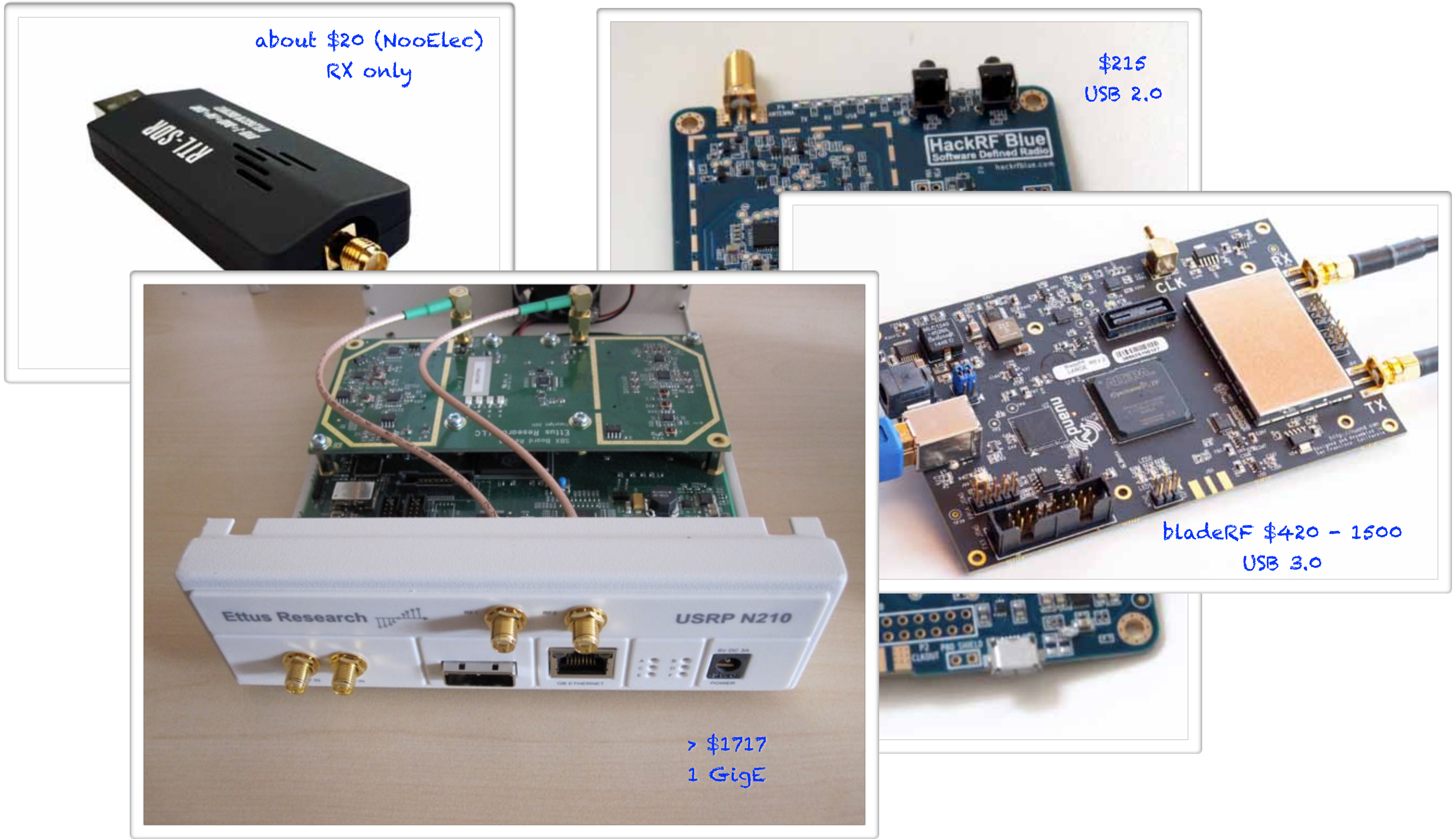
GNSS Hacking in the Wild and Cryptographic Protections

Tomas Rosa
Raiffeisen BANK

Software Defined Radio



SDR as a Threat

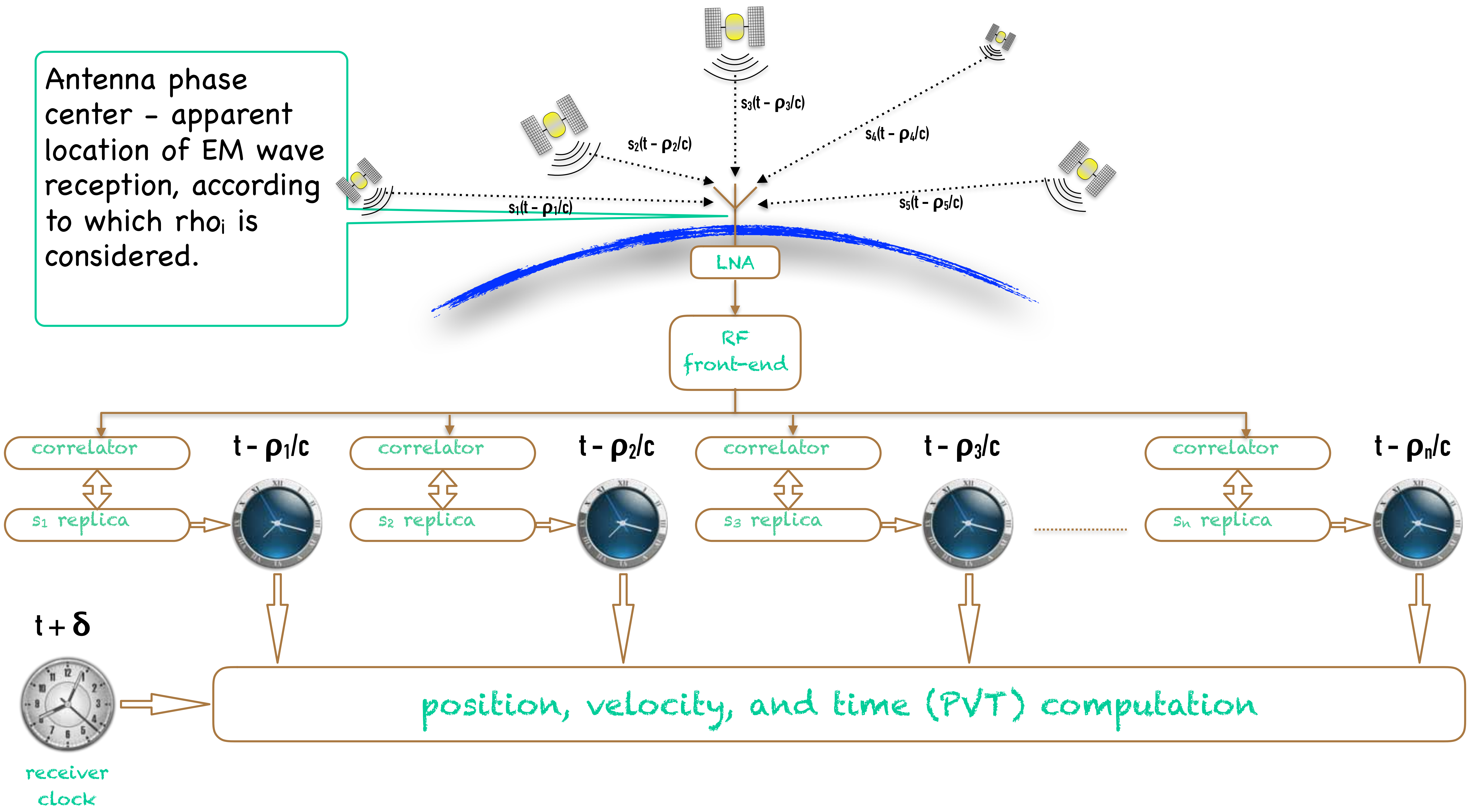
DSP routines implementing an RF attack are software, now. This can be shared, installed, and executed all around the world instantly with a very modest background.

Just like any other exploit code.

Just a Quick Recap

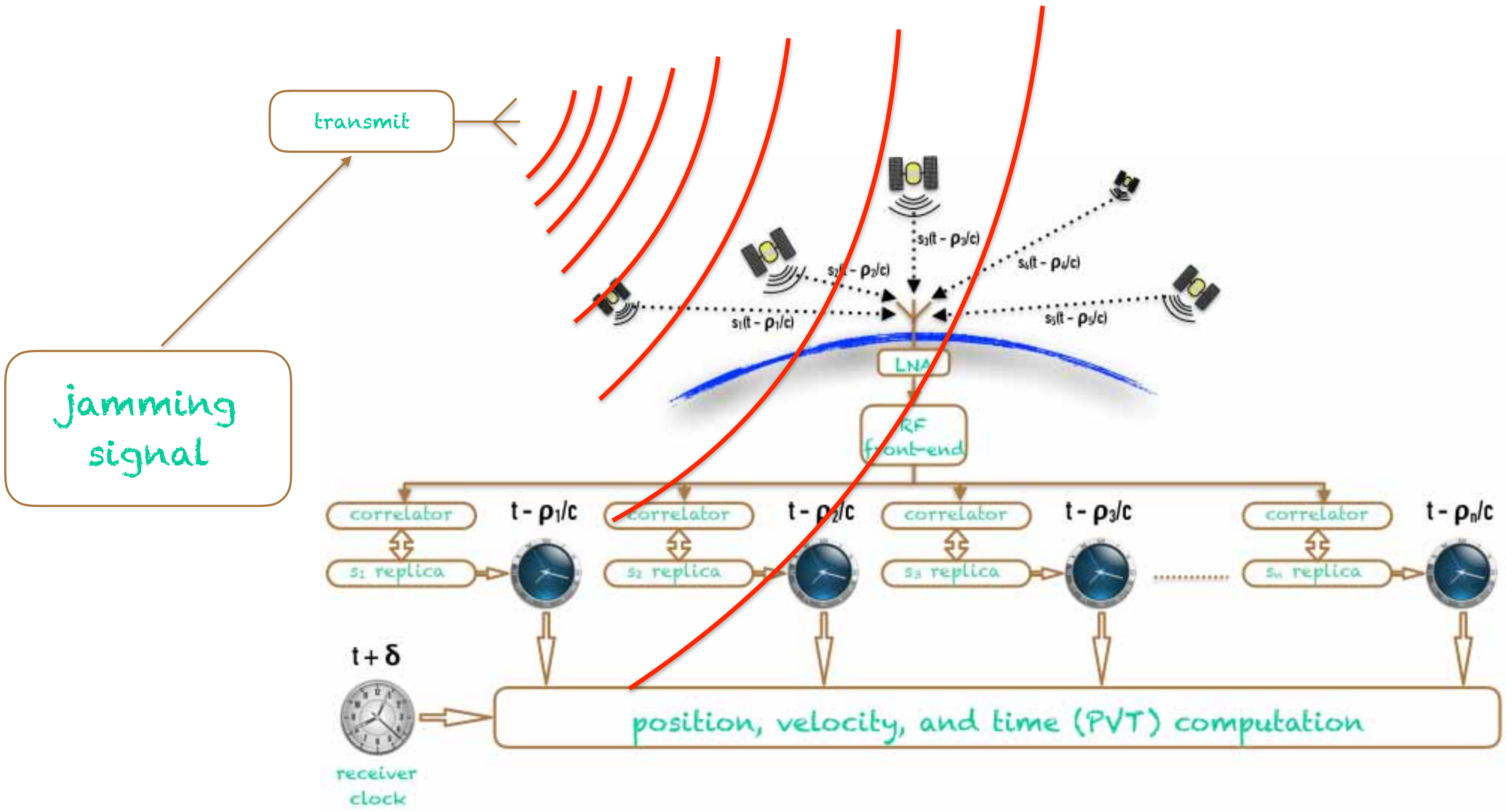
GNSS Tracking for Attacking Playground Illustration

Antenna phase center - apparent location of EM wave reception, according to which rho_i is considered.



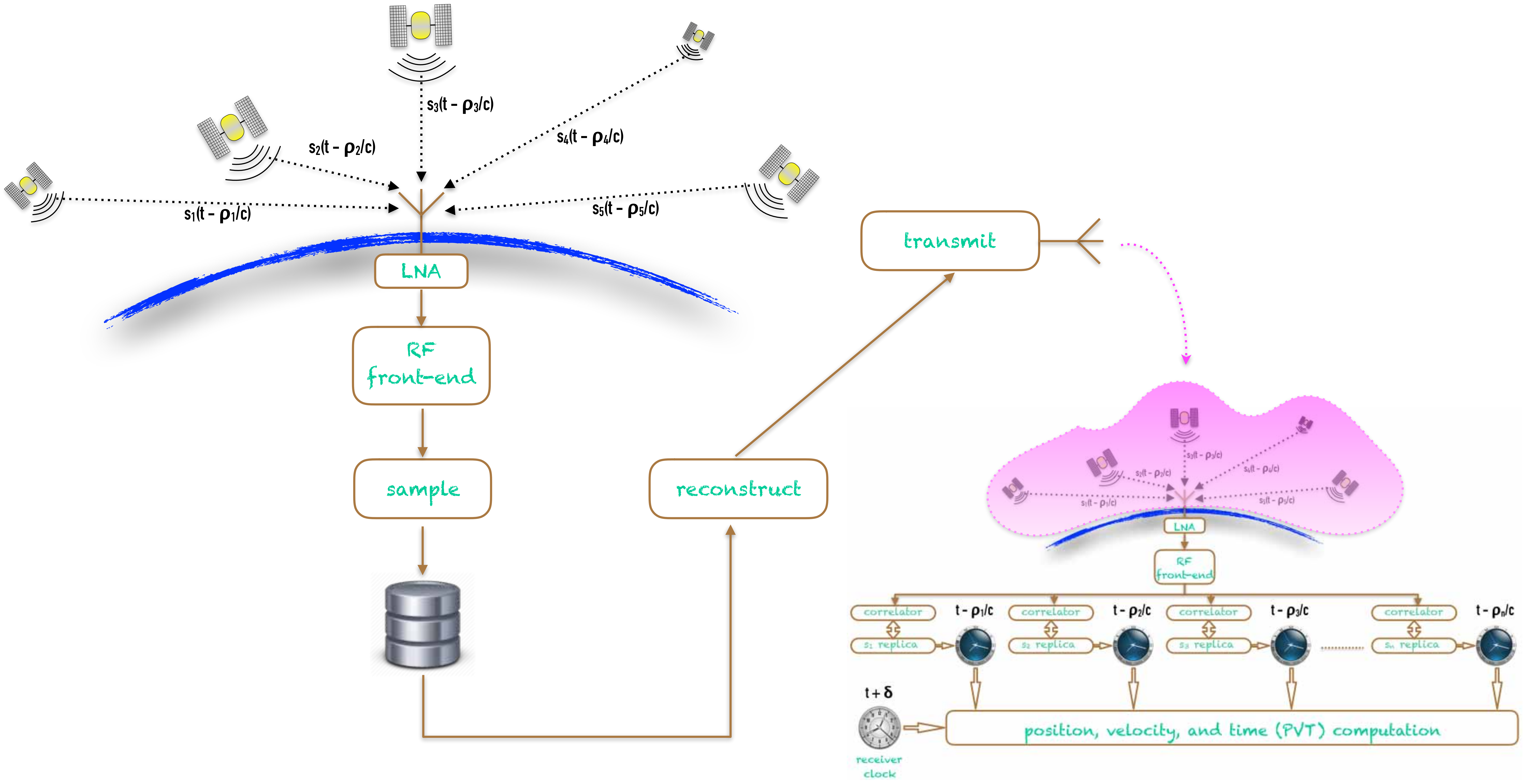
Just a Quick Recap

GNSS Jamming Attack



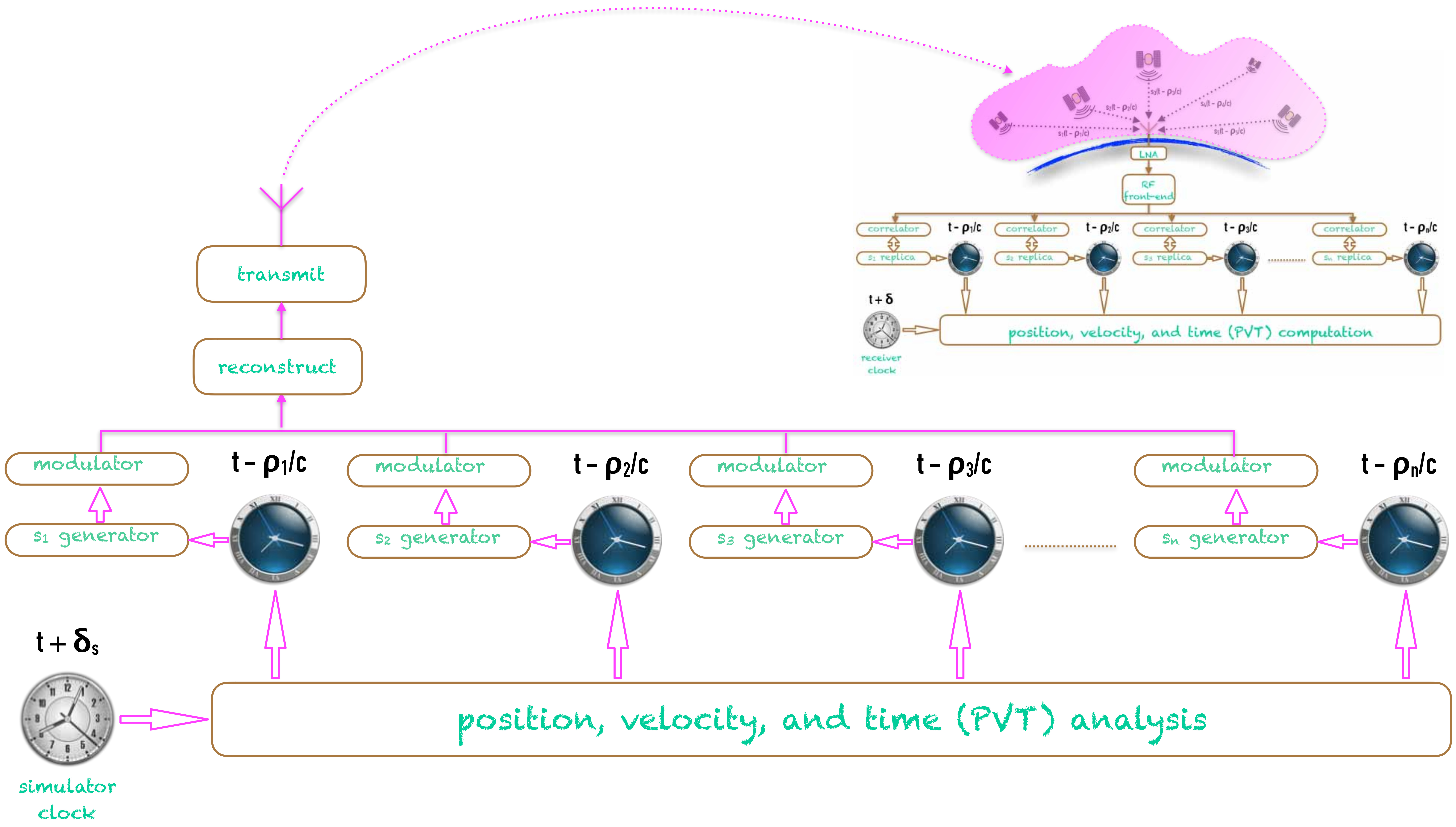
Just a Quick Recap

GNSS Replay Attack (Meaconing)



Just a Quick Recap

GNSS Spoofing Attack by Tracking Reversal



For Your Reference

Super Simple Software Used for Meaconing

- We need bandpass signal quadrature sampling and reconstruction at 1575.42 MHz for GPS L1 C/A (cf. below for GLONASS differences)

  … it was verified the **`rx_samples_to_file`** and **`tx_samples_from_file`** examples from the UHD source tree are all we need for USRP N210

  … similar radios can have similar standard utilities

- We shall carefully balance the sampling rate and word length

  … 8-bit (or even 4-bit and less) A/D resolution at 2.5 Ms/s can be well enough with a suitable RF front-end

  … recall, we still have, however, 16 bits per one I/Q complex sample then

  … from here, we can compute the storage capacity needed

- We can also employ more sophisticated frameworks, such as **GNU Radio** or even the **LabView** project at http://www.ni.com/white-paper/13881/en/

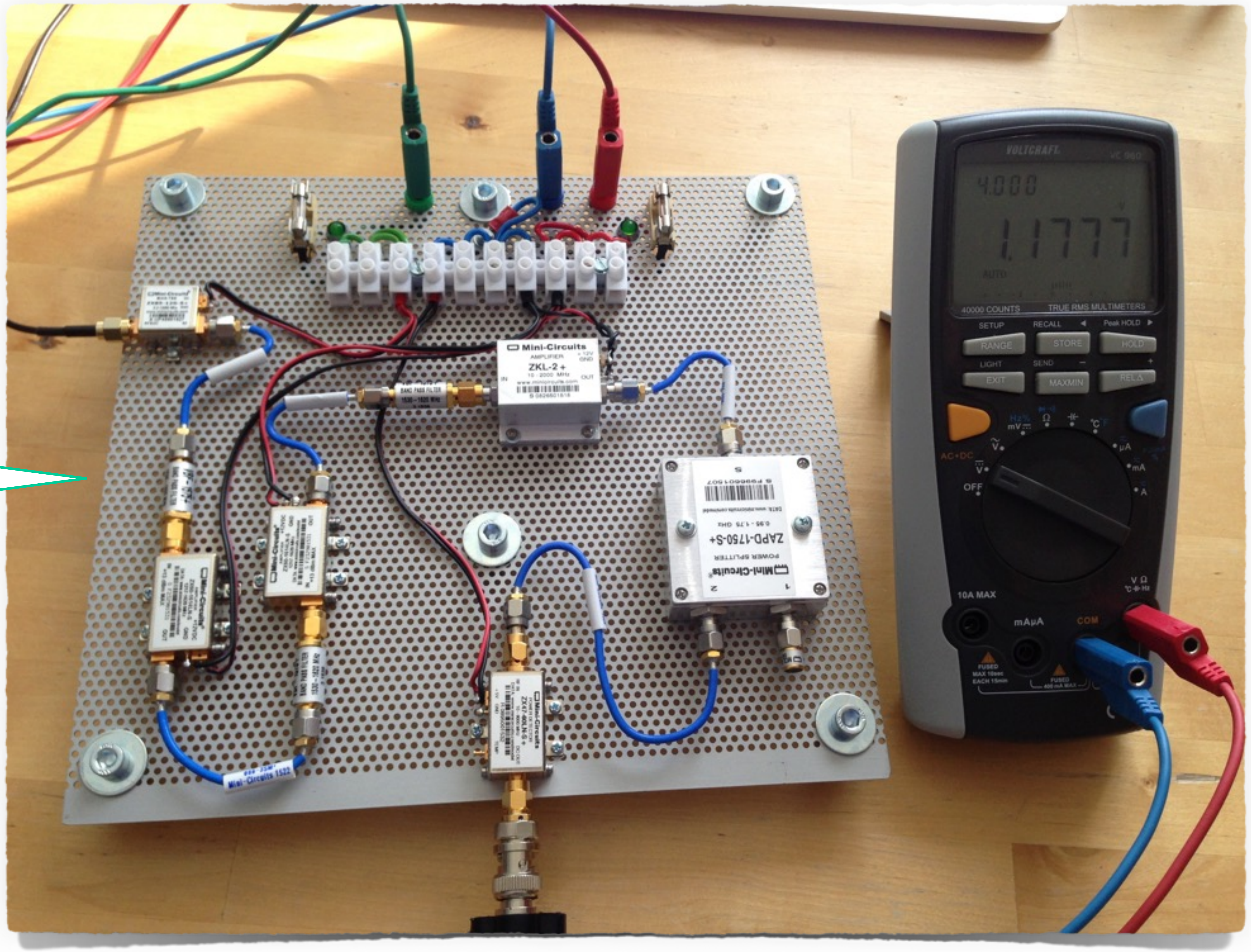
Just a Quick Preview

RF Front-End Example

Besides the internal SDR RF board, we need such an external front-end due to the extremely weak GNSS signals.

Basically, this is a versatile LNA (1530 to 1620 MHz, 49 dB typ.) featuring bias-tee, power splitter, and RSSI monitor.

Its fully based on the Mini-Circuits(R) components, so anybody can easily build their own.



Just a Quick Preview

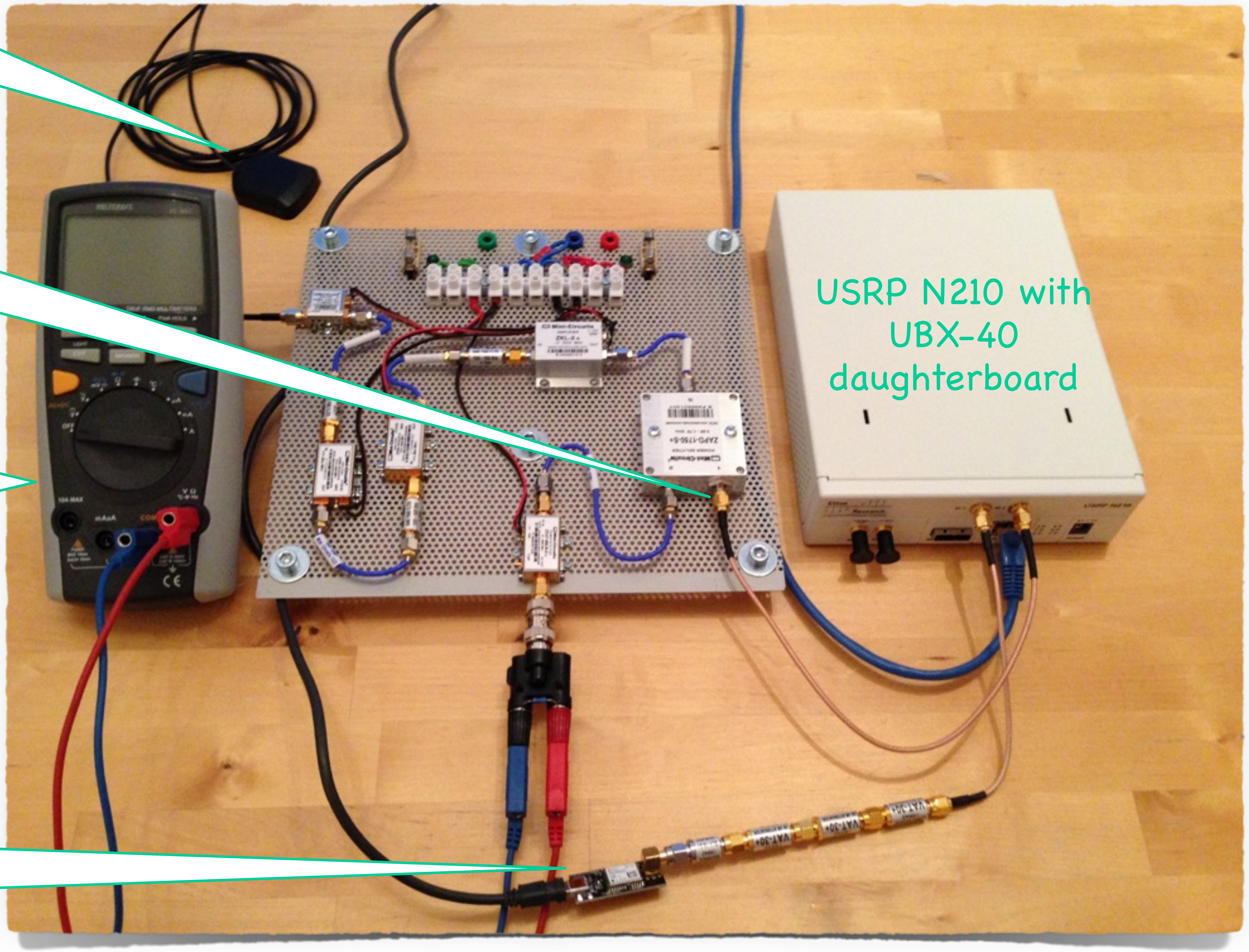
Record & Replay (Meaconing) Setup

Active antenna

Rx path delivers the original GNSS signal to be recored.

RSSI monitor checks the original RF signal received.

Later on, Tx path verifies the replayed signal with u-blox NEO-M8N GNSS receiver board via an external antenna feed and USB monitor connection.



For Your Reference

GPS L1 C/A Meaconing in Particular

- We used the following commands for our quick test GPS meaconing with USRP N210 plus UBX-40 daughterboard

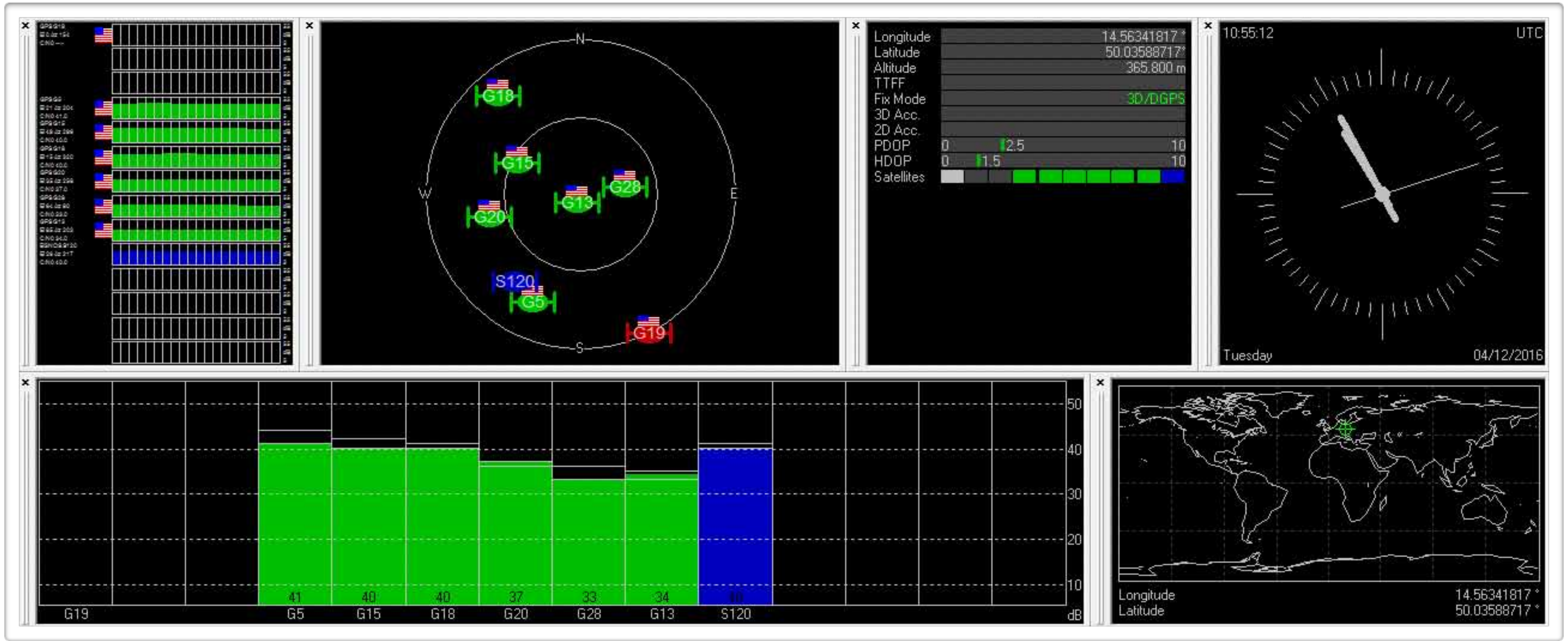
… $ **rx_samples_to_file** --type short --duration 300 --spb 1000000 --rate 2500000 --freq 1575420000 --gain 30 --progress

… $ **tx_samples_from_file** --type short --repeat --spb 1000000 --rate 2500000 --freq 1575420000 --gain 15

… that leads to 16-bit sampling (32b for I/Q pair), as we cannot go lower with the standard command line interface and it is also pretty safe and so recommended for a quick initial experiment

… we have also increased the output power amplifier gain, as to stay with same attenuators setup as in the next experiment with a synthetic signal (cf. following slides below)

GPS L1 C/A Meaconing Verification



Note we have also successfully recorded the SBAS/EGNOS signal channel PRN120 coming from Inmarsat 3F2 AOR-E. The DGPS indicator above shows this signal has already been used for a fix assurance.

Incidental Radiation

- Despite the direct shielded connection in between the SDR and demo GNSS receiver, there was an incidental radiation strong enough, so a smartphone nearby was able to get a fix to the fake signal.
- The distance to the smartphone was several meters from the table where SDR was running.
- We can imagine how powerful the attack can be if one would really decide to transmit via a full-fledged antenna.

[screenshot & idea courtesy by Jiří Buček]

For Your Reference

GLONASS Meaconing

- The L1OF (Open FDMA) service of GLONASS shares practically the same vulnerabilities as GPS L1 C/A.

  - to illustrate that, we present a replay attack on GLONASS L1OF

- There are just a few practical obstacles [Betz, 16], [GLONASS ICD, 08]:

  ... L1OF uses FDMA scheme employing several carrier frequencies instead of the CDMA on a single carrier

  ... the worldwide (exc. Russian territory) multiplex spectrum is centred at around 1602 MHz, spanning roughly 8.3345 MHz

  ... we used the NAVILOCK NL-280 GG SMA 90° GLONASS + GPS MULTI GNSS active antenna

For Your Reference

In Particular

- We used the following commands for our quick test GLONASS replay attack (meaconing) with USRP N210 plus UBX-40 daughterboard

```
... $ rx_samples_to_file --type short --duration 300 --spb 13500000000 --rate 8333333 --freq 1602000000 --gain 30 --progress
```

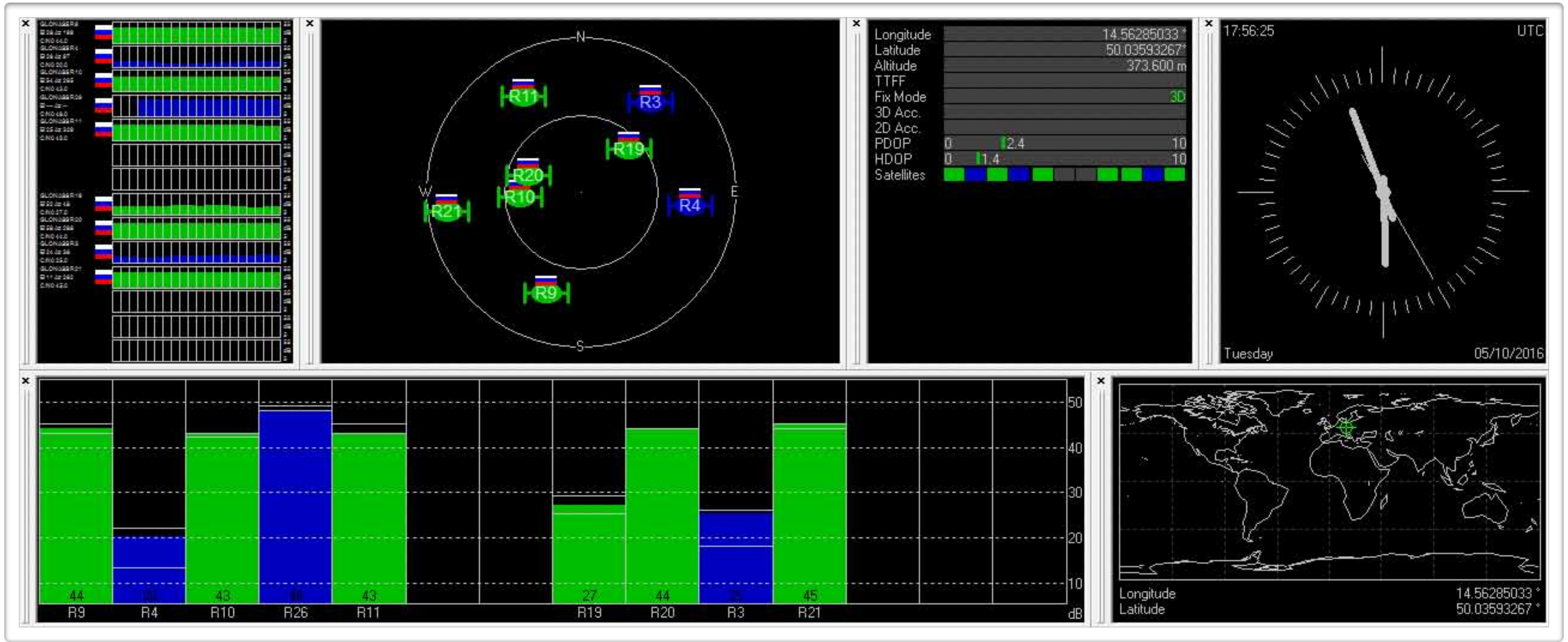
```
... $ tx_samples_from_file --type short --repeat --spb 13500000000 --rate 8333333 --freq 1602000000 --gain 15
```

... complex envelope sampling of the whole L1 Open FDMA multiplex signal

... the sampling rate used is the closest one that is possible with this SDR

... for this higher rate, the original example utilities are significantly suboptimal; we compensate this by the extremely large RAM buffer; alternatively the code can be rewritten for a higher throughput using multithreading

GLONASS L1OF Meaconing Result



Each SV in this view uses its own carrier frequency [GLONASS ICD, 08], however, we have recorded the whole FDMA multiplex centred at 1602 MHz with 8.333333… MHz bandwidth (adjusted for USRP N210 clock ratio) via bandpass signal complex sampling.

Incidental Radiation Again…

[screenshot & idea courtesy by Jiří Buček]

For Your Reference

Synthetic Signal Spoofing

- **GPS-SDR-SIM**
  - https://github.com/osqzss/gps-sdr-sim
  - GPS L1 C/A signal generator
  - its core is a compact C module `gpssim.c` that is easy to compile (provided you have OpenMP at hand)
  - generates a file with I/Q samples of the L1 C/A signal complex envelope that is ready to be transmitted via any SDR offering quadrature modulation (cf. below) in L1 band
  - the file generation runs offline, so it is not time critical
  - uses platform specific players for the final signal Tx (bladeRF, HackRF, USRP)
  - successfully used in experiments of [Wang et al., 15] as well as here; please see also further comments in its `README.md`, [Wang et al., 15], and below

For Your Reference

Software Used for Synthetic Spoofing

- The I/Q envelope samples of the spoofed GPS L1 C/A signal were precomputed using the `gps-sdr-sim` module noted above.

- We used `gps-sdr-sim-uhd.py` from the same project to modulate and transmitt the I/Q samples via USRP N210 with UBX-40 daughterboard.

  - this needs gnuradio Python framework up and ready

  - works fine, but be careful with signal parameters!

  - in the version used here (master/887079b), the default parameters for `gps-sdr-sim` produced incompatible output

  - in particular, we need to use "**-s 2500000 -b 8**" with `gps-sdr-sim` to produce correct samples for the gnuradio flow-graph implemented in `gps-sdr-sim-uhd.py`

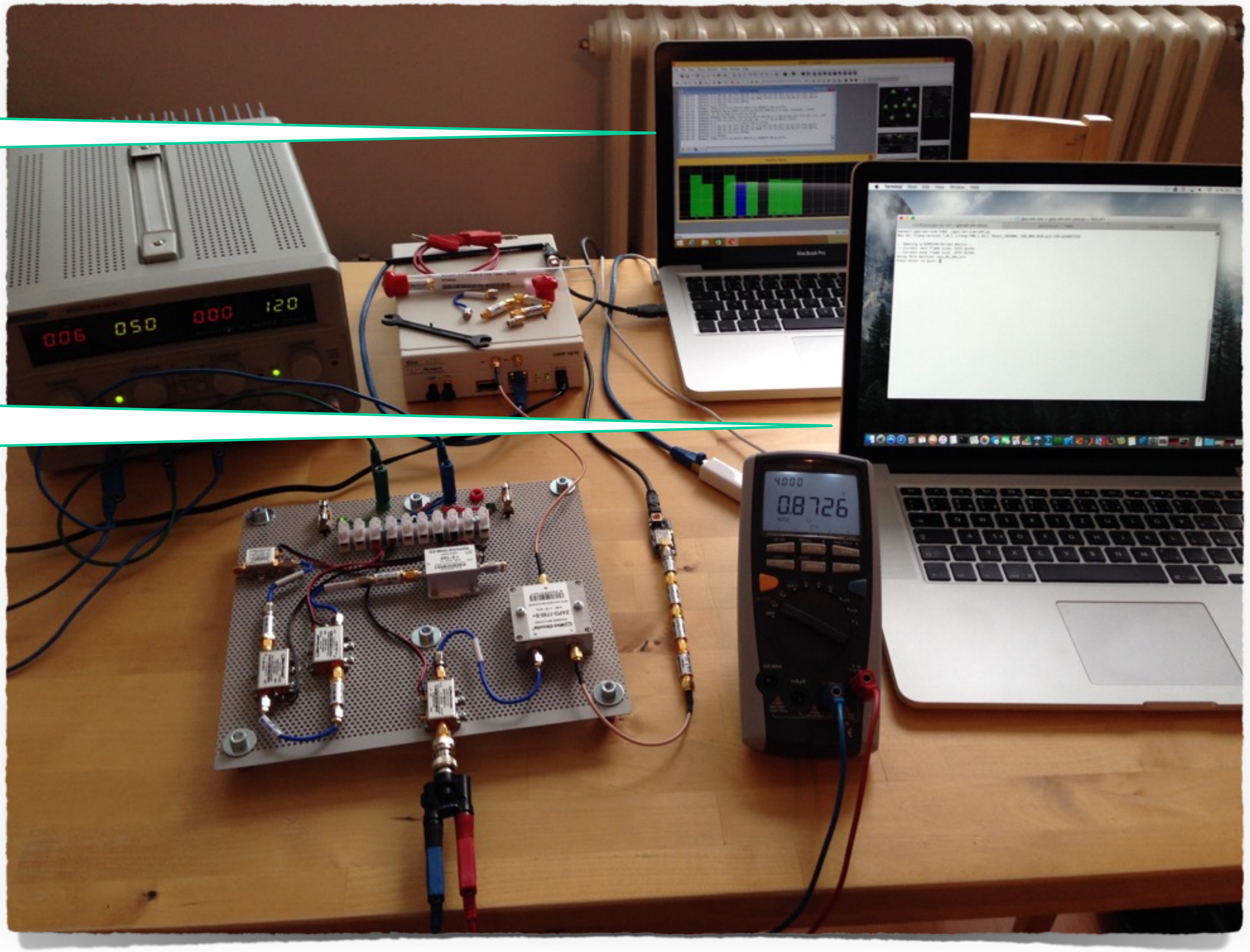
Synthetic Signal Spoofing Demo

u-center evaluation SW, running on an independent computer, confirms successful spoofing.

We can also verify the conditions of all emulated L1 C/A channels.

Spoofing machine running gps-sdr-sim-uhd.py

This in turns invokes gnuradio Python framework to transmit the L1 bandpass signal, prepared in the form of I/Q complex envelope samples, through the USRP N210.



Map View

…based on the spurious radiation again

[screenshot & idea courtesy by Jiří Buček]

The Next Target?

- There are 37 500 bits of navigation data transmitted on each and every L1 C/A channel

- It has been observed the baseband processors in GPS user modules seldom care about the integrity of this data as well as of the plausibility of PVT results obtained

... [Sheppard and Humphreys, 11], [Nighswander et al., 12]

- Interestingly, this suggests a new infection vector allowing malware installation right into the GPS receiver…

SBAS to the Rescue?

- Satellite-Based Augmentation System (in general)

  ... European Geostationary Navigation Overlay Service (EGNOS), for example, in particular

- Provides integrity report and differential corrections for the original L1 C/A signal

  ... however, it rather applies to the *transmitted signal*, instead of the signal received by the individual user station

In Other Words

"… Degradations of the received signal that occur after transmission, such as … reception of invalid signals transmitted by others, are not addressed by SBAS integrity indications. …" [Betz, 16]

Long story short, e.g. EGNOS offers practically no protection against the individual attacks discussed here.

… please see also the successful EGNOS record&replay attack in our meaconing experiment described above

… of course, this is not to say it is useless, it just serves a different purpose

So, Cryptography to the Rescue?

- It is a good initial guess, but despite having really rich cryptographic primitives portfolio nowadays, the remedy for GNSS is by no means straightforward
- We need an easy-to-implement broadcast data origin authentication that is <u>resistant to meaconing</u>

... as a general message authentication code (e.g. HMAC) alone would not do

... e.g. TESLA algorithm [Perring, et al., 02] and a suggestion for TESLA in Galileo Commercial Service (CS) enlightening the main issues [Hernandez, et al., 15]; cf. also studies in [Dovis, 15], [Humphreys, 13], [Wesson, 12]

And yes, please stop thinking like *encrypted = secured*!

Signal Space Cryptography

- **Instead of payload data, we need to protect the waveforms**

  … cryptography seldom faces such a challenge; similar issues are connected with *distance bounding protocols*

- Deeper incorporation of cryptography into the modulation scheme is needed, provided - for instance - the prevention of even a partial signal tracking is our security goal

  … as the semi-codeless tracking of L1/L2 P(Y) [Woo, 99] used routinely by e.g. EGNOS [Betz, 16] is actually nothing but a successful partial cryptanalysis of the military GPS signal protection scheme

False Alarm vs. Miss Rates

- Recognition of the presented attacks can be best formulated as a statistical signal detection problem

  … cryptographer’s main task is then to equip the signal with verifiable unpredictable patterns

- Working this way we have to carefully set the threshold in between false alarm and miss rates

- Since the false alarm rate seems to be non-negligible, we shall design a robust recovery procedure

  … this is especially true for autonomous devices in e.g. Radio Access Network of a mobile infrastructure

Conclusion

- **Software-defined radio breaks the barrier in between eager hackers and security-by-obscurity radio systems**

  … what used to be a question of deep radio understanding and practical HW skills, is now a question of a few off-the-shelf components, basic course in DSP, and widespread SW frameworks for SDR

  … in this light, the risk of many RF applications is clearly underestimated

- **Together with GSM/3G/LTE, the GPS - as well as other GNSS - civil services seem to be among the first victims of emerging massive attacks**

  … hopefully, Galileo Open Service (OS) will offer accessible and robust countermeasures even(!) for non-governmental applications

  … as it would be clearly pointless to invest such a huge effort into a brand new service that would be de facto broken by design, now*

*) Despite certain proclamations of GSA, however, the only "protection" explicitly noted in the OS SIS ICD issue 1.2 from November 2015 besides a forward error correction code is a simple CRC.

Please Consider Also The Extended Technical Version Containing Further Details and References

http://crypto.hyperlink.cz/files/rosa-qubit-2016.pdf

Acknowledgements

The author is grateful to Jiří Buček (FIT CTU), Tomáš Jabůrek (RBCZ), Radek Komanický (RBCZ), and Martin Opava (truconneXion).

They all have contributed with non-trivial help to make this research possible and pleasant.