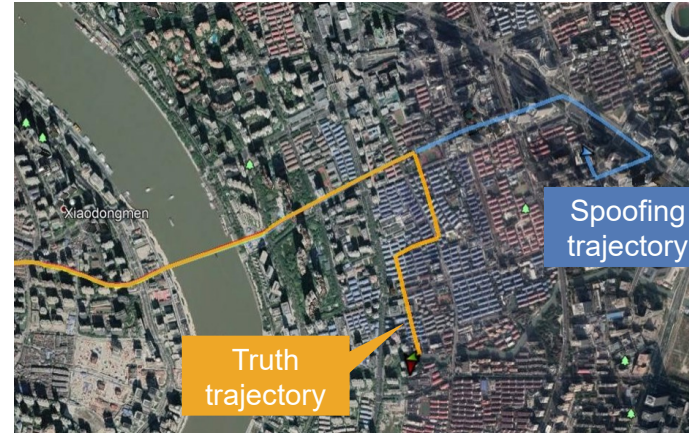
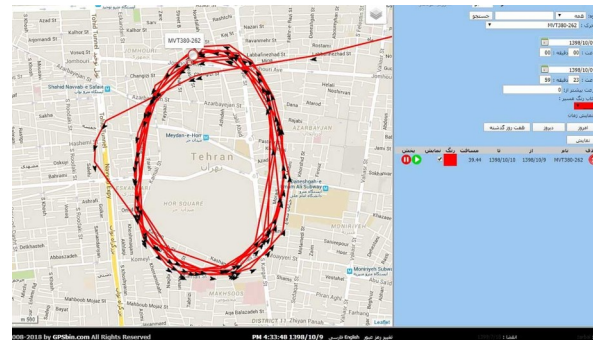


Improved Test Tools for increasing Robustness of Navigation Systems against **Spoofing** of GPS/GNSS Signals



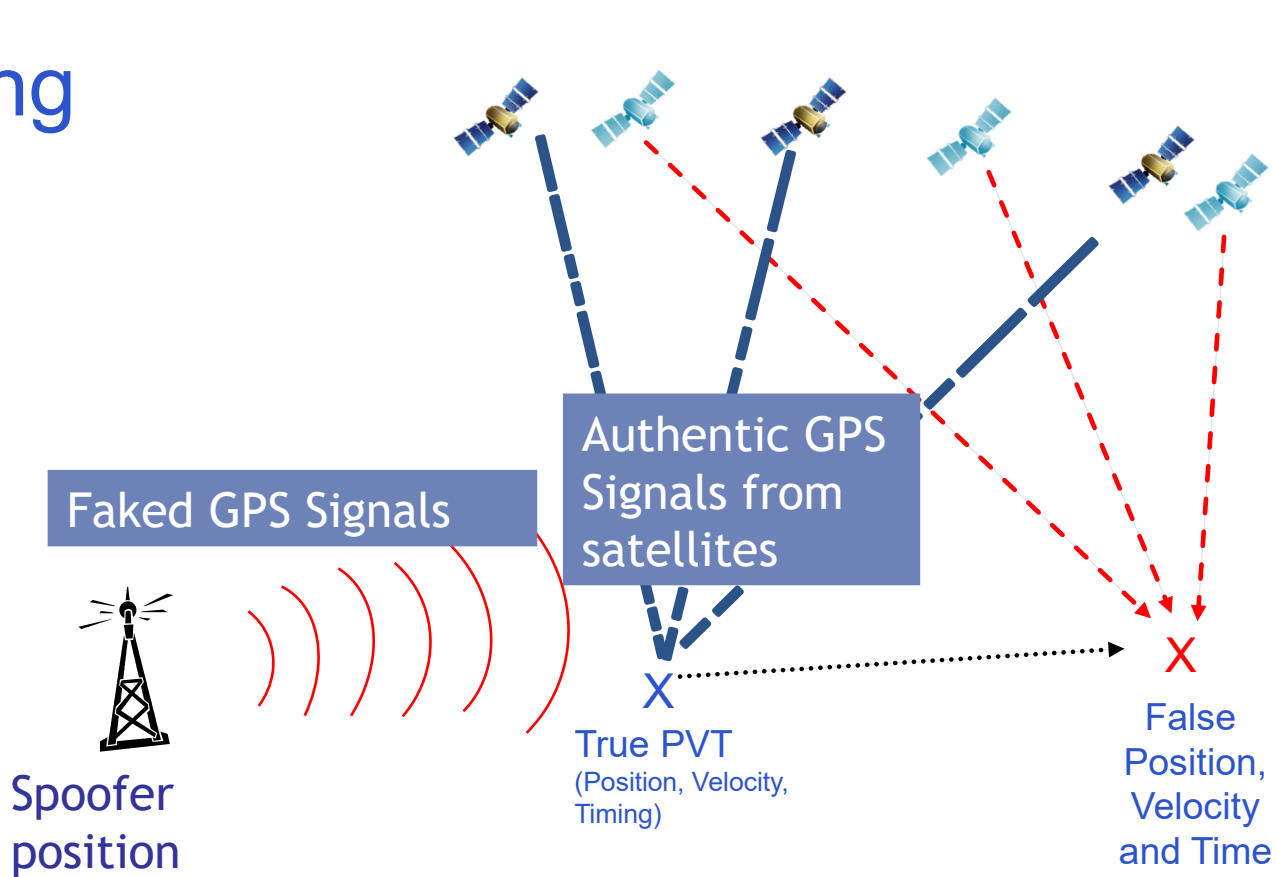
Agenda

- What is Spoofing of GPS/GNSS Signals?
- Different types of Spoofing
- Test Tools and Functions:
 - Simulator control software:
 - Multi-copy Constellation
 - Trajectory Spoofing Feature
 - New Spoofing Functions for Laboratory Tests
 - Standpoint Synchronization
 - IQ File Record and Replay



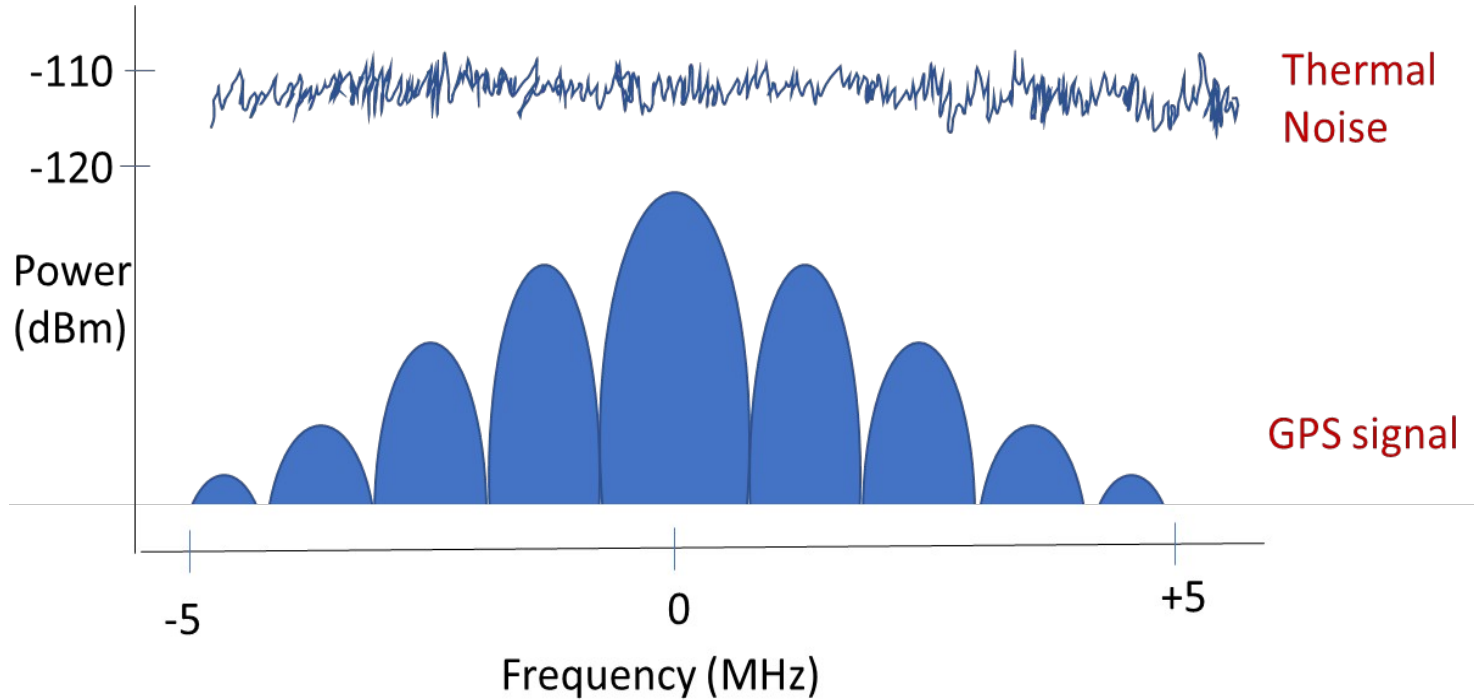
Teheran 2020 Crop Circle
Spoofing
Screenshot Dana Goward

Spoofing



Spoofing is often harder to detect than jamming

Why are GPS Signals vulnerable?





Meaconing

- The re-transmission of authentic GNSS signals
(with some inherent delay)
- Legitimate use of GNSS repeaters and pseudolites
(GNSS Global Navigation Satellite Systems)
- Example: Hannover airport 2010 – GPS retransmission in Hangar

Probability of encountering this attack

Low ● ● ● ● ● High

Impact this attack likely has on the receiver

Low ● ● ● ● ● High

Main types of RF based GNSS spoofing attacks (2/3)



Code / Carrier Attack

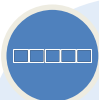
- The attacker **replicates** GNSS signals using an RF signal generator
- **and manipulates the power, code and carrier phase of the replica signals**
- in order to take control of the target receiver tracking loops.
- The attacker can then **manipulate the fake signals to spoof and control the Position, Velocity Timing (PVT) solution** reported by the target receiver

Probability *of encountering this attack*

Low ● ● ● ● ● High

Impact this attack likely has on the receiver

Low ● ● ● ● ● High



Navigation Data Attack

This uses the same equipment as a code/carrier attack

Modify navigation message content

This attack can cause

- denial of service or
- produce gross errors in the target receiver.

Probability of encountering this attack

Low ● ○ ○ ○ ○ High

Impact this attack likely has on the receiver

Low ● ● ● ● ○ High

What can be done against spoofing?

- **Detection / Monitoring**

 - z.B. GIDAS - GNSS Interference Detection & Analysis System

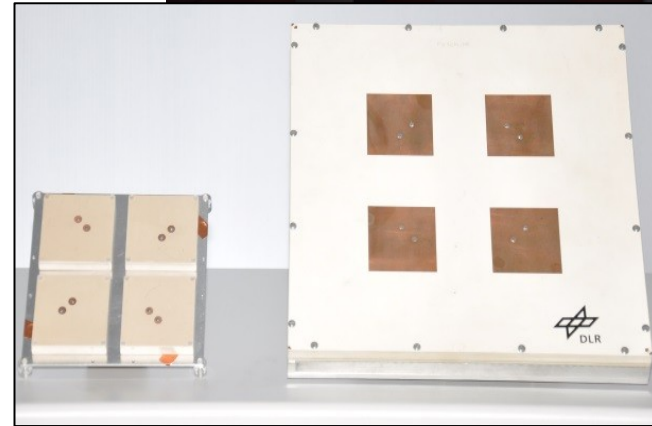
- **Mitigation,**

 - z.B. CRPA antennas

- **Testing**

 - **Field Testing**
 - **Laboratory Testing**

GIDAS system for
mobile field monitoring



Testing: Why test?

Improve robustness of receivers and navigation systems

- Use realistic scenarios
- Test spoofing attacks in different locations
- Use different types of attack
- Repeat tests as many times as necessary
- and control all test conditions
- Test and compare different mitigation methods

Advantages of Testing

Flexibility

- ▶ choose anytime, anywhere
- ▶ Recreate past events

Security

- ▶ no transmission of threat scenarios
- ▶ no need for permits

Repeatability

- ▶ regression testing
- ▶ validation of algorithms

GSS7000 and SimGEN Software

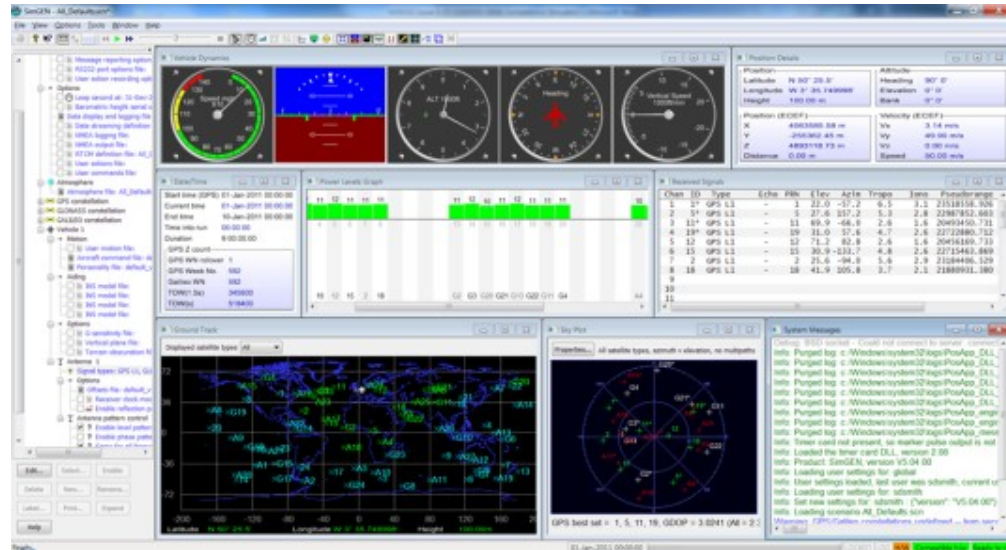
- GSS7000 is Spirent's mid-range multi-frequency, multi-constellation GNSS RF simulator with up to 256 CH



- SimGEN™ offers complete control and definition of all scenario and signal parameters (including specialist features such as the ability to user-defined constellations, **modify navigation data.**)
- Full 6 DOF remote motion for HWIL (HW in the loop) at the maximum SIR (simulation iteration rate) and full dynamic spec of the system

SimGEN™

Full capability scenario definition, signal and data modifications and errors, model parameter tuning, simulation control, 6 DOF (degrees of freedom) remote motion and comprehensive truth data



Spoofing Test functionality embedded in SimGEN

Level one

Multi-copy constellations

Trajectory Spoofing Feature

Extended Level two

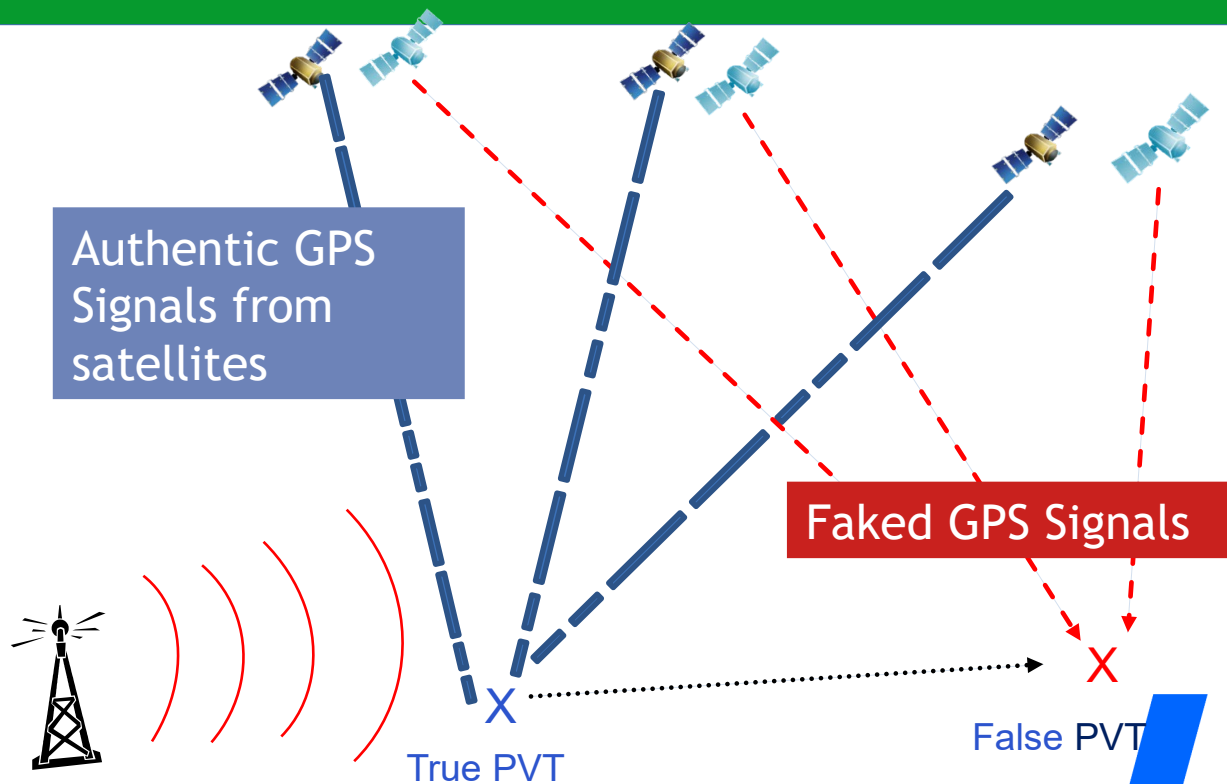
Complex Spoofer Configuration

- Multiple transmitters
- Multiple constellations
- Multiple spoofer vehicle trajectories

Level 1: Multi-copy Constellation inside SimGEN

The 'multi-copy constellation' feature allows up to 10 copies of ANY constellation to be simulated

each with full manipulation of parameters (GSS9000)



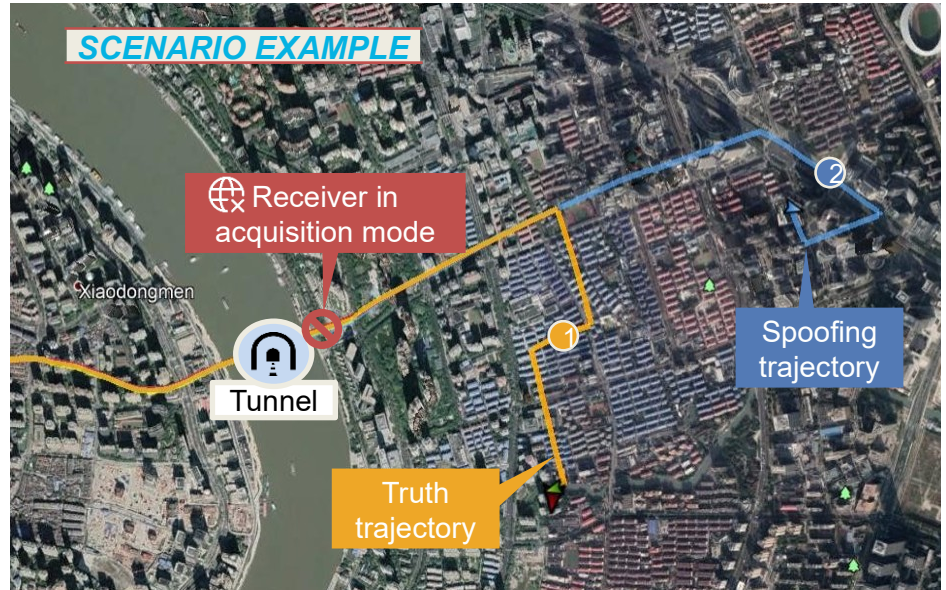
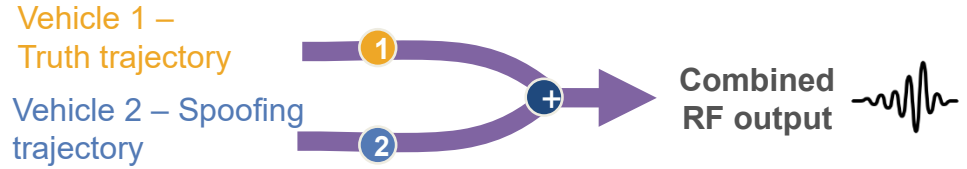
Level One: Trajectory Spoofing Feature

allowed 2 independent trajectories to be defined and send to 1 combined RF output

GSS7000 and GSS9000

One trajectory represents the authentic signals received by the vehicle and the second trajectory represents the transmitted spoofing signals i.e., the deceptive position

- An example scenario is that RF signals for each vehicle will be originally aligned until the trajectories of 2 vehicles part at the user defined time

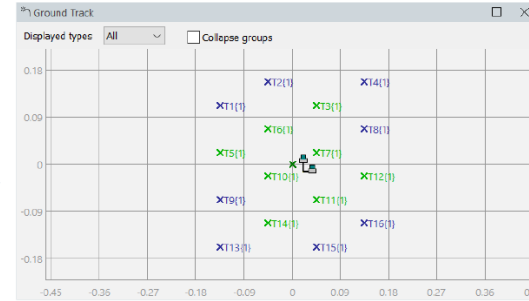


Ground transmitters

Constellation Editor

Spoof Vehicle

- Many different transmitters (64)
 - Can be arranged in a matrix over a wide area
 - Modelled or fixed signal power
 - ◆ Equivalent to multi-copy constellation
 - ◆ Change navigation message and health status
 - ◆ Almanachs, orbits, reference time and more
- Different **spoofer vehicle types** and trajectories independent of truth vehicle type and trajectory, e.g. **spoofer vehicle UAV flying, instead of land vehicle car**



Advantages: Complex Spoofer Configuration

Allows to simulate all types of spoofing attacks without limitations, including the ones of level one



Much more dynamic simulation, with several spoof trajectories possible

-- more spoof vehicles – more spoof transmitters

The resulting spoofer signal will be automatically calculated with the correct:

- Spoofer signal power level
 - Spoofer signal arrival angle
 - Spoof signal content

Allows to carry out timing attacks

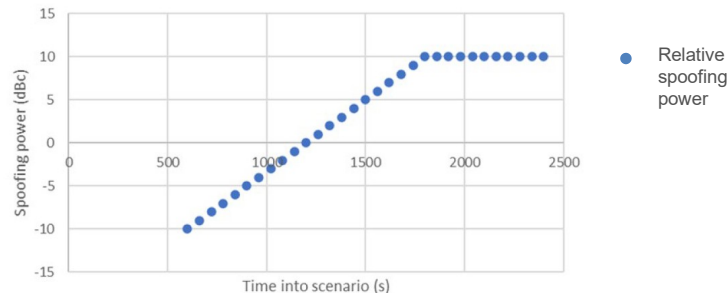
time offset between truth and spoof signals

Basic spoofing testing: Setup

a meaconing scenario based on an incident in 2010 at Hannover Airport

Spoofing Scenario

- GPS repeaters were installed to test the avionics of business jets in a hangar
- Sometimes the repeaters were in use when the hangar doors were open, **multiple aircraft experienced problems with GPS**
- *HPE – Horizontal Positioning Error*



Test scenario setup:

Vehicle 1 transmits the truth position,
Vehicle 2 is located 50 meters east of V1 and acts as the spoofing signal and is being increased in power (see chart)

Basic spoofing testing: Results

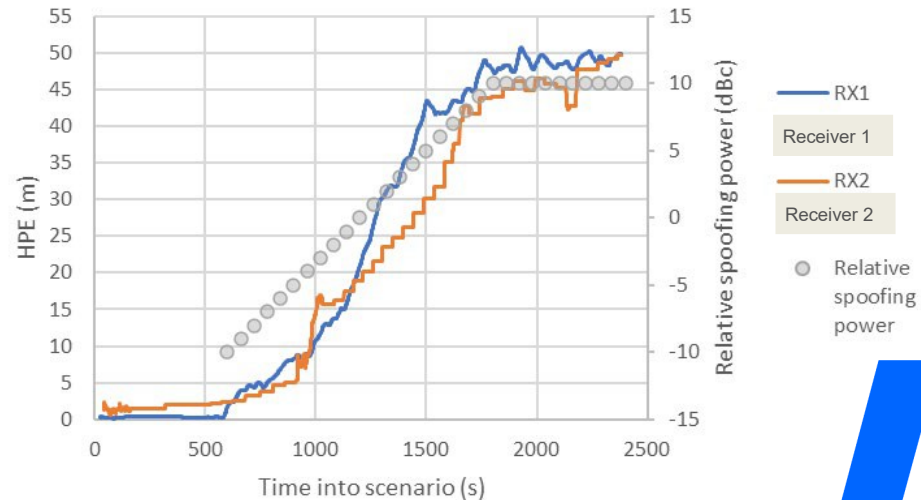
This test assessed the ability of 2 receivers to reject a fake spoofing signal

- Both receivers eventually showed large horizontal position errors (HPE) but with different underlying behavior



Almost **all** commercial **receivers can be spoofed** in certain scenarios - it is critical to **understand** the **limitations** and resulting **(mis-)behavior**

Test Results



SimIQ Capture

Capture GNSS Data into I/Q Files

- For **GSS7000** & **GSS9000**



CAPTURE

REPLAY

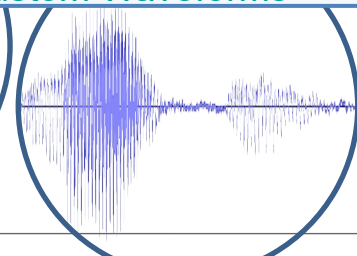
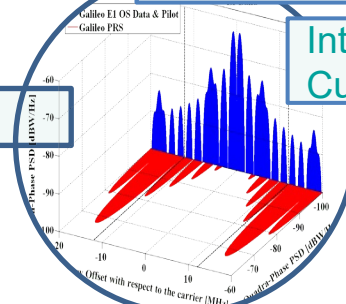
GNSS Software Receivers

Virtual Environments

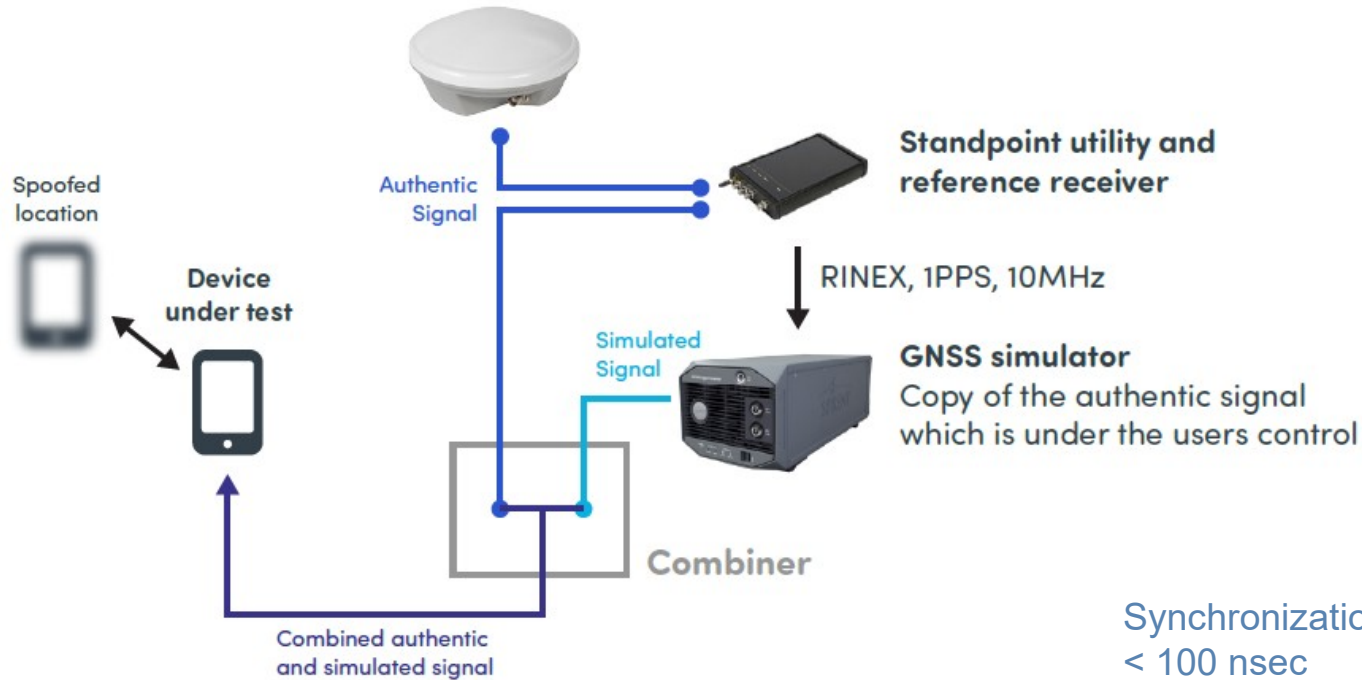


All GNSS Signals

Interference & Custom Waveforms

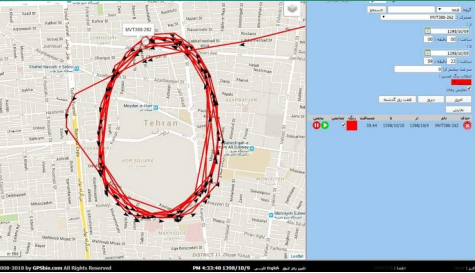


Typical standpoint configuration



- Spoofing poses a very serious threat
 - It provides misleading information, and is thus hard to detect
- What can we do: Monitoring, Mitigation, **Testing**
- **New** functions inside simulator control software to test spoofing:
 - Much more complex scenarios possible
 - All types of attacks including timing spoofing attacks can be tested
- live sky synchronization tool Standpoint (half live-sky / half simulated)
- I/Q capture and replay includes jamming and spoofing signals
- Result: complex and advanced spoofing test options to improve GPS/GNSS Receivers' robustness and resilience

Acknowledgement and Point of Contact:



Thank you to Guy Buesnel and
Matthew Haywood from
Spirent Communications

Any questions?

Lange-Electronic GmbH

Rudolf-Diesel-Str. 29A

D- 82216 Gernlinden

info@lange-electronic.com

Tel: 0049 - 8142 - 28 45 82-0

