VIRGINIA TECH

NAVIGATION for A.V. INTEGRITY

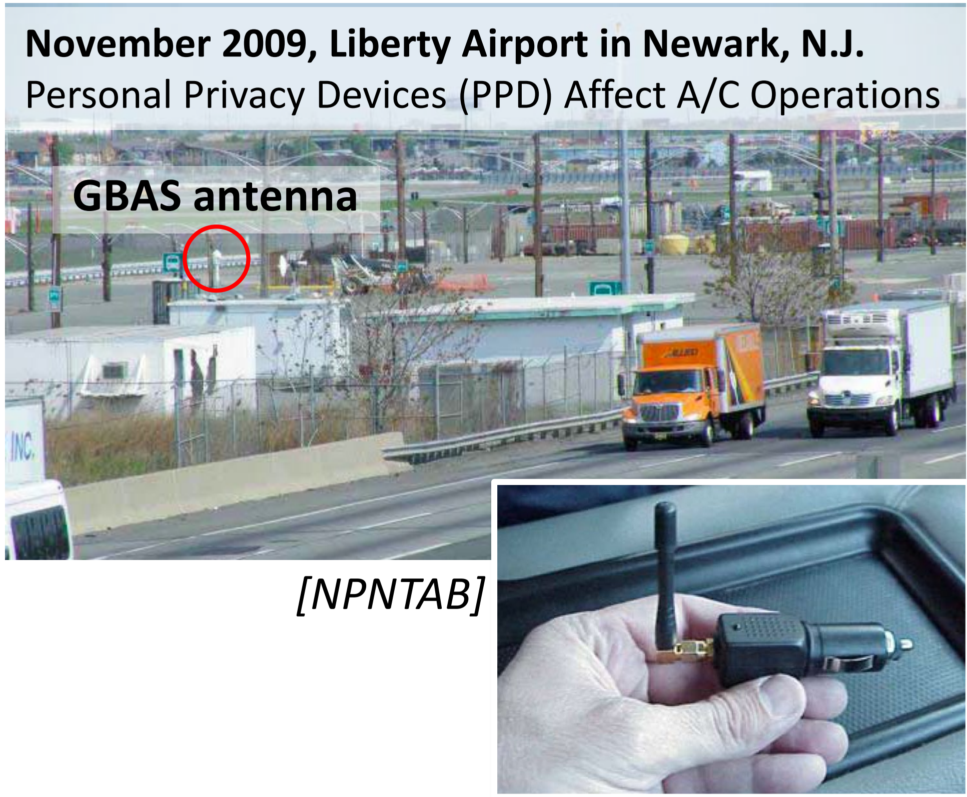
Sharing and Crowdsourcing GNSS Data to Monitor and Protect the GNSS RF Environment

Mathieu Joerger
Assistant Professor of Aerospace and Ocean Engineering
Virginia Tech, Blacksburg, VA
joerger@vt.edu

December 2022 - 10th ICG Workshop on GNSS Spectrum Protection and Interference Detection and Mitigation

Background

- GNSS Radio-Frequency Interference (RFI), including **jamming and spoofing**, are a growing threat to GNSS *[NSBPNTAB, Brunker]*
  - Local-area jamming, e.g.,
    from Personal Privacy Devices (PPDs)
  - Wide-area jamming, e.g., in conflict areas,
    or due to unintentional jamming
    - ➢ with **growing reliance on GNSS** for tracking and automation comes **new motives** for disturbance and manipulation


November 2009, Liberty Airport in Newark, N.J.

Personal Privacy Devices (PPD) Affect A/C Operations

[NPNTAB]

- Yet, **we are lacking a coordinated, deliberate, public response** to achieve Positioning Navigation and Timing (PNT) situational awareness
  - we need a “weather channel” for the RF environment (this does not need to be limited to GNSS RFI)

[NSBPNTAB] National Space-Based PNT Advisory Board. “Protect, Toughen, and Augment Global Positioning System for Users.” gps.gov, 2018.

[Brunker] M. Brunker, “GPS under attack as crooks, rogue workers wage electronic war,” News Brief at NBC, 2016.

[NPNTAB] National PNT Advisory Board, “Comments on Jamming the Global Positioning System - A National Security Threat: Recent Events and Potential Cures,” 2010

Motivation and Focus

- RFI monitoring using publicly available data has been demonstrated, **but typically provides circumstantial evidence of jamming/spoofing using opportunistic data** *[C4ADS, GBS Scott, Miralles, Strizic]*
  - using crowd-sourced data, shared by **volunteers**
  - using data of opportunity: **not dedicated** to RFI monitoring (often missing), posted with significant **latency**
    - *Were the detected events **actual RFIs?** Are they **impacting GNSS now?***
    - *What if we made **a more deliberate effort** to address RFI?*

- In this presentation:
  - Example: **GNSS jamming monitoring** using data of opportunity from traffic management systems
  - Our effort: opportunistic data to **find suspected jammers**, dedicated equipment to **prove jamming**

[C4ADS] C4ADS. “Above us only stars.” Tech. Rep., 2019.

[GBS] Bjorn Bergman. “Systematic Data Analysis Reveals False Vessel Tracks.” Data and technology, News & Views, Research and analysis, 2021

[Scott] L. Scott, “J911: The case for fast jammer detection and location using crowdsourcing approaches,” ION GNSS 2011

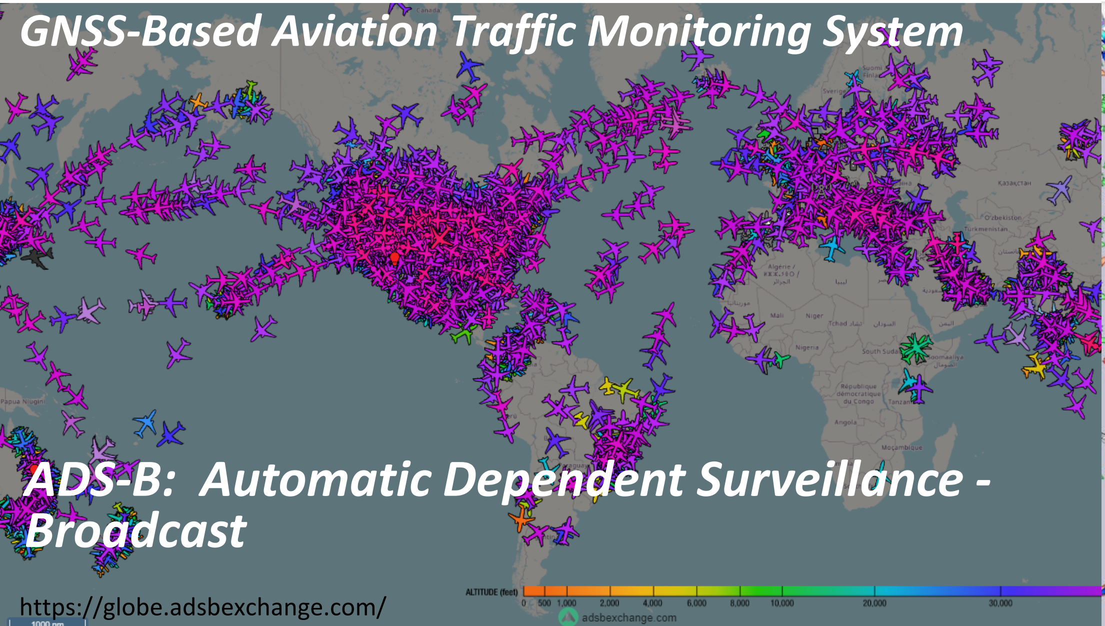
[Miralles] D. Miralles, N. Levigne, D. M. Akos, J. Blanch, and S. Lo, “Android raw GNSS measurements as the new anti-spoofing and anti-jamming solution,” ION GNSS+ 2018.

[Strizic] L. Strizic, D. M. Akos, and S. Lo, “Crowdsourcing GNSS jammer detection and localization,” ION ITM 2018.

GNSS Jamming and Spoofing

- Threats to GNSS and a major concern in aviation:
  - **Spoofing**: faking GPS (for misleading, high-jacking)
  - **Jamming**: denial of service

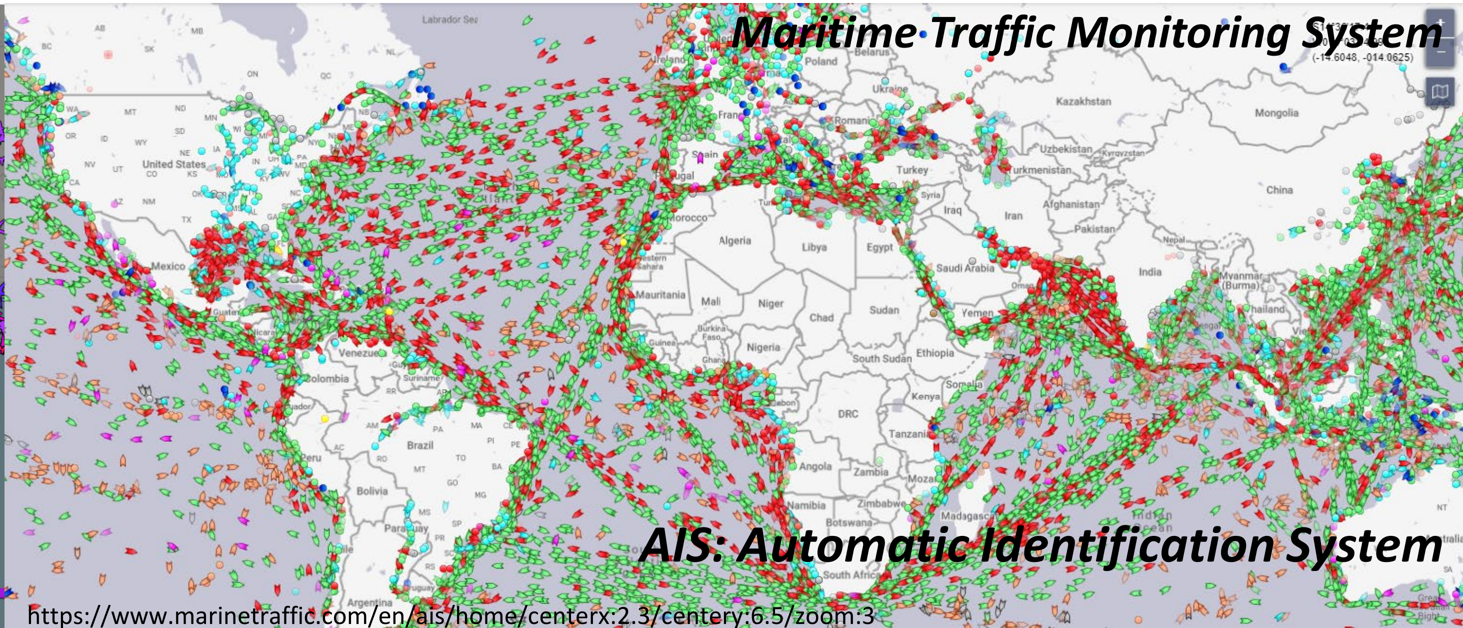
- **Large, wide-spread GNSS jamming** can be observed using publicly available data



GNSS-Based Aviation Traffic Monitoring System

ADS-B: Automatic Dependent Surveillance - Broadcast

https://globe.adsbexchange.com/



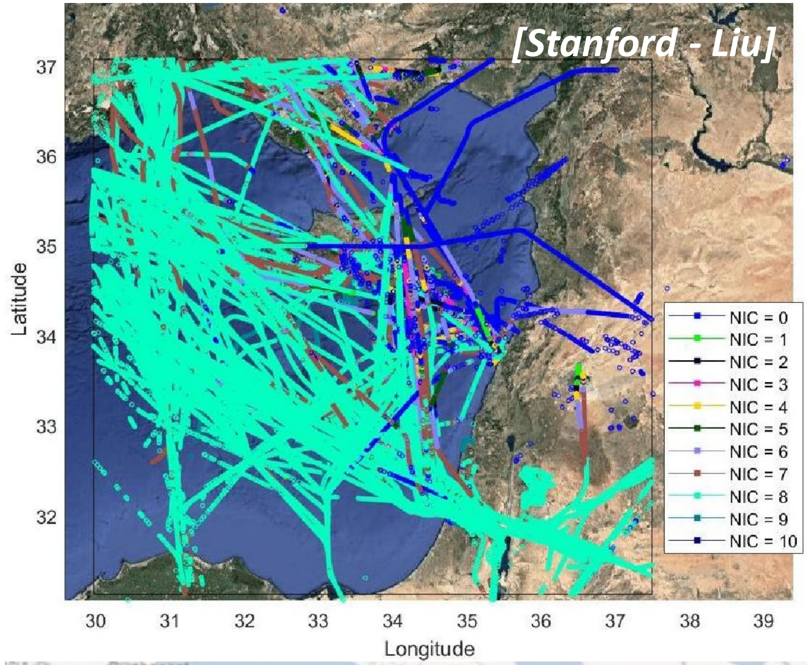
Maritime Traffic Monitoring System

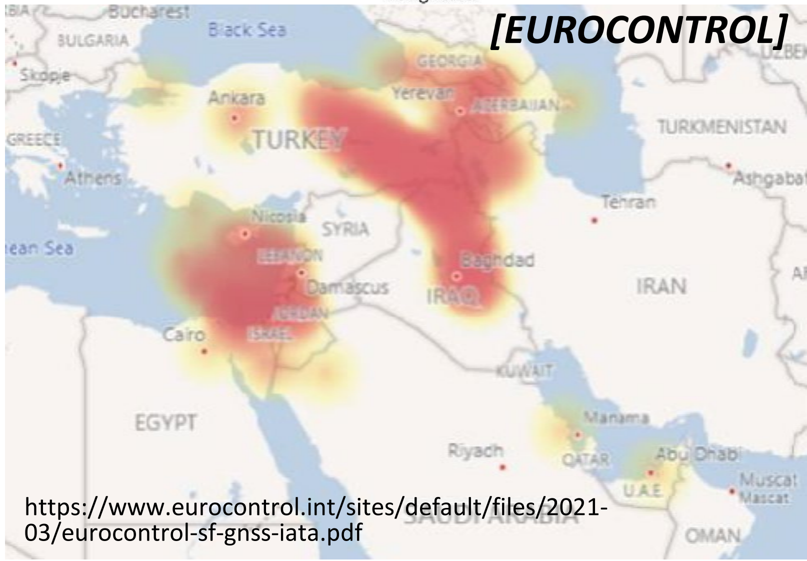
AIS: Automatic Identification System

https://www.marinetraffic.com/en/ais/home/centerx:2.3/centery:6.5/zoom:3

Using ADS-B to Localize Jamming in Syria (September 2020)

- ADS-B is a GNSS-based traffic monitoring system
  - aircraft are required to share their location
  - ADS-B In receivers (e.g., VT) access air traffic data and can voluntarily share it online (e.g., adsbexchange.com)
- Liu et al. analyzed ADS-B data during jamming incidents in Cypriot and Syrian airspace in September 2020. *[Liu]*
  - ADS-B data include **NIC: Navigation Integrity Category** – indicator of containment radius
- A heat map of RFI pilot reports in the region was also generated *[EUROCONTROL].*


[Stanford - Liu]

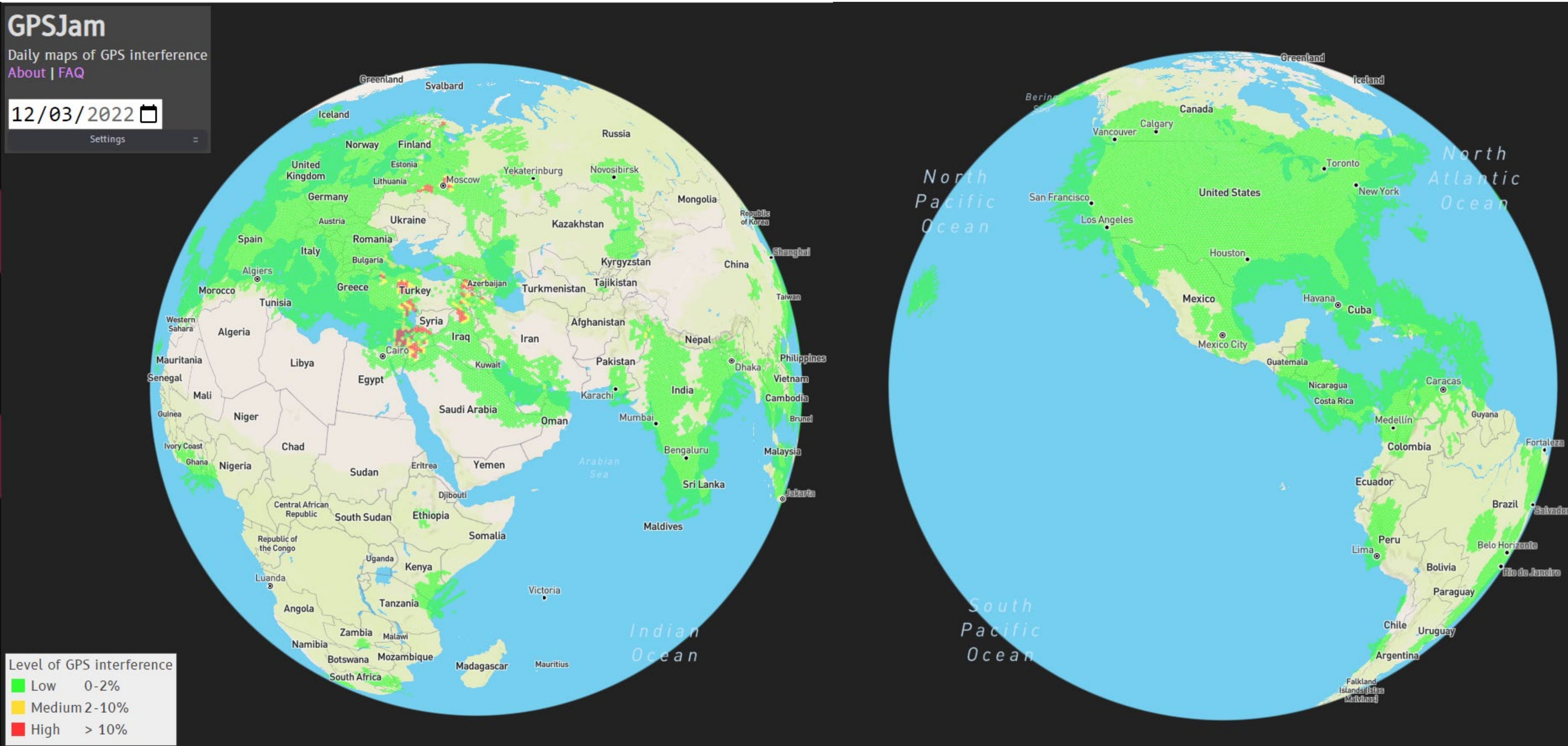

[EUROCONTROL]

https://www.eurocontrol.int/sites/default/files/2021-03/eurocontrol-sf-gnss-iata.pdf

[Stanford – Liu] Liu, Z., Lo S., & Walter, T. “GNSS Interference Detection Using Machine Learning Algorithms on ADS-B Data.” *ION GNSS+ 2021.*

[EUROCONTROL] N. Pringvanich, “GNSS Interference: Impacts to airline operations.” 2021.

ADS-B-based Online Daily RFI Monitor



GPSJam

Daily maps of GPS interference

About | FAQ

12/03/2022

Settings

Level of GPS interference

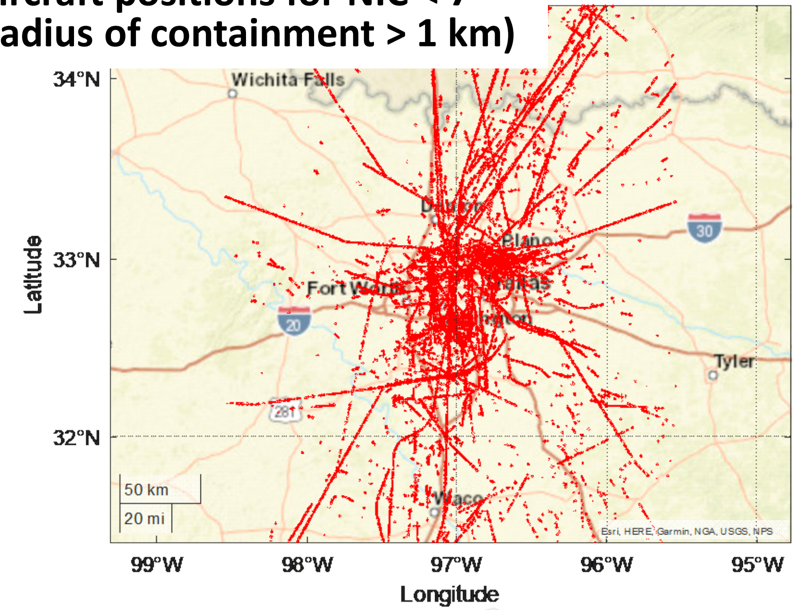
🟩 Low 0-2%

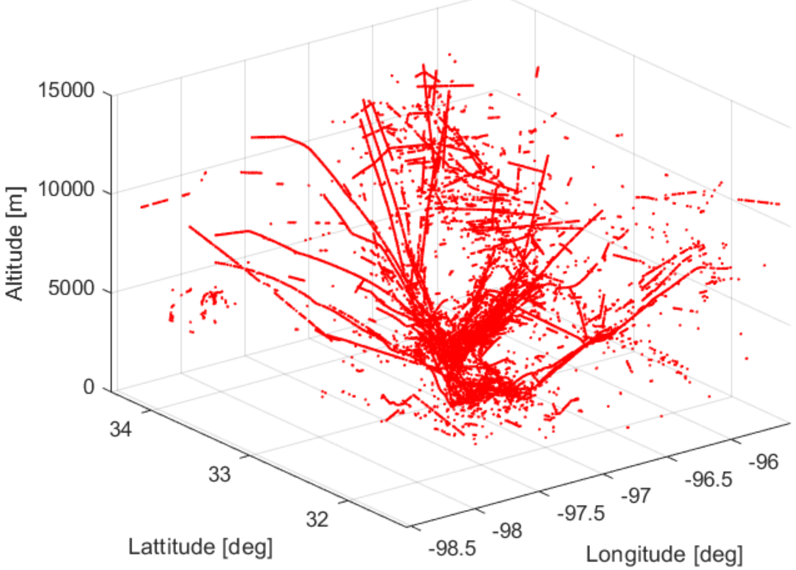
🟨 Medium 2-10%

🟥 High > 10%

Dallas Fort Worth (DFW) Airport (October 17-18 2022)

Aircraft positions for NIC < 7
(radius of containment > 1 km)

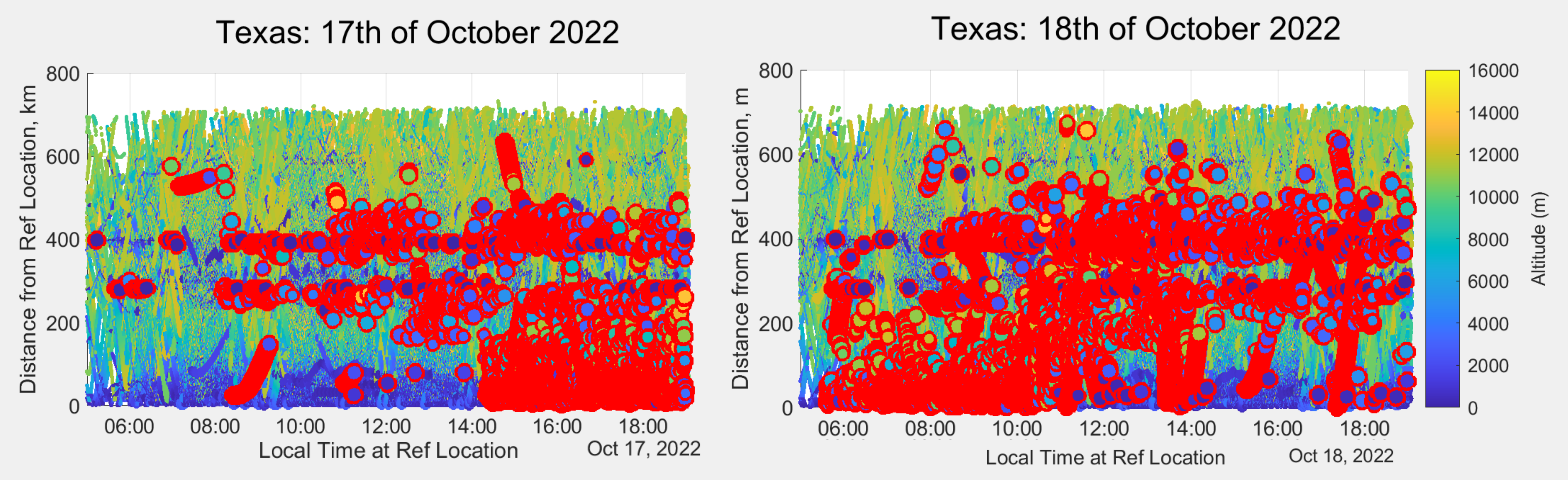




(UTC)

Dallas Fort Worth (DFW) Airport (October 17-18 2022)

- Widescale disturbance in the US National Airspace System – *cause unknown*
  - This event: obvious strong, wide-scale disturbance – **proof** by number of impacted users
  - In general: **how to identify actual jamming ?**
    and distinguish it from a large containment radius dur to poor GNSS?

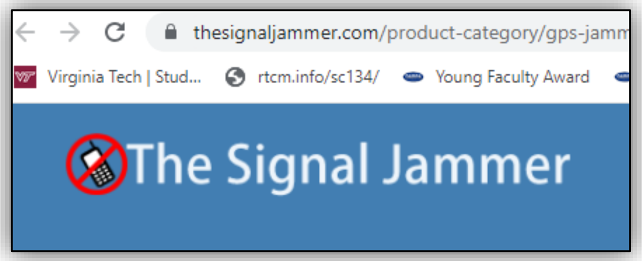


Texas: 17th of October 2022

Texas: 18th of October 2022

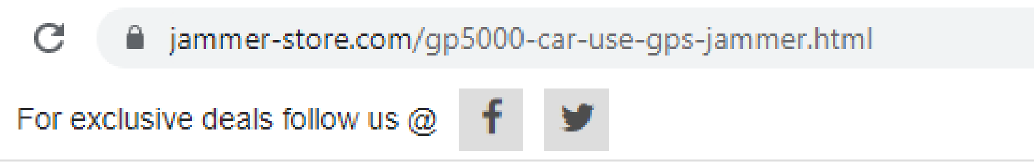
Focus on Widespread Jamming Issue

- **Motivation**:
  - avoid tracking by employers, authorities, (fishing, trafficking, toxic waste disposal), tracking by a significant other…
- **Jamming devices:**



thesignaljammer.com/product-category/gps-jamm

The Signal Jammer

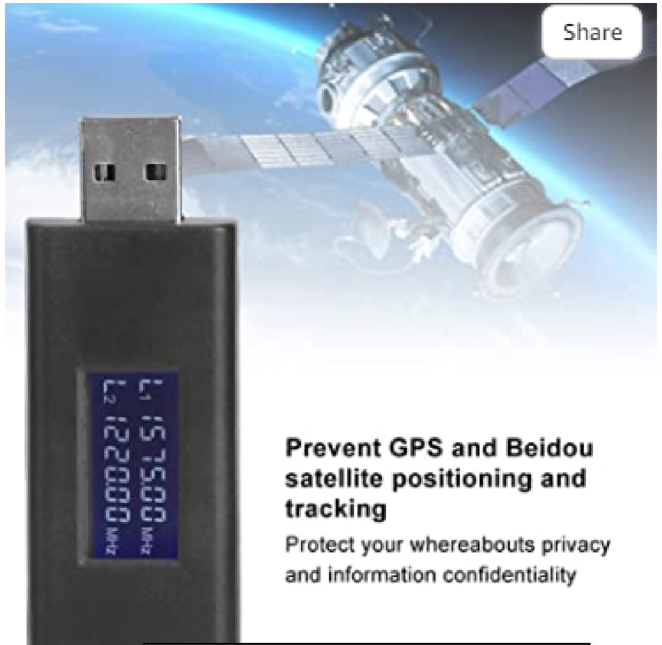


jammer-store.com/gp5000-car-use-gps-jammer.html

For exclusive deals follow us @

JAMMER-STORE

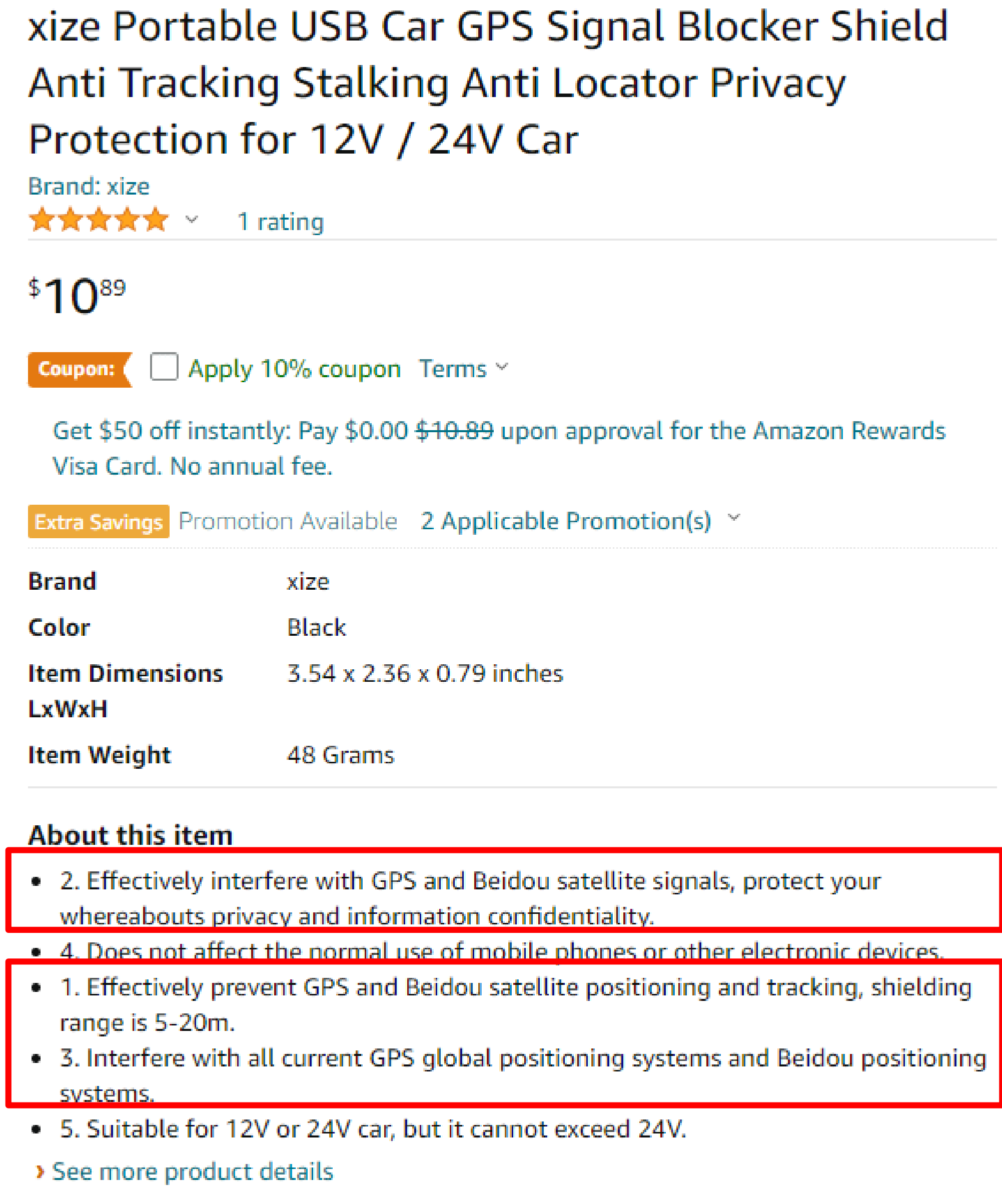
Privacy Protection



Prevent GPS and Beidou satellite positioning and tracking

Protect your whereabouts privacy and information confidentiality

> *"Your work is important, thanks for helping protect people from the tyranical exploitation of advanced technology"*
>
> TechCrunch.com



xize Portable USB Car GPS Signal Blocker Shield Anti Tracking Stalking Anti Locator Privacy Protection for 12V / 24V Car

Brand: xize

★★★★★ 1 rating

$10.89

Coupon: □ Apply 10% coupon Terms

Get $50 off instantly: Pay $0.00 ~~$10.89~~ upon approval for the Amazon Rewards Visa Card. No annual fee.

Extra Savings Promotion Available 2 Applicable Promotion(s)

Brand	xize
Color	Black
Item Dimensions LxWxH	3.54 x 2.36 x 0.79 inches
Item Weight	48 Grams

About this item

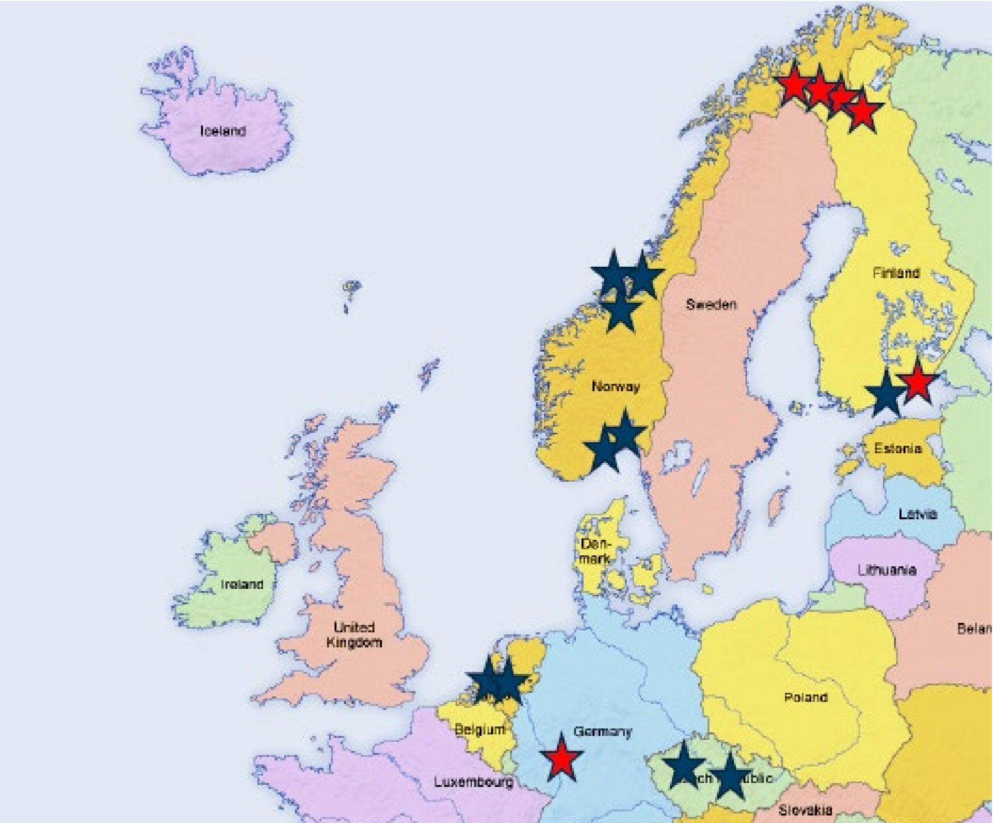
- 2. Effectively interfere with GPS and Beidou satellite signals, protect your whereabouts privacy and information confidentiality.
- 4. Does not affect the normal use of mobile phones or other electronic devices.
- 1. Effectively prevent GPS and Beidou satellite positioning and tracking, shielding range is 5-20m.
- 3. Interfere with all current GPS global positioning systems and Beidou positioning systems.
- 5. Suitable for 12V or 24V car, but it cannot exceed 24V.

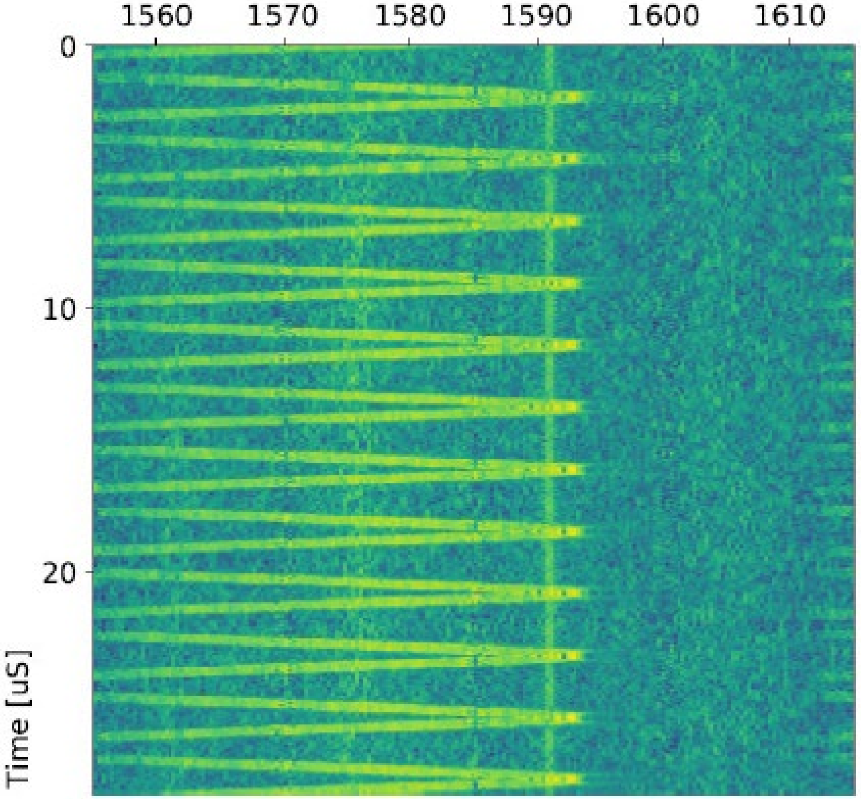
› See more product details

Getting Evidence Using Dedicated Equipment

- Example: European Union STRIKE3 program (H2020) found 160,000 GNSS interference events over 18 months in 14 countries.
  - "Standardisation of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation"

- Example: Norway's SINTEF
  - Finding evidence of PPD chirp jammers
  - tens of thousands of events *[SINTEF]*





[SINTEF]
Aiden J. Morrison, Nadezda Sokolova, Nicolai Gerrard, Anders Rødningsby, Christian Rost, Laura Ruotsalainen, "RFI Considerations for Utility of the Galileo E6 Signal," ION GNSS+ 2021.

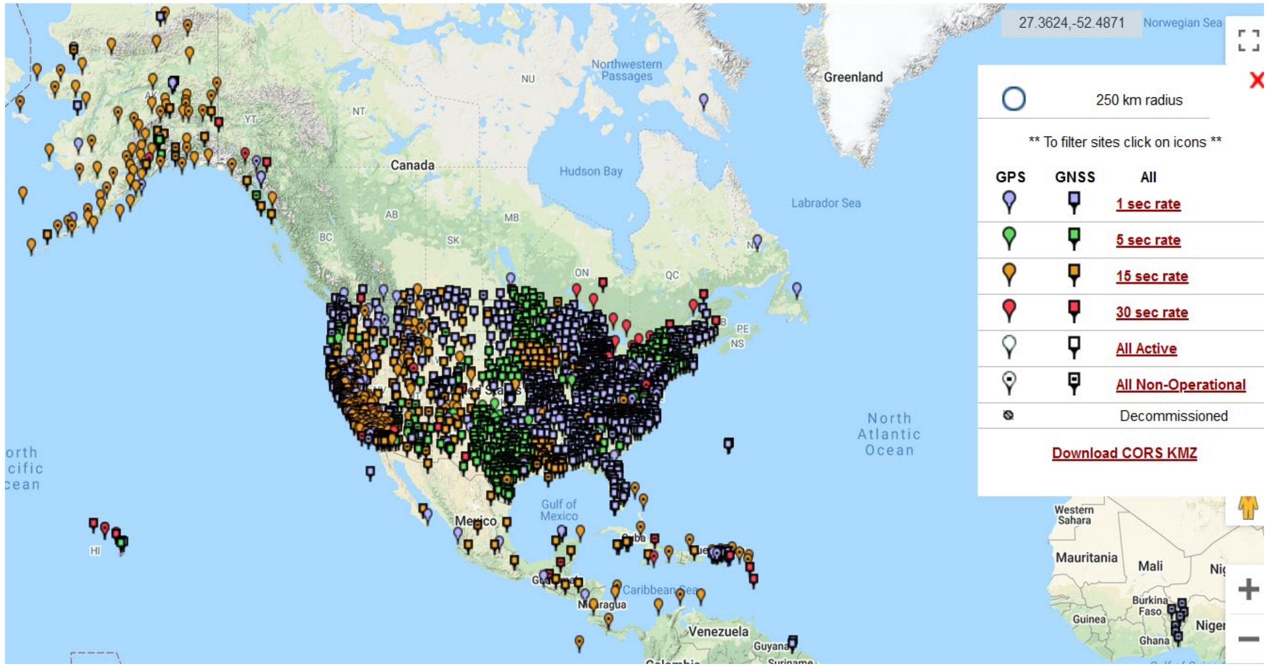
Evaluation Using NGS CORS Site Data

- We leverage **a receiver networks** providing publicly-available data
  - signal quality “C/N0” data
  - no RF front end data (still better than NIC)

- We want to improve detection using a receiver network as compared to a single receiver:
  - We want to **identify temporal an spatial interference patterns**

- To **prove the presence** of RFI:
  - We will **predict RFI,** and deploy our equipment

Map of CORS Network Reference Stations



○ 250 km radius

** To filter sites click on icons **

GPS	GNSS	All
		1 sec rate
		5 sec rate
		15 sec rate
		30 sec rate
		All Active
		All Non-Operational
		Decommissioned

Download CORS KMZ

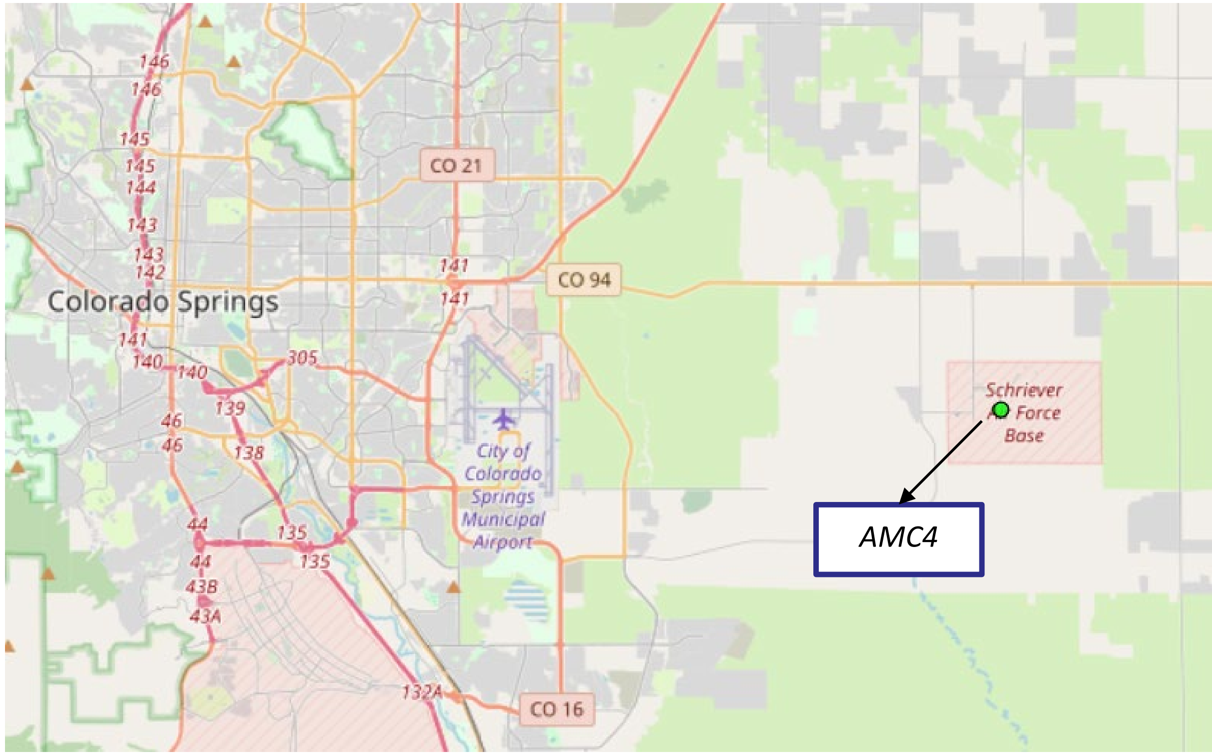
Source: https://www.ngs.noaa.gov/CORS_Map/

*NOAA National Geodetic Survey (**NGS**) Continuously Operating Reference Stations (**CORS**) is a network of ~2000 reference stations.*

Jada, S., Psiaki, M., Landerkin, S., Langel, S., Scholz, A., & Joerger, M. (2021, September). Evaluation of PNT Situational Awareness Algorithms and Methods. In *ION GNSS+ 2021*

Jamming Detection on US Highways Using CORS and IGS Data

- We designed a C/N0-based jamming detectors *[Jada 2021]*:
  - **highly-sensitive** (locally Neyman-Pearson optimal)
  - ensuring a **quantifiable risk of false alerts**
- The monitor **is self-calibrating**:
  - a **high-fidelity** mean-C/N0 model and a **robust** probabilistic model of nominal deviations
  - automatically adjusts to different receivers, antennas, local multipath environments
- We processed data from **900 stations** along US highways



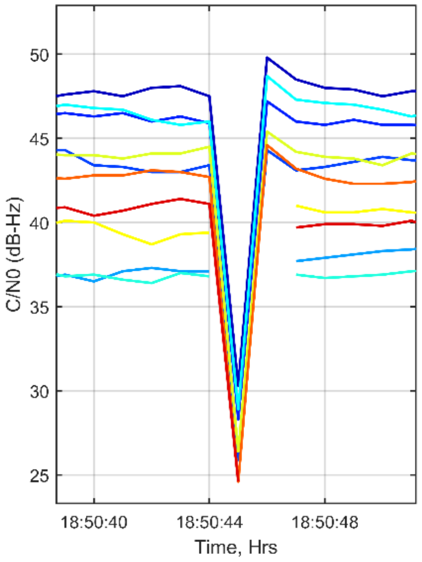
The IGS (International GNSS Service) site lies near a highway. We could deploy our equipment on a parking lot near the highway.

[Jada 2021] Jada, S., Psiaki, M., Landerkin, S., Langel, S., Scholz, A., & Joerger, M. (2021, September). Evaluation of PNT Situational Awareness Algorithms and Methods. In *ION GNSS+ 2021*

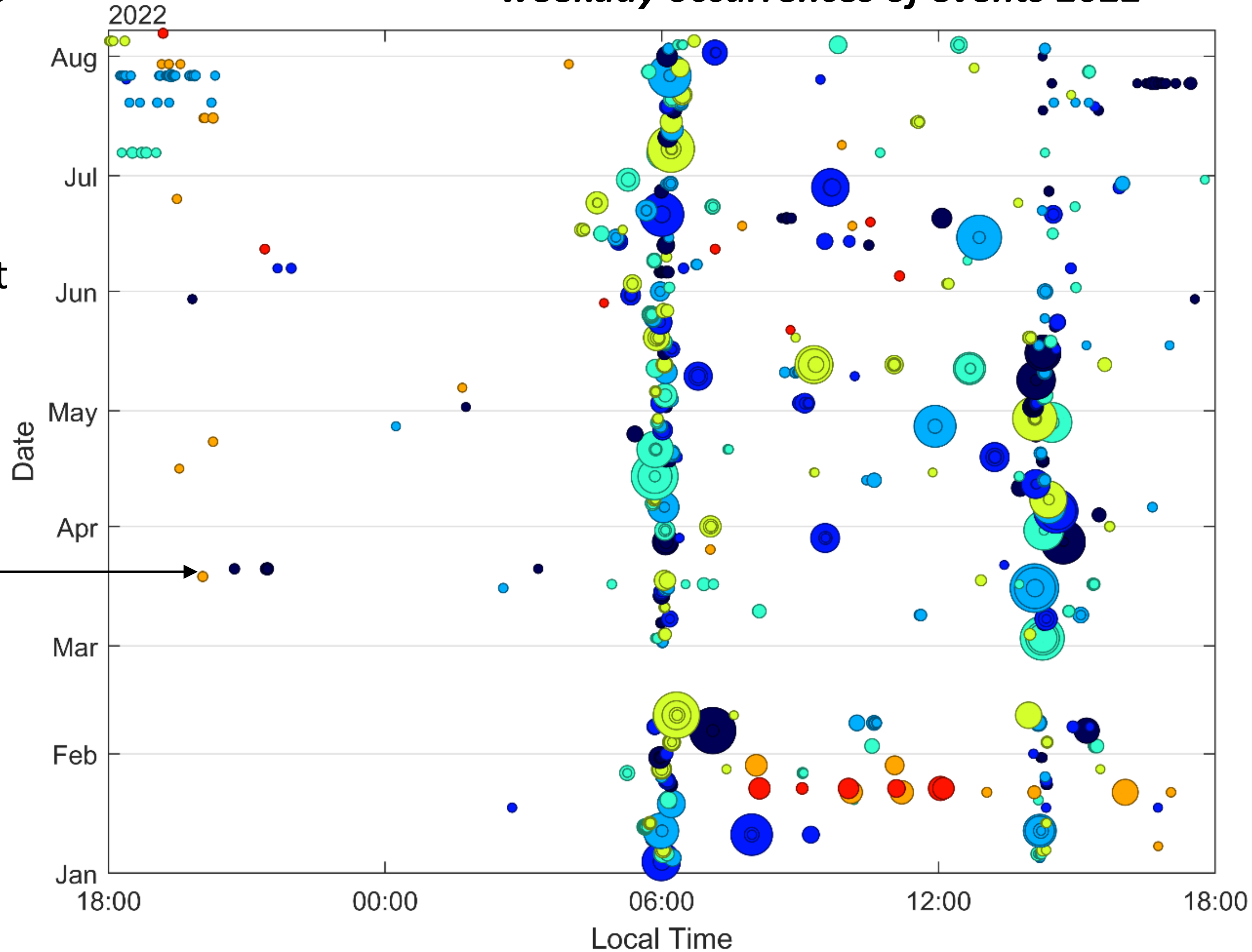
IGS Data Analysis: Colorado Springs

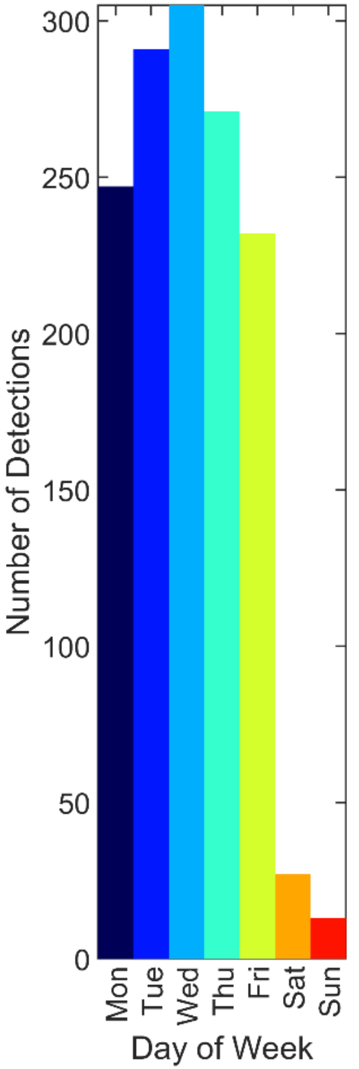
- We found RFI patterns at an IGS station in Colorado Springs, CO.
  - RFI: 6:00 am and 2:00 pm on weekdays over the past 8 months.

Example event



C/N0-based jamming detector results showing ***weekday occurrences of events 2022***





[Jada 2022] Jada, S., Bowman, J., Psiaki, M., Fan, C., Joerger, M. "Time-Frequency Analysis of GNSS Jamming Events Detected on US Highways." In *ION GNSS+ 2022*

Wideband RF Data Collection Hardware

- To characterize GPS interference, we designed a **portable wideband RF data collection setup**
  - using a **Universal Software Radio Peripheral (USRP)**
  - a non-GPS-disciplined osccillator
  - an extra COTS (commercial off-the-shelf) receiver
- We designed a process to store memory-expensive wideband RF data
  - activated by an RF-signal **power-based detector**

Tallysman 33-8829NMAT

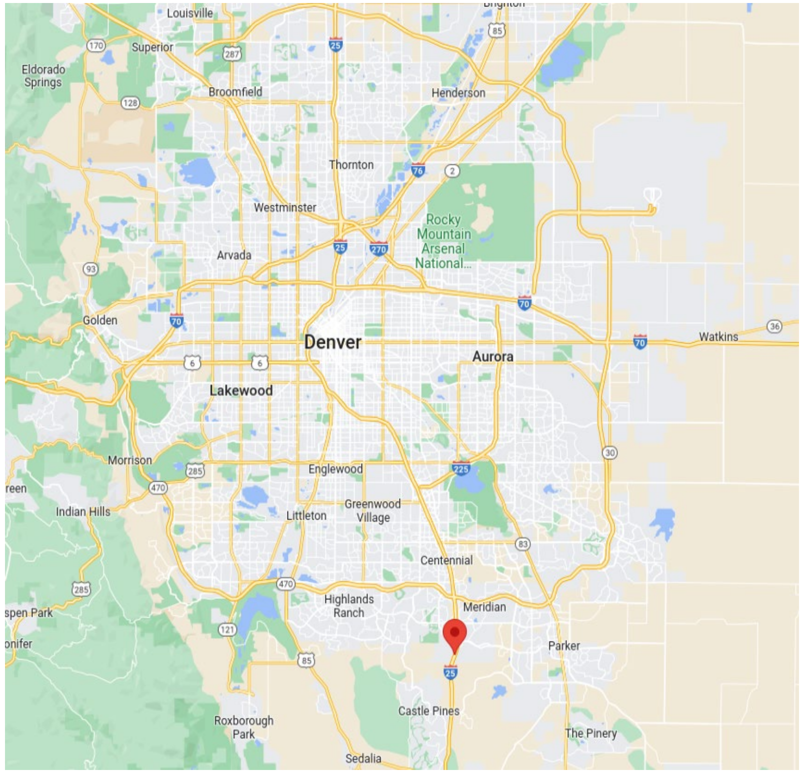
Connor Winfield OCXO-OH100

Ettus USRP N200 + DBSRX2 Daughter Board

Intel Next Unit in Computing - 6 (NUC6)

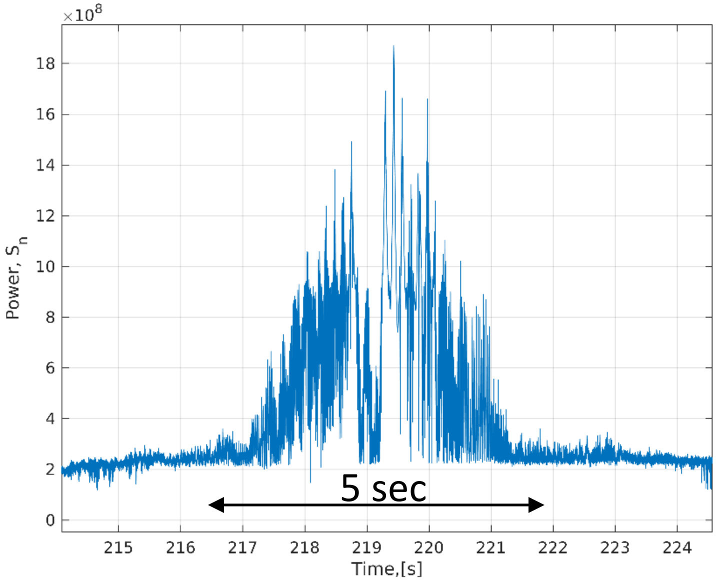
u-blox EVK M8F

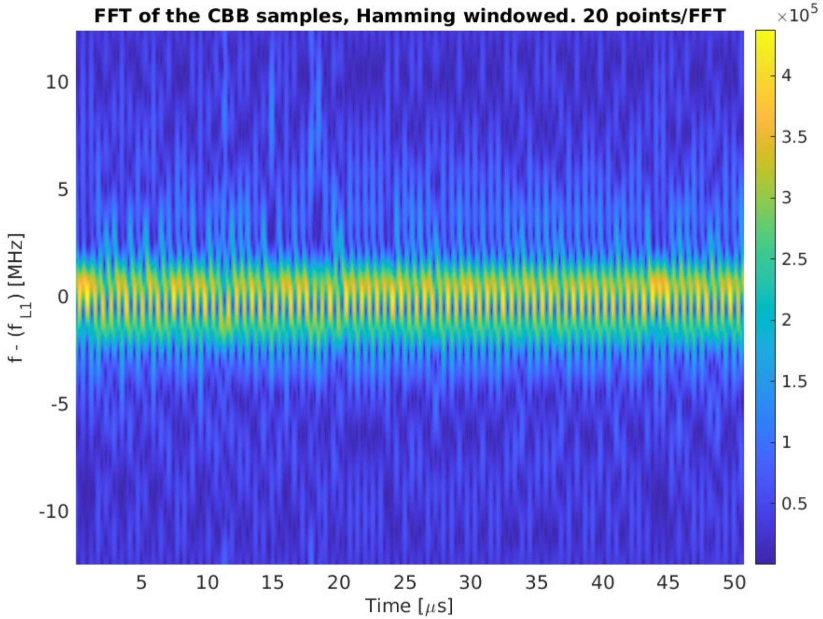
Spectrogram of a PPD Jamming Signal

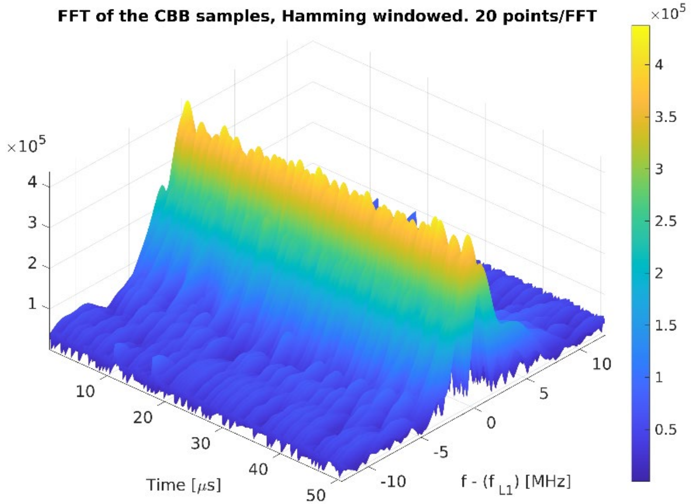


We identified a PPD near Denver on Interstate I-25, on September 21, 2022 at 8 AM**.**

Antennas mounted on our car







Conclusion

- GNSS plays a key role in **localization and coordination**
  - Positioning, Navigation, and Timing (PNT) infrastructure must be “**protected, toughened, and augmented**”

- Crowdsourced data from ADS-B (and cell-phone) can be used to detect and localize suspected jamming and spoofing
  - detection is **only possible a-posteriori, for wide-scale events**
    - proof of jamming comes from the number of impacted users
  - detection is not obvious for localized, temporary events

- We used publicly available data to **predict jamming events** on US highways
  - We then used our own equipment to observe and **identify jammers**

Way Forward

- There are numerous **connected GNSS receiver networks** that could be leverage for RFI monitoring
  - **traffic management** (ADS-B, AIS, in the near-term future: cars/trucks) and **scientific purposes** (CORS, IGS)
  - **differential GNSS** networks, **cell phone** towers (even cell phone users), etc.

- **Suggestions** --- we would improve GNSS RFI monitoring by:
  - designing messaging standards to include GNSS signal quality data fields (C/N0, AGC, RF front end bandwidth)
    - Radio Tech. Comm. for Marit. Serv.: **RTCM SC-134**, Integrity for GNSS-based High Accuracy Applications
    - **NMEA** (National Marine Electronics Association) – message proposed by Dong Kyeong Lee (UC Boulder)
  - developing **dedicated, robust** data collection and **low-latency sharing** systems
  - **coordinating data-monitoring** efforts and **alerting** system