

Kolloquium Satellitennavigation

Real-World GNSS Spoofing and Authentication

Daniel Maier

Universität der Bundeswehr, Neubiberg

The importance of GNSS as a backbone technology increases in many areas and applications. The need of a trustworthy and reliable position, velocity and timing information is a key feature for future public GNSS services, especially for applications like road toll systems, autonomous driving or geofencing and surveillance.

To study the influences of spoofing attacks on GNSS receivers a real-world GNSS test field was developed and build up at the University of the Bundeswehr Munich (UBM). We present spoofing incidences happened in the recent years and categorize these attacks. We show how we can mimic spoofing attacks on the test field and how we evaluate them.

Additionally, we present the spoofing detection performance of GNSS signals with new induced authentication methods. Especially the new Galileo OS Navigation Message Authentication (OS-NMA) scheme, which is based on the TESLA protocol, and a new developed Spreading Code Authentication (SCA) scheme will be presented.

Datum und Zeit: Donnerstag, den 19. Dezember 2019, 17:00 – 17:45

Ort: Technische Universität München,
Gebäude N8, 3. Stock, **Raum N3823**.

Co-Organisation: Christoph Günther, Urs Hugentobler, Thomas Pany,
Roland Pail, Thomas Wunderlich, Patrick Henkel

Internet: <http://www.nav.ei.tum.de/kolloquium>