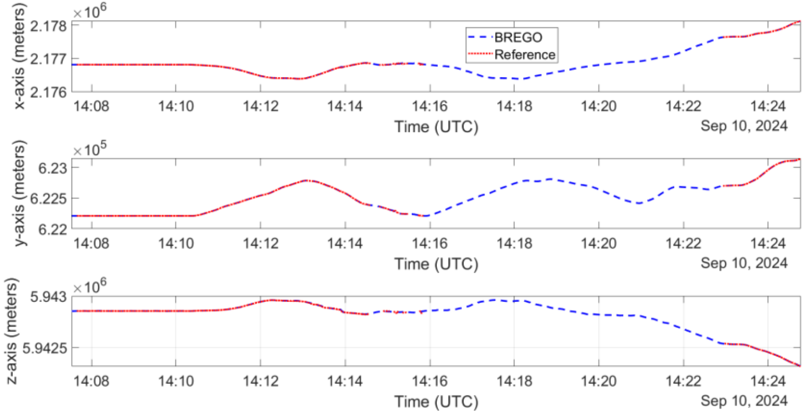
BREGO

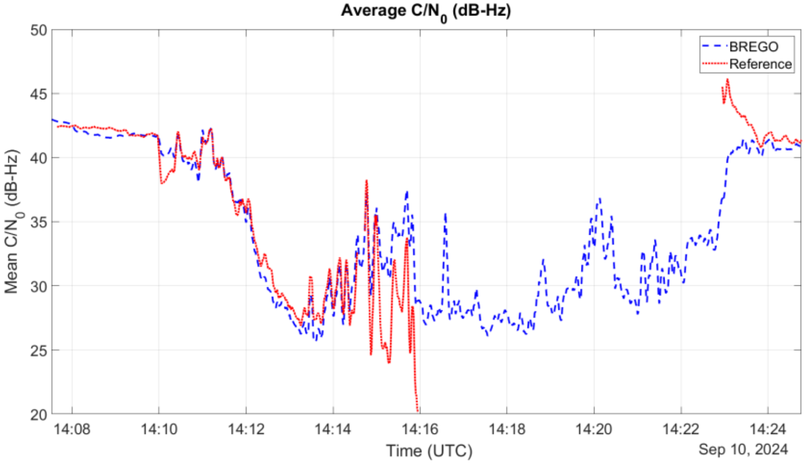


Reference Receiver



Position Curve

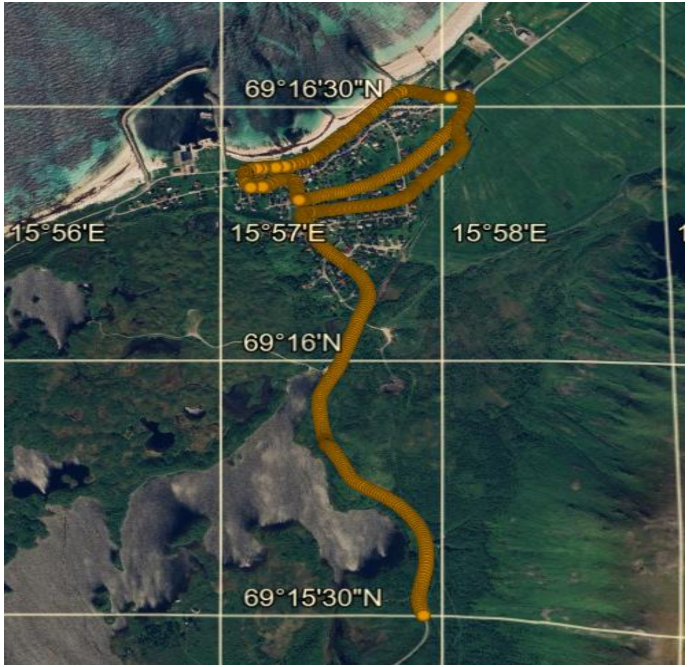




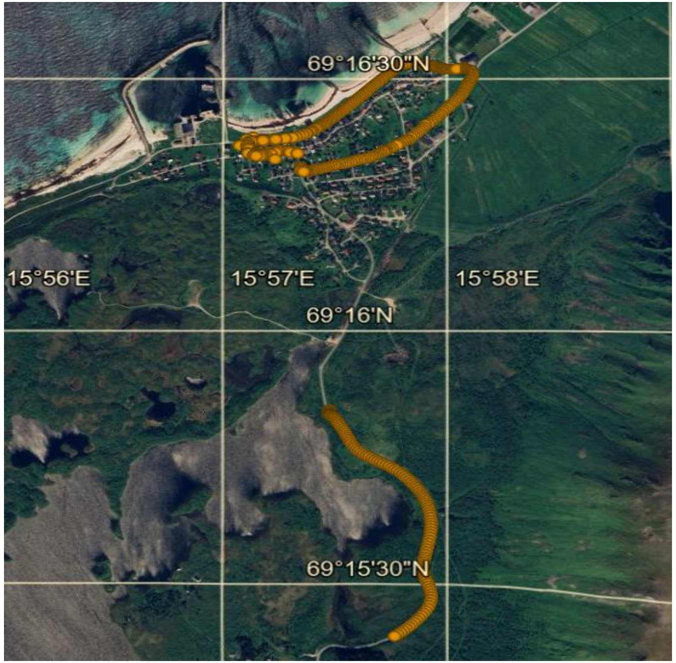
Results: Narrowband Interference cont’d

- **Path of Jammed vs mitigated Vehicle**

Path of the receiver with interference mitigated

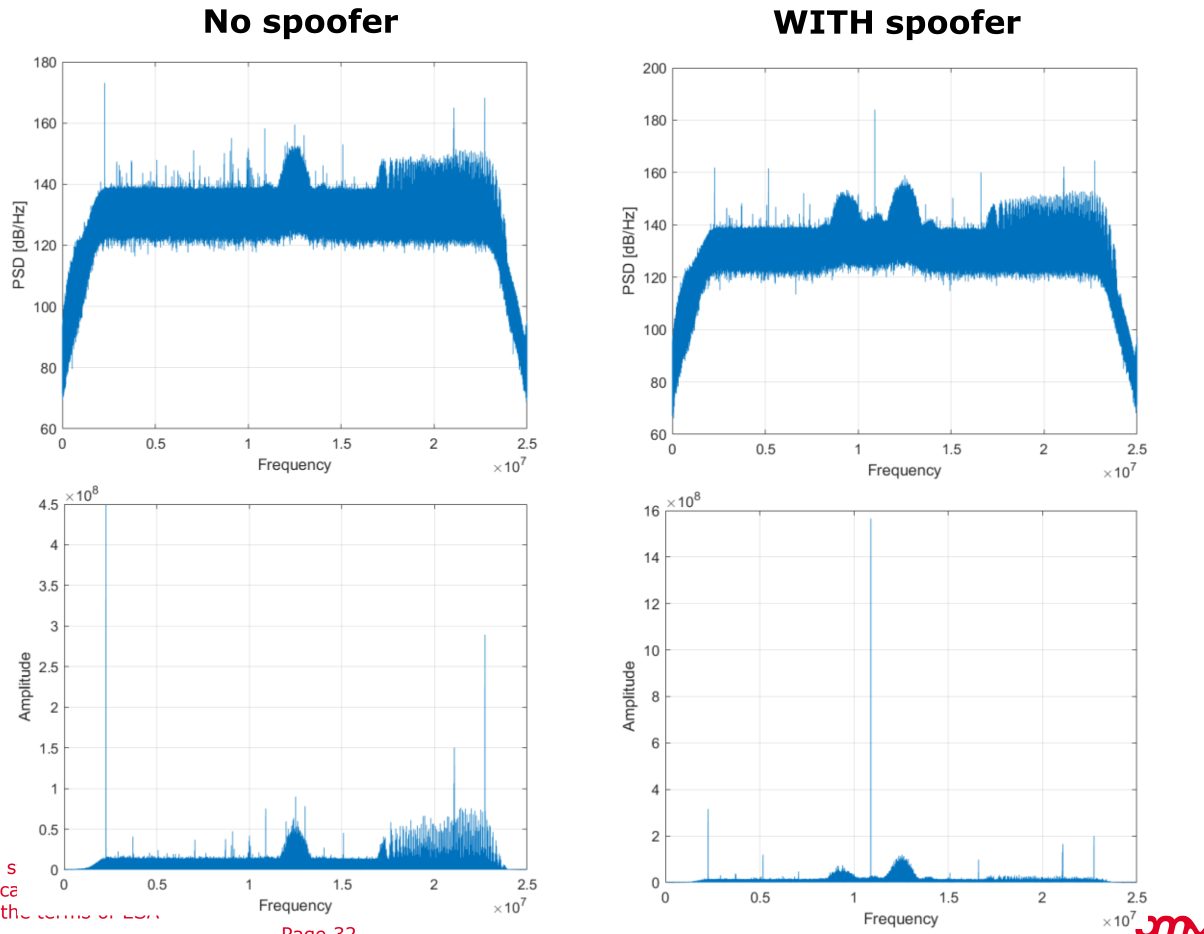


Path of the receiver without mitigation



Results: Spoofing mitigation on TEXBAT data

- The spoofer signal power is only 1.3dB higher than the authentic signal power.
- Difficult to mitigate with CDMA jamming detection and mitigation.

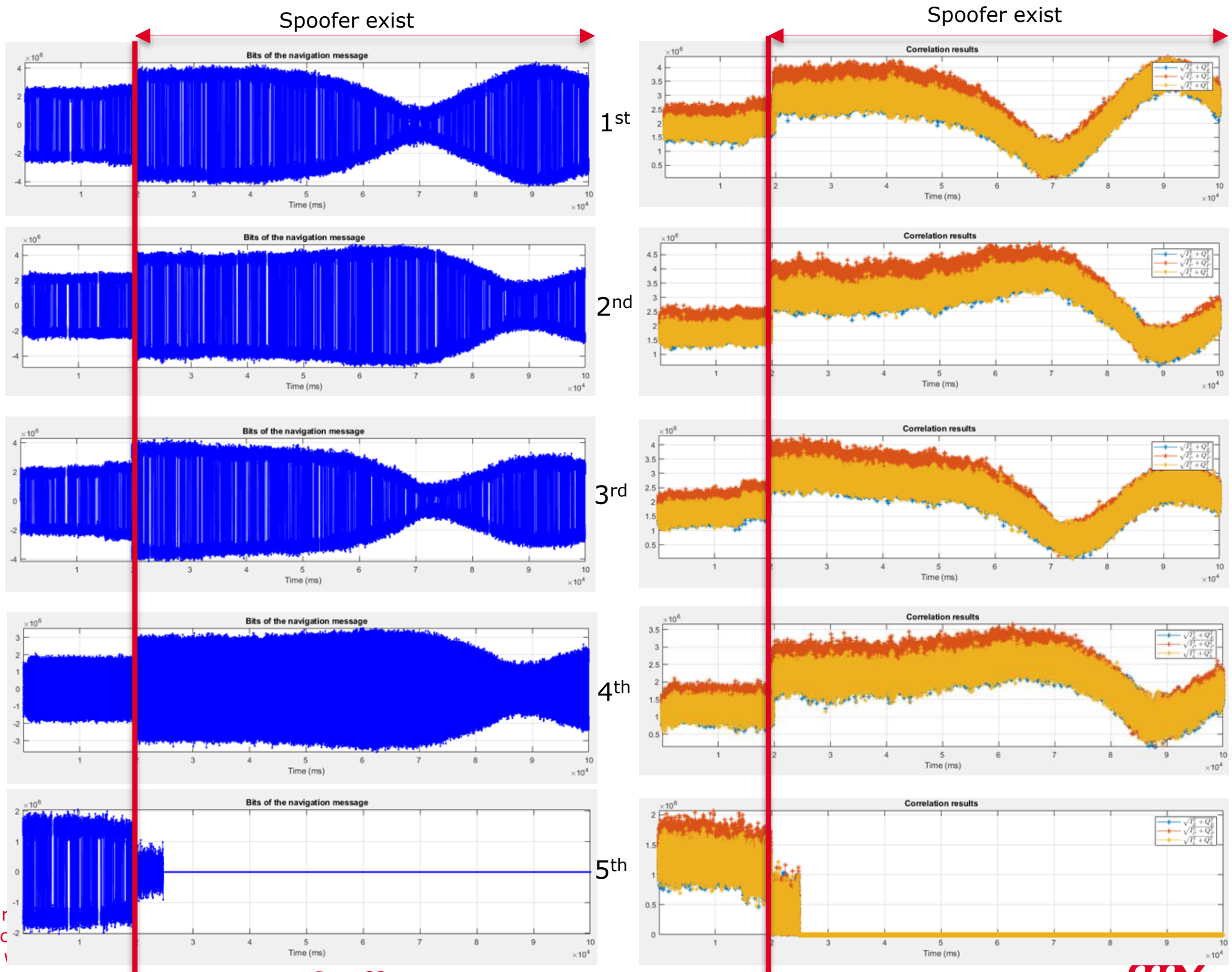


No spoofer

WITH spoofer

Results: Spoofing mitigation on TEXBAT data cont'd

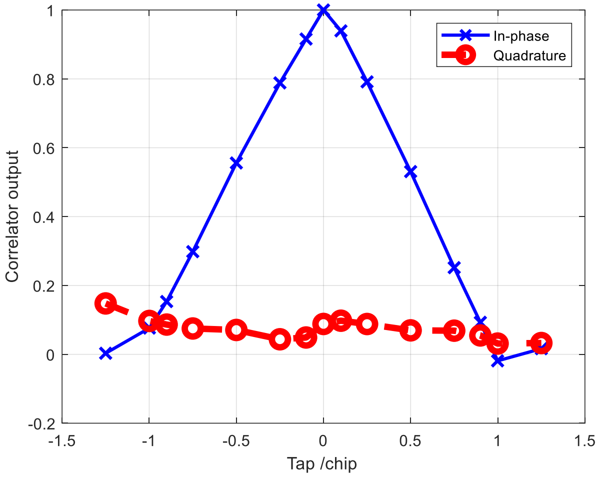
- Tracking post-processing is applied to TEXBAT data for the five PRN with the highest C/N0
- It turns out that when spoofer. exists, only 4 PRN signals are trackable and used for solutions.
- That is why, when we only remove 4 PRN on TEXBAT data, we can see some effects.

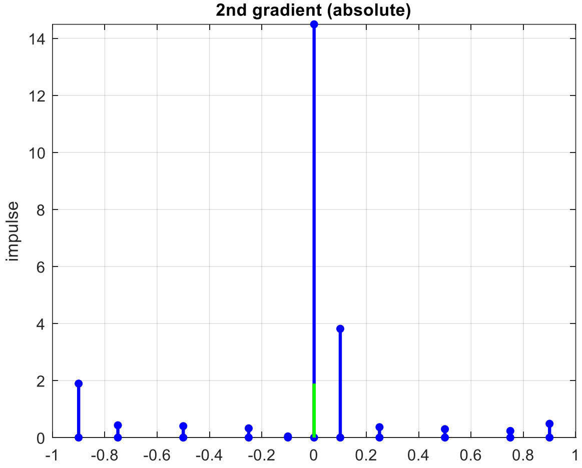


Results: Spoofing mitigation on TEXBAT data cont'd

No spoofer

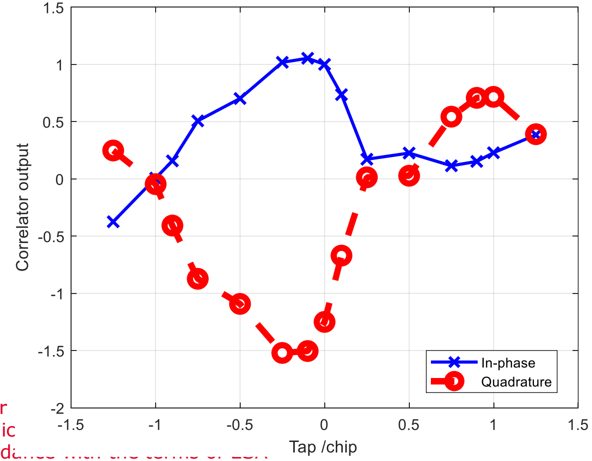
- Estimate code delay = 0 chip
- No spoofer

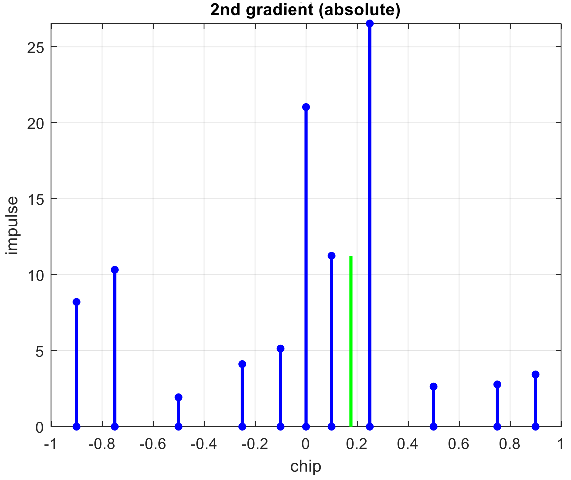




With spoofer

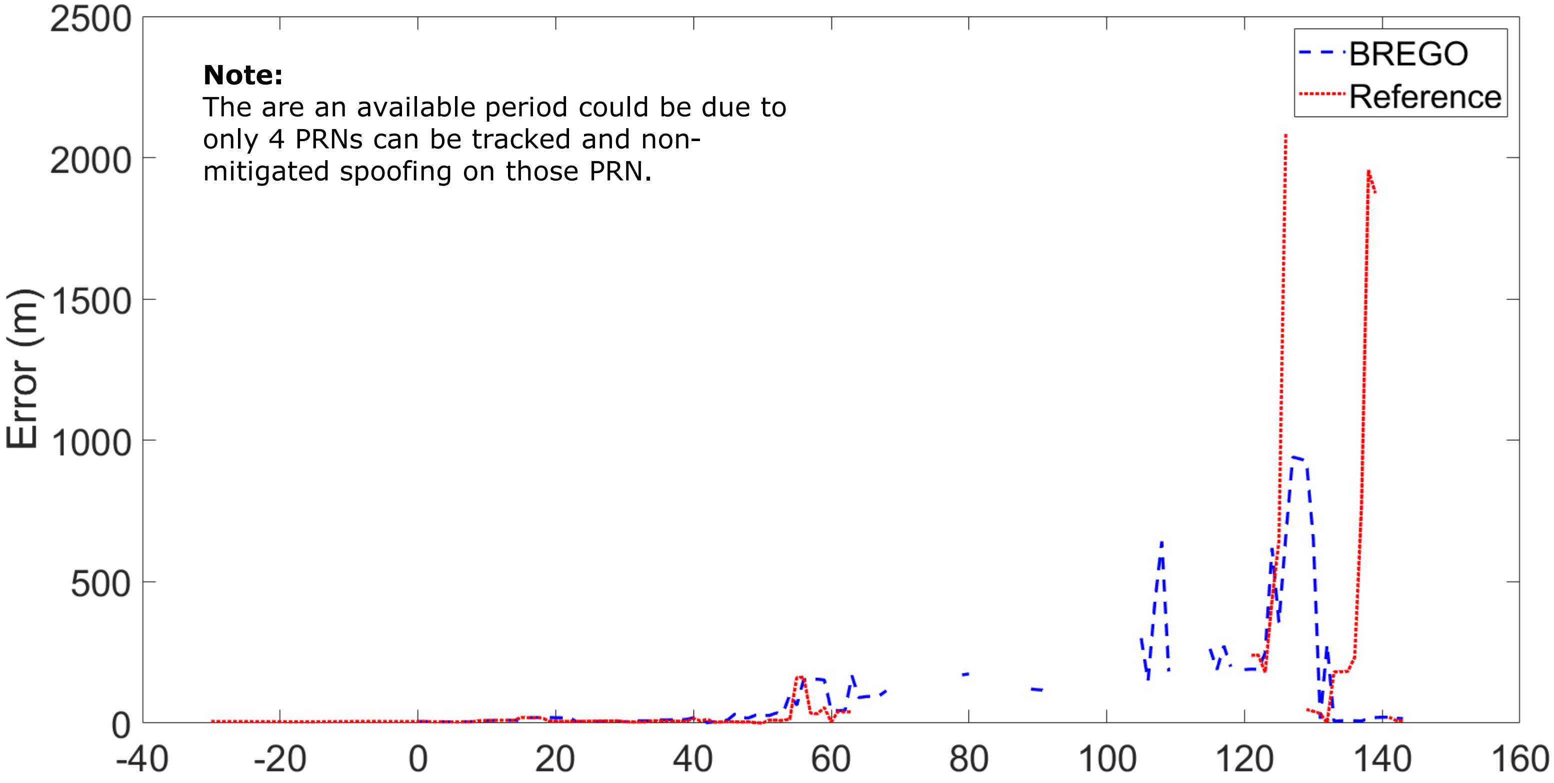
- Estimate code delay = 0.176 chip
- Spoofer exists
- Spoofer starting distance is about **53m** (0.176 chip difference to the prompt)





Chip coarse resolutions also limit the estimation accuracy of code delays

Results: Spoofing mitigation on TEXBAT data cont’d



Note:
The are an available period could be due to only 4 PRNs can be tracked and non-mitigated spoofing on those PRN.

Technology strength

- The block-box system is receiver agnostic and its effectiveness is validated using Septentrio, GNSS SDR and snapshot receiver.
- The block-box system is flexible and configurable. The system configuration can use different RFFE and processing unit (PC or breadboarding development in future)
- Affective interference mitigation systems to mitigate for both chirp and CDMA based interference attacks in real-time is developed and implemented
- A variant of adaptive notch filter developed as part of the project that can a) track fast time-varying chirps because of additional post-processing step and b) mitigates interferences without causing non-linear phase distortions by employing zero-phase filtering.
- The spoofer mitigation may help interference mitigation in case of low-power spoofing attack (low power CDMA/PRN attack).

Technology weakness & lesson learnt

- Constraint on the breadboarding development:
  - Difficult to integrate FPGA implementation (for high computational load processing) into a full Linux OS (to be accessed by C/C++ software).
  - Full software implementations are limited to the processor capability to perform multithreading (not all the 20 cores of the Intel i7 can be used due to internal-thread communication bottleneck).
- Jamming detection and mitigation limitations: cannot mitigate
  - Multiple equally powered chirp interferences (ANF based methods struggle in this scenario)
  - Broadband noise (is not sparse in any domain)
- Spoofing detection and mitigation limitations:
  - Require the receiver to initially track authentic signals.
  - Only mitigate 4 PRNs with the highest C/N0 to reduce computational loads (real-time processing requirement).
  - The algorithm is signal-structure-specific, meaning each different GNSS signal with different structure will require different mitigation algorithm (currently only for GPS L1).
  - Require feedback from receivers or other sensors to detect and mitigate various spoofing scenarios.

Benefits of working with ESA

- Technical discussions, brainstorming and suggestions during development stages.
- The usage of the data provided by ESA for interference characterization.
- The usage of different devices. For example, in this project, at ESA-ESTEC lab, we used Septentrio Mozaic-X5 with dual channel for testing.
- The usage of the ESTEC facility and the real data collected on field to understand the shortcomings of the design:
  - Finding the weakness of the system: Low power spoofing mitigation considered for the design that does perform well against high power spoofing attack
  - Real jammer test vector allowed for testing and perform characterisation in a non-controlled environment

Future directions

- Considers more spoofing scenarios to improve the current mitigation algorithms.
- Integrating feedback form receivers and other sources for spoofing detection and mitigation of wider scenarios.
- Implementing the jamming and spoofing detection and mitigation in silicon (FPGA) for fast processing and compact block-box system.
- Investigate the use of GPU programming to speed up the software implementation.
- Explore combination of jamming and spoofing mitigation for high powered spoofers.
- **Element 2** considerations:
    - Investigate the combination with antenna array methods and dual-polarisation for equal powered interferences, broadband noise and spoofers.
    - A compact Breadboarding implementation (FPGA implementation).
    - Possible business case (customers): GNSS receiver for high-value assets (private and government assets).