SPOOFING AN ANDROID DEVICE

Francisco Jurado Romero

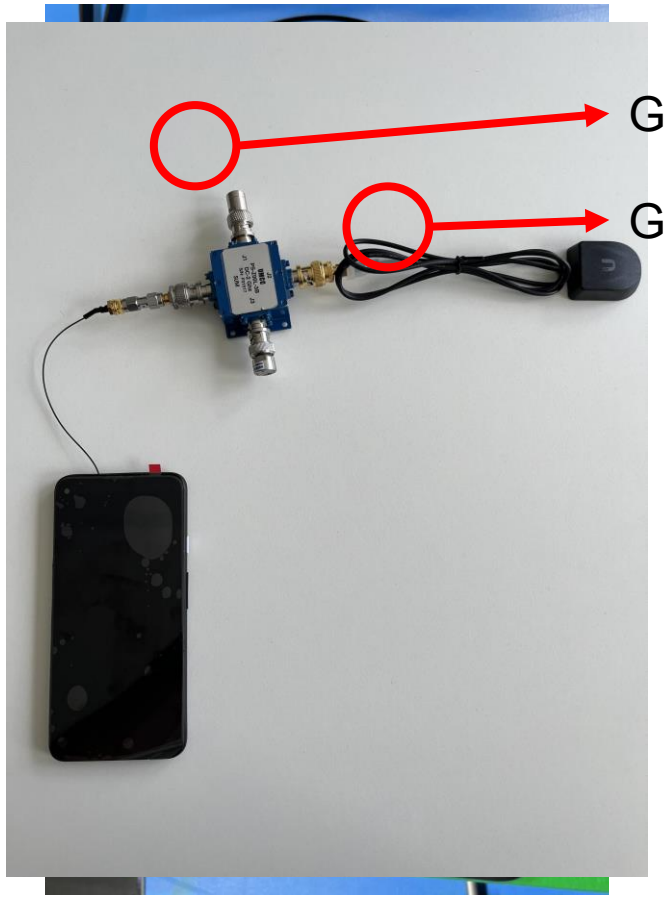
63rd CGSIC Meeting. Denver, CO

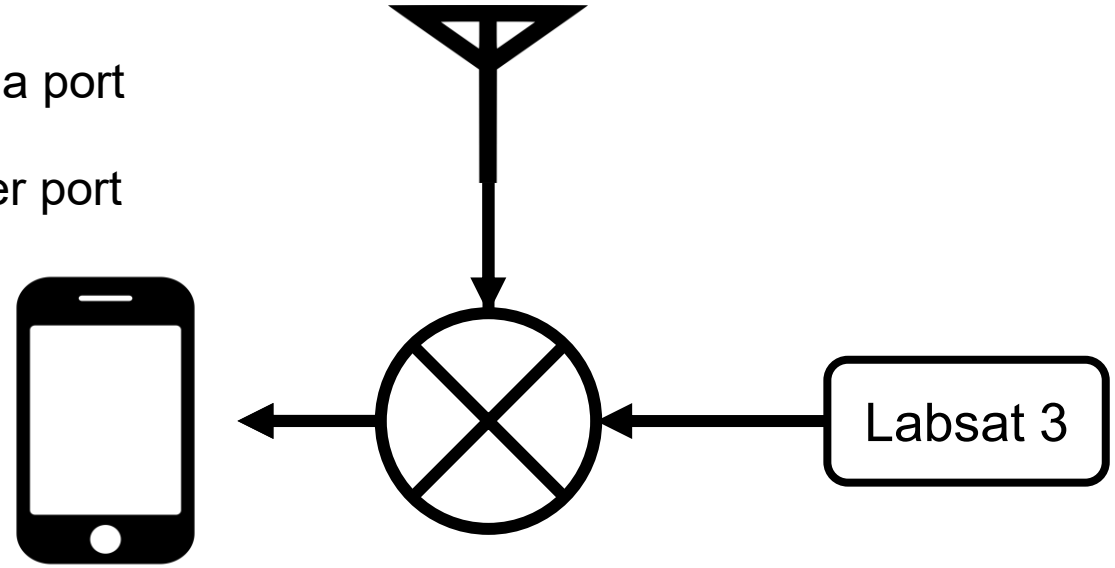
September 11, 2023

DLR


SWIPE
+RIDE
EINFACH MVV FAHREN.
Jetzt registrieren und testen
FAIRTIQ
MVV
München, Hauptbahnhof
START
6015
POST
NO ENTRY
TRAMS EXCEPTED
30
PT

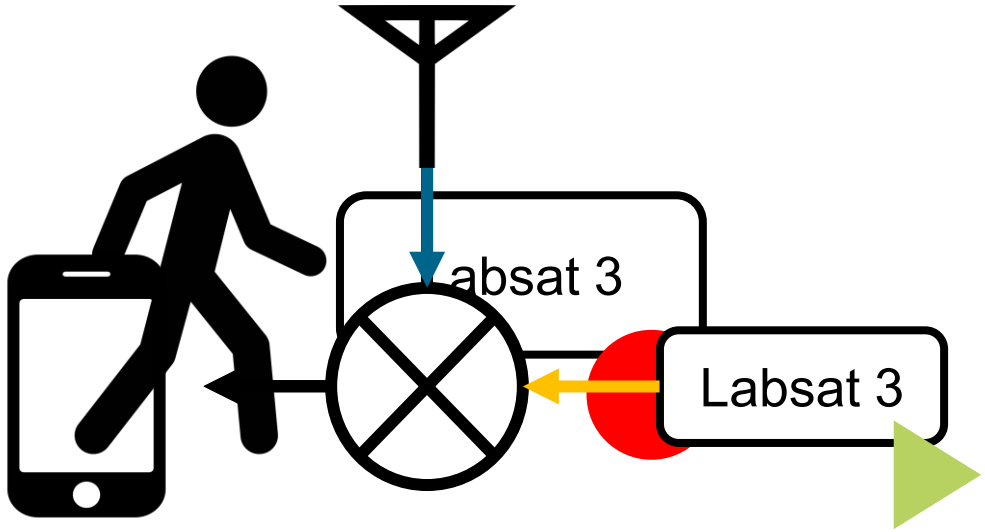
Experimental set-up

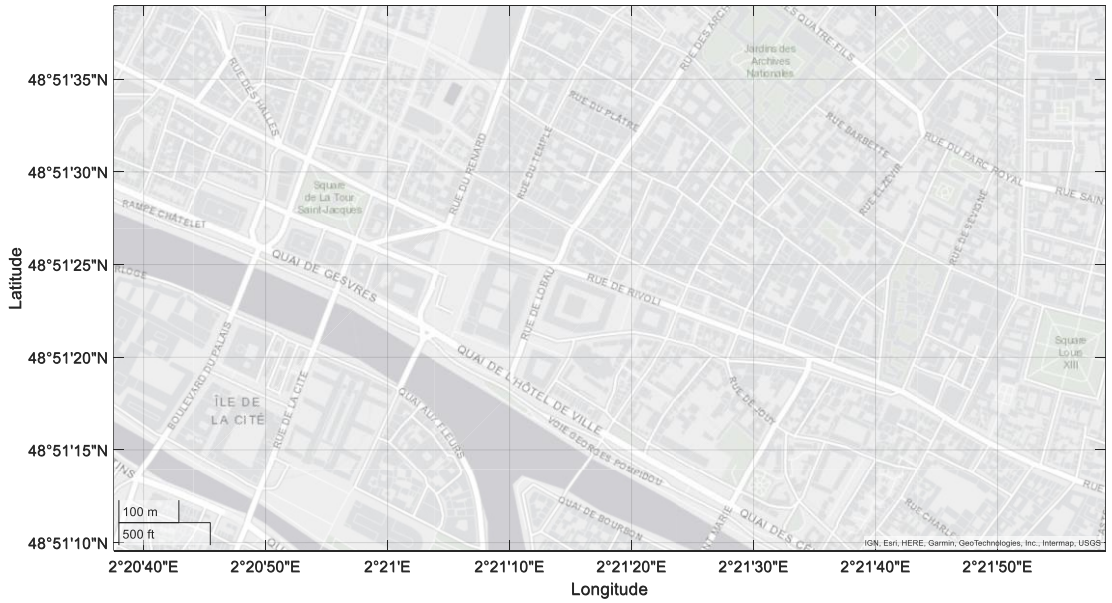


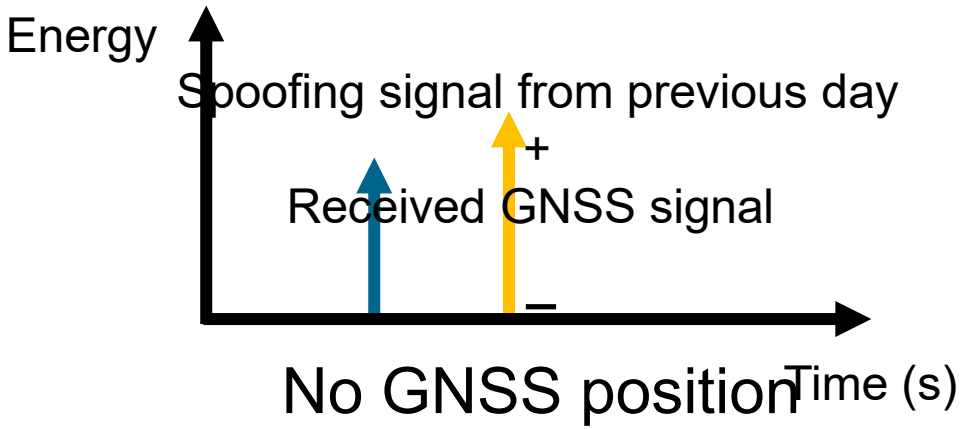


- Records raw GNSS signal
- Reproduces as generator the recorded signal

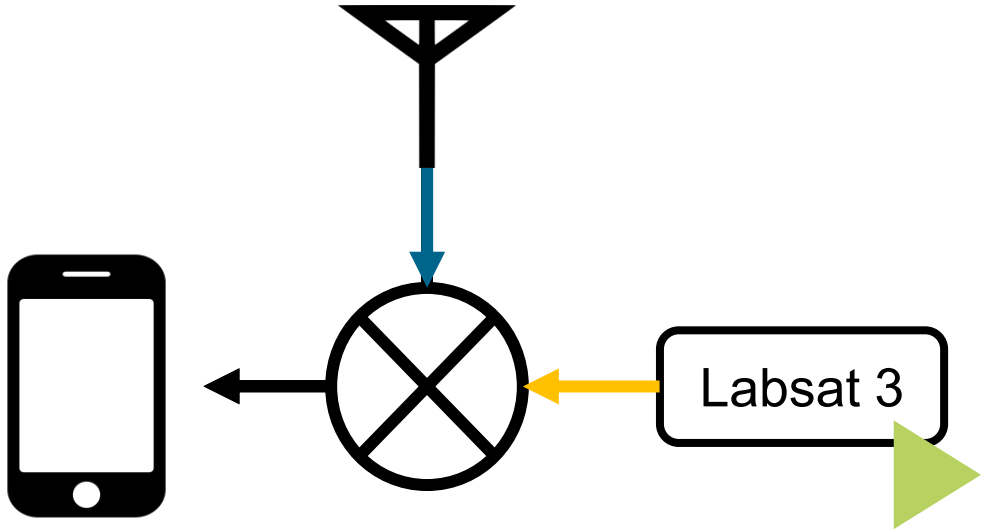
Spoofing tests in real scenarios

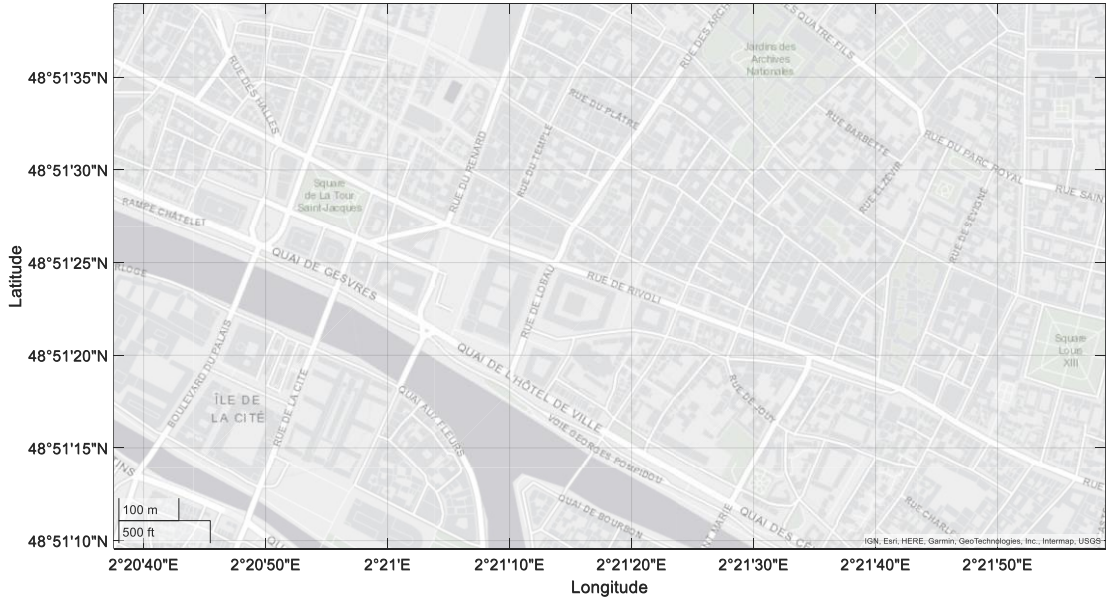






Spoofing tests in real scenarios





Spoofing signal from previous day

+

Received GNSS signal

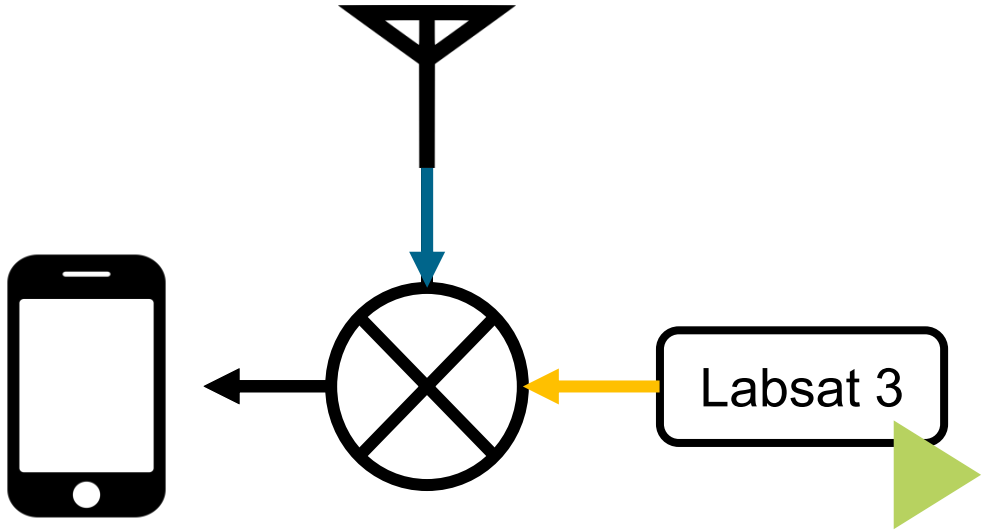
+

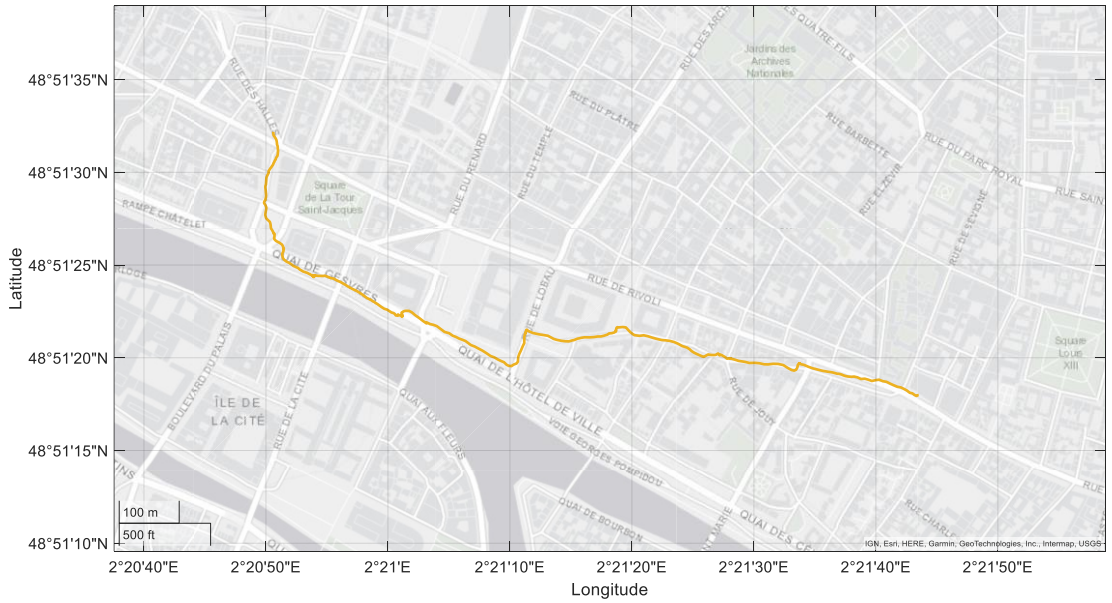
LTE, WiFi, Bluetooth: Off

=

No GNSS position

Spoofing tests in real scenarios





Spoofing signal from previous day

+

Received GNSS signal

+

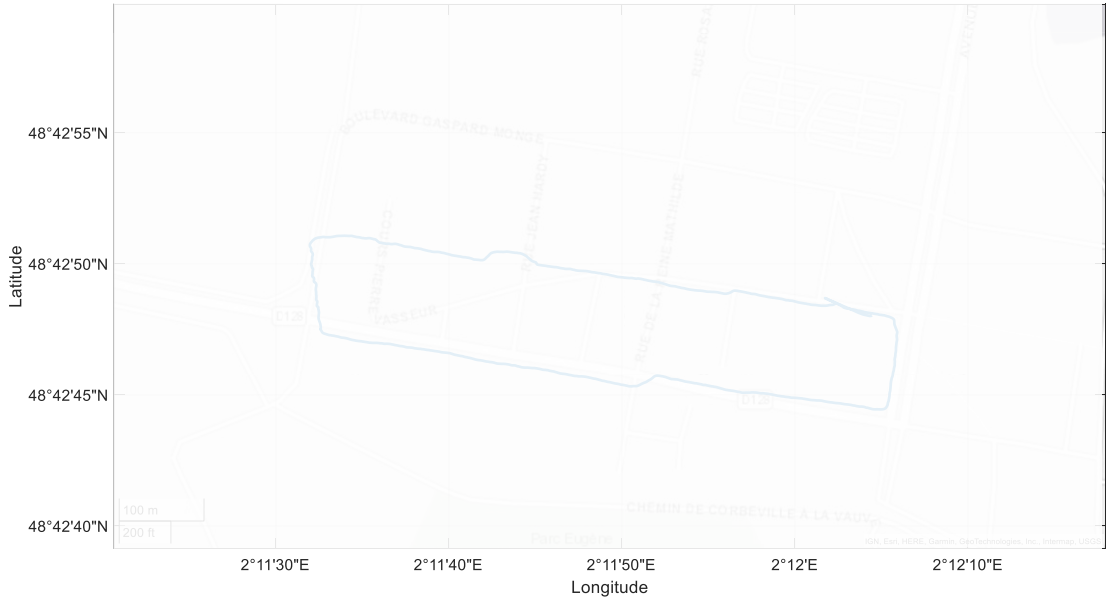
LTE, WiFi, Bluetooth: Off

+

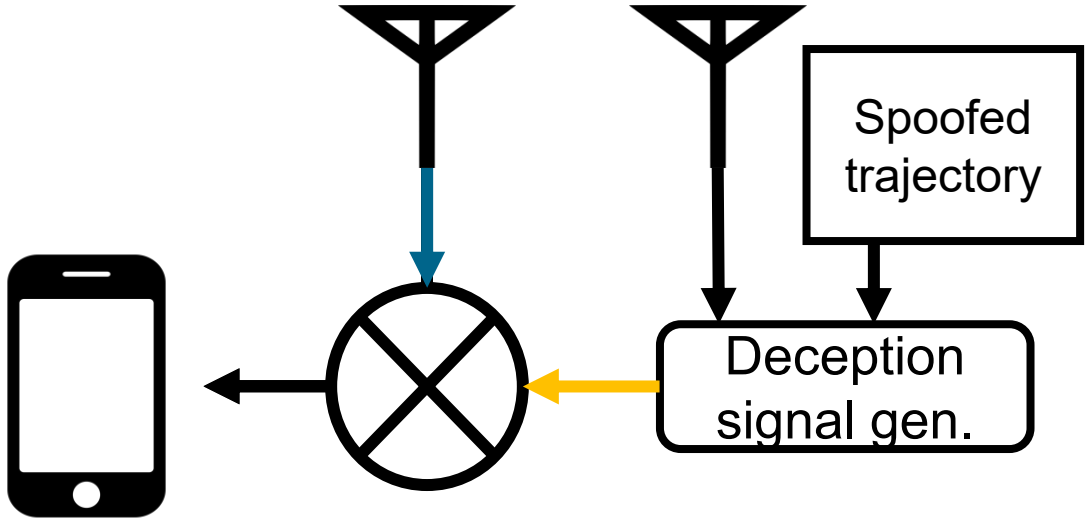
Manually setting date and time

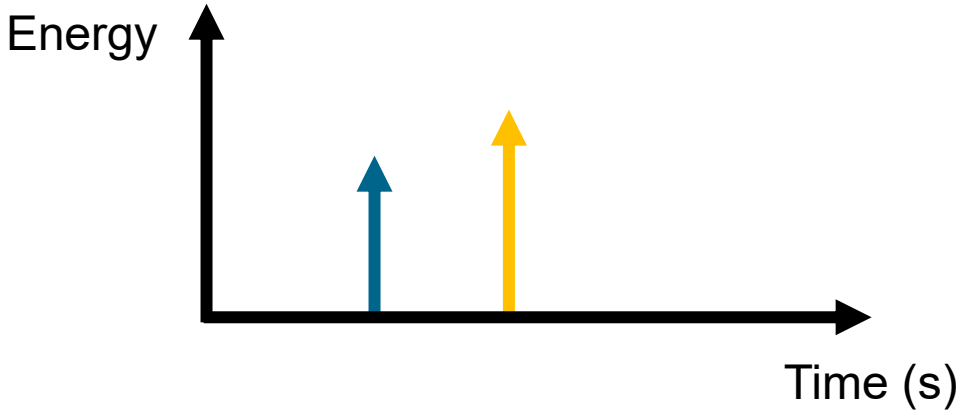
=

Spoofed GNSS position



Synchronous spoofing

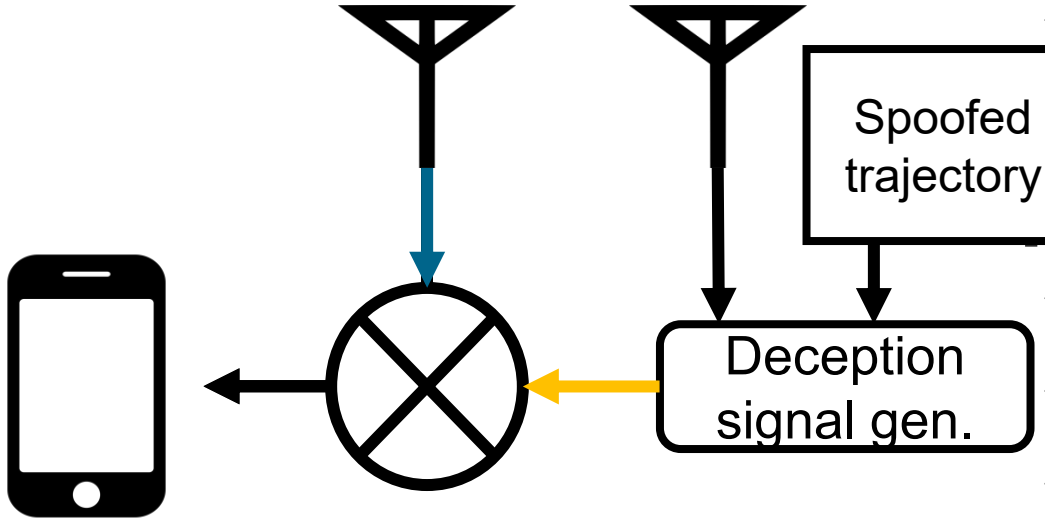


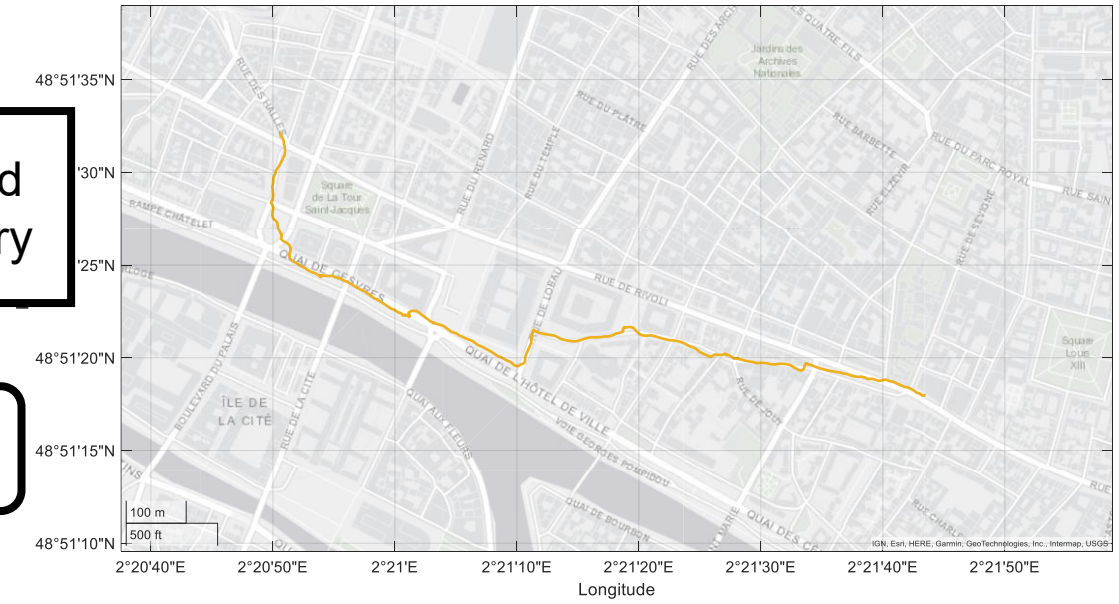


Analog Devices
AD936x System-on-Module (SoM)

- Generation of the replica signals generated locally in the receiver
- Shifted in code phase and carrier frequency.

Synchronous spoofing





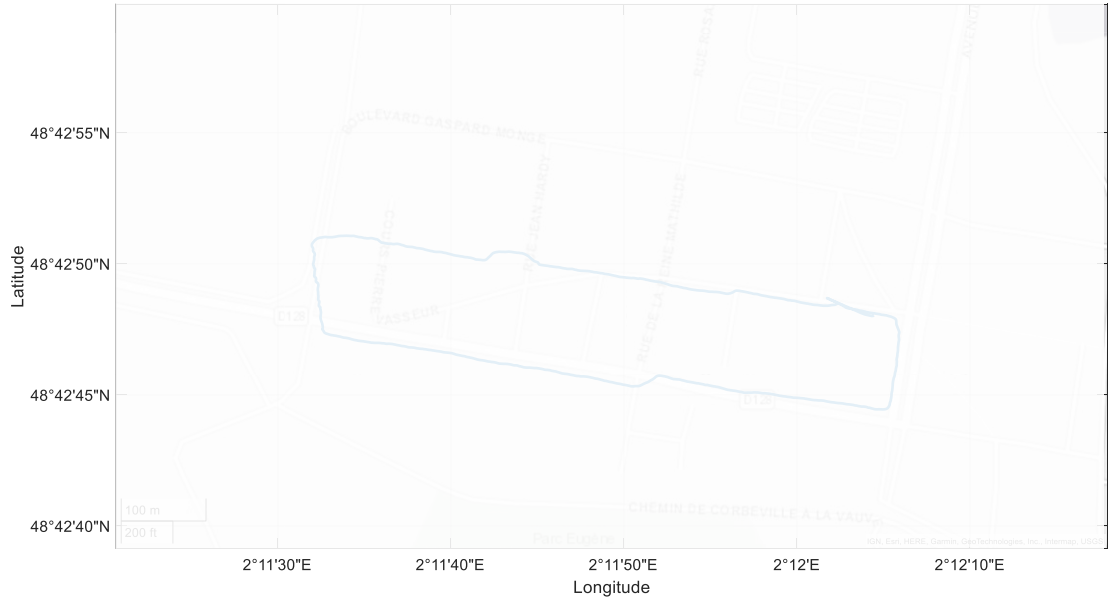
Spoofing signal from previous day

+

Received GNSS signal

=

Spoofed GNSS position



Conclusions

- It is possible to deceive the GNSS position of an Android smartphone

Asynchronous spoofing

- Android smartphones cross-check the position from GNSS with LTE, WiFi and Bluetooth positioning
- With no available network, GNSS time information is cross checked with the smartphone‘s date and time

Synchronous spoofing

- Android smartphones are vulnerable to synchronous spoofing attacks
- With a synchronized spoofer, the smartphone does not cross-check the information with any other sources of information