OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

A Multi Method Framework for GNSS Anomaly Detection in Vehicular Systems Using NMEA Data

Mathias Gerstner, Tobias Reichel, Sebastian Fischer, Rudolf Hackenberg

20.04.2026

IARIA

OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

Mathias Gerstner

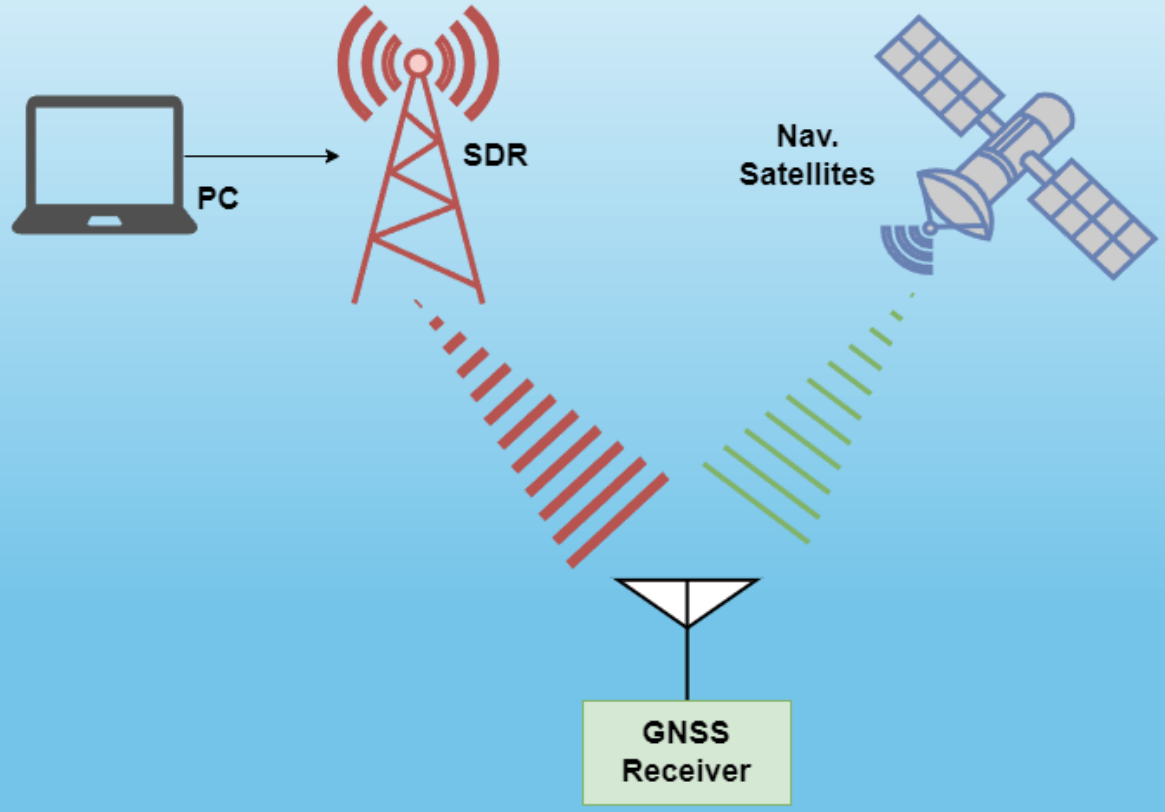
mathias.gerstner@oth-regensburg.de

- Masters' degree in Applied Research (Data Science)
- Ph.D. Student CarSec-Lab at OTH Regensburg
- Research focus:
  - Mobile Network Analysis and Prediction for Automated Vehicles
  - Intrusion Detection Systems for GNSS and V2X

IARIA

Motivation

- GNSS is a key component for navigation, especially in autonomous driving systems
- Civilian GNSS signals are unencrypted and vulnerable
- Increasing threats: spoofing and jamming
- Manipulated signals → incorrect positioning
- Critical risk for safety-relevant systems

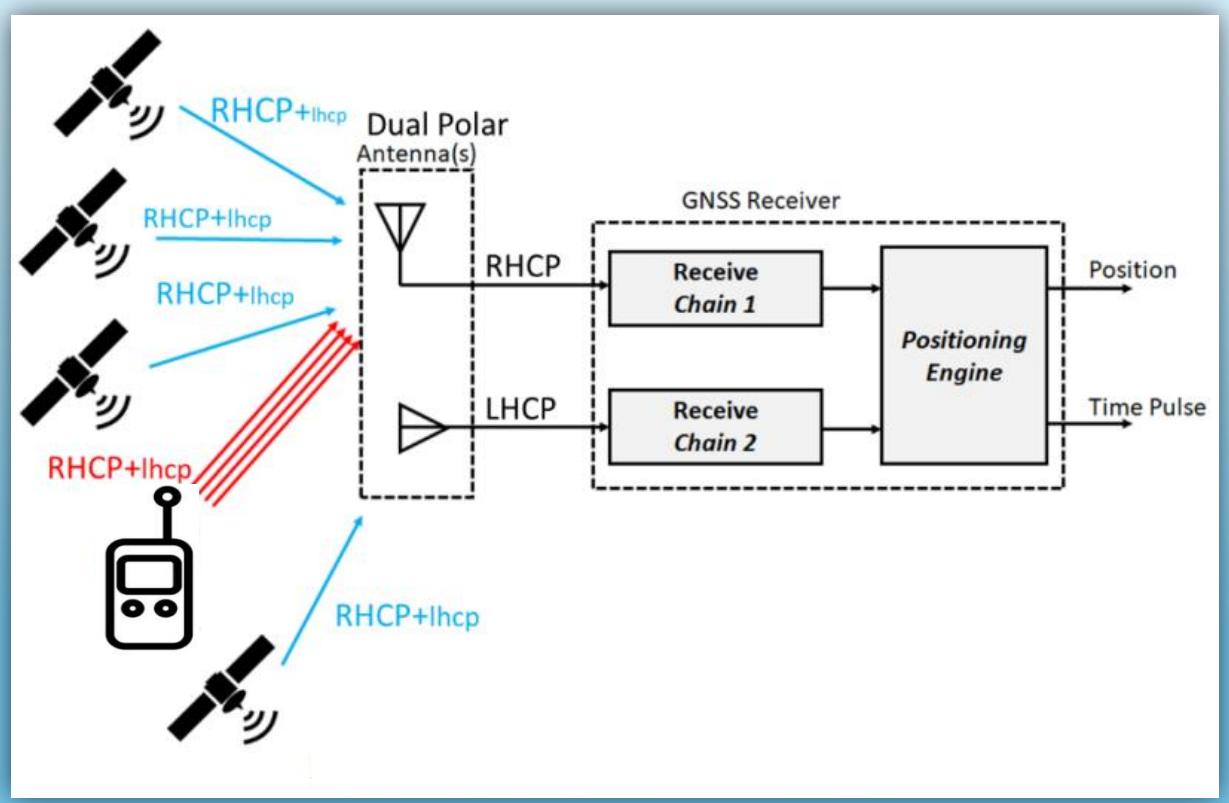


OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

IARIA

Problem Statement

- GNSS data is often blindly trusted by systems
- Existing IDS solutions:
  - Require additional hardware
  - Focus on maritime environments
- Lack of lightweight, automotive-compatible solutions
- Need for real-time anomaly detection



OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

IARIA

Objective and Core Idea

- A lightweight GNSS Intrusion Detection System for standard NMEA data
- No need for labeled attack data
- Real-time capable
- Deployable on standard vehicular hardware
- Combine multiple detection methods:
  - Threshold-based detection
  - Rule-based consistency checks
  - Machine Learning
- Fuse all outputs into a unified anomaly score to improve robustness and detection reliability

OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

NMEA Example

- *$GNRMC,121116.00,A,4748.56417,N,01205.80483,E,35.489,188.60,240325,4.06,E,A*14*
- *$GNVTG,188.60,T,184.54,M,35.489,N,65.726,K,A*35*
- *$GNGGA,121116.00,4748.56417,N,01205.80483,E,1,10,0.66,487.8,M,45.7,M,,*4D*
- *$GNGSA,A,3,05,16,18,23,25,26,27,28,29,31,,,1.14,0.66,0.94*1A*
- *$GPGSV,3,1,10,05,23,049,43,16,45,303,45,18,78,123,46,23,22,145,45*77*
- *$GPGSV,3,2,10,25,07,139,37,26,69,268,46,27,18,274,43,28,14,205,42*77*
- *$GPGSV,3,3,10,29,37,077,45,31,29,226,45*78*
- *$GPGSV,3,1,09,05,23,049,38,18,78,123,46,23,22,145,42,25,07,139,32*79*
- *$GPGSV,3,2,09,26,69,268,43,27,18,274,40,28,14,205,40,29,37,077,41*7E*
- *$GPGSV,3,3,09,31,29,226,40*4B*
- *$GNGLL,4748.56417,N,01205.80483,E,121116.00,A,A*7C*
- *$GNGST,121116.00,21,1.4,1.2,5.8,0.56,0.49,1.0*64*
- *$GNZDA,121116.00,24,03,2025,00,00*7C*

Information in NMEA

Time and Date (GNRMC, GNZDA)
UTC-Time: 12:11:16
Date: 24.03.2025

Position (GNRMC, GNGGA, GNGLL)
Latitude: 47° 48.56417' N
Longitude: 12° 05.80483' E

Vehicle Motion (GNRMC, GNVTG)
Speed over ground: 35.489 kn ≈ 65.7 km/h
Course over ground: 188.60°

Altitude and Fix Information (GNGGA, GNGSA)
Altitude above mean sea level: 487.8 m
Geoid separation: 45.7 m
Number of satellites used: 10
Horizontal Dilution of Precision (HDOP): 0.66

Accuracy and Quality Parameters (GNGST)
PDOP: 1.14
HDOP: 0.66
VDOP: 0.94
Position standard deviation:
- Lateral: 1.4 m
- Longitudinal: 1.2 m
- Altitude: 5.8 m

Satellite Information (GPGSV, GNGSA)
Visible GPS satellites: 9–10
SNR values: 32–46 dB-Hz
PRNs: 05, 16, 18, 23, 25, 26, 27, 28, 29, 31

Data Analysis and Thresholds

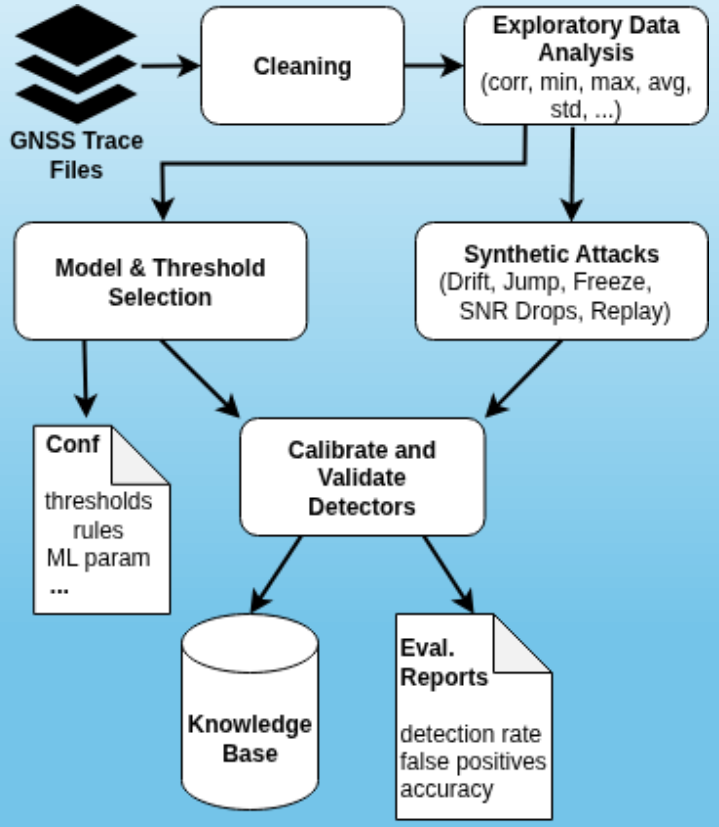


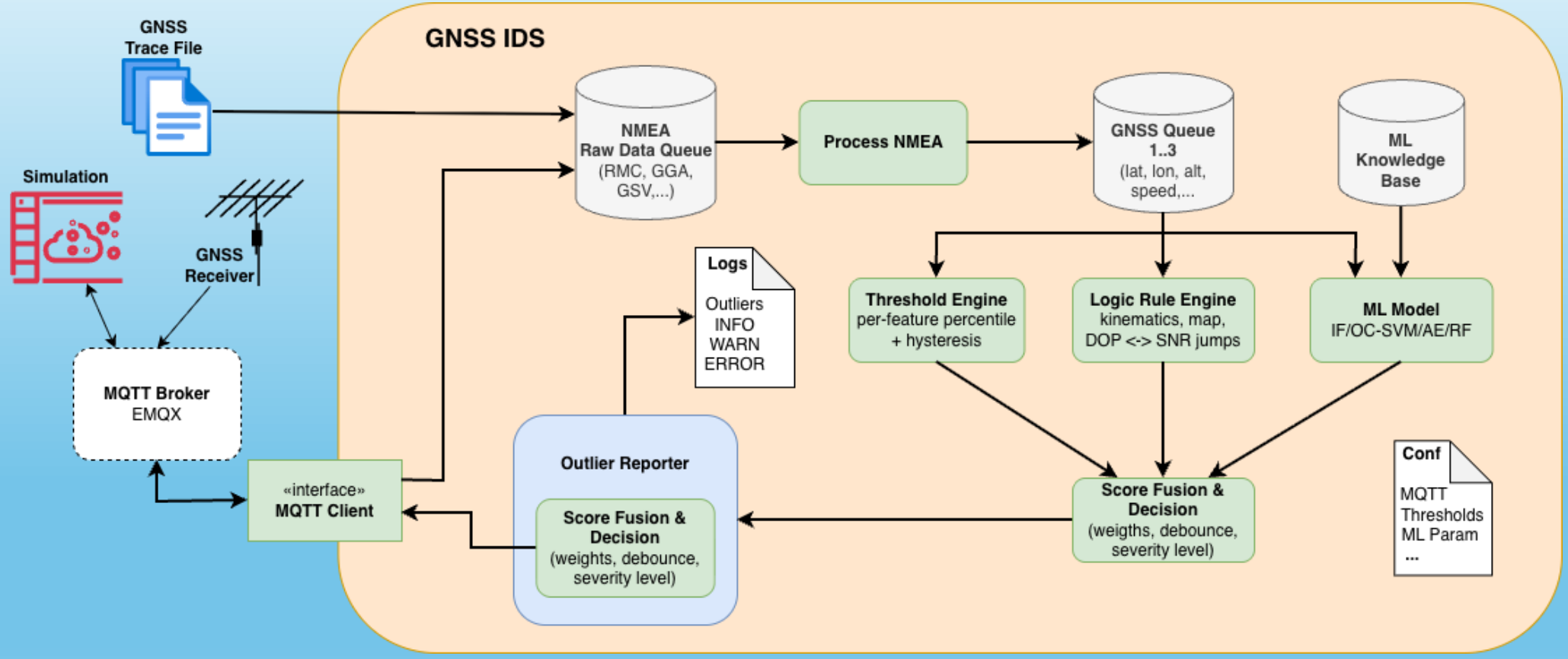
TABLE I. THRESHOLDS USED FOR ANOMALY DETECTION

Metric	Threshold	Overshoot Threshold
PDOP	> 2.03	> 22.54
HDOP	> 1.13	> 19.94
VDOP	> 1.71	> 22.01
RMS range	$> 45.0\,\mathrm{m}$	$> 135.0\,\mathrm{m}$
Std. major axis	$> 10.0\,\mathrm{m}$	$> 199.0\,\mathrm{m}$
Std. minor axis	$> 5.7\,\mathrm{m}$	$> 66.0\,\mathrm{m}$
Std. latitude	$> 4.0\,\mathrm{m}$	$> 109.0\,\mathrm{m}$
Std. longitude	$> 2.5\,\mathrm{m}$	$> 147.0\,\mathrm{m}$
Std. altitude	$> 6.7\,\mathrm{m}$	$> 500.0\,\mathrm{m}$
GPS satellites	< 9	$< 7 \vee > 17$
Mean SNR	$< 22.7\,\mathrm{dB}$	$< 5.0\,\mathrm{dB}$
SNR std. dev.	$> 6.2\,\mathrm{dB}$	$< 1.5\,\mathrm{dB}$
Max. speed	$> 120\,\mathrm{km/h}$	$> 160\,\mathrm{km/h}$

OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

IARIA

System Architecture

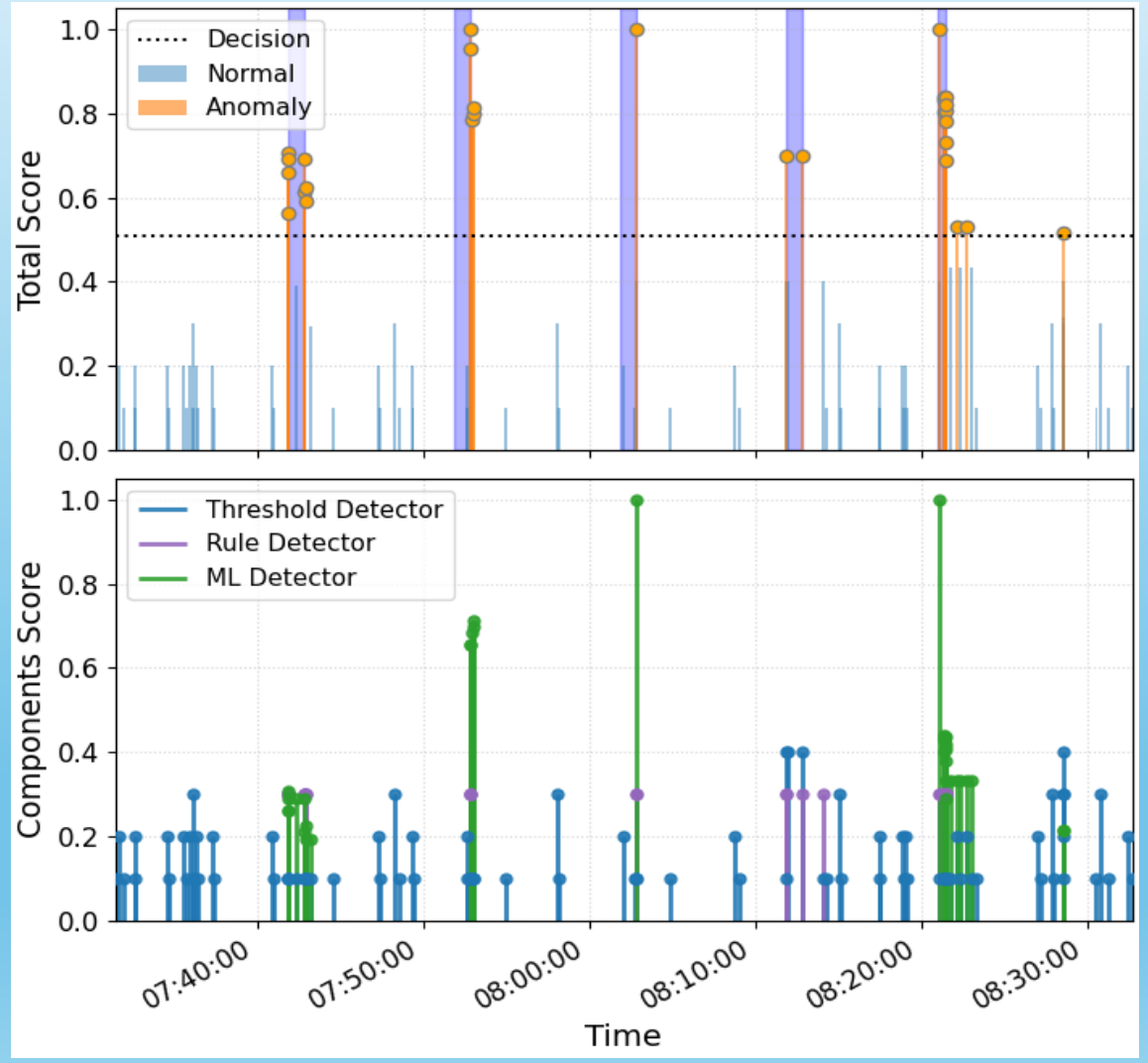


OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

IARIA

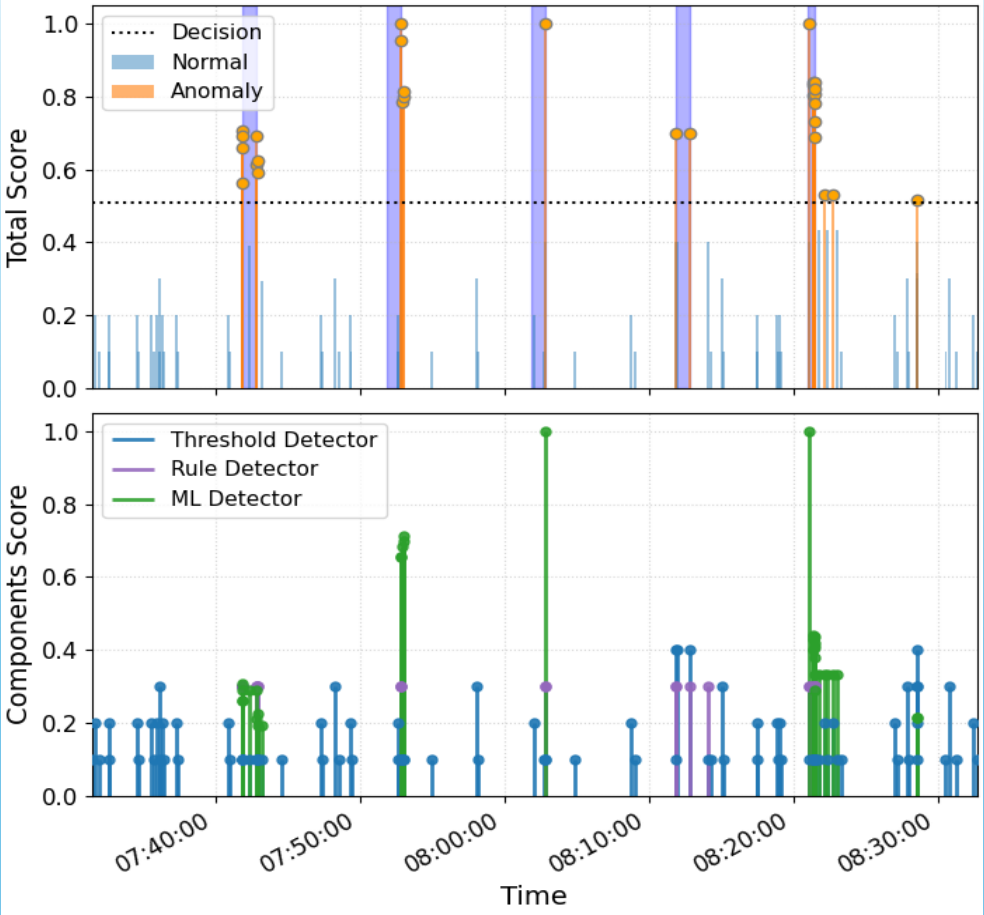
Attrack Scenarios

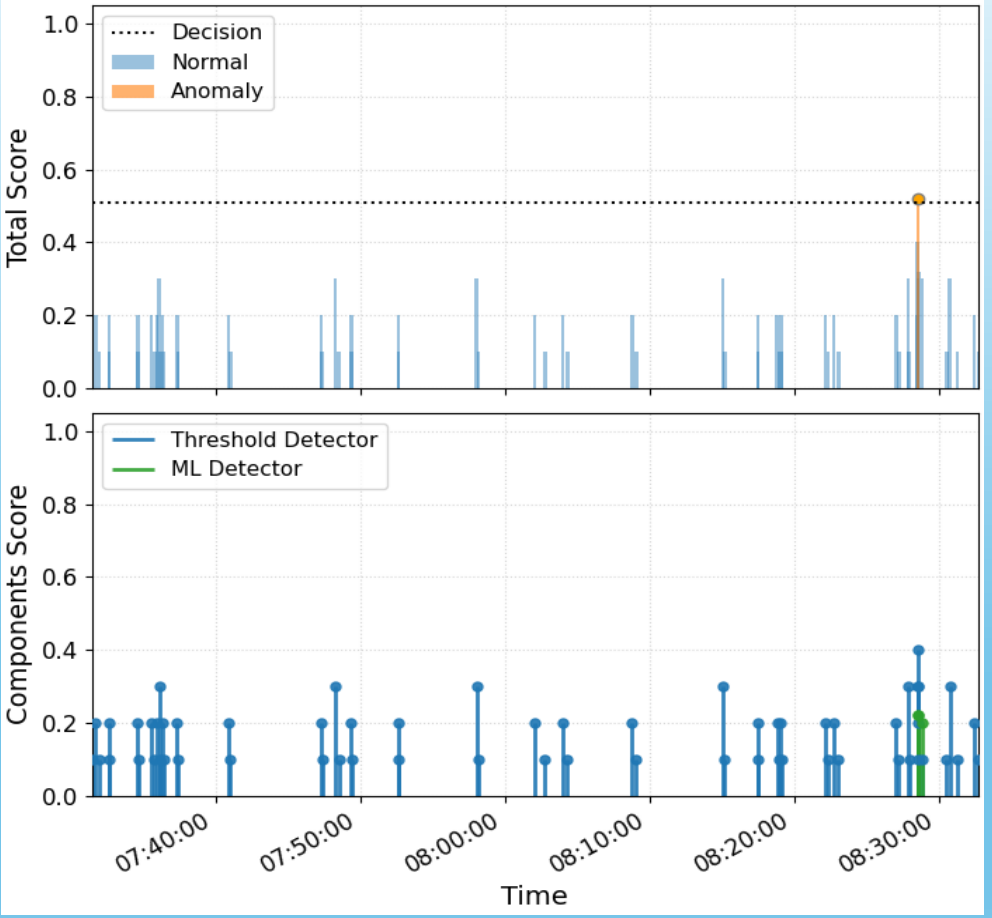
- Blue markers indicate the phase of the attack
- Orange markers indicate detected anomalies
- Attacks from left to right:
  - Position jump
  - Slow drift attack
  - Location freeze attack
  - Jamming (SNR drop)
  - Replay attack



OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

Attacks and Baseline





OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

IARIA

Detection Results

TABLE II. PERFORMANCE OF THE GNSS IDS EVALUATED ON 3550 KM OF DRIVES.

Metric	False positives per hour
Mean false positive rate	2.27
Median false positive rate	1.80
Maximum false positive rate	10.80

TABLE III. MOST FREQUENT CAUSES OF FALSE POSITIVE EVENTS ACROSS ALL ATTACK FREE RUNS.

Detector and Feature	Occurrences
Threshold: mean SNR	54
LOF: RMS range	52
LOF: major axis position error	51
LOF: Position DOP	47
Threshold: RMS range	41

- The IDS detects all investigated spoofing and jamming attacks
- For slow drift and location freeze attacks, a short detection latency occurs
- False positive rate of 2.27 / hour
- False alarms are primarily caused by poor GNSS signal quality (low SNR, high DOP)

→ Test with new parameters based on quantiles: 1.63fp / hour

OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

IARIA

Conclusion and Future Work

- Multi-method IDS improves detection reliability
- Works with standard GNSS receivers → suitable for automotive deployment
- No labeled data required (but the system must be calibrated on the receiver)

Future Research Directions:

- Integration of additional sensor data
- Incorporating a map and the environmental context
- Improved handling of signal degradations

→ Goal: better detection of more sophisticated spoofing attacks

OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

Thank you for your attention!

Mathias Gerstner, Tobias Reichel, Sebastian Fischer, Rudolf Hackenberg

IARIA

Key References

- **Amro et al. (2022)**
  "Navigation data anomaly analysis and detection"
  → Rule-based NMEA anomaly detection
- **Spravil et al. (2023)**
  "Detecting maritime GPS spoofing attacks based on NMEA sentence integrity monitoring"
  → Maritime NMEA-based anomaly detection (MANA) with threshold and consistency monitoring
- **Boudehenn et al. (2021)**
  "Navigation anomaly detection"
  → Maritime GNSS anomaly detection using Machine Learning
- **Lemieszewski (2022)**
  "Transport safety: GNSS spoofing detection using the single-antenna receiver and speedometer of a vehicle"
  → GNSS spoofing detection via speedometer consistency checks.