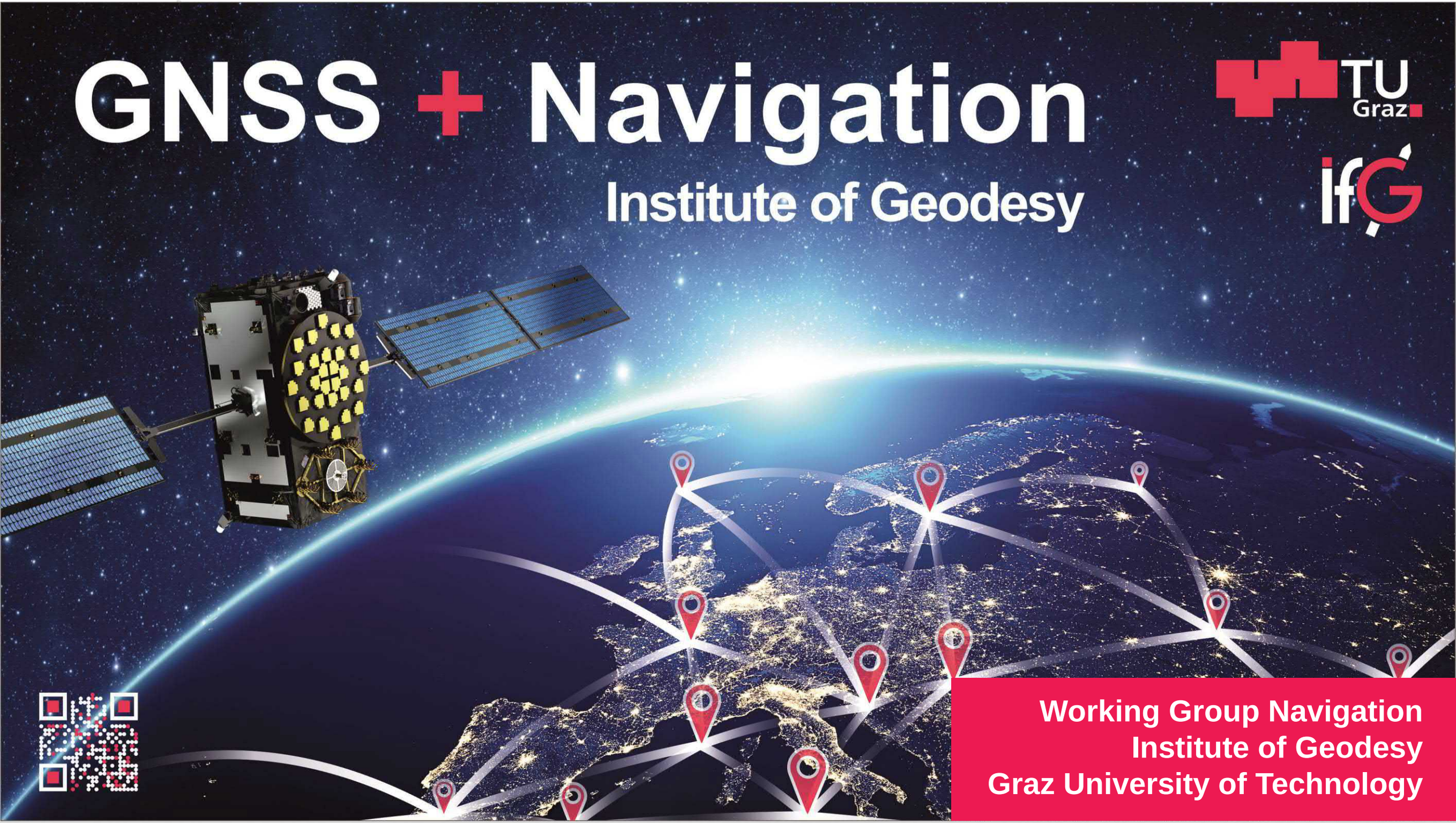
GNSS + Navigation

Institute of Geodesy



Working Group Navigation
Institute of Geodesy
Graz University of Technology

WISSEN
TECHNIK
LEIDENSCHAFT

GNSS Interference – jamming & spoofing

GNSS Under Attack Workshop

Univ.-Prof. Dr. Philipp Berglez

6 February 2026

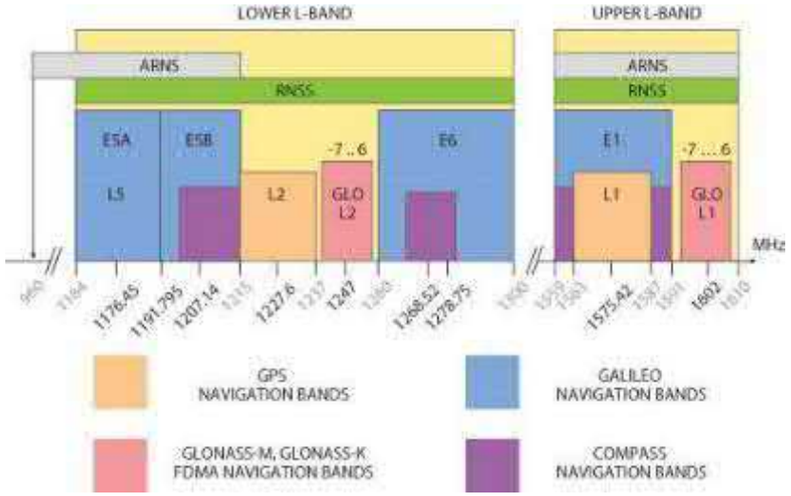
Objectives

- Introduction to GNSS interference
- Jamming
  - Detection
  - Mitigation
- Spoofing
  - Detection
  - Mitigation

Introduction to GNSS interference

GNSS frequencies

- Frequency allocation strictly regulated by International Telecommunications Union (ITU)
- GNSS frequency bands

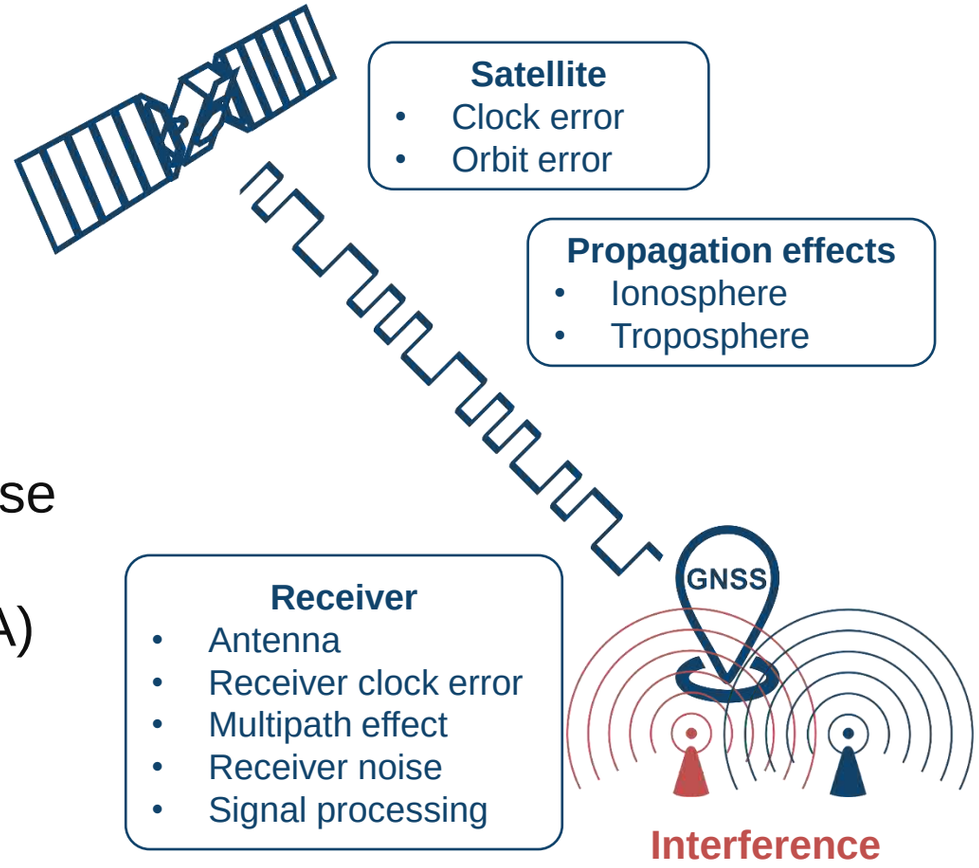


MicrowaveJournal.com May 2012

- Interference can be described as the effect of energy change due to the superposition of electromagnetic waves

Why are GNSS signals vulnerable?

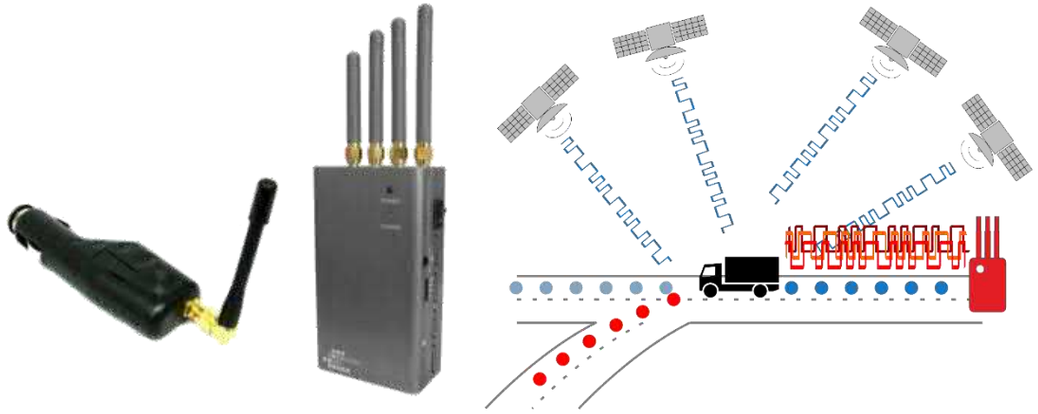
- GNSS are highly complex systems
- GNSS signals received on Earth are very weak
  - Power level is equivalent to that of a 30 Watt light bulb after traveling more than 20,000 km
  - GNSS signal bands are dominated by white noise
- Signal design dates back to the 70s/80s (GPS L1 C/A)
  - Civil signal design is well known / published
  - Intentional interference for civil users was of minor concern
- GNSS signals are vulnerable to all types of errors / interference



Classification of interference

- Unintentional interference
  - Natural interference → Ionosphere (especially solar storms)
  - Intra-system interference (e.g., Galileo SV1 ⇔ SV2)
  - Inter-system interference (e.g., Galileo ⇔ GPS)
  - Self-interference: e.g., inter-symbol interference; inter-modulation product
  - External interference (other RF systems)

- Intentional interference
  - Jamming
  - Spoofing
  - Meaconing



Intentional interference

- Jamming
  - Transmission of interference signals (noise) and drowning of the useful signal in noise
  - Decreased accuracy or no position information
- Spoofing
  - Transmission of counterfeit GNSS-like signals
  - Produces a false position / time within the victim receiver
  - Without disrupting operations
- Meaconing
  - Interception and rebroadcast of navigation signals
  - Multipath – environmental meaconing

The possession and operation of jammers is illegal throughout the EU.

GNSS jamming

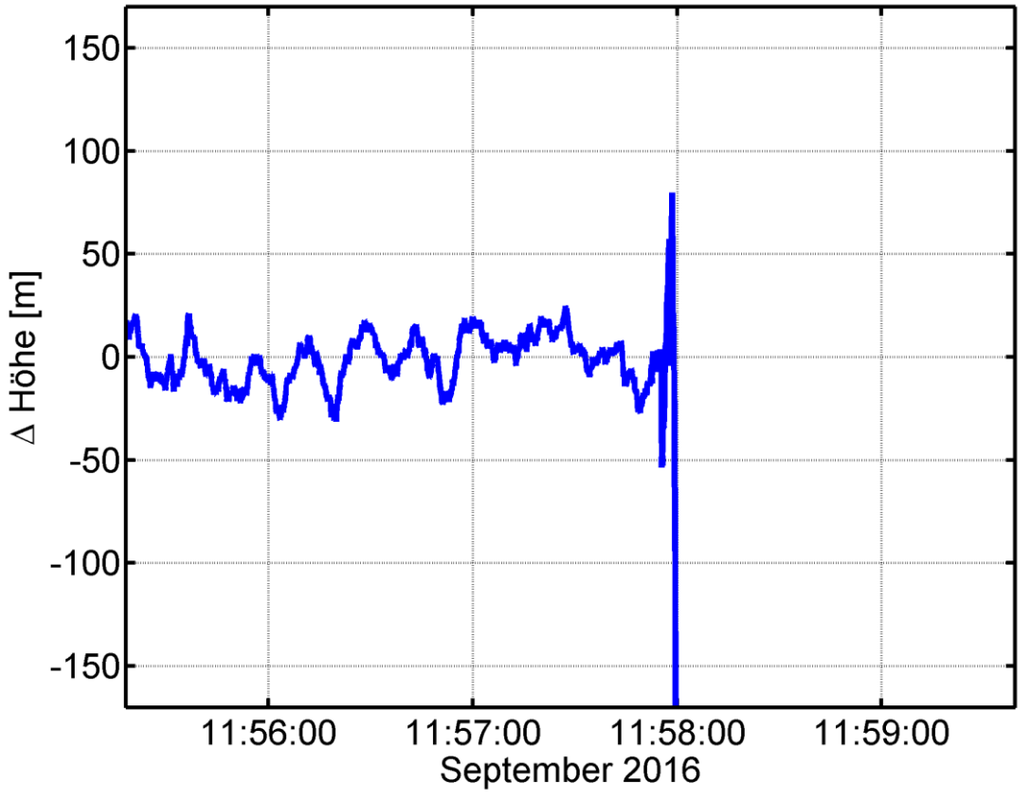
How does it work?

- The aim of jamming signals is to disrupt navigation services by superimposing strong noise on GNSS signals.
  - Intentional transmission of RF energy to hinder a navigation service by drowning (masking) GNSS signals with noise
  - Objective to cause a receiver to lose tracking and impede signal reacquisition

- Motivation:
  - Turning off car anti-theft-systems
  - Bypassing pay-as-you-drive insurance
  - Withdrawing Fleet Management System
  - Protecting the privacy of parcel delivery agents from their employers
  - Protection of critical infrastructure
  - Electronic warfare
  - Etc.

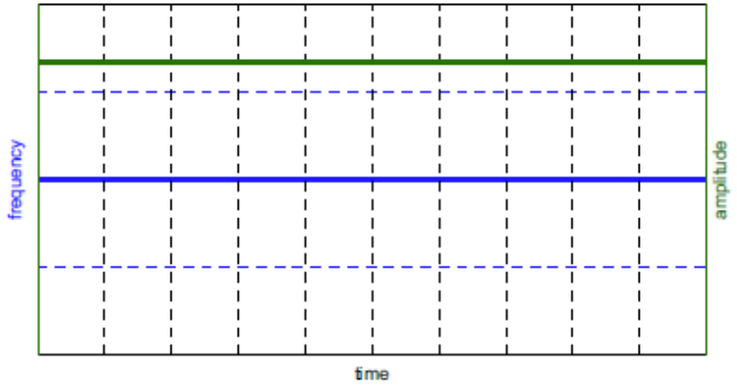
Impact of jamming

- Signal strength and quality
  - Decreased/degradation of SNR and C/N0
  - Lower availability of observables
  - Longer acquisition time and longer time-to-first-fix
  - Loss of signal tracking
- Measurement quality
  - Increased noise within tracking loops → degradation of accuracy
  - Increased number of cycle slips
- PVT accuracy → Denial of service
- Damage the receiver hardware

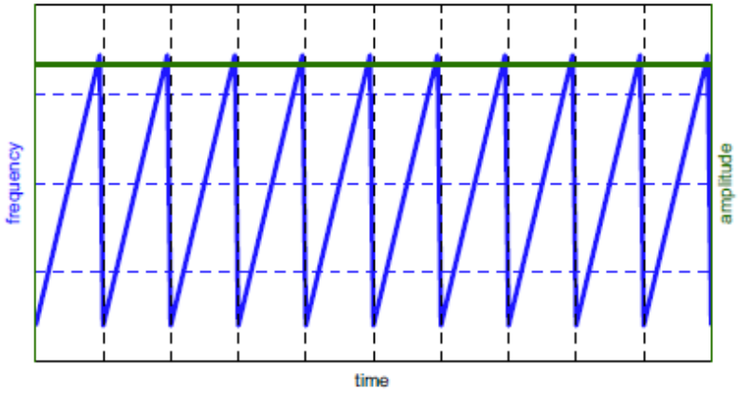


Classes of jammer

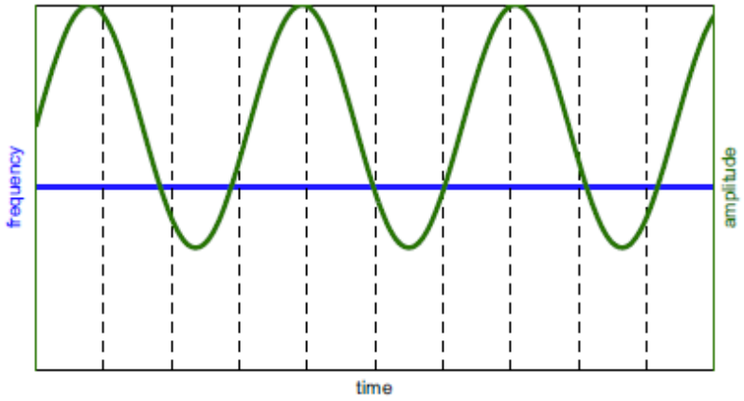
Continuous wave



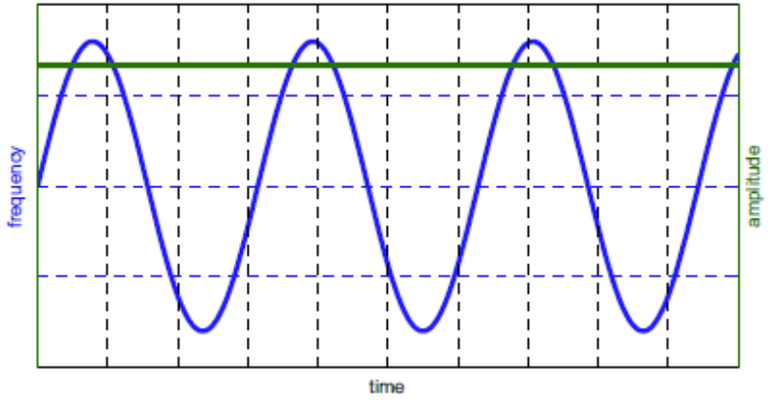
Swept Continuous wave



Amplitude modulation

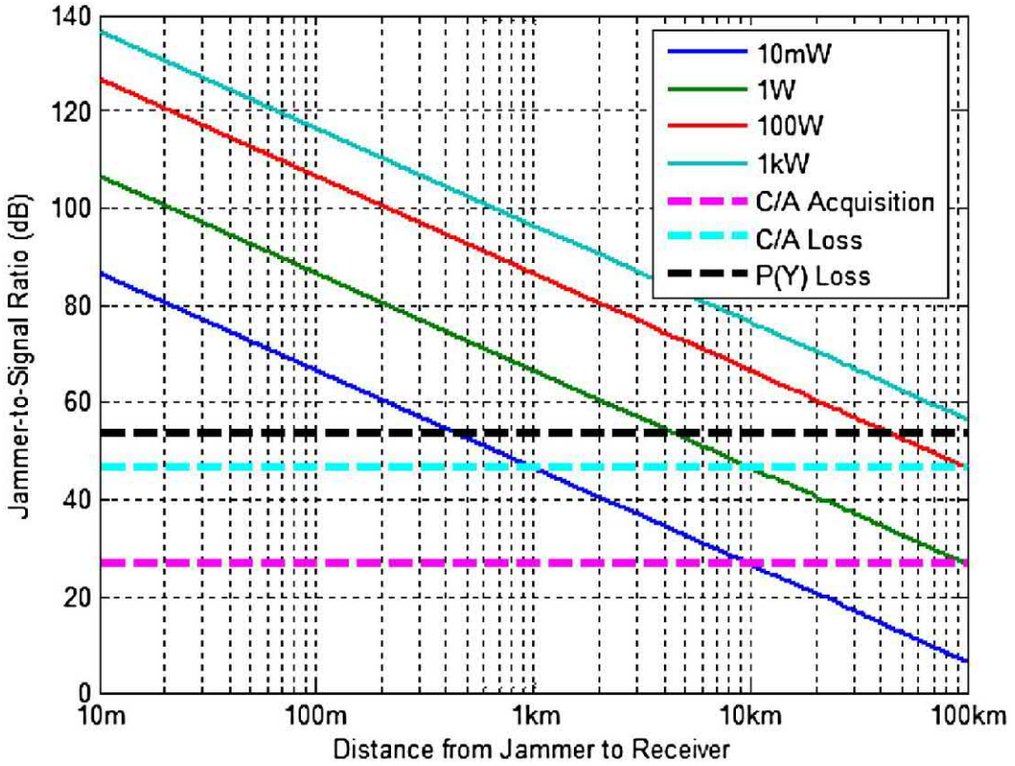


Frequency modulation



Jamming considerations (1/2)

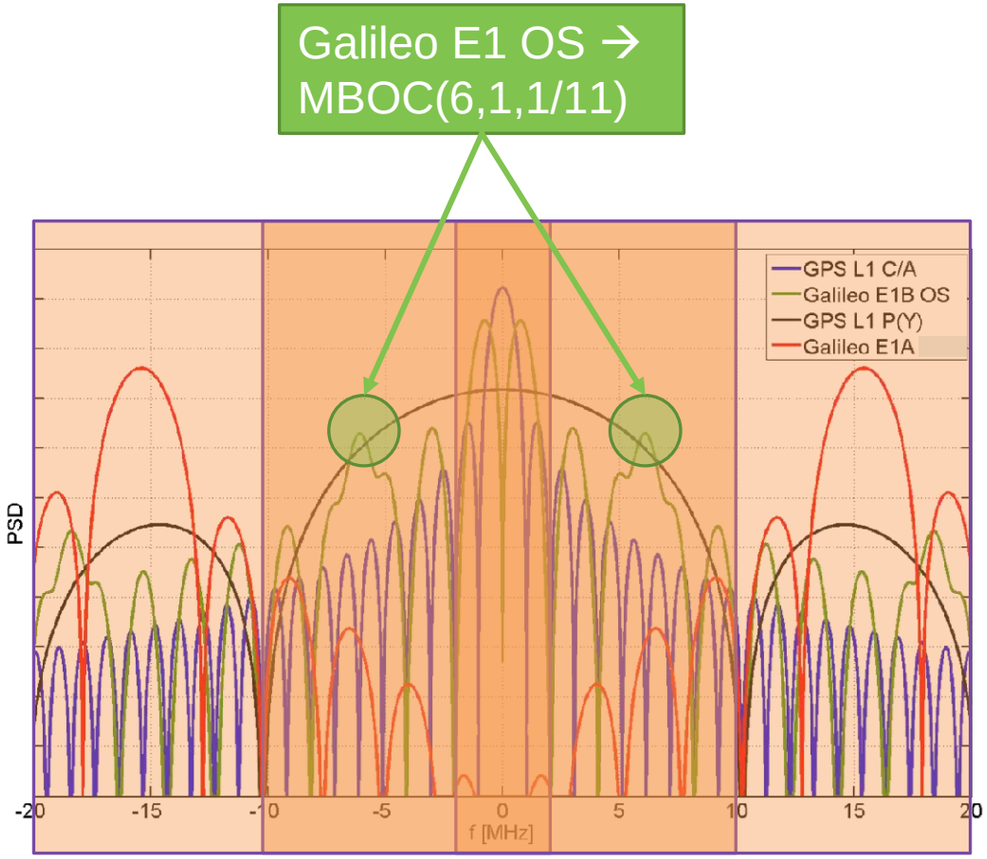
- Jamming power → Jamming radius
- Jamming power and jammer height
  - >100 m within cars/urban environment
  - up to 30 km at heights of 10 m
  - >100 km on weather balloons
- Protection of own system



Ref.: Jones, M. (2011): The Civilian Battlefield. Protecting GNSS Receivers from Interference and Jamming. *InsideGNSS* March/April 2011, 40–49.

Jamming considerations (2/2)

- Target receiver capabilities
  - i.e. systems, frequencies, signals, bandwidth, algorithms implemented
  - Jamming bandwidth: 2 MHz
    - Low-cost receivers
    - GPS L1 C/A jammed
    - Other signals still available
  - Jamming bandwidth: 10 MHz
    - Medium performance receivers
    - Galileo PRS still available
    - Jamming bandwidth: 20 MHz
  - High-end receivers



Jamming detection and classification

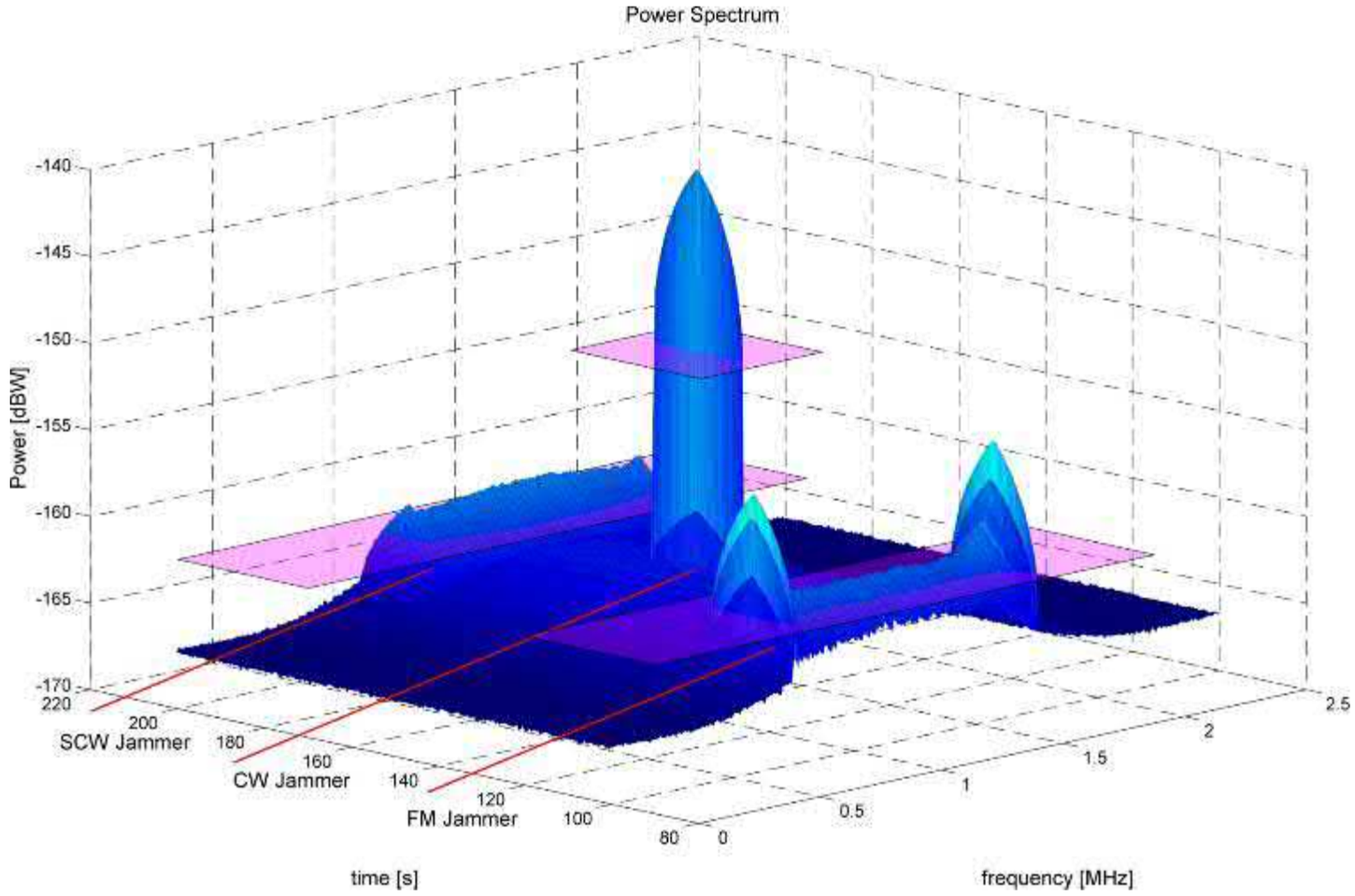
Detection

- Automatic Gain Control (AGC) monitoring
- Time-domain statistical analysis
- Spectral monitoring (PSD monitoring)
- Post-correlation statistical analysis
- Carrier-to-noise power ratio monitoring
- Pseudorange monitoring (accuracy and outliers)
- PVT solution monitoring (position monitoring)
- ML / AI strategies
  - Lots of training data required
  - Black box → critical for safety critical applications

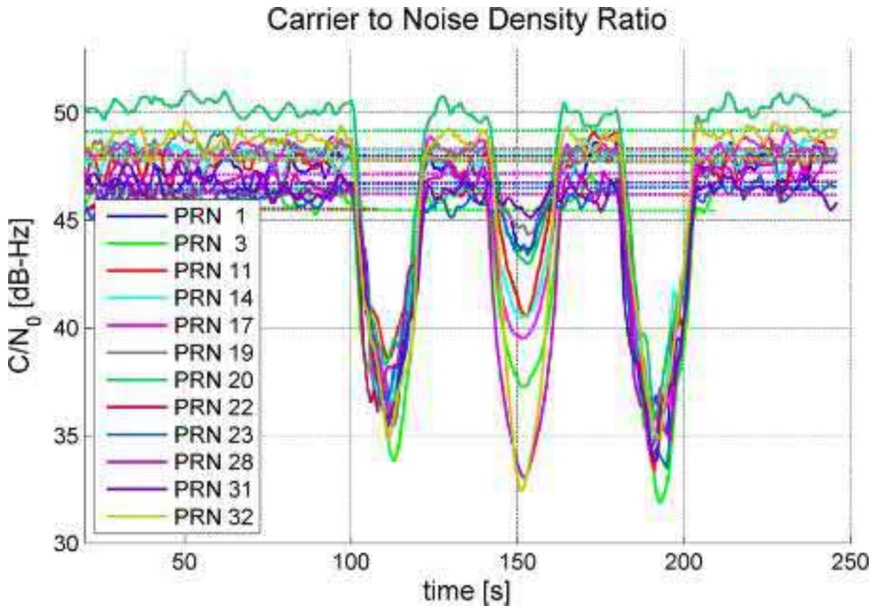
Classification

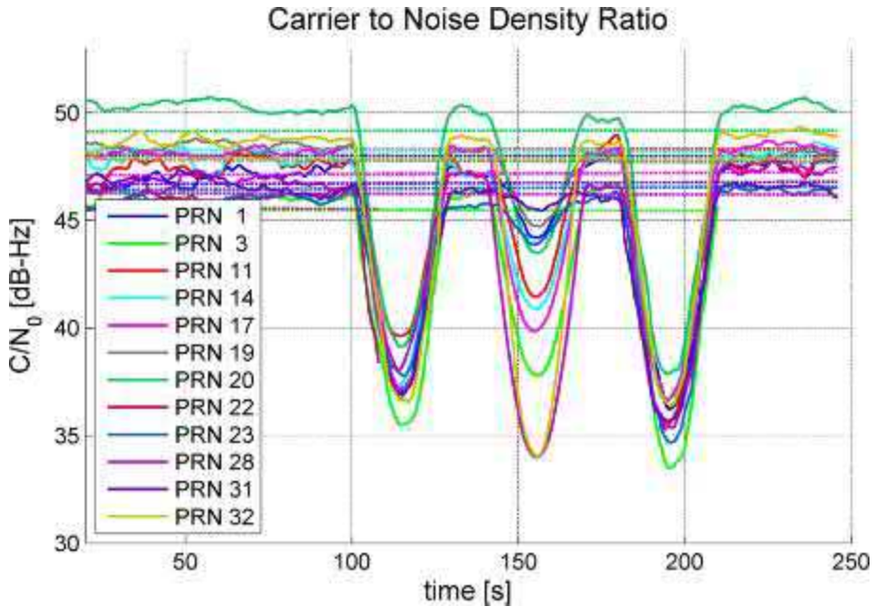
- Estimate parameters of jammers
  - Received jammer power
  - Frequency behaviour
  - Bandwidth
  - Repetition rate
  - Pulse duration
- Important for countermeasures

Detection of Jammer – PSD Monitoring - Example



Detection of Jammer – $\left({}^{C}/_{N_0}\right)_{eff}$ - Example





CNR Averaging Time

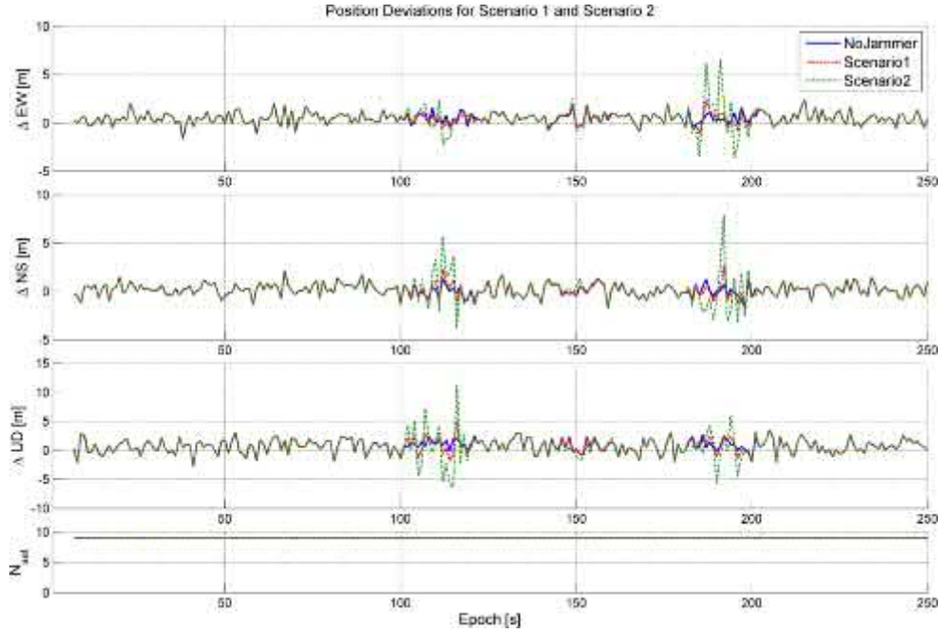
3 s 10 s

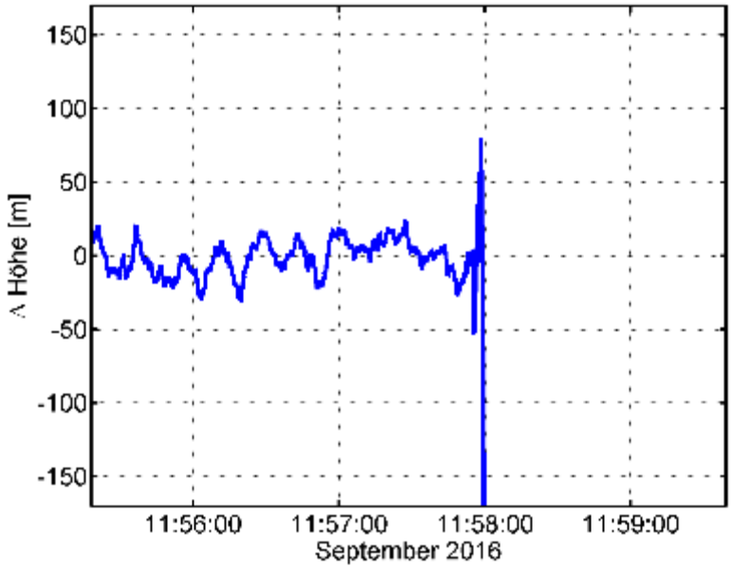
Detection of different jammers possible

Longer averaging time leads to less false alarms, but later detection

Position monitoring - Example

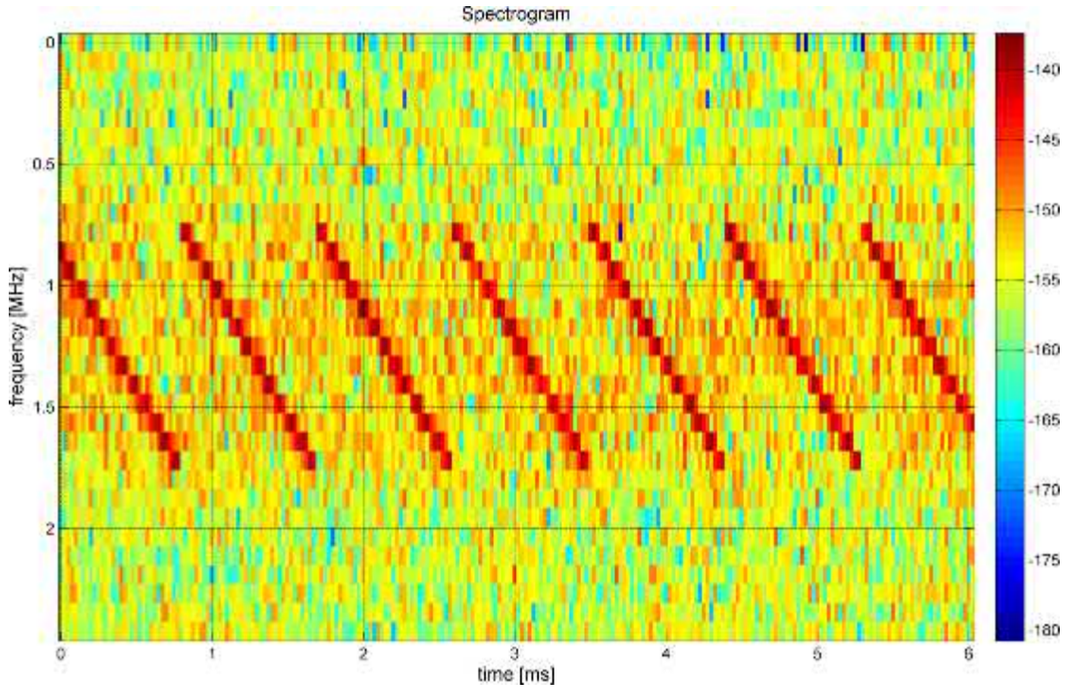
- Comparing calculated position with reference position (only in static case)
- Deviation threshold depends on several factors
- Prior to losing the position an increase in the accuracy (DLL, PLL as well as position) can be observed





Classification of jammers - Example

- Estimate Parameters of Jammers
  - Repetition Rate
  - Bandwidth
  - Received Jammer Power
  - Pulse duration
- Spectrogram
  - time-frequency resolution trade-off
- Adaptive Notch Filter

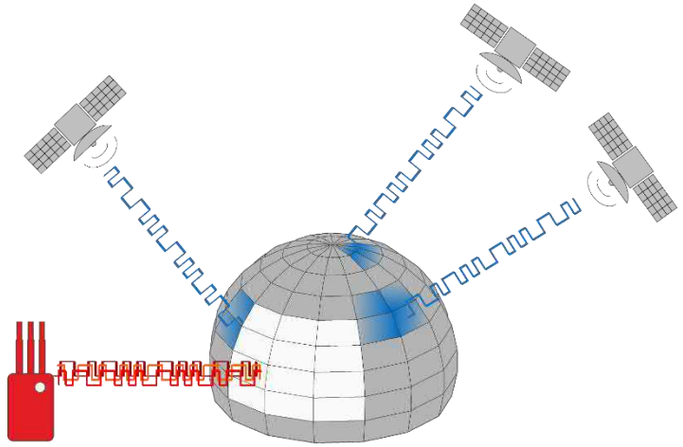


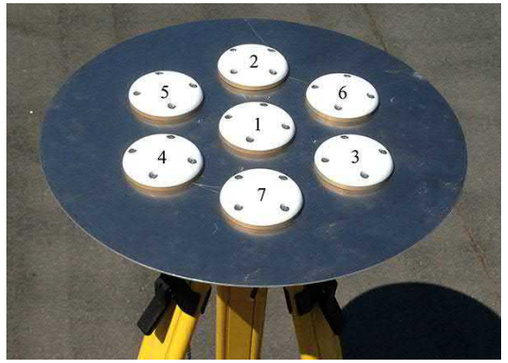
Ref.: Bokan U., Duregger M., Berglez P., Hofmann-Wellenhof B. (2019): Detection and mitigation strategies for GNSS interference attacks. In: Zeitschrift für Vermessung & Geoinformation, Heft 2/2019: 83 – 94.

GNSS anti-jamming techniques

- Jamming signals need to be detected first to apply a mitigation approach

- Antenna solutions
    - Low elevation nulling
    - Controlled radiation pattern antenna
    - Adaptive beamforming
      (Spatial signal processing with an array of receivers)

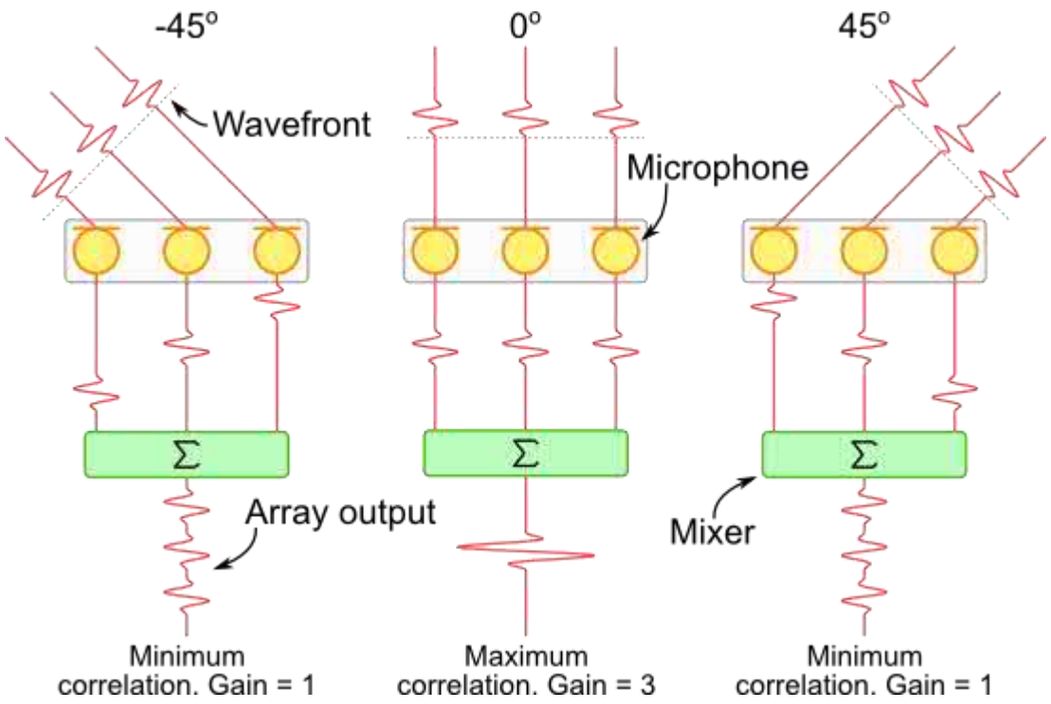




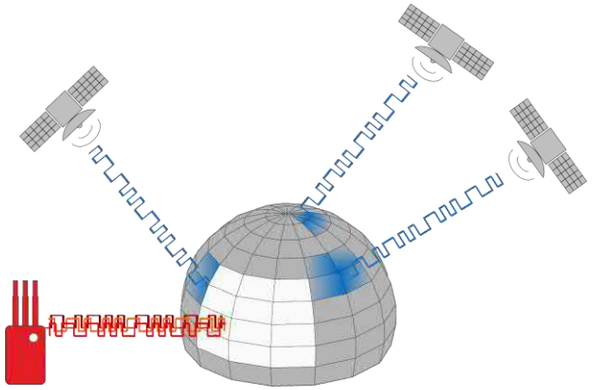
Adaptive nulling vs. beamforming

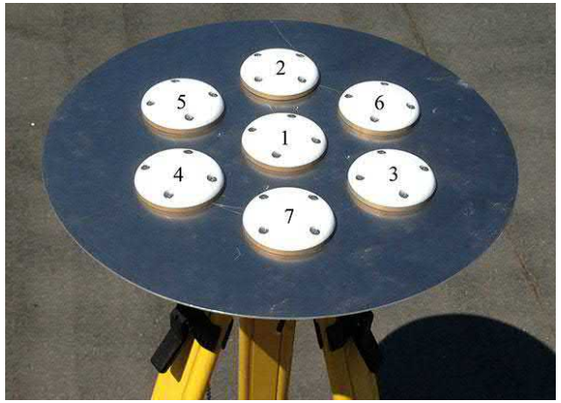
Technique combines signals from arrays of antennas

- single-output nulling antennas
- multiple-output beam-steering antennas



http://gnss-sdr.blogspot.com





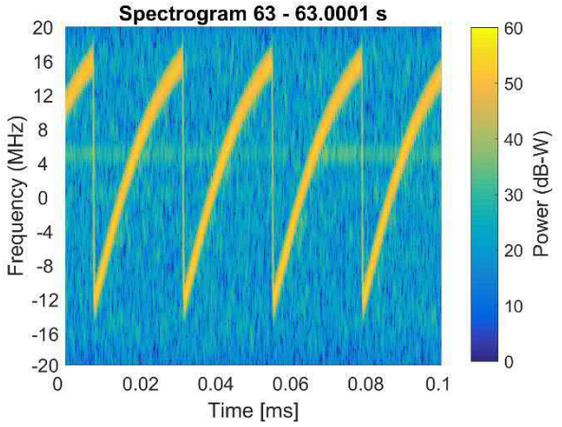
GNSS anti-jamming techniques

- Receiver solutions
  - Adaptive filtering (filtering of frequencies)
  - Switching frequencies (multi-GNSS / multi-frequency)
  - Integrating GNSS with INS (inertial navigation system)
  - Applying an interference suppression unit

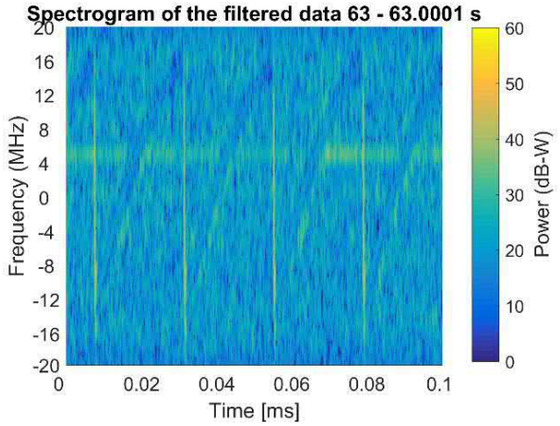
Mitigating jamming signals

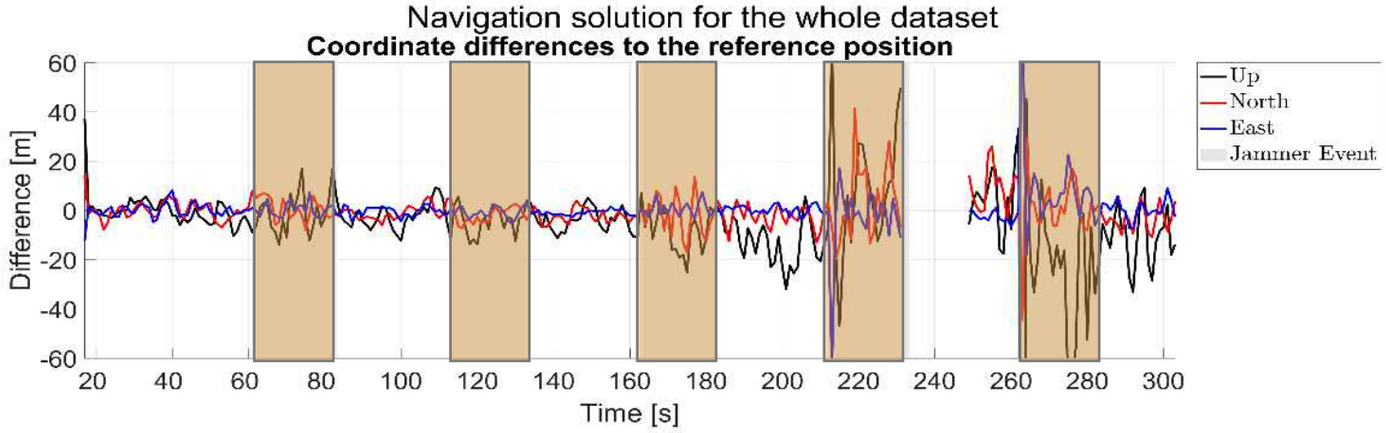
- Adaptive Notch Filter

unfiltered



filtered



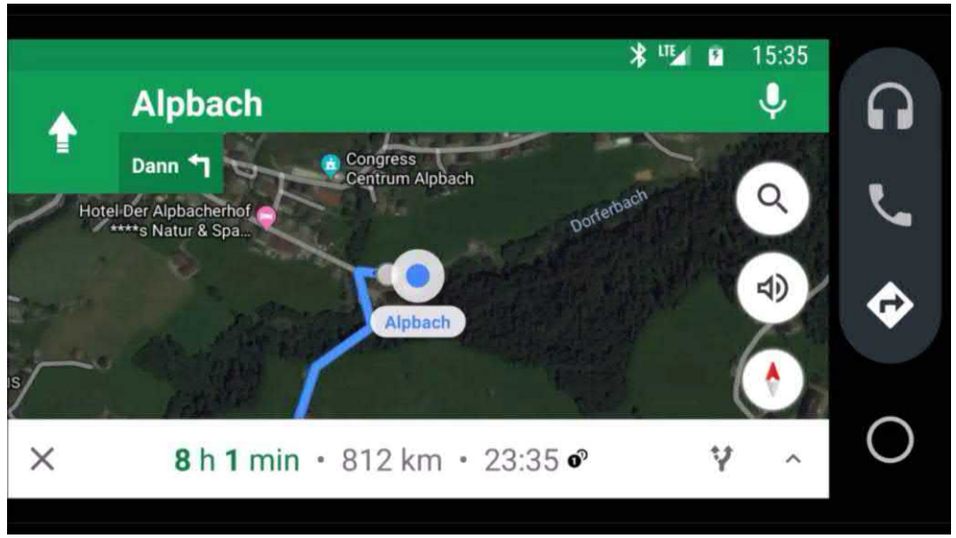


Ref.: Bokan U., Duregger M., Berglez P., Hofmann-Wellenhof B. (2019): Detection and mitigation strategies for GNSS interference attacks. In: Zeitschrift für Vermessung & Geoinformation, Heft 2/2019: 83 – 94.

GNSS spoofing

Can you or anybody trust GNSS data?

- A participant in the European Forum Alpbach 2018 received a phone call from his wife asking why he was actually in Rome and not in Alpbach as promised.



- He was attending my presentation on ‚The need for GNSS resilience‘
- He forgot to stop sharing his real-time location with his wife on his smartphone
- He became a victim of GNSS interference!

GNSS spoofing reported

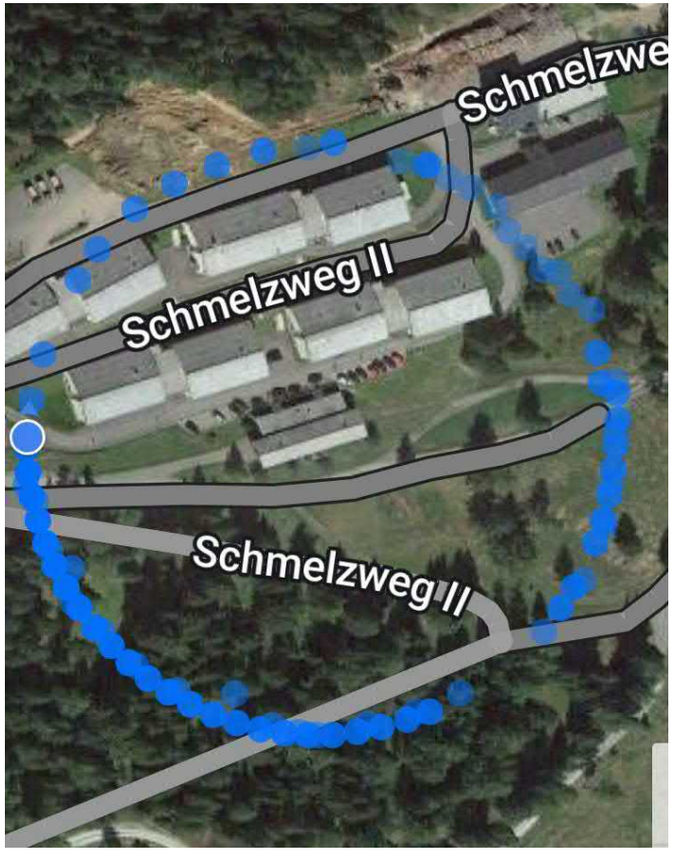
- 2012/2013 - University of Texas demonstrated spoofing several times
- June 2017 – Ships showed position near an airport instead of in the Black Sea
- March 2019 – Car navigation systems from different manufacturers at Geneva international motor show location in Buckingham in England
- December 2019 - GPS ‘circle spoofing’ moves ship locations thousands of miles

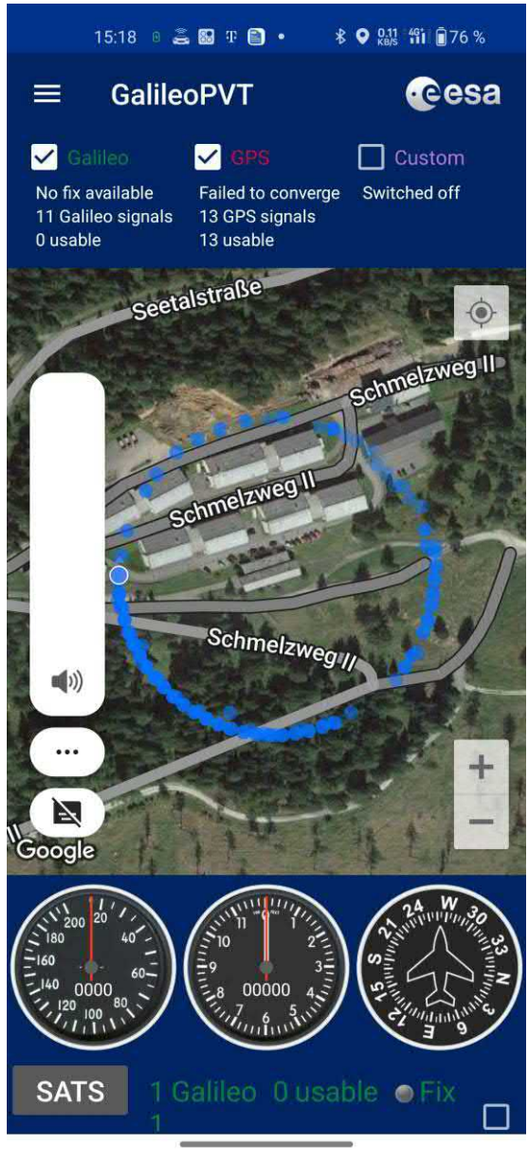
- Successful demonstrated spoofing attacks at various events in Austria
- Jamming and spoofing investigations at TU Graz currently running

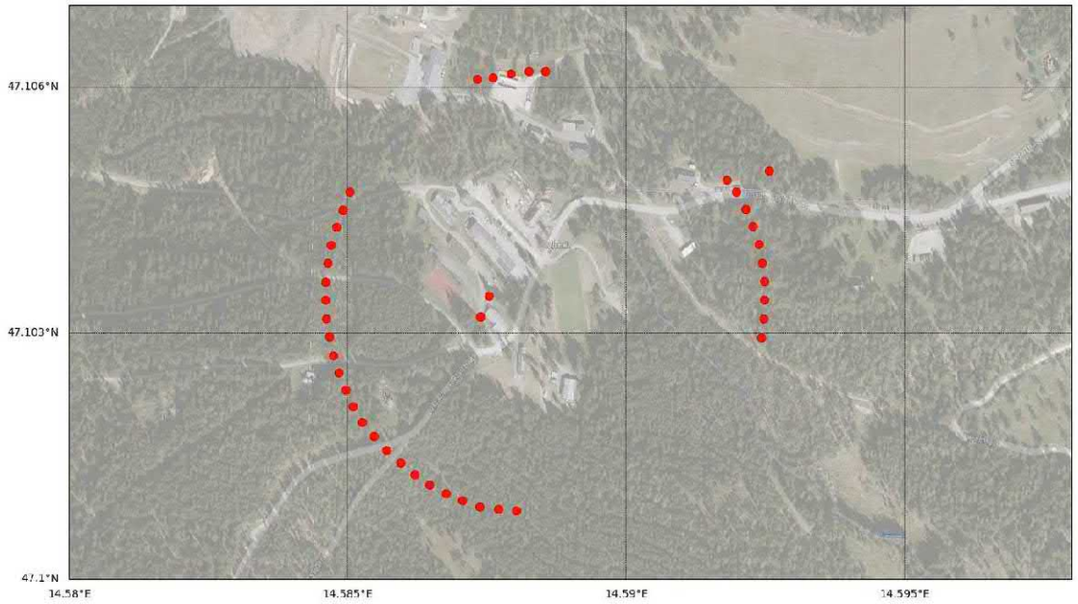
The possession and operation of jammers is illegal throughout the EU.

GNSS crop circles (3/3)

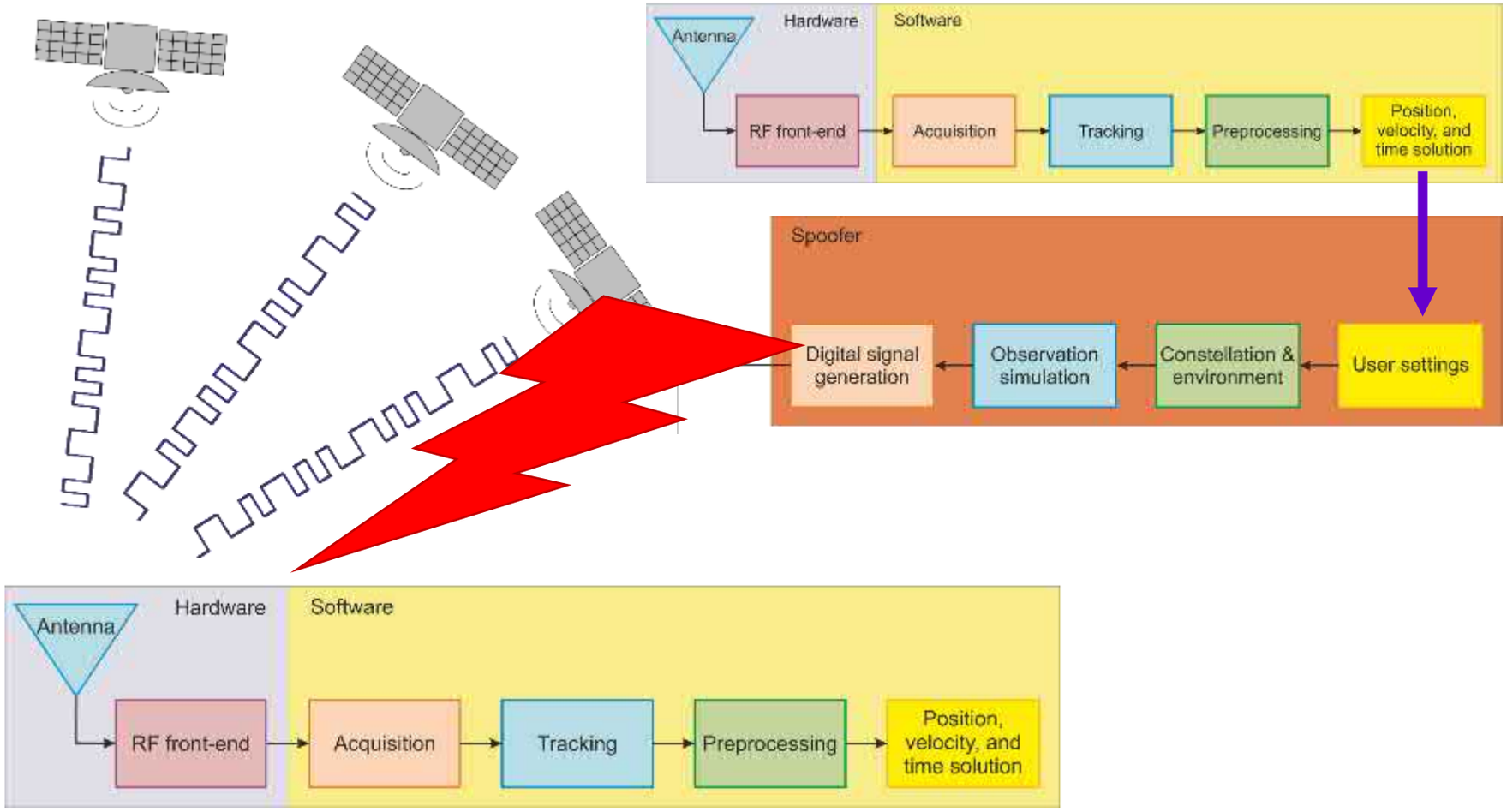
- Test campaign at TÜPl Seetaler Alpe
  October 2024







Intermediate spoofing attack



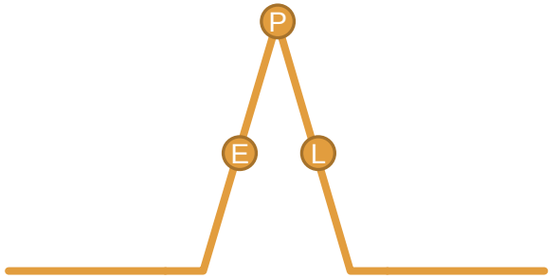
Spoofing prerequisites (1/2)

- Successful spoofing requires
  - Take-over the receiver (tracking loops)
  - Movement control of the receiver
  - Requires sound knowledge and experience in GNSS
    - Sophisticated algorithms
    - Signal generation capabilities

- Low-cost receivers are more vulnerable than high-end receivers
- Most reported spoofing attacks were achieved in close vicinity of the victim receiver (< 150 m)

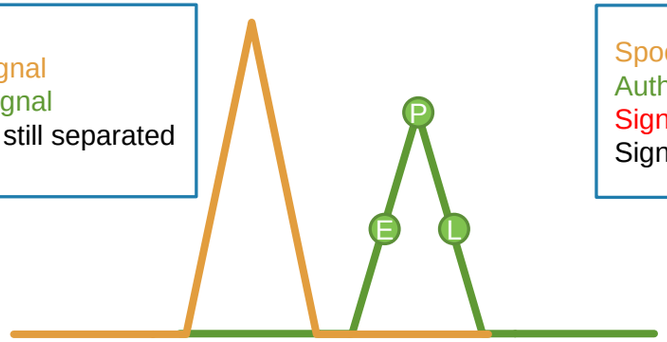
Spoofing prerequisites (2/2)

- Take-over the signal
  - Correlation peak
    - Receiver monitors discrete points (early, prompt and late)
    - Prompt should be at the peak
    - Early and late should be equally (chip spacing)
    - Tracking loop (steers the replica)
  - Frequency
    - Each satellite signal has different Doppler (relative motion between SAT and RX)
    - Spoofing signal has to be on the right Doppler as well

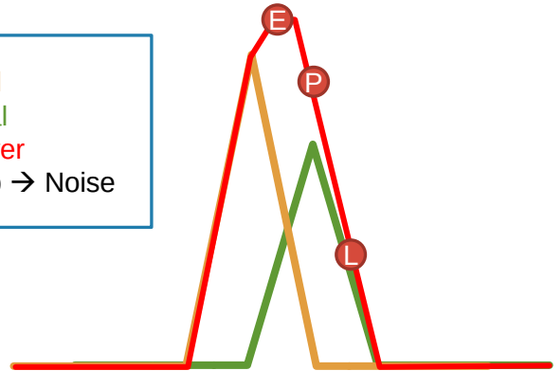


Take over correlation peak (example)

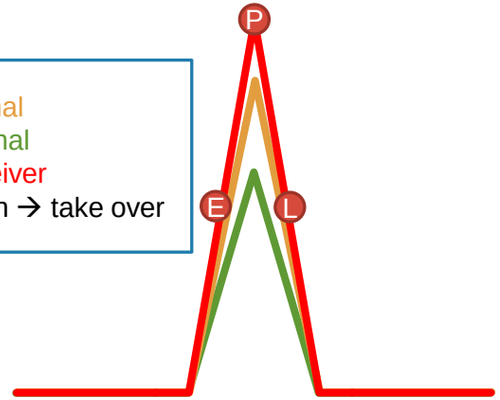
Spoofing signal
Authentic signal
Signals are still separated



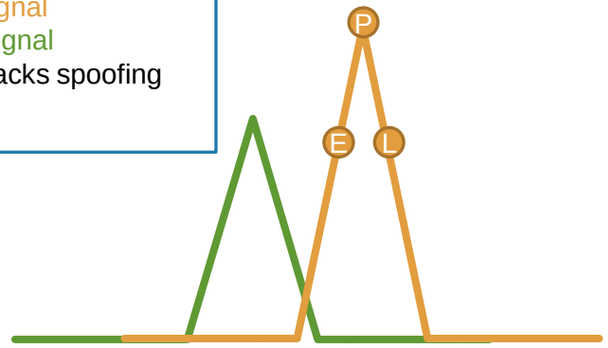
Spoofing signal
Authentic signal
Signal in receiver
Signals overlap → Noise

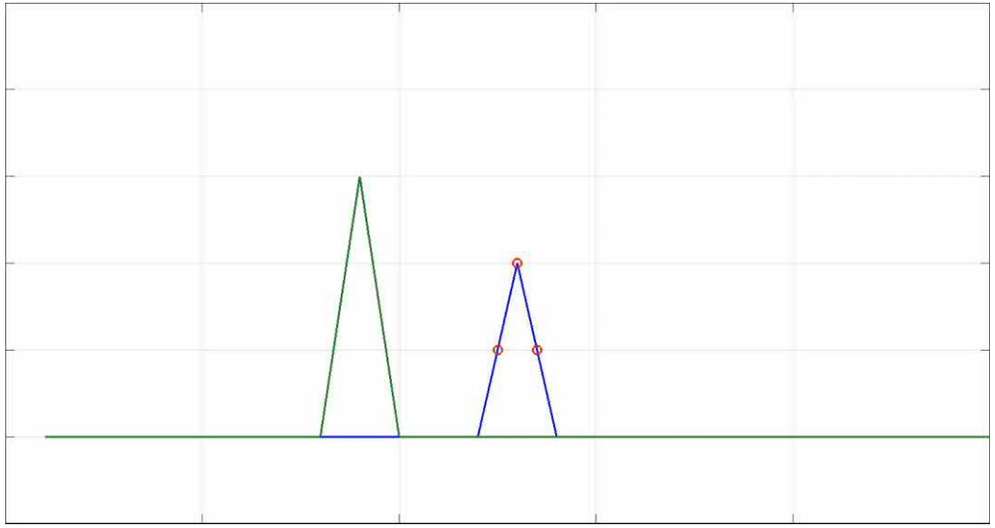


Spoofing signal
Authentic signal
Signal in receiver
Signals match → take over



Spoofing signal
Authentic signal
Receiver tracks spoofing signal





A-synchronous spoofing

- A-synchronous spoofing
  - Spoofing signals are not synchronized (in time) with the authentic ones
  - Spoofing signals are transmitted with high power and force the victim receiver to loos lock → re-acquisition

- Advantages
  - Very easy and cheap

- Disadvantages
  - Easy to detect
  - Success rate limited
  - Different satellites might be visible (no actual ephemeris data used)

Synchronous spoofing

- Spoofing attacks need to be synchronized with the GNSS signals
  - Failing to do so will let the spoofer act as a jammer and cause a loss of lock
  - Spoofing signal needs to be aligned within ½ chip length in case of GPS L1 C/A
    - Recall: 1 chip ≈ 300 m
  - Actual ephemeris data needed → e.g. reference receiver
  - Synchronization with GNSS time required → e.g. reference receiver

- Accurate knowledge of victim receiver required
  - Satellite orbits of all available satellites at the victim receiver
  - Doppler of all satellites at the victim receiver
  - Position and velocity of the victim receiver
  - Victim receiver performance parameters (tracking capabilities, algorithms)

How to deal with spoofing?

- Awareness is the key
- Successful detection is a pre-requisite for mitigation
- Spoofing detection methods
  - Signal power monitoring
  - Carrier-to-noise ratio monitoring
  - Carrier phase / Doppler variations
  - Correlation peak monitoring
  - Angle of arrival / multi-antenna array
  - Monitoring position, velocity and time output
  - External sensors (e.g. inertial measurement units)

Anti-spoofing techniques overview

- Software solution
  - Amplitude discrimination
  - Time-of-arrival discrimination
  - Vestigial signal defence

- Hardware solution
  - Consistency of navigation IMU cross-check
  - Polarization discrimination
  - Angle-of-arrival discrimination

- System-wide solution
  - Cryptographic authentication

Anti-spoofing techniques - Software

- Amplitude discrimination
  - Identification of jumps in amplitude and signal-to-noise ratio
- Time-of-arrival discrimination
  - Identification of clock-offsets caused by unsynchronized attacks
- Vestigial signal defence
  - Check for remaining genuine GNSS signals
  - Transmission of a suppressor signal requires centimetre-level knowledge of the relative vector between spoofer and target
- Amplitude and time-of-arrival discrimination are only effective against the most simplistic spoofing attacks

Anti-spoofing techniques - Hardware

- Consistency of navigation IMU cross-check
  - Cross-check of GNSS and IMU solutions
  - IMU measurements will most likely differ from GNSS positions
  - Inertial measurement unit required

- Polarization discrimination
  - Comparison of the polarization of spoofing and genuine signal
  - Spoofer may send out signals with different polarization

- Angle-of-arrival discrimination
  - Authentic signals will arrive from different directions
  - Spoofed signals will most likely arrive from a single direction
  - Array antennas required to check directions

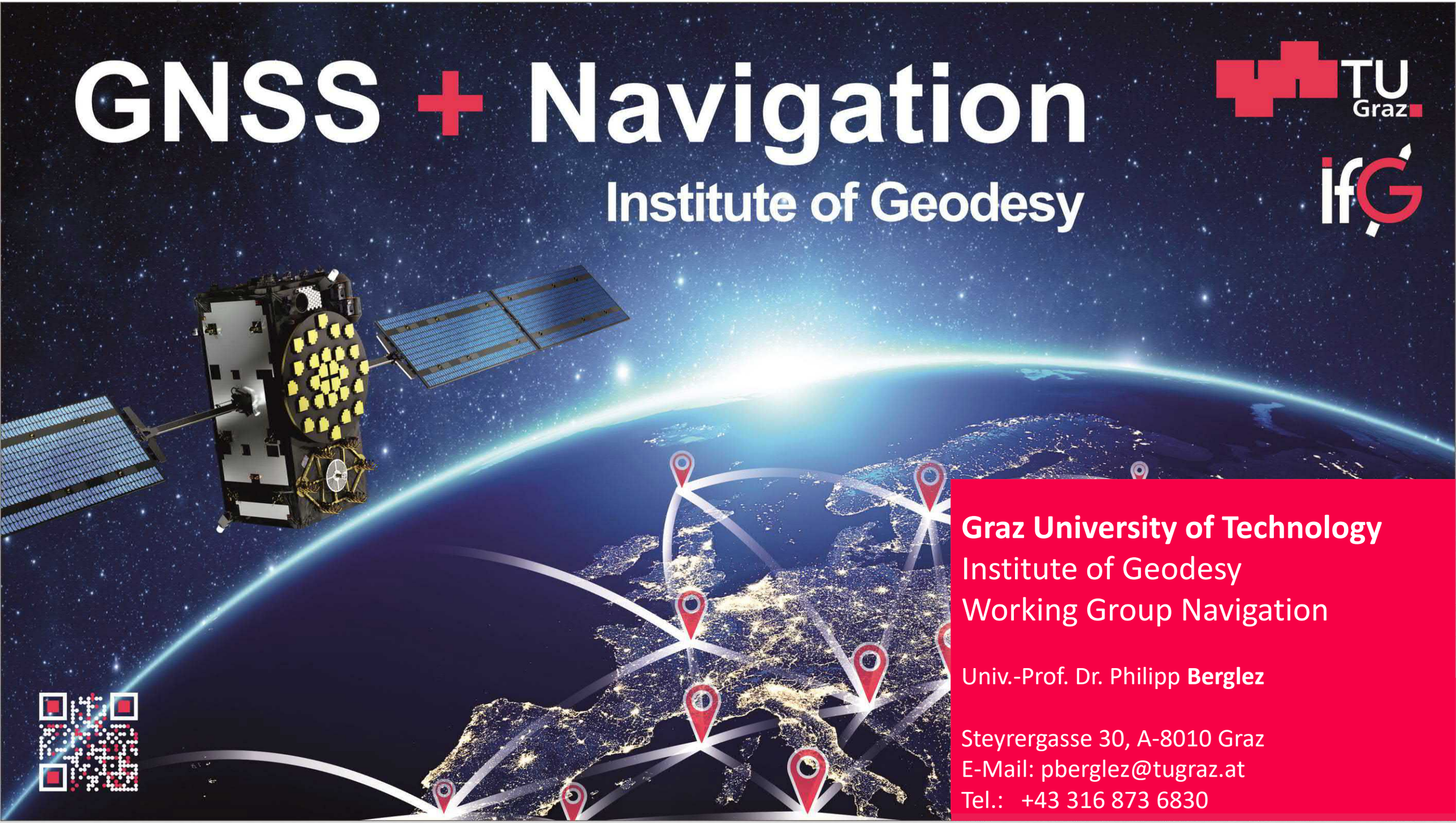
Anti-spoofing techniques - System-wide

- Some cryptographic authentication techniques
  - Navigation Message Authentication (NMA)
  - Public Spreading Code Authentication (PubSCA)
  - Private Spreading Code Authentication (PrivSCA)
  - Navigation Message Encryption (NME)
  - Spreading Code Encryption (SCE)

- GNSS encryption examples
  - GPS military P-code
  - Galileo Open Service Navigation Message Authentication (OSNMA)
  - Galileo Public Regulated Service (PRS)
  - Galileo Signal Authentication Service (SAS)

GNSS + Navigation

Institute of Geodesy



Graz University of Technology
Institute of Geodesy
Working Group Navigation

Univ.-Prof. Dr. Philipp **Berglez**

Steyrergasse 30, A-8010 Graz
E-Mail: pberglez@tugraz.at
Tel.: +43 316 873 6830