ETH zürich

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

LEO-Range:

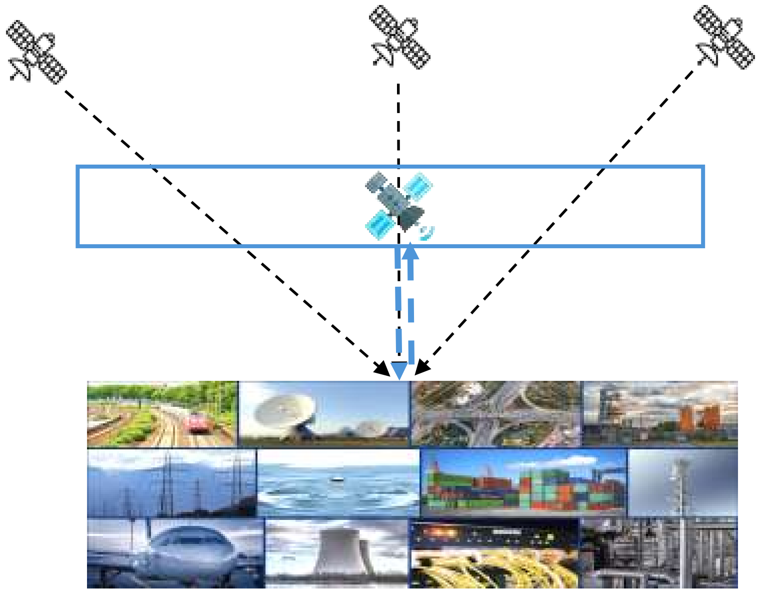
Physical Layer Design for Secure Ranging with Low Earth Orbiting Satellites

Daniele Coppola, Arslan Mumtaz, Giovanni Camurati, Harshad Sathaye, Mridula Singh, Srdjan Capkun

The problem

Existing GNSS

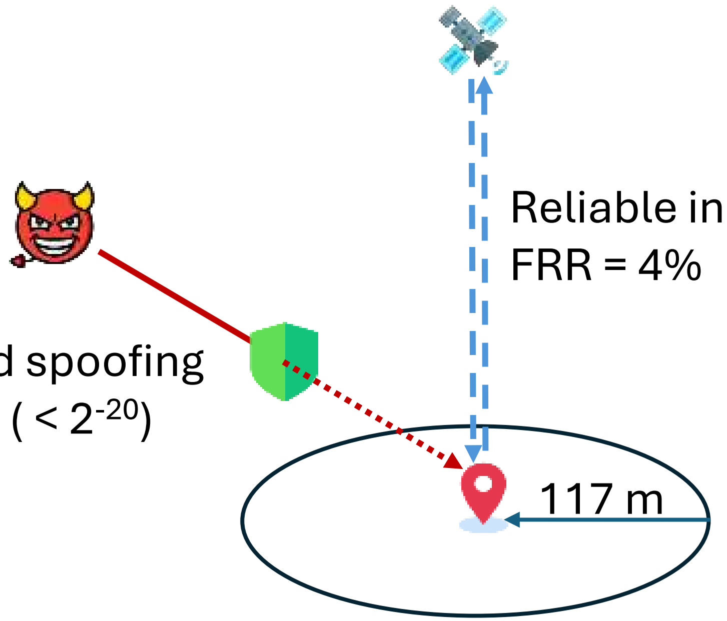
LEO-Range
Shows how to achieve secure ranging with LEO satellites



- The resilience and security of GNSS can be improved with LEO satellites
- Two-way ranging provide additional security even in case of cold starts

How to perform **secure TWR with LEO satellites**?

Our Solution: LEO-Range



Reliable in LEO channels
FRR = 4%

Bounded spoofing success (< 2^{-20})

117 m

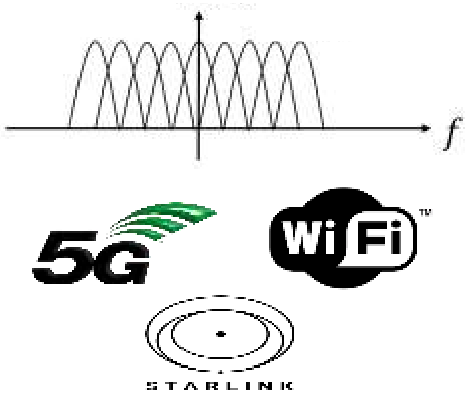
Prevents distance reductions

Prototype

- The physical signal is pushed through the channel emulator
- Closest possible testing of real LEO-Ground channels before deployment on a satellite.

Key Features

Compatibility with OFDM

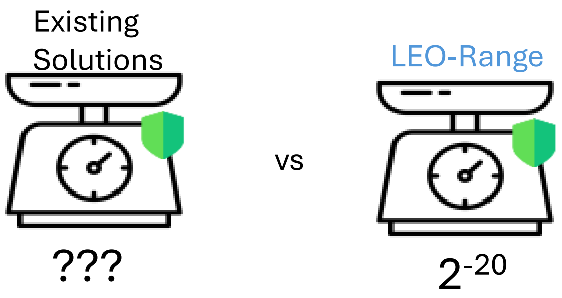


LEO-Range uses OFDM which is typical in 5G, WiFi and satellite communications

Randomized Signal

A shared key is used to encode an unpredictable secret on the OFDM waveform

Quantifiable security



Existing Solutions

???

vs

LEO-Range

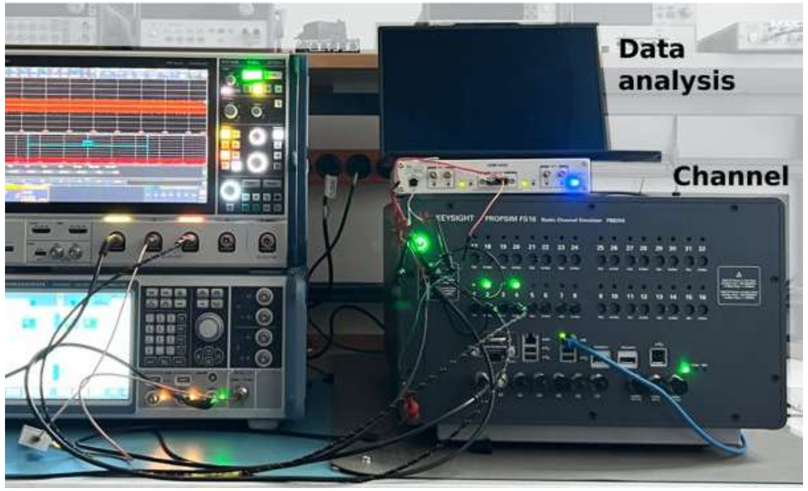
2^{-20}

Our security proof bounds the attacker success probability against arbitrary attacker strategies

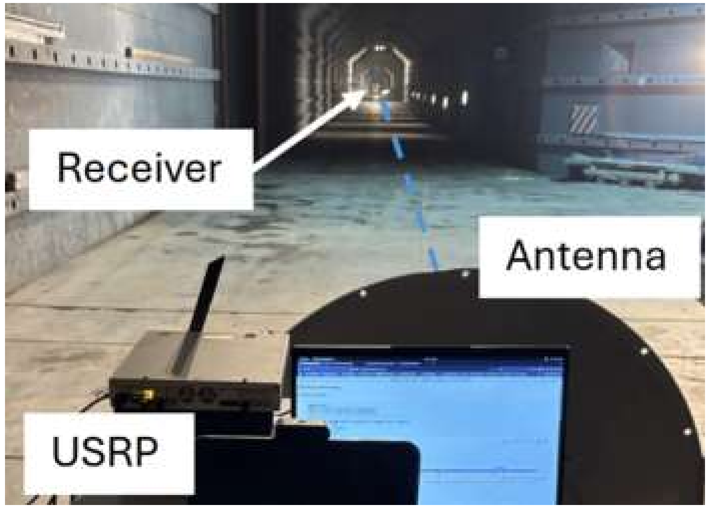
Where are we now?

Check out our paper for more details!

Hardware emulator
In field testing
Today



- New Radio (NR) **non-terrestrial network channels**
- SNR > 12 dB
- Including Doppler Effects



- USRP based prototype
- Tested on a **real channel** (stationary)

Test our system on a **real satellite**