Cyber Breakfast - Crime in the Radio Field

Tomas Rosa, Raiffeisen BANK Cryptology & Biometrics Competence Centre

Cryptology and Software-Defined Radios

Cryptology

- Cryptography
  - design of mathematical/physical methods for information protection
  - security based on intractable noise or presumably hard problems
- Cryptanalysis
  - searches for the ways on how to break cryptosystems
  - by solving those supposedly intractable or hard problems

Security Notions

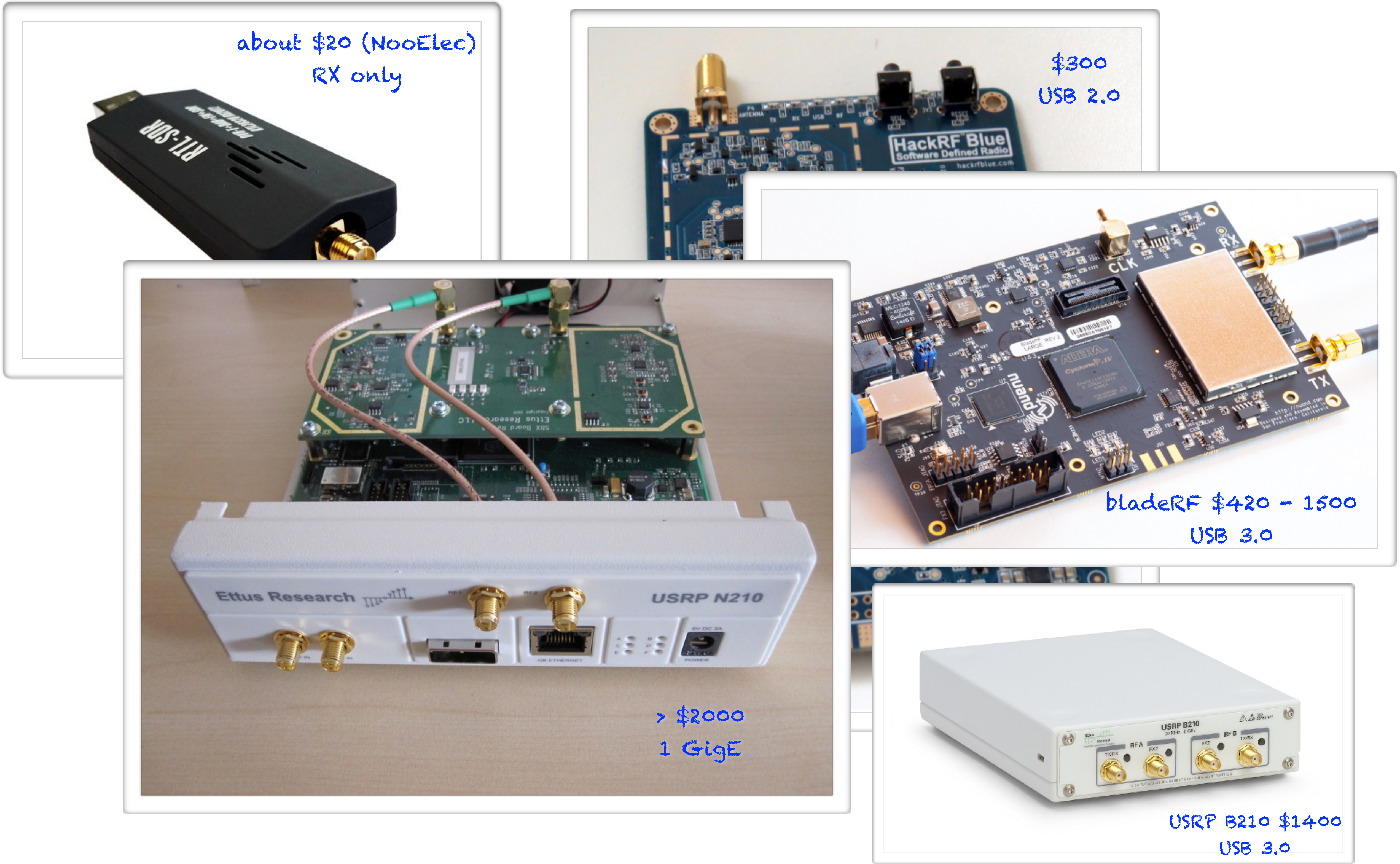
- Information-theoretics viewpoint
  - perfect secrecy
  - $\Pr[M = m \mid C = c] = \Pr[M = m]$
- Computational complexity approach
  - practical security against attackers with a limited computing power
  - AES, SHA-2/3, RSA, (EC)DSA, (EC)DH, etc.

Protocol Failures

The way we present research results

The way we really get them…

Software Defined Radio



about $20 (NooElec)
RX only

$300
USB 2.0

bladeRF $420 - 1500
USB 3.0

> $2000
1 GigE

USRP B210 $1400
USB 3.0

Baseband Sampling Theorem (ST)

- Let *s*(*t*) be a Fourier-integrable signal having its highest non-negligible frequency $|f_{max}| < f_s/2 = 1/(2T_s)$.

- Such *s*(*t*) can be then accurately reconstructed from its discrete-time samples as:

$$s(t) = \sum_{k=-\infty}^{\infty} s(kT_s) \frac{\sin \pi(\frac{t-kT_s}{T_s})}{\pi(\frac{t-kT_s}{T_s})} = \sum_{k=-\infty}^{\infty} s(kT_s)\,\mathrm{sinc}(\frac{t-kT_s}{T_s})$$

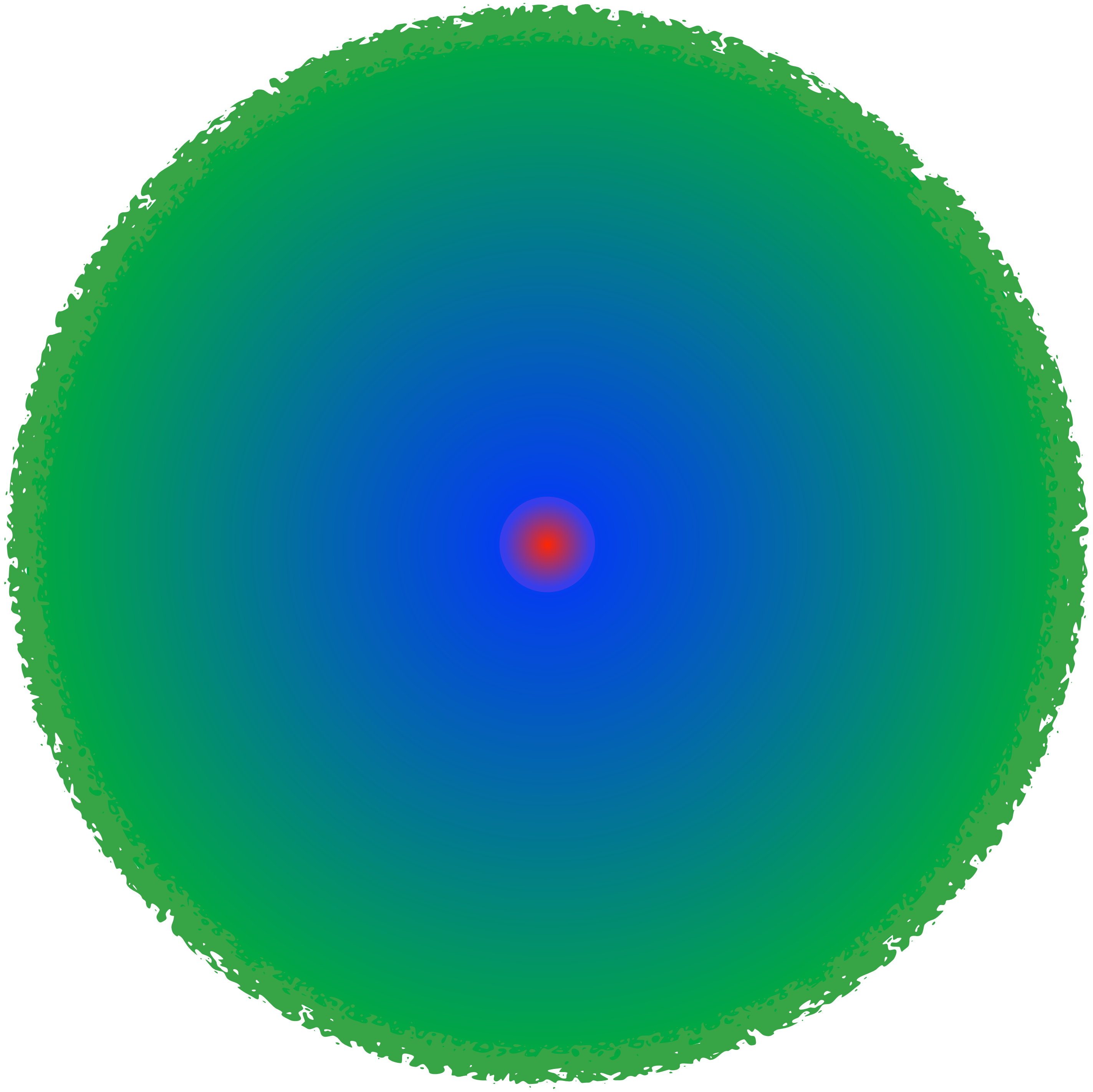
— Kotelnikov, Nyquist, Shannon, Whittaker

SDR as a Threat

DSP routines are SW. This can be shared, installed, and executed all around the world instantly with a very modest background.

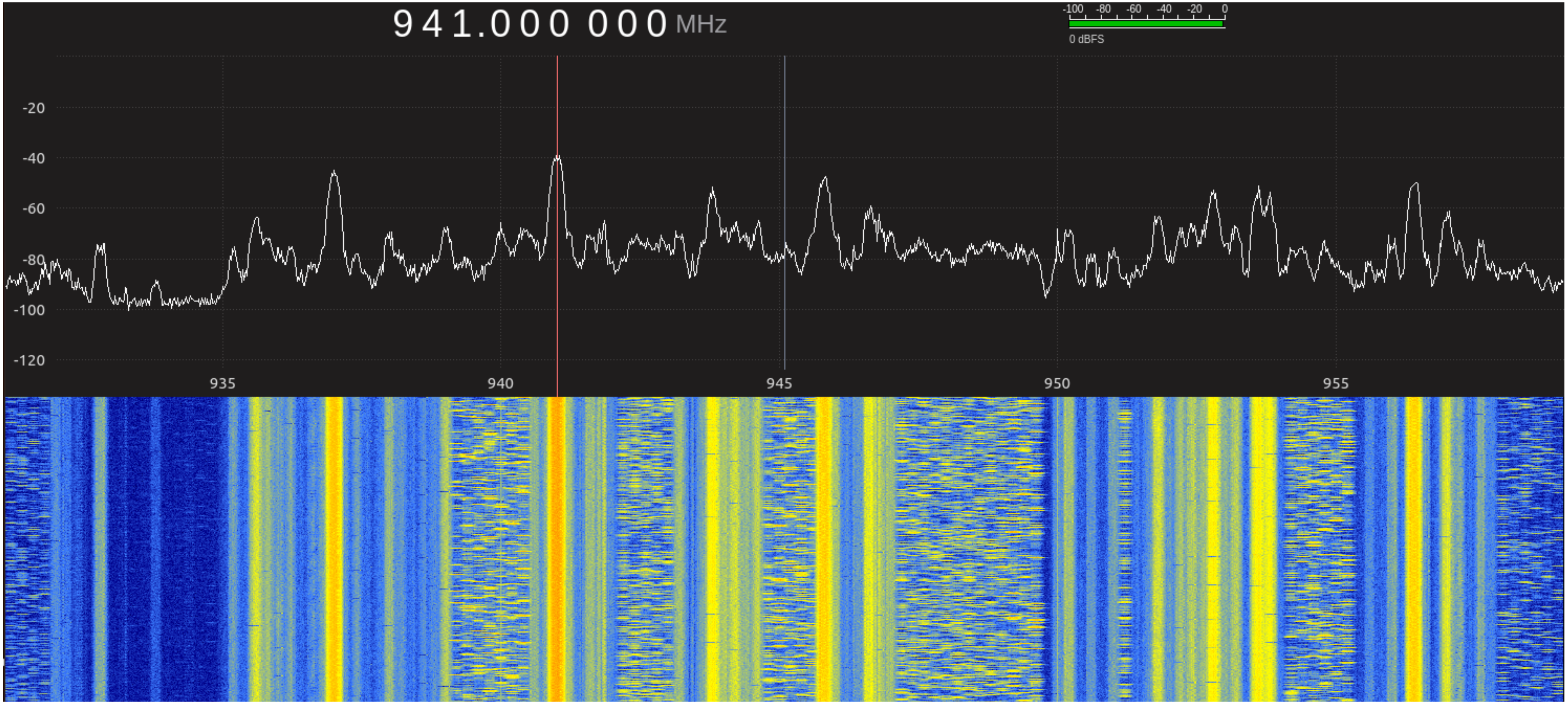
Just like any other exploit code.

EM Radiation Regions

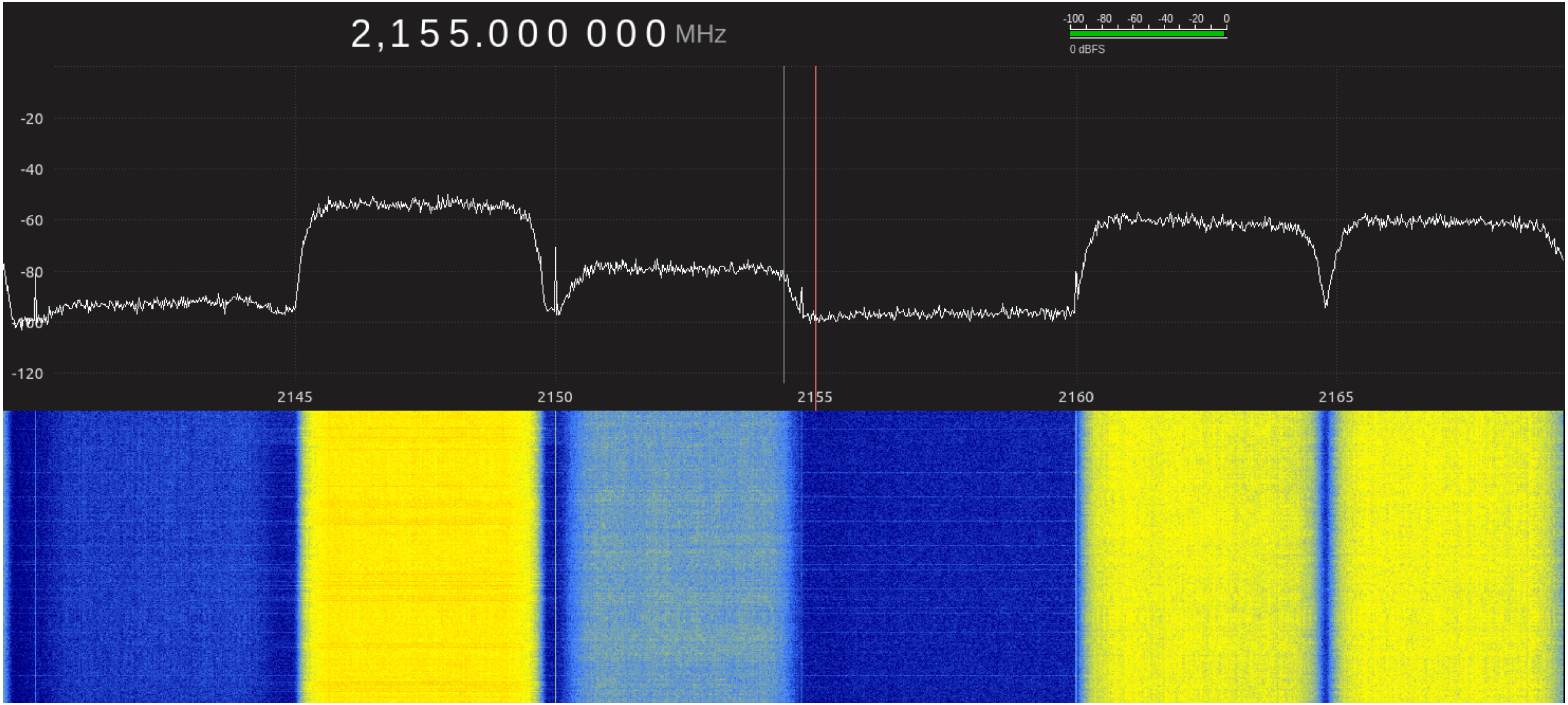


Mobile Networks

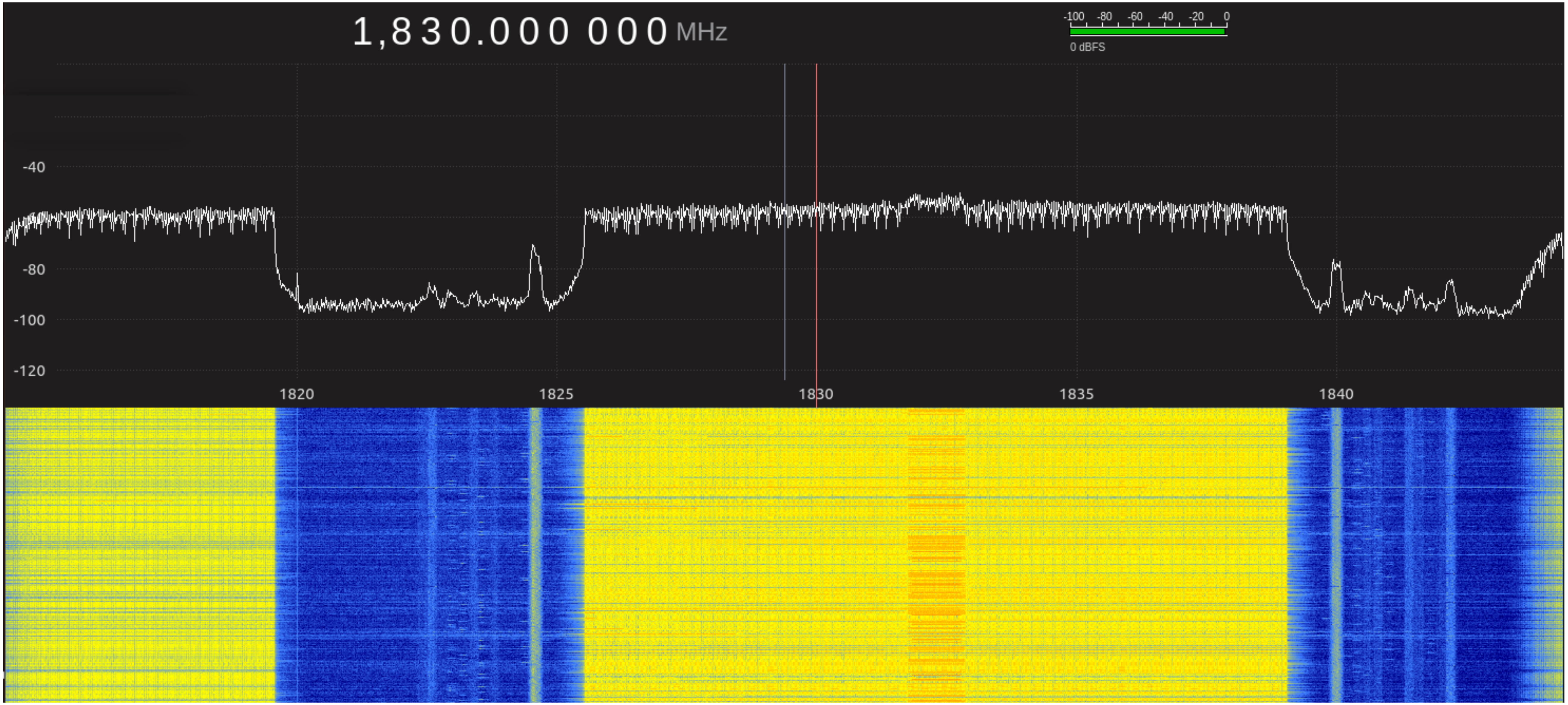
GSM / EDGE Radio Access Network (GERAN) Downlink Spectrogram



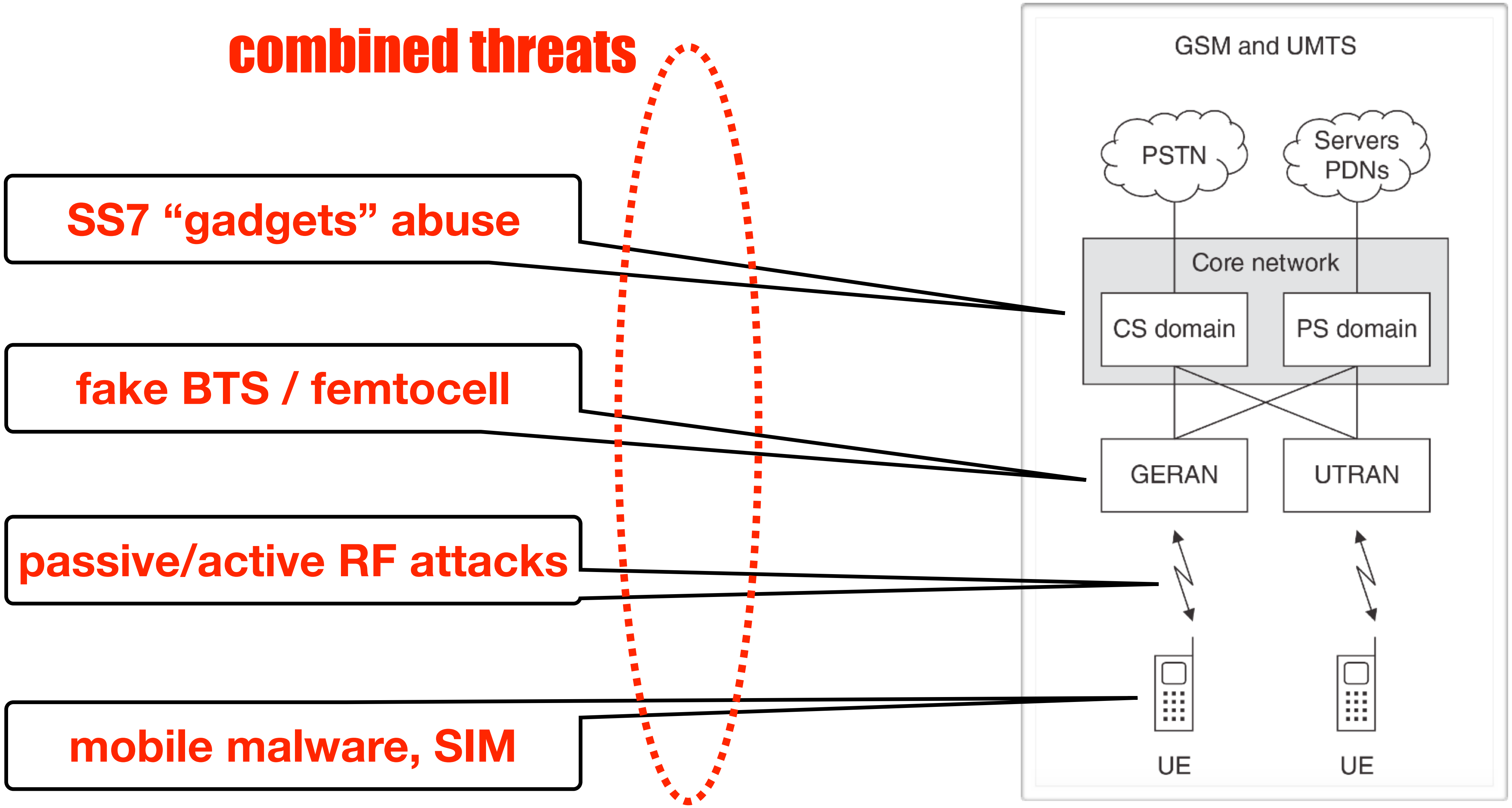
UMTS Terrestrial Radio Access Network (UTRAN) Downlink Spectrogram



Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) Downlink Spectrogram



Mobile Attacks Playground



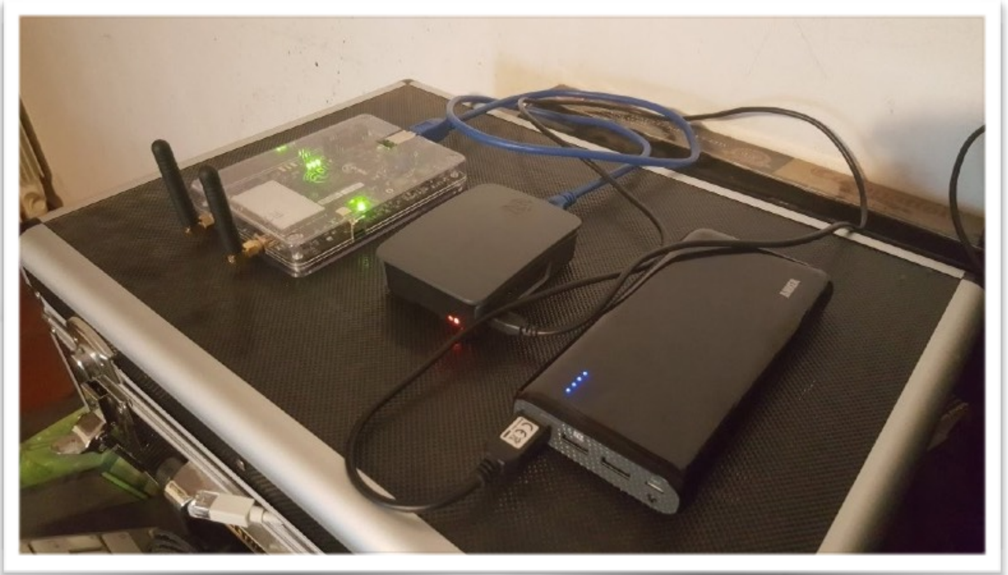
combined threats

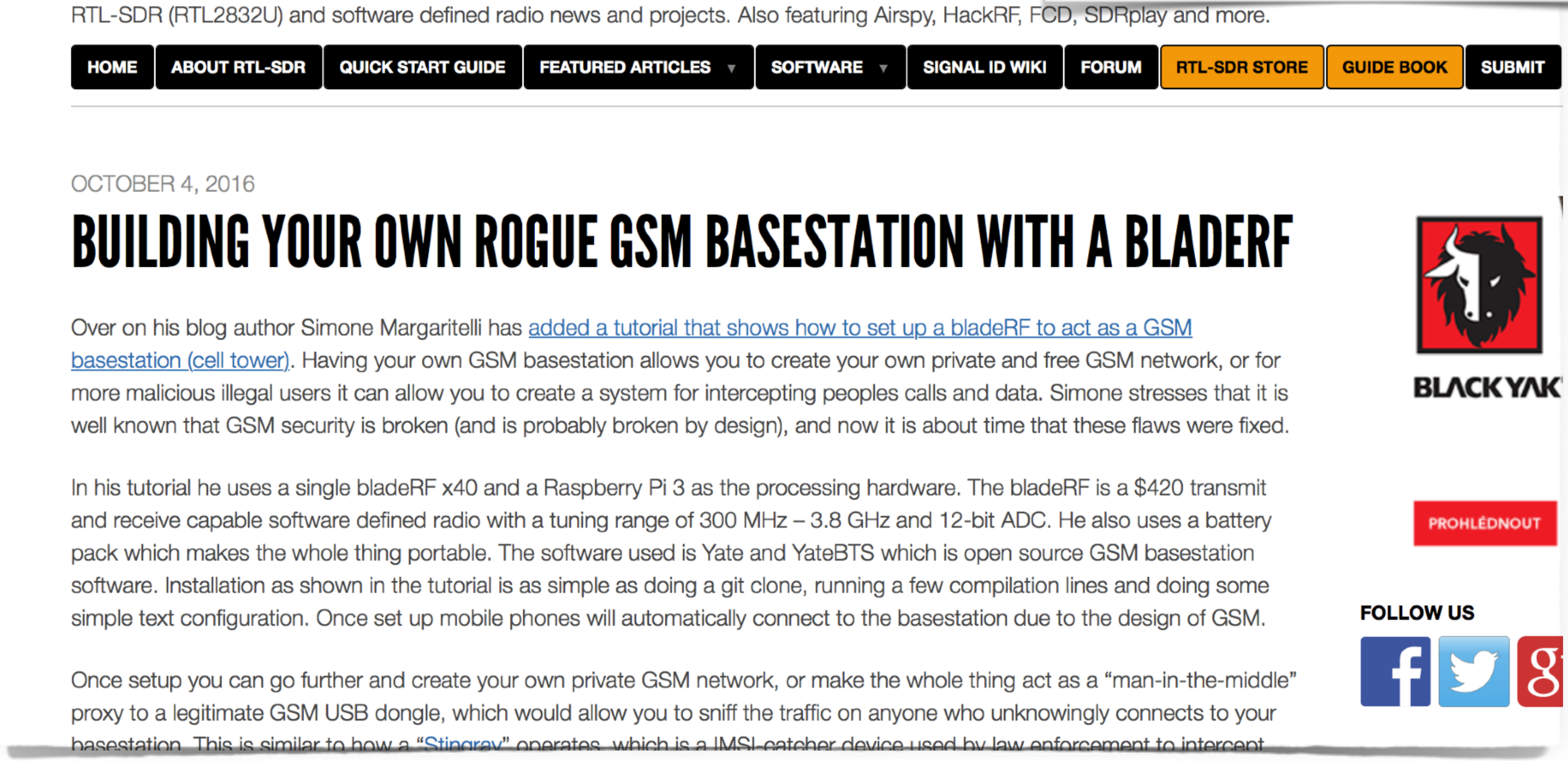
SS7 “gadgets” abuse

fake BTS / femtocell

passive/active RF attacks

mobile malware, SIM





RTL-SDR.COM

RTL-SDR (RTL2832U) and software defined radio news and projects. Also featuring Airspy, HackRF, FCD, SDRplay and more.

OCTOBER 4, 2016

BUILDING YOUR OWN ROGUE GSM BASESTATION WITH A BLADERF

Over on his blog author Simone Margaritelli has added a tutorial that shows how to set up a bladeRF to act as a GSM basestation (cell tower). Having your own GSM basestation allows you to create your own private and free GSM network, or for more malicious illegal users it can allow you to create a system for intercepting peoples calls and data. Simone stresses that it is well known that GSM security is broken (and is probably broken by design), and now it is about time that these flaws were fixed.

In his tutorial he uses a single bladeRF x40 and a Raspberry Pi 3 as the processing hardware. The bladeRF is a $420 transmit and receive capable software defined radio with a tuning range of 300 MHz – 3.8 GHz and 12-bit ADC. He also uses a battery pack which makes the whole thing portable. The software used is Yate and YateBTS which is open source GSM basestation software. Installation as shown in the tutorial is as simple as doing a git clone, running a few compilation lines and doing some simple text configuration. Once set up mobile phones will automatically connect to the basestation due to the design of GSM.

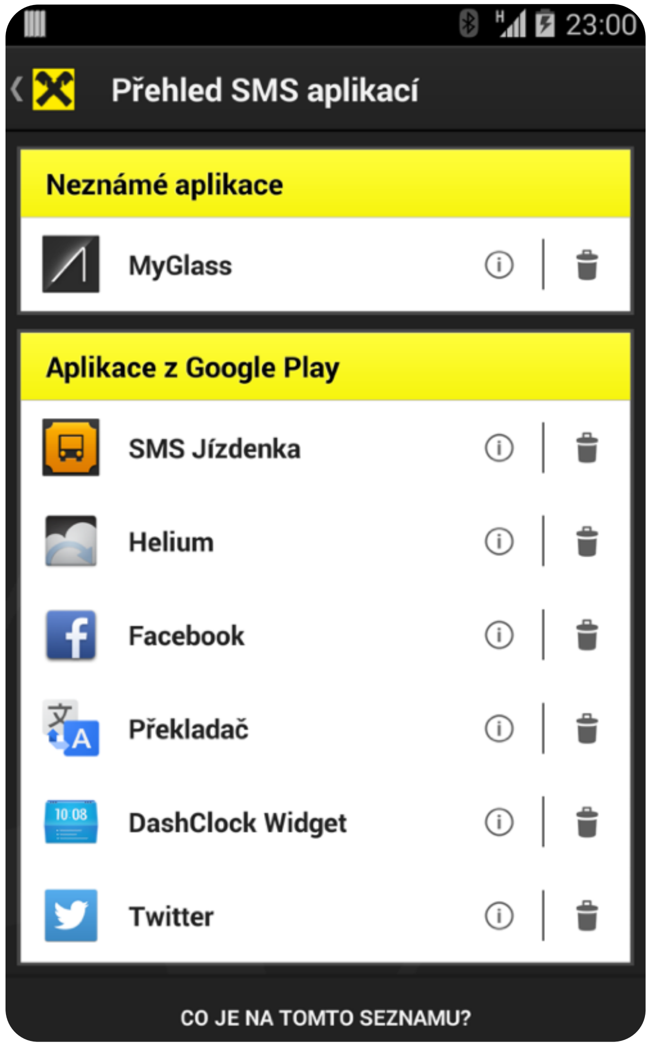
Once setup you can go further and create your own private GSM network, or make the whole thing act as a “man-in-the-middle” proxy to a legitimate GSM USB dongle, which would allow you to sniff the traffic on anyone who unknowingly connects to your basestation. This is similar to how a “Stingray” operates, which is a IMSI-catcher device used by law enforcement to intercept

Mobile-Terminated (MT) versus Mobile-Originated (MO)

- If any, we shall definitely **stay with Mobile Terminated services** (SMS reception, voice call answer) if we want to get at least “something”
- Mobile Originated based checks (SMS sender, voice call originator) are far easier to spoof
- Paris Hilton was already able to use a Caller ID spoofer in 2009

[Paris Hilton, 2012]

S.A.S. Sidekick of a Mobile Banking Application



23:00

Přehled SMS aplikací

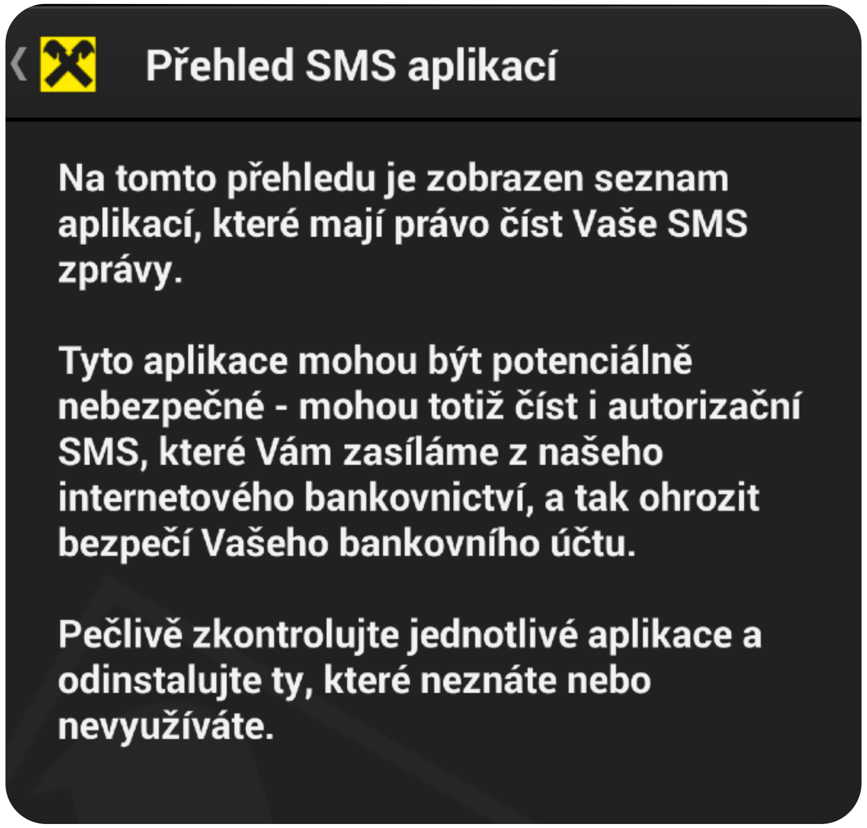
Neznámé aplikace

- MyGlass

Aplikace z Google Play

- SMS Jízdenka
- Helium
- Facebook
- Překladač
- DashClock Widget
- Twitter

CO JE NA TOMTO SEZNAMU?



Přehled SMS aplikací

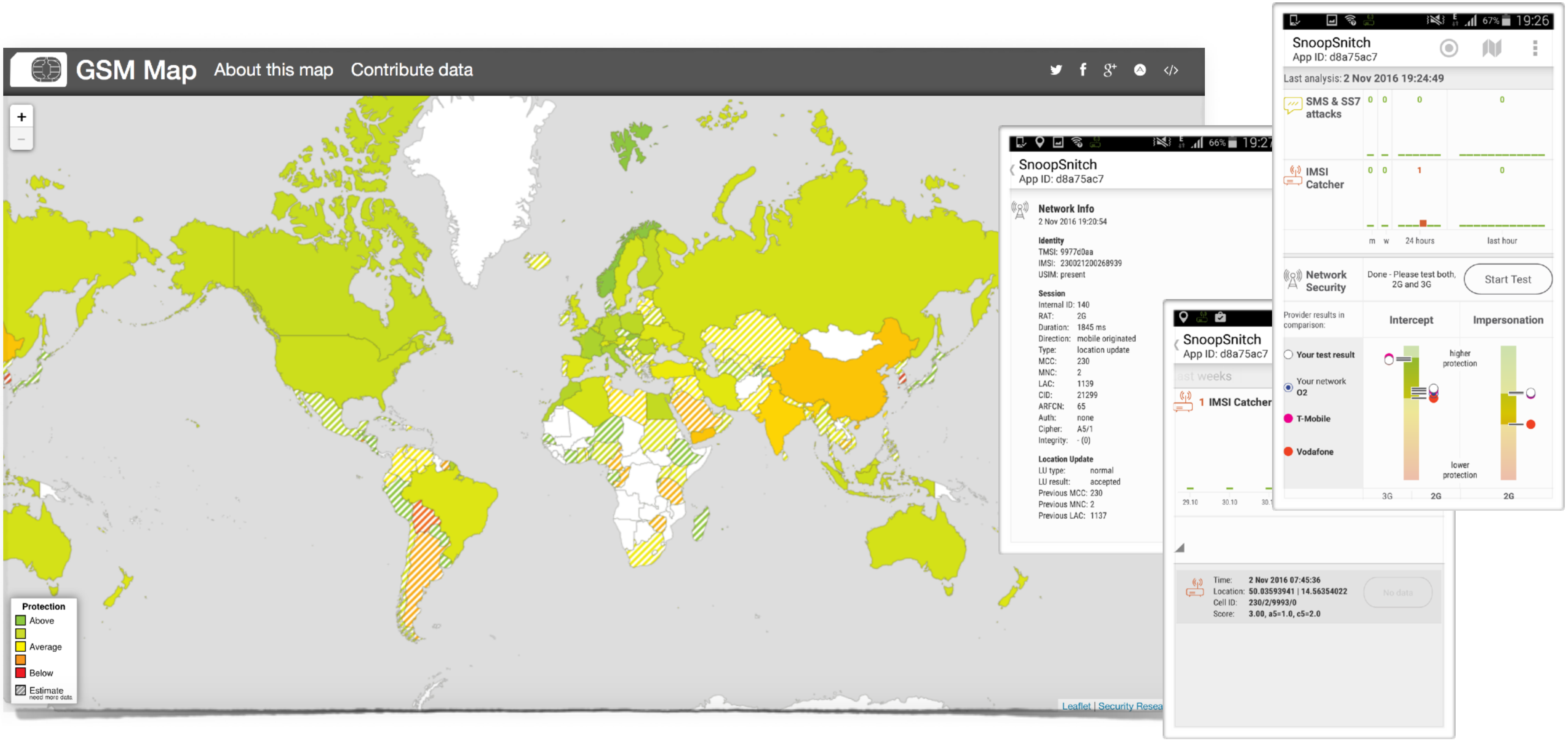
Na tomto přehledu je zobrazen seznam aplikací, které mají právo číst Vaše SMS zprávy.

Tyto aplikace mohou být potenciálně nebezpečné - mohou totiž číst i autorizační SMS, které Vám zasíláme z našeho internetového bankovnictví, a tak ohrozit bezpečí Vašeho bankovního účtu.

Pečlivě zkontrolujte jednotlivé aplikace a odinstalujte ty, které neznáte nebo nevyužíváte.

- Seek-And-Smash
- This honest mobile application searches for the specific type of *broadcast receiver* that is potentially capable of SMS interception
- When found, it issues a warning to the user suggesting the suspicious application removal

One weak operator to rule them all…



SnoopSnitch
App ID: d8a75ac7

Network Info
2 Nov 2016 19:20:54

Identity
TMSI: 9977d0aa
IMSI: 230021200268939
USIM: present

Session
```
Internal ID: 140
RAT:         2G
Duration:    1845 ms
Direction:   mobile originated
Type:        location update
MCC:         230
MNC:         2
LAC:         1139
CID:         21299
ARFCN:       65
Auth:        none
Cipher:      A5/1
Integrity:   - (0)
```

Location Update
```
LU type:       normal
LU result:     accepted
Previous MCC:  230
Previous MNC:  2
Previous LAC:  1137
```

SnoopSnitch
App ID: d8a75ac7

ast weeks

1 IMSI Catcher

```
Time:      2 Nov 2016 07:45:36
Location:  50.03593941 | 14.56354022
Cell ID:   230/2/9993/0
Score:     3.00, a5=1.0, c5=2.0
```

SnoopSnitch
App ID: d8a75ac7

Last analysis: 2 Nov 2016 19:24:49

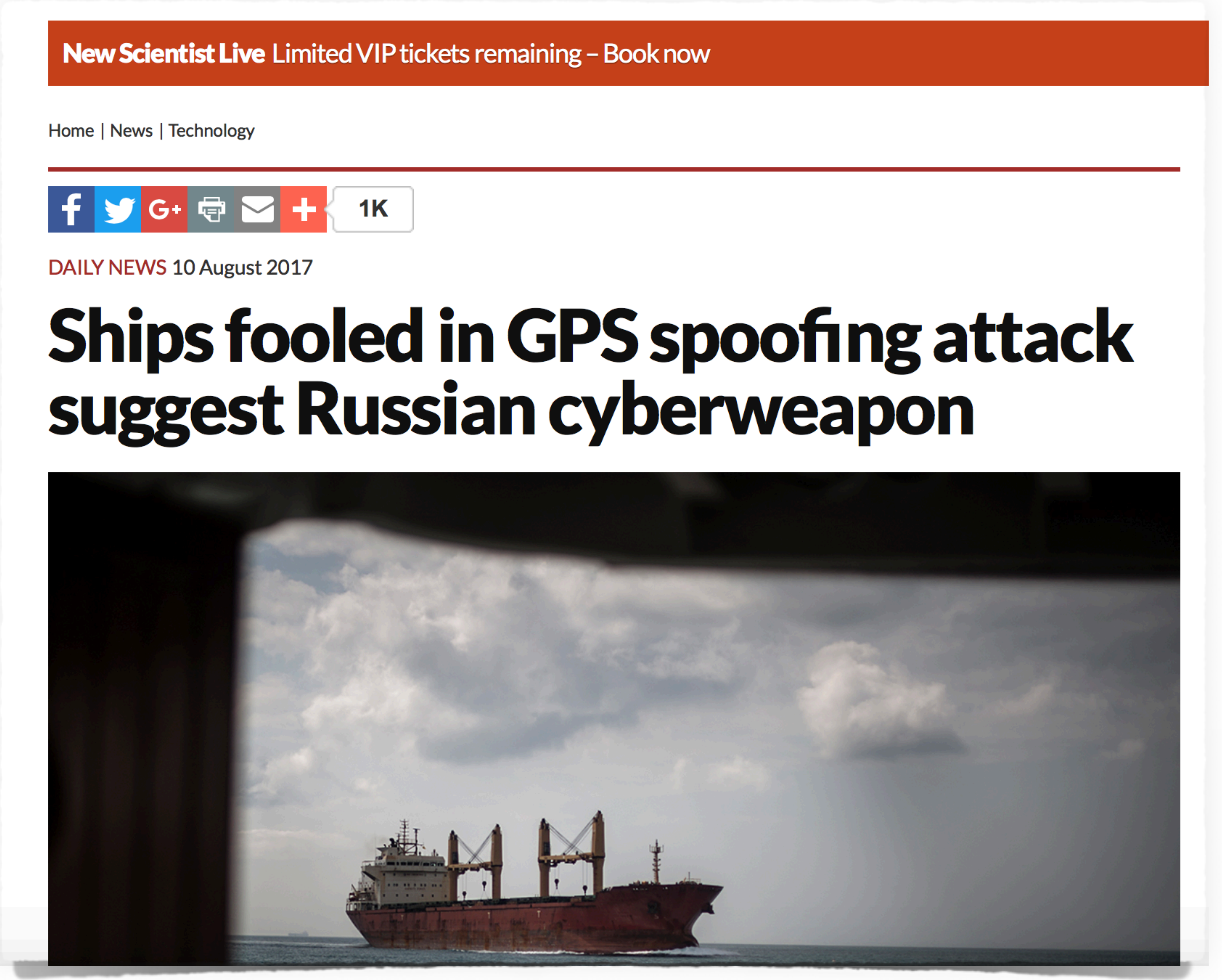
	m	w	24 hours	last hour
SMS & SS7 attacks	0	0	0	0
IMSI Catcher	0	0	1	0

Network Security — Done - Please test both, 2G and 3G

Provider results in comparison:

○ Your test result
● Your network O2
● T-Mobile
● Vodafone

GNSS - Global Navigation Satellite Systems

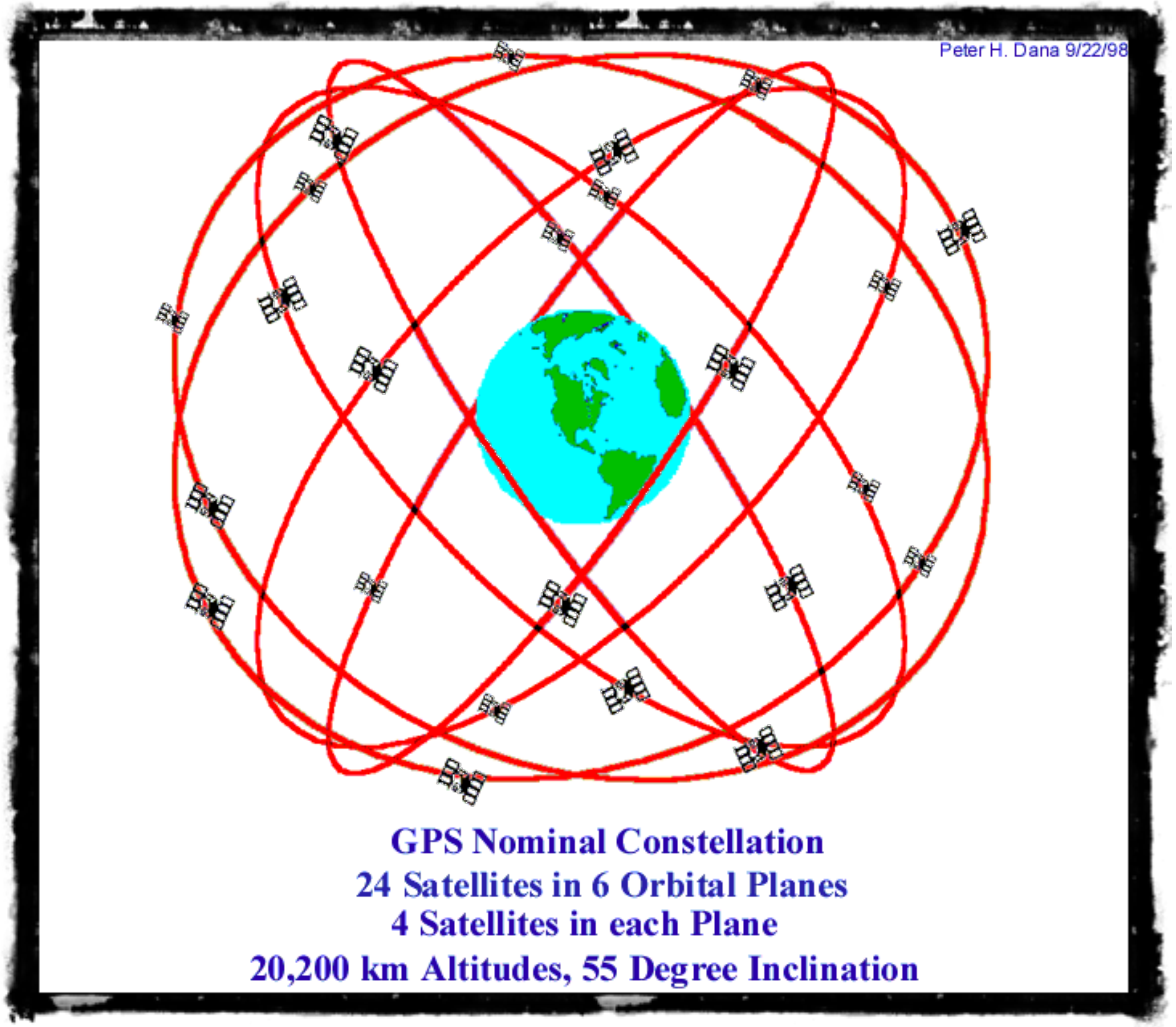


Home | News | Technology

DAILY NEWS 10 August 2017

Ships fooled in GPS spoofing attack suggest Russian cyberweapon

GPS Space Segment Constellation



Peter H. Dana 9/22/98

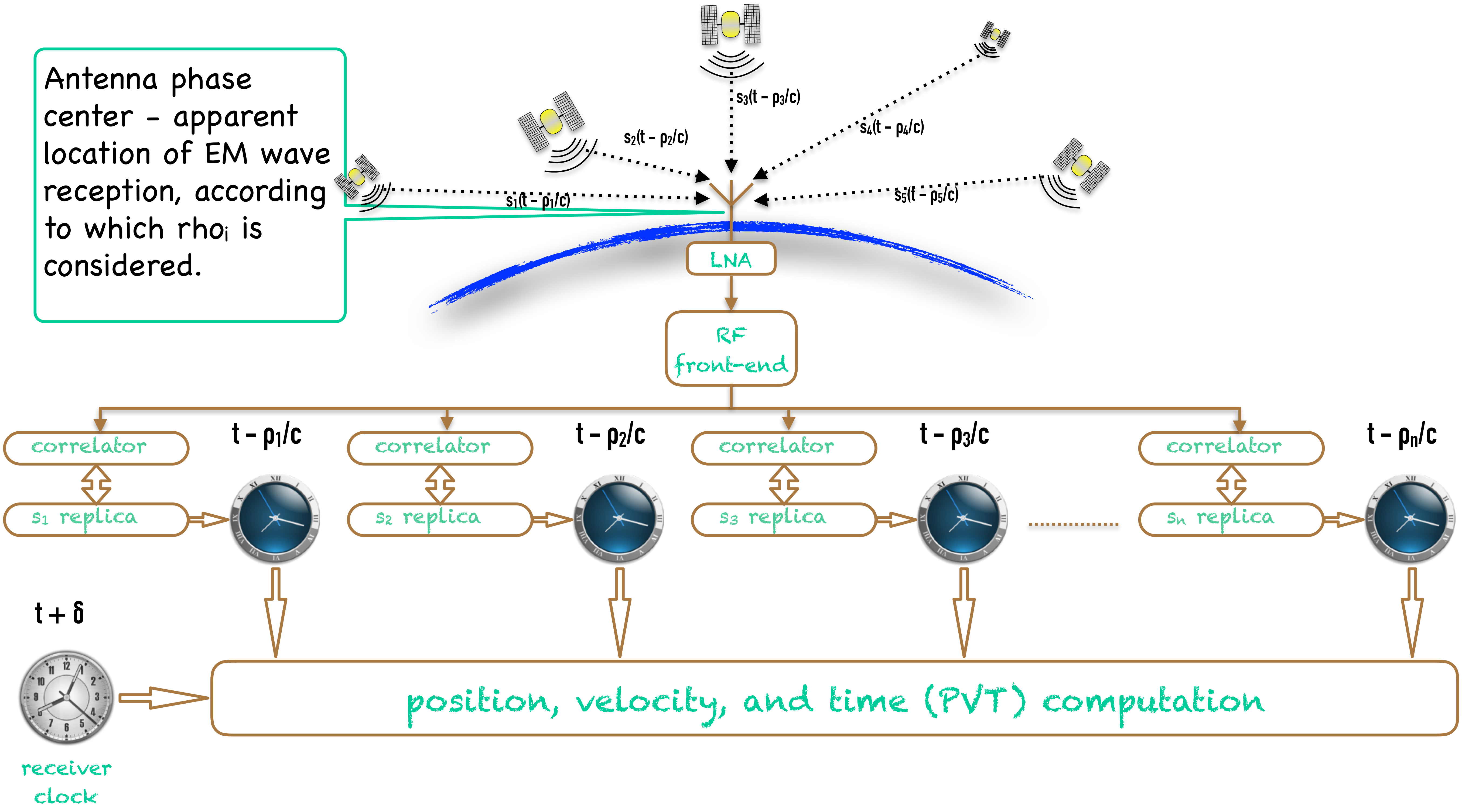
GPS Nominal Constellation
24 Satellites in 6 Orbital Planes
4 Satellites in each Plane
20,200 km Altitudes, 55 Degree Inclination

Satellite clock observation expose time delay that in turn reveals the satellite distance

t_{sent_sv1}
t_{sent_sv2}
t_{sent_sv3}
t_{sent_sv4}
$t_{rec}+t_{bias}$

four satellites to get X, Y, Z, and t_bias

GNSS Tracking Illustration



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

$s_1(t - \rho_1/c)$

$s_2(t - \rho_2/c)$

$s_3(t - \rho_3/c)$

$s_4(t - \rho_4/c)$

$s_5(t - \rho_5/c)$

LNA

RF front-end

correlator

s_1 replica

$t - \rho_1/c$

correlator

s_2 replica

$t - \rho_2/c$

correlator

s_3 replica

$t - \rho_3/c$

correlator

s_n replica

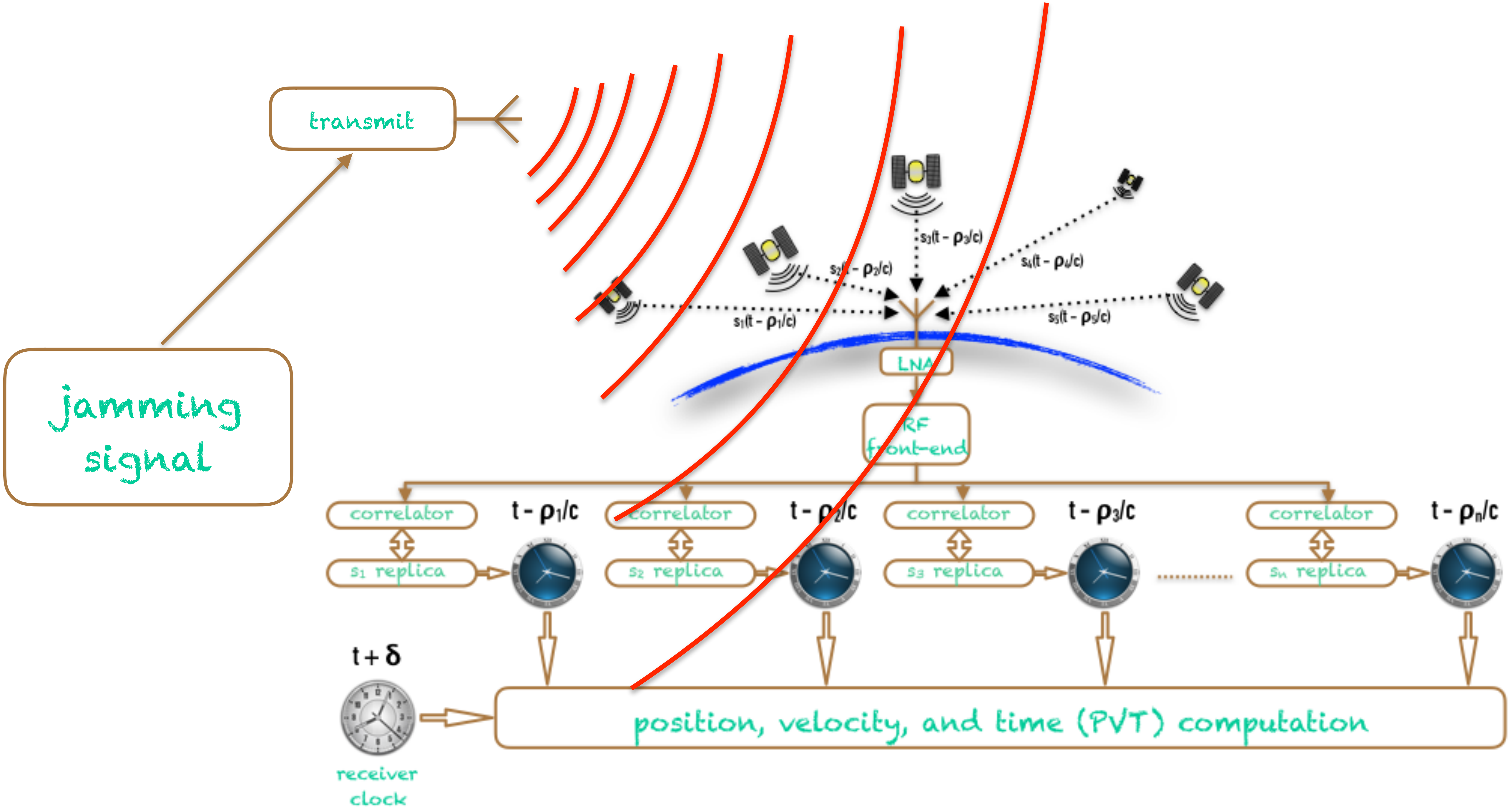
$t - \rho_n/c$

$t + \delta$

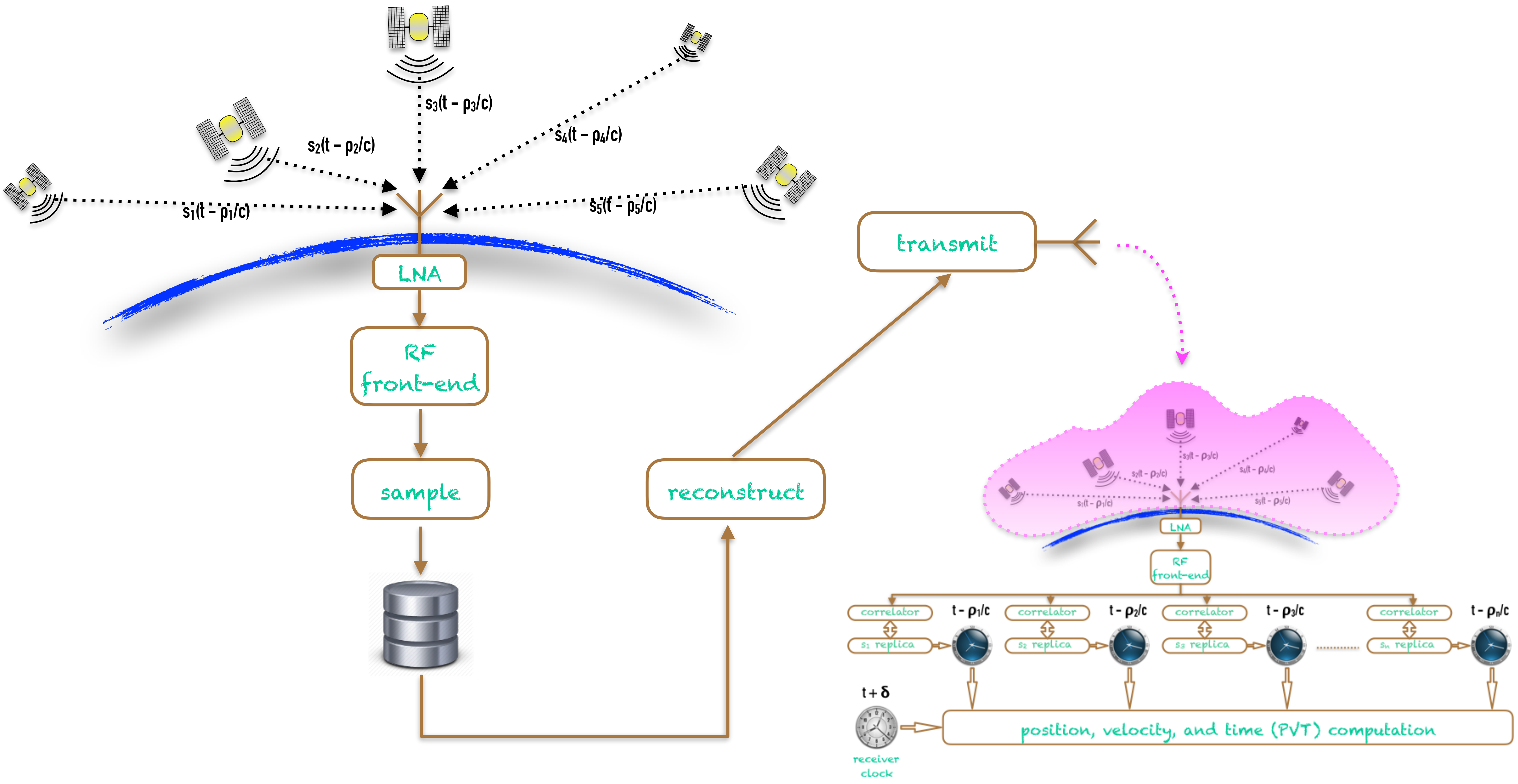
receiver clock

position, velocity, and time (PVT) computation

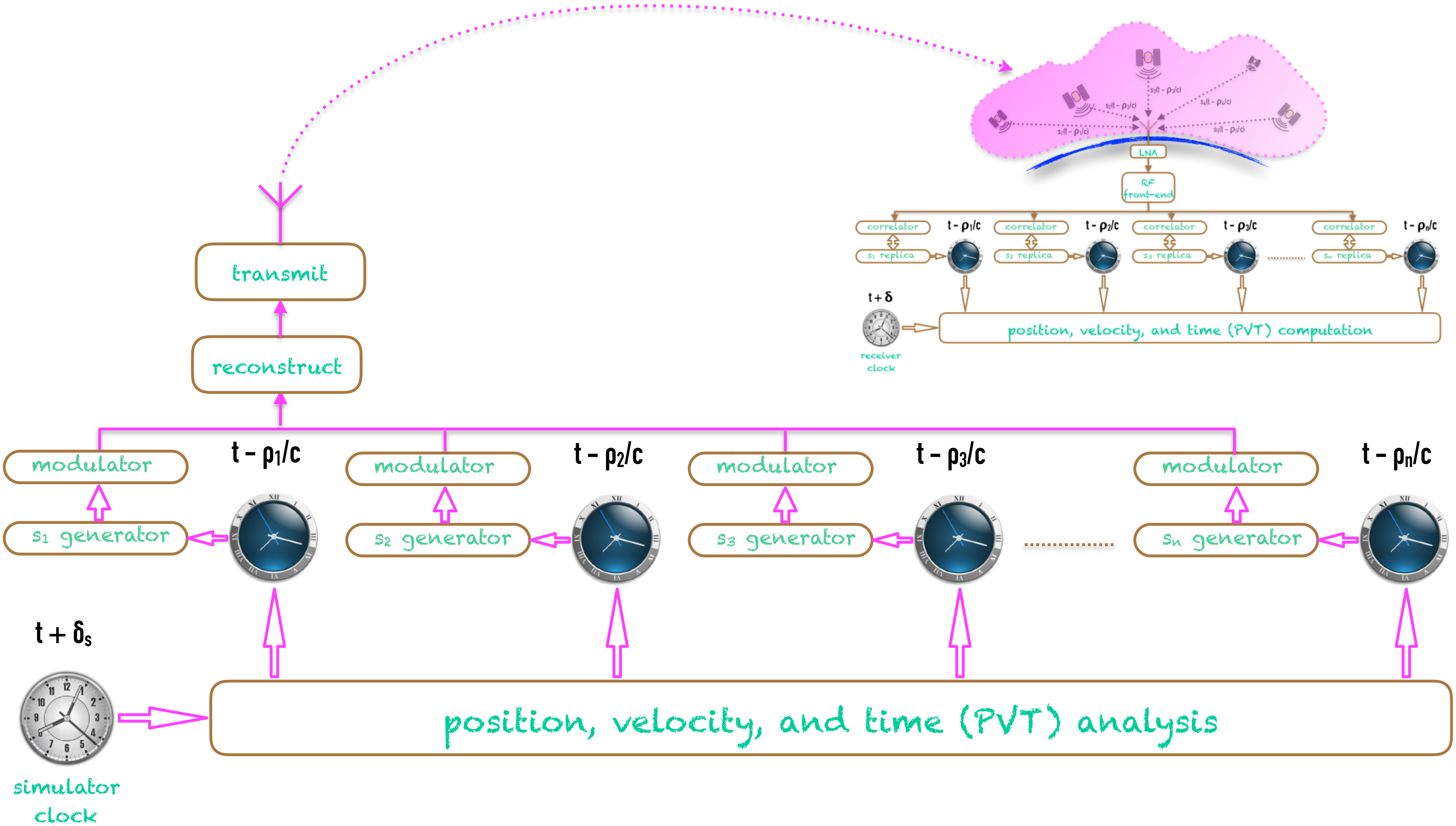
GNSS Jamming Attack



GNSS Replay Attack (Meaconing)



GNSS Spoofing Attack by Tracking Reversal



$s_1(t - \rho_1/c)$

$s_2(t - \rho_2/c)$

$s_3(t - \rho_3/c)$

$s_4(t - \rho_4/c)$

$s_5(t - \rho_5/c)$

LNA

RF front-end

correlator

s_1 replica

$t - \rho_1/c$

correlator

s_2 replica

$t - \rho_2/c$

correlator

s_3 replica

$t - \rho_3/c$

correlator

s_n replica

$t - \rho_n/c$

$t + \delta$

receiver clock

position, velocity, and time (PVT) computation

transmit

reconstruct

modulator

s_1 generator

$t - \rho_1/c$

modulator

s_2 generator

$t - \rho_2/c$

modulator

s_3 generator

$t - \rho_3/c$

modulator

s_n generator

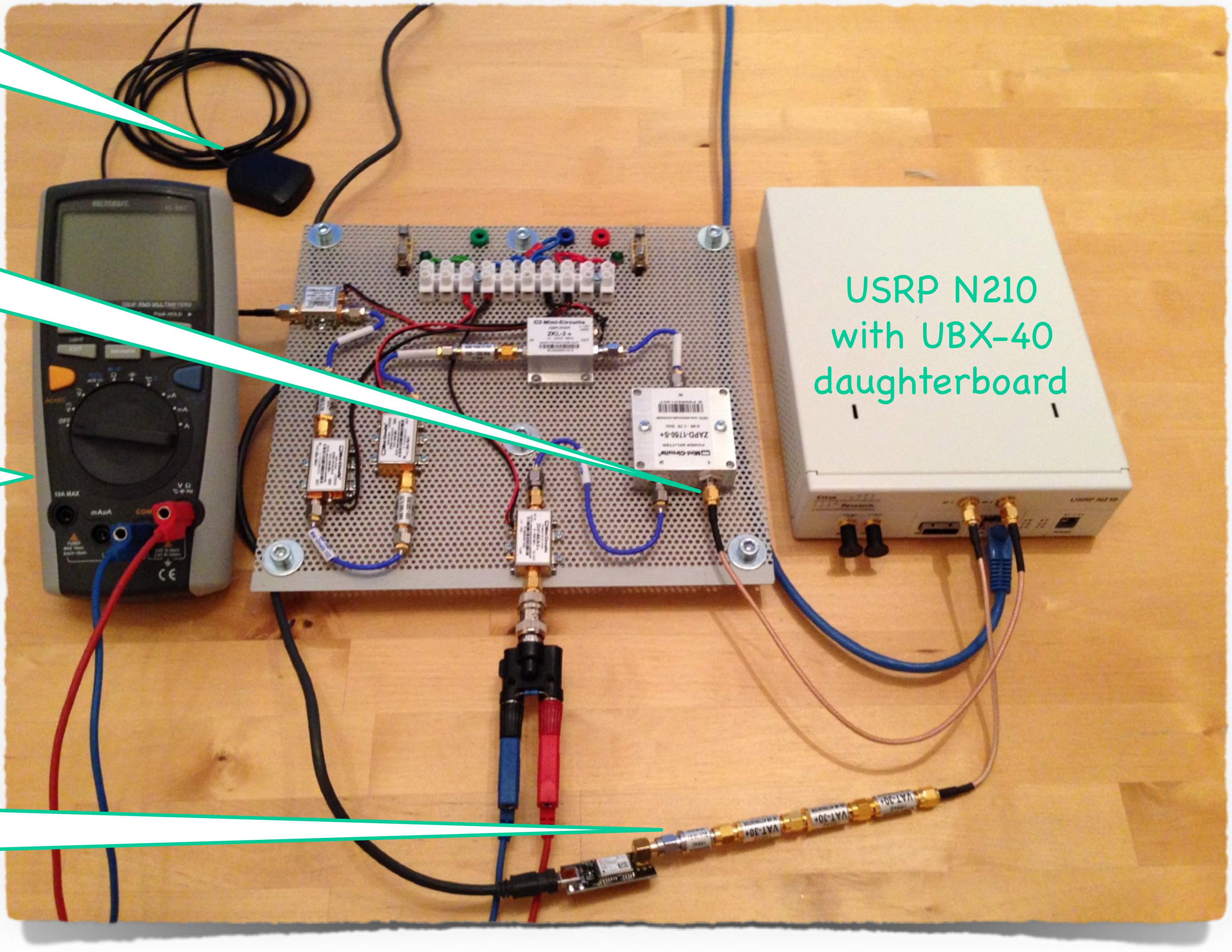
$t - \rho_n/c$

$t + \delta_s$

simulator clock

position, velocity, and time (PVT) analysis

Record & Replay (Meaconing) Setup



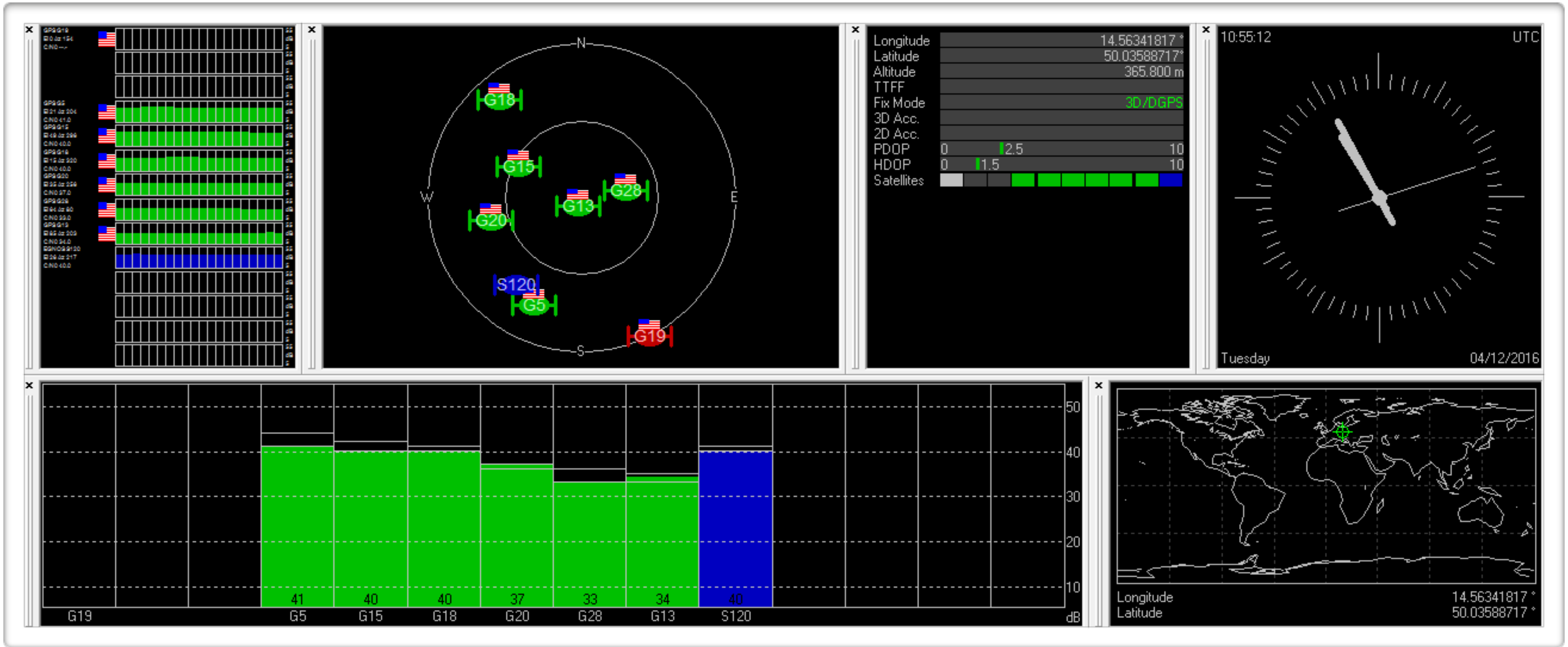
Active antenna

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 receiver. Don't forget the DC block and attenuators (3x30 dB in this case)!

GPS L1 C/A Meaconing Verification



Longitude 14.56341817 °
Latitude 50.03588717°
Altitude 365.800 m
TTFF
Fix Mode 3D/DGPS
3D Acc.
2D Acc.
PDOP 0 2.5 10
HDOP 0 1.5 10
Satellites

10:55:12 UTC
Tuesday 04/12/2016

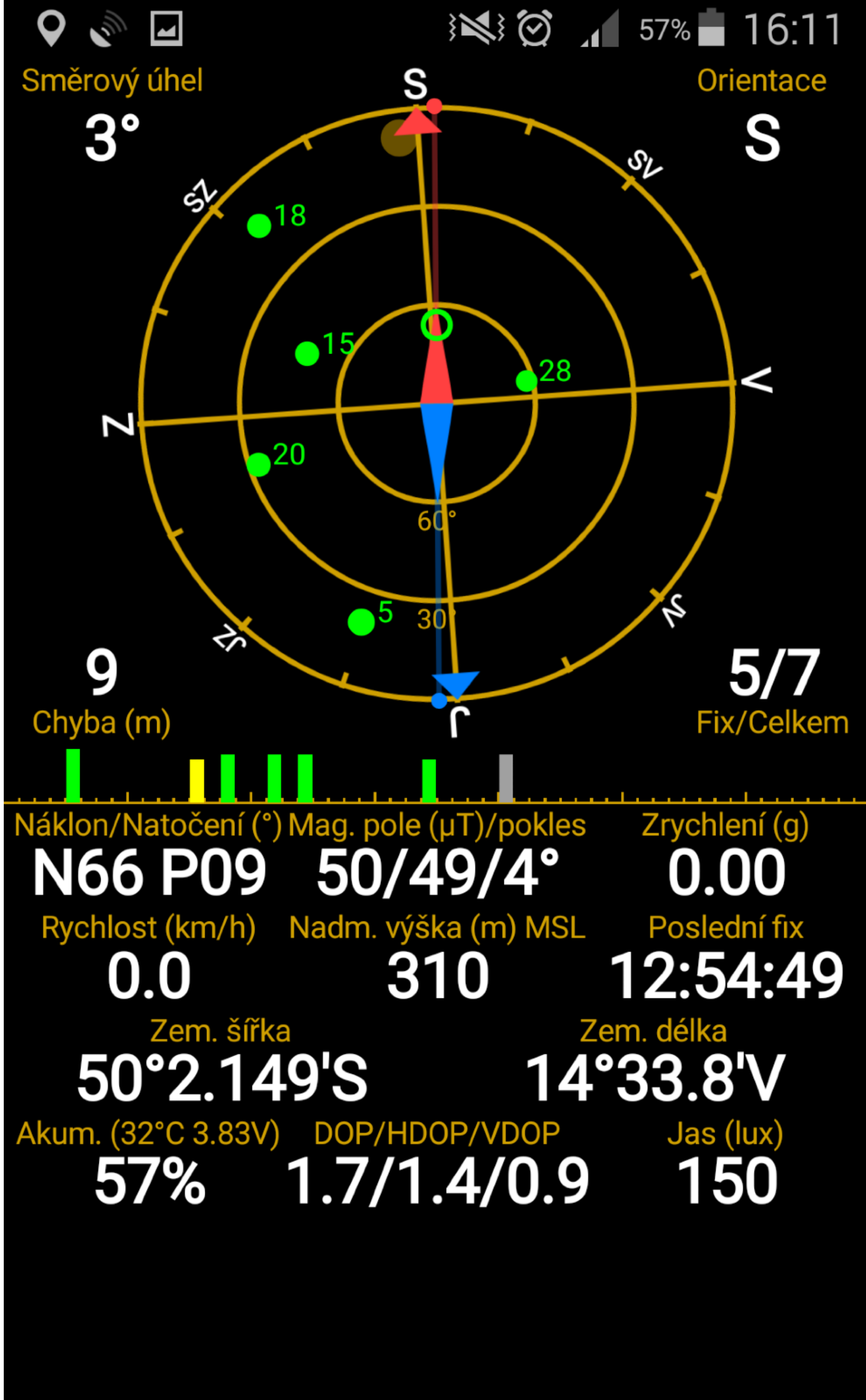
Longitude 14.56341817 °
Latitude 50.03588717 °

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

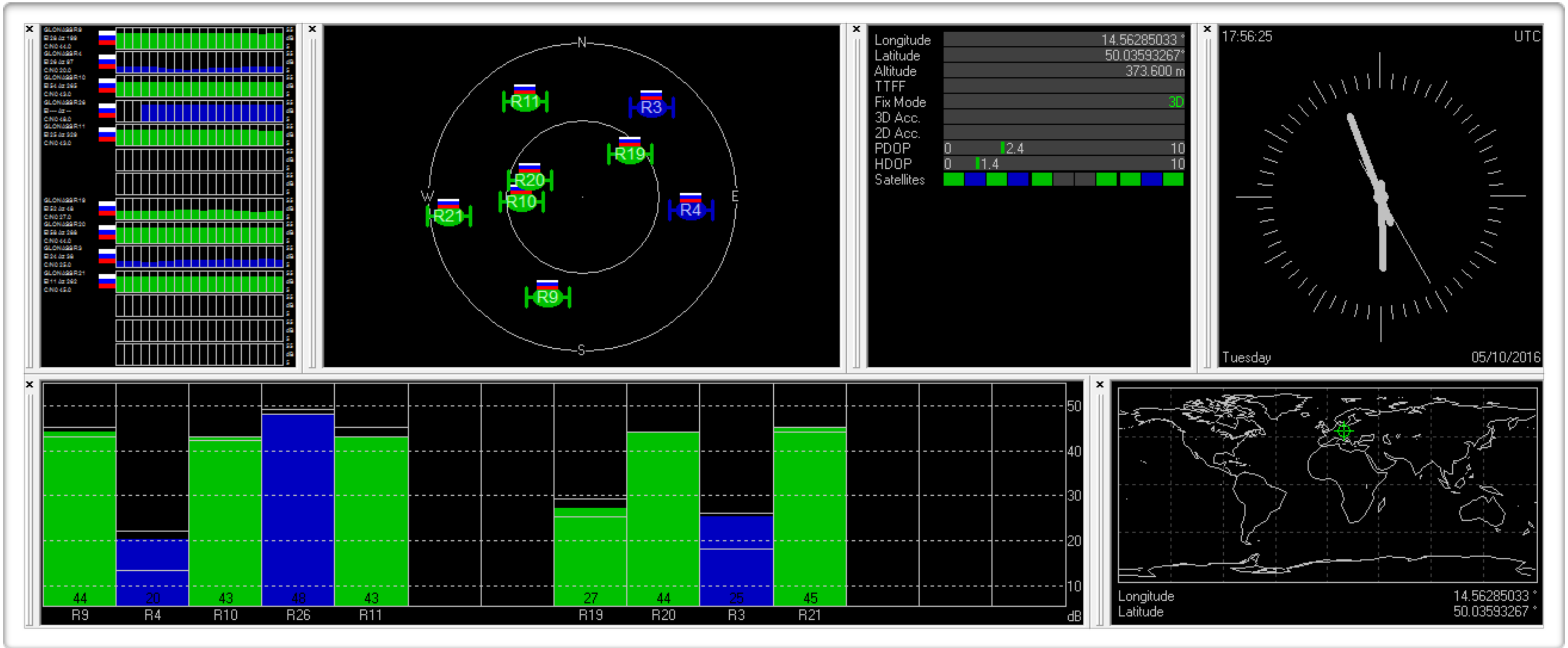
- Despite the direct shielded connection in between the SDR and demo GNSS receiver, there was an incidental radiation strong enough, so a smartphone nearby was able to get a fix to the fake signal.
- The distance to the smartphone was several meters from the table where SDR was running.
- We can imagine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

[screenshot & idea courtesy by Jiří Buček]



Směrový úhel		Orientace
3°		S
9		5/7
Chyba (m)		Fix/Celkem
Náklon/Natočení (°)	Mag. pole (µT)/pokles	Zrychlení (g)
N66 P09	50/49/4°	0.00
Rychlost (km/h)	Nadm. výška (m) MSL	Poslední fix
0.0	310	12:54:49
Zem. šířka		Zem. délka
50°2.149'S		14°33.8'V
Akum. (32°C 3.83V)	DOP/HDOP/VDOP	Jas (lux)
57%	1.7/1.4/0.9	150

GLONASS L1OF Meaconing Result



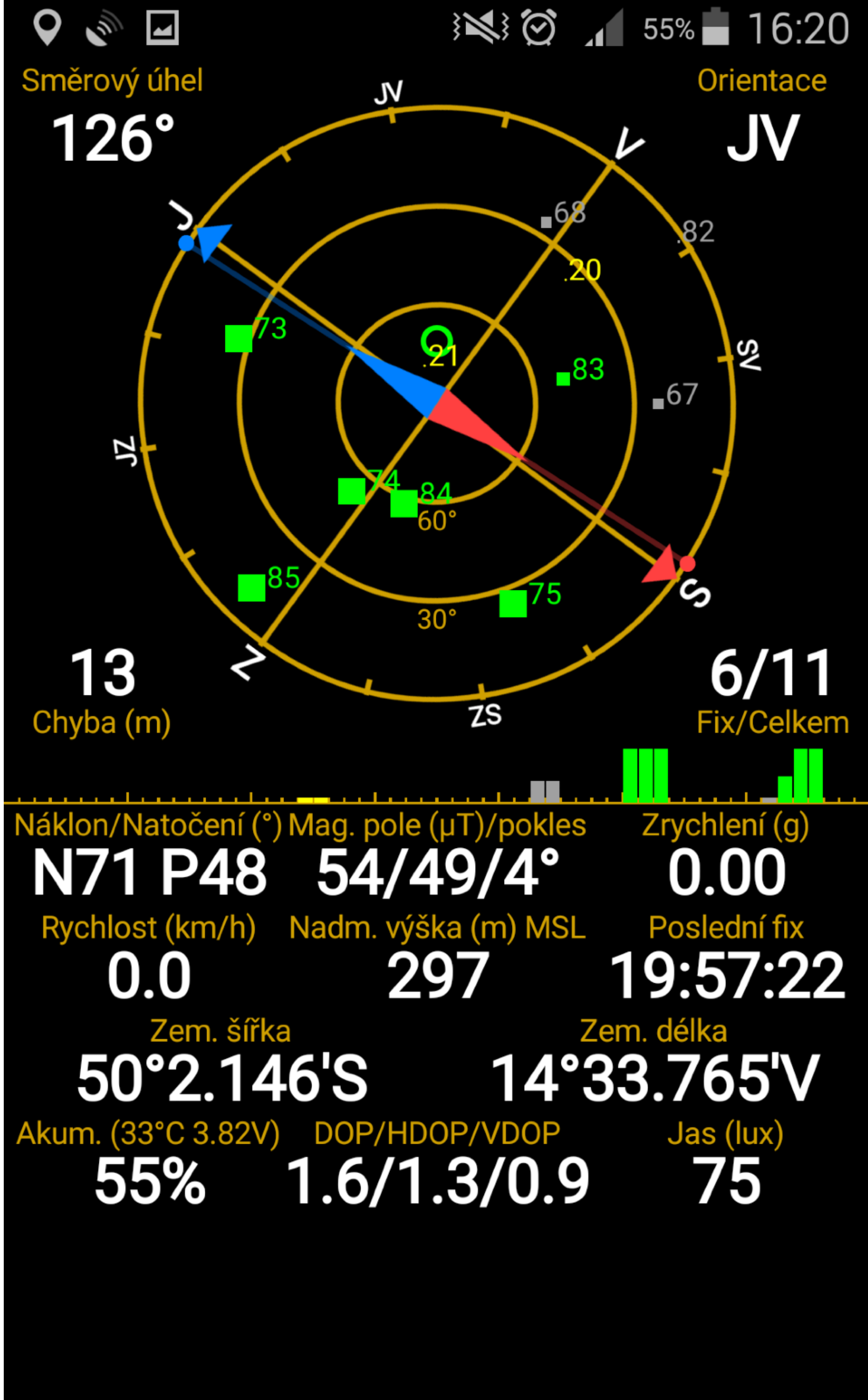
Longitude 14.56285033 °
Latitude 50.03593267°
Altitude 373.600 m
TTFF
Fix Mode 3D
3D Acc.
2D Acc.
PDOP 0 2.4 10
HDOP 0 1.4 10
Satellites

17:56:25 UTC
Tuesday 05/10/2016

Longitude 14.56285033 °
Latitude 50.03593267 °

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…



Směrový úhel
126°

Orientace
JV

13
Chyba (m)

6/11
Fix/Celkem

Náklon/Natočení (°)
N71 P48

Mag. pole (µT)/pokles
54/49/4°

Zrychlení (g)
0.00

Rychlost (km/h)
0.0

Nadm. výška (m) MSL
297

Poslední fix
19:57:22

Zem. šířka
50°2.146'S

Zem. délka
14°33.765'V

Akum. (33°C 3.82V)
55%

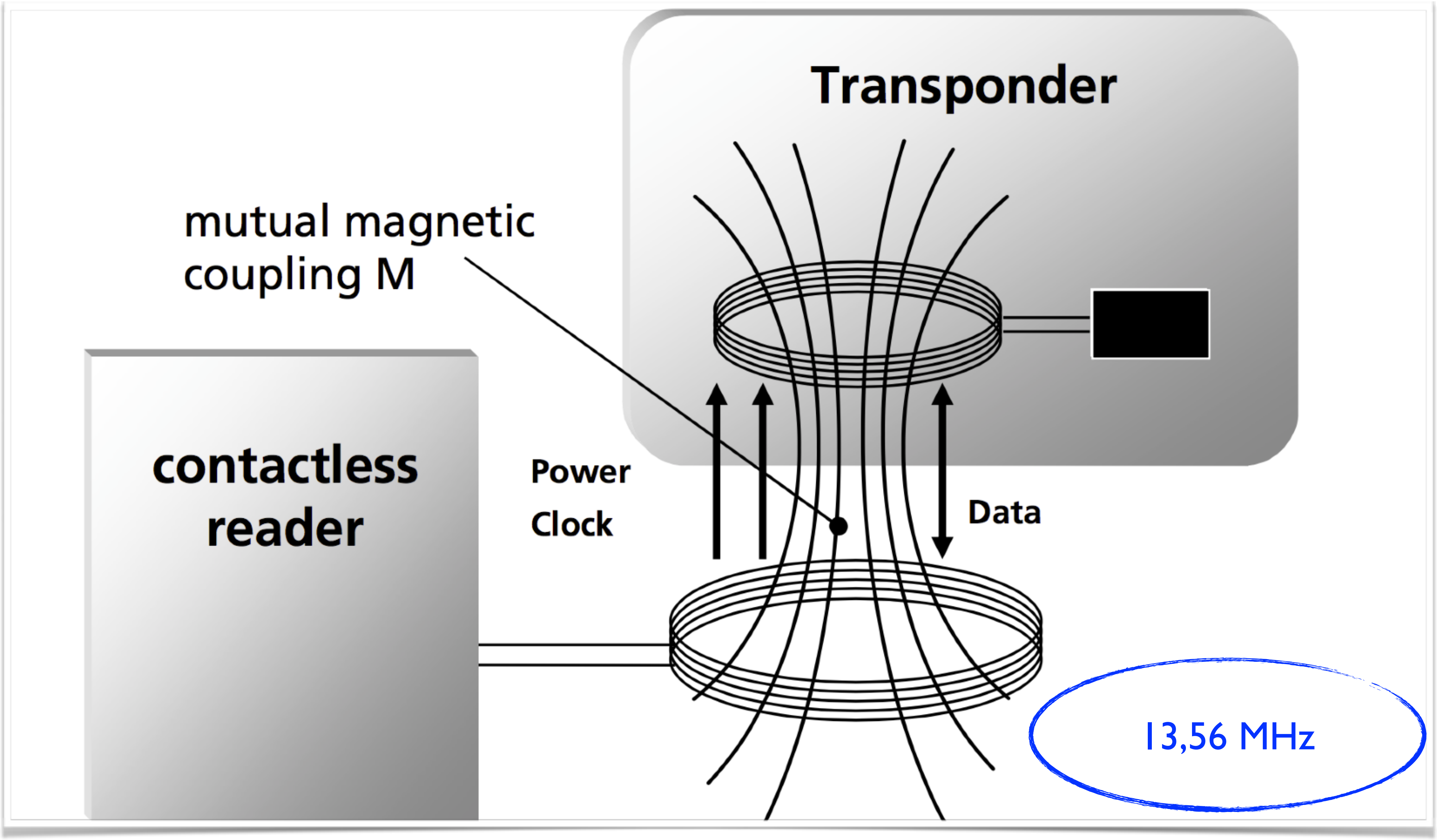
DOP/HDOP/VDOP
1.6/1.3/0.9

Jas (lux)
75

[screenshot & idea courtesy by Jiří Buček]

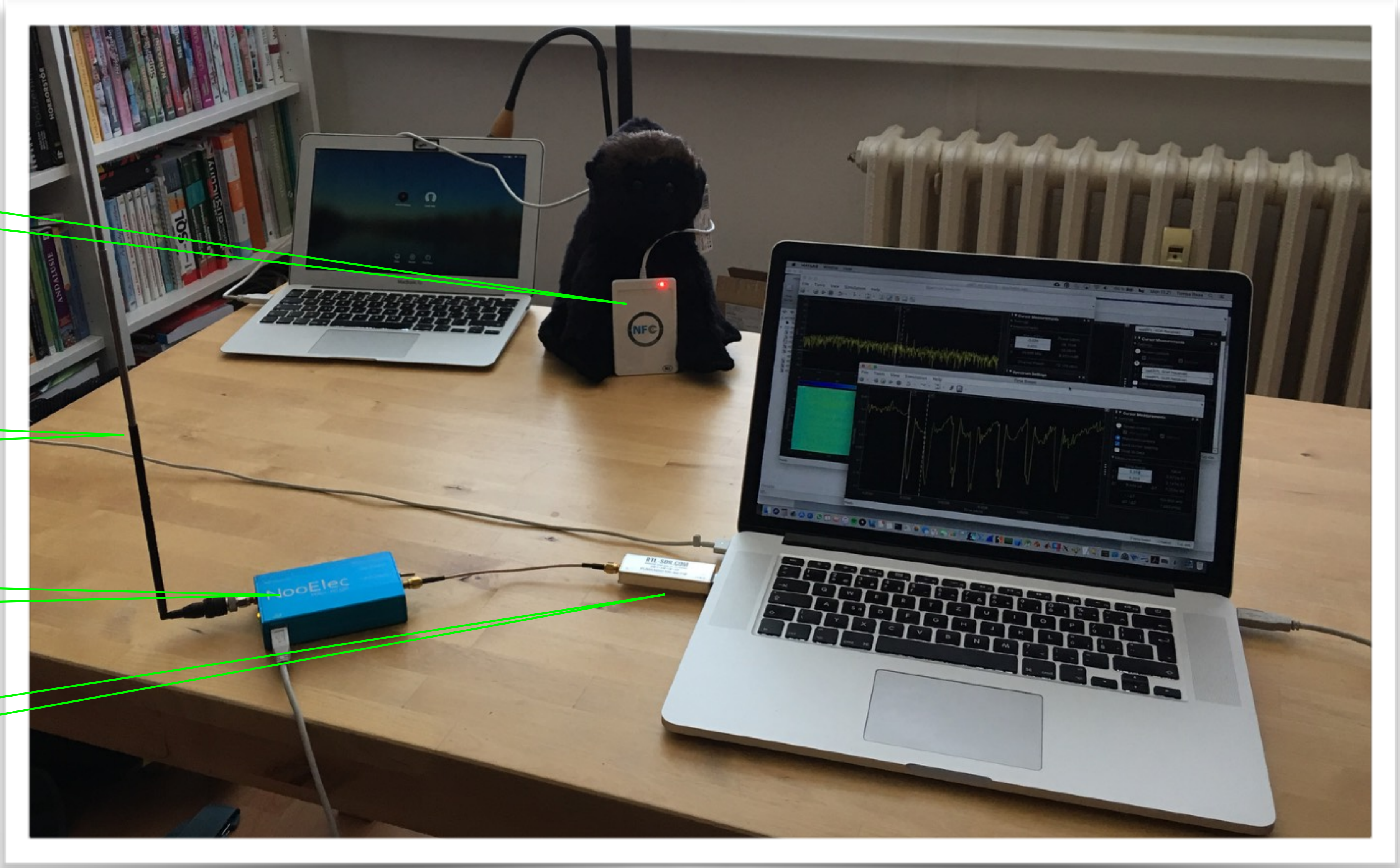
NFC - Near Field Communication

NFC General Operation Mode



13,56 MHz

Hardware Setup



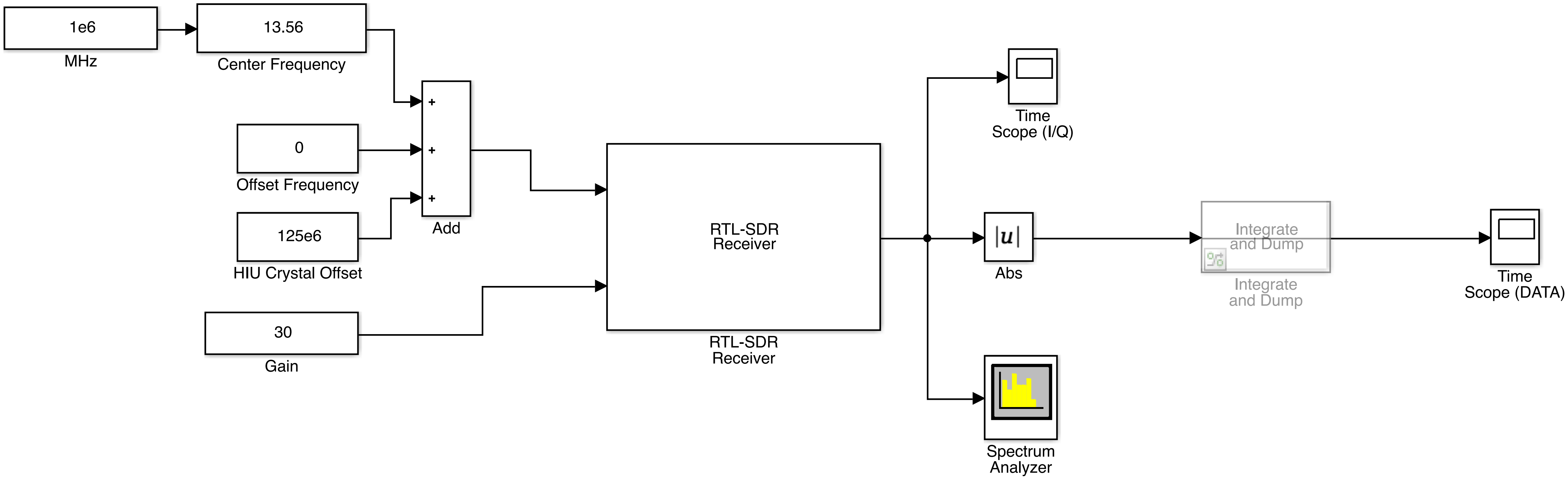
ACR122 NFC reader

Simple telescopic antenna (untuned - a place for

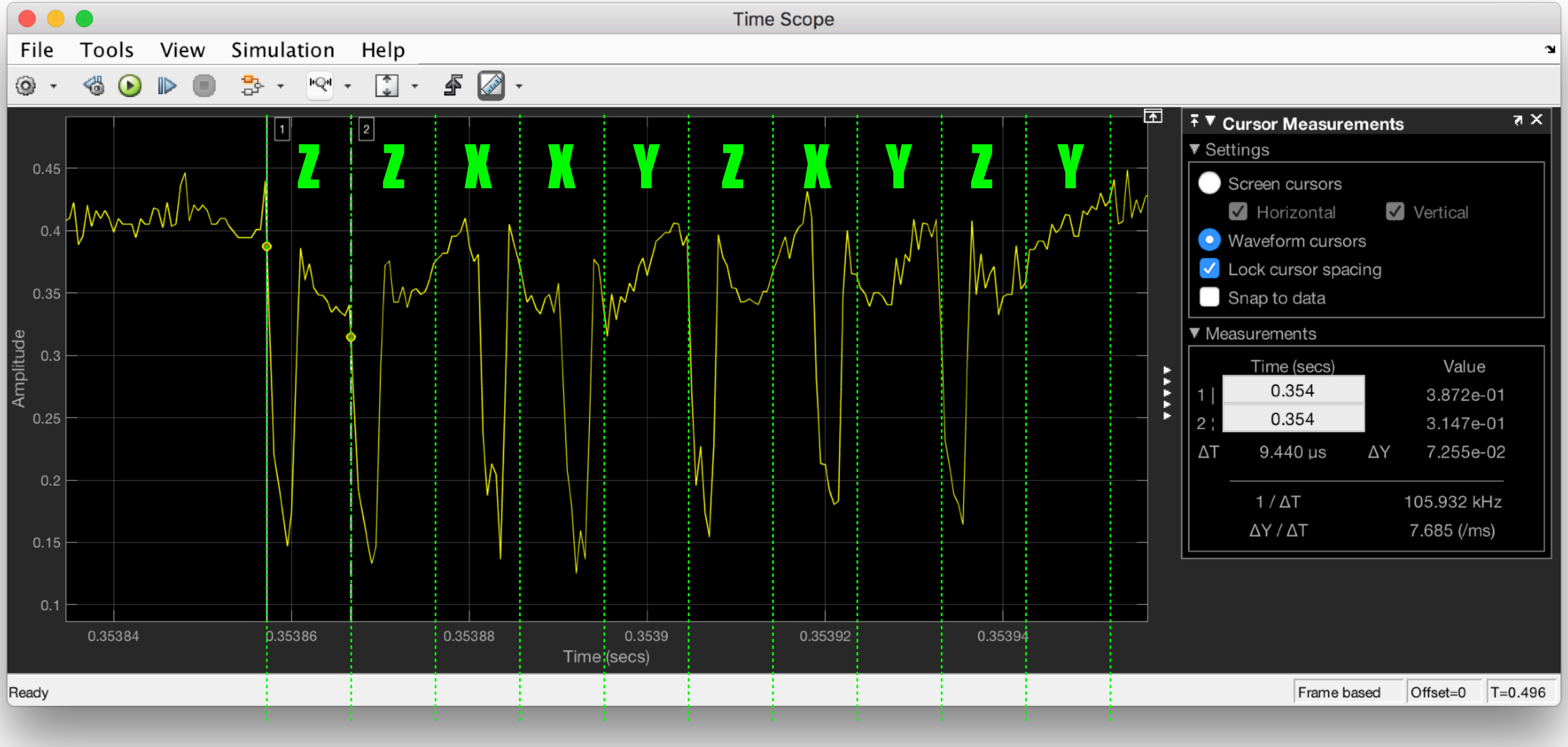
NooElec HAM It Up upconverter

RTL-SDR v.3

Radio Definition in Simulink



Identifying Miller Code Symbols



Cursor Measurements

Settings

○ Screen cursors

☑ Horizontal ☑ Vertical

● Waveform cursors

☑ Lock cursor spacing

□ Snap to data

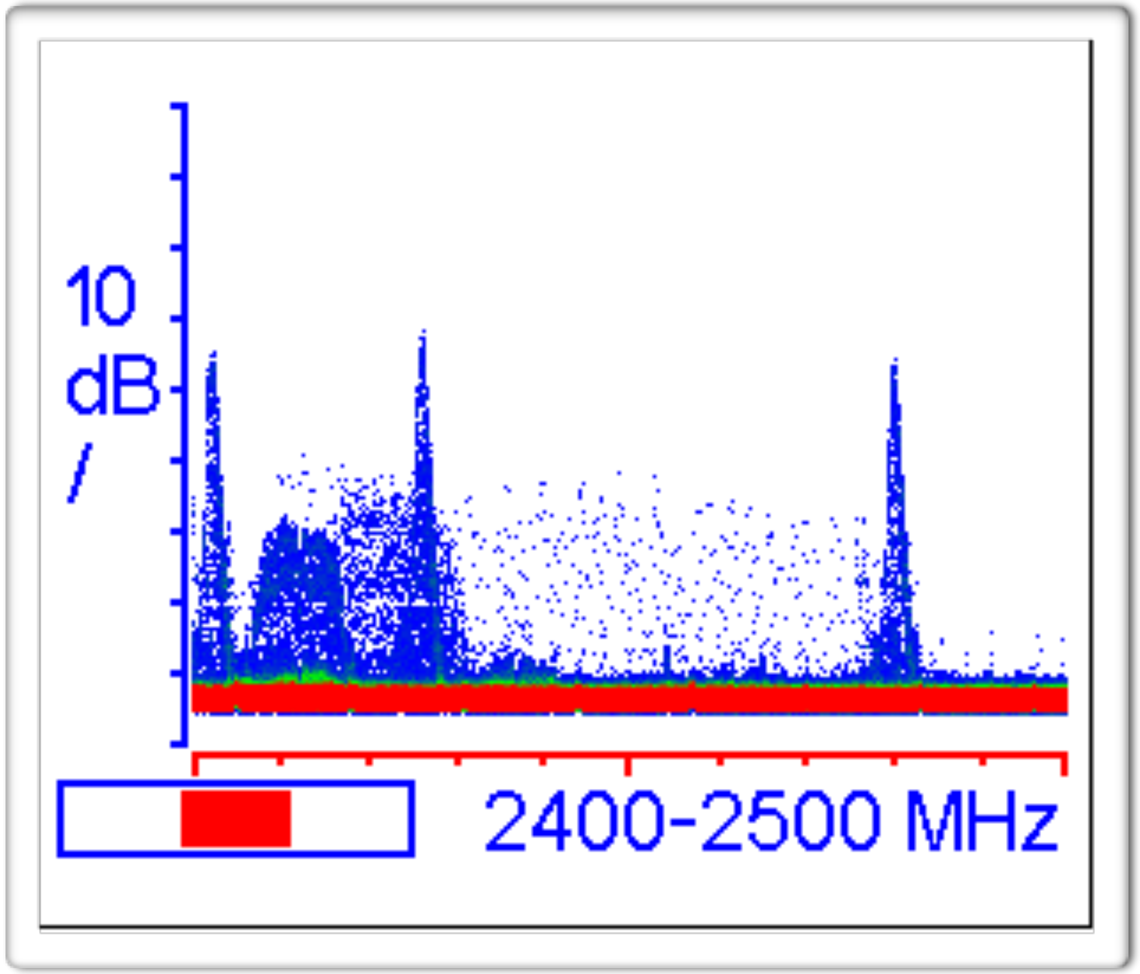
Measurements

	Time (secs)		Value
1	0.354		3.872e-01
2	0.354		3.147e-01
ΔT	9.440 µs	ΔY	7.255e-02
	1 / ΔT		105.932 kHz
	ΔY / ΔT		7.685 (/ms)

Attack in Changing Room

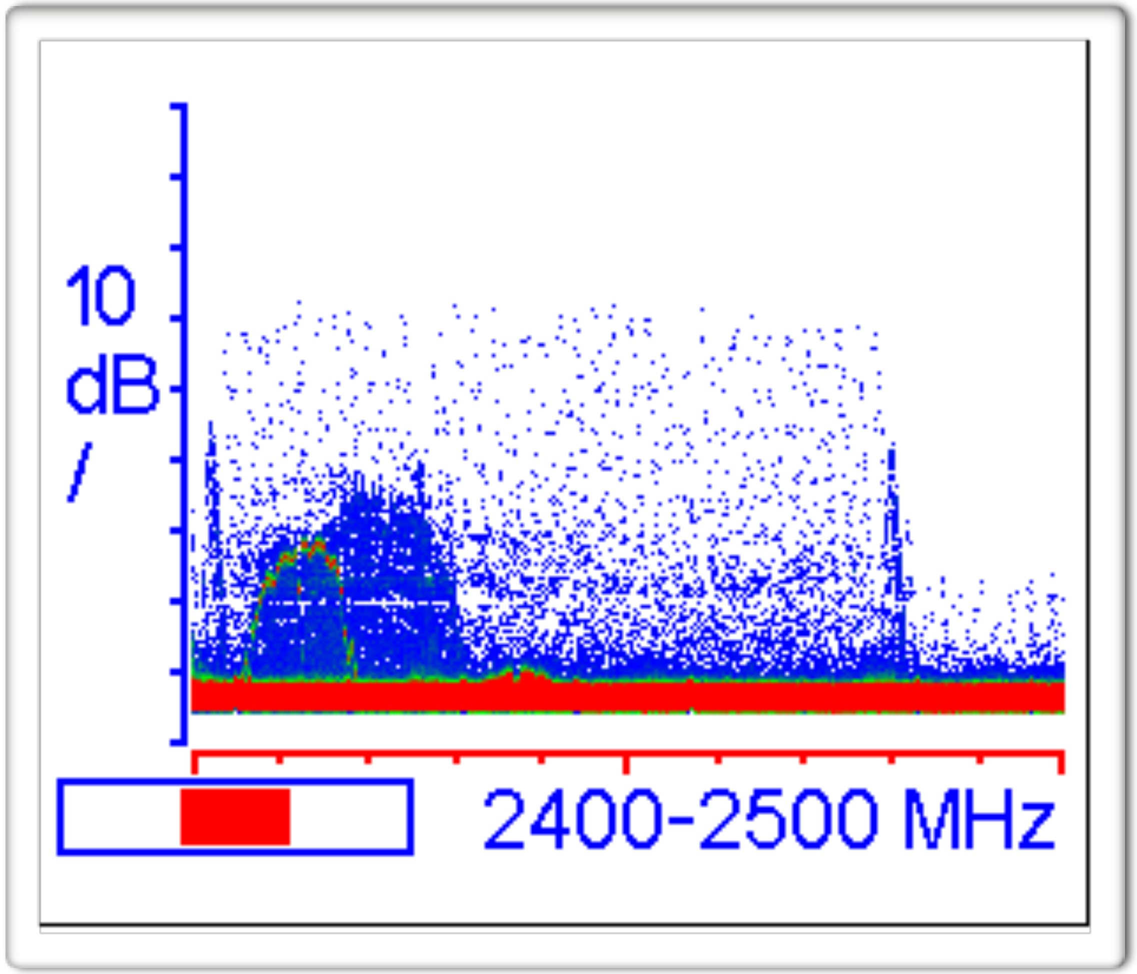
BLE - Bluetooth Low Energy
… (a.k.a. Bluetooth Smart)

BLE Radio Spectrum



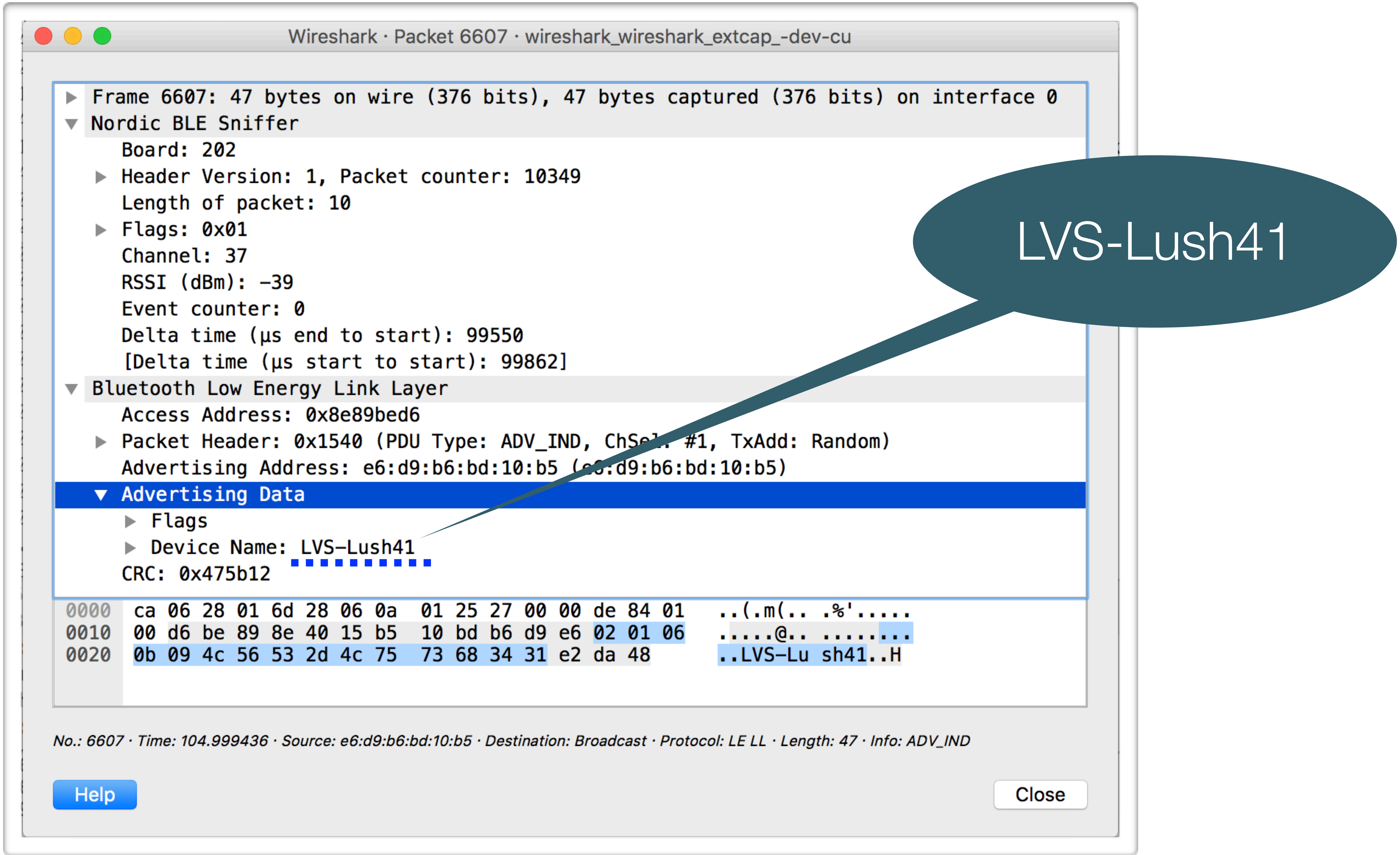
advertising

connection



[Indicative wide-band RF scans by RigExpert IT-24 analyser for 2.4 GHz]

Device Identification



Wireshark · Packet 6607 · wireshark_wireshark_extcap_-dev-cu

```
▶ Frame 6607: 47 bytes on wire (376 bits), 47 bytes captured (376 bits) on interface 0
▼ Nordic BLE Sniffer
    Board: 202
  ▶ Header Version: 1, Packet counter: 10349
    Length of packet: 10
  ▶ Flags: 0x01
    Channel: 37
    RSSI (dBm): -39
    Event counter: 0
    Delta time (µs end to start): 99550
    [Delta time (µs start to start): 99862]
▼ Bluetooth Low Energy Link Layer
    Access Address: 0x8e89bed6
  ▶ Packet Header: 0x1540 (PDU Type: ADV_IND, ChSel: #1, TxAdd: Random)
    Advertising Address: e6:d9:b6:bd:10:b5 (e6:d9:b6:bd:10:b5)
  ▼ Advertising Data
    ▶ Flags
    ▶ Device Name: LVS-Lush41
    CRC: 0x475b12
```

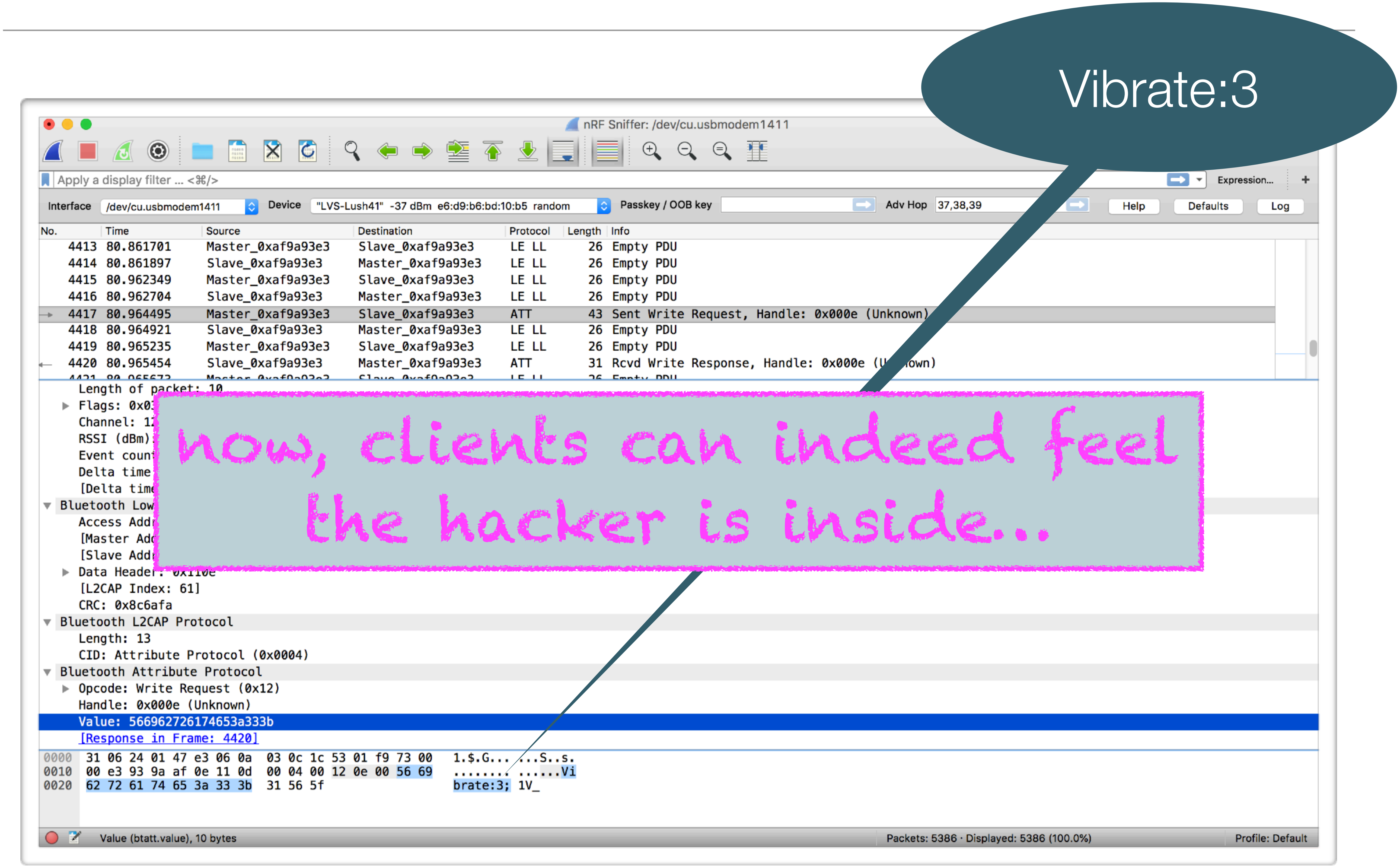
```
0000  ca 06 28 01 6d 28 06 0a  01 25 27 00 00 de 84 01   ..(.m(.. .%'.....
0010  00 d6 be 89 8e 40 15 b5  10 bd b6 d9 e6 02 01 06   .....@.. ........
0020  0b 09 4c 56 53 2d 4c 75  73 68 34 31 e2 da 48      ..LVS-Lu sh41..H
```

No.: 6607 · Time: 104.999436 · Source: e6:d9:b6:bd:10:b5 · Destination: Broadcast · Protocol: LE LL · Length: 47 · Info: ADV_IND

LVS-Lush41

LVS-Lush41: Lovense Lush

Unprotected Control Commands 😉😳😁



Vibrate:3

nRF Sniffer: /dev/cu.usbmodem1411
Apply a display filter ... <⌘/>
Expression...
Help
Defaults
Log

Interface /dev/cu.usbmodem1411 Device "LVS-Lush41" -37 dBm e6:d9:b6:bd:10:b5 random Passkey / OOB key Adv Hop 37,38,39

```
No.   Time       Source             Destination        Protocol Length Info
 4413 80.861701  Master_0xaf9a93e3  Slave_0xaf9a93e3   LE LL    26 Empty PDU
 4414 80.861897  Slave_0xaf9a93e3   Master_0xaf9a93e3  LE LL    26 Empty PDU
 4415 80.962349  Master_0xaf9a93e3  Slave_0xaf9a93e3   LE LL    26 Empty PDU
 4416 80.962704  Slave_0xaf9a93e3   Master_0xaf9a93e3  LE LL    26 Empty PDU
 4417 80.964495  Master_0xaf9a93e3  Slave_0xaf9a93e3   ATT      43 Sent Write Request, Handle: 0x000e (Unknown)
 4418 80.964921  Slave_0xaf9a93e3   Master_0xaf9a93e3  LE LL    26 Empty PDU
 4419 80.965235  Master_0xaf9a93e3  Slave_0xaf9a93e3   LE LL    26 Empty PDU
 4420 80.965454  Slave_0xaf9a93e3   Master_0xaf9a93e3  ATT      31 Rcvd Write Response, Handle: 0x000e (U    own)
 4421 80.965673  Master_0xaf9a93e3  Slave_0xaf9a93e3   LE LL    26 Empty PDU
```

```
    Length of packet: 10
  ▶ Flags: 0x0
    Channel: 1
    RSSI (dBm)
    Event coun
    Delta time
    [Delta tim
▼ Bluetooth Low
    Access Addr
    [Master Add
    [Slave Addr
  ▶ Data Header: 0x110e
    [L2CAP Index: 61]
    CRC: 0x8c6afa
▼ Bluetooth L2CAP Protocol
    Length: 13
    CID: Attribute Protocol (0x0004)
▼ Bluetooth Attribute Protocol
  ▶ Opcode: Write Request (0x12)
    Handle: 0x000e (Unknown)
    Value: 566962726174653a333b
    [Response in Frame: 4420]
```

```
0000  31 06 24 01 47 e3 06 0a  03 0c 1c 53 01 f9 73 00   1.$.G... ...S..s.
0010  00 e3 93 9a af 0e 11 0d  00 04 00 12 0e 00 56 69   ........ ......Vi
0020  62 72 61 74 65 3a 33 3b  31 56 5f                  brate:3; 1V_
```

Value (btatt.value), 10 bytes   Packets: 5386 · Displayed: 5386 (100.0%)   Profile: Default

now, clients can indeed feel the hacker is inside..

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