ISTA INSTITUTE OF SPACE TECHNOLOGY & SPACE APPLICATIONS

Universität der Bundeswehr München

GNSS Enhancement in hazardous Environments

9th ICG Meeting, Prague
ICG WG-B: Enhancement of GNSS Services Performance

Elias Gkougkas, Roland Bauernfeind, Thomas Kraus, Bernd Eissfeller

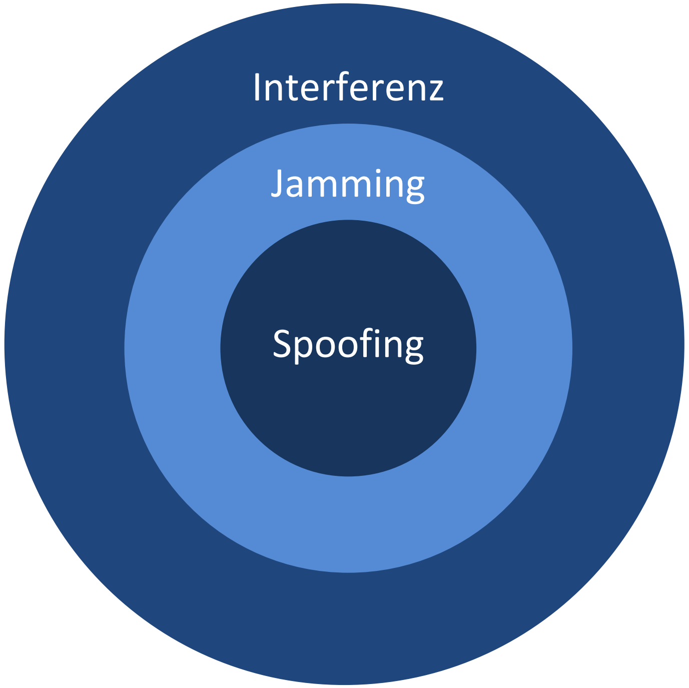
ISTA – Institute of Space Technology and Space Applications
University FAF Munich

Overview

- GNSS Interference
- Interference in Vehicle Applications
- Mitigation Techniques
    - Exploiting Polarization
- Conclusions

GNSS Interference

- Interference
  - Signal overlay on the GNSS signals causing degradation of the receiver's functionality (harmonics, intermodulation products, etc.)
- Jamming
  - Intentional transmission of signals, which are superimposed to GNSS signals with the aim of denying the position determination
- Spoofing
  - Transmission of almost identical GNSS signals with the aim of manipulating the position estimation of a receiver



GNSS Interference

Examples

- Interference
  - Television transmitters' harmonics
  - Light-Squares
- Jamming
  - Matched-spectrum jammer
  - Noise jammer
- Spoofing
  - Repeaters
  - Sophisticated Spoofers (receiving the GNSS Signal and transmitting it with a slightly code delay offset)

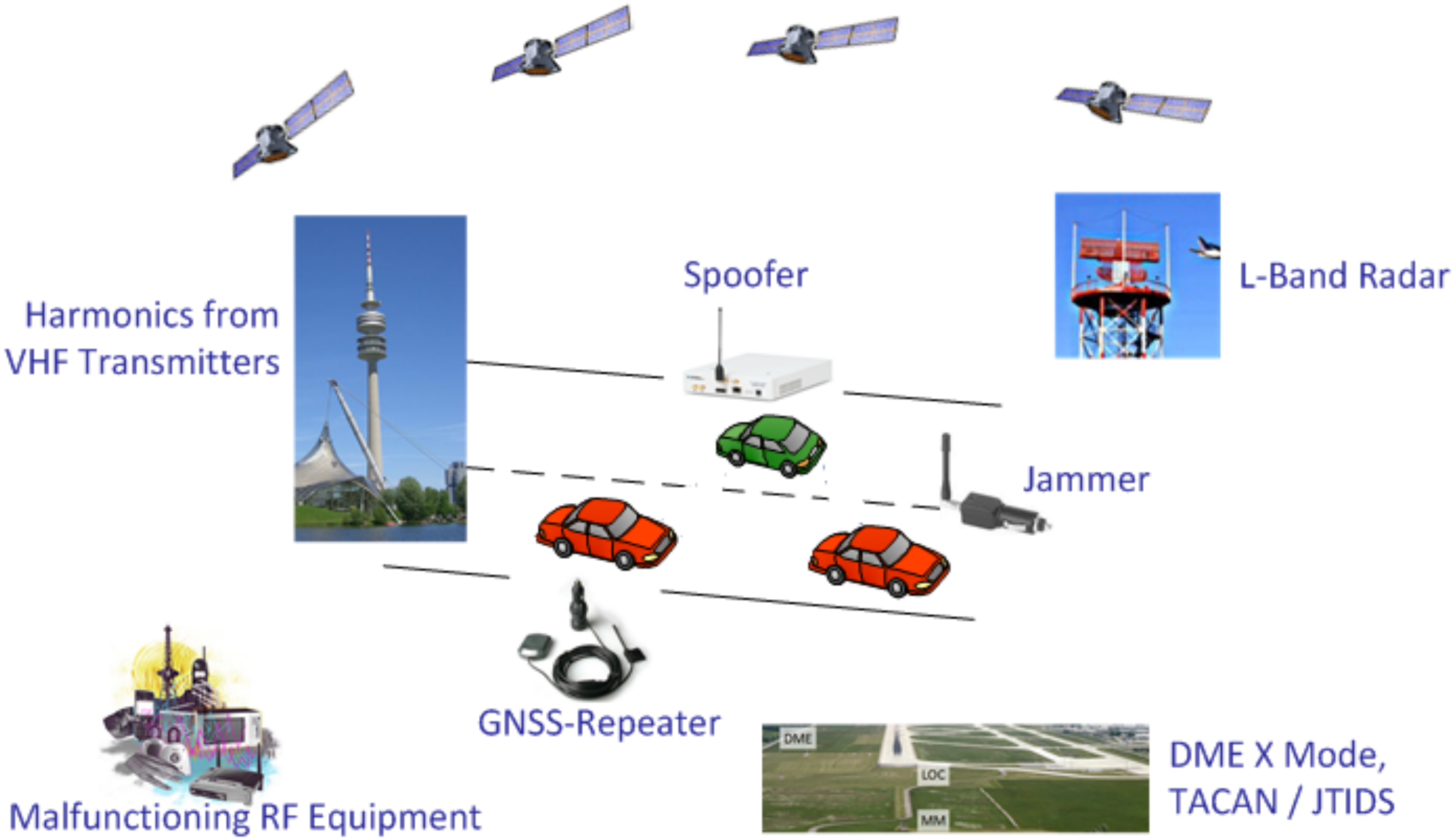
Interference in Vehicle Applications

Vehicular applications

- Distance based Road User Charging
  - for the first time in the world, a GPS-based road user toll system for heavy trucks has been put operational in Germany. Here the GPS position is used to detect road segments upon which the road toll is calculated
- Pay as You Drive Insurance
  - vehicle insurance fee is calculated based on driven mileage as well as driving behavior
- Access Control
  - to allow special purpose vehicles which have restrictions due to their increased size or mass to operate on a limited road network in order to protect road infrastructure, such as bridges, culverts and pavements
- Digital Tachograph
  - liability critical / legally binding recording of commercial truck driver hours. Snapshot position of start and stop point as well as hourly waypoints

Interference in Vehicle Applications

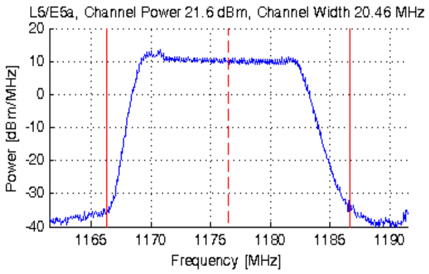
Hostile environment

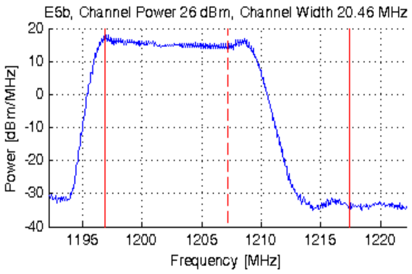


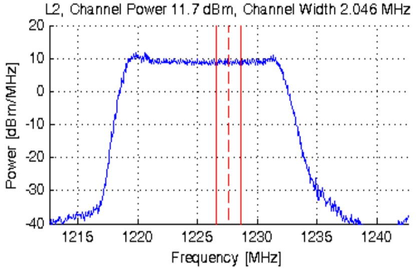
Interference in Vehicle Applications

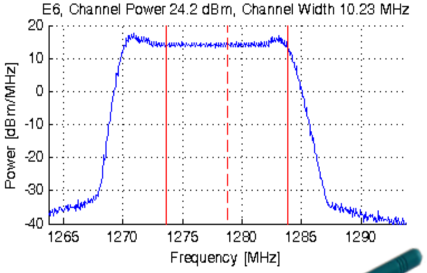
GNSS jammers

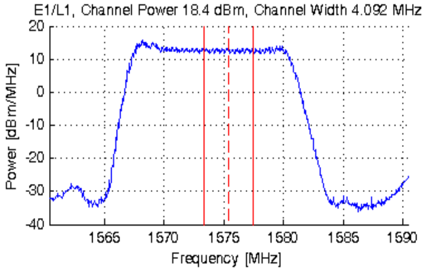
- Denial of GNSS positioning for privacy protection, vehicle theft, police electronic bracelets, etc.
- Observed Jammer Characteristics
  - Chirp signals (few continuous wave signals)
  - Bandwidth 10 – 40 MHz
  - Sweep Time 10 – 20 µs
  - Transmitted power > -20 dBm
- According to transmitted power, jammers affect not only the targeted vehicle GNSS receiver but also vehicles in their vicinity

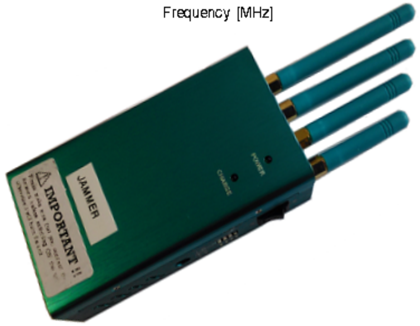








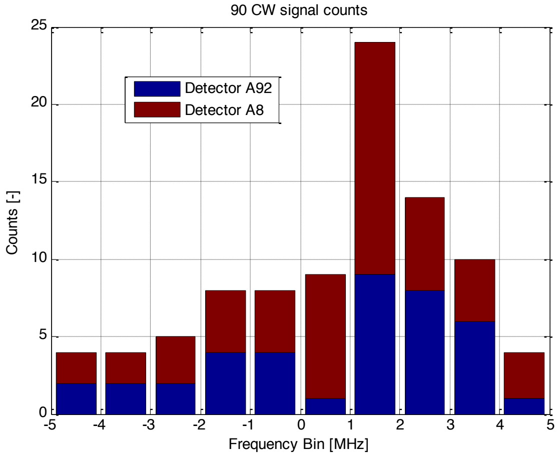




Interference in Vehicle Applications

Measurement campaign in Munich

- Two measurement sites on highway gantries in the area of Munich
- Record IF-Sample Snapshots for further investigation
- Around 6 events per week (L1/E1 band)
  - A8: 54 evens in 64 days
  - A92: 40 events in 48 days
- 90 CW signals, 4 chirp signals
- Power levels of recorded interference events were in a range of [-10, 0] dBm



Interference in Vehicle Applications

Detection coverage consideration (1)

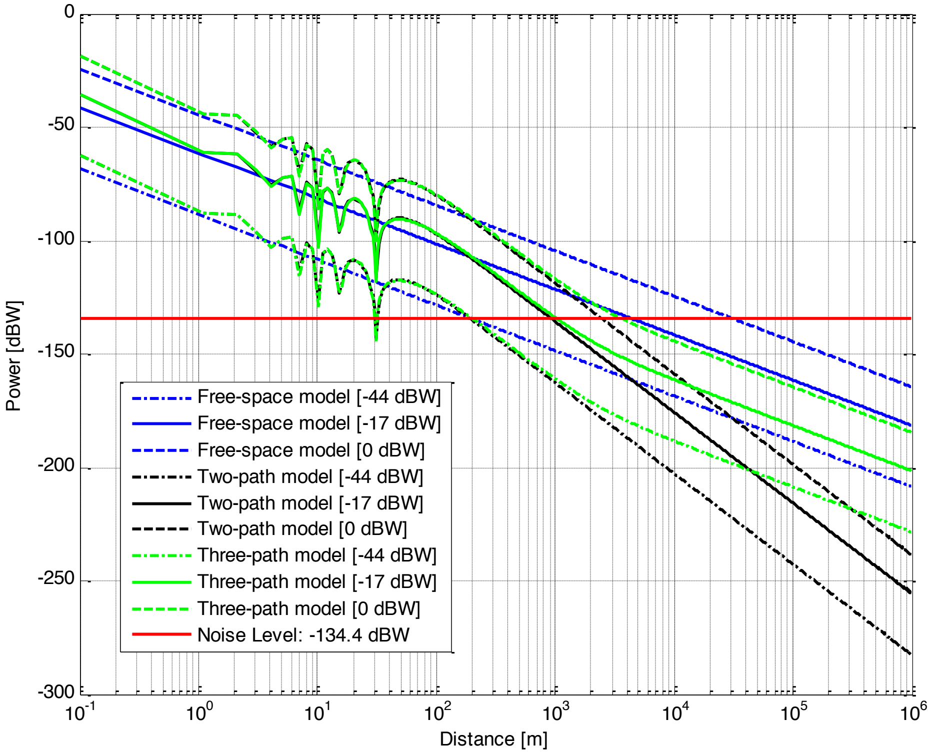
- Detection could be based on reference station networks

- Reference station networks (Germany)
  - IALA DGPS (7)
  - SAPOS (273)
  - EGNOS (1)
  - IGS (9)

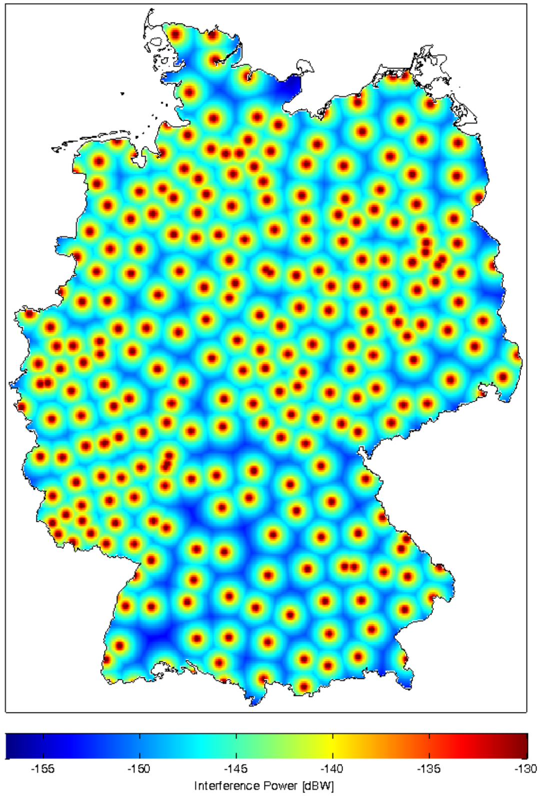
Interference in Vehicle Applications

Detection coverage consideration (2)

- L1/E1 band with 4.092 MHz reference bandwidth
- 3 power levels, 3 propagation loss models



- 17 dBW (free-space loss)
For each grid point the received power at the closest reference station

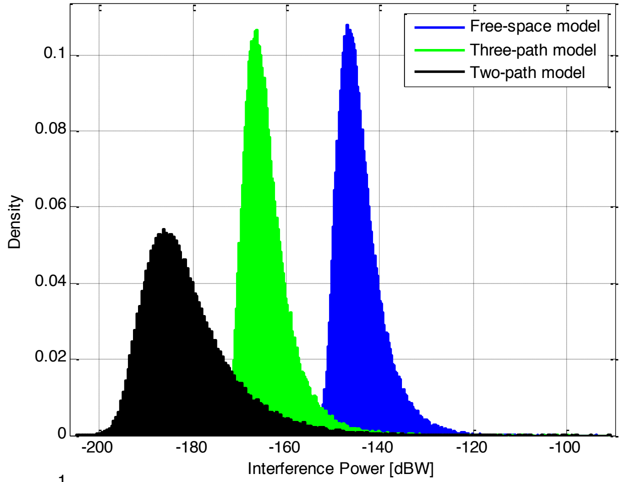


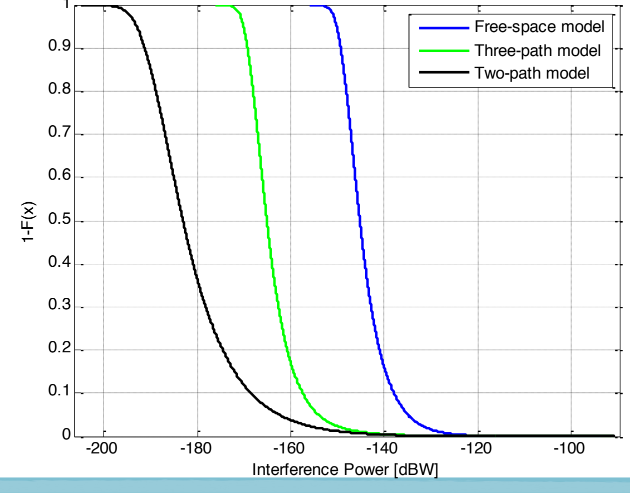
Interference in Vehicle Applications

Detection coverage consideration (3)

- Histogram over all grid points for the three propagation models
- Survivor function of received interference power (from grid points)
- Percentage of Germany that is covered:

Propagation Models	**Coverage -17 dBW**	Coverage 0 dBW
Free-space loss	**4,6 %**	98 %
Two-path loss	**0,2 %**	1,4 %
Three-path loss	**0,25 %**	3,1 %

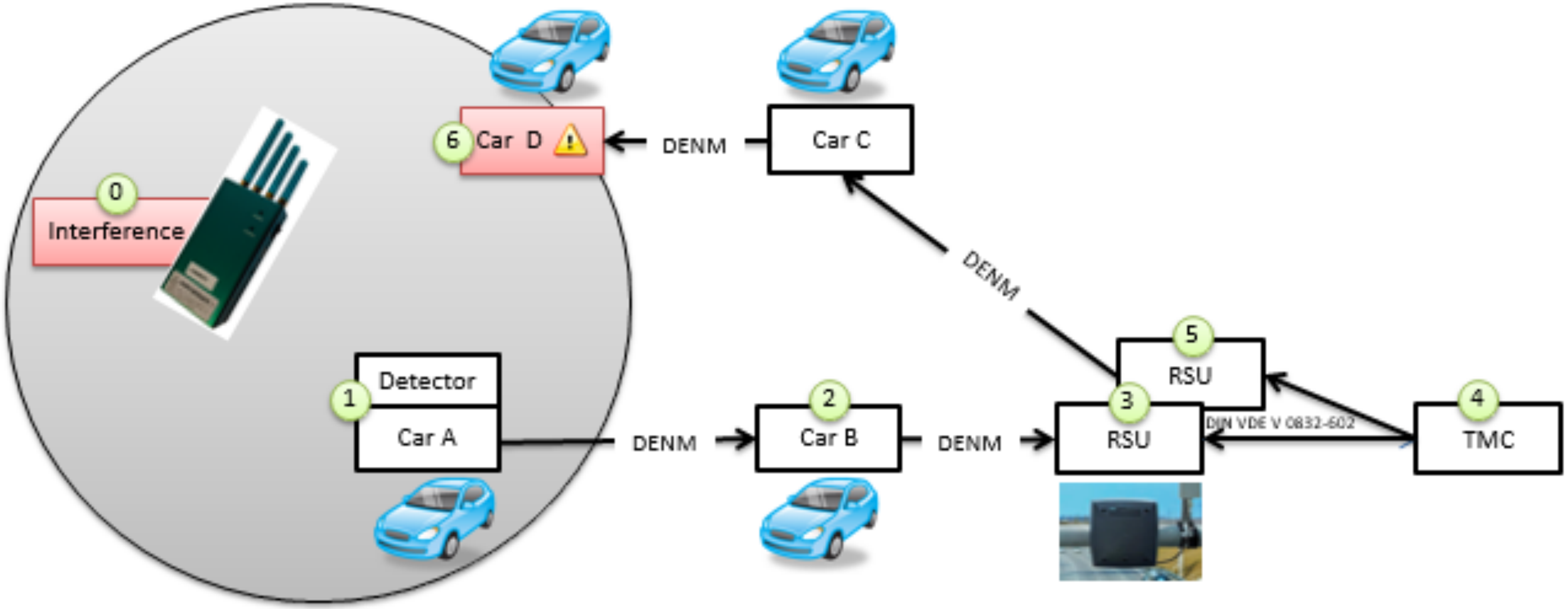




Interference in Vehicle Applications

Information Exchange – V2V/V2I

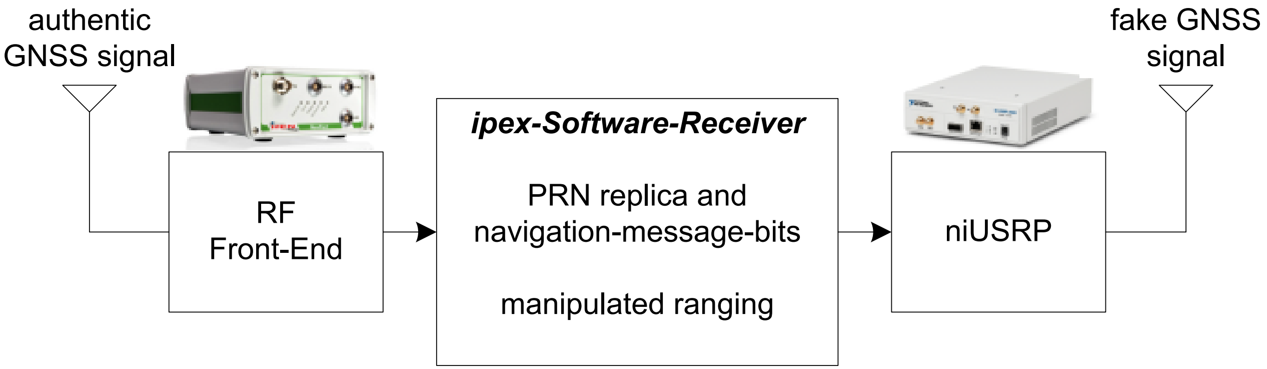
- Decentralized Environmental Notification Messages (DENM)



Interference in Vehicle Applications

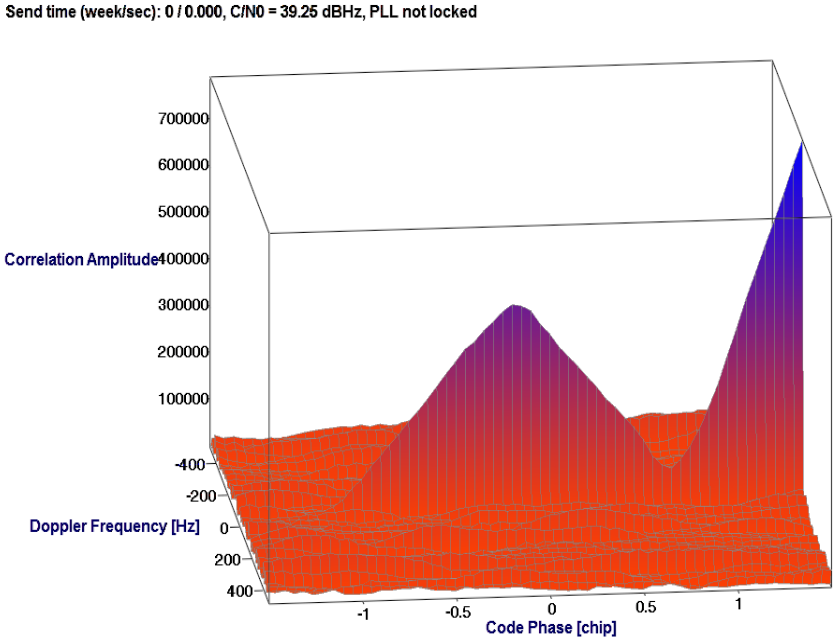
Spoofing Threat

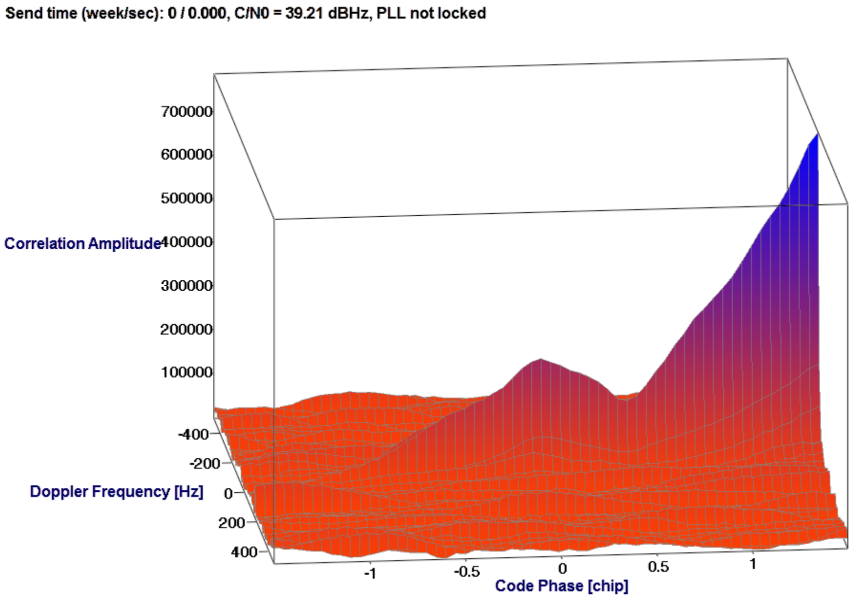
- Direct or manipulated re-broadcast of navigation signals for fraud against distance-based insurance and toll systems, police electronic bracelets, Geo-fence, etc.
- For an ideal spoofing attack an exact alignment of the fake signal with the authentic signal is necessary
- Unprotected receivers can be captured by initiation with a jamming attack or sweeping over the code and Doppler range with increased signal power



Interference in Vehicle Applications

Spoofing Threat – Example (not synchronized)

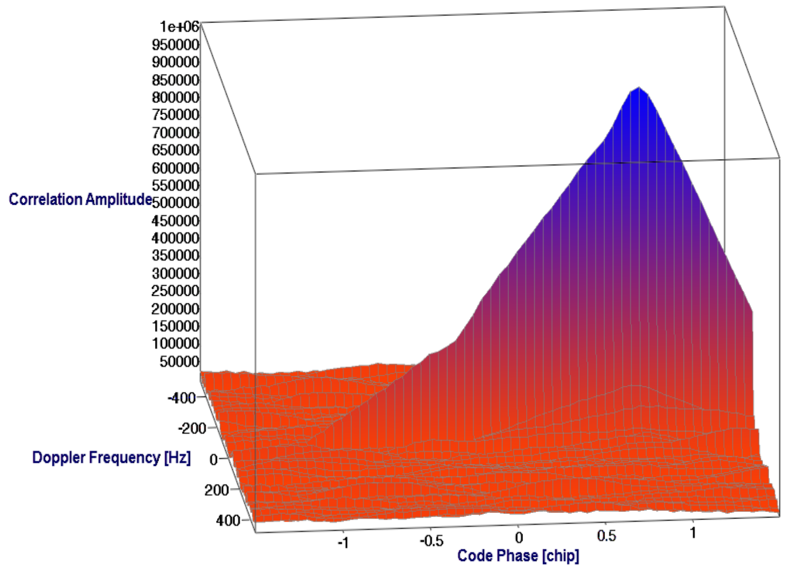




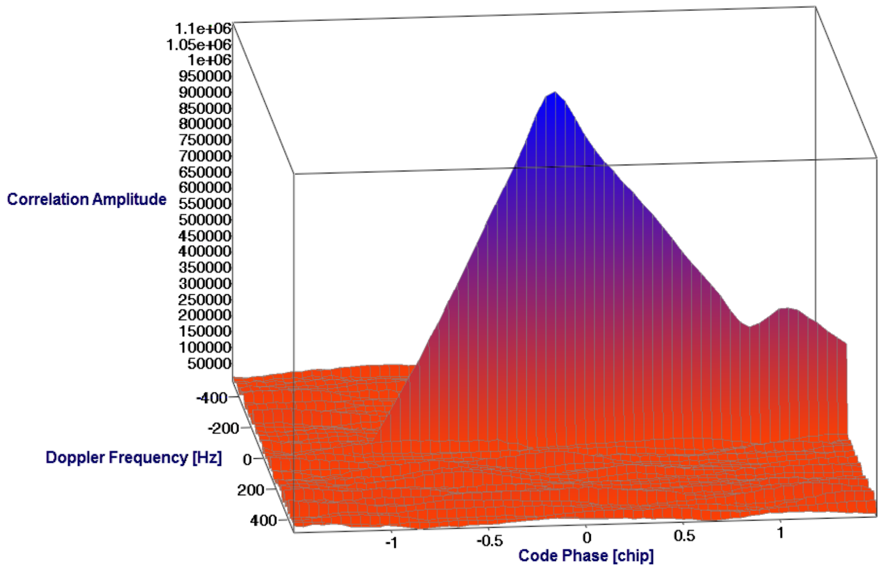
Interference in Vehicle Applications

Spoofing Threat – Example (not synchronized)

Send time (week/sec): 0 / 0.000, C/N0 = 39.12 dBHz, PLL not locked



Send time (week/sec): 0 / 0.000, C/N0 = 48.36 dBHz, PLL not locked



Mitigation Techniques

- Automatic Gain Control (AGC)
- Transformation based methods
  - Fast Fourier Transformation (FFT)
  - Short Time Fourier Transformation (STFT)
  - Fractional Fourier Transformation (FrFT)
  - Wavelet Decomposition
  - Karhunen-Loeve Transformation
- Signal Tracking and Suppression
- Antenna Arrays (Beamstearing, Nulling)
- Exploiting Polarization

Mitigation Techniques

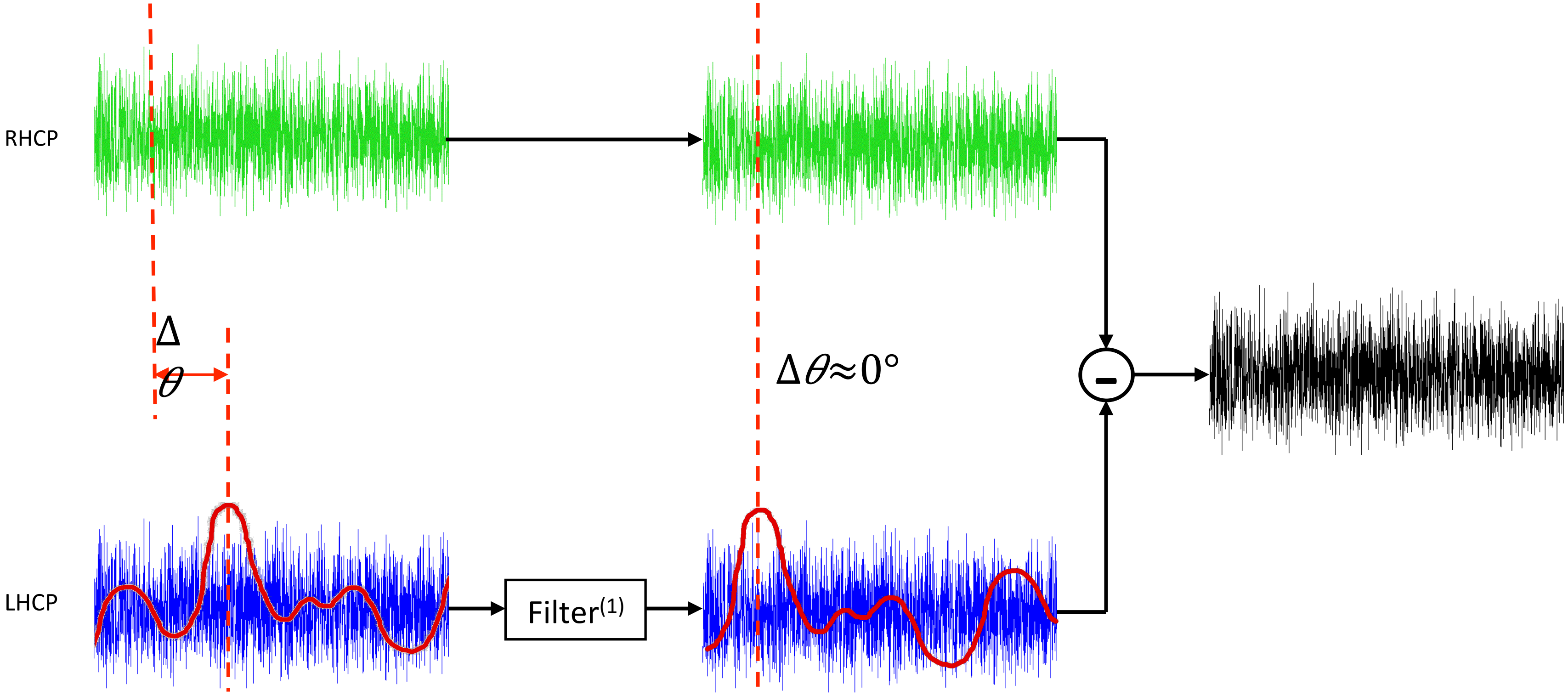
Exploiting Polarization

Concept: Distinguish GNSS Signals from other sources by exploiting signal polarization

Assumption: Jammer should be linear polarized

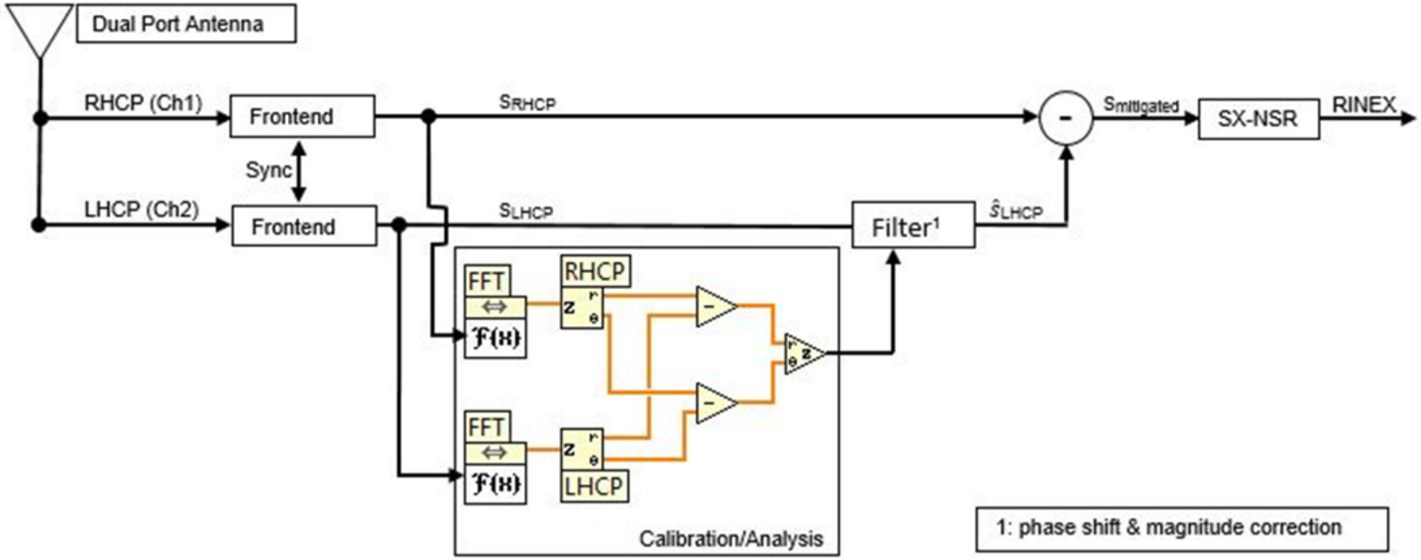
Mitigation Techniques

Exploiting Polarization – Simplified Explanation



Mitigation Techniques

Exploiting Polarization – Implementation Scheme



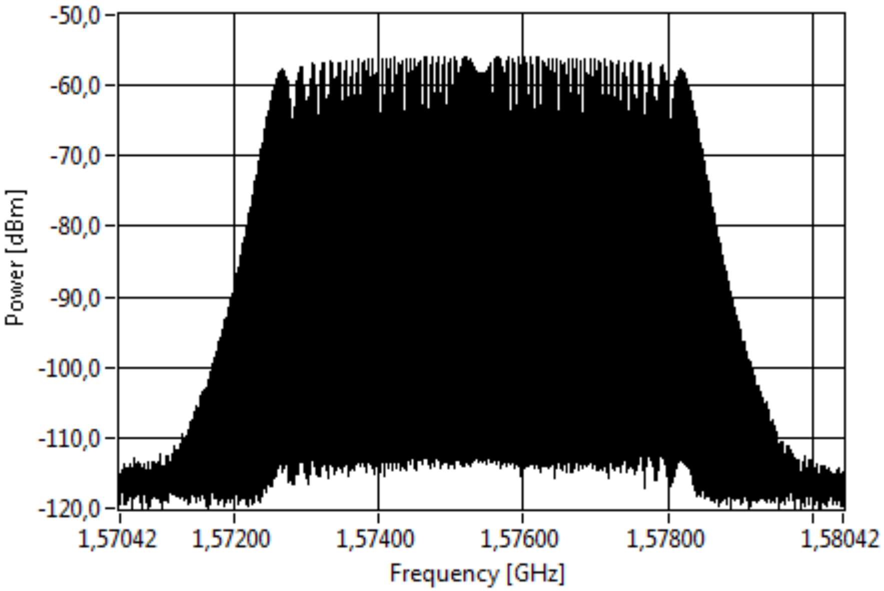
General tasks of the Calibration and Filter

- To align the phase of the frontends (from phase-coherent to phase aligned)
- To shift the phase of the LHCP signal so that the phase of the interference is equal in both channels (RHCP and LHCP)
- To correct the amplitude (error sources: antenna, LNAs, RF-FEs, ..)

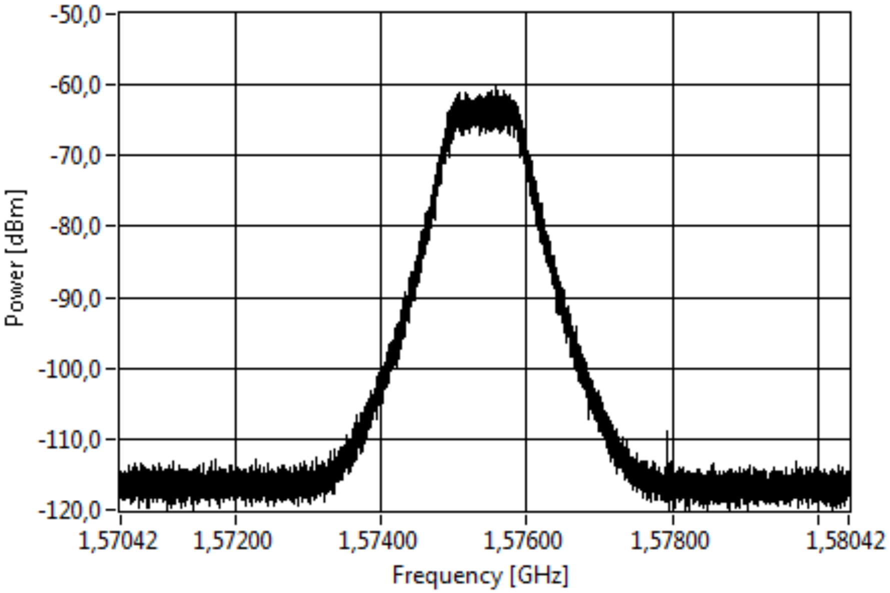
Mitigation Techniques

Exploiting Polarization – Analyzed Jammer

- **PPD Signal**
  - Chirp signal
  - BW= 6 MHz
  - Sweep Time= 6 µs



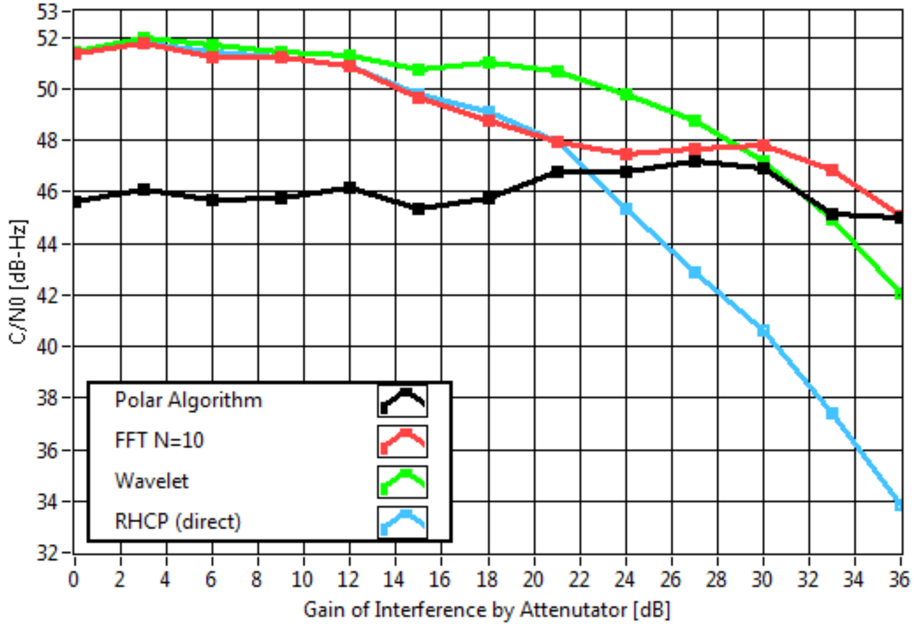
- **Filtered Noise Signal**
  - Pseudorandom noise generator
  - IIR Butterworth Filter
  - BW=1 MHz (3 dB)

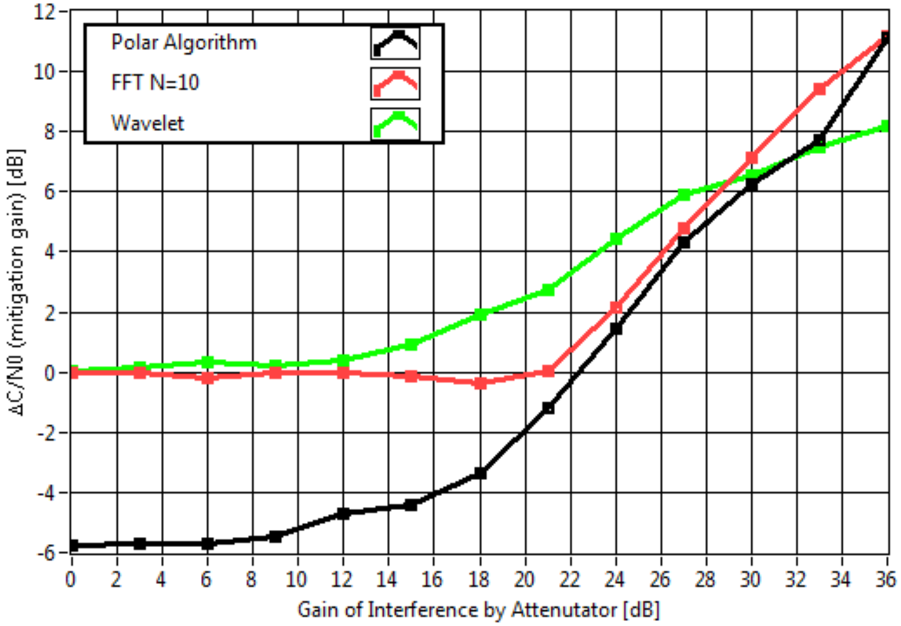


Mitigation Techniques

Exploiting Polarization-Results: GPS C/A

- Jammer Type: PPD
- Polarization algorithm can compete the FFT/STFT after J/N=5 dB (Gain of interference by attenuator = 22.5 dB)
- (-) Loss of 6 dB

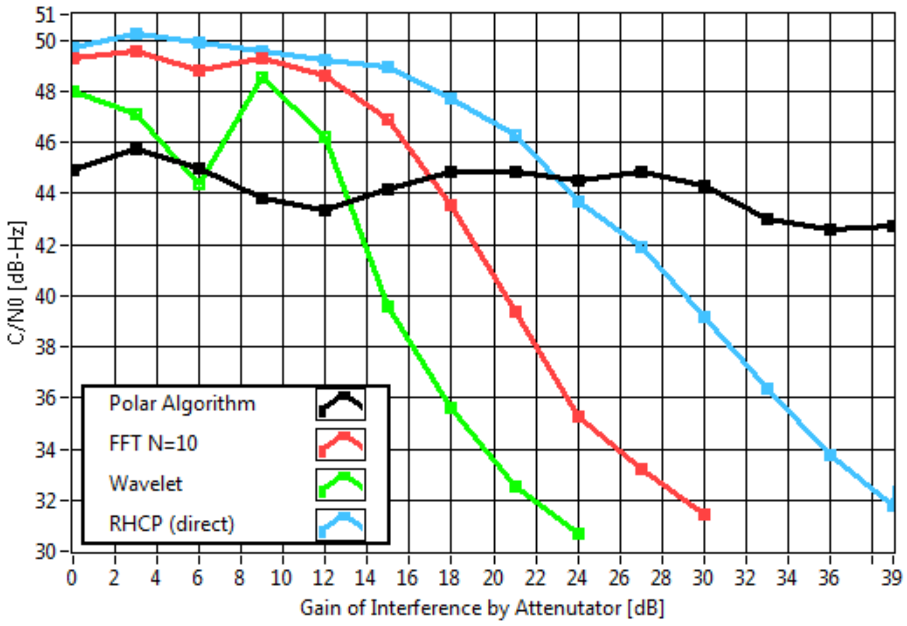


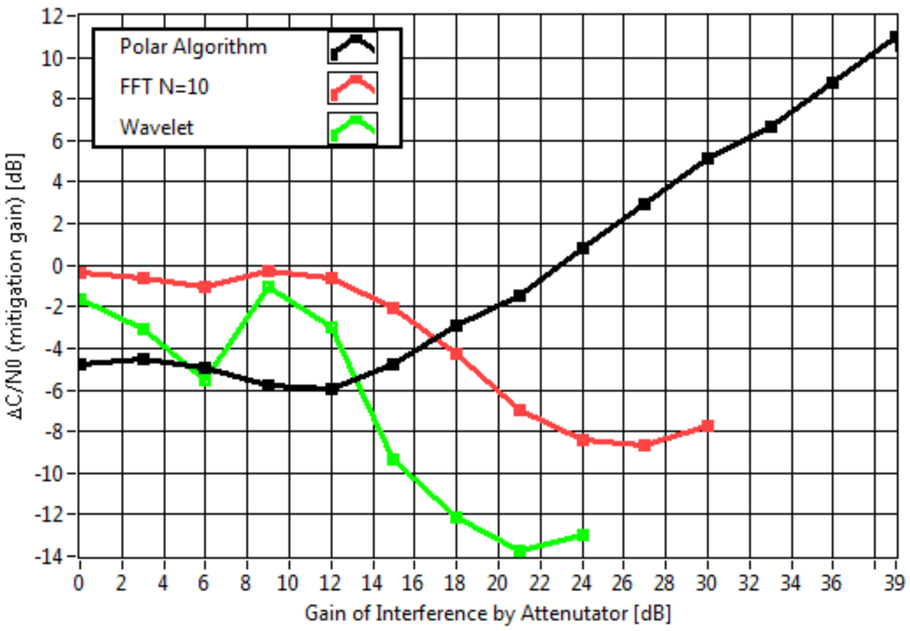


Mitigation Techniques

Exploiting Polarization-Results: GPS C/A

- Jammer Type: Noise
- Polarization algorithm is the only algorithm, which is able to mitigate noise after J/N=5 dB (Gain of interference by attenuator = 22.5 dB)
- (-) Loss of 6 dB

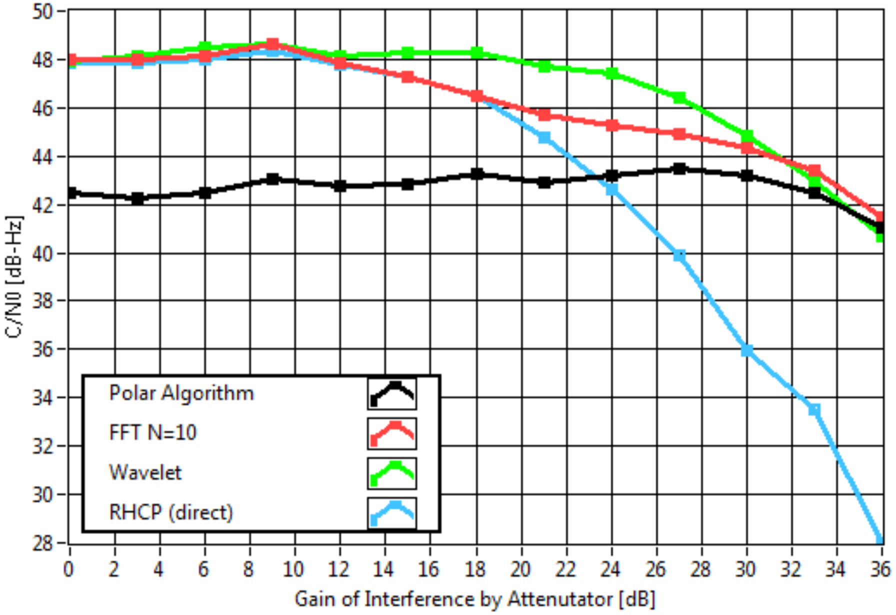


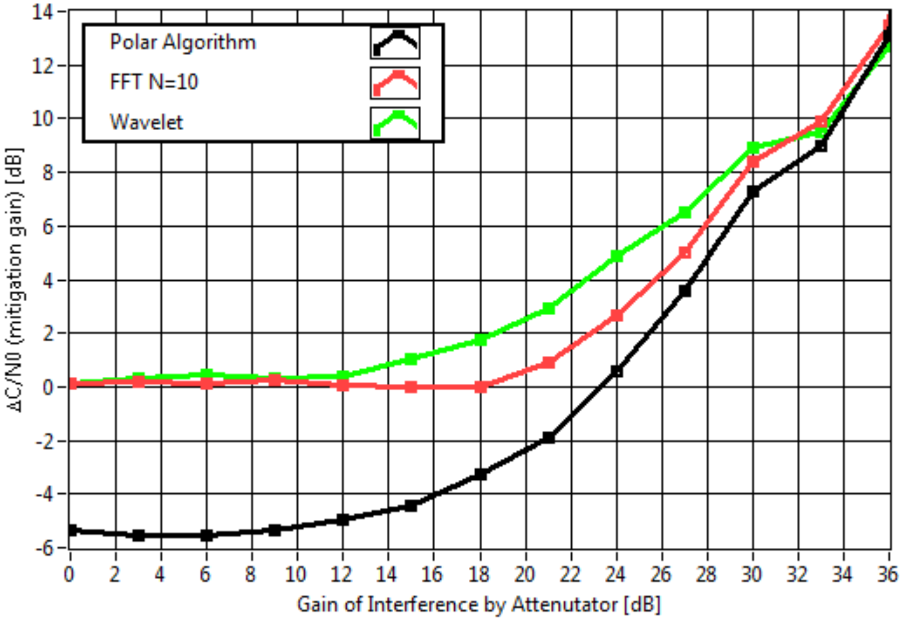


Mitigation Techniques

Exploiting Polarization-Results: Galileo E1 OS

- Jammer Type: PPD
- Polarization algorithm is the only algorithm, which is able to mitigate noise after J/N=14 dB (Gain of interference by attenuator = 33 dB)
- (-) Loss of 6 dB

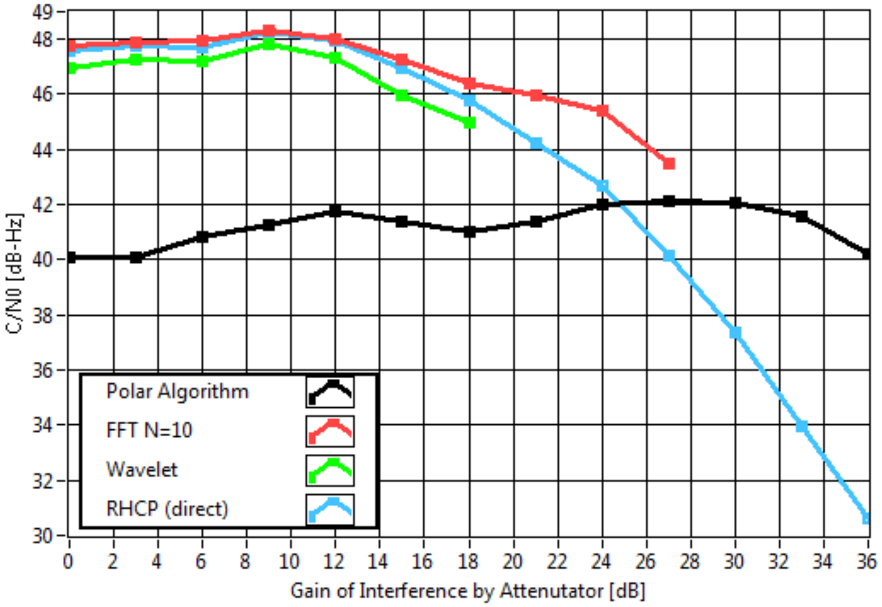


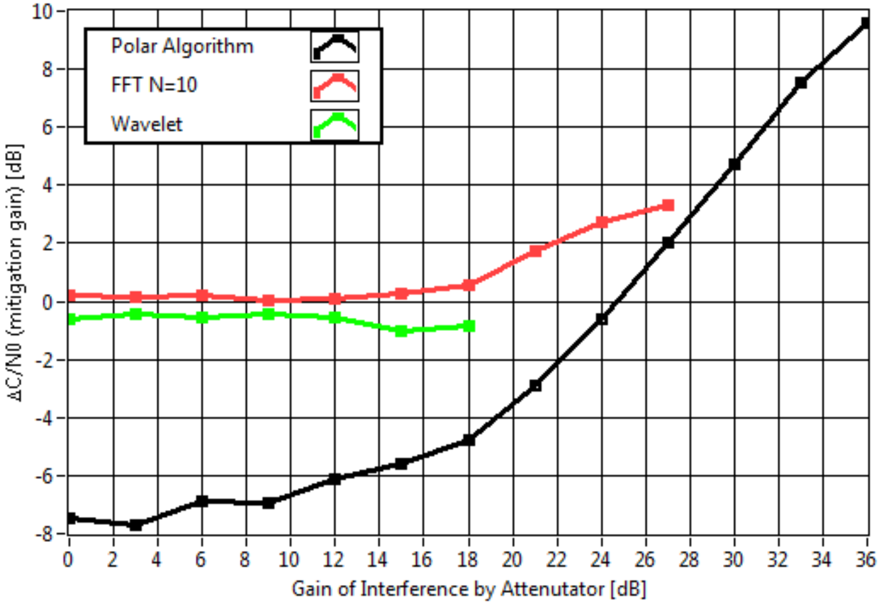


Mitigation Techniques

Exploiting Polarization-Results: Galileo E1 OS

- Jammer Type: Noise
- Polarization algorithm becomes effective after J/N=6 dB (Gain of interference by attenuator = 25 dB)
- (-) Loss of 7 dB





Conclusions

- Monitoring of interference and exchange of data is important to identify trends and react in time in vehicle applications
- Spoofing is becoming a threat (repeaters)
- Interference mitigation exploiting signal polarization has been demonstrated
  - Against chirp and noise signals
  - Competes with the transformation based methods but has a loss of 6 dB
- The signal polarization could also be used for anti-spoofing

Thank you for your attention!

Acknowledgments

The results presented were developed during the projects:

- **InCarITS II:** Interference Localization and Cooperative GNSS Signal Processing Algorithms for Intelligent Transport Systems, Grant No. 50NA1219
  Founded by: German Federal Ministry of Economics and Technology (BMWi) and administrated by the Project Management Agency for Aeronautics Research of the German Space Agency (DLR), Bonn
- **TERMINATE**: Interference Mitigation based on Novel Signal Processing and RF-Front-End
  Founded by: European Space Agency (ESA/ESTEC), Technical Officer: Francisco Amarillo Fernandez