WHITEPAPER

Robuste GNSS-Systeme für automatisierte Mobilität

Dr. Paulo Mendes
Dr. Martin Margreiter

www.iabg.de

Robuste GNSS-Systeme für automatisierte Mobilität

Analyse und Testmethodik zur Absicherung gegen Jamming und Spoofing

Abstract

Automatisierte Mobilitätssysteme verlassen sich in entscheidender Weise auf Satellitennavigationssysteme (Global Navigation Satellite Systems, GNSS) für präzise Positionierung und Zeitsynchronisation. Die Verwundbarkeit von GNSS durch Funkinterferenzen (Jamming) und Signalmanipulationen (Spoofing) stellt jedoch ein wachsendes Sicherheitsrisiko dar – insbesondere für Systeme, deren Funktionen direkt von GNSS-Daten abhängen.

Die IABG hat eine integrierte Testmethodik entwickelt, die Labor- und Freifeldtests kombiniert, um die Resilienz von GNSS-Empfängern unter realitätsnahen Bedingungen zu bewerten. Im Zentrum stehen reproduzierbare Angriffs- und Störszenarien, die auf dem Mobility Innovation Campus (MIC) in Ottobrunn mit Genehmigung der BNetzA durchgeführt und mithilfe eines „Experimental Twins“ digital gespiegelt werden. Das Ergebnis ist ein skalierbares, normorientiertes Prüfkonzept für sichere und verlässliche Navigation automatisierter Fahrzeuge.

1. Einleitung und Motivation

Automatisiertes Fahren basiert auf einer engen Verzahnung von Sensorik, Datenfusion und Algorithmen zur Entscheidungsunterstützung. Kameras, LiDAR, Radar, Inertial Measurement Units (IMUs) und GNSS-Empfänger liefern Daten, die im Fahrzeug in Echtzeit fusioniert werden. Diese Sensoren bilden zusammen das sog. „Perception- und Localization-Stack“ – das Herzstück der automatisierten Fahrzeugführung.

GNSS-Daten spielen darin eine doppelte Rolle: Sie ermöglichen einerseits die absolute Positionierung in einem globalen Koordinatensystem, andererseits liefern sie hochgenaue Zeitsignale für die Synchronisation der Sensoren. Bereits Fehler im Bereich weniger Meter oder Mikrosekunden können bei automatisierten Fahrfunktionen zu sicherheitskritischen Situationen führen – etwa bei Spurwechseln, Kreuzungsüberquerungen oder Notbremsungen.

Da GNSS-Signale mit einer typischen Empfangsleistung von etwa -160 dBW extrem schwach sind, kann selbst ein handelsüblicher Störsender mit einer geringen Sendeleistung den Empfang vollständig blockieren. Im europäischen STRIKE 3-Projekt wurden über 450 000 Störereignisse dokumentiert, die Mehrzahl davon durch sogenannte „Privacy-Protection-Devices“ [1]. Solche Geräte werden häufig von LKW-Fahrern genutzt, um eine Überwachung ihres Fahrverhaltens zu verhindern – ihre Signale reichen über das eigene Fahrzeug hinaus und gefährden die Positionsbestimmung benachbarter Verkehrsteilnehmer.

2. Bedrohungslage und technische Hintergründe

2.1. Jamming

Beim Jamming werden hochfrequente Störsignale in den GNSS-Frequenzbändern ausgesendet – typischerweise L1 (1575,42 MHz) und L5/E5 (1176,45 MHz). Abhängig von der Modulation der Interferenzsignale können diese breitbandig typischerweise mehrere zig MHz sein, wie dies z.B. bei

rauschähnlichen Störsignalen der Fall ist oder schmalbandig wie z. B. bei einem Sinus-Ton. Für eine Beurteilung der Störrobustheit sind neben den GNSS signalspezifischen Modulationsfahren, auch die empfängerseitig implementieren Härtungsmaßnahmen entscheidend.

Bereits eine Sendeleistung von wenigen Mikrowatt kann in einem Umkreis von 100 m zum Signalverlust führen. In Testreihen der IABG traten bei 1 µW Störleistung Positionsfehler von 6–8 m und ein Anstieg der Phasenrauschleistung um bis zu 15 dB auf.

2.2. Spoofing

Beim Spoofing werden gefälschte Satellitensignale erzeugt, die echten GNSS-Signalen in Frequenz, Phase und Datenstruktur nachempfunden sind. Moderne Software-Defined-Radios (SDR) ermöglichen es, solche Signale gezielt zu erzeugen, auszustrahlen und damit Empfängern eine falsche Position vorzutäuschen.

Im Gegensatz zu Jamming-Ereignissen, die für den Anwender unmittelbar erkennbar sind, können qualitativ hochwertige Spoofing-Angriffe vom Nutzer nicht erkannt werden. Ein driftender Positionsfehler von nur 0,5 m/s kann in wenigen Minuten zu einer Abweichung von über 100 m führen – ohne dass der Empfänger eine Anomalie meldet.

In Feldversuchen der University of Texas und der Universität der Bundeswehr München wurde gezeigt, dass Spoofing-Angriffe auf Fahrzeuge der SAE-Level-2-Automatisierung zu abrupten Spurwechseln, Fehlbremsungen und sogar Navigationsabbrüchen führen können [2] [3].

2.3. Multisensorische Absicherung

Eine wirksame Gegenmaßnahme ist die sensorische Redundanz. Durch Abgleich von GNSS-Daten mit inertialen (IMU), optischen (Kamera) und aktiven (LiDAR) Sensorsystemen lässt sich die Plausibilität der Positions- und Bewegungsdaten prüfen. Diskrepanzen zwischen den Sensorkanälen können in Echtzeit detektiert werden – z. B. durch modellbasierte Integritätsüberwachung (Integrity Monitoring). Solche Verfahren bilden den Kern aktueller Forschungsprojekte wie VorTNAF („Vorbereitung von Test & Zertifizierung robuster Navigation für autonomes Fahren“), an dem die IABG mitwirkt.

3. Testmethodik der IABG

3.1. Laborinfrastruktur

Im GNSS-Labor der IABG können reale Satellitenkonstellationen und Signalverhältnisse präzise nachgebildet werden. Der eingesetzte GNSS-Simulator erzeugt Multi-Konstellations-Szenarien (GPS, Galileo, GLONASS) in mehreren Frequenzbändern (E1, E6) und kann bei Bedarf auch auf andere Frequenzbereiche erweitert werden.

Das Labor erlaubt:

- die Simulation authentischer GNSS-Signale einschließlich Satellitenbewegungen, Ionosphären-verzögerungen und Mehrwege-Effekten,
- die Einblendung synthetischer Jamming-Signale mit konfigurierbarer Bandbreite, Modulation und Leistung,
- die Erzeugung von Spoofing-Szenarien mit Manipulationen der Satellitennavigationssignale auf Navigationsbit-, Spreizkode- und Dopplerfrequenzebenen.

Alle Signale können in einer operationellen Umgebung aufgezeichnet und später im Labor wiederholt abgespielt werden – auch in Kombination mit neuen Angriffsmustern. So entsteht eine Testumgebung mit vollständig reproduzierbaren Signalen, die verlässliche Vergleichstests zwischen Empfängertypen oder Softwareständen ermöglicht.

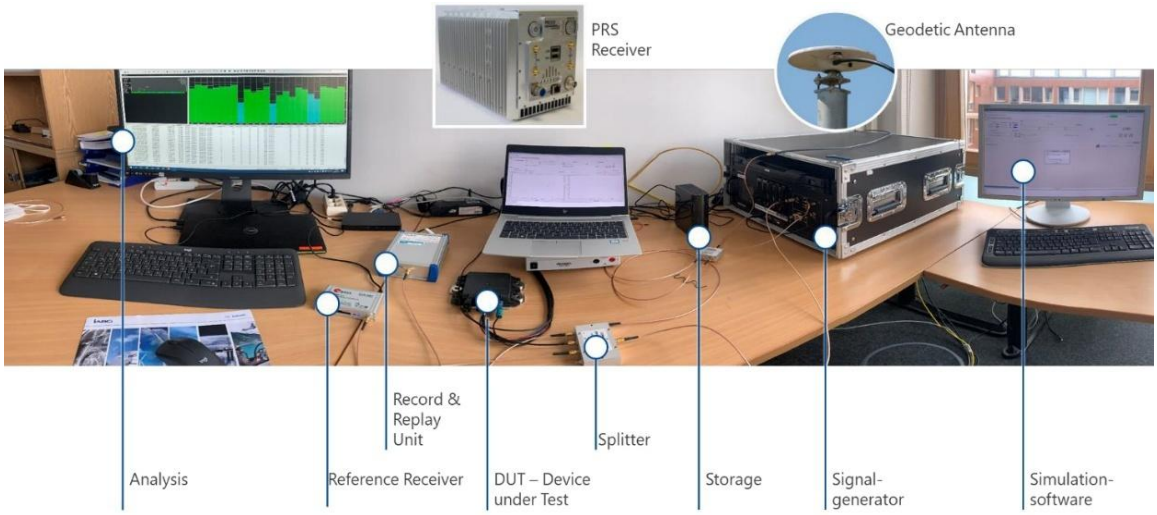

Abb. 1: GNSS-Laboraufbau der IABG

3.2. Freifeldtests auf dem Mobility Innovation Campus (MIC)

Für realitätsnahe Tests betreibt die IABG auf dem Mobility Innovation Campus (MIC) in Ottobrunn ein Testfeld für verschiedene Automotive-Anwendungen, auf dem mit Genehmigung der BNetzA Jamming- und Spoofing-Signale ausgesendet werden dürfen. [4].

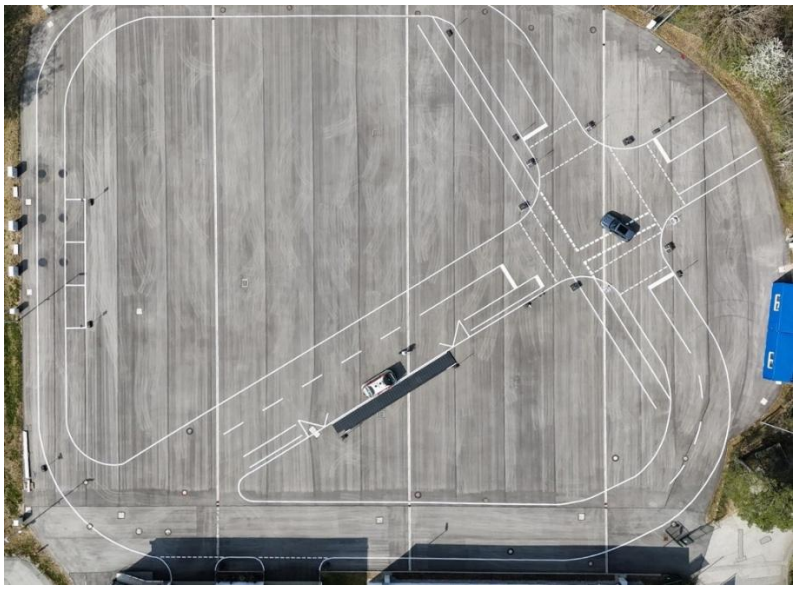

Abb. 2: Außenversuchsfläche des Mobility Innovation Campus (MIC)

Die Trajektorie der Testfahrzeuge wird über ein verteiltes LiDAR-Netz erfasst, das Positionsdaten mit einer Genauigkeit von < 2 cm liefert. Diese Ground-Truth-Daten dienen als unabhängige Referenz, um GNSS-Positionsfehler exakt zu quantifizieren.

3.3. Der „Experimental Twin“

Der Experimental Twin ist das digitale Abbild der realen Testumgebung. Alle Sensor-, Fahrzeug- und Angriffsdaten werden in einer synchronisierten Datenbank erfasst. Die Vorteile sind:

- Virtuelle Wiederholung realer Szenarien mit unterschiedlichen Parametern
- Erweiterung von Angriffsmustern ohne neue Feldversuche
- Integration in Simulationsplattformen für Software-in-the-Loop-Tests

4. Ergebnisse und Analyse

4.1. Jamming-Effekte

Die Auswertung des Spektrogramms zeigt, dass die automatische Verstärkungsregelung (AGC) des Empfängers rein auf das Störsignal ausregelt. Das führt zu einer Verringerung der nutzbaren Bits für die Quantisierung des Signals und damit zu einer Reduktion des sogenannten Träger-zu-Rauschleistungs-dichteverhältnisses (C/N_0).

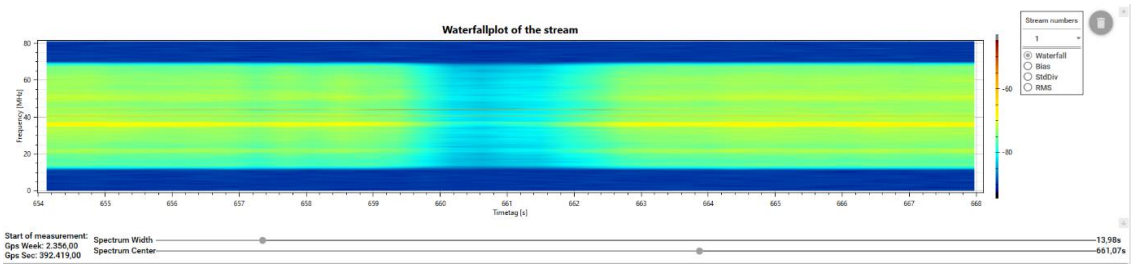

Abb. 3: Spektrogramm eines aufgezeichneten Jamming-Ereignisses

In den Tests betrug das Träger-zu-Rausch-Verhältnis (C/N_0) bezogen auf die Rauschleistungsdichte im Mittel 10–15 dB, was bei einfachen Empfängern bereits zum Verlust der Phase-Lock-Loop (PLL) führte.

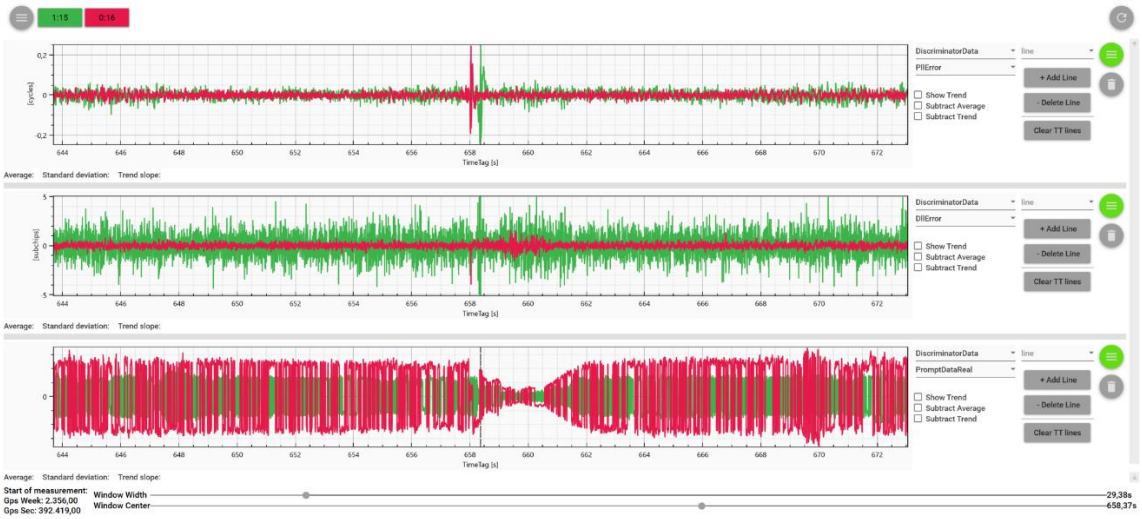

Abb. 4: Tracking-Fehler während eines Jamming-Ereignisses
Zeitverlauf von PLL- und DLL-Fehlern, sowie der Promptkorrelatorwerte für zwei Satellitenkanäle (rot = GPS, grün = Galileo)

4.2. Spoofing-Effekte

Bei Spoofing-Tests mit SDR-basierten Angriffen zeigten sich Drift-Raten zwischen 0,2 und 0,6 m/s – je nach Empfängerarchitektur. Besonders anfällig sind Systeme, die keine Echtzeit-Integritätsprüfung durchführen.

4.3. Wirksamkeit von Gegenmaßnahmen

Die Implementierung von Mehrfrequenz-Empfängern und Sensordaten-Fusion (GNSS + IMU + LiDAR) zeigte eine erhebliche Robustheitssteigerung. In allen Tests blieb die kombinierte Positionsabweichung unter 2 m, auch bei vollständigem GNSS-Signalverlust bis zu 20 s.

Erste Untersuchungen zu Galileo OSNMA (Open Service Navigation Message Authentication) bestätigen internationale Forschungsergebnisse zur Funktionalität kryptografischer Schutzmechanismen. Die Authentifizierung der Navigationsdaten wird durch Spoofing-Angriffe zwar deutlich erschwert, aber noch nicht vollständig verhindert – insbesondere, wenn Empfänger das Authentifizierungssignal mit einer Latenz verarbeiten.

5. Schlussfolgerungen und Ausblick

Die Tests der IABG belegen, dass selbst geringe Störleistungen die GNSS-Navigation beeinträchtigen können. Eine reine Signalbewertung ist daher unzureichend – erforderlich ist eine ganzheitliche Systemanalyse.

Die erzielten Ergebnisse fließen u.a. in die Weiterentwicklung der europäischen EN-16803-Normreihe ein, die Verfahren zur Bewertung von Genauigkeit, Verfügbarkeit, Kontinuität und Integrität definiert. Darüber hinaus ist die IABG in der Lage Cyber-Resilience-Aspekte gemäß ISO/IEC 27000 und TISAX in Test- und Zertifizierungsprozesse zu integrieren.

Zukünftig sollen die entwickelten Methoden auch auf andere sicherheitskritische Anwendungsbereiche übertragen werden – etwa Bahn-, Schiffs- und Drohnennavigation oder landwirtschaftliche GNSS-Anwendungen. Hierbei steht die Entwicklung eines skalierbaren Prüfrahmens im Mittelpunkt, der physische Tests, Simulationen und normative Bewertung kombiniert.

Mit dieser interdisziplinären Expertise verbindet die IABG Ingenieur-, Simulations- und Sicherheits-kompetenz zu einem integrativen Ansatz für verlässliche, souveräne Mobilitätssysteme.

Literaturverzeichnis

[1] STRIKE-3-Projekt (2019): *European GNSS Interference Monitoring*, ARIC Aachen.

[2] Universität der Bundeswehr (2025): *MuSNAT – Multi-Sensor Analysis Tool for GNSS Evaluation*.

[3] Clements Z.; Yoder J. E.; Humphreys T. E. (2022): *Carrier-Phase and IMU Based GNSS Spoofing Detection for Ground Vehicles*, Institute of Navigation, Long Beach (CA).

[4] Margreiter M. (2025): Whitepaper IABG Mobility Innovation Campus.

Sprechen Sie uns gerne an!

Mehr erfahren