Jamming and Spoofing of GNSS Signals – An Underestimated Risk?!

Alexander Rügamer — Fraunhofer IIS
Dirk Kowalewski — NavXperience GmbH

 1 Source: http://securityaffairs.co/wordpress/wp-content/uploads/2012/02/Spoofing.jpg

Fraunhofer IIS

Motivation
Applications of GNSS

- Since the last 10 years GNSS entered in many daily life applications…

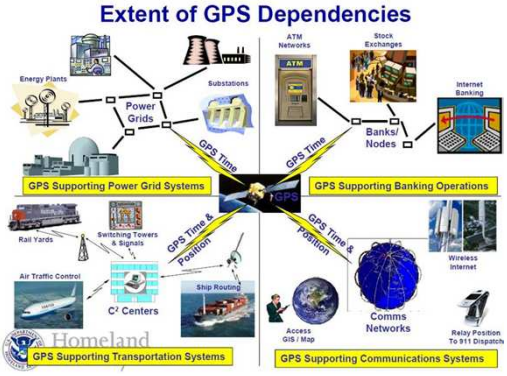
- Huge market
  - €270 billion GNSS revenue in 2015
  - Seven billion GNSS devices by 2022 – almost one for every person on the planet

 2 Source: GNSS Market Report – Issue 3, Oktober 2013

Fraunhofer IIS

Motivation
Applications of GNSS

- … and also in safety critical applications



- …all relying on the availability and functionality of GNSS

Source: http://www.insidegnss.com/auto/popupimage/GPS%20Dependencies_small.jpg

Fraunhofer IIS

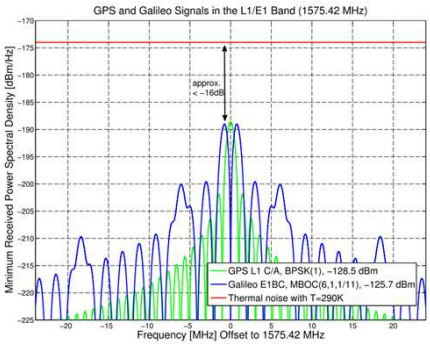
Content
Jamming and Spoofing of GNSS Signals – An Underestimated Risk?!

- GNSS Interference
  - Jamming
  - Spoofing
- Incidents
  - Jamming Attacks
  - Spoofing Attacks
- Counter Measures: Interference Detection and Mitigation
  - Array-Antenna Processing
  - Cryptographic GNSS Signals
- Conclusion

Fraunhofer IIS

GNSS Interference

- GNSS signals received on earth are very weak
  - Approx. -130 dBm received signal power
  - GNSS bands dominated by white noise, SNR typ. -15…-35 dB
- ➔ GNSS signals extremely susceptible to all types of interference:
  - Unintentional: harmonics, co-operations with other services,…
  - Intentional: Jammers and Spoofers



 5

Fraunhofer IIS

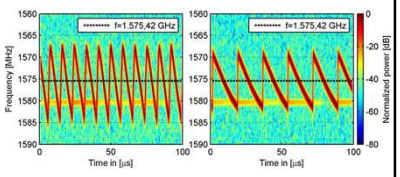
GNSS Interference
Jamming

- Denial of service attack
- Military jammers
  - "Friendly jamming"
  - Disabling of civilian GNSS while keeping military services intact
- Personal or Privacy Protection Devices (PPD)s
  - Sold over the internet starting at 30€
  - Usage is illegal in almost every country
- 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

 6

Fraunhofer IIS

GNSS Interference
Jamming - PPDs



- Characteristics:
  - Chirp output signal
  - Output power +12 dBm….+33 dBm
  - ➔ resulting in a J/S of >150 dB
- Jamming radius
  - Strongly depending on jammer height and environment
  - >100 m within cars/urban env.
  - up to 30 km at heights of 10 m
  - >100 km on weather balloons
- Advertised with
  "…protect the privacy of its user in a radius of at least 15 m..."
- Users often don't know the real impact…

 7

Fraunhofer IIS

Incidents
Jamming attacks

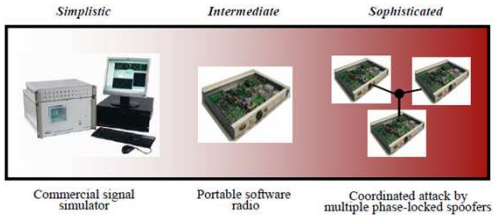
- FCC fines operator of GPS jammer that affected Newark Airport GBAS (2013)
  - But still several similar incidents a day
- Car-jammer monitoring campaigns:
  - Munich, Germany reported approx. 6 jamming incidents a week
  - London, UK is reported with 10 jamming incidents a day
- South Korea suffers heavy maritime GPS jamming from North Korea:
  - Within 16 days over 1000 planes and over 250 ships experienced GPS disruption

 8

Fraunhofer IIS

GNSS Interference
Spoofing

- Spoofing: transmission of fake GNSS signals with the intention of fooling a GNSS receiver into providing false Position, Velocity and Time (PVT)
- Different types of attacks
  - Meaconing: rebroadcasting a received signal
  - Simplistic attack
  - Intermediate attack
  - Sophisticated attack
- Spoofers exist:
  - SimSAFE from Spirent with GSS8000: >200k€
  - Proof-of-concept demonstrators



Humphreys et al., "Assessing the spoofing threat: Development of a portable GPS civilian spoofer", In Proceedings of ION GNSS 2008, Savannah, GA, 2008.

Fraunhofer IIS

Incidents
Spoofing attacks

- Iran - U.S. RQ - 170 incident
- "Iran military downs US spy drone". *Press TV*. 4 December 2011.
- "Obama appeals to Iran to give back downed US drone". *The New York Times*. 9 December 2011
- "Iran says captured US drone is their 'property' now". *The Daily Telegraph*. 13 December 2011.
- "Iran carries successful test flight of reverse engineered RQ-170". 10 November 2014.

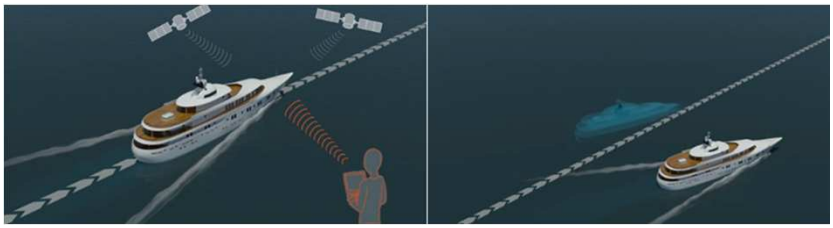
Lockheed Martin RQ-170 Sentinel

Fraunhofer IIS

Incidents
Spoofing attacks

- Successful demonstration of spoofing attack
  - on drone
  - on $80M Yacht
  - on time of power grid

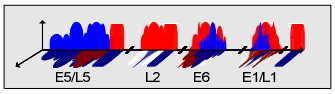
by Uni. of Austin, TX



Daniel P. Shepard, Jahshan A. Bhatti, T. E. Humphreys, and Aaron A. Fansler. "Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks". In Proceedings of ION GNSS 2012, Nashville, TN, September 2012, pp. 3591-3605., 2012.

Fraunhofer IIS

Counter Measures
Jamming



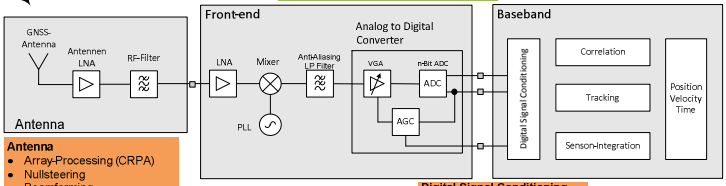
Detection

Mitigation

GNSS Signal
- Chip Rate
- Modulation
- Frequency band
- „Spot Beam"
- Encryption

Front-end
- Automatic Gain Control (AGC) variation monitoring
- ADC raw sample distribution

Correlator/Tracking
- Vector Delay-Locked-Loop
- C/N0 monitoring
- Code/Carrier consistency
- Step detections



Antenna
- Array-Processing (CRPA)
- Nullsteering
- Beamforming
- Direction of Arrival (DoA)
- Direction of Interference (DoI)

Digital Signal Conditioning
- Pulse-Blanking
- Adaptive Filtering
- Frequency Domain Adaptive Filtering (FDAF)

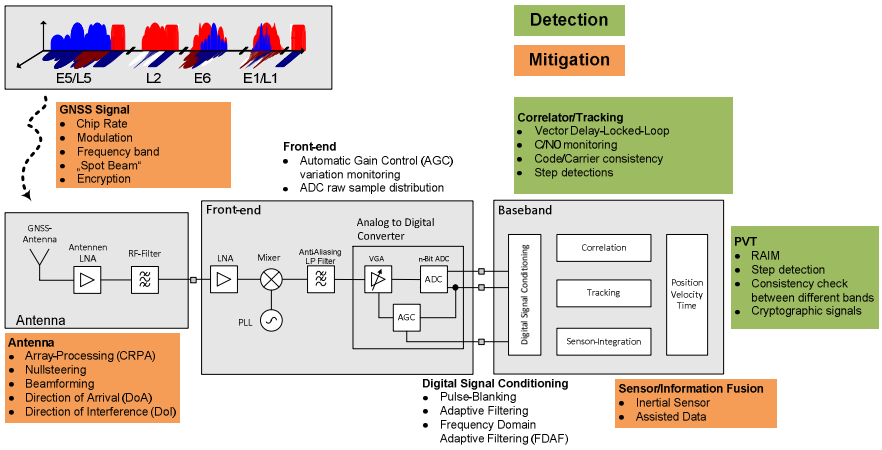
Sensor/Information Fusion
- Inertial Sensor
- Assisted Data

PVT
- RAIM
- Step detection
- Consistency check between different bands
- Cryptographic signals

 12

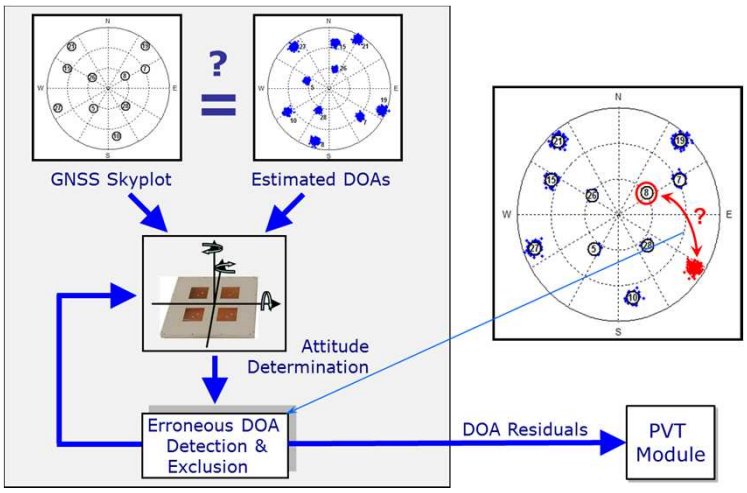
Fraunhofer IIS

Counter Measures
Spoofing



Fraunhofer IIS

Counter Measures
Array Antenna

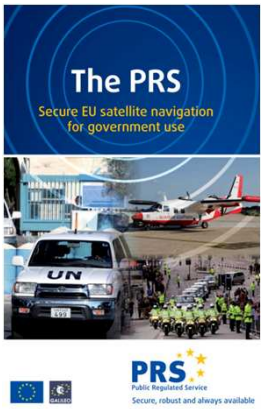


A. Rügamer et al, "BaSE-II: A Robust and Experimental Galileo PRS Receiver Development Platform." In ION GNSS+ 2014, September 8-12, Tampa, Florida, USA

Fraunhofer IIS

Counter Measures
Signals

- Cryptographic Techniques in Open GNSS
  - Public key infrastructure authentication elements or digital signatures in message
  - Under discussion for GPS L1C
- Galileo Public Regulated Service (PRS)
  - Strong encryption ➔ Anti-spoofing
  - Fully open to civil users
  - Key opener to many critical and demanding applications mostly in security related areas
  - Only protection against spoofing, not jamming



 15

Fraunhofer IIS

Conclusion

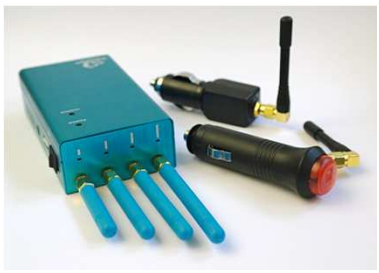
- GNSS service is often taken for granted
  - No real awareness of how fragile it is, despite many incidents
  - Most professional receivers do not detect jamming or spoofing events
  - Even though commercial jammers and spoofers are emerging
- Operators depending on GNSS should critically review their GNSS receivers
  - Upgrade to jamming and spoofing resilient receivers
  - … or at least to receivers that detect incidents and warn the users
  - Use cryptographically protected signals
- Spoofing resistant signal (like Galileo PRS) together with appropriate array antenna processing techniques seems to be the best protection against intentional GNSS interference available

 16

Fraunhofer IIS

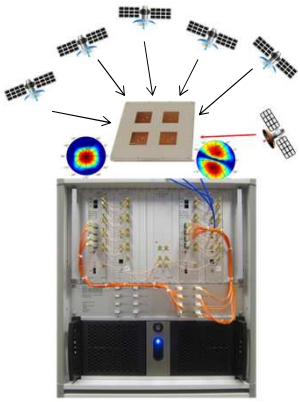
Questions?

alexander.ruegamer@iis.fraunhofer.de



Fraunhofer IIS

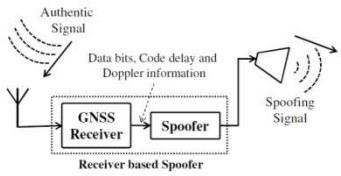
Backup
Bavarian Security Receiver (BaSE)
Demonstration of PRS with Anti-Spoofing and -Jamming

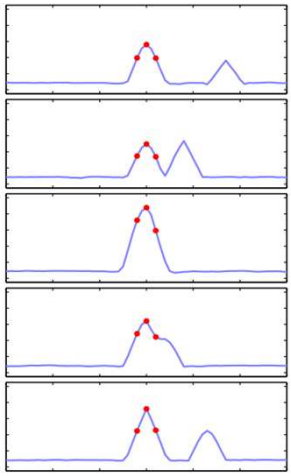


- Picture of "BaSE" (Bavarian Security Receiver)
  - 2x2 Array Antenna
  - Galileo PRS
  - Dual-Frequency
  - Interference detection and mitigation in
    - Time
    - Frequency
    - Spatial domain
- Developed by Fraunhofer IIS, Airbus, DLR, Siemens, IABG, NavCert

Fraunhofer IIS

Backup
Spoofing



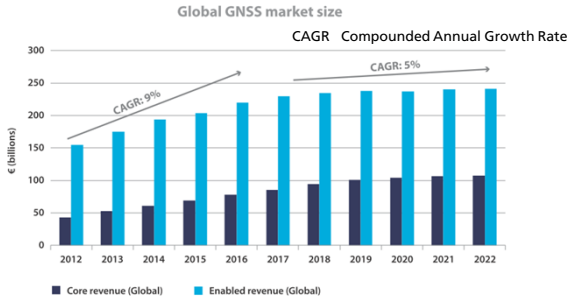


Todd E. Humphreys, Brent M. Ledvina, Mark L. Psiaki, Brady W. O'Hanlon, and Paul M. Kintner Jr. "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer." In Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008), Savannah, GA, 2008.

Fraunhofer IIS

Backup
Billion Dollar Market

- 200 billion € market in 2015
- Seven billion GNSS devices by 2022
  – almost one for every person on the planet



- Jamming and Spoofing of GNSS Signals – An Underestimated Risk?!

Source: GNSS Market Report – Issue 3, Oktober 2013

Fraunhofer IIS