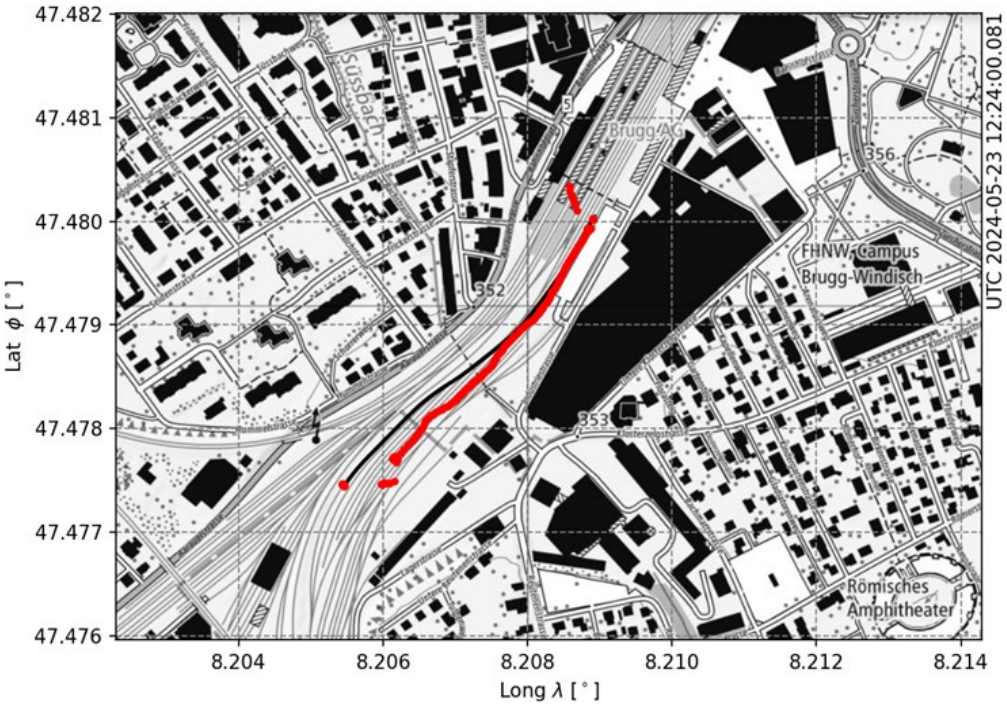

Abbildung 1 - Die Grafik zeigt den Spoofing-Angriff, wobei die schwarzen Punkte die Positionen des Referenzsystems und die roten Punkte die berechneten Positionen des GNSS-Empfängers unter Spoofing anzeigen (Karte: Bundesamt für Landestopografie – Swisstopo).

GNSS Jamming und Spoofing – Deutsches Expertenwissen im Eisenbahnprojekt

Satellitennavigation ist längst nicht mehr nur eine Schlüsseltechnologie für Luft- und Raumfahrt, sondern gewinnt auch im Eisenbahnwesen an Bedeutung. Besonders im Rahmen der Weiterentwicklung des European Rail Traffic Management Systems (ERTMS) wird der Einsatz von GNSS diskutiert. Doch mit der Nutzung von GNSS gehen auch neue Bedrohungen durch Stör- und Täuschungsangriffe (Jamming und Spoofing) einher. Das europäische Forschungsprojekt EGNSS MATE hat diese Herausforderungen untersucht und erstmals Szenarien für den sicherheitskritischen Bahnbetrieb experimentell erprobt. Ziel war es, robuste Fusionsalgorithmen zu entwickeln und die Verwundbarkeit im Bahnbetrieb systematisch zu bewerten.

Hintergrund: ERTMS und die Rolle von GNSS

Das European Train Control System (ETCS) ist das Herzstück des ERTMS. Es überwacht Zugbewegungen, gibt Streckenabschnitte frei und kann Züge automatisch zum Stehen bringen. Heute geschieht dies über Eurobalisen, Odometrie und GSM-R-Kommunikation.

Die Integration von GNSS soll diese Verfahren ergänzen und langfristig eine höhere Streckenkapazität bei geringeren Infrastrukturkosten ermöglichen. Die globale Verfügbarkeit, hohe Genauigkeit und niedrigen Empfängerkosten machen GNSS hierfür attraktiv. Gleichzeitig bestehen technische Herausforderungen – etwa Mehrwegeausbreitung und Signalabschattungen – sowie Sicherheitsrisiken durch Jamming und Spoofing.

Bedrohungslage: Jamming und Spoofing im Bahnbereich

GNSS-Signale sind aufgrund ihrer geringen Leistung am Boden (-157 dBW) sehr störanfällig. Jamming beschreibt die Überlagerung echter Signale durch Rausch- oder Störsignale, wodurch Empfänger ihre Positionsinformationen verlieren. Spoofing geht einen Schritt weiter: Angreifer senden manipulierte Signale aus, die Empfänger zu falschen Positionslösungen verleiten. Für EGNSS MATE wurde ein Bedrohungskatalog entwickelt, der realistische Angriffsprofile im Eisenbahnkontext abbildet.

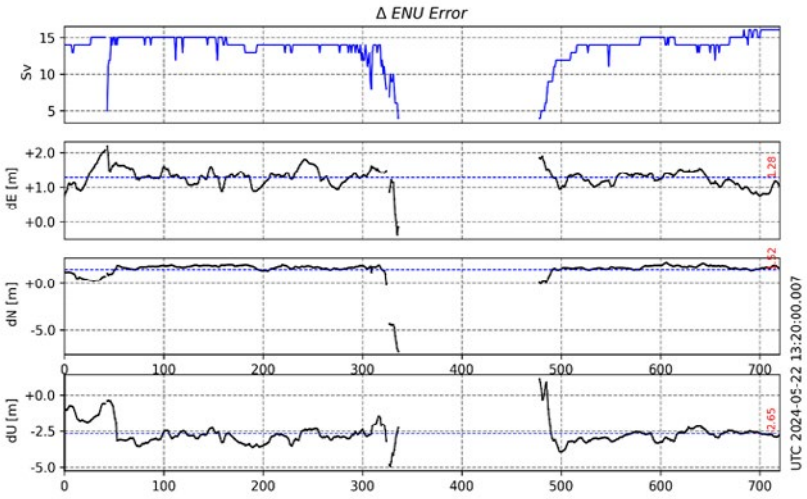

Abbildung 2 – En-Route-Chirp-Störtest und die ermittelten ENU-Fehler. Das obere Diagramm zeigt die Anzahl der verwendeten Satelliten. Die gestrichelten blauen Linien kennzeichnen den mittleren Fehlerwert für die entsprechenden ENU-Koordinaten.

Praxistests mit den Schweizerischen Bundesbahnen (SBB)

Jamming-Szenario

Im ersten Test wurde ein sogenanntes Chirp-Signal simuliert, wie es etwa von Störsendern in Fahrzeugen ausgehen könnte.

- **Aufbau**: GNSS-Simulator wurde über Kabel an den Empfänger eines SBB-Messzugs gekoppelt.
- **Ergebnis**: Deutlicher Anstieg des Positionsfehlers zwischen 310 und 500 Sekunden – die GNSS-Ortung bricht infolge fehlender Signalverfügbarkeit zusammen.

Die Tests zeigen: Bereits handelsübliche Jammer können im parallelen Verlauf von Straßen und Gleisen den Empfang massiv stören.

Spoofing-Szenario

In einem zweiten Szenario wurden manipulierte GNSS-Signale eingespielt, die zu falschen Positionslösungen führten. Besonders kritisch: Im Bereich einer Weiche lieferte der Empfänger fälschlich eine Gleisposition, die nicht mit der Realität übereinstimmte.

- Konsequenz: Gefälschte Signale können in sicherheitskritischen Abschnitten wie Weichenbereichen zu Fehlentscheidungen führen.
- Visualisierung: Die Abweichungen zwischen Referenzdaten und manipulierten Empfängerdaten sind deutlich sichtbar.

Fazit und Ausblick

Die Ergebnisse machen deutlich: Jamming kann zu vollständigen Ausfällen der Positionsbestimmung führen. Spoofing-Angriffe bergen das Risiko falscher Gleiszuordnungen, ebenfalls mit potenziell gravierenden Folgen. Für die sichere Integration von GNSS in ETCS und ERTMS sind deshalb robuste Fusionsalgorithmen, zusätzliche Sensorsysteme und gezielte Abwehrstrategien unerlässlich.

Das Projekt EGNSS MATE leistet damit einen wichtigen Beitrag zur Stärkung der Cybersicherheit im Eisenbahnsektor und zeigt, wie deutsches Expertenwissen im europäischen Kontext innovative Lösungen ermöglicht.

Projektpartner und deutsche Expertise

Die Tests wurden von IABG gemeinsam mit SBB und dem Deutschen Zentrum für Luft- und Raumfahrt (DLR) durchgeführt. IABG brachte ihr Know-how aus dem Bereich Galileo Public Regulated Service (PRS) ein. Das Unternehmen verfügt über eigene Testbeds für Jamming- und Spoofing-Szenarien, die für Bahnanwendungen adaptiert wurden.

Das Projekt wurde im Rahmen des ESA-Programms NAVISP Element 2, Aktivität NAVISP-EL2-131, umgesetzt.

Ihr Kontakt

Paulo Mendes

Projektleiter und Analyst im Satellitennavigation

silveira-mendes@iabg.de

www. iabg.de