Zentrale Stelle für Informationstechnik im Sicherheitsbereich

OTH OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

ZITiS

A Forensic Analysis of GNSS Spoofing Attacks on Autonomous Vehicles

Tobias Reichel, Mathias Gerstner, Leo Schiller,
Andreas Attenberger, Rudolf Hackenberg, Klara Dološ

IARIA

Zentrale Stelle
für Informationstechnik
im Sicherheitsbereich

OTH OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

ZITiS

Tobias Reichel

tobias.reichel@zitis.bund.de

- Master` s degree in Mathematics
- Researcher at ZITiS
- Focus on forensic of autonomous vehicles

Mathias Gerstner

mathias.gerstner@oth-regensburg.de

- Master` s degree in Applied Research (Data Science)
- Ph.D. Student CarSec-Lab at OTH Regensburg
- Research focus on automated vehicles communication

Leo Schiller

leo.schiller@oth-regensburg.de

- Master` s degree in Computer Science
- Ph.D. Student CarSec-Lab at OTH Regensburg
- Research focus is on automotive security

IARIA

Project DiForIT

- Development of a forensic process chain specifically for automated and connected road mobility.
- Evaluation of vehicle communication interfaces and network protocols to identify potential security risks.
- Assessment of the forensic relevance of collected vehicle data, considering technical, legal and regulatory factors.
- Implementation of robust data recording systems that ensure data security, integrity and privacy.

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

The Role and Vulnerabilities of Location Tracking Systems

Ubiquity of location-based technology

- Location tracking is essential in navigation, logistics, emergency response and more.
- Autonomy: SAE Level 3 (and higher) vehicles rely on GNSS for partial autonomy.

GNSS Jamming

- High-power interference signals
- Disrupts signal reception

  -> Loss of positioning

GNSS Spoofing

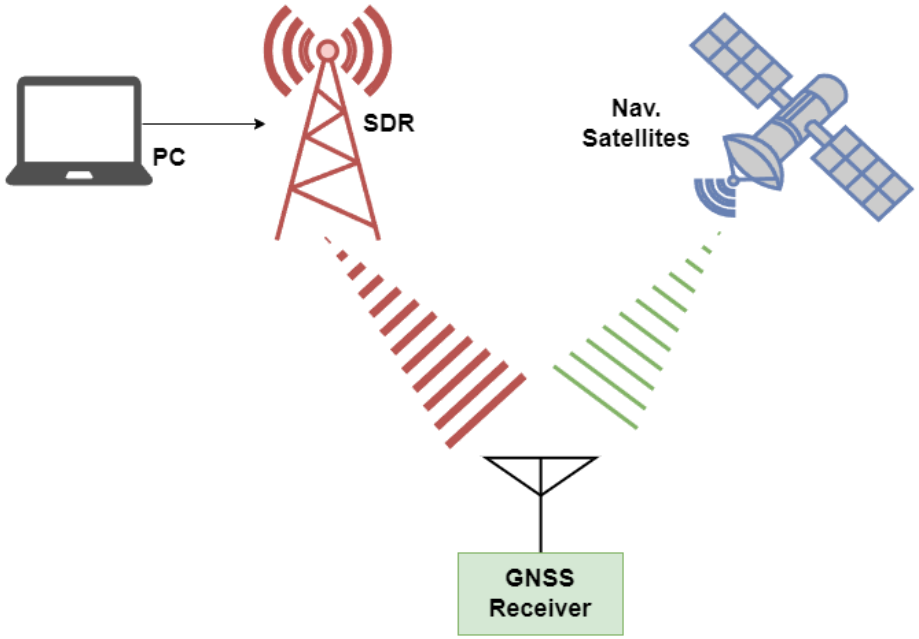
- Transmitting counterfeit signals
- Stronger signals overlay real ones

  -> Calculation of wrong position

GNSS Spoofing Explained

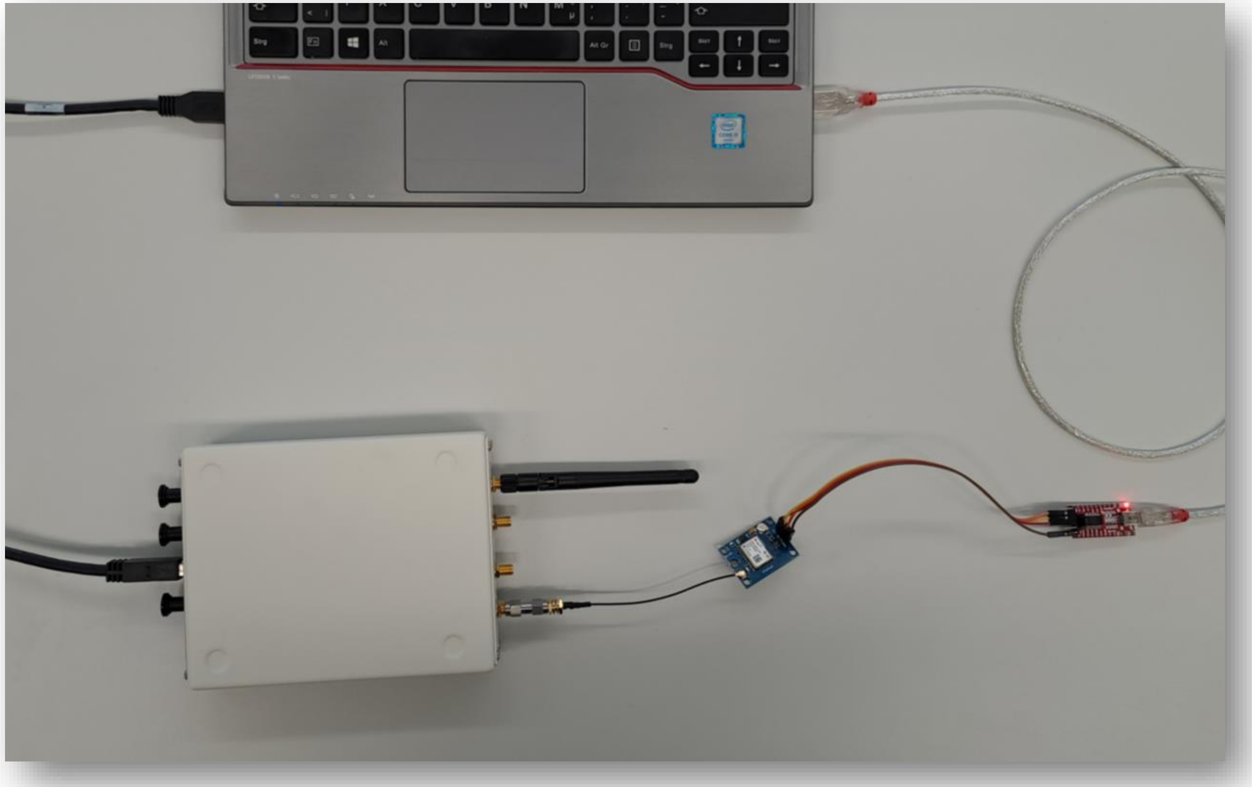
GNSS Spoofing Overview:

- Spoofing transmits fake signals stronger than the satellite signals.
- Goal: Trick the receiver into computing false position/time.
- Most common spoofing types:
  - Meaconing – replayed GNSS signals
  - Code Carrier Attack – fake replicated signals
  - Navigation Data Attack – forged navigation messages
  - App-Level Spoofing – Man-in-the-Middle
  - Multi-method – combinations for complex attacks



GNSS Spoofing – Practical Setup

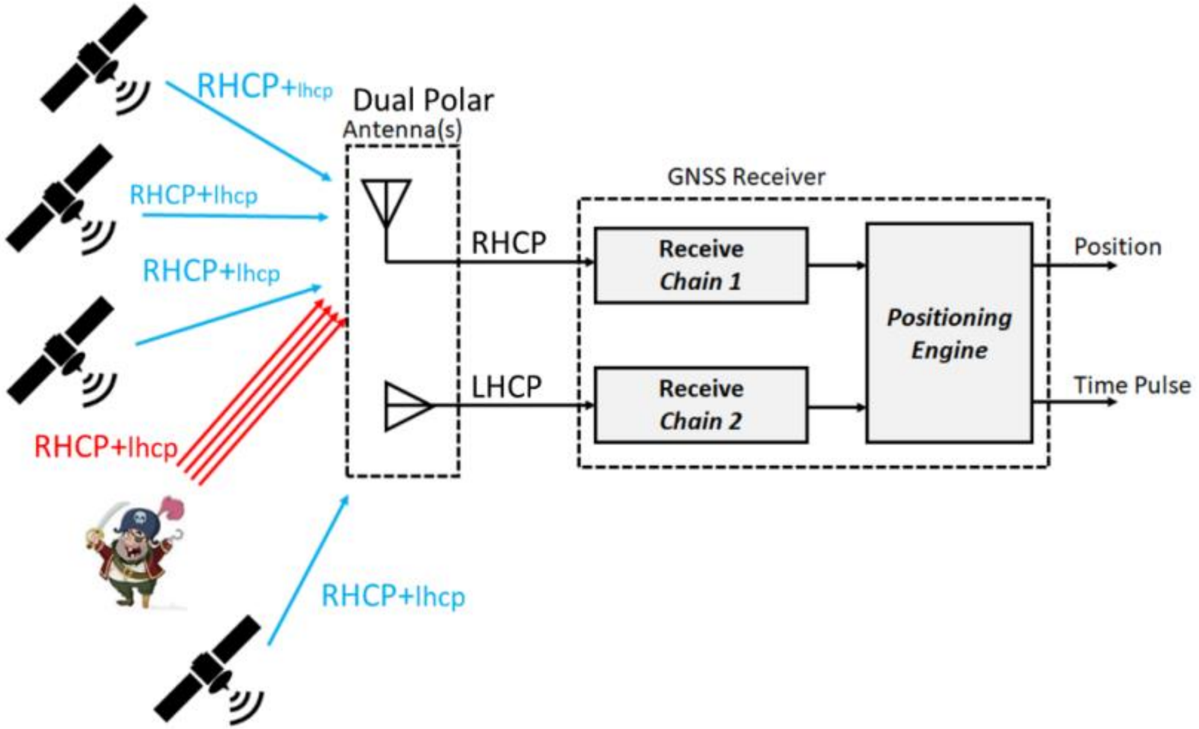
- This is how the setup from the previous slide might look like in practice.
- Note the cable used to connect SDR and receiver to avoid broadcasting spoofed signals and possibly impacting other devices.



OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

Countermeasures

- Discarding messages with an abnormally high signal strength.
- Ensuring signals from different satellites arrive from different directions, by utilizing signal polarization.
- Better Standards:
  - Galileo OS-NMA
  - Galileo CAS on E6 (for AD)



Simulation Setup

- Position comes from the simulation

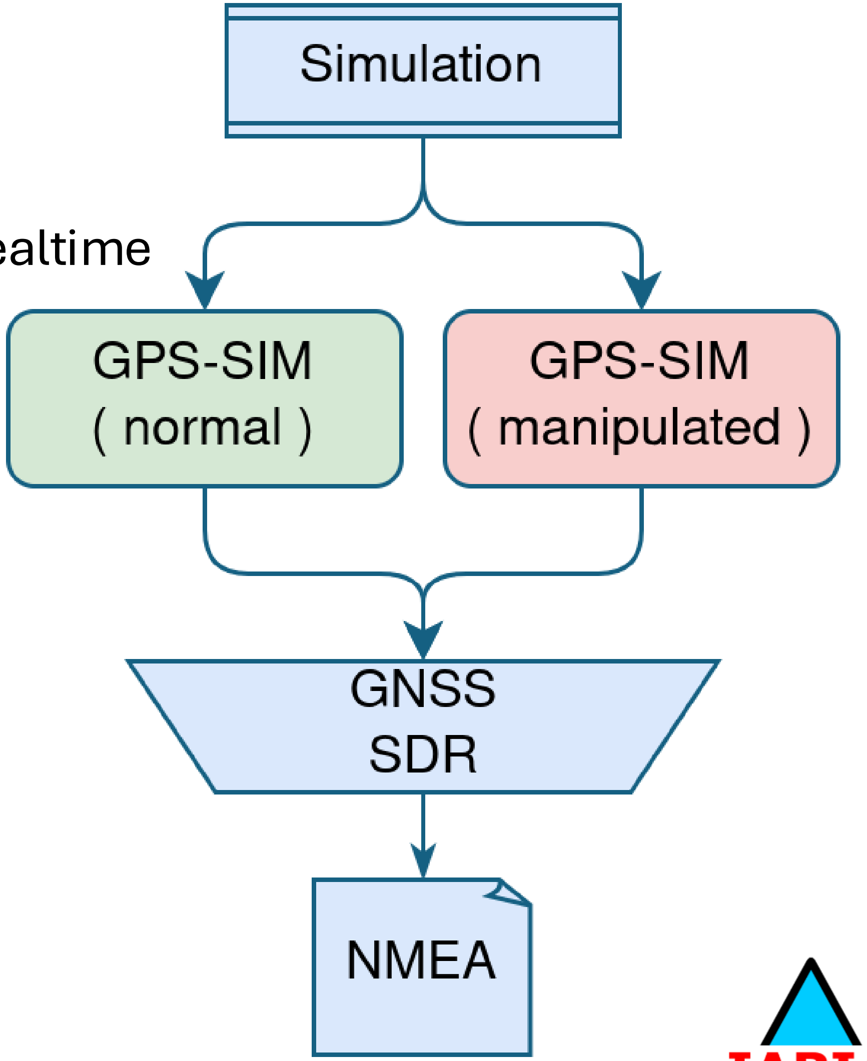
- Corresponding I/Q data is computed with gps-sdr-sim-realtime

  - Once for the true position

  - Once for the wrong position –> Spoofing

- Outputs are merged, with the "normal" signal dampened

- GNSS-SDR is used to reinterpreted the data to NMEA



OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

GNSS Spoofing Detection in Autonomous Vehicles

Detection Techniques:

- LSTM models for anomaly detection (Dasgupta et al.)
- Error covariance analysis in Kalman filters (Liu et al.)
- Hybrid sensor fusion: GNSS + IMUs + odometry
- Slow-drift attacks in urban settings highlight stealth
- Physics-based IDS monitor vehicle behavior in real time
- Machine learning enhances early spoofing detection

Forensic Recorders

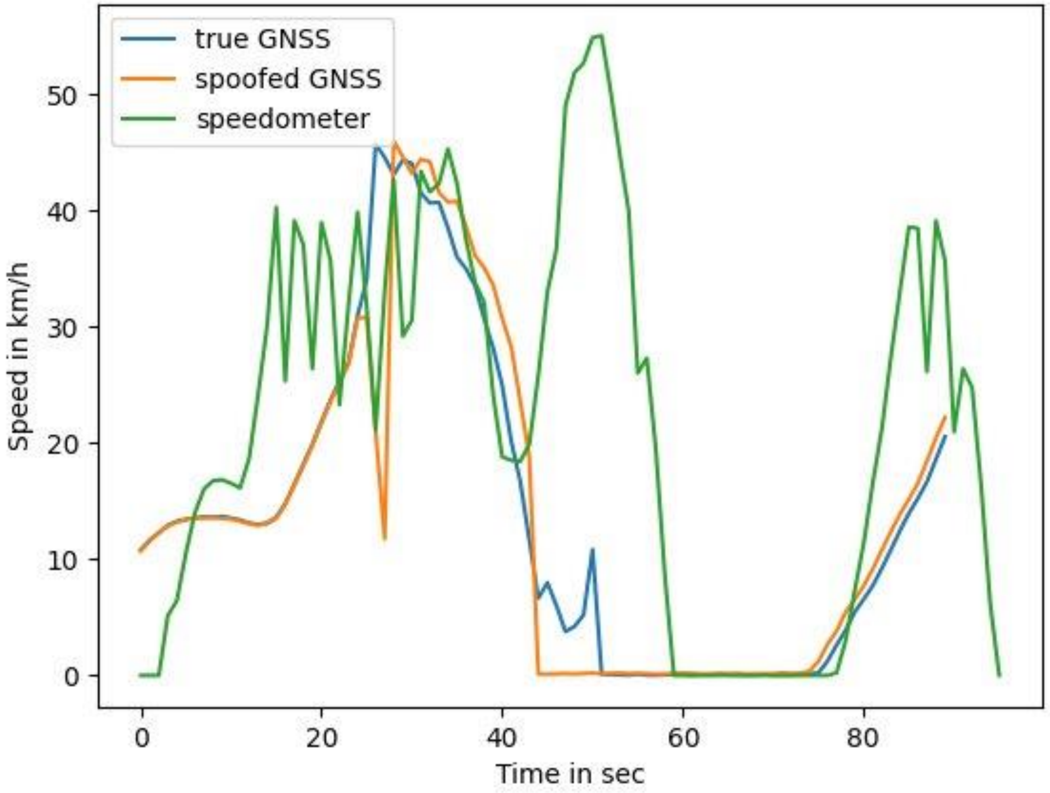
- Multiple forensic frameworks could be investigated
- Standard forensic investigation:
  - Strategic preparation
  - Operational preparation
  - Data collection
  - Investigation
  - Data analysis
  - Documentation

EDR	DSSAD	AV-Guard
- Mandatory	- (soon) mandatory	- Not mandatory
- Last 5 seconds	- Last few minutes	- Days to years
- Crash related data	- ADAS related data	- Processed sensor data

Forensic Analysis

- EDR:
  - Speed data of GNSS and speedometer
- DSSAD:
  - Check if and how much control the vehicle systems had
- AV Guard:
  - Route data as GPS points

Result: Difficulties in detecting GNSS Spoofing with such a limited amount of data.



Zentrale Stelle
für Informationstechnik
im Sicherheitsbereich

Forensic Advice

- Consider use cases for attacks
  - Geofencing
  - Kidnapping executed by triggering the vehicles safe mode
- Consider interesting data points
- Validate it with the simulation setup

Expected interesting data points:

- Route data and camera pictures, i.e. dashcams
- Raw sensor data, e.g. NMEA

Thank you for your attention

Do you have any questions?

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages