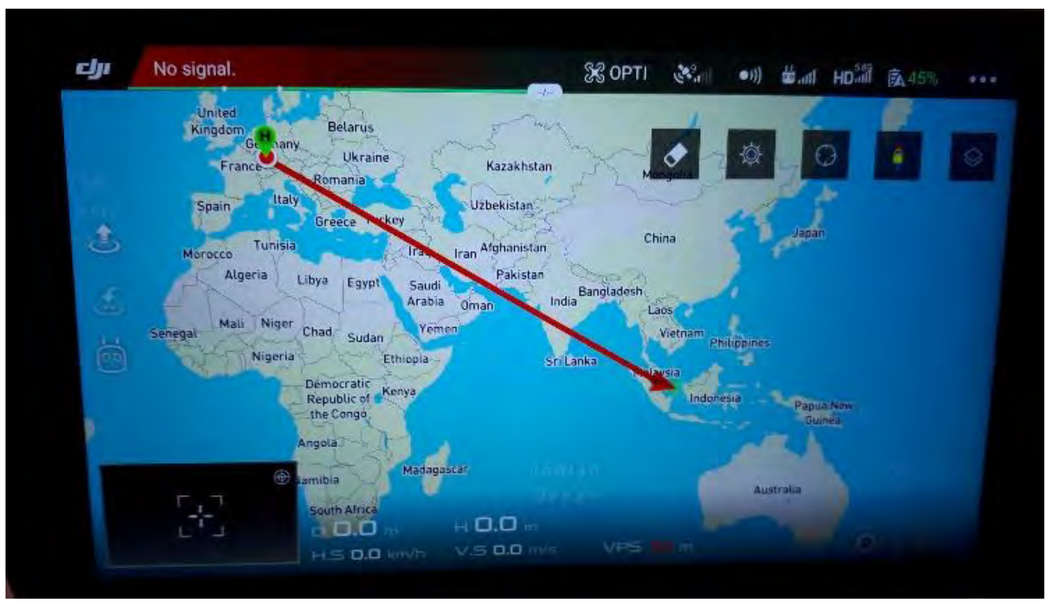
VOLOCOPTER

Hochschule Karlsruhe
Technik und Wirtschaft
UNIVERSITY OF APPLIED SCIENCES

Näher dran.

# Analyse der Gefährdung von GNSS-Navigation durch low-cost Spoofing

GNSS-Spoofing ist ein Verfahren zur Übermittlung simulierter oder manipulierter Satellitensignale. Die Auswertung des Signals liefert dem Empfänger somit eine falsche Position. Heutzutage können Spoofing-Signale mit kostengünstiger Hardware und open-source Software ohne großen Aufwand erzeugt werden. Dennoch verzichten die meisten Anwendungen auf eine Prüfung ihrer empfangenen Signale.

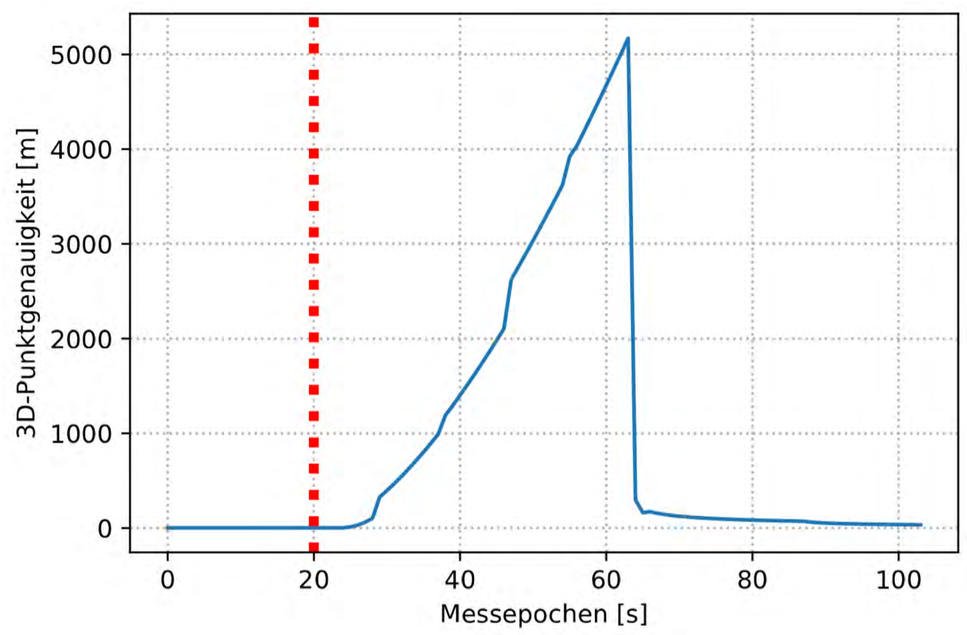



*Spoofingszenario mit der DJI Phantom 4 Pro*

## Tests mit verschiedenen Empfängern

Im Rahmen dieser Arbeit wurde ein Spoofer aufgebaut, mit dem simulierte Satellitensignale an einen Empfänger gesendet werden konnten. Die Signalgenerierung beschränkte sich dabei auf GPS. Mit dem funktionsfähigen Spoofer wurde geprüft, ob die nachgebildeten Signale von verschiedenen Empfängern ausgewertet werden können und welche Effekte dabei zu beobachten sind.
Für die Tests standen Smartphones unterschiedlicher Hersteller, Empfängermodule von u-blox und eine DJI Phantom 4 Pro zur Verfügung.

Zuerst wurden die Testobjekte in abgeschatteter Umgebung gespooft. Ohne den Einfluss realer Satellitensignale werteten alle Empfänger die simulierten Signale korrekt aus. Genauere Analysen der berechneten Beobachtungsgrößen ergaben keine signifikanten Unterschiede zwischen realen und simulierten Signalen. Änderungen konnten bei der empfangenen Signalstärke- und Qualität beobachtet werden. Bei Tests unter freiem Himmel waren Systemen, die zur Berechnung der Position mehrere GNSS-Frequenzen oder zusätzliche Bewegungssensoren verwenden, besser geschützt. Die gespoofte Position konnte dabei nicht ausgewertet werden. Wurde kein zusätzliches Verfahren verwendet, berechneten die Empfänger nach Unterbrechung die falsche Position.




*Der Verlauf der 3D-Punktgenauigkeit bei Aktivierung des Spoofers (rote Linie).*

## Spoofing-Detektion

Mit dem erlangten Wissen konnten Methoden zur Spoofing-Detektion bewertet werden. Das angewandte Spoofing-Verfahren könnte über Änderungen in der Signalstärke erkannt werden. Für fortgeschrittenes Spoofing bietet sich an mehrere Positionierungssysteme zu vergleichen. Die Analyse der Gefährdung von GNSS-Empfänger ergab eine vernachlässigte Spoofing-Detektion vieler Systeme. Einfache Methoden können eine Absicherung gegen leicht zugängliche Spoofing-Verfahren bieten.

**Hochschule Karlsruhe – Technik und Wirtschaft**
Fakultät IMM • Studiengang Geodäsie & Navigation
www.hs-karlsruhe.de
Bearbeiter: Stefan Keller
E-Mail-Adresse: kest1018@hs-karlsruhe.de
Referent: Prof. Dr.-Ing. Reiner Jäger
Korreferent: Dr.-Ing. Jan Zwiener