THE THREAT OF GNSS JAMMING AND INTERFERENCE

Aiden Morrison, 24.10.2023

United Nations/Finland Workshop on the Applications of GNSS

GNSS disruption incidents – a growing problem

Truck driver has GPS jammer, accidentally jams Newark airport

An engineering firm worker in New Jersey has a GPS jammer so his bosses don't know where he is all the time. However, his route takes him close to Newark airport, and his jammer affects its satellite systems.

'Forgotten' GPS jammer costs motorist €2,000

Pilotene mister GPS-signalet i Finnmark. Det kan knyttes til russiske øvelser

«Det er grunn til å tro at det kan relateres til militære øvelsesaktiviteter utenfor norskekysten», sier Luftfartstilsynet.

'We hacked U.S. drone': Iran claims it electronically hijacked spy aircraft's GPS and tricked aircraft into landing on its soil

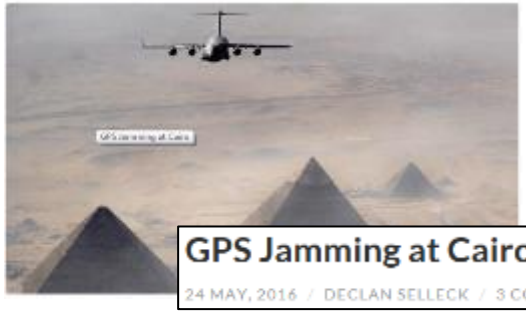
By: Craig Mackenzie and Mark Duell
Updated: 10:36 EDT, 19 December 2011

The Chirp Jammer: a GPS hit and run

The C50 device that brought a multi-million euro project to a standstill

Luftambulansen mistet navigasjonssystemet på vei til pasient. Årsaken sto i sigarettenneren til en bil.

Piloten var overlatt til det han så ut vinduet for å finne veien til den kritisk syke pasienten.

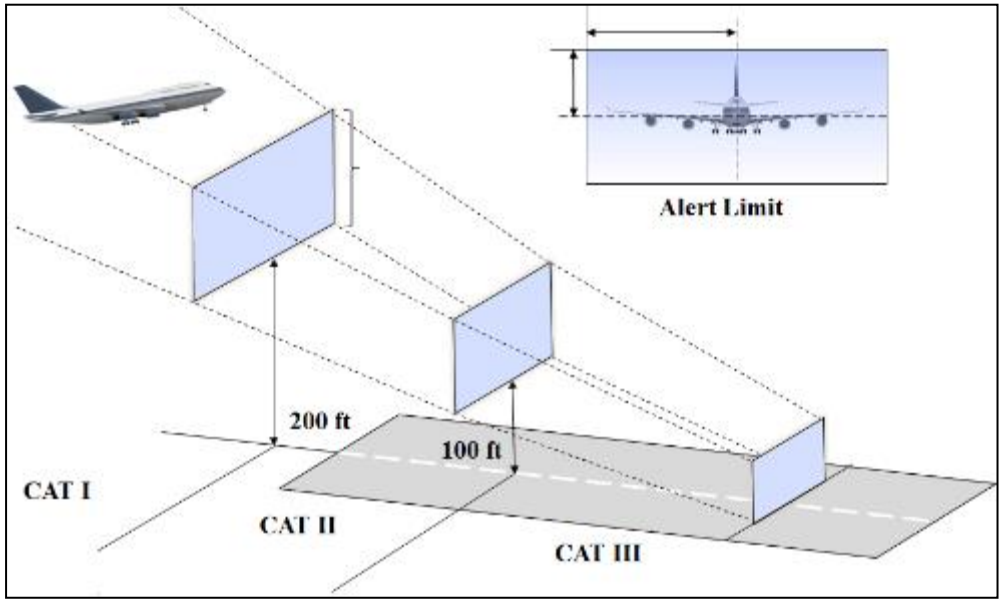


GPS Jamming at Cairo

24 MAY, 2016 / DECLAN SELLECK / 3 COMMENTS

SINTEF

Some systems are more sensitive than others



GBAS Precision Operation		CAT I	CAT II	CAT III
Accuracy [m] 95 %	Horizontal	16.0	6.9	6.1
	Vertical	7.7	2.0	2.0
Integrity	Time-to-Alert [s]	3	2	2
	Alert Limit [m]	H: 40 V: 10-15	H: 17.3 V: 5.3	H: 15.5 V: 5.3
	P_{HMI} / approach	$2x10^{-5}$	$2x10^{-9}$	**$2x10^{-9}$**
Continuity	Failure Rate	$5x10^{-5}$ / approach	$5x10^{-6}$ / 15 sec	**10^{-7} / 15 sec**
Availability		0.99 – 0.99999	0.99 – 0.99999	**0.99 – 0.99999**

- GBAS has the advantage of using multiple ground antennas but RFI at even 1 antenna can reduce availability unacceptably
  - We have observed multiple instances of jamming in Trondheim strong enough to be simultaneously visible to sites **1km apart**
  - Baselines between GBAS receivers are typically <1km
- GBAS GAST-F should utilize L1+L5 and E1/E5a – can we fall back to L5/E5a?

SINTEF

Our GNSS RFI Monitoring Network

2019-2020

- 3 x SINTEF and Nkom, Trondheim
- University of Helsinki
- ESTEC, Noordwijk
- NLR, Amsterdam
- Indra Navia, Asker
- Nkom, Moss (south of Oslo)

2021

- 2x GNSS Centre of Excellence, Czech Republic
- Norwegian Coastal Administration, Ålesund

2022

- Sodankylä, Finland
- 2 x Aurora ITS test road, Finland

2023

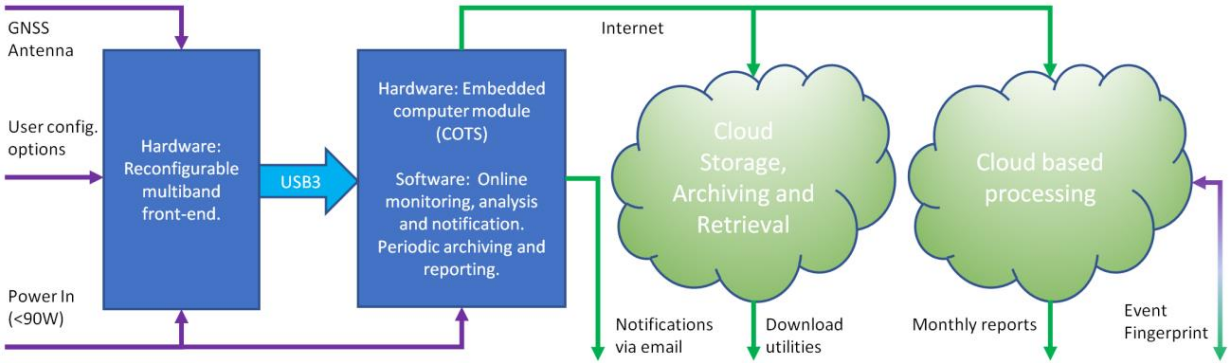
- EUSPA Prague

- In total 20 site-years of monitoring
- What is monitored and why?

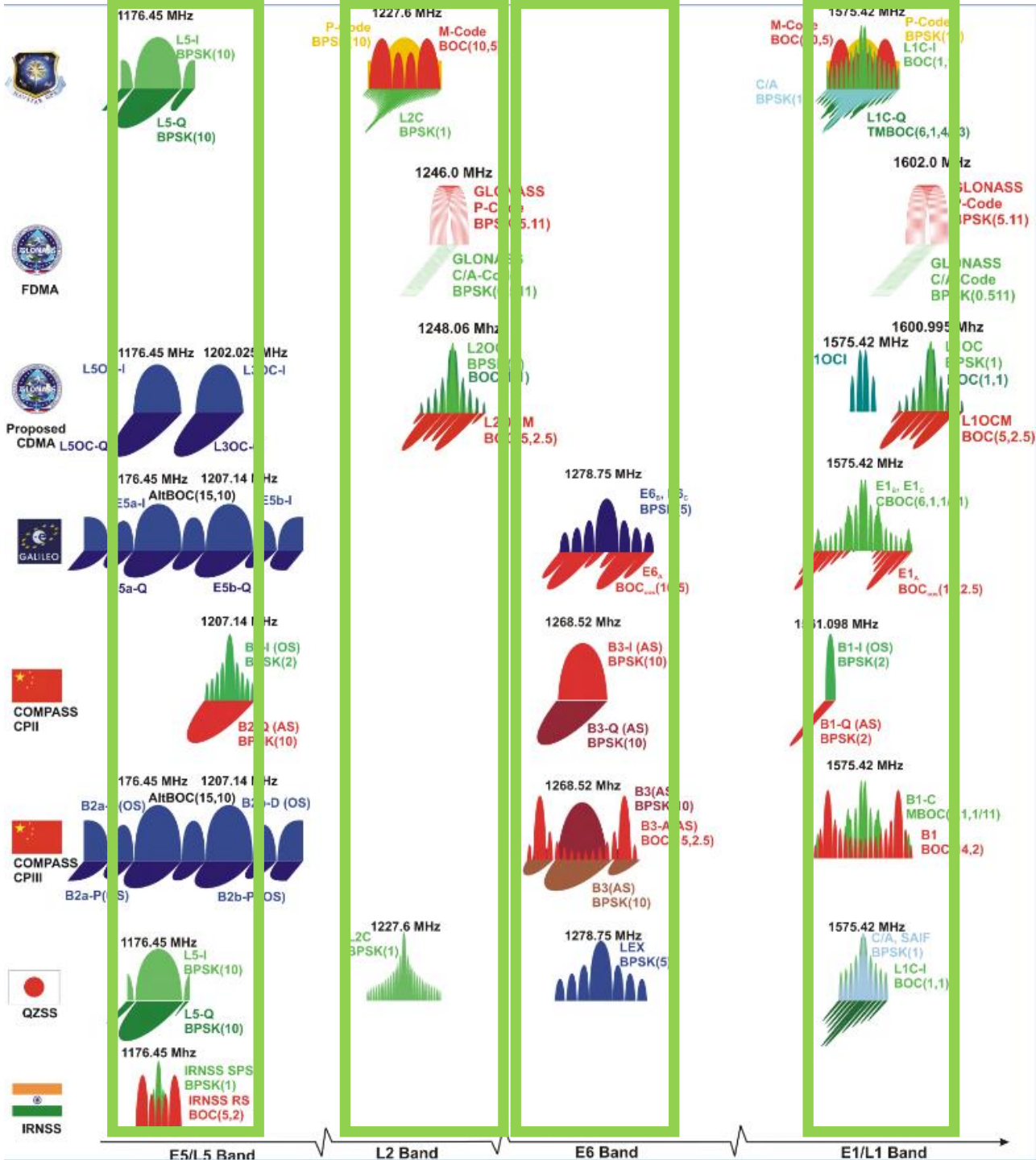
Locations of previously deployed ARFIDAAS systems, the number of systems indicated in brackets.

Data captured

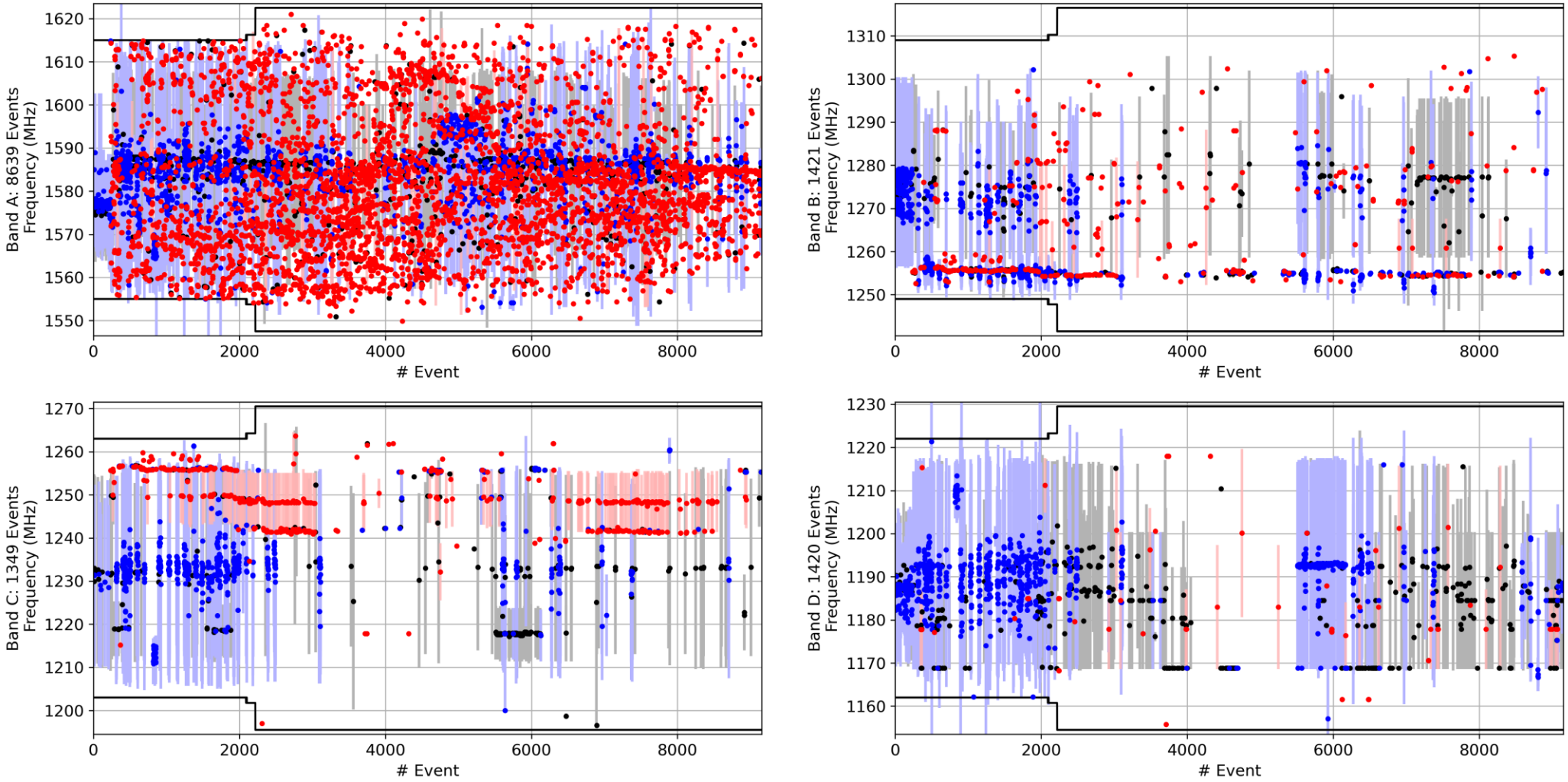
- The system covers 220 to 280 MHz of spectrum
  - Covers all of the main lobes of all the L-band signals
  - On the updated systems 75 MHz is available, so the side-lobes of Alt-BOC can partially covered
  - First, notifications are sent then data is uploaded
  - Centralized cloud analysis on all captured events from all sites



  - How many events from a single site?



One site



- Events that occur at the same time at different bands are given the same event number.
- The center frequency of each event is marked with a dot and the bandwidth with a vertical line.
- Narrowband events are indicated with red, wideband black and time-modulated blue.
- Black horizontal lines indicate the band limits. This site was updated from 60 MHz x4 to 75 MHz x4
- Who does this?

SINTEF

Jammer purchase is far too easy, and far too disruptive

Here is the full list of frequencies which this device is able to work with:

- GSM800 and GSM1900 in USA, GSM900 and GSM1800 in Europe
- CDMA850 in both USA and Europe
- GPS L1, L2 and L5 bands, GLONASS
- WiFi, Bluetooth and all devices operating at 2.4GHz
- 3G frequency

Specifications:

- Working Radius: 15 meters
- Signal Power: 1200mW

www.jammer-store.com

- The way jammers are marketed is troubling
  - People are paranoid about tracking
  - People do not understand the legality
    - Nowhere in the marketing material does it say 'highly illegal'
  - The advertised range makes it sound like this is a 'bubble' around your car

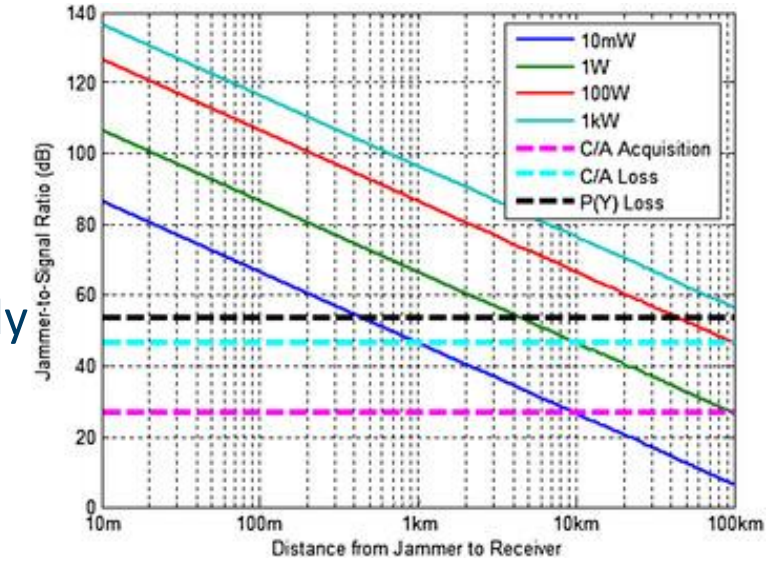


Image from Glomsvoll and Bonenberg

- Even if the 1200 mW is shared between all six bands this is > 1km range
- The propagation environment between the jammer and the victim varies widely
- What do these disruptions look like to a GNSS user?

SINTEF

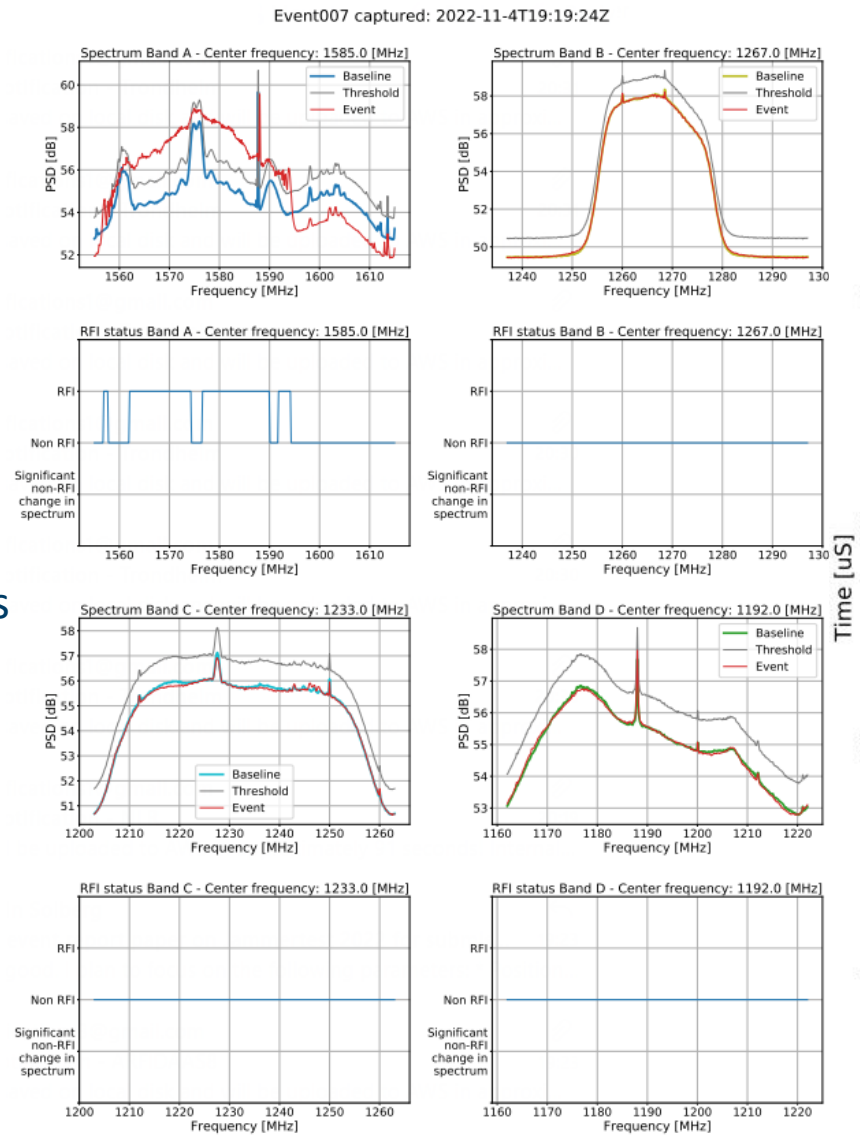
Notifying site stakeholders

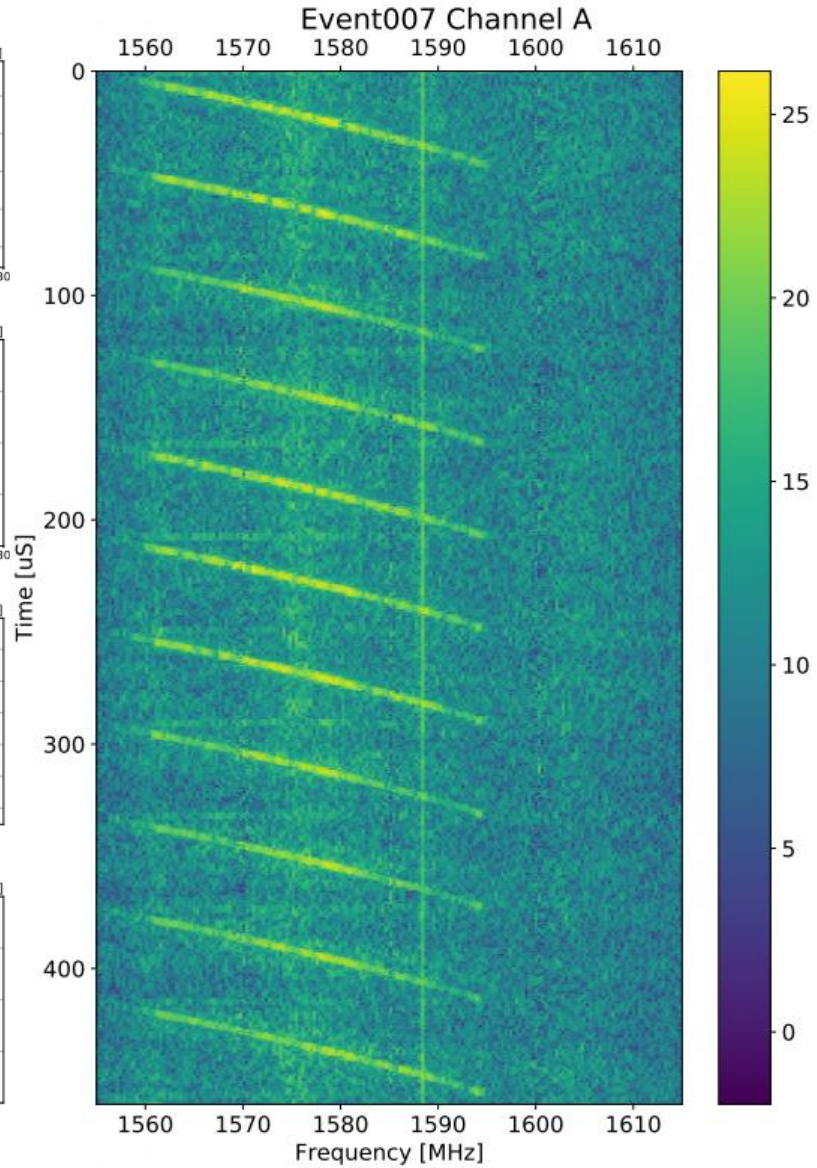
- One of our goals has been to warn site operators that they are experiencing jamming

- Detection is multi-staged
  - 1) In-band power after the SAW filters
  - 2) Automatic gain control feedback state in bands
  - 3) Magnitude and duration gating

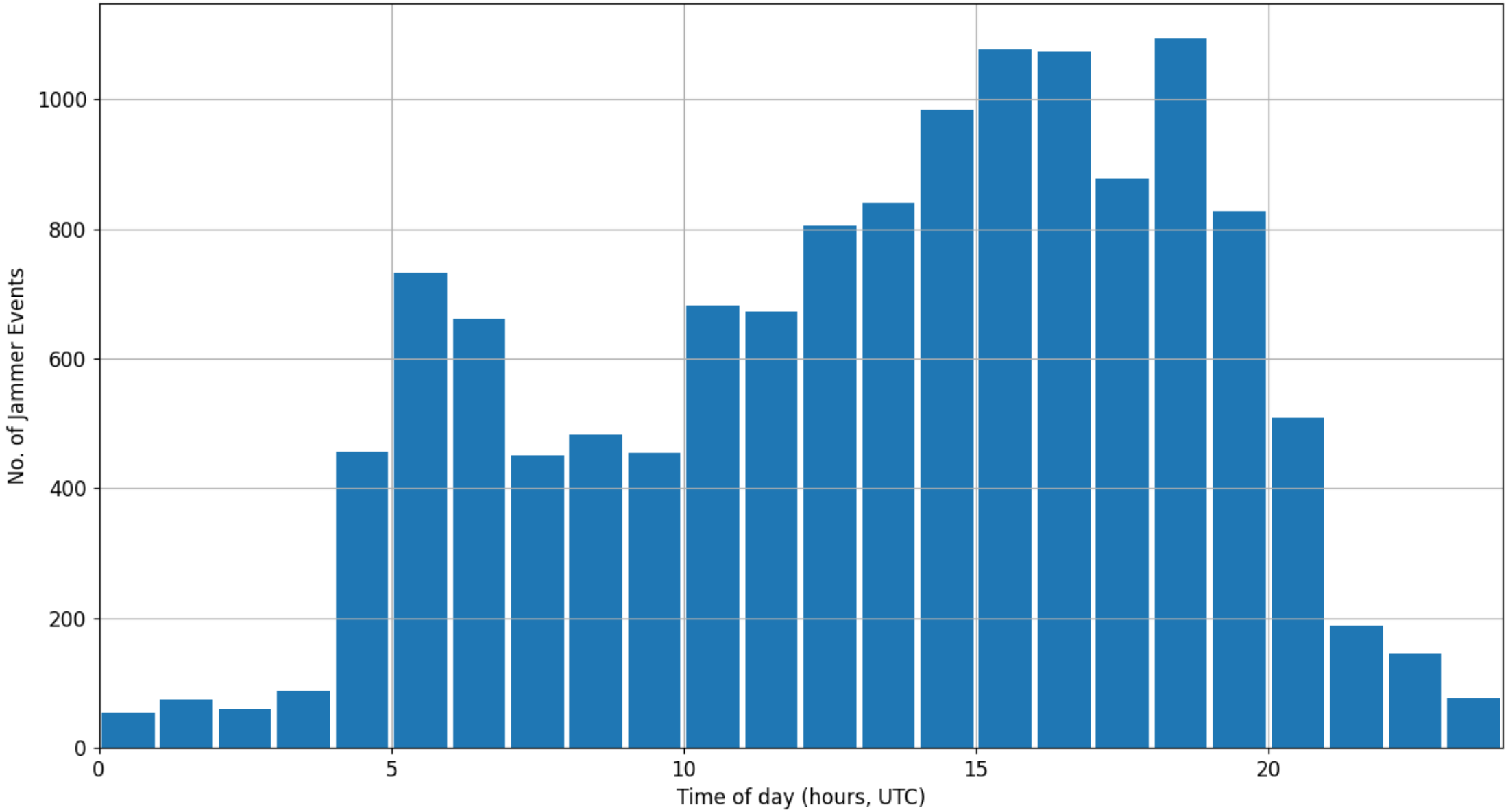
- We are quite certain that disruptive signals are present, but we need to know more
  - First, notify the users
  - After, the notification is classification
  - Later, centralized analysis of data batches is run

    - What do we find?



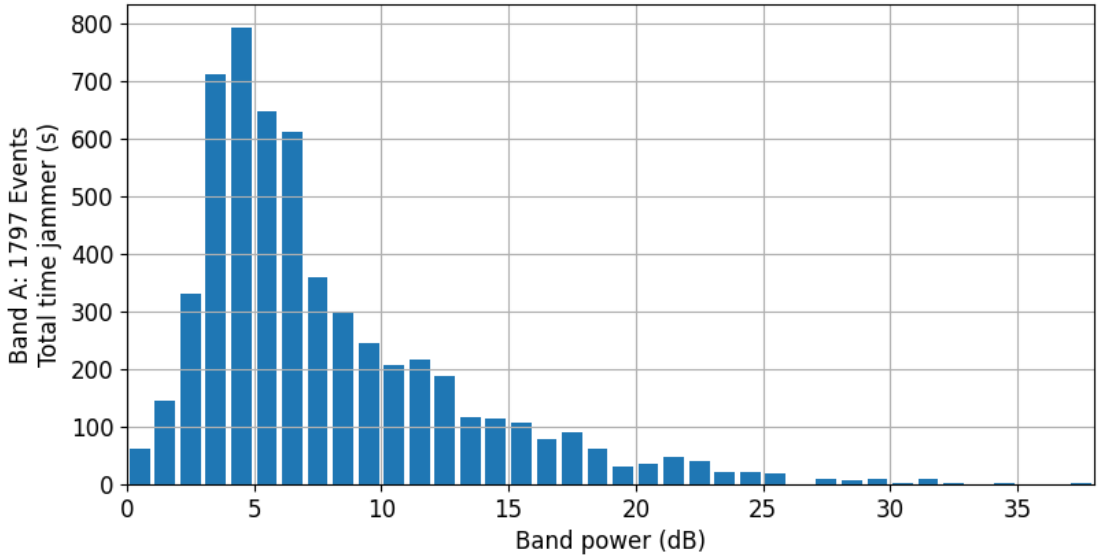


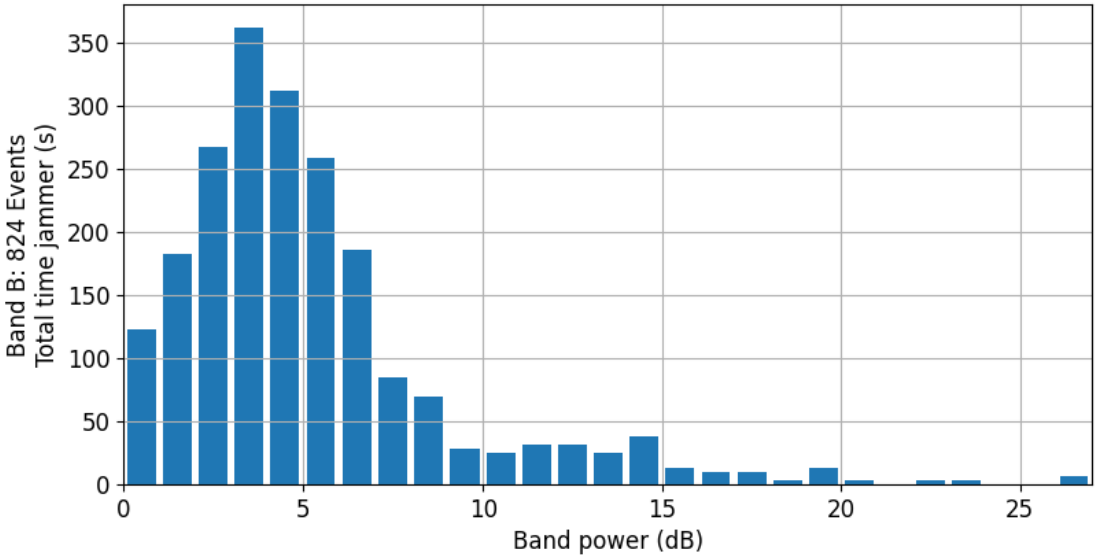
Cloud data analysis and trends - 1

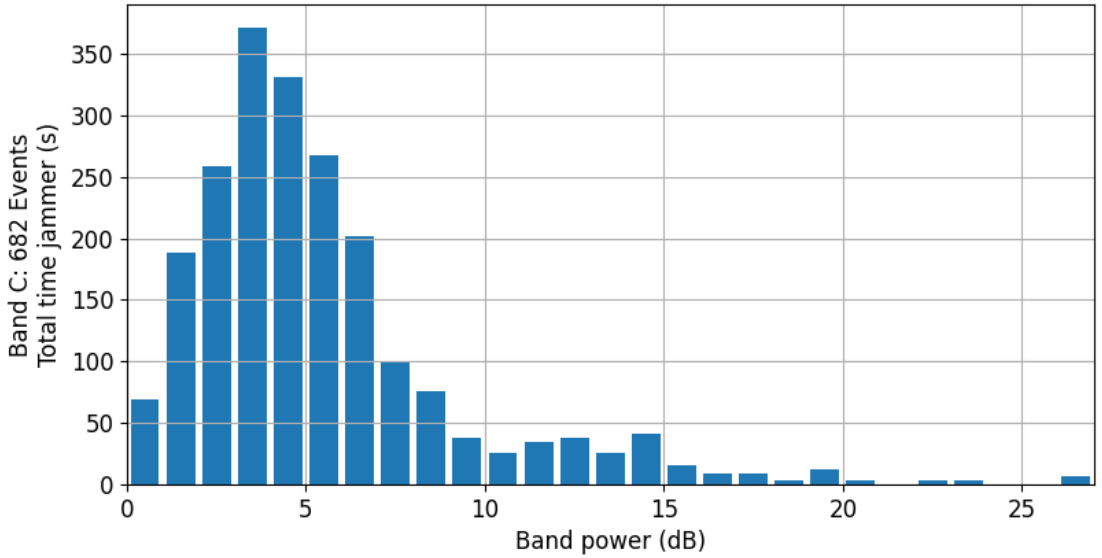


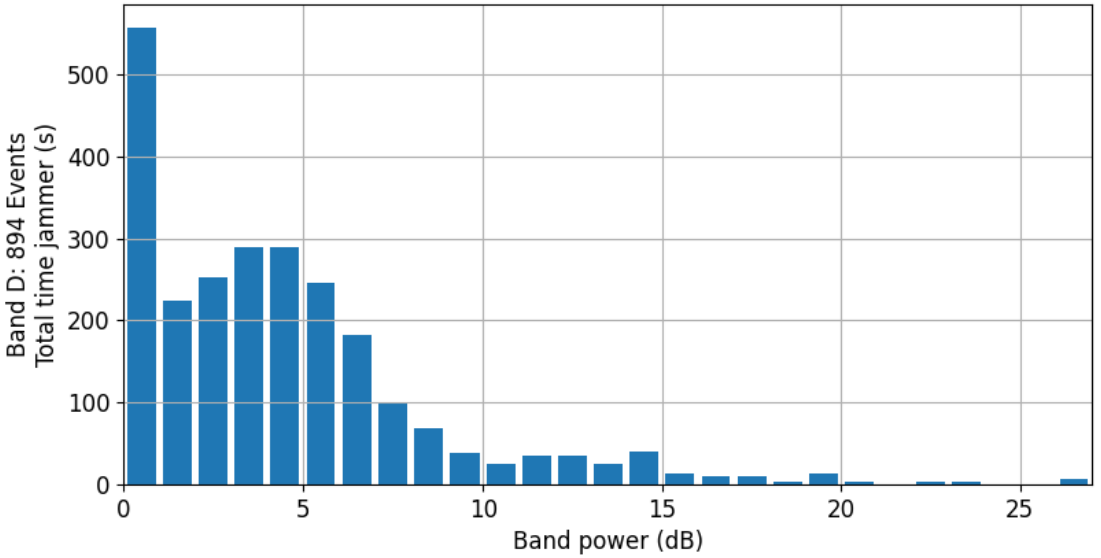
Cloud data analysis and trends - 2

Time-modulated jammer events

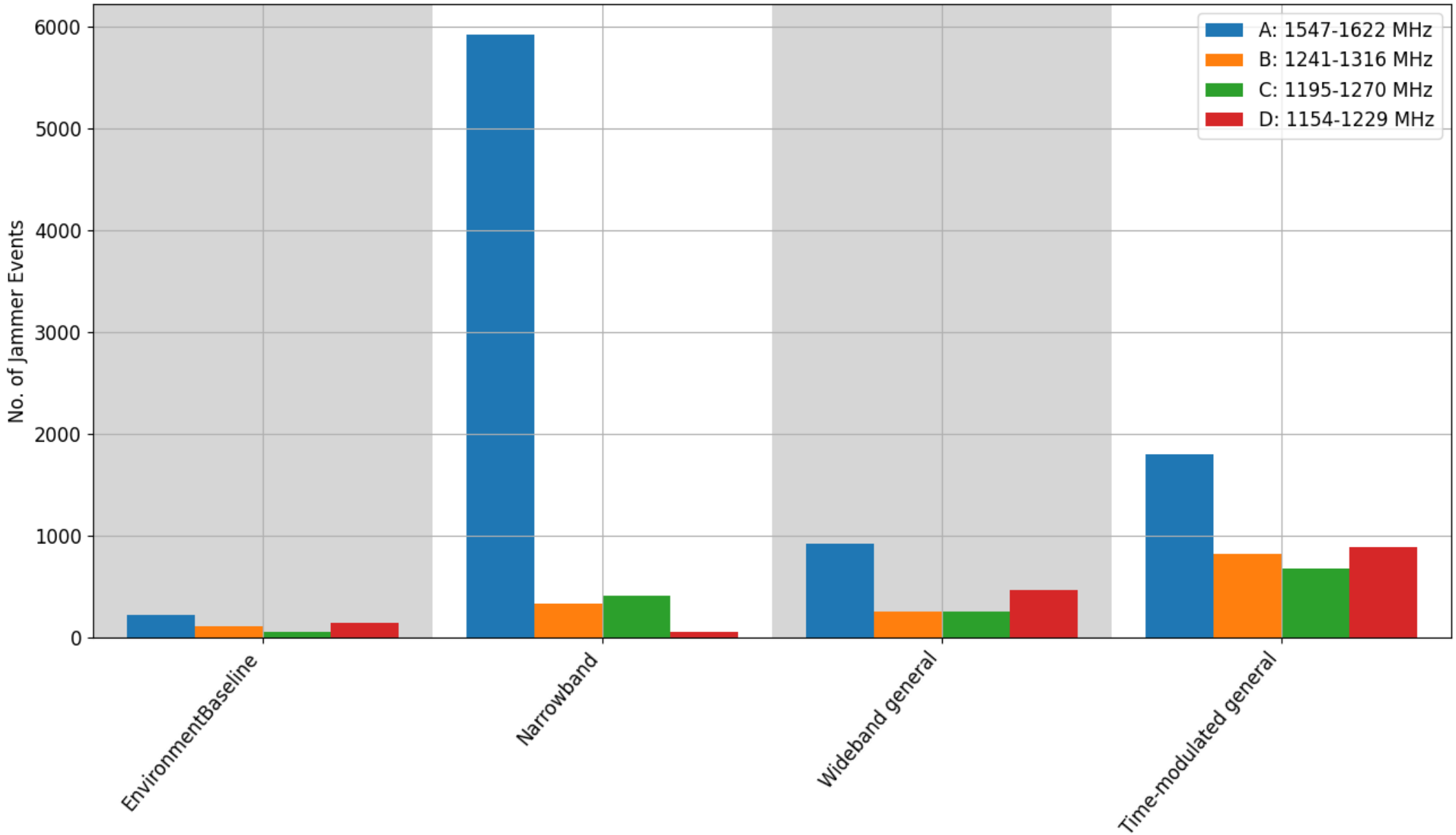




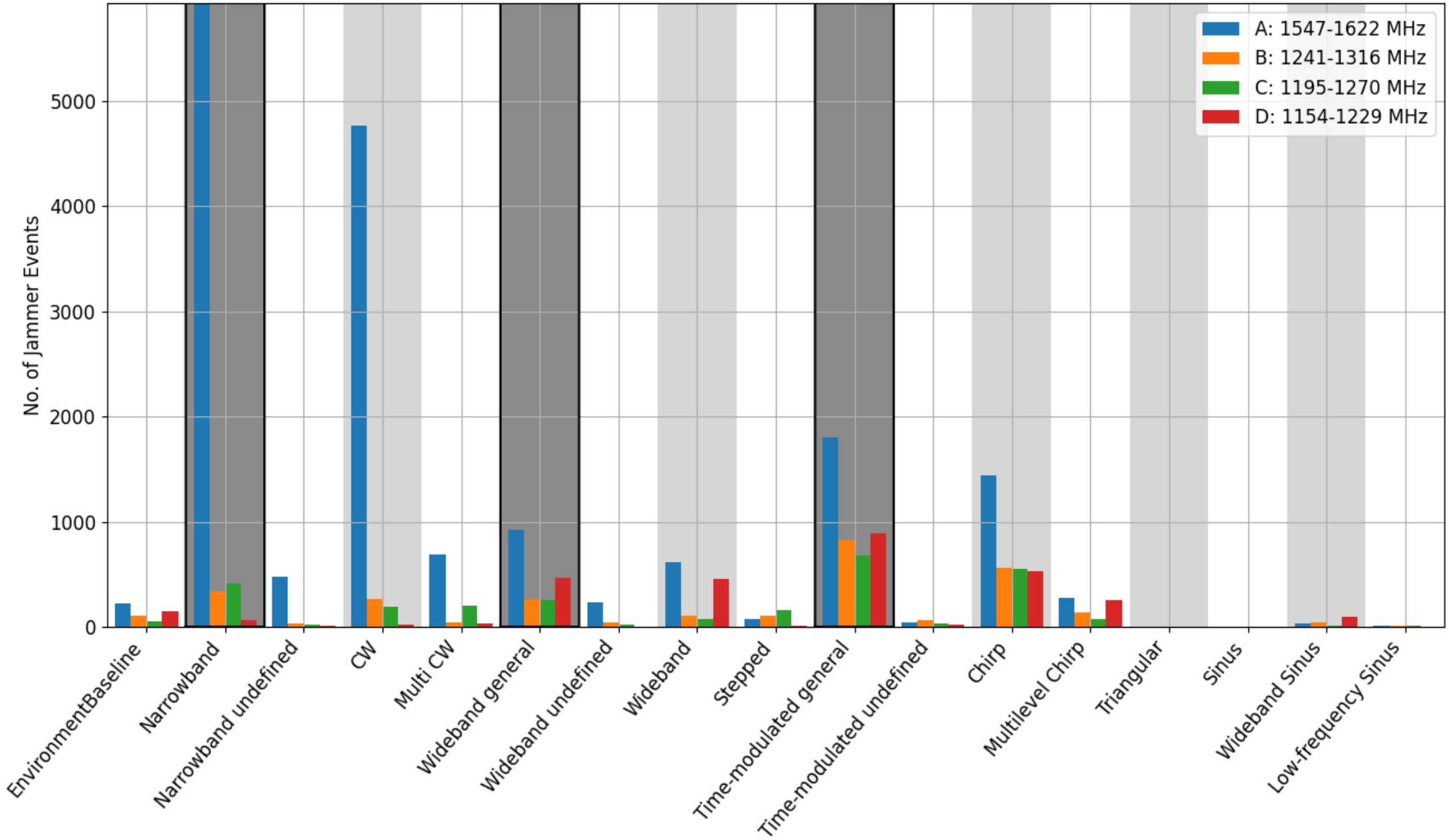




Cloud data analysis and trends - 3



Cloud data analysis and trends - 4



Specialized sub-band analysis - 1

Average RFI presence per day (sec)									
Site	**Days of obser-vation**	**Total number of events**	**All bands accumulated**	**L1/E1**	**L5/E5a**	**E5b**	**L1/E1 + E5a**	**L1/E1 + E5b**	**L1/E1 + E5a + E5b**
Moss	463	5670	30.2	29.3	7.2	5.5	6.0	4.9	4.6
Trondheim	561	2551	17.3	15.6	2.1	3.0	1.4	1.4	1.3
Trondheim B	535	909	7.8	7.5	1.5	1.7	1.3	1.4	1.3
Trondheim C	730	5016	37.9	32.4	11.2	10.7	6.8	5.7	5.6
Asker	342	1444	19.2	17.9	7.3	6.6	6.0	6.4	5.7
Amsterdam	485	2183	27.7	27.6	3.9	1.5	3.8	1.5	1.4
Total	**3116**	**18600**							
Average			**23.4**	**21.7**	**5.5**	**4.8**	**4.2**	**3.6**	**3.3**

Occurrence ratios					
L1/E1 vs L5/E5a	**L1/E1 Vs E5b**	**L1/E1 vs L1/E1 + L5/E5a**	**L1/E1 vs L1/E1 + E5b**	**L1/E1 vs L1/E1 + L5/E5a + E5b**	**E5a vs E5b**
3.9	**4.5**	**5.1**	**6.1**	**6.5**	**1.1**

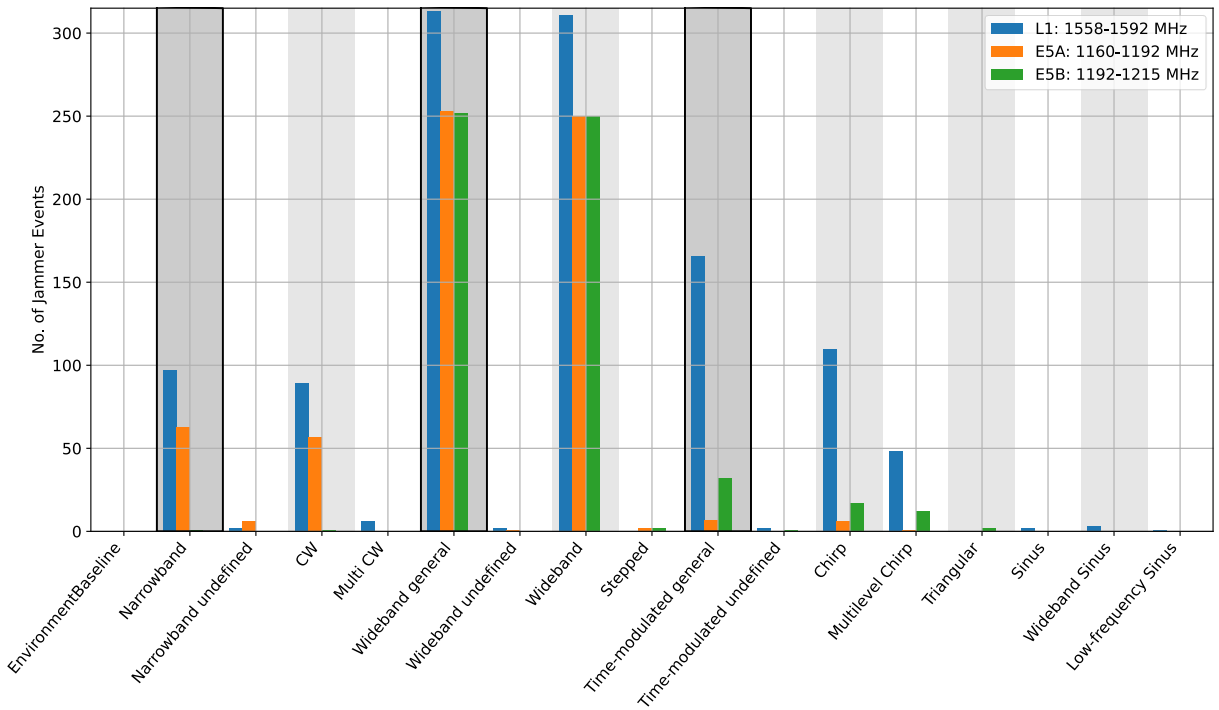
SINTEF

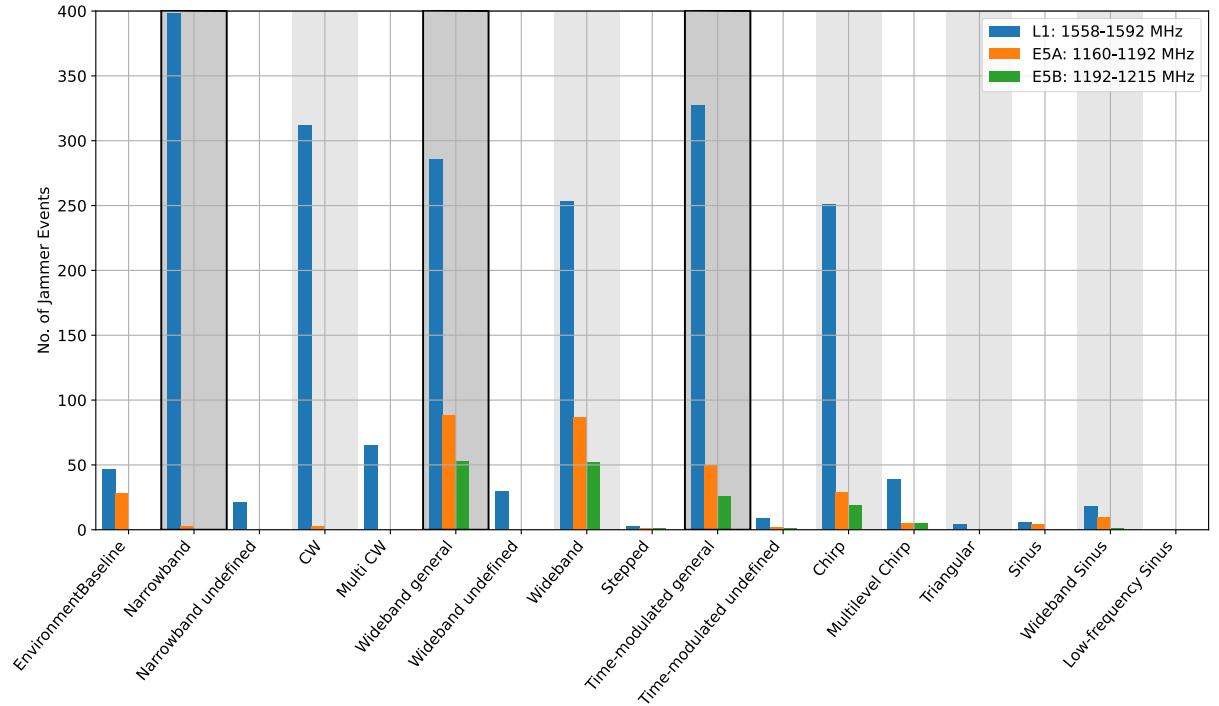
Specialized sub-band analysis - 2

	Probability of RFI occurrence					
Site	**L1/E1**	**L5/E5a**	**E5b**	**L1/E1 + L5/E5a**	**L1/E1 + E5b**	**L1/E1 + E5a + E5b**
Moss	3.34e-04	8.30e-05	6.37e-05	7.00e-05	5.65e-05	5.32e-05
Trondheim	1.80e-04	2.42e-05	3.52e-05	1.57e-05	1.57e-05	1.47e-05
Trondheim B	8.67e-05	1.74e-05	1.96e-05	1.53e-05	1.66e-05	1.53e-05
Trondheim C	3.75e-04	1.30e-04	1.24e-04	7.91e-05	6.63e-05	6.54e-05
Asker	2.07e-04	8.40e-05	7.58e-05	6.96e-05	7.46e-05	6.55e-05
Amsterdam	3.20e-04	4.52e-05	1.76e-05	4.44e-05	1.72e-05	1.68e-05
Average	**2.50e-04**	**6.39e-05**	**5.60e-05**	**4.90e-05**	**4.12e-05**	**3.85e-06**

SINTEF

Specialized sub-band analysis - 3





SINTEF

Thankfully the problem is being taken seriously in Norway

Statens vegvesen
Norwegian Public Roads Administration

Norwegian Communications Authority

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment

- Thanks up front to Nkom, FFI and SVV, and the other organizers
  - Justervesenet for spoofing tests
- Jammertest 2022 was carried out in Norway on the island of Andoya, near the settlement of Bleik
- Jammertest 2023 used the same venue with additional secondary testing sites
- Jammertest 2024 should return

Event overview

Photo: Nicolai Gerrard

- What was special about the location
  - The test site at Bleik is surrounded on 3 sides by mountains
    - Photo taken from the top of the ridgeline
    - Prevents propagation of the signal in most directions
    - One small community with one road in, one road out
    - High mountains also effectively mask airspace inland
  - Some signal exits but it's out to sea

- The map shows the location of the high power jammers operated by FFI
  - The primary testing was carried out at the Bleik community house
    - Location 3 in the map and photo

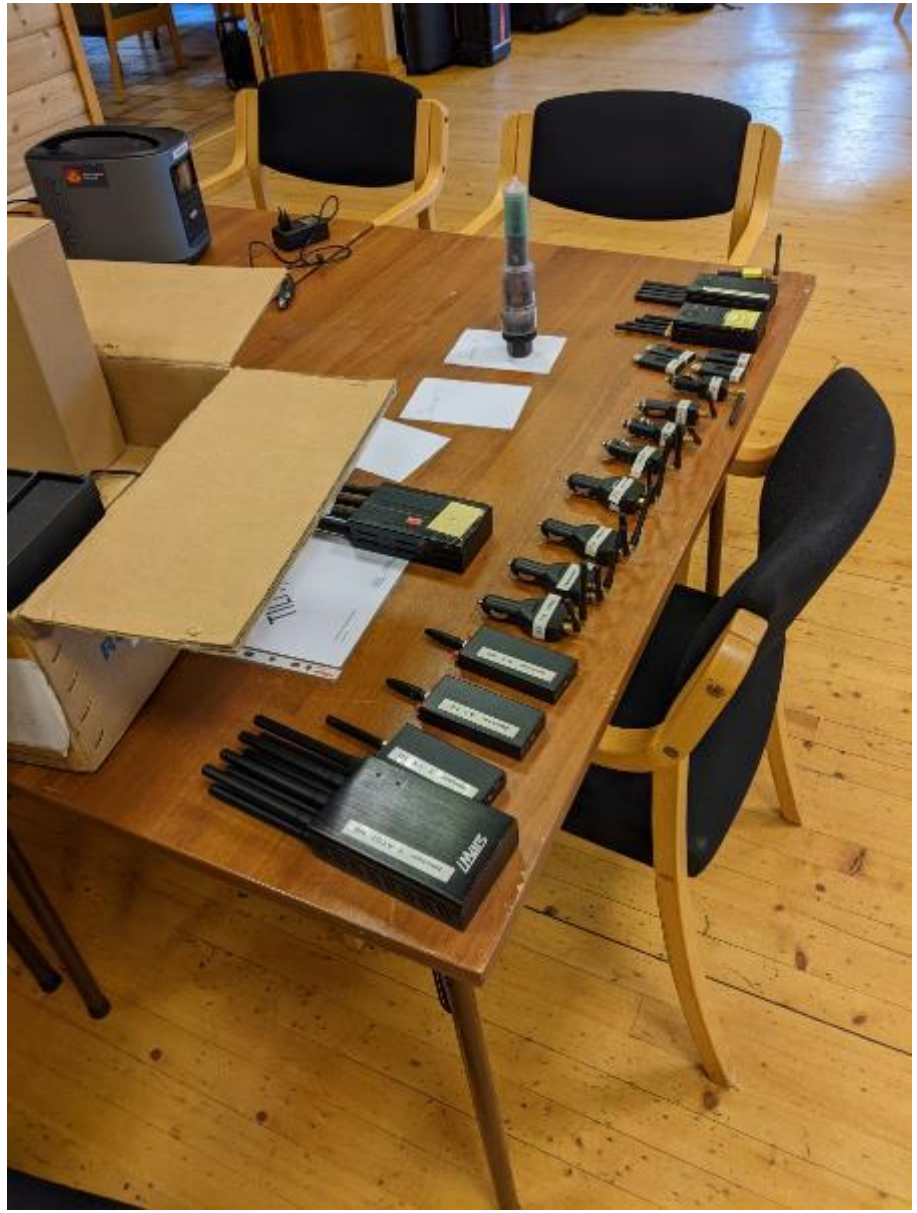
- Secondary testing was done at a location further south

- The test plan was extensive…

Event overview - 2

- The geography is perfect for isolating the test area from the mainland
  - Airspace is also protected by the high mountain ridge
  - Arrays of low power ‘personal privacy devices’ on the table
  - High power sources shown on the mountain top below
  - Well executed spoofing attacks (correct ephemeris, 10ns level synch.)

Photos:
Left: Jammertest 2023 – David Jensen
Right: Jammertest 2022 – Aiden Morrison



The Bad News

- Sadly collectively there are still large vulnerabilities in the ways systems work together
- Despite having active internet connections, inertial sensors and sometimes even barometers many platforms are more than willing to teleport in position and time
  - Reminds of the 2016 Portland ION simulator spoofing ‘accident’

- Some receivers required resets to regain functionality
  - Some receivers believed they had violated COCOM limits and shut down

- Some receivers believed they had passed their license expiry
  - These Devices purge expired licenses
  - Needed to be re-authorized to start working again

- Some receivers entered unrecoverable error states from jamming
  - Not spoofing. Just jamming.

Photo: Duus Media

The good news

- Norway is taking the RFI situation very seriously
  - The days of hiding the problem are over
  - Jammertest activities are open for publication
  - It's better to openly test and compare results than to pretend the problem doesn't exist

- It's one of the only jamming & spoofing events where publication of results is allowed and encouraged

- It's great, but room is limited
  - 120+ attendees or registrants, of which ~75 shown in top image
  - 2023 had over 200 attendees
  - 2024 might be even busier

- The US DHS has announced limited public tests
  - Attitudes are changing – open discussion now

2022

2023

Photos: David Jensen

Related references

- Sokolova, N., Morrison, A., and Diez, A. (2022). Characterization of the GNSS RFI Threat to DFMC GBAS Signal Bands. *Sensors,* Vol 22, no. 22: 8587. https://doi.org/10.3390/s22228587
- Diez, A., Morrison, A., and Sokolova, N. (2022), Automatic classification of RFI events from a multi-band multi-site GNSS monitoring network, in proceedings of the 35th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2022), 19-23 Sept. Denver, CO, US.
- Morrison, A., Sokolova, N., Gerrard, N., Rost, C., and Ruotsalainen, L. (2022), Radio frequency interference considerations for utility of the Galileo E6 signal based on long term monitoring by ARFIDAAS, *NAVIGATION*: Journal of the Institute of Navigation March 2023, 70 (1) navi.560; https://doi.org/10.33012/navi.560
- Morrison A., Sokolova N., Swinden R., Musumeci L. and G. Caparra (2022). Advanced RFI Detection, Alert and Analysis System Design and Monitoring Campaign Results, in proceedings of NAVITEC 2022, April 2022.
- Gerrard, N., Morrison, A., Sokolova, N., Rødningsby, A. and Rost, C. (2022). Exploration of Unintentional GNSS RFI Sources: Causes, Occurrence Rates, and Predicted Future Impact, in proceedings of the 35th International Technical Meeting of the Satellite Di-vision of The Institute of Navigation (ION GNSS+ 2022), 19–23 Sept. 2022, Denver, CO, US.
- Morrison A., N. Sokolova, N. Gerrard, A. Rødningsby and C. Rost (2021), RFI Considerations for Utility of the Galileo E6 Signal, in proceedings of the 34th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2021), 20-24 Sept. St. Louis, Missouri, US.

SINTEF

SINTEF

Teknologi for et bedre samfunn