Tampere University
Tampere University of Applied Sciences

Resilient PNT (positioning, navigation, and timing): emerging challenges and future directions

Prof. Heidi Kuusniemi, Tampere University

SEDDIT annual workshop 2025, 19.11.2025, Linköping University

Agenda

- What is PNT – and why does it matter?
- How GNSS works
- Vulnerabilities & threat models
- Real-world incidents
- Principles of resilient PNT
- Emerging mitigation & authentication
- Multi-layer PNT & LEO-PNT of the future
- Takeaways about the future of resilient PNT

What is Positioning, Navigation and Timing (PNT)?

- PNT stands for Positioning, Navigation and Timing:
  - Positioning: the ability to determine location and orientation
  - Navigation: the ability to determine current and desired position
  - Timing: the ability to acquire and maintain accurate and precise time from a standard anywhere in the world
- PNT underpins many everyday activities in modern society including transport, telecommunications, computers, emergency services, personal navigation and finances
- Global Navigation Satellite Systems (GNSS) are the primary sources of PNT information worldwide

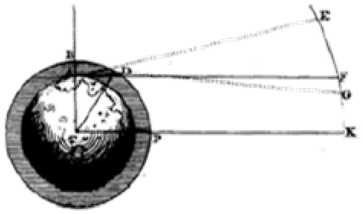
The history of PNT

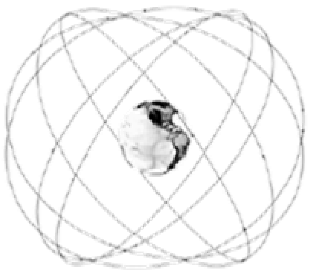
Celestial/Chrono
1770-1920
3000 m

Loran
1940s-2010
460 m

Transit
1964-1996
25 m

GNSS
1996-present
3 m - cm




Sextant, p. 1932.



Modified from: Xona Space Systems, SCPNT Symposium, Stanford University, October 2020

Tampere University
Tampere University of Applied Sciences

Why PNT matters

GNSS is for everyone - whether they know it or not

- Telecommunication networks rely on GNSS for time synchronization
- Banking transactions & stock exchanges → traceable global timing
- Power grids → phase synchronization
- Logistics & transportation → routing, AIS maritime, ADS-B aviation
- Everyday apps → Google Maps, Foodora, delivery routing etc

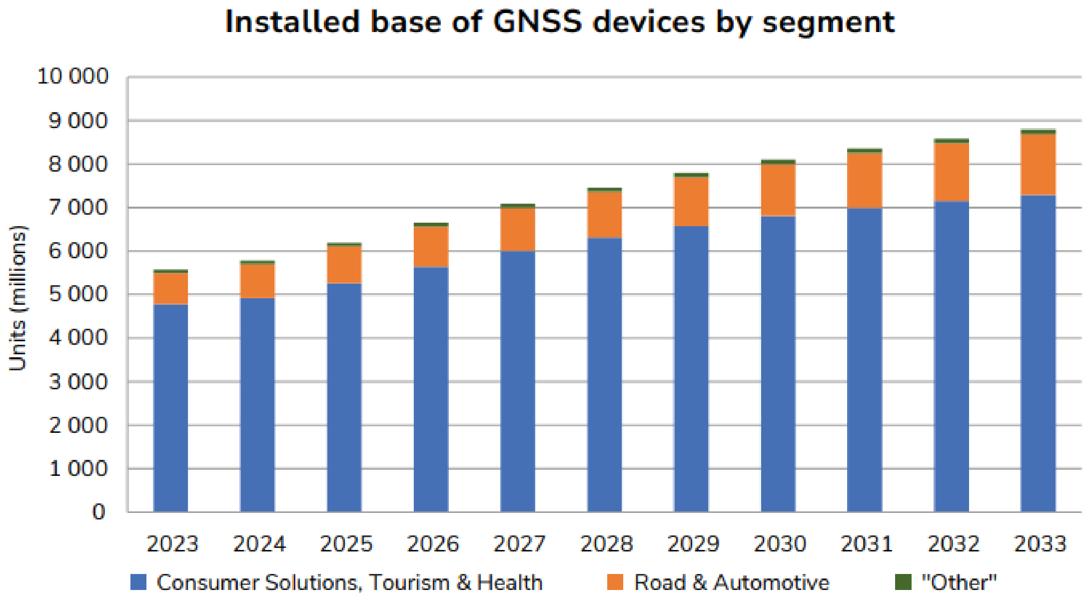
Tampere University
Tampere University of Applied Sciences

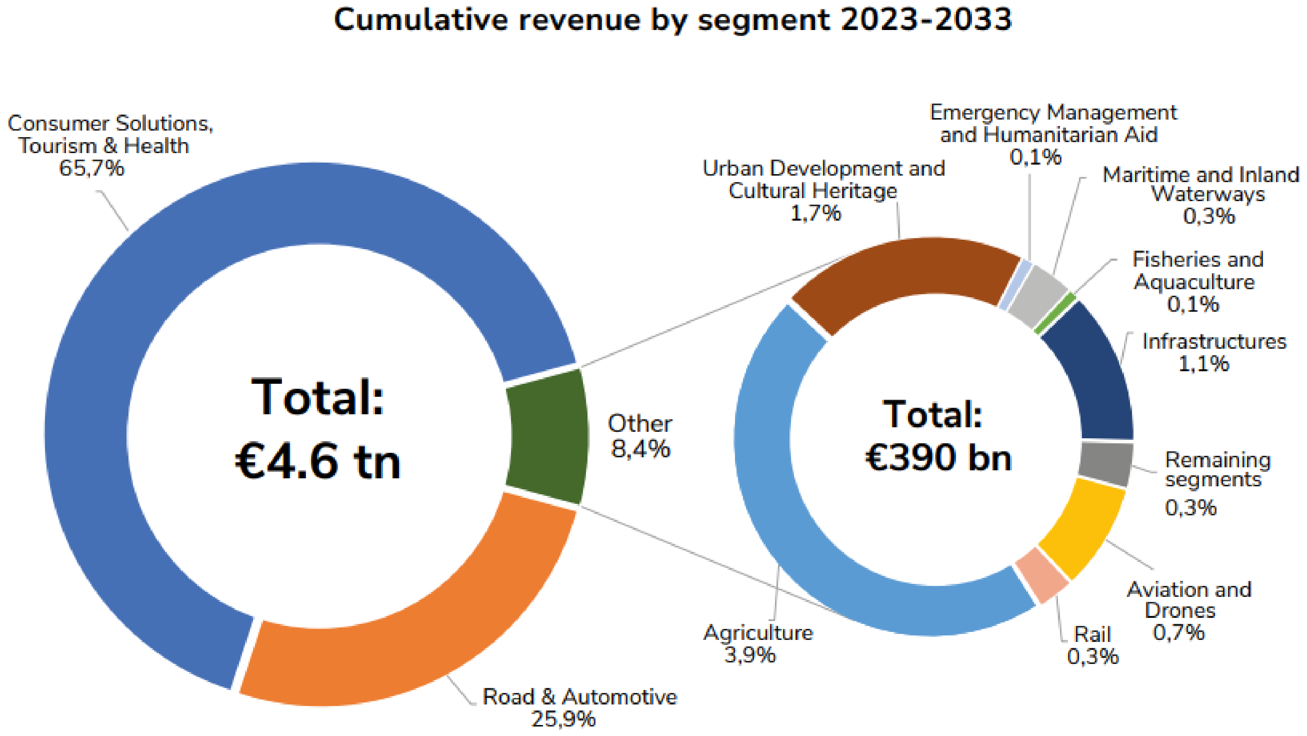
PNT economically

Satellite navigation related revenue is ever increasing

“Cumulative global GNSS downstream market revenues over the 2023 to 2033 period are expected to surpass €4.5 trillion”

“GNSS global revenues will rise from more than €260 billion in 2023 to around €580 billion in 2033”





* Remaining segments includes Space, Forestry, Insurance and Finance, Energy and Raw Materials

Source: European Commission
[EUSPA Market Report 2024]

How GNSS works (1)

- Multiple GNSS constellations exist (GPS, Galileo, GLONASS, BeiDou)
- Basic ranging principle: time-of-flight
- Satellites transmit open signals at very low power (~ −160 dBW at Earth's surface!)
  - by the time GNSS signals reach Earth, they are extremely faint, making them highly susceptible to RF interference
- GNSS receivers assume
  - signals are authentic
  - signals are unmodified
  - signals come from where they should in the sky

→ This is where cybersecurity intersects

- GNSS operates on trust: civilian GNSS signals have been unencrypted and unauthenticated, leaving them vulnerable to spoofing attacks

How GNSS works (2)

Velocity x Time = Distance

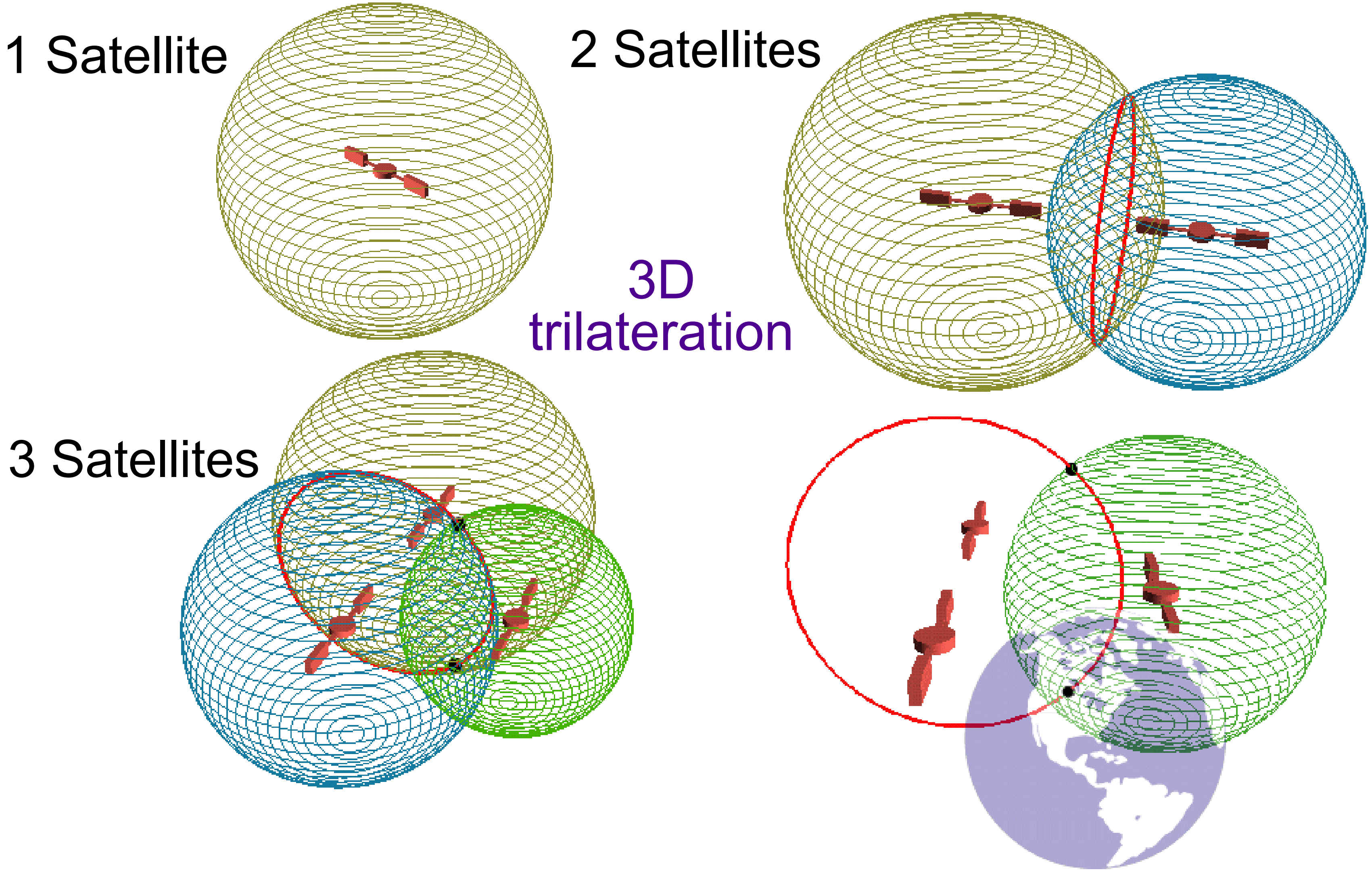
Radio waves travel at the speed of light 299 792 458 m/s (i.e., around $3*10^8$ m/s)

If it took, for example, 0.067 seconds to receive a signal transmitted by a satellite floating directly overhead, the travel distance of the received signal can be calculated using the above formula.

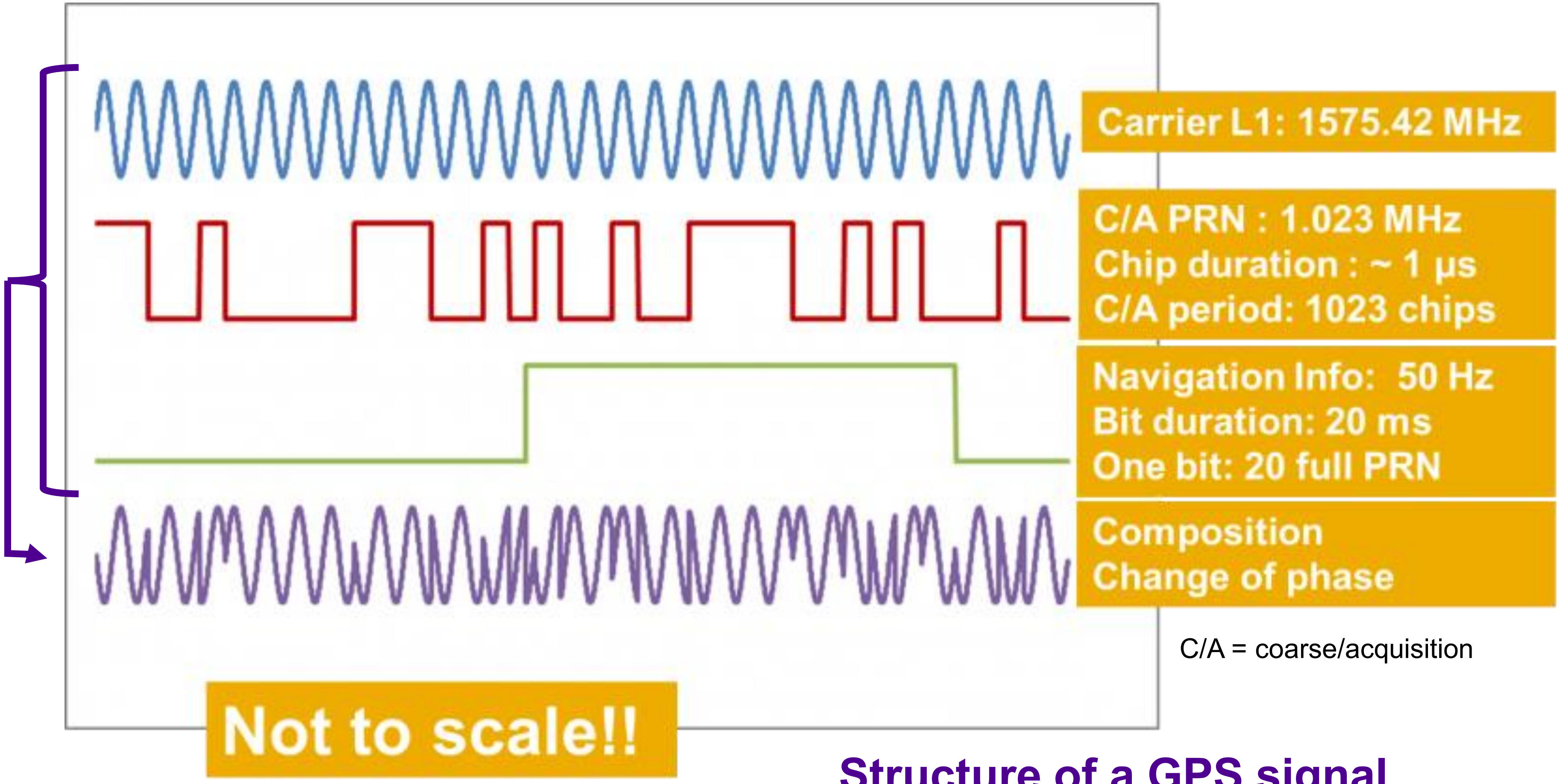
Travel distance: 299792458 m/s x 0.067 s = 20086094.69 m ~20086 km

Precise **position of the satellite** at the time of signal transmission and travel **time** must be resolved!

How GNSS works (3)



How GNSS works (4)

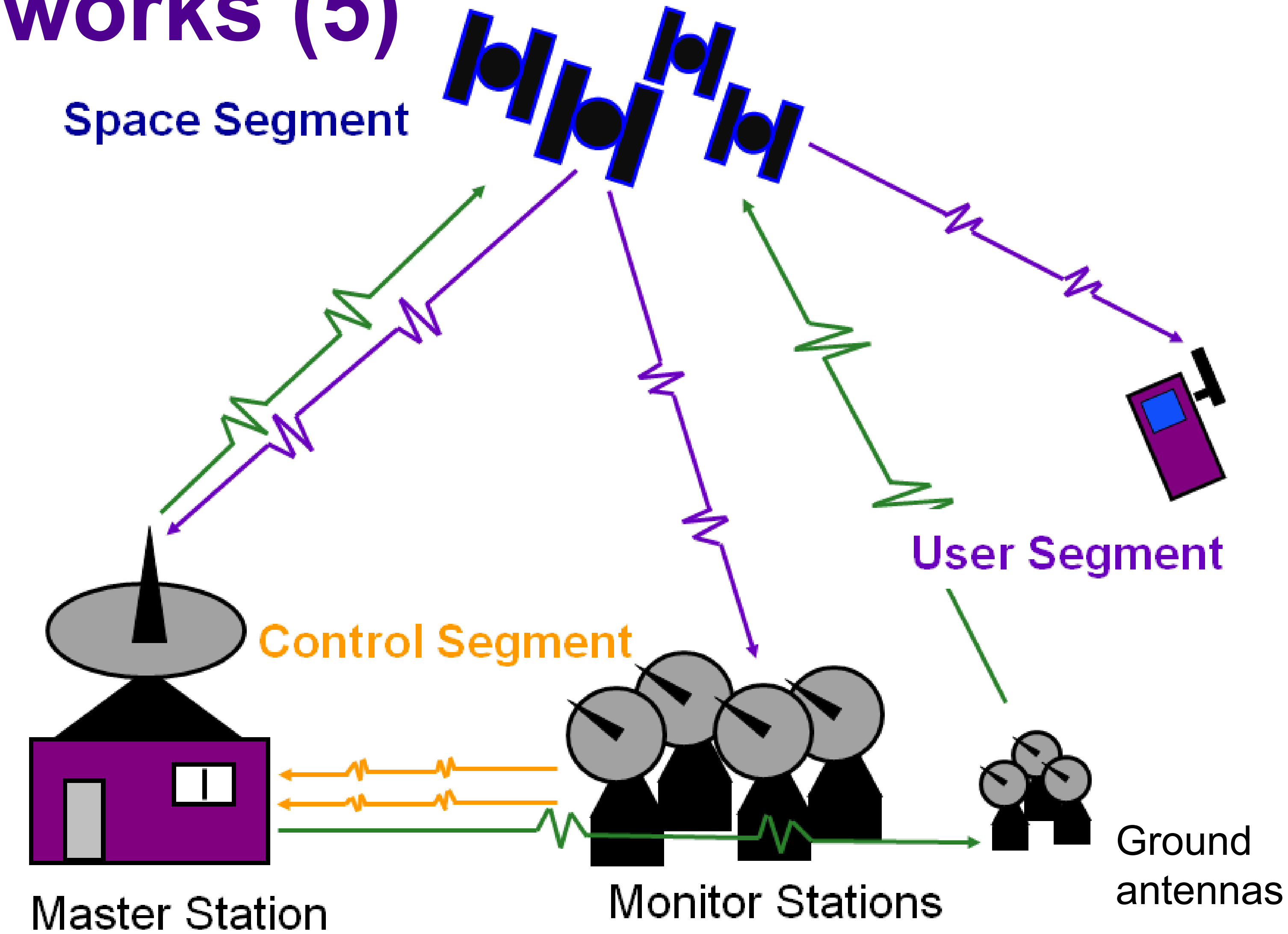


C/A = coarse/acquisition

Structure of a GPS signal

Source: European Space Agency, Navipedia

How GNSS works (5)



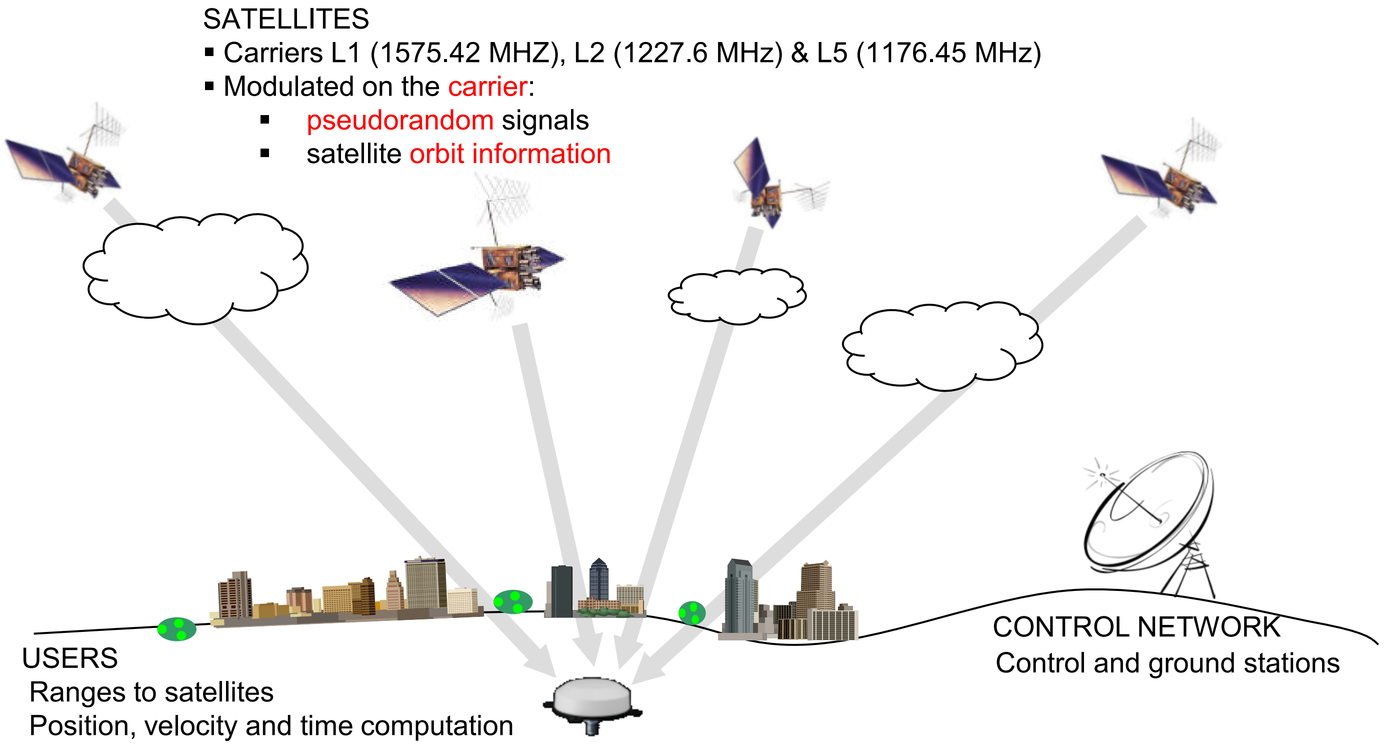
The three segments in a GNSS

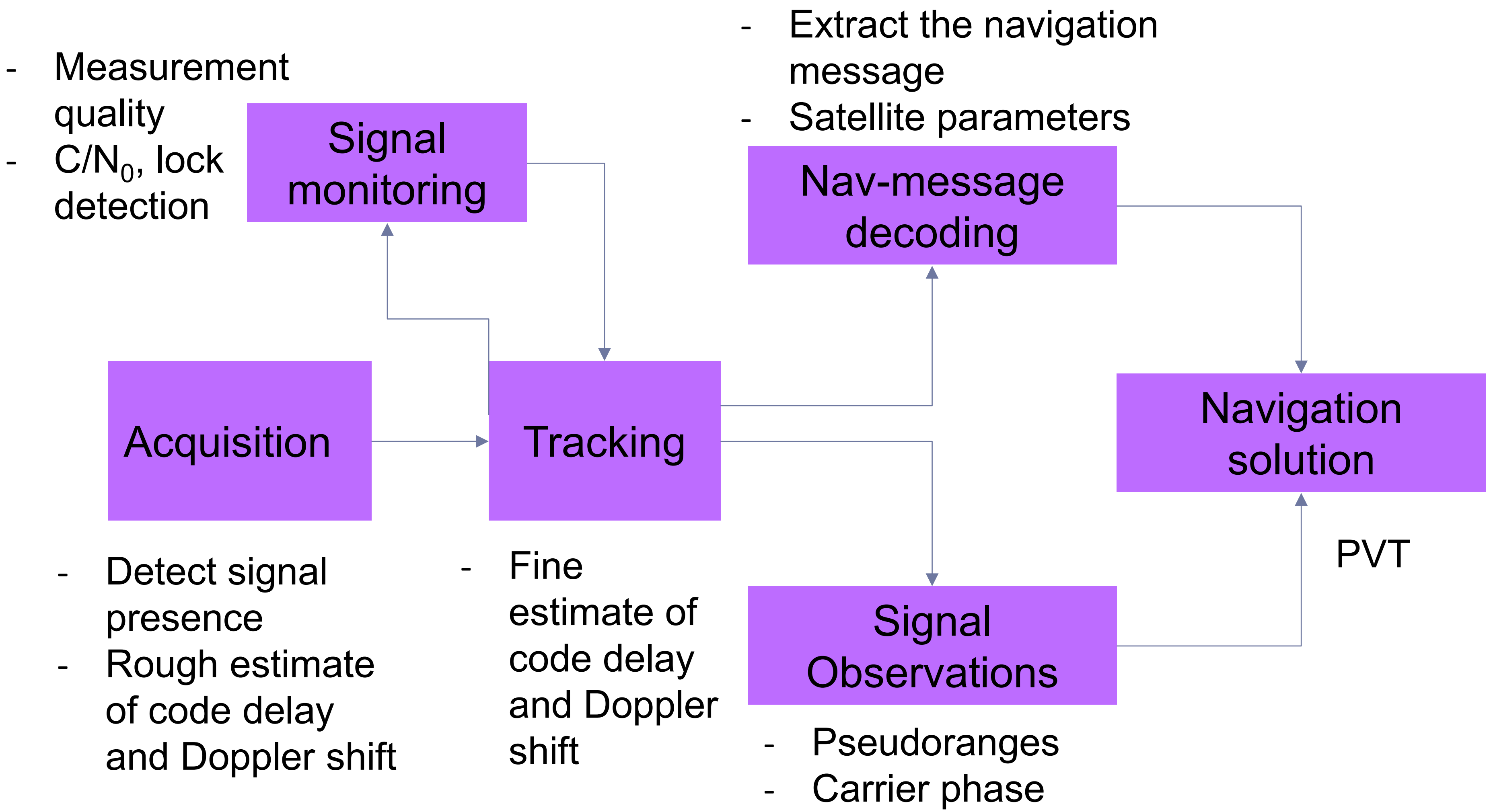
Tampere University
Tampere University of Applied Sciences

GPS as an GNSS example – basics

- Satellite navigation is based on radio signals transmitted by Earth-orbiting satellites and distance measurements between satellites and a user receiver
- A GPS receiver 1) measures the signal travel time from the satellite to the Earth, or 2) computes the number of full carrier cycles between a satellite and a receiver
  - → range measurements
- A receiver receives simultaneously information from multiple satellites through multiple channels
- When satellite locations are known, the user receiver location can be estimated based on the range measurements

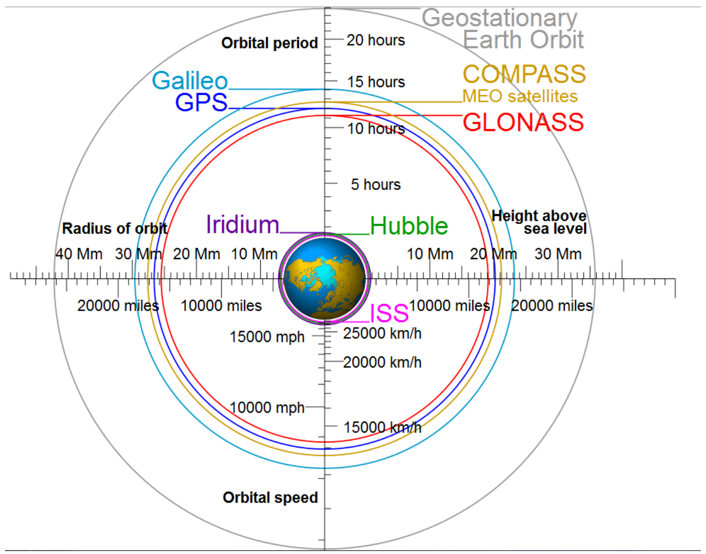
GPS:





GNSS signal processing stages in a receiver

GNSS requirements



- GNSS needs a common time system
  - Each GNSS satellite has atomic clocks
  - User receivers have their own time
- The signal transmission time has to be measurable
  - Each GNSS satellite transmits a unique digital signature, which consists of an apparent random sequence
  - A time reference is transmitted using the *Navigation Message*
- Each signal source has to be distinguishable
  - GNSS utilizes code division multiple access (CDMA) or frequency division multiple access (FDMA)
- The position of each signal source must be known
  - Each satellite sends its orbit data using the *Navigation Message*
  - Orbit data: Almanac and Ephemeris

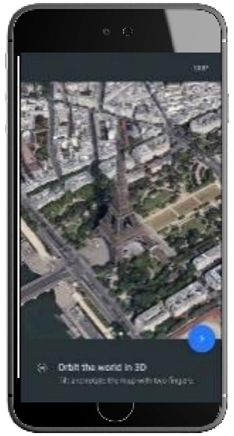
GNSS accuracy

Accuracies obtainable:

10 m	Navigation; code measurement; one receiver
1 m	DGNSS; code measurement + base station
0.1 m	carrier phase observations + base station
0.01 m	Static positioning; phase observations, network of base stations, post processing
0.001 m	Permanent stations; time series

Issues affecting GNSS accuracy:

- *Receiver technology used*
- *Location and environment of the antenna*
- *Weather conditions*



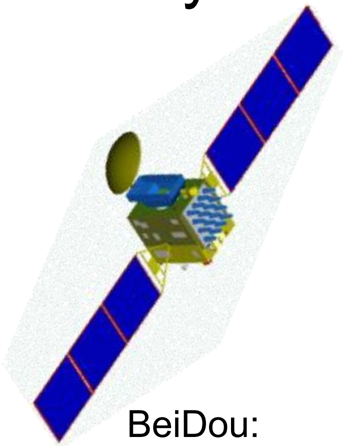
Multiple GNSSs

- The European **Galileo**, the Russian **Glonass,** and the Chinese **BeiDou** are similar systems with GPS
  - Glonass is however currently a FDMA system when GPS is and Galileo & BeiDou will be CDMA
    - Glonass has planned to be modernized to CDMA
- Also **GPS** has been modernized: new civil and military signals on L2 and L5

GPS
~31 SV
operational

Galileo
~29 SV operational

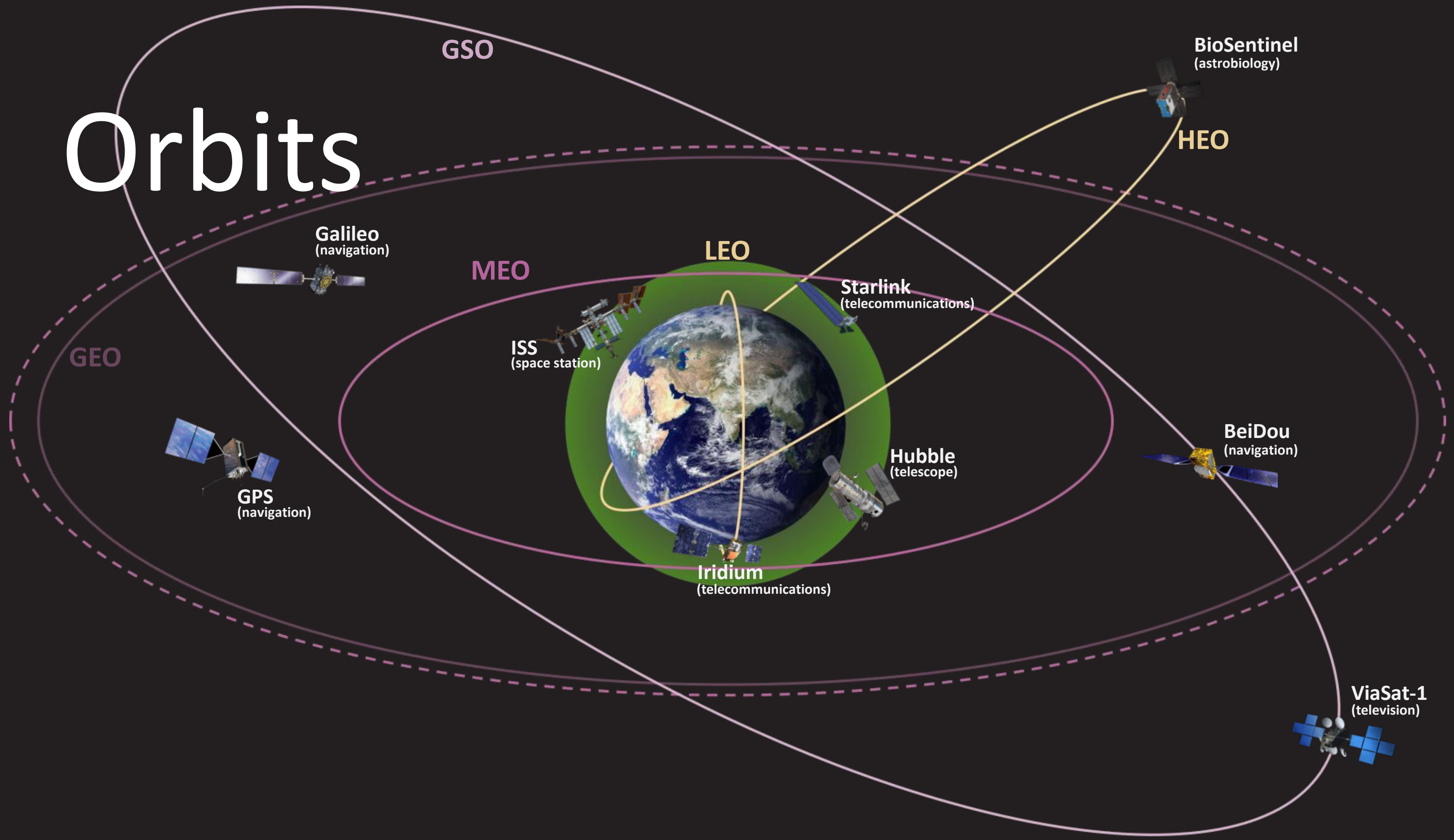
Glonass
~24 SV
operational



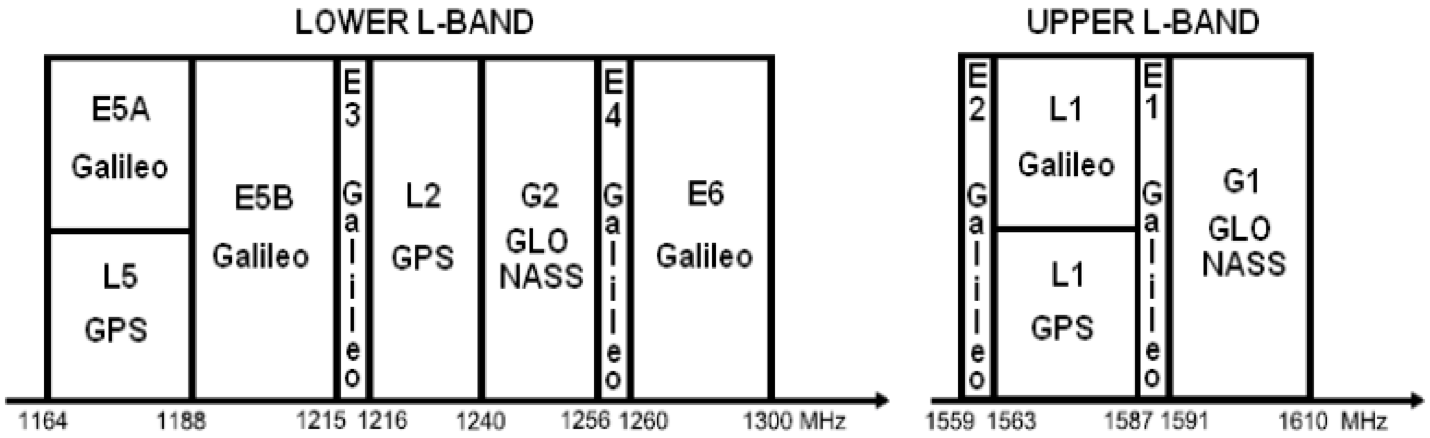
BeiDou:
~44 SV
operational

Tampere University
Tampere University of Applied Sciences

Orbits



GNSS frequency-wise (1)



	GPS	GLONASS	Galileo	Beidou	WAAS	QZSS	NAVIC	EGNOS	MSAS	GAGAN
Operational	31	23	20	27	2	3	5	2	2	2
Nominal	24 MEO	24 MEO	30 MEO	27 MEO & IGSO, 5 GEO	3 GEO	4 HEO	7 GEO	3 GEO	2 GEO	1-3 GEO
In full operation	1995-	2011	2020	2020	2008	2014-2017	2015 -	2009	2007	2014 -

Currently augmenting GPS

Tampere University
Tampere University of Applied Sciences

GNSS frequency-wise (2)

F r e q u e n c i e s

GPS

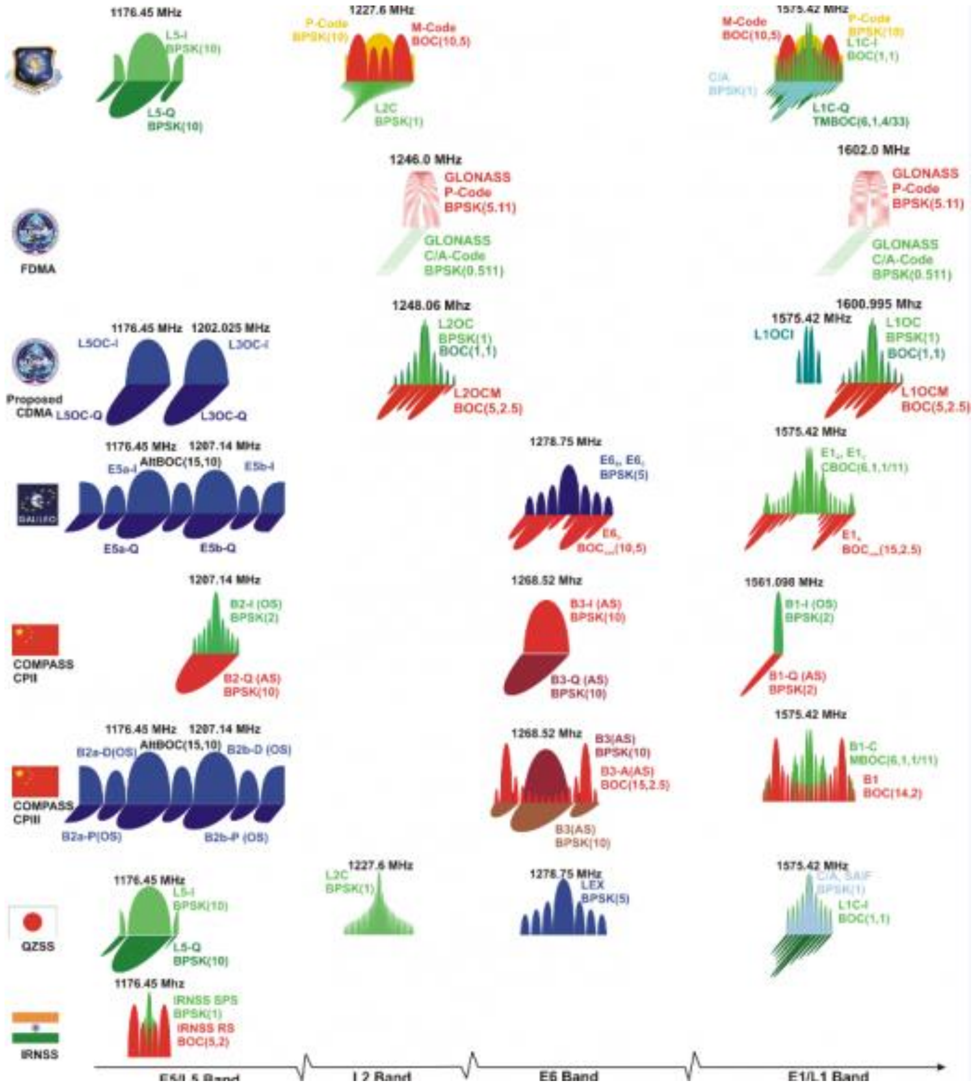
GLONASS

Galileo

BeiDou

Japanese QZSS

Indian NAVIC/ IRNSS

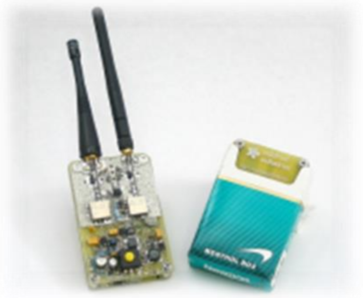


E5/L5 band L2 band E6 band E1/L1 band

Source: Stefan Wallner, ESA

Tampere University
Tampere University of Applied Sciences

GNSS shortcomings



S. Pullen, G. Gao, "GNSS Jamming in the Name of Privacy", Inside GNSS, March/April 2012, 34-43.

- Signal's susceptibility to unintentional or malicious radio frequency interference (RFI) or jamming
- GNSS signals are typically too weak to be observable indoors
  - GNSS signals need to be augmented with external sensors to function accurately indoors
- Signal cannot provide an orientation solution easily, a feature that is indispensable in many vehicle navigation and guidance applications
  - GNSS and integrated navigation:
    - Inertial navigation systems (INSs) have been integrated with GNSSs with considerable success. This fusion between GNSSs and INSs is complementary: INS helps mitigate the shortcoming of the GNSS and vice versa. Other sensors are also commonly integrated with GNSS (e.g. other radio frequency (RF) signals, magnetometer, LIDAR, barometer)

Vulnerabilities & threat models related to GNSS (1)

Layer	Threat type	Example
RF / Physical layer	**Jamming**	Intentional, unintentional, EW
Signal structure layer	**Spoofing**, **meaconing**	Takeover attacks
Navigation solution layer	**Fault injection**	Differential/RTK correction manipulation
System layer	**Ephemeris manipulation, signal authentication bypass**	State-level threat

Vulnerabilities … els related to GNSS (2)

1 kW wideband jammer can deny service to the best COTS GNSS receivers over a ~200 km (line-of-sight) effective range

Intentional

- Jamming: transmission of a disruptive signal

- Spoofing: transmission of false GNSS signals to deceive a GNSS receiver
- Meaconing: re-transmitting genuine satellite signals with a short delay to create errors in the GNSS receiver
- Software attacks: targeting base stations or assistance data

Unintentional

- Severe space weather: ionospheric storms can cause GNSS errors

- Signal multipath reflections: no direct signal path from the satellite to the receiver's antenna
- Orbital data and clock errors
- Unintentional narrowband and wideband radio interference

Tampere University
Tampere University of Applied Sciences

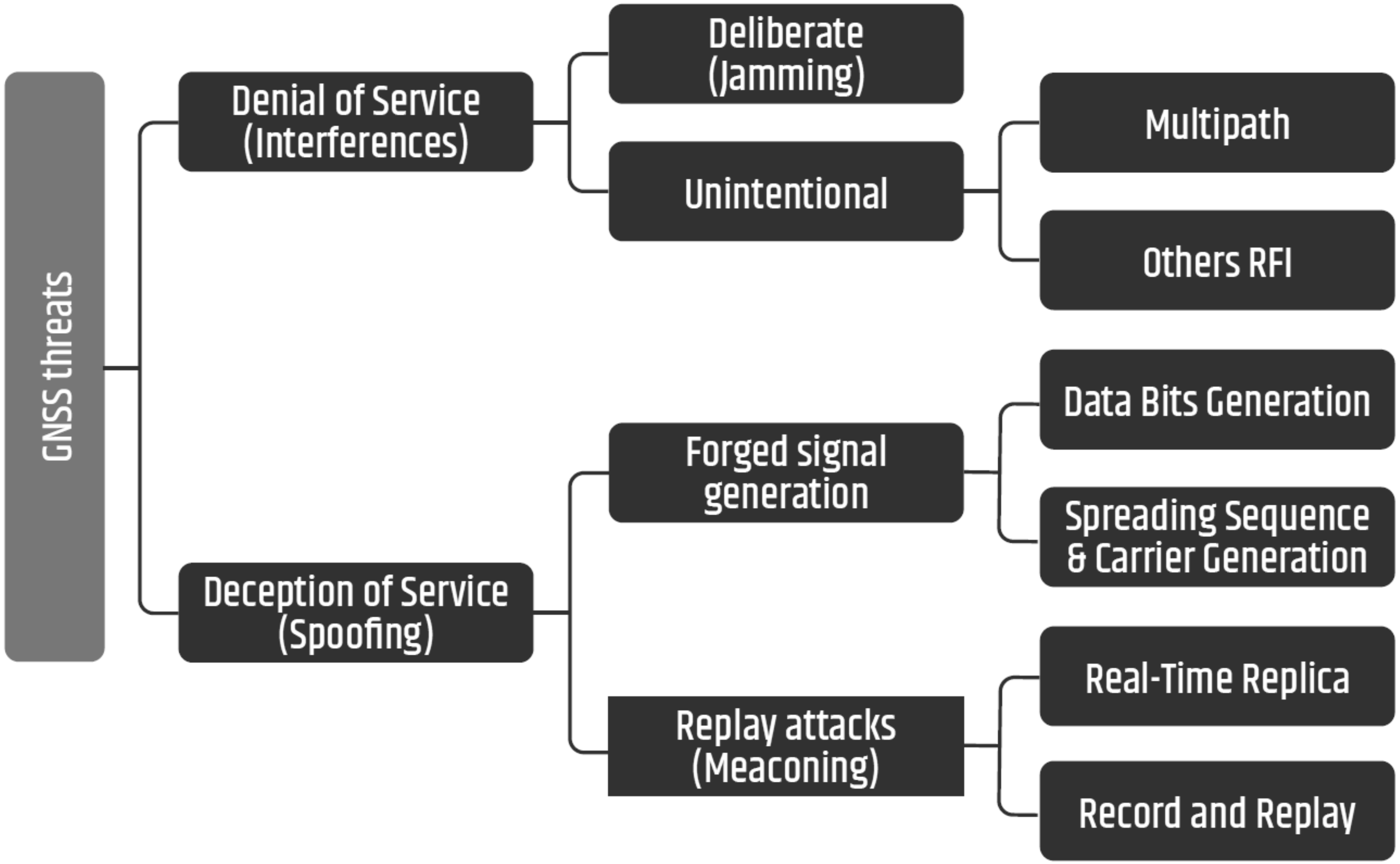
GNSS interferences (1)

Interferences							
Man-made					***Channel-based***		
Intentional			***Unintentional***		***Space weather***	***Multipath***	***Other***
Jamming	*Spoofing*	*Meaco-ning*	*Adjacent channel*	*Co-channel*	*atmospheric scintillation*	*line-of-sight + multipath* *non-line-of-sight only*	*fading* *shadowing* *doppler effects* *scattering*
single band *multiband*	*simplistic* *intermediate* *sophisticated*	*GNSS repeaters*	*intermodulation products*	*radio resource allocation* *crosstalk*			

- Disruption of critical systems
- Potential safety and security risks

Source: GNSS User Technology Report, EUSPA, European Commission, 2020

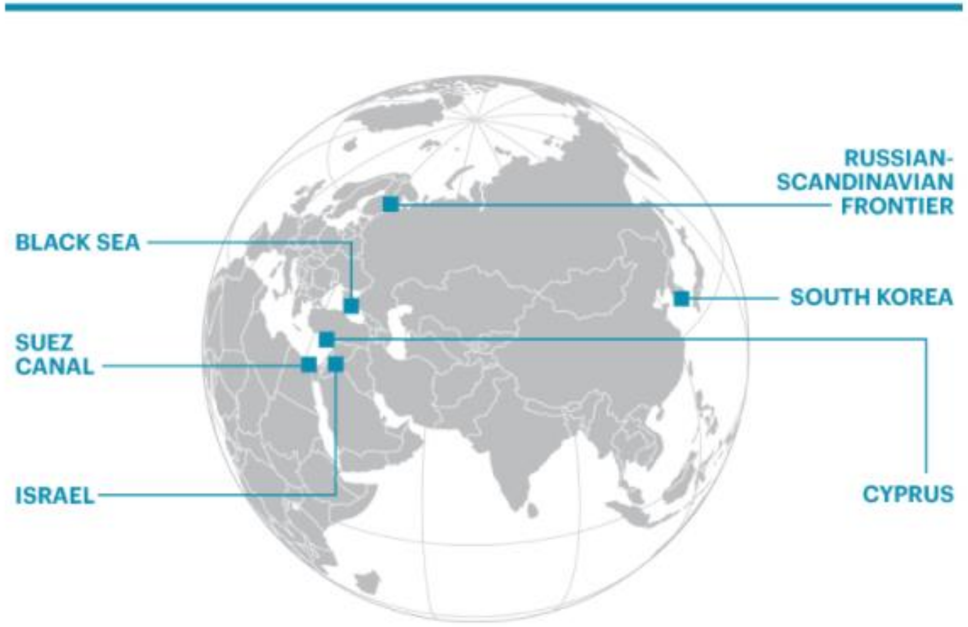
GNSS interferences (2)



RFI = radio frequency interference

Real-world incidents

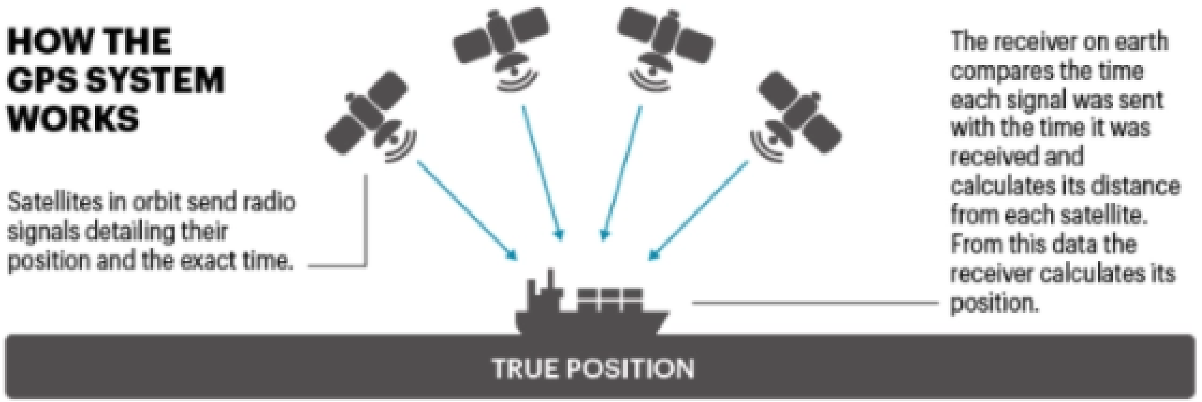
- GNSS interference is no longer theoretical – despite illegal, it is operational, frequent and sometimes even strategic

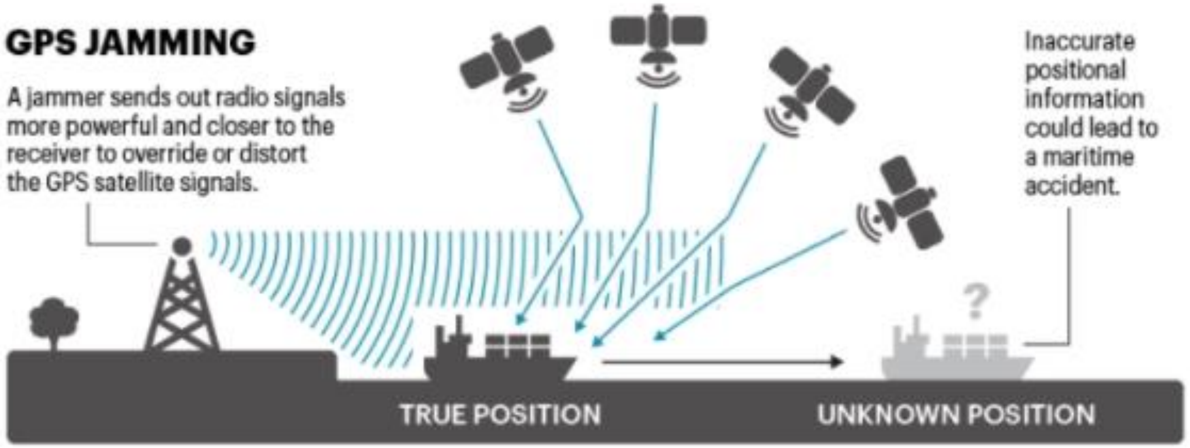


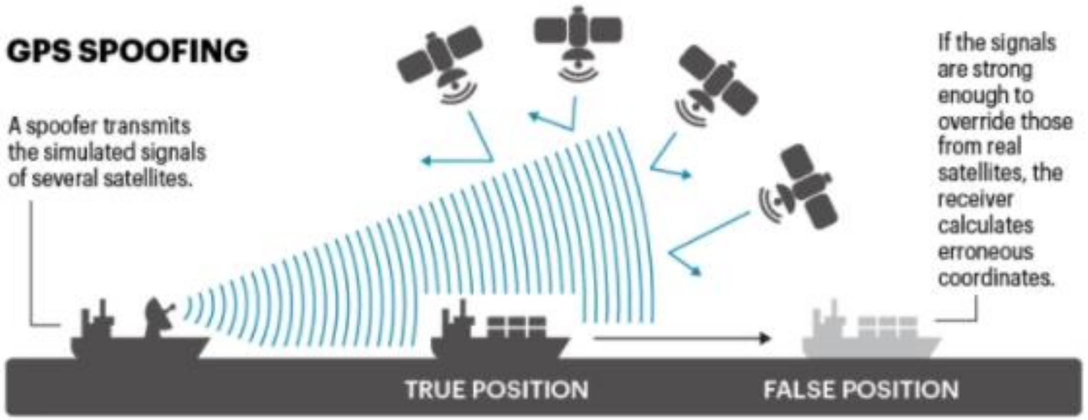
K. Dunn, “Mysterious GPS outages are wracking the shipping industry - For the global maritime shipping industry, spotty satellite navigation is a disaster waiting to happen”, FORTUNE magazine, January 22, 2020

How Sinister Signals Stop Ships

The global positioning system, a network of satellites maintained by the U.S. Air Force, is widely seen as both reliable and nearly impregnable. But even the strongest satellite signals grow weaker as they get closer to earth's surface, and that creates opportunities for mischief. Here's how military forces, spies, and even criminal networks can interfere with GPS and other navigation systems.





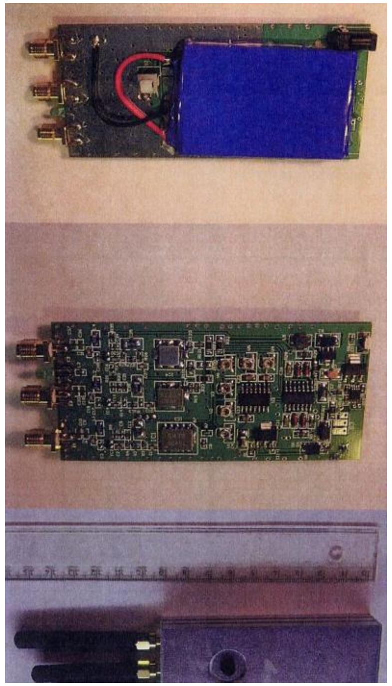


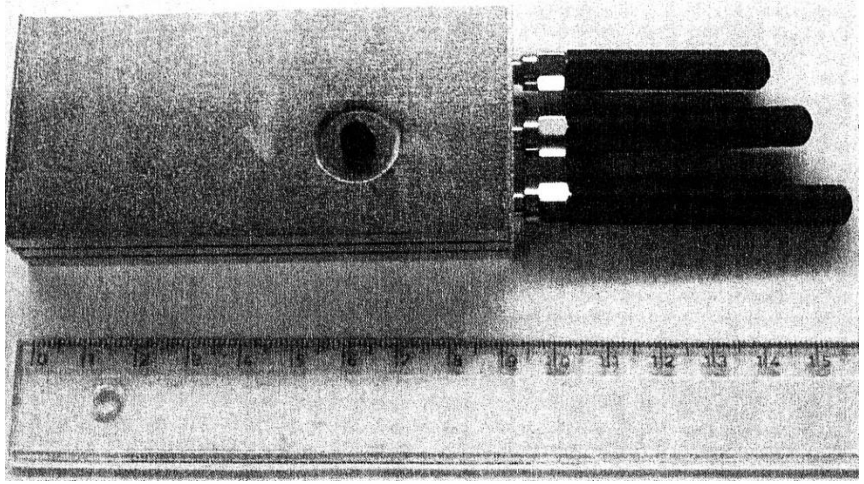
K. Dunn, "Mysterious GPS outages are wracking the shipping industry - For the global maritime shipping industry, spotty satellite navigation is a disaster waiting to happen", FORTUNE magazine, January 22, 2020

GNSS vulnerability examples (1)

Newark Airport in 2009 –
daily GPS signal disruptions
GPS jamming: No jam tomorrow",
The Economist, 2011

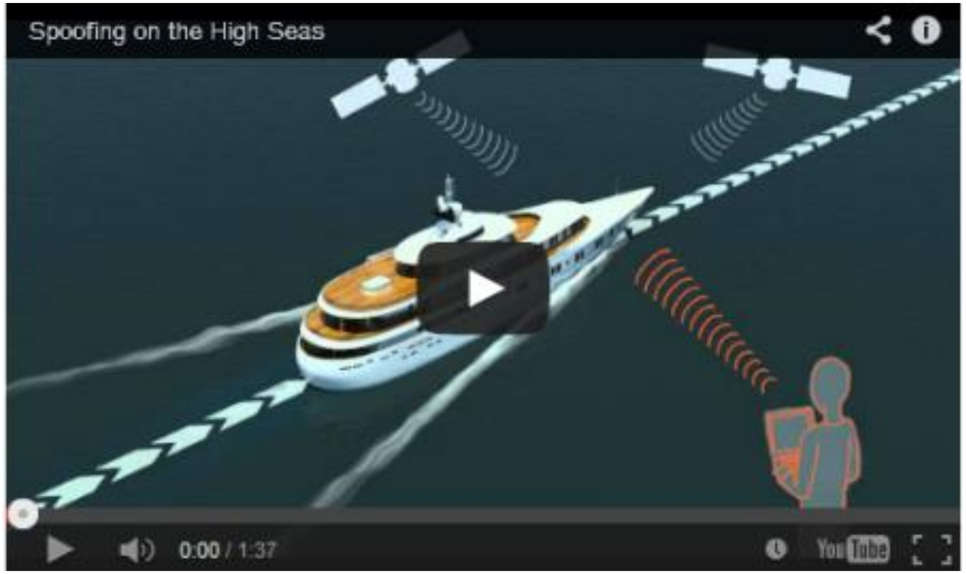
"Moottoripyöräjengiltä löytynyt outo laite ihmetytti poliisia."
MTV Uutiset, Lokakuu 2011





GNSS vulnerability examples (2)

University of Texas at Austin spoofed a luxurious private yacht to showcase the threat, KVH Mobile World, 2014




KYBERASEET | Miina Rautiainen 11.8.2017 klo 11:04

Outoja GPS-ongelmia Mustallamerellä: laivan sijainti heitti yli 30 km sisämaahan - testasiko Venäjä uudenlaista asetta?

JAA ARTIKKELI

Satelliittinavigoinnin ongelmat Mustallamerellä saattavat johtua Venäjän uuden GPS-häirintäjärjestelmän kokeiluista, kirjoittaa New Scientist. Tämä voisi lehden mukaan olla ensimmäinen vihje uudenlaisesta sähköisestä aseesta, johon kaikilla on pääsy ilkeistä valtioista pikkurikollisiin.

Kesäkuun 22. päivä Yhdysvaltojen merenkulkulaitos julkaisi tapausraportin. Venäläisen Novorossiysk-sataman edustalla olleen aluksen kapteeni oli huomannut GPS-laitteensa sijoittavan hänet väärään paikkaan, yli 52 kilometriä sisämaahan Gelendzhikin lentokentälle.

Tampere University
Tampere University of Applied Sciences

GNSS vulnerability examples (3)

2018-12-17
POSTET AV LIVE
OFTEDAHL

GPS-jamming: 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 v
kritisk syke pasienten, skriver Bergens Tidende.

Illustrasjonsfoto: Live Oftedahl

Tredje oktober i år rykket luftambulansen ut på et akutt oppdrag. Etter kun tre minutter var redningsmannskapet i luften på vei til en kritisk syk pasient.

Helikopteret fløy sørover, over E39 på Vellaheiene. Piloten fulgte ruten som var plottet inn på et di
avanserte GPS-systemene viste dem hvor de var hele veien.

Akuttsentralen fulgte helikopterets ferd på sine skjermer. Slik kunne sentralen gi viktige beskjeder
ankom skadestedet.

Plutselig forsvant helikopteret fra kartet. GPS-signalet var borte.

GPS-häirintä ulottui Lappiin Naton sotaharjoituksen aikana – häirinnästä on epäilty Venäjää

Norjan viranomaisten mukaan vastaavaa häirintää on tullut Venäjältä. Suomen viranomaiset vaikenevat lähteestä.

Lentoliikenne 9.11.2018 klo 06.00 | päivitetty 13.11.2018 klo 12.19

Kuva: Jonathan Nackstrand / AFP

Nyheter

Okända gps-störningar drabbar svenska flyg

PUBLICERAD 2019-02-05

ska och norska plan har drabbats av att deras gps-system slagits ut. Foto: Gorm Kallestad/NTB Scanpix

De okända störningssignaler som misstänks ha slagit ut gps-system på flygplan i norskt luftrum de senaste månaderna har observerats även ovanför Sverige,

2018

GNSS vulnerability examples (4)

Nettavisen Nyheter. Nyheter Økonomi Sport Livsstil Norsk debatt Meny

Ukraina

Flere europeiske rutefly rammet av GPS-forstyrrelser

BEKREFTER: Flyselskapet Finnair bekrefter overfor Nettavisen at flyene deres er blitt rammet av GPS-forstyrrelser de siste dagene. Foto: Jonathan Nackstrand (AFP)

Finnair opplyser at GPS-en har vært ubrukelig. - Kan være knyttet til russisk elektronisk krigføring, sier ekspert på russisk sikkerhetspolitikk.

Del

10.03.22 15:08 10.03.22 15:36

DAGENS NYHETER. E-DN ARKIVET KORSORD KUNDSERVICE SNILLE KUNDERBJUDANDEN

Nyheter Sverige Världen Ekonomi Kultur Sport Klimatet Ledare DN Debatt Meny

VÄRLDEN

Gps-störningarna runt Finland blir allt fler

PUBLICERAD 2022-03-10

Piloter från Finnair har rapporterat hur deras gps-system påverkats. Foto: Finnair/TT

Finland har under flera dagar drabbats av störningar i gps-nätet. Från att först ha upptäckts vid landets östra gräns hade de på torsdagen också

yle Uutiset Areena Urheilu Valikko

Uutiset Tuoreimmat Venäjän hyökkäys Sää Kotimaa Ulkomaat Talous

Lentoliikenne

Lentokerhon vetäjä arvelee, että gps-signaalia Suomessa häiritään tahallaan – "Vaarallista touhua, jos signaali katkeaa huonoissa olosuhteissa"

Alkuviikosta liikenne- ja viestintävirasto Traficom varoitti lentoliikennettä siitä, kuinka Suomen itärajalla on havaittu paikannuksessa häiriöitä. Traficom on kertonut selvittävänsä syitä häiriöiden taustalla. Savonlinnan Lentokerhon puheenjohtaja uskoo, että häiriöt on aiheutettu tahallisesti.

Savonlinnan Lentokerhon omistaman Cessna 172N Skyhawkin ohjaamon mittaristo kertoo GPS-signaalin häiriöistä. Kuva: Kati Rantala / Yle

KATI RANTALA, JUHO LIUKKONEN

10.3. 12:57

2022

Tampere University
Tampere University of Applied Sciences

Recent GNSS vulnerability examples

Liikenne

Kaksi Finnairin konetta joutui palaamaan Virosta takaisin Suomeen GPS-häirinnän takia

GPS-häirintä on yleistä, mutta useimmiten se ei aiheuta lentojen kääntymistä takaisin, kertoo Finnairin viestintäjohtaja.

Tarton lentokenttä on erityisen altis GPS-häirinnälle, sillä siellä lähestyminen vaatii GPS-signaalia. Arkistokuva. Kuva: Sami Jumppanen / Korpipaja

LAURA KANGAS
27.4. 9:15 · Päivitetty 27.4. 10:05

Maatalous

Traktorit sekosivat itärajalla – piirtävät nyt peltoon vihreitä raitoja

Viljely itärajalla on ongelmissa, koska traktorit eivät saa oikeaa paikkatietoa GPS-paikannusjärjestelmästä. Häirintä tulee ilmeisesti Venäjältä.

Kari Pekosen pellolle jää vihreitä raitoja satelliittipaikannuksen ongelmien vuoksi.

KALLE SCHÖNBERG
7.6. 8:51 · Päivitetty 7.6. 10:14

Ett flygplan över Kristianstad anmälde störningar i GPS-systemet. Foto: Janerik Henriksson/TT

SATELLIT

Nya GPS-störningar i sydöstra Sverige

0:39 min Dela

Publicerat lördag 13 januari kl 12.39

- Störningar i GPS-systemet fortsätter och så sent som i onsdags så upplevde ett flygplan störningar som rapporterades till Transportstyrelsen, det rapporterar SVT.
- Flygplanet flög över Kristianstadstrakten och de tidigare störningarna har också märkts i södra Sverige och sydöstra Östersjön, framför allt nattetid.

Andrea Jilder
andrea.jilder@sverigesradio.se
P4 Blekinge

Nyheter

Långvariga GPS-störningar över Gotland

TT
Publicerad 2025-01-17
Mejla Dela Spara

Flygtrafik och sjöfarten påverkas av GPS-störningarna som har återkommit över Östersjön under lång tid. Arkivbild.
Foto: Jonas Ekströmer/TT

Gotland och delar av Öland har i minst 60 dagar i rad omfattats av stundtals kraftiga GPS-störningar som påverkar fartyg och flygtrafik, skriver Expressen.

Suomessa "ennennäkemättömiä" gps-häiriöitä – tänne ne keskittyivät

Häiriöiden määrä on kasvanut Suomessa kahden viime vuoden aikana.

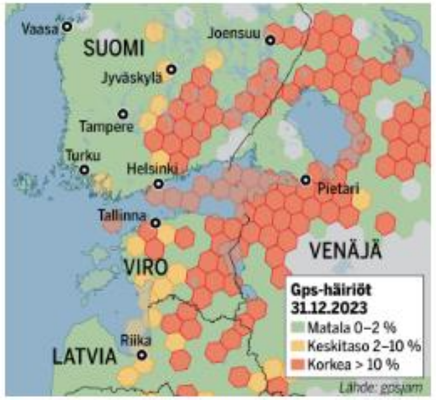
JAA TALLENNA

STT-IS
2.1. 14:48

SATELLIITTIPAIKANNUSJÄRJESTELMÄ gps:ssä esiintyi sunnuntaina häiriöitä Itä- ja Kaakkois-Suomessa, Liikenne- ja viestintävirasto Traficomista kerrotaan.

Häiriöt tulivat aiemmin ilmi avointen lähteiden gps-dataa keräävältä GPSjam-sivustolta. Samaisen sivuston mukaan häiriöitä ilmeni muun muassa Savon ja Pohjois-Karjalan seuduilla maanantaina.

Tiedot häiriöistä perustuvat lentokoneiden tekemiin ilmoituksiin, joita tuli sunnuntaina kohtalaisen laajalta alueelta, ilmailusta vastaava johtaja Jari Pöntinen Traficomista kertoo.



Pöntisen mukaan häiriöt eivät vaikuttaneet lentoturvallisuuteen, koska koneilla on käytössään vaihtoehtoisia navigointijärjestelmiä. Pöntinen ei halunnut ottaa kantaa häiriöiden syihin.

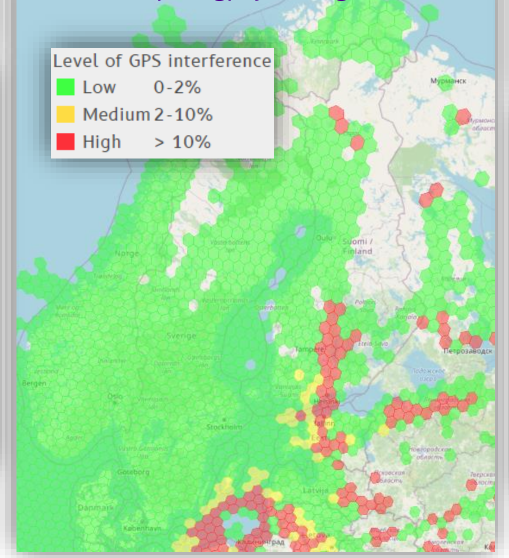
GPS-jamming er den nye hverdagen over Finnmark

Frekvensforstyrrelser skjernærmest daglig i Finnmark. Politimesteren sier situasjonen er alvorlig.

10.000 fot i lufta over Øst-Finnmark måler norske myndigheter frekvensforstyrrelser fra Russland.
FOTO: SEBASTIAN FAUGSTAD / NRK

Sebastian Faugstad
Journalist

Source: https://gpsjam.org, 1.1.2025



Kraftig økning av GPS-jamming over Finnmark

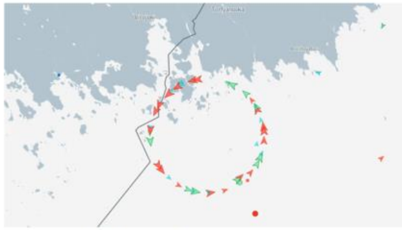
Russisk GPS-jamming har rammet Øst-Finnmark nesten hver dag hittil i år. Nå settes det opp målere som skal kartlegge omfanget.

Jamming fra Russland merkes høyt oppe i luftrommet over Nordkalotten. Fly må derfor navigere på andre måter når GPS-signalene blir borte.

Merenkulku

Venäjän varjolaivaston outo ympyräleikki lähellä Suomen merirajaa hämmentää

Meriliikennekartoilla näyttää siltä, kuin alukset tanssisivat letkajenkkaa Suomen merirajan tuntumassa. Oikeasti aluksia ei paikalla ole.



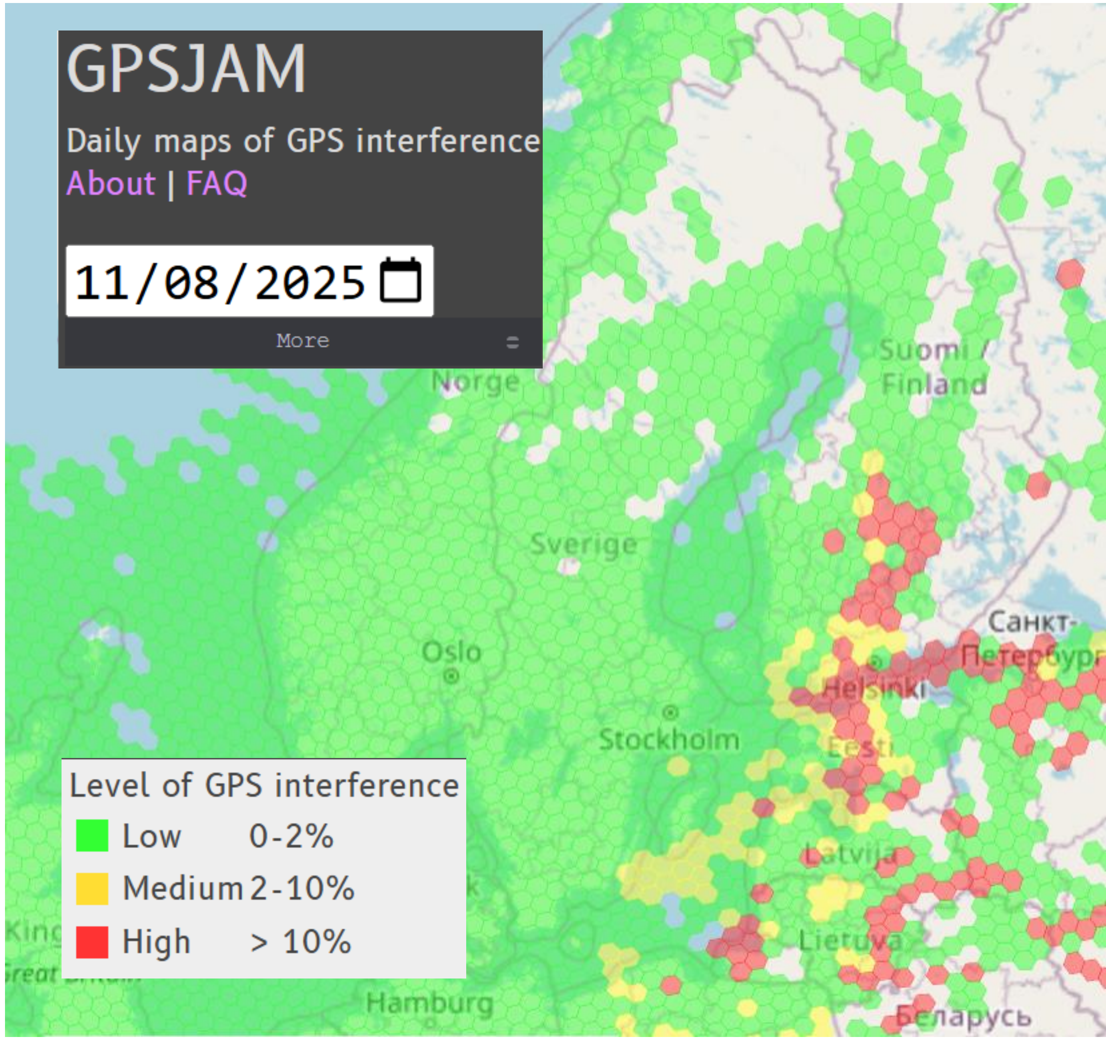
Kuvakaappaus MarineTrafficin sivustolta tiistaiaamuna 20.5.2025. Kuvassa näkyy Venäjän varjolaivaston muodostama ympyrä Suomenlahdella. Kuva: Kuvakaappaus MarineTraffic-sivustolta

2023-2025

Interference monitoring (1)

https://gpsjam.org/

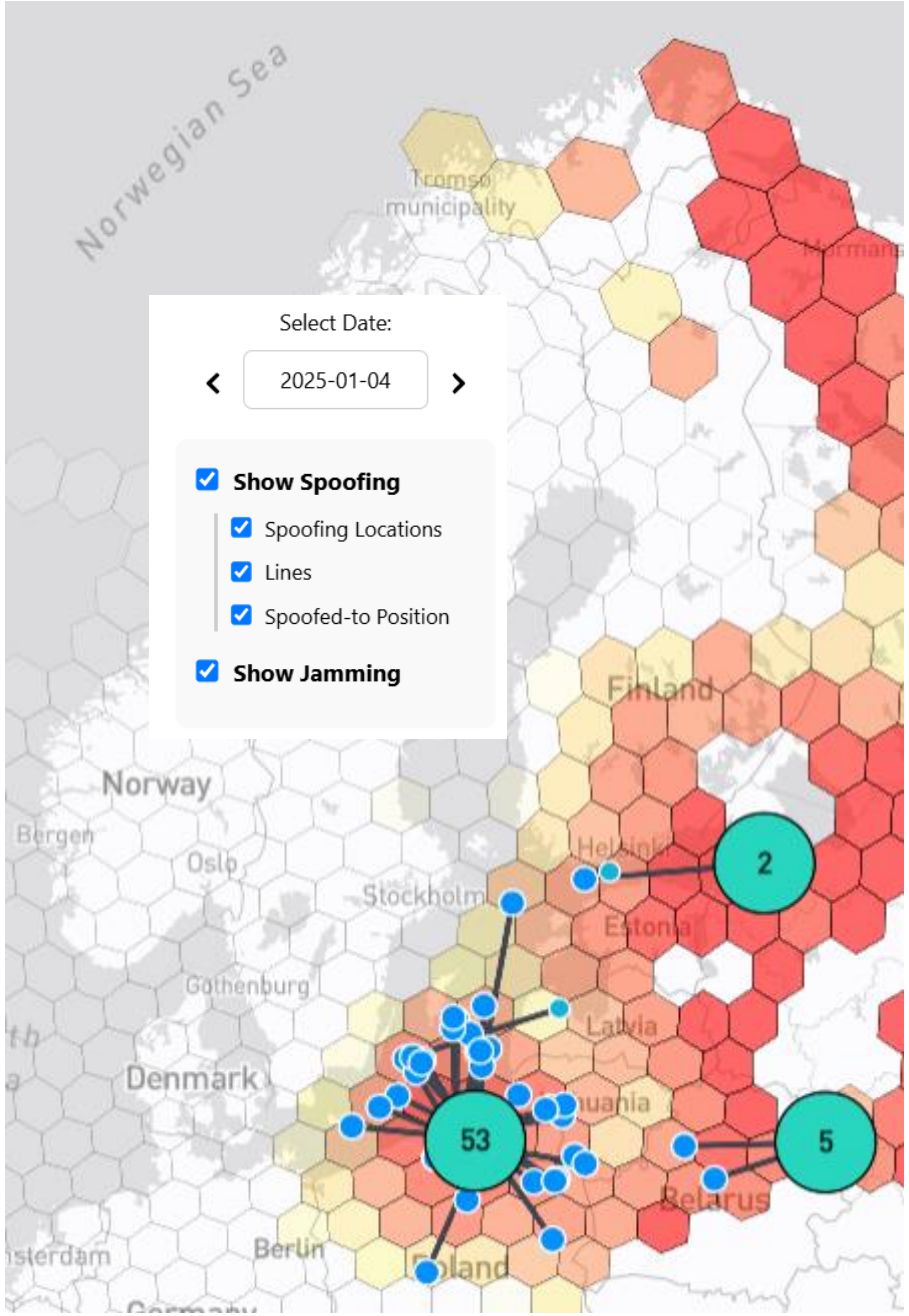
- gpsjam.org aggregates ADS-B aircraft data to infer GNSS signal disruption affecting aviation navigation systems
- Uses C/N_0 degradation patterns reported by aircraft avionics to detect areas where jamming is ongoing
- Provides near real-time heatmaps of interference globally, updated continuously
- Shows persistent GNSS denial zones in regions of geopolitical tension, conflict operations, or military training exercises
- Civil aviation is already navigating in contested PNT environments



https://spoofing.skai-data-services.com/

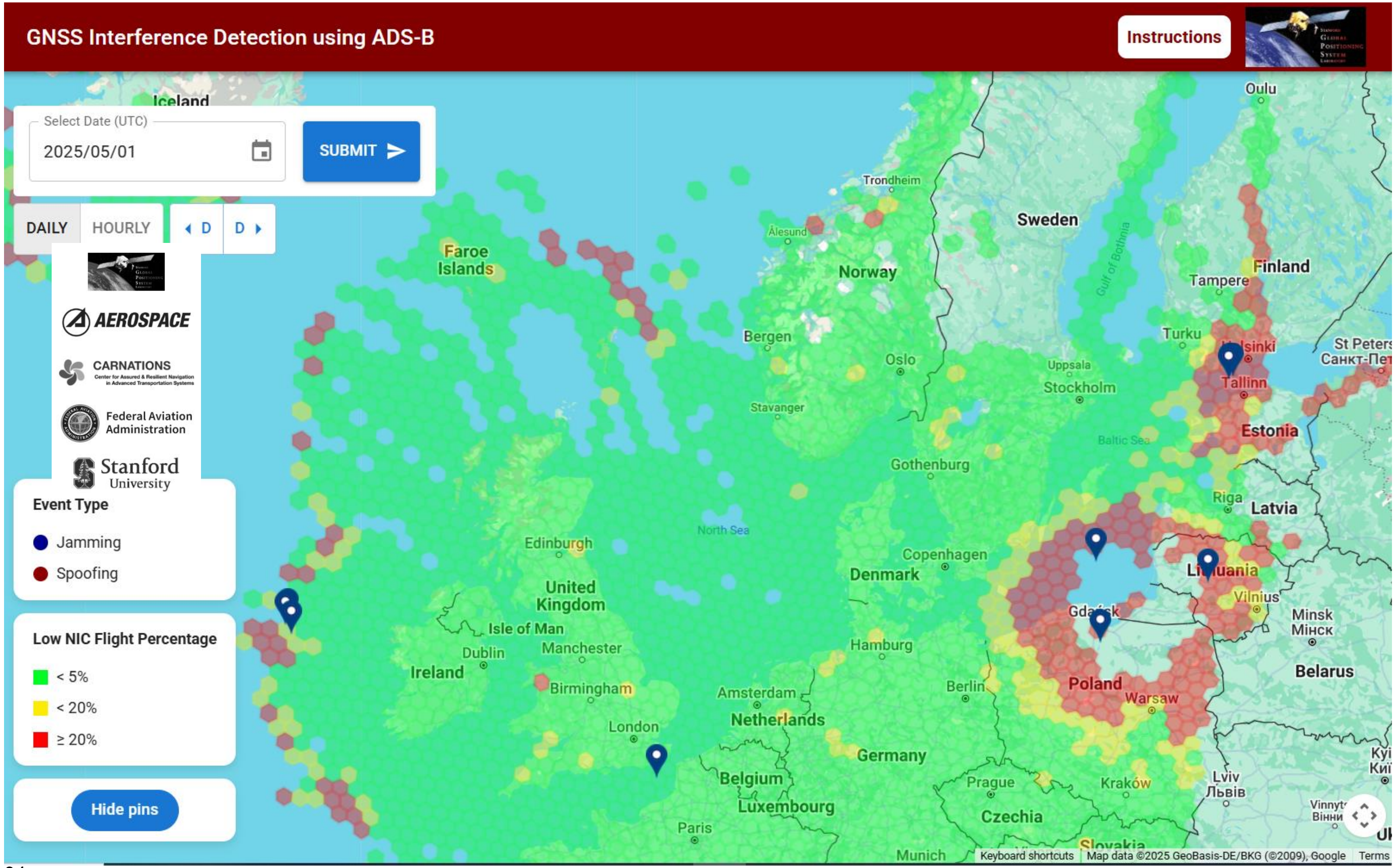
Interference monitoring (2)

- Real-time GPS interference mapping service by SkAI Data Services and Zurich University of Applied Sciences
  - ADS-B detected GNSS spoofing (blue dots) and jamming (coloured hexagons) from commercial aircraft (Jan 4, 2025)
- The map displays clusters that indicate areas where spoofed (or "fake") GPS positions of aircraft have been detected
  - the numbers within each cluster show how many flights were spoofed at that specific location
- The markers in blue markers represent the positions of aircraft just before they were spoofed
  - The lines connect these real positions to their corresponding spoofed (fake) locations
- Areas of potential GPS jamming or radio frequency interference indicated by colored hexagons



Interference monitoring (3)

Similar tool has also been developed by the Stanford University GPS Lab



rfi.stanford.edu

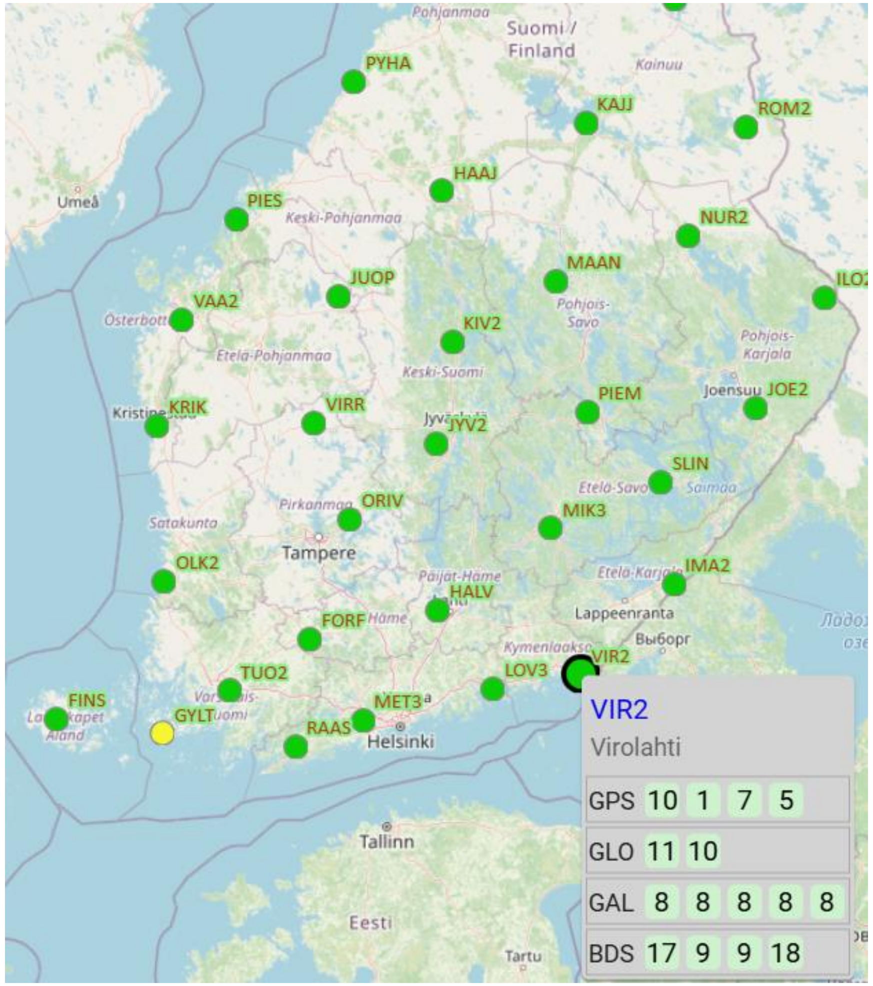
Tampere University
Tampere University of Applied Sciences

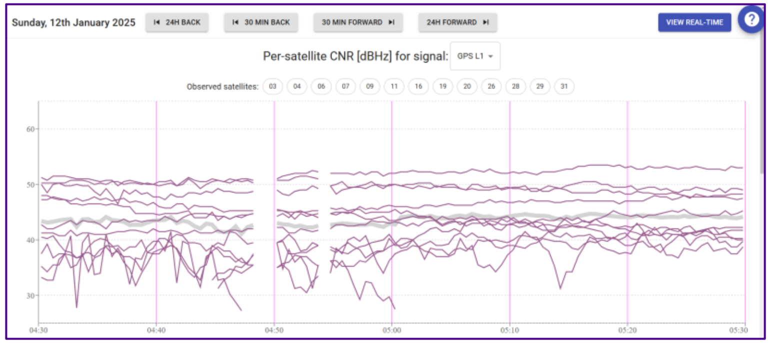
GNSS Finland monitoring service

- GNSS-Finland Service bases on the national GNSS reference station network FinnRef maintained by the National Land Survey of Finland
  - Data from the network is analyzed by the service in real time
- Signals monitored at different stations along with signal strength estimation parameters
- The service continuously monitors strength of each signal and produces a signal quality indicator as "good", "satisfactory" or "poor"

https://gnss-finland.nls.fi

- GPS L1
- GPS L1C
- GPS L2C
- GPS L5
- GLONASS G1
- GLONASS G2
- Galileo E1
- Galileo E5a
- Galileo E5b
- Galileo E5ab
- Galileo E6
- BeiDou B1
- BeiDou B1C
- BeiDou B2a
- BeiDou B3



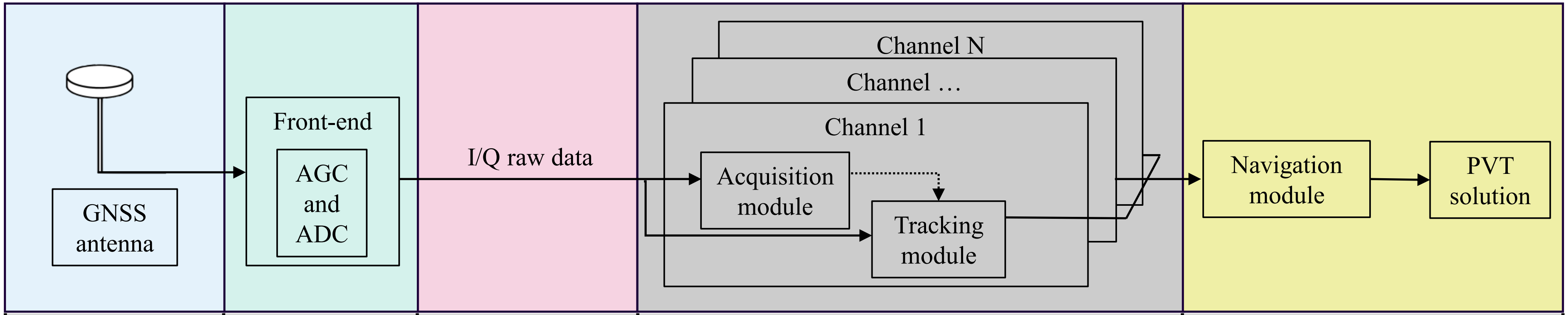


Principles of Resilient PNT

Resilience = Detect + Withstand + Recover

Defense layer	Examples
Signal & RF layer	Interference monitoring, adaptive antennas, nulling
Measurement layer	Receiver Autonomous Integrity Monitoring (RAIM/FDE/ARAIM)
System layer	Signal authentication (Galileo OSNMA), frequency and system redundancy
Multi-source layer	GNSS + 5G + Wi-Fi + IMU + maps + other sensors

GNSS interference mitigation possibilities



	Antenna based techniques	Front-end techniques	Pre-correlation	Post-correlation	Navigation level
Detection	●	●	●	●	◐
Classification			●	◐	
Mitigation	●	◐	●	●	●
Localization	●	●	●	●	

GNSS receiver stages and typical places for interference detection, classification, localization, and mitigation

Interference management techniques

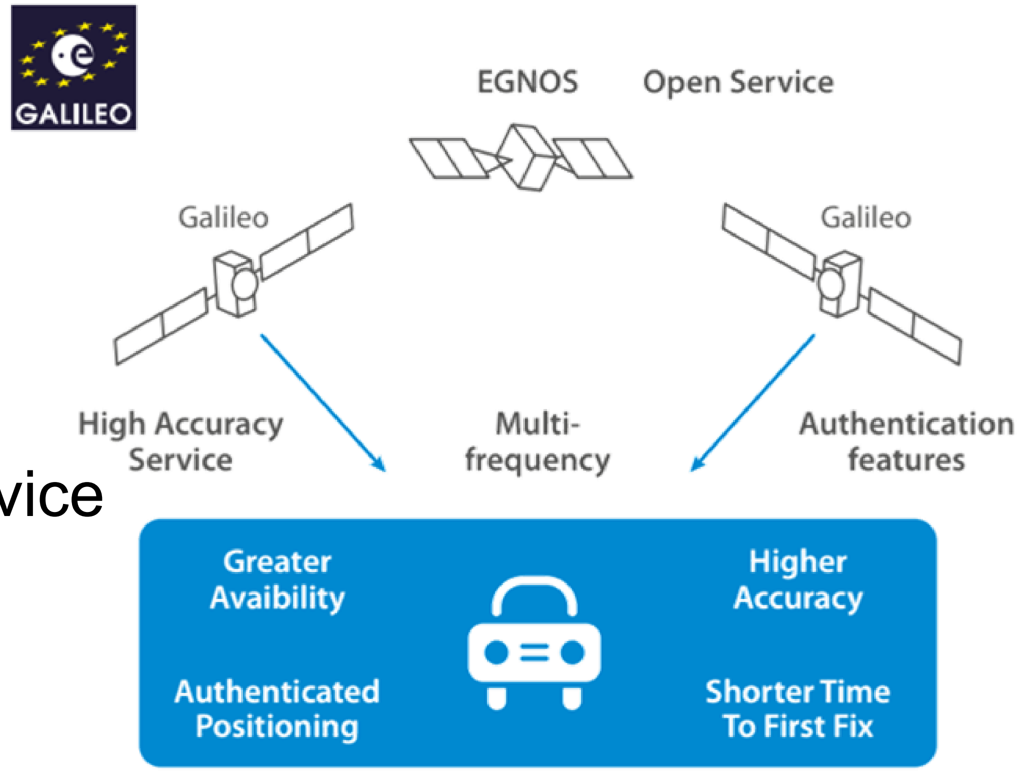
Class	Approach and algorithms	Strengths	Limitations
Antenna based techniques	Use of **antenna array** to filter out interference signals, for example using angle of arrival.	Can handle different types of interferences. Outstanding performance.	Requires **multiple receiver antennas**, high hardware complexity, sometimes export-controlled.
Front-end techniques	Process signals before the ADC, e.g., **Automatic Gain Control** (AGC).	Can handle different types of interferences.	Poor performance for low power spoofing.
Pre-correlation	Uses **raw received signal features**; can be signal-processing based or ML-based (e.g., RF fingerprinting).	Early detection and classification; high detection probability before filtering stages.	Limited mitigation/localization; cannot identify affected satellites; ML requires large training datasets.
Post-correlation	Use **signal after correlation** (SQM, C/N_0 monitoring, peak monitoring, scatter diagrams)	Can detect, mitigate, localize, identify genuine vs spoofed signals.	Struggles with induced spoofing; ML may require large datasets.
Navigation level	Uses multi-signal, multi-satellite, multi-frequency and multi-receiver **consistency tests**.	Integration with sensor fusion is intuitive and well developed.	Long processing time; **delayed interference response**.

Emerging countermeasures & authentication (1)

- The Galileo system, once fully operational, will offer eight high-performance services worldwide:
  - Open Service (OS)
  - Open Service Navigation Message Authentication (OSNMA)
  - Public Regulated Service (PRS)
  - High Accuracy Service (HAS)
  - Timing Service (TS)
  - Signal Authentication Service (SAS)
  - Search and Rescue Service (SAR)
  - The Galileo Emergency Warning Satellite Service
- Signal authentication in the Galileo system
  - Ensures trust in positioning data
  - Detects and prevents spoofing

European GNSS Service Center

EUSPA EO and GNSS Market Study, European Commission 2024.



Strengthening European MEO-based GNSS

Emerging countermeasures & authentication (2)

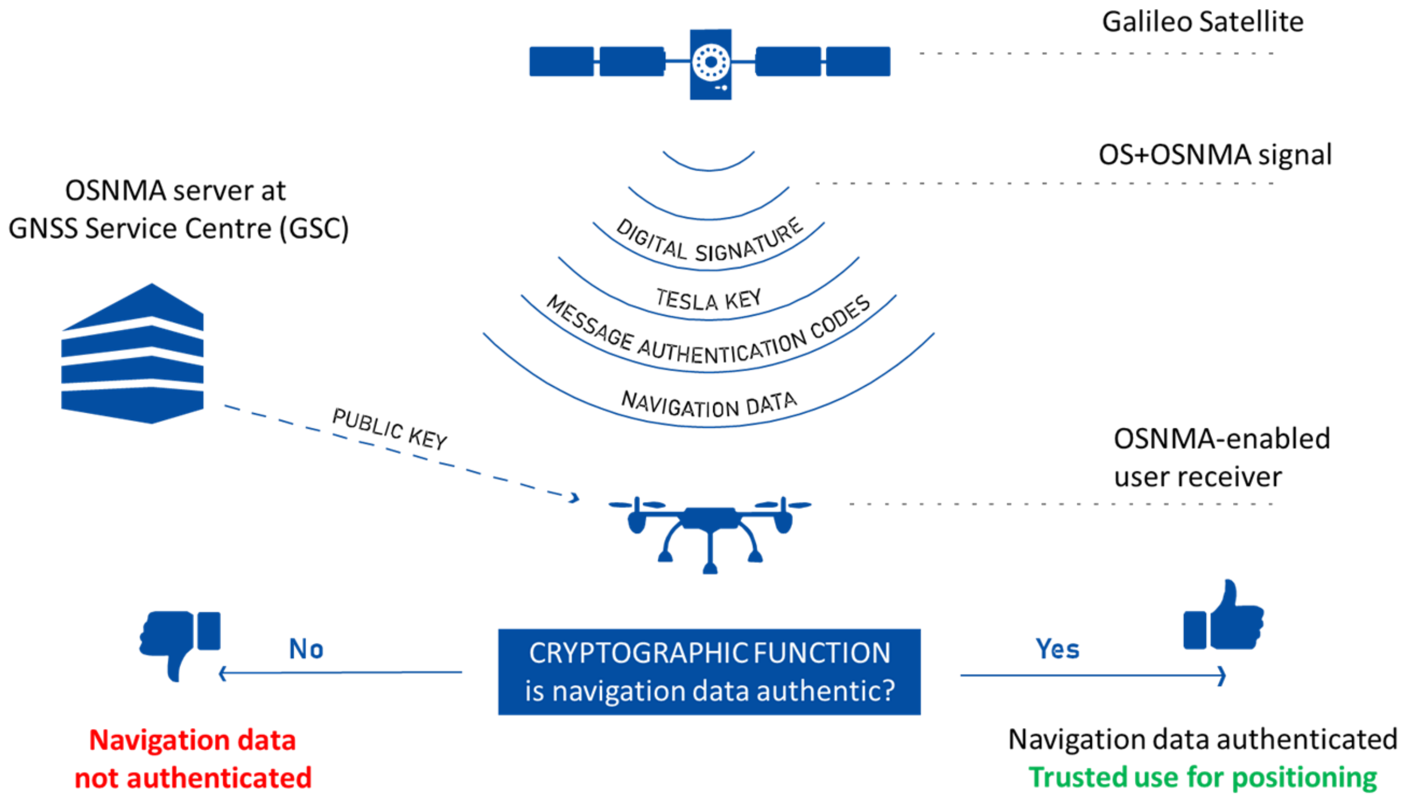
Service	Description
Open Service (OS)	Free for all users; provides positioning, navigation, and timing globally.
High Accuracy Service (HAS)	Offers centimeter-level accuracy (≈20 cm) for free since Jan 2023.
Commercial Service (CS)	Provides encrypted signals and additional data for commercial applications.
Public Regulated Service (PRS)	Encrypted, robust service for authorized government and critical infrastructure users.
Safety of Life Service (SoL)	Designed for applications requiring integrity and reliability (e.g., aviation).
Search and Rescue (SAR)	Integrated with MEOSAR; enables faster detection and location of distress signals.
OSNMA	Open Service Navigation Message Authentication: Provides authentication for navigation messages to enhance security.
CAS	Commercial Authentication Service: Offers advanced authentication for high-security commercial applications.
New Features	HAS free access for high precision positioning; PRS signals broadcasting started in 2024; Ground segment upgrade for enhanced cyber protection and readiness for Second Generation (G2) satellites.

Security moves from trusting the signal to trusting the solution

Galileo services

Open Service Navigation Message Authentication OSNMA (1)

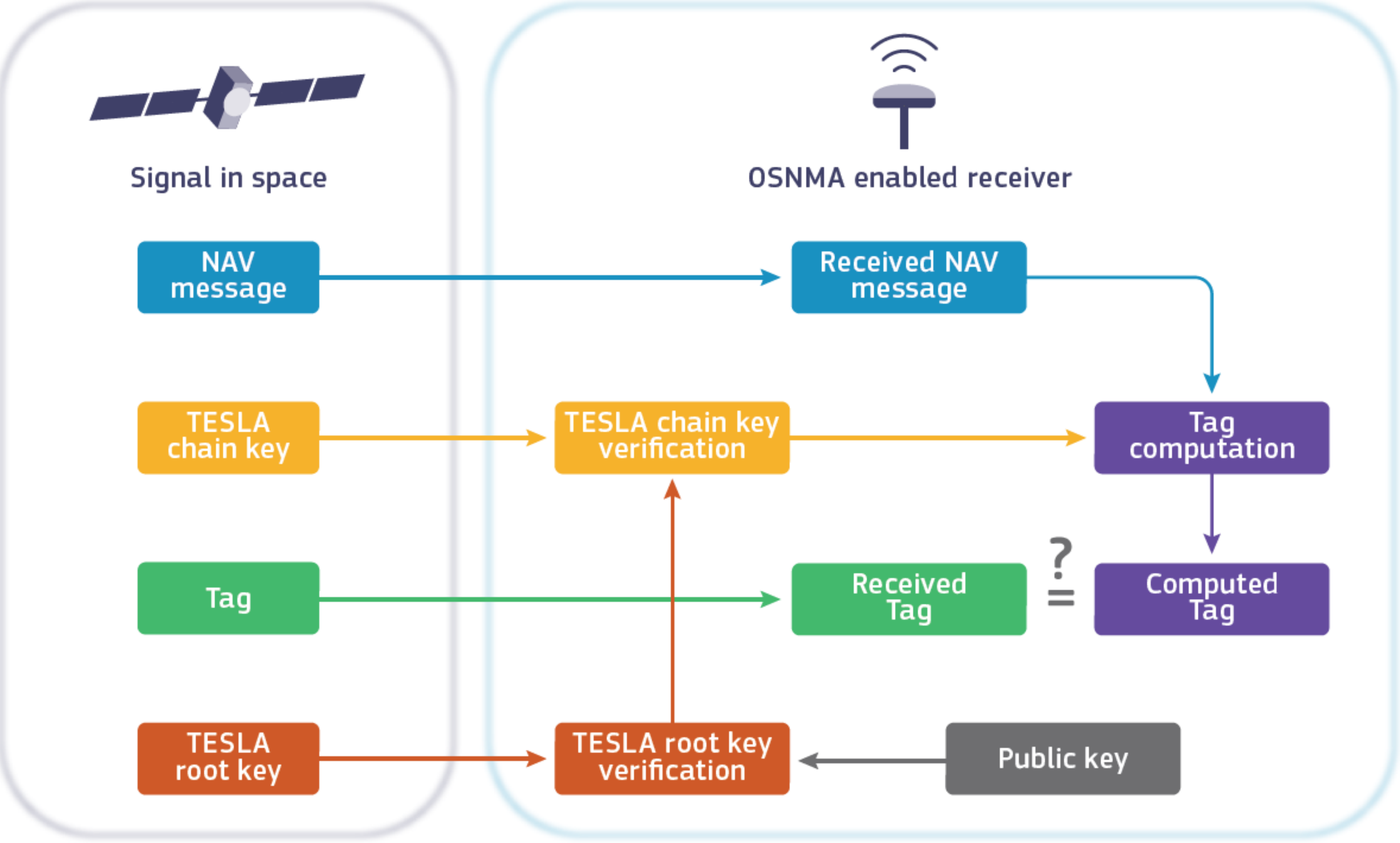
- OSNMA is a new feature of the Galileo Open Service which enables users to **verify that the navigation data** they receive **originated from the Galileo satellite** and **has not been modified**
- OSNMA is **now available for testing** by receiver manufacturers and application developers



Source: European Commission, Joint Research Centre (JRC)

Open Service Navigation Message Authentication OSNMA (2)

- Navigation data are verified through the computation of a truncated Message Authentication Code (MAC), named **tag**, which is compared against a **received tag**.
- The tag is computed with a **key**, released after the tag. To ensure the timely reception of OSNMA data, **time synchronization** to GST is required.
- The key is part of a TESLA chain, and can be used to derive previous keys, as the **TESLA root key**.
- The TESLA root key is verified with a **public key** through a digital signature algorithm.



Source: European Commission, Joint Research Centre (JRC)

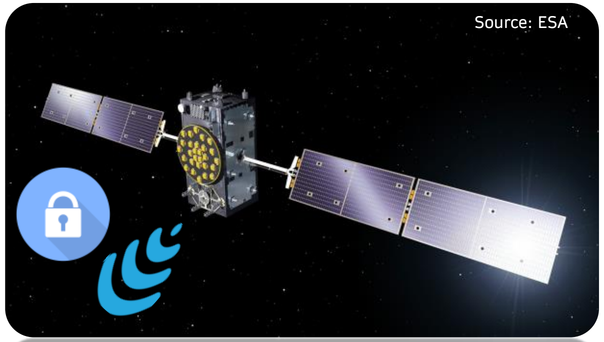
Tampere University
Tampere University of Applied Sciences

Real-world resilience testing important

- For example the Jammertest in Norway: controlled GNSS interference, also in open air (www.jammertest.no)
- Realistic conditions, realistic consequences
- Cross-sector collaboration
- Data to drive PNT innovation & also policy

Tampere University
Tampere University of Applied Sciences

Multi-layer PNT & LEO-based PNT



- Resilient PNT is becoming inherently **multi-layered, authenticated, and intelligent**
- **Interference management and authentication** to fight GNSS jamming and spoofing
- Robustness and redundancy also via **Low Earth satellite systems**
- Terrestrial systems (**5G/6G, WLAN** etc)

Source: Inside GNSS, 2023

LEO-PNT to complement GNSS

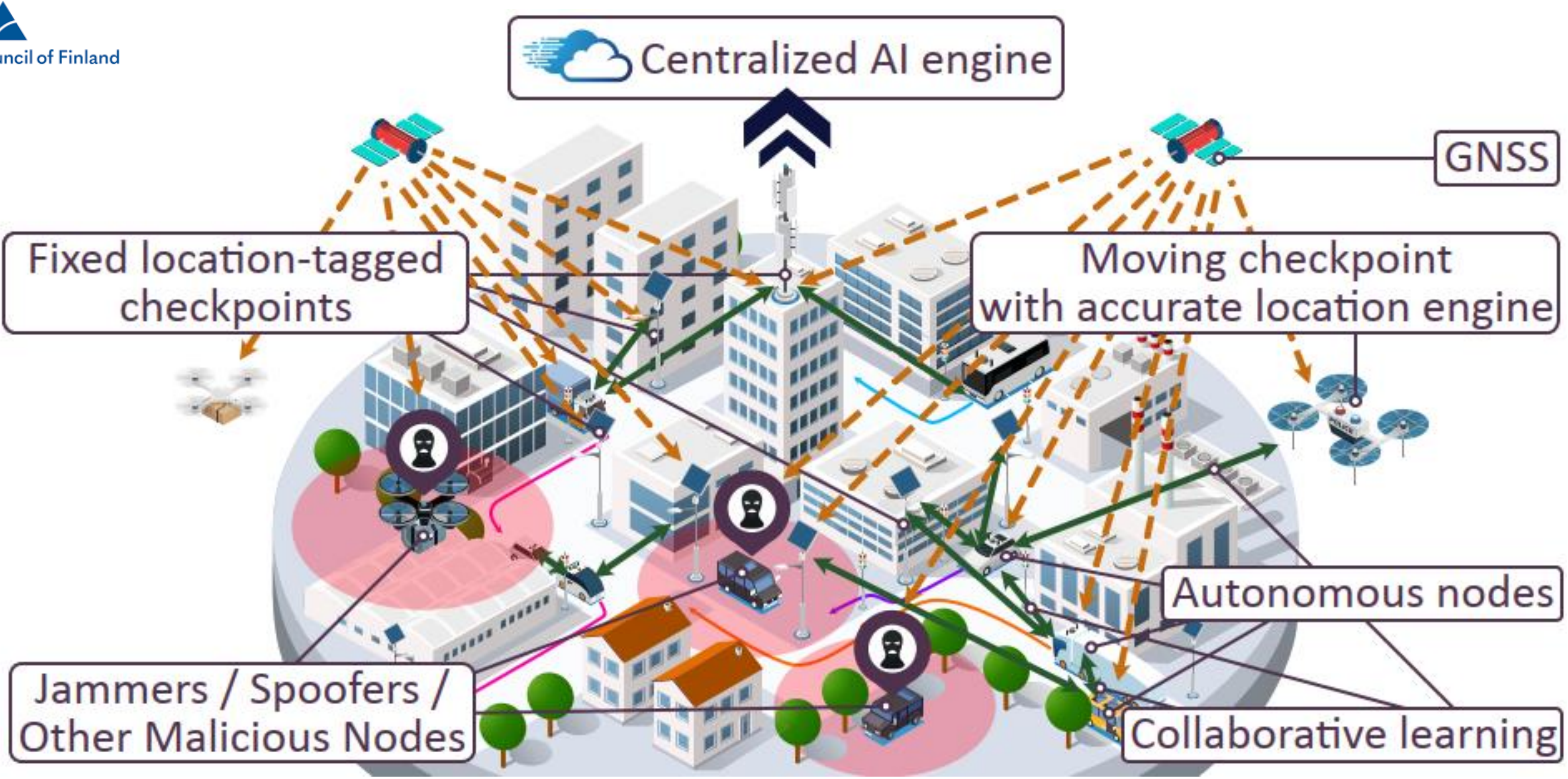
Celeste is the the LEO-PNT In-Orbit Preparatory Phase (IOPP) of the FutureNAV Programme at ESA

A LEO PNT complement to the backbone Galileo and EGNOS infrastructures within a global EU PNT architecture will significantly enhance the resilience and accuracy of and the derived PNT services

Operating closer to Earth, LEO-PNT will support precise and robust PNT services, even in environments subject to jamming, interference, or degradation, thus ensuring reliable access to critical geolocation and timing information in any scenario

Celeste LEO-PNT
Image credit: ESA

National project INCUBATE on LEO PNT, funded by Technology Industries Finland (Aalto University, Tampere University, University of Vaasa, Finnish Geospatial Research Institute)



CONCEPT OF PROJECT RESILIENT

Distributed AI for enhanced security in satellite-aided wireless navigation

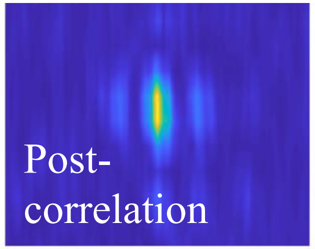
Collaboration project of Tampere University (FIN) and Northeastern University (US)

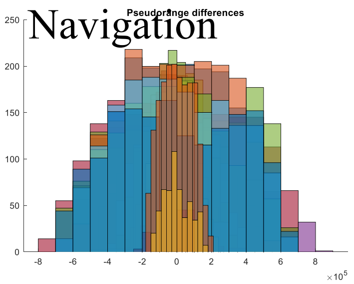
Tampere University
Tampere University of Applied Sciences

Collaborative Interference Mitigation and Robust Positioning

THRUST I

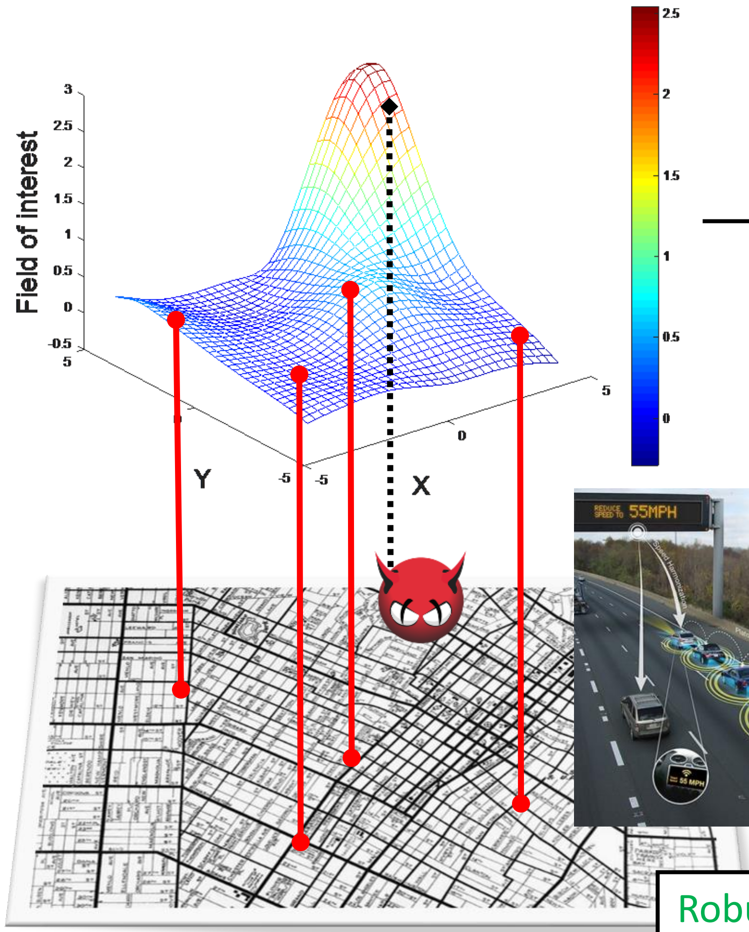
RF fingerprinting for interference management
(hybrid data/model-driven)

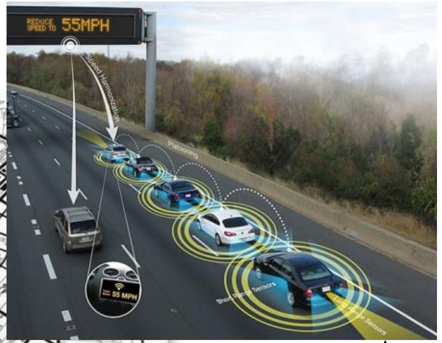




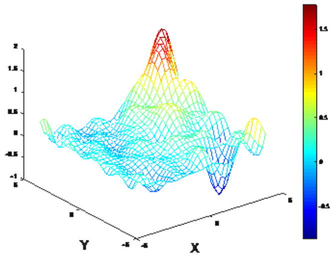
THRUST II

Field of interest
(Threat fingerprint or threat probability)





Distributed, privacy-preserving sensing
(Federated Learning field reconstruction)



Threat localization and tracking
(Active learning)

Meta-learning
(Task level knowledge)

Robustification / Collaboration with fixed anchors and exploiting strong interferers
(Reinforcement learning/ Factor Graph Optimization)

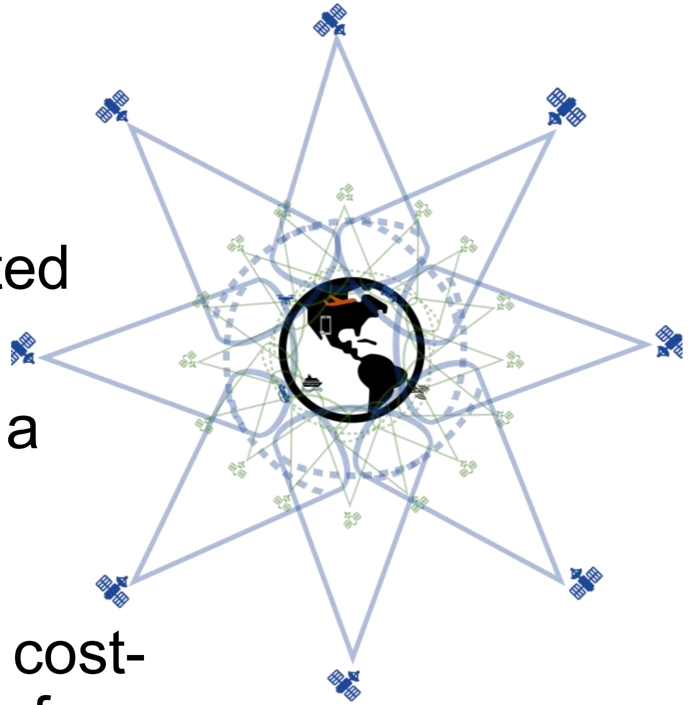
THRUST III

- Optimized robust positioning using **Factor Graph (FG)** in combination with threat detection
- Adaptive positioning strategies using **Reinforcement Learning (RL)**

Key takeaways (1)

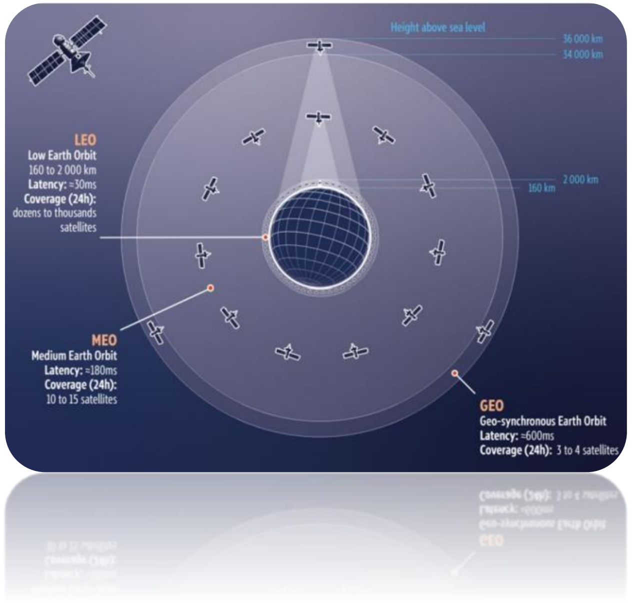
- GNSS receivers should exploit **multi-constellation multi-frequency diversity** for robust PNT services
- Modernized GNSS signals and services such as Galileo E1 **OSNMA** and Galileo E6 **CAS** encryption should be utilized to protect users from spoofing attacks
- Intelligent advanced **algorithms at tracking and measurement layers** will make future receivers better resilient against adverse GNSS vulnerabilities
- The Standards Working Group for Resilient PNT User Equipment **(P1952) in IEEE** is working towards refinement and development of ‘Resilient PNT Conformance framework’
- **Low-cost antenna array solutions** can improve PNT resilience in the form of interference/spoofing source detection, localization, and mitigation
  - By multi-element antennas we can toughen GNSS receivers enough to withstand 1 kW wideband Gaussian jammer at a distance of 2 km

Key takeaways (2)



- **LEO signals and satellite constellations** specifically dedicated to PNT are transitioning towards practical implementation
- Receiver specific implementation that is yet to be emerged as a commercial solution to exploit **GNSS+INS+LEO+SOOP** with intelligent fallback mechanism
- **Space-borne interference monitoring at LEO** can be a very cost-effective solution with a global coverage, including monitoring of interference over sea and difficult terrain with limited physical access
- Another important expected technological evolution is the **coupling of communication and localization capabilities**, which is expected to benefit all sectors, including surveillance and communication applications

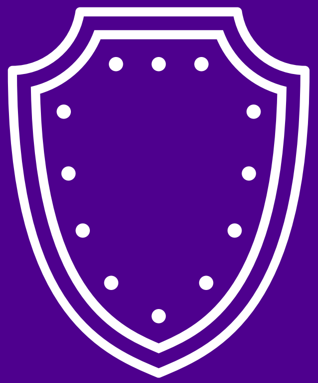
Source: [Satellites – state of play and challenges for the EU](), European Parliament

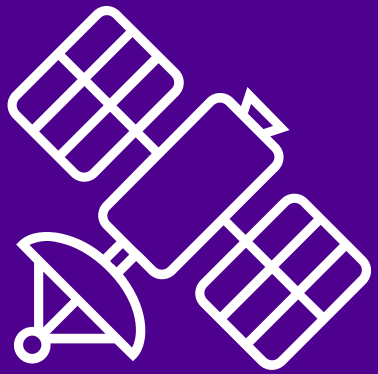


Key takeaways (3)

- There is currently **little coordinated effort** on a European level to **fight** a potentially pan-European GNSS **interference problem** (i.e., military-level jamming, wide-spread jamming that can cause serious threat to safety of life applications, etc.)
- A **wide area GNSS threat monitoring system** can be developed utilizing existing national or international continuously operated reference stations, that can simultaneously monitor all GNSS frequency bands
- **Crowdsourced interference detection** is a relatively new concept, and researcher are looking at how crowdsourced GNSS data could be better utilized for GNSS interference/signal quality heatmap generation.
  - This heatmap data can then be utilized for different perspectives including real time optimum route guidance alerting to affected GNSS stakeholders of severe GNSS outage

Tampere University
Tampere University of Applied Sciences





Thank you!

Any questions or comments?

heidi.kuusniemi@tuni.fi