QuBit

UNIVERSE OF **CYBER SECURITY**
AND **DIGITAL FORENSICS**

GNSS/GPS Radio Hacking

From Beautiful Equations to Serious Threats

Tomas Rosa

http://crypto.hyperlink.cz

CONFERENCE 2016
PRAGUE
APRIL 12-14

updated 05/26/2016

Revisions

- **05/12/2016**: GLONASS replay attack (meaconing) example described; minor typographic corrections; references added/ edited
- **05/26/2016**: incidental radiation snapshots

Agenda

Civil GPS service

- principles and vulnerabilities of L1 C/A signal

GNSS security research workbench

- software-defined radio (SDR)
- signal sampling and reconstruction
- noise in radio signal processing
- RF front-end based on Mini-Circuits design

Accessible experiments and further encouragement

How Do We Approach This

First method

> "Hey folks, look what I've done!
>
> All you need is: `$ sudo wtfbbq -hEy -b01b16 -Go`"
>
> Nope, too shallow.

Second method

> "Hmm, you are just citing Euler, aren't you?!"
>
> Nope, too arrogant here.

… and yes, we have something like 30 minutes or less…

So, let's try to go through theoretically correct and practically understandable snapshots of the fascinating area of GNSS security research.

Have you said *GNSS*?

GNSS stands for Global Navigation Satellite System(s)

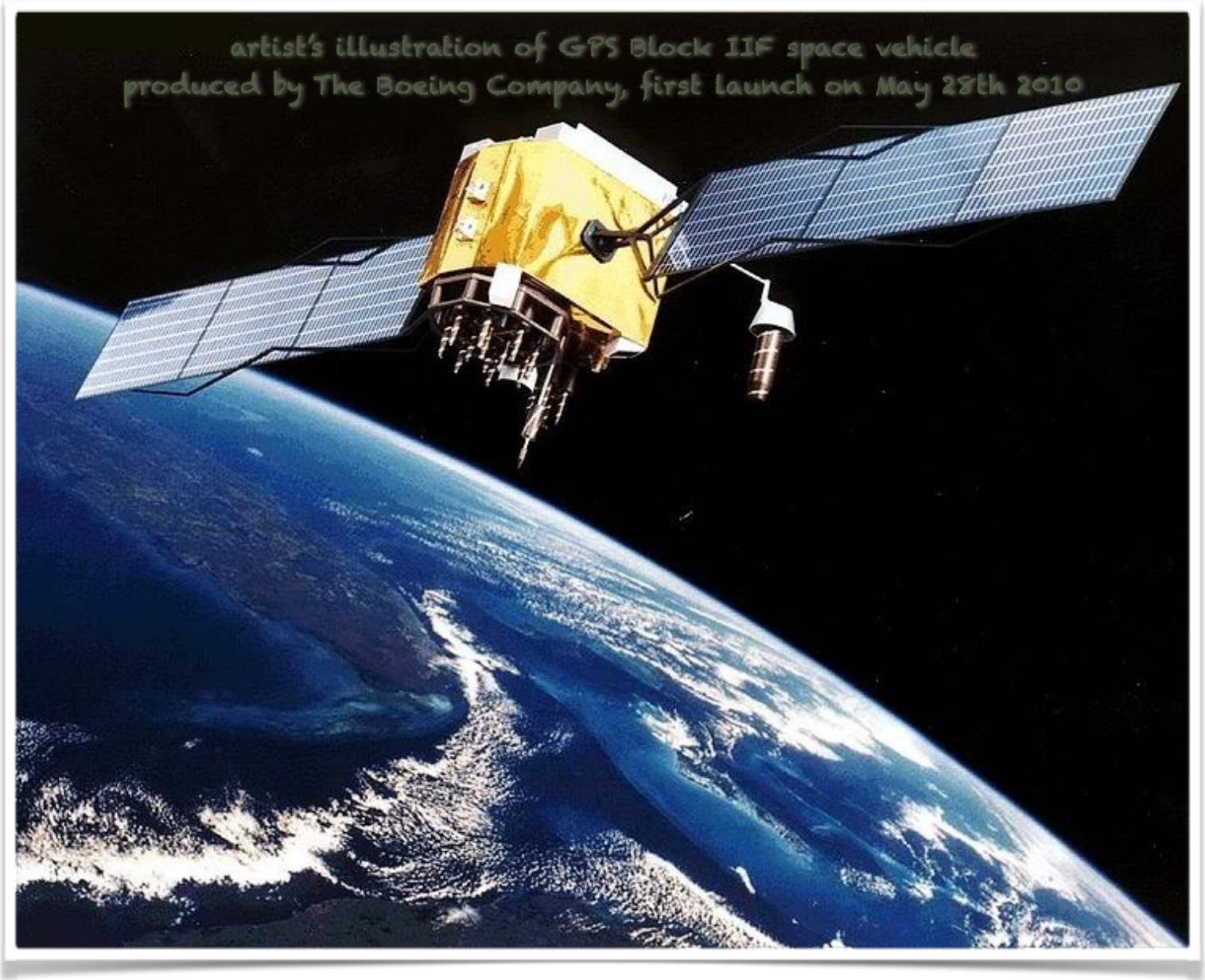
NAVSTAR GPS is one particular kind of GNSS

The other ones are namely:

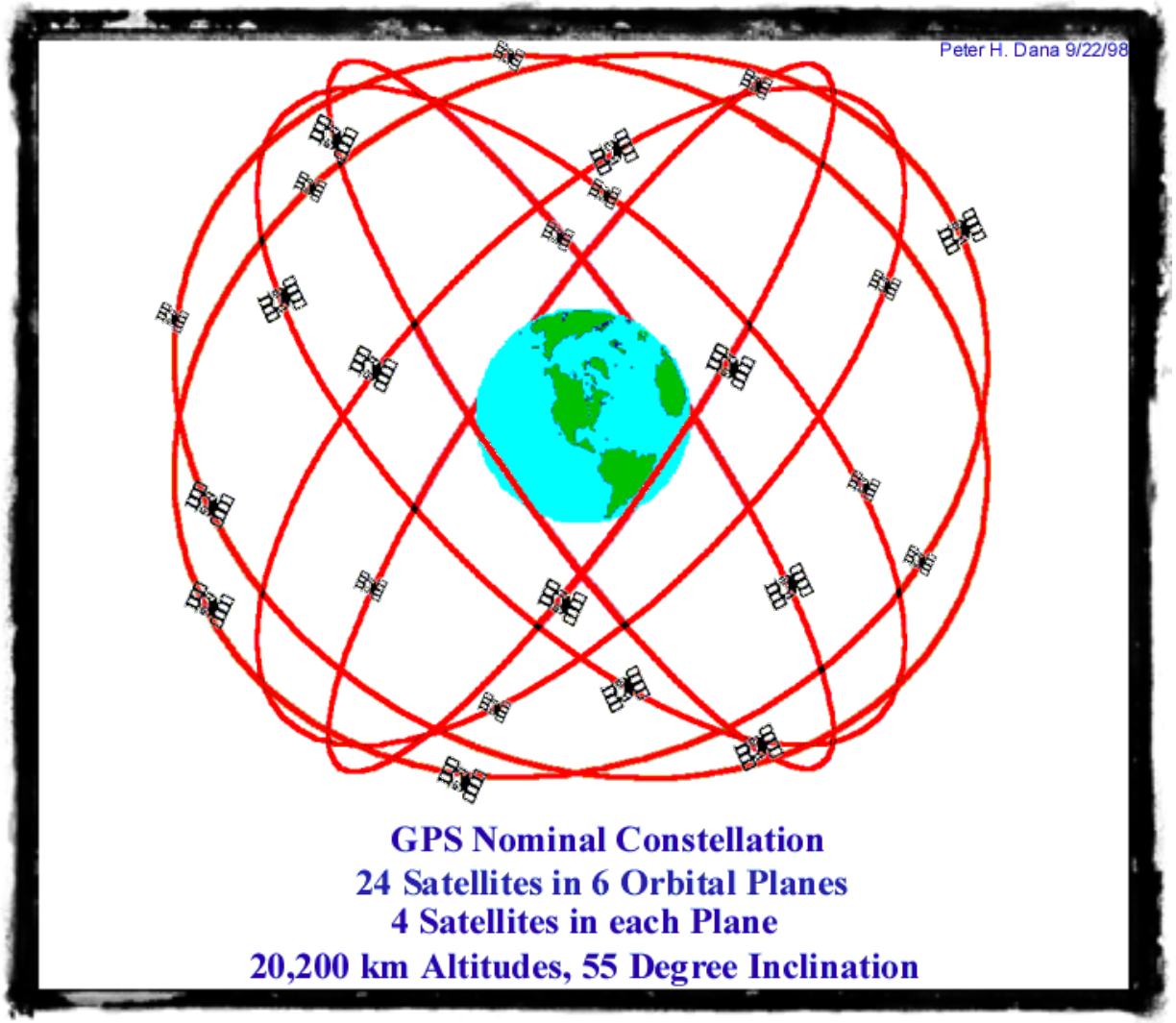
- Chinese BeiDou-2 (former COMPASS)
- European Galileo (governed by GSA in Prague)
- Russian GLONASS (Globalnaya Navigatsionnaya Sputnikovaya Sistema)

All of them are facing very similar problems with their civil services

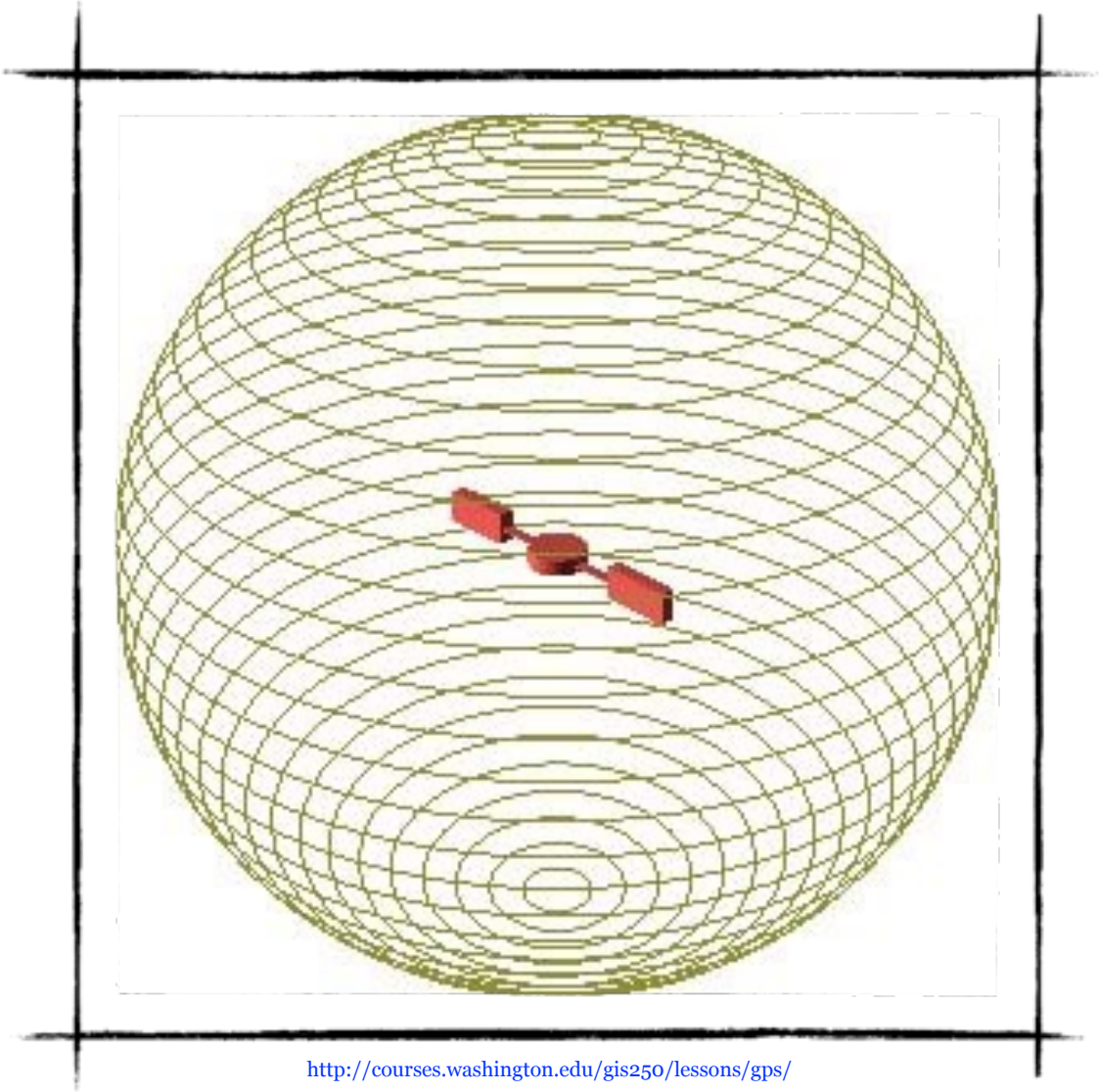
GPS Space Segment Vehicle - SV - (Block IIF)



GPS Space Segment

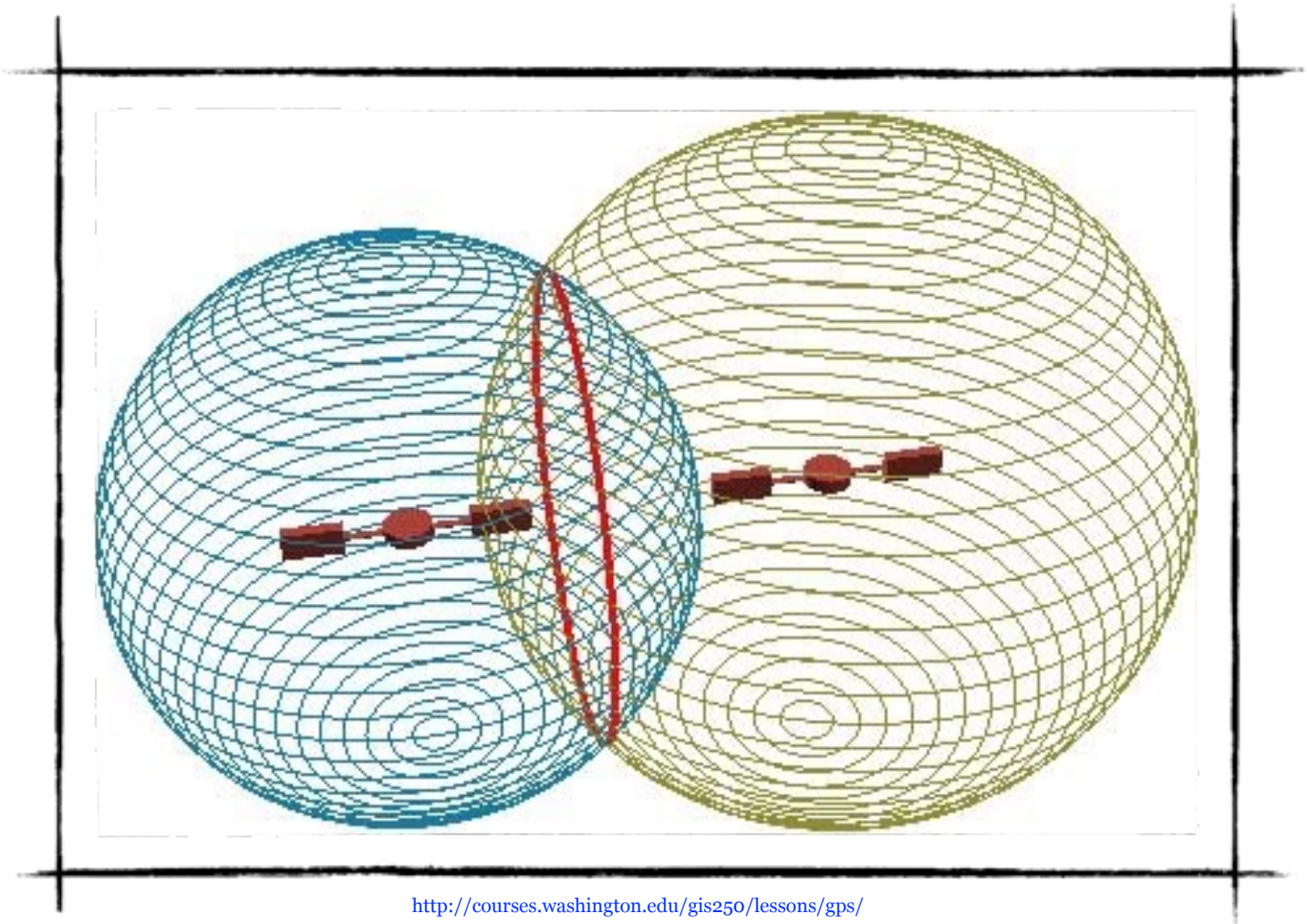


Trilateration I



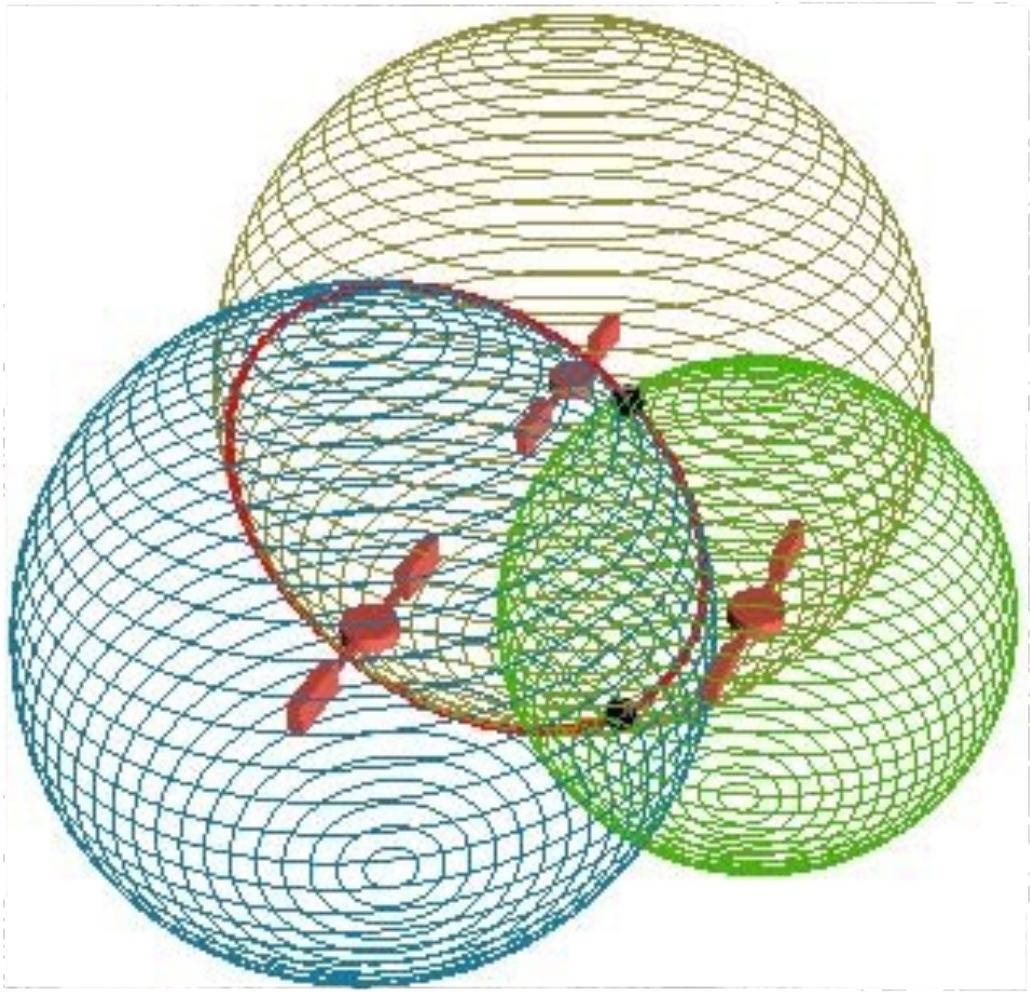
http://courses.washington.edu/gis250/lessons/gps/

Trilateration II



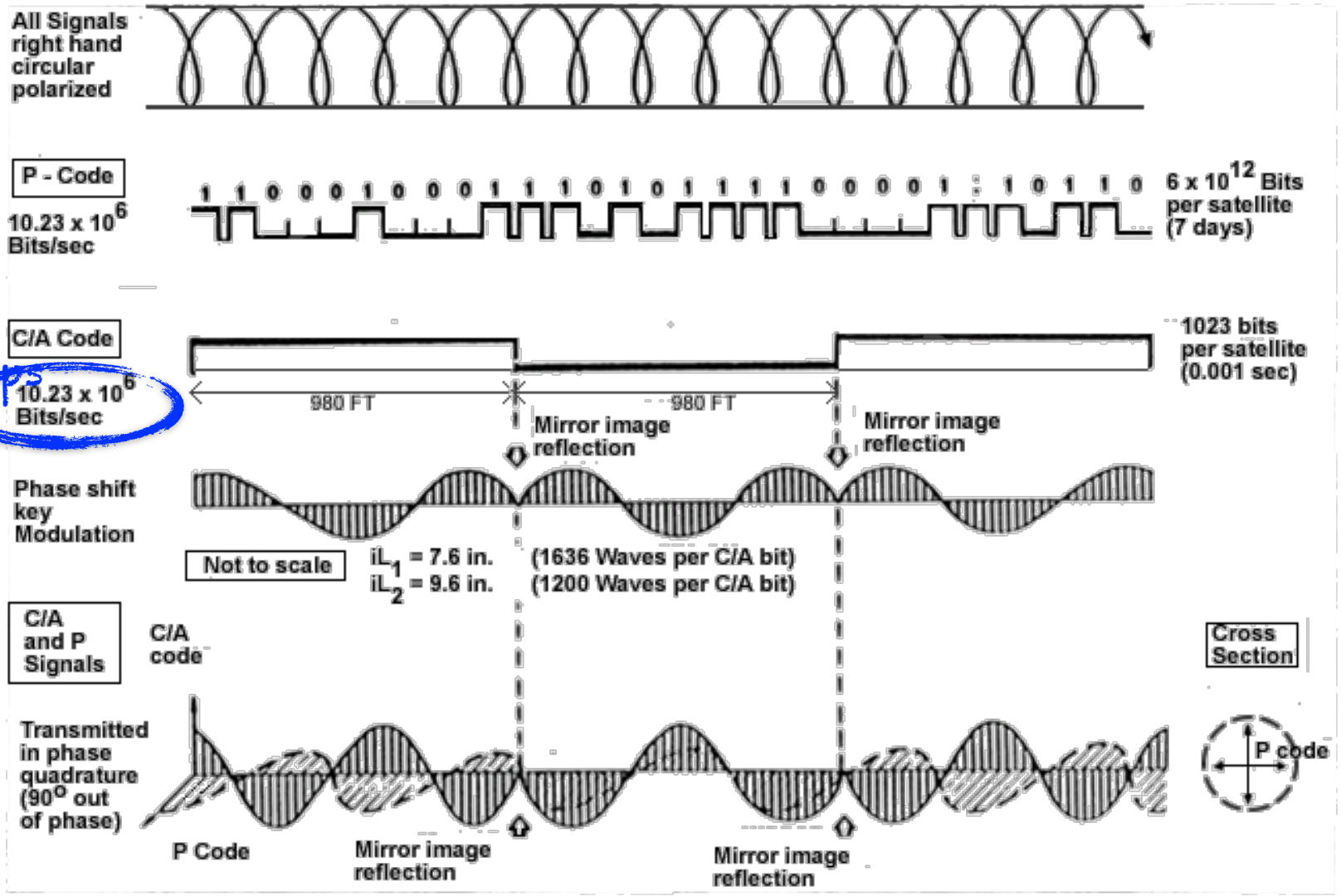
http://courses.washington.edu/gis250/lessons/gps/

Trilateration III



http://courses.washington.edu/gis250/lessons/gps/

GPS L1 C/A ⊗ P(Y) (Illustration ONLY)



actually 1.023 Mbps

Kulshreshta, 1997

Satellite clock observations expose time delays that in turn reveal the distance in between the particular satellite and the observer

t_{sent_sv1}

t_{sent_sv2}

t_{sent_sv3}

four SVs to get
X, Y, Z, and t_{bias}

t_{sent_sv4}

$t_{rec}+t_{bias}$

L1 C/A Signal in Brief

CDMA (Code Division Multiple Access) at the carrier frequency of 1575.42 MHz

... BPSK-R(1) Direct Sequence Spread Spectrum (DSSS) according to the notation of [Betz, 16]

Satellites distinguished by their unique chipping sequence (Gold codes)

Allows creation of a delayed replica clock of the particular satellite (embedded time synchronisation)

Carries in total 37 500 bits of navigation data sent on each individual satellite signal (channel) for explicit time synchronisation, position computation, and faster acquisition of other SVs

Includes corrections according to the General Theory of Relativity

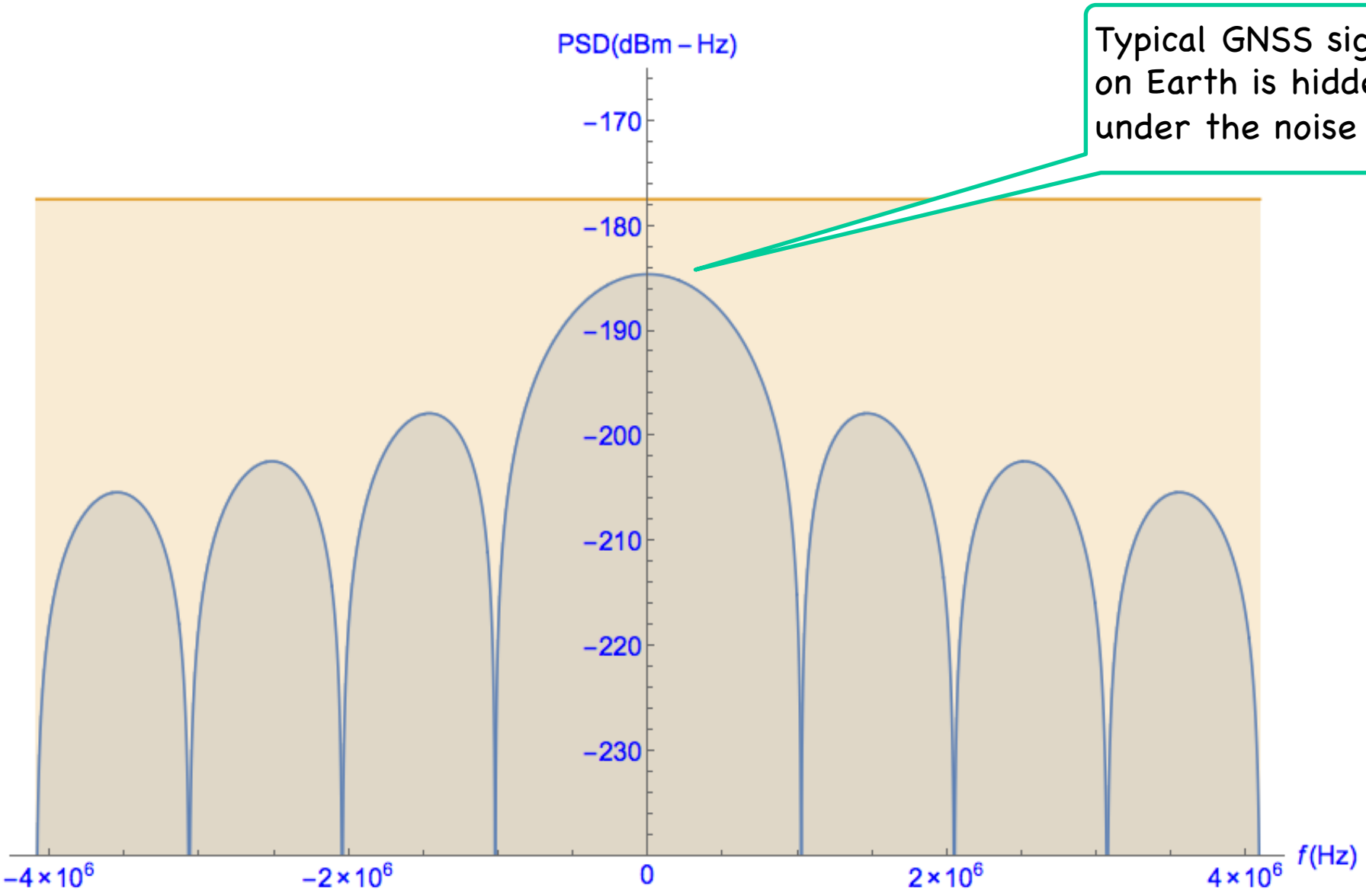
… does not include any cryptographic protection

L1 C/A Signal in Detail

Carrier frequency	L1: 1575.42 MHz = 154 x 10.23 MHz
Minimum received power	-158.5 dBW = -128.5 dBm
Polarization	Right-Hand Circular Polarization (RHCP)
Multiple access	Code Division Multiple Access (CDMA)
Spreading modulation	Binary Phase-Shift Keying with Rectangular symbols and chipping rate 1 x 1.023 MHz ~ BPSK-R(1)
Tx bandwidth	±15.345 MHz; first null-to-null BW is 2.046 MHz
Spreading codes	Length 1023-bit Gold codes, duration 1 ms
Data message structure	NAV
Data rate	50 bps
Data error control code	Extended (32,26) Hamming code
Data modulation	50 sps biphase modulation
Pilot and data components	100% power data
Overlay code	None
Multiplexing with other signals	In phase quadrature to L1 P(Y), etc.

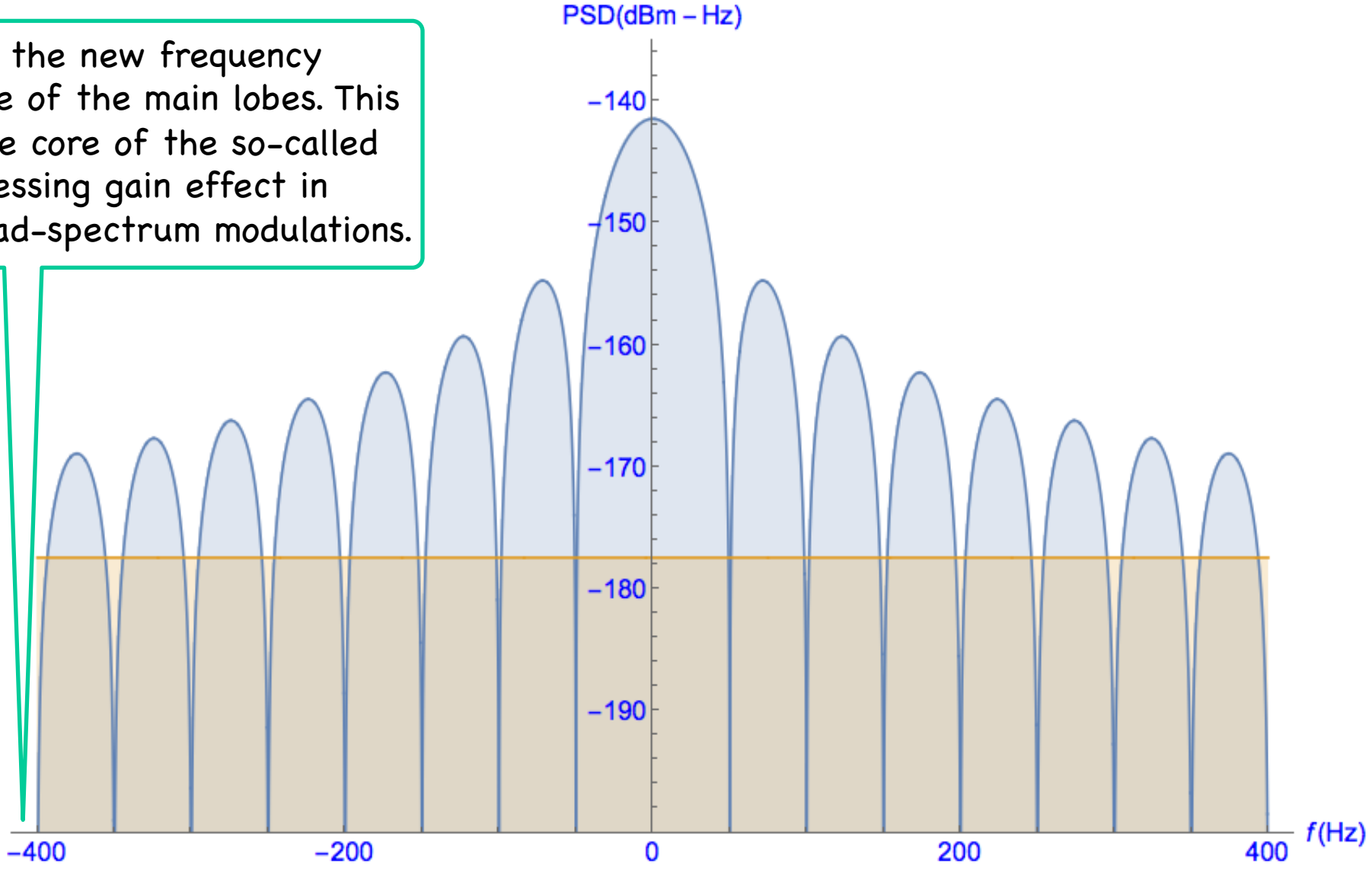
[Betz, 16]

L1 C/A Typical Antenna Received Signal Power Spectral Density Envelope vs. Background Noise Level (130 K)



L1 C/A After Correlation-Based Despreading

Note the new frequency range of the main lobes. This is the core of the so-called processing gain effect in spread-spectrum modulations.



Satellite Clock Observation Revisited

Let s_i denote the signal generated by SV_i, and let $\varphi(t)$ be any "reasonably" smooth function of time.

Then one can recover $\varphi(t)$ by observing the received signal

$$s\_recv_i(t) = s_i(\varphi(t))$$

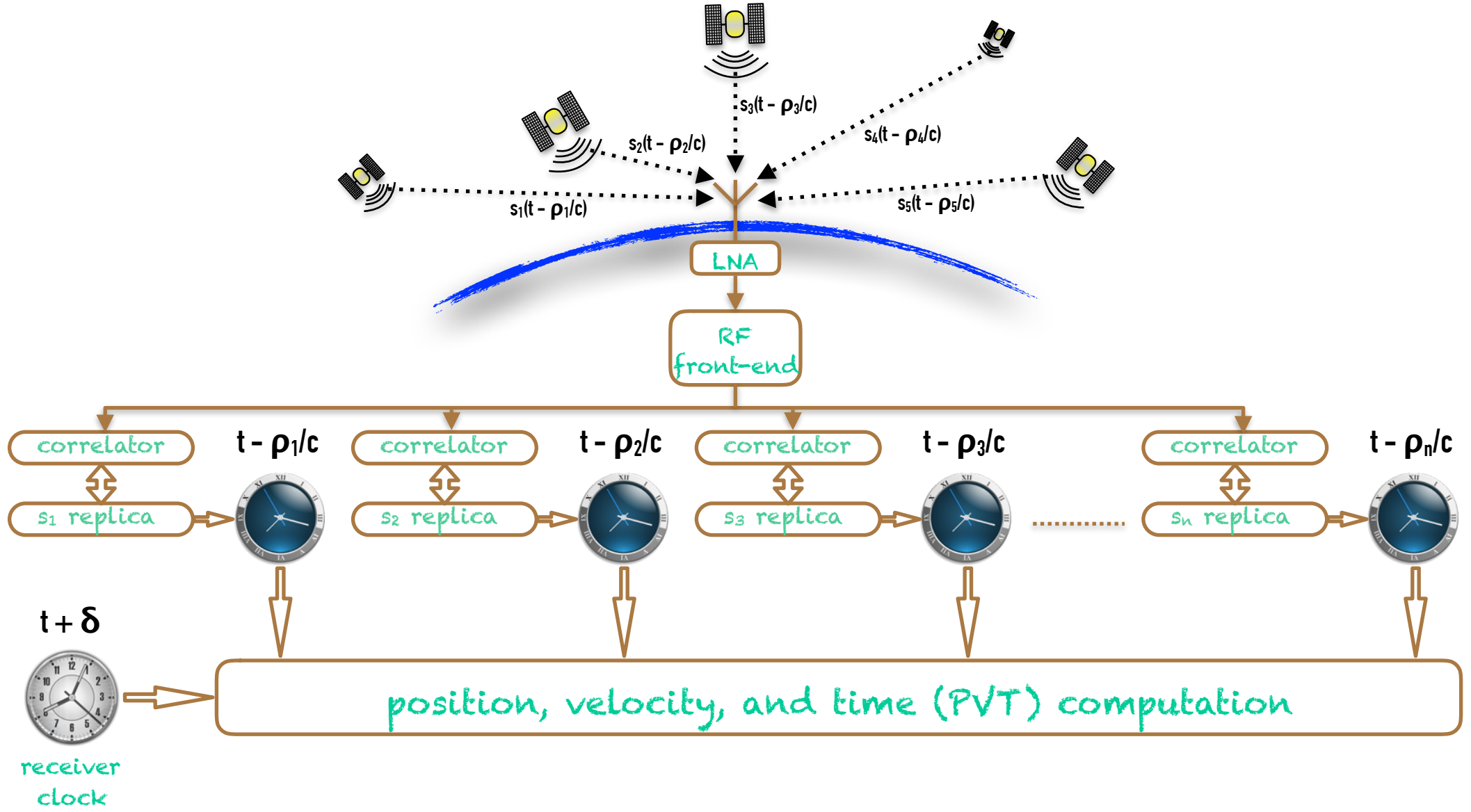
... this is achieved through implicit (*carrier, chipping sequence, data modulation*) and explicit (*navigation data*) time stamps embedded into the satellite signal

In first approximation, we let

$$\varphi(t) = t - \frac{\rho_i}{c}$$

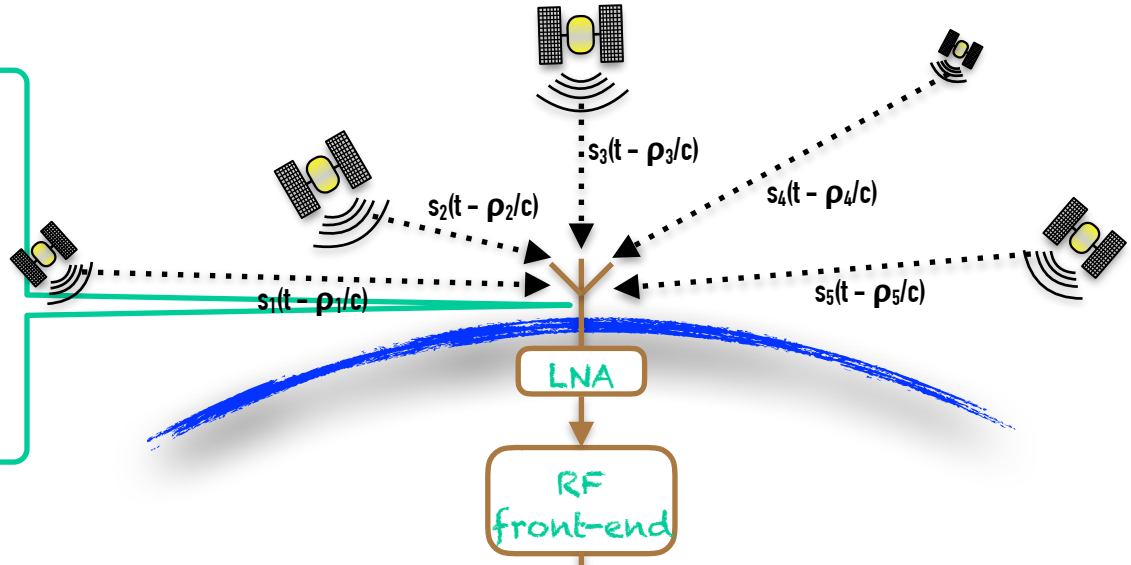
where ρ_i represents the distance travelled by the signal in between the observer and SV_i and t is the GPS master time, all in the observer's frame on Earth.

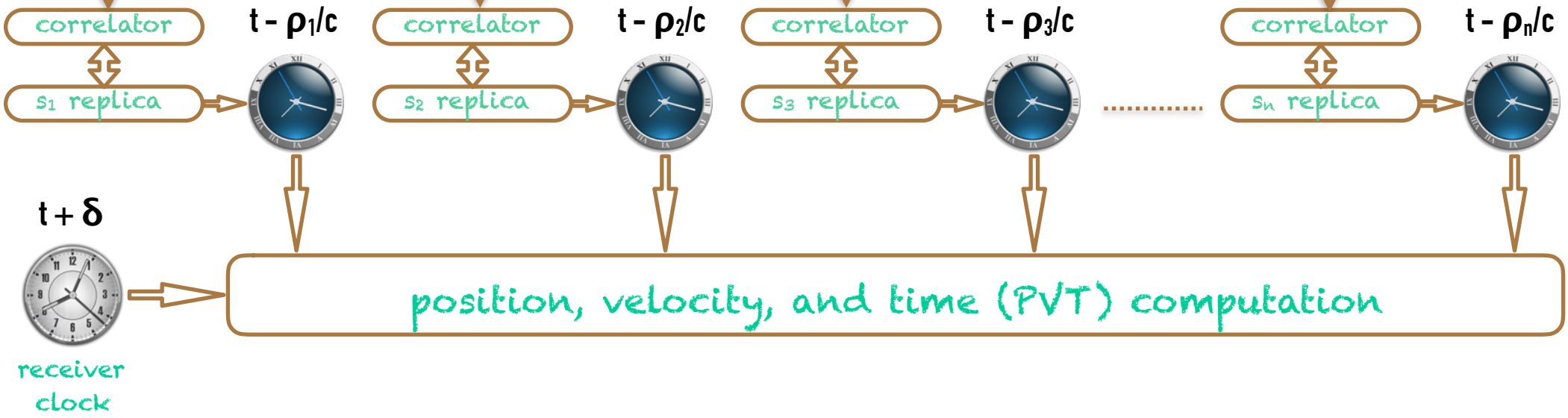
GNSS Tracking Illustration



GNSS Tracking Illustration

Antenna phase center – apparent location of EM wave reception, according to which rho$_i$ is considered.





Civil GPS in Serious Applications

NTP server
governing e.g.
financial transactions

The importance is recognised, great!

L1 C/A Security

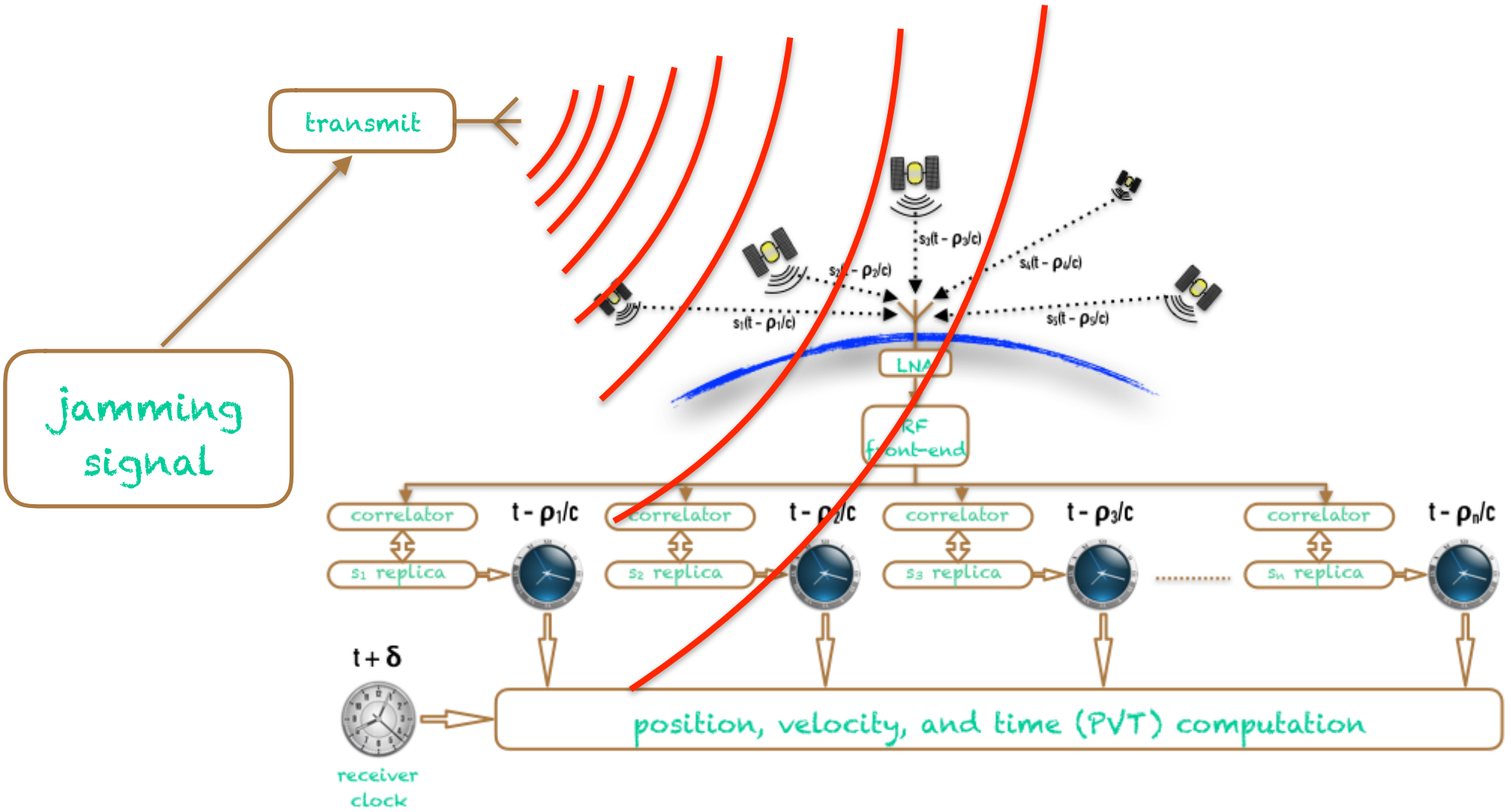
Position/Velocity/Time (PVT) manipulation is accessible to a moderate-level attacker

- real-life scenario may (allegedly) be that "**Iran–U.S. RQ-170 incident**"
- actually, a GPS "replay attack" (meaconing) is a standard advanced tutorial for the LabView platform using the USRP Software Defined Radio (SDR)

OK, this signal was never meant as a military-grade service and the lack of protection here can hardly be called a "discovery"

On the other hand, a lot of L1 C/A applications have grown up to be vital parts of our critical infrastructure today… [Volpe's center, 01]

GNSS Jamming Attack

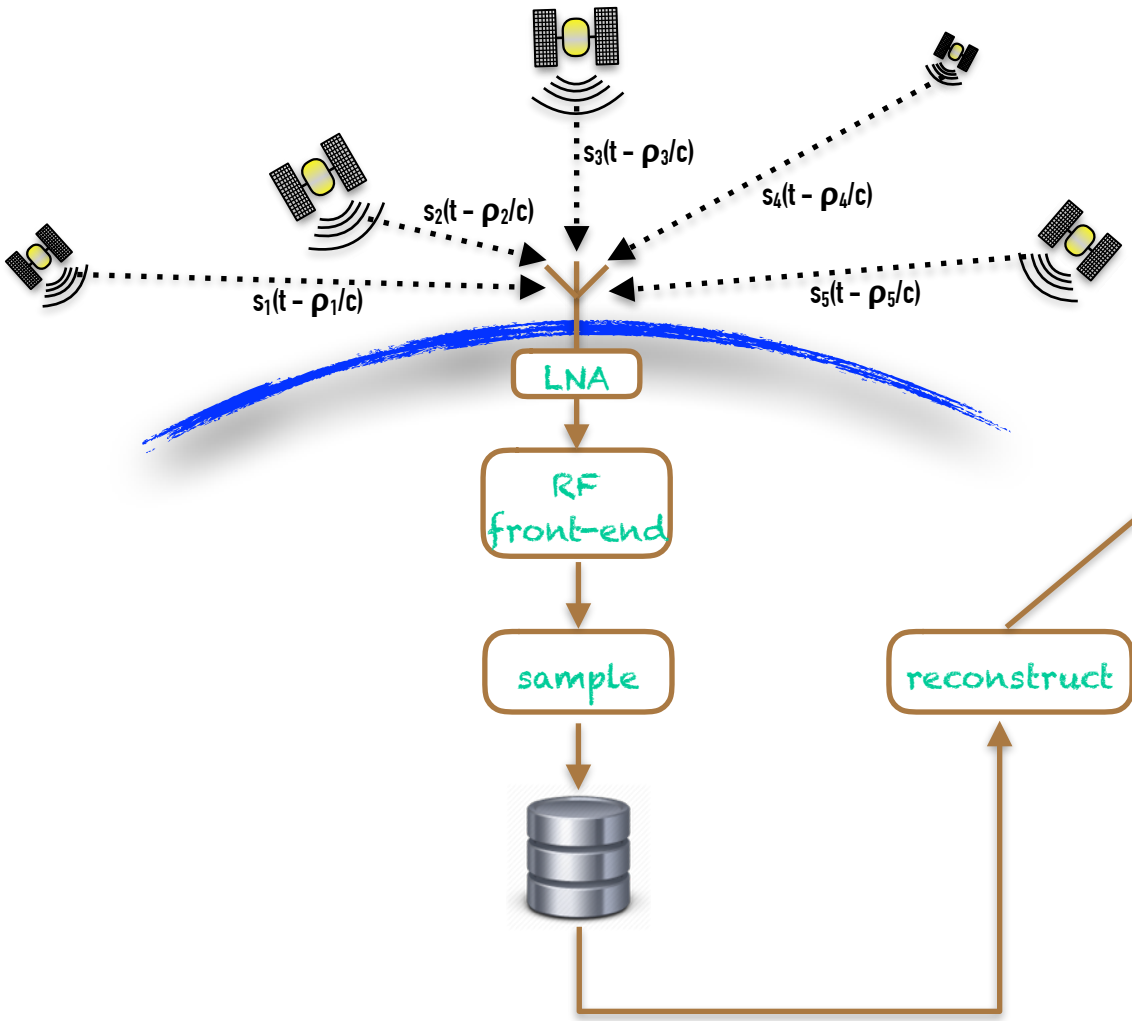


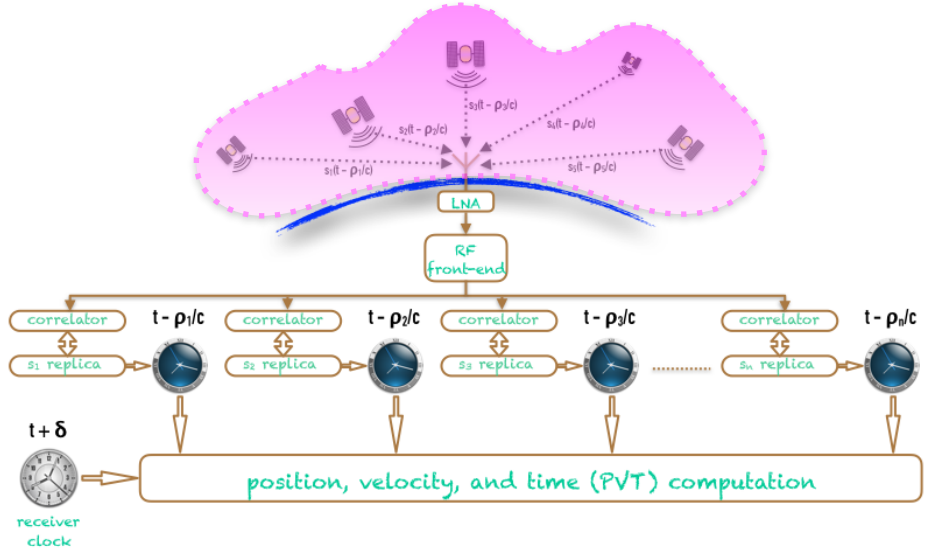
Jamming is Really a Serious Threat

South Korea issues warning over suspected North Korean GPS disruption

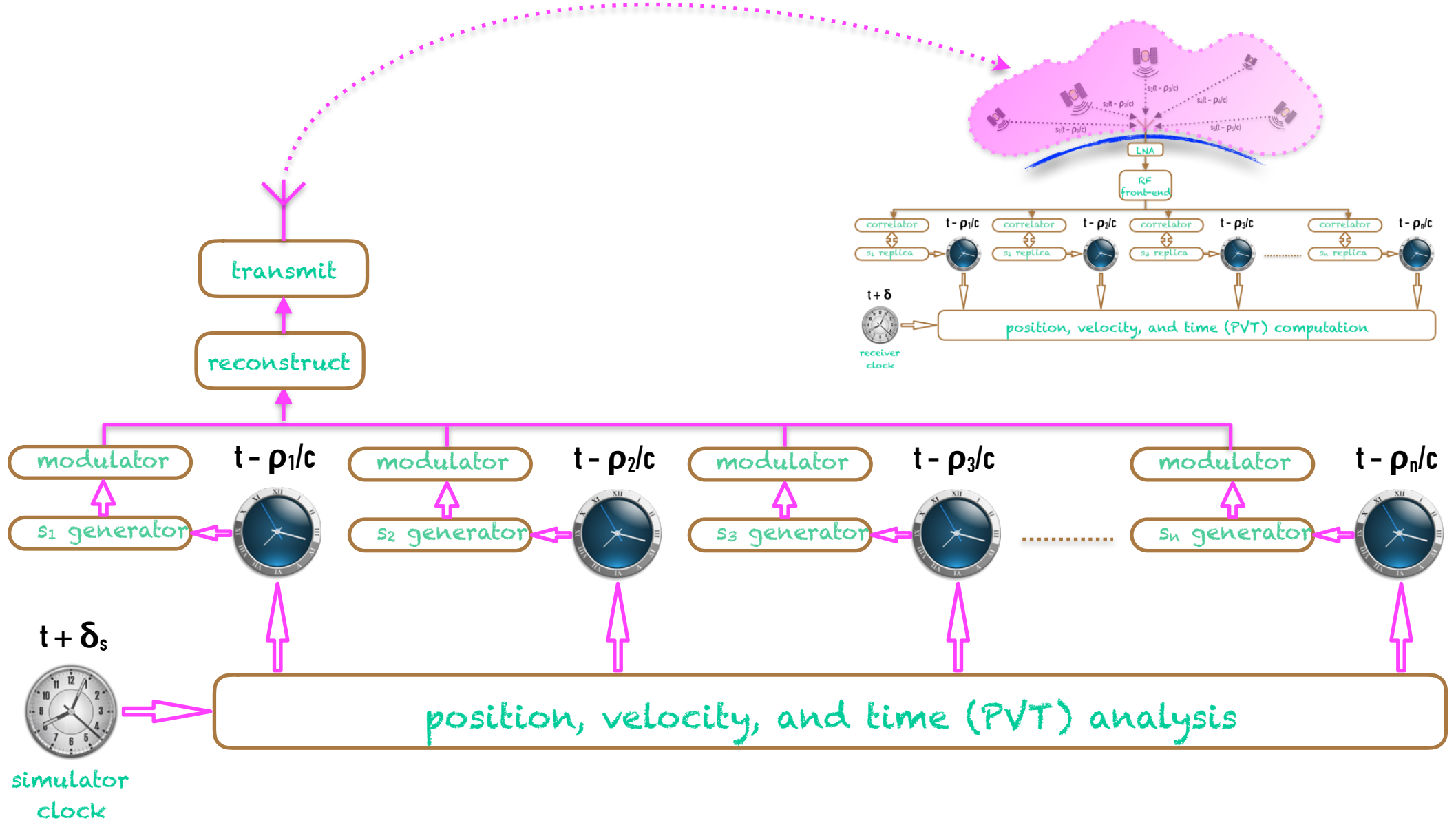
March 31, 2016 - By GPS World staff

GNSS Replay Attack (Meaconing)





GNSS Spoofing Attack by Tracking Reversal



Further Classification

By the fake signal injection scenario requirements

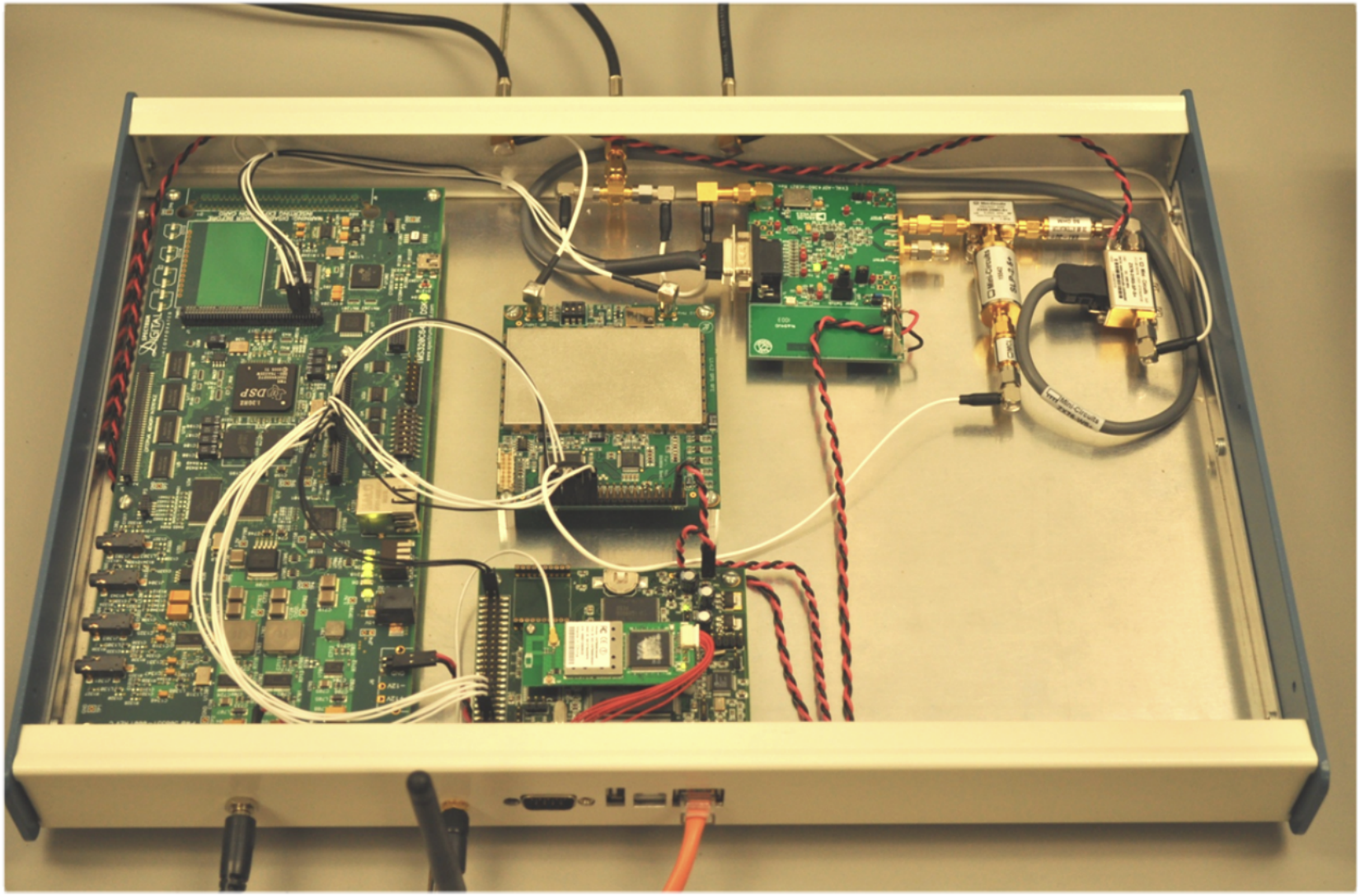
- receiver cold start necessary
- receiver warm start (remembering last PVT)
- nothing special - the attacker can hijack the receiver while it is tracking the original signal

By Tx path diversity

- one signal source
- multiple synchronised spatial signal sources

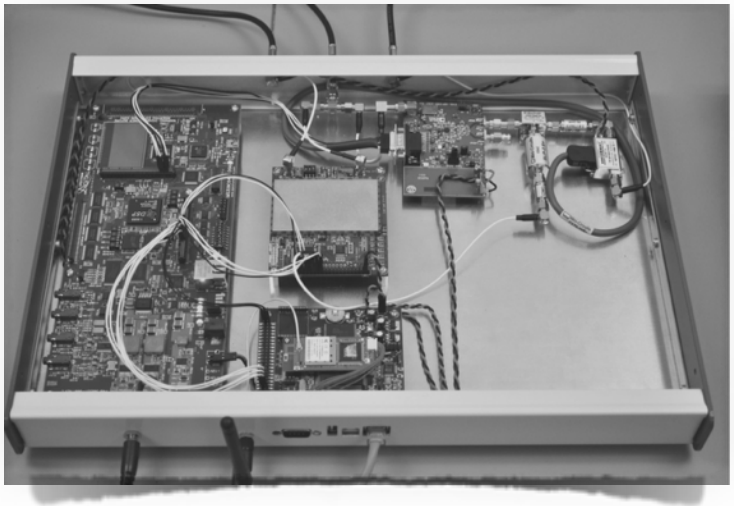
cf. also [Dovis, 15]

Civil GPS Under Serious Attack



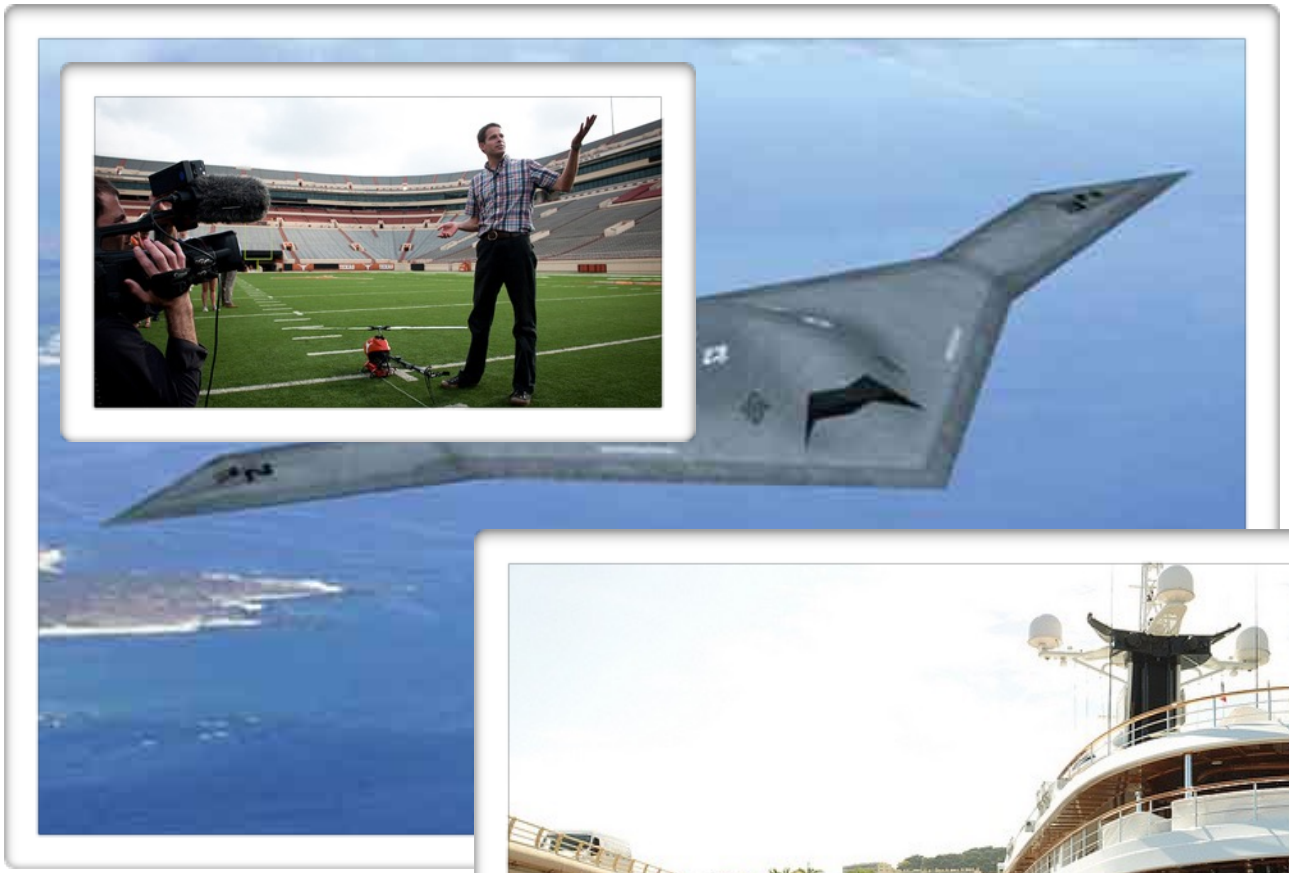
[Humphreys, Ledvina, and Shepard, 2008-2011]

Precise SDR-based Spoofer (Hijack Style)



[Humphreys, Ledvina, and Shepard, 08-11]

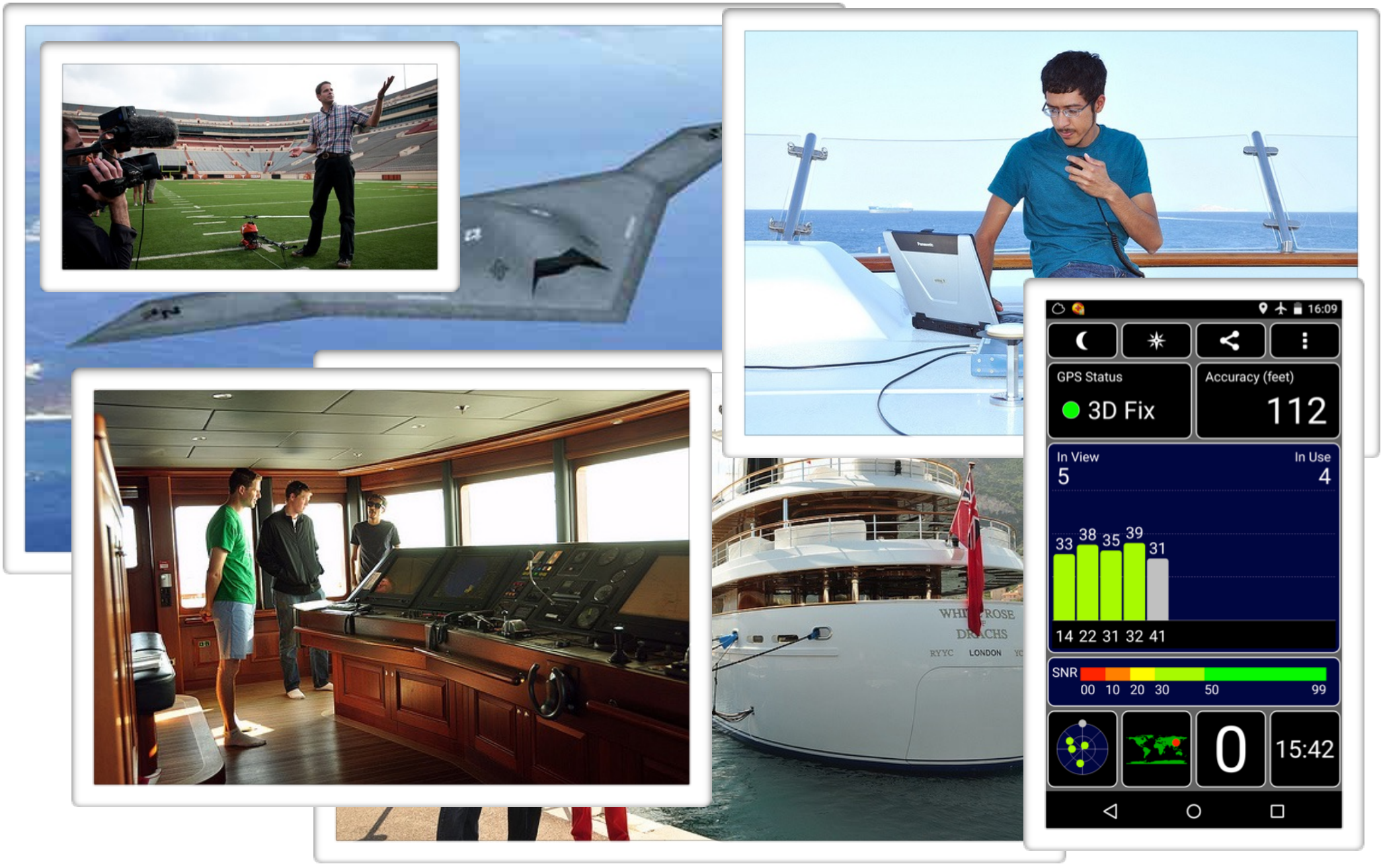
- receiver-spoofer (MITM) architecture
- tracks original L1 C/A and L2C
- manipulates individual SV signal channels of L1 C/A (up to 12)
- re-mixes and re-transmits the spoofed signal
- precise phase sync for a smooth take over
- SDR architecture; someday it could be just downloaded and run
- HW parts were off-the-shelf components of approx. $1500 (2008)



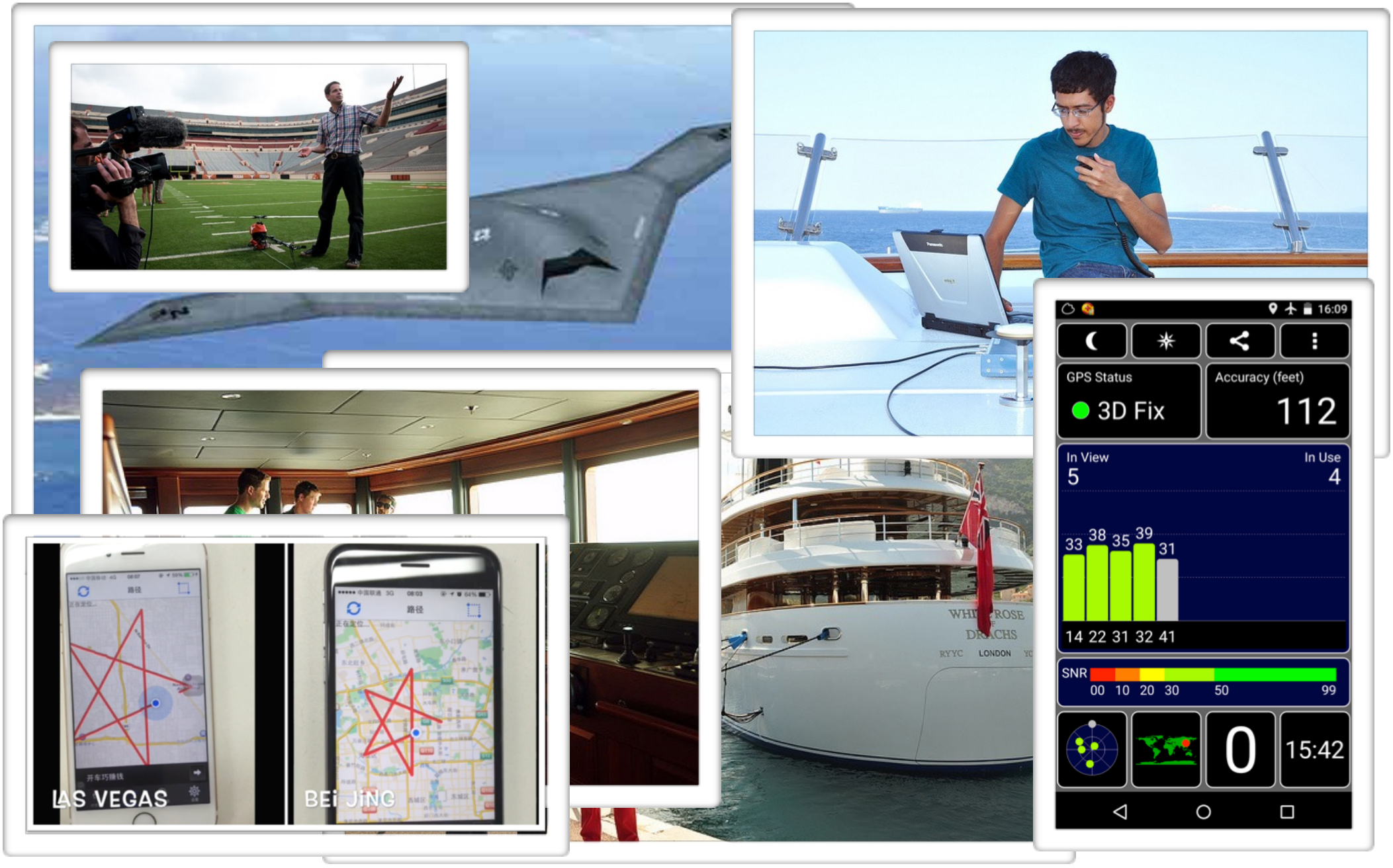
[Bhatti, Humphreys, Ledvina, Pesyna, Shepard, Huang, Yang, Wang, Chen, Pan, et al. - cf. references]

[Bhatti, Humphreys, Ledvina, Pesyna, Shepard, Huang, Yang, Wang, Chen, Pan, et al. - cf. references]

[Bhatti, Humphreys, Ledvina, Pesyna, Shepard, Huang, Yang, Wang, Chen, Pan, et al. - cf. references]



[Bhatti, Humphreys, Ledvina, Pesyna, Shepard, Huang, Yang, Wang, Chen, Pan, et al. - cf. references]



[Bhatti, Humphreys, Ledvina, Pesyna, Shepard, Huang, Yang, Wang, Chen, Pan, et al. - cf. references]

[Bhatti, Humphreys, Ledvina, Pesyna, Shepard, Huang, Yang, Wang, Chen, Pan, et al. - cf. references]

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 below

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

The Next Target?

Recall those 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…

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.

Easy-to-implement broadcast data origin authentication that is resistant to meaconing

... 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]

Deeper incorporation of cryptography into the modulation scheme, provided - for instance - signal detection prevention 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

Also, be prepared that, once deployed, infrastructure users will probably try to legally tweak our cryptoscheme to get more of it

... e.g. this controlled, server-side meaconing of Galileo Public Regulated Service (PRS) [Rugamer, et al., 14]; *btw PRS is the highly promising Galileo flagship service, however, it is a totally closed design with unclear security goals, cryptographic techniques, and last but not least user license, so - despite the indisputable effort of many people - it somehow brings more questions than answers…*

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

Selected SDR Projects

- GNSS-SDR
- A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach
- GPS-SDR-SIM
- GPS-SIM

Selected SDR Projects

GNSS-SDR

- http://gnss-sdr.org
- open source project of a very robust, general GNSS receiver based on using popular and accessible SDRs (even RTL-SDR is supported)
- C/C++ project based on the GNU Radio framework
- besides this SW and the SDR itself, you will usually need an RF front-end like the one described below
- great opportunity to learn practical aspects of GNSS signal processing with the ability to put your results back to the research community
- especially reasonable choice if you want to experiment with the latest Galileo signals

A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach

GPS-SDR-SIM

GPS-SIM

Selected SDR Projects

GNSS-SDR

A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach

- distributed together with the book of the same title [Bore et al., 16]
- basic support web page is now at http://gfix.dk/matlab-gnss-sdr-book/
- MATLAB code focused on the digital signal processing part
- in comparison with GNSS-SDR, it is somewhat dated, especially with respect to Galileo
- anyway, you can still find it in some experiments and you can use it as a basic MATLAB-based tutorial of the GPS L1 C/A service

GPS-SDR-SIM

GPS-SIM

Selected SDR Projects

GNSS-SDR

A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach

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

GPS-SIM

Selected SDR Projects

GNSS-SDR

A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach

GPS-SDR-SIM

GPS-SIM

- https://github.com/sywcxx/gps-sim
- certain variant is also here (if you read Chinese): https://code.csdn.net/sywcxx/gps-sim-hackrf
- **not to be confused with GPS-SDR-SIM!**
- MATLAB-based code that is, however, somehow half-way done
- anyway, it was successfully used in experiments of [Huang, Yang, 15]; they did not publish their extensions, however, namely their final signal generation and composition procedure `gensignal(…)`
- can be useful, if you enjoy reversing and extending MATLAB projects

Let’s go physical, now.

I am Bell. Deci Bell. (spelled decibel)

$$G_{dB} = 10\log\frac{P_{out}}{P_{in}}\ \text{dB} = 10\log\left(\frac{V_{out}}{V_{in}}\right)^2\ \text{dB} = 20\log\frac{V_{out}}{V_{in}}\ \text{dB}$$

gain

$$P_{dB} = 10\log\frac{P\ \text{W}}{1\ \text{W}}\ \text{dB (or dBW)} = 10\log\frac{P\ \text{W}}{10^{-3}\ \text{W}}\ \text{dBm}$$

total power

$$SNR_{dB} = 10\log\frac{P_{signal}}{P_{noise}}\text{dB} = 10\log SNR\ \text{dB} = (P_{signal,dB} - P_{noise,dB})\ \text{dB}$$

signal-to-noise ratio

$$F_{dB} = 10\log\frac{SNR_{in}}{SNR_{out}}\ \text{dB} = (SNR_{in,dB} - SNR_{out,dB})\ \text{dB}$$

noise figure

$$N_{0,dB} = 10\log\frac{N_0\ \text{WHz}^{-1}}{1\ \text{WHz}^{-1}}\ \text{dBW-Hz} = 10\log\frac{N_0\ \text{WHz}^{-1}}{10^{-3}\ \text{WHz}^{-1}}\ \text{dBm-Hz}$$

(noise) power spectral density

... then $N_{0,dB} + 10\log\frac{B\ \text{Hz}}{1\ \text{Hz}} = P_{noise}$ dB or dBm, respectively

Antenna Specials

We also employ the notion of gain for antenna performance comparison

Unless stated otherwise, the directions of maximum values of the antenna radiation intensities U_x (power radiated in a given direction per solid angle) are implied

In the gain ratio denominator, we use a reference antenna radiation intensity, so we can see on how well or bad would our antenna perform with respect to:

$$G_{dBi} = 10 \log \frac{U_{our\_antenna}}{U_{isotropic\_radiator}} \text{ dBi}$$

isotropic radiator

$$G_{dBic} = 10 \log \frac{U_{our\_antenna}}{U_{isotropic\_radiator\_circularly\_polarized}} \text{ dBic}$$

circularly polarized isotropic radiator

$$G_{dBd} = 10 \log \frac{U_{our\_antenna}}{U_{half-wave\_dipole}} \text{ dBd} = (G_{dBi} - 2.15) \text{ dBd}$$

half-wave dipole

Digital Signal Processing (DSP)

… uses the correspondence of continuous-time functions and discrete-time sequences to process the input signals by digital operations instead of analog circuits

… the sampling theorem described below is the cornerstone primitive that establishes the aforementioned relation

Software-Defined Radio (SDR)

… components that have been typically implemented in (analog) hardware are instead implemented by means of DSP software on a personal computer or an embedded system

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 fully reconstructed from its discrete-time samples as:

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

— Kotelnikov, Nyquist, Shannon, Whittaker

Complex or Real?

In general, $s(t)$ can be a complex-valued function of a real time value. We then have:

$$s(t) = x(t) + iy(t)$$

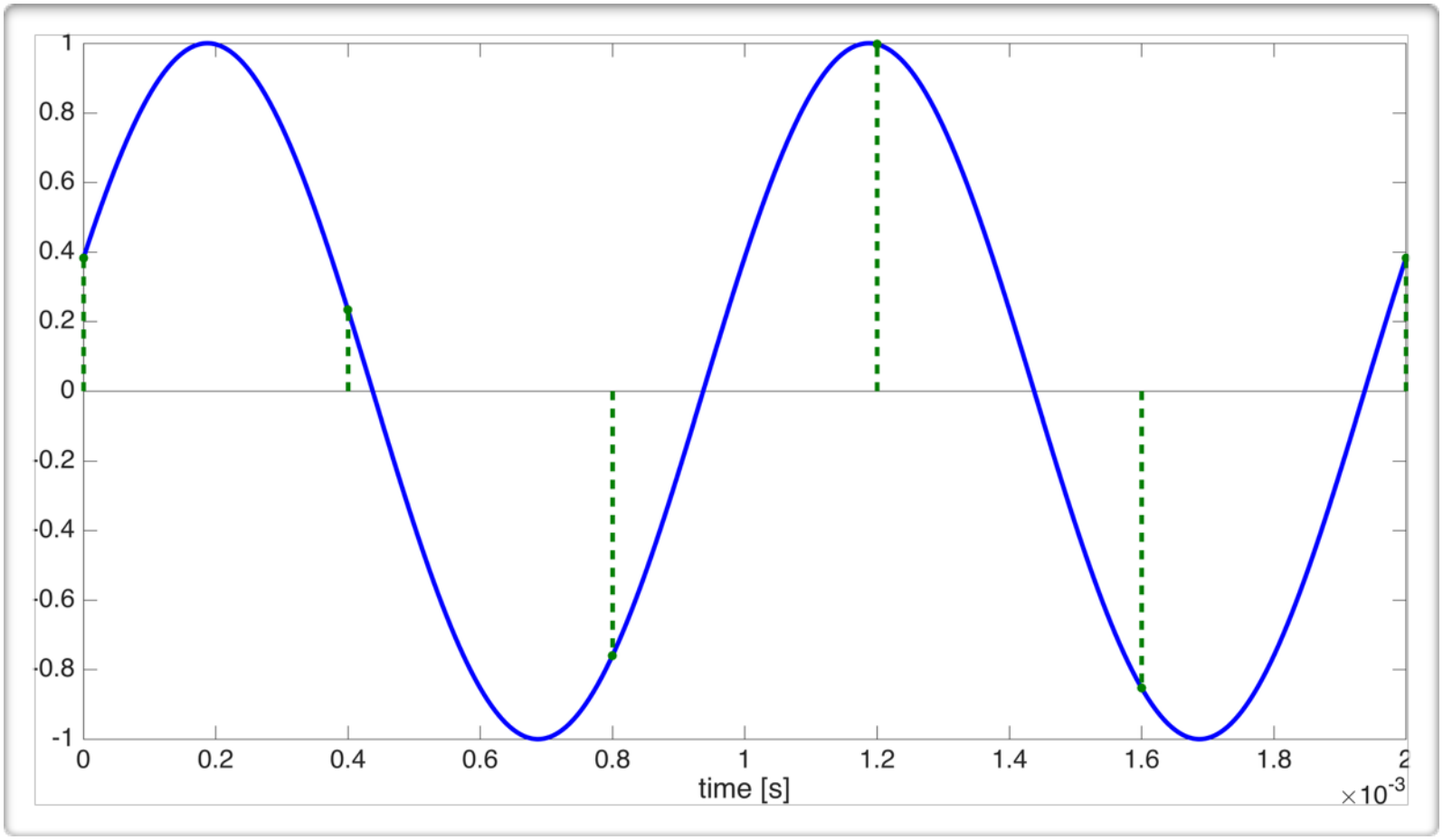
where $x(t)$ and $y(t)$ are real functions of the continuous time.

... also called in-phase (**I**) and quadrature (**Q**) components, respectively

... we need I/Q signal processing to describe the baseband envelope of a bandpass signal, since such a signal cannot be generally expected to have the Hermitian spectrum symmetry

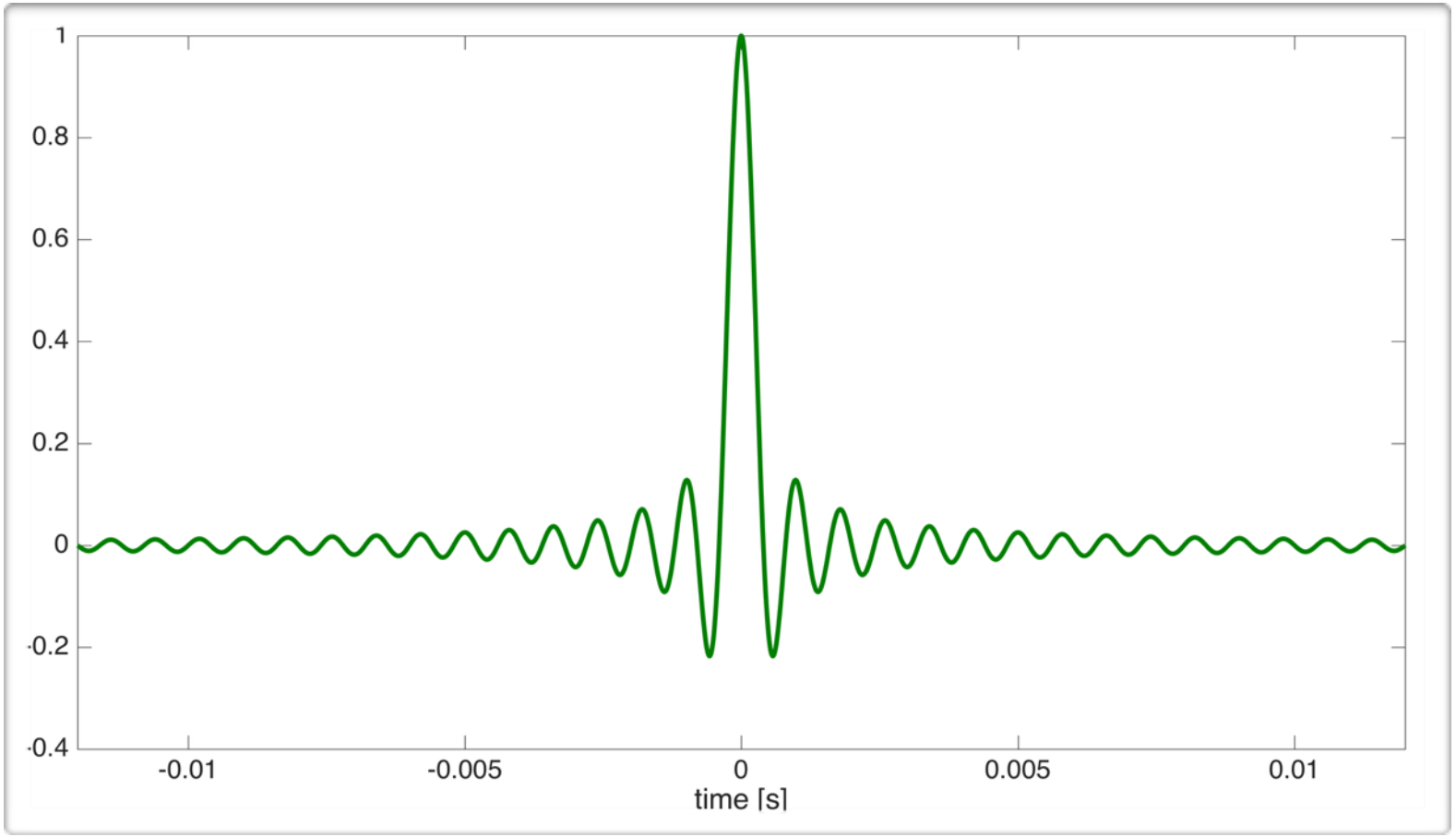
... by substituting this $s(t)$ into the sampling theorem equation, we see we can actually work with I/Q parts separately as with two components of the complex vector $s(t)$ on $\boldsymbol{C_R}$ space with its standard basis {1, **i**}

Real Signal Sampling



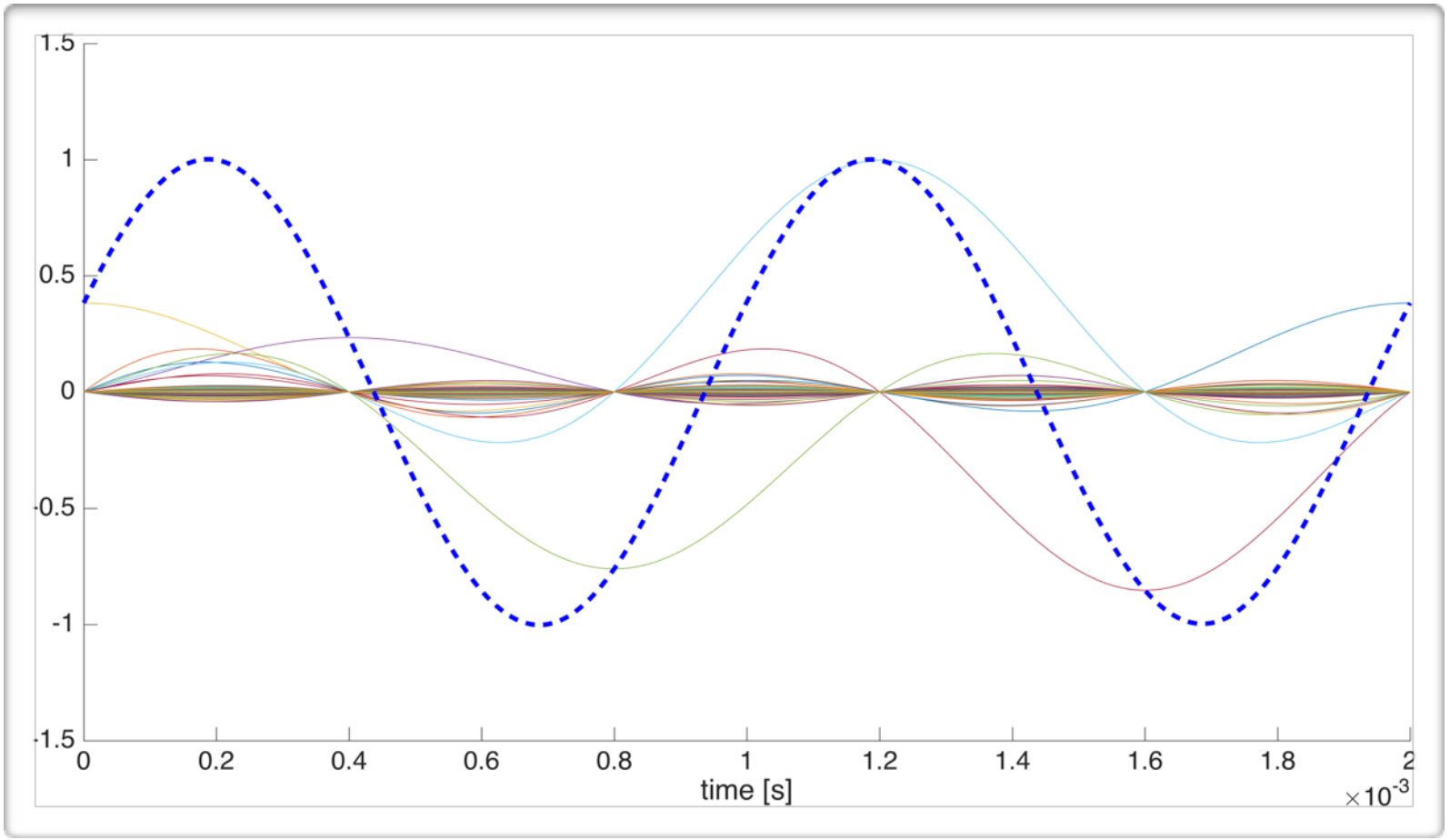
1 kHz harmonic signal sampled at f_s = 2.500 kHz

Sinus Cardinalis (sinc)



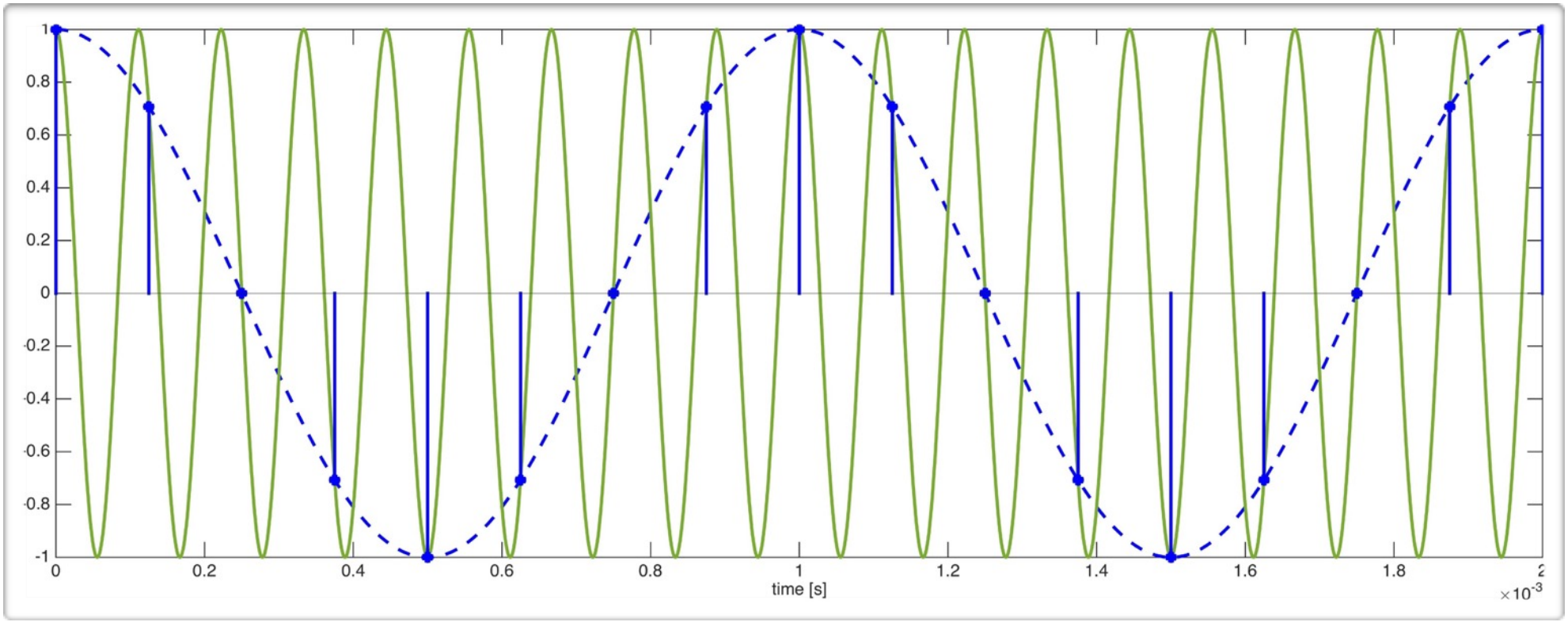
in lowpass filter impulse response time-scale for f_s = 2.500 kHz

Real Signal Reconstruction



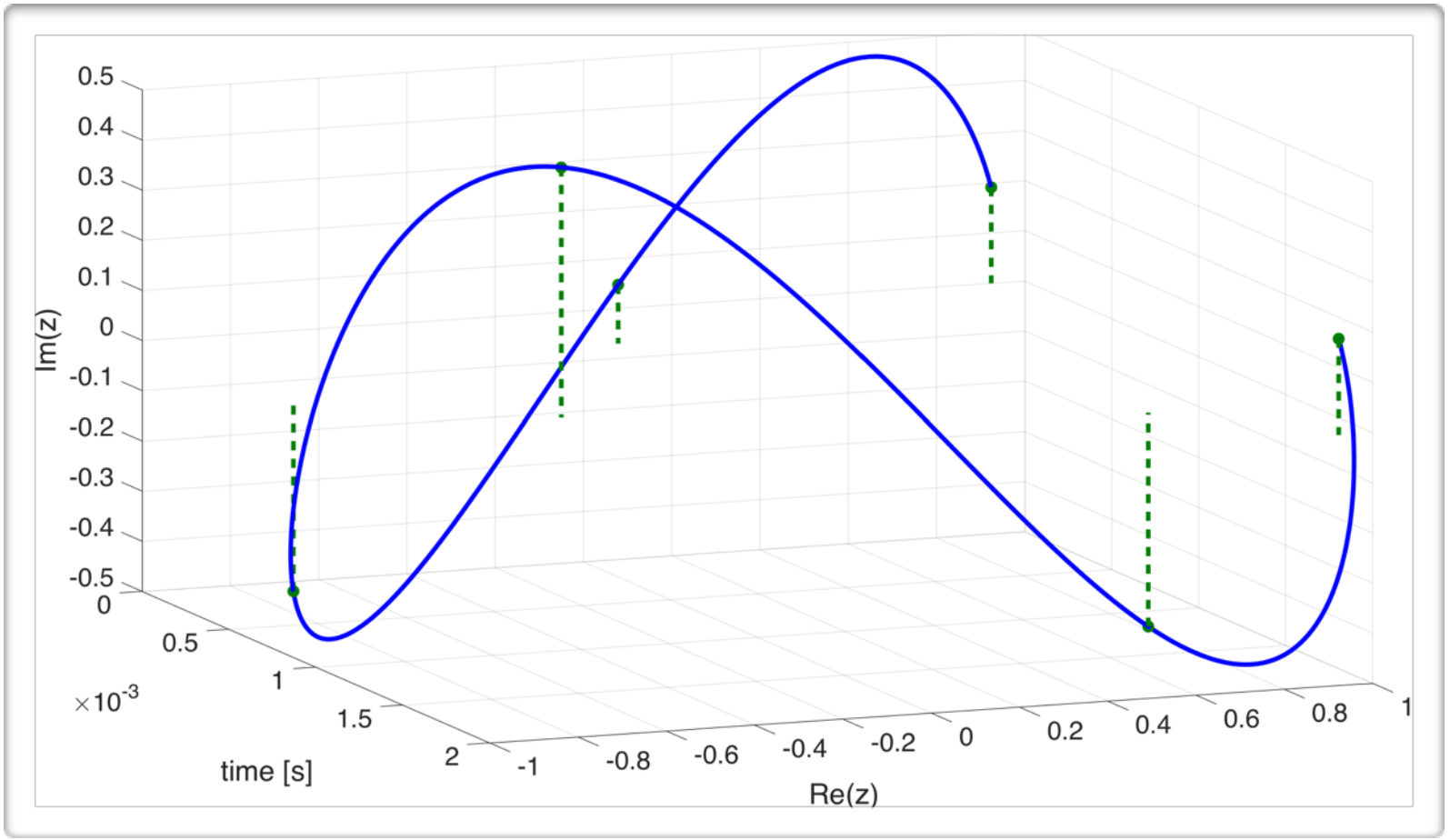
interpolation by shifted and scaled replicas of sinc at f_s = 2.500 kHz time-scale with finite 30-sample delay

Aliasing Example



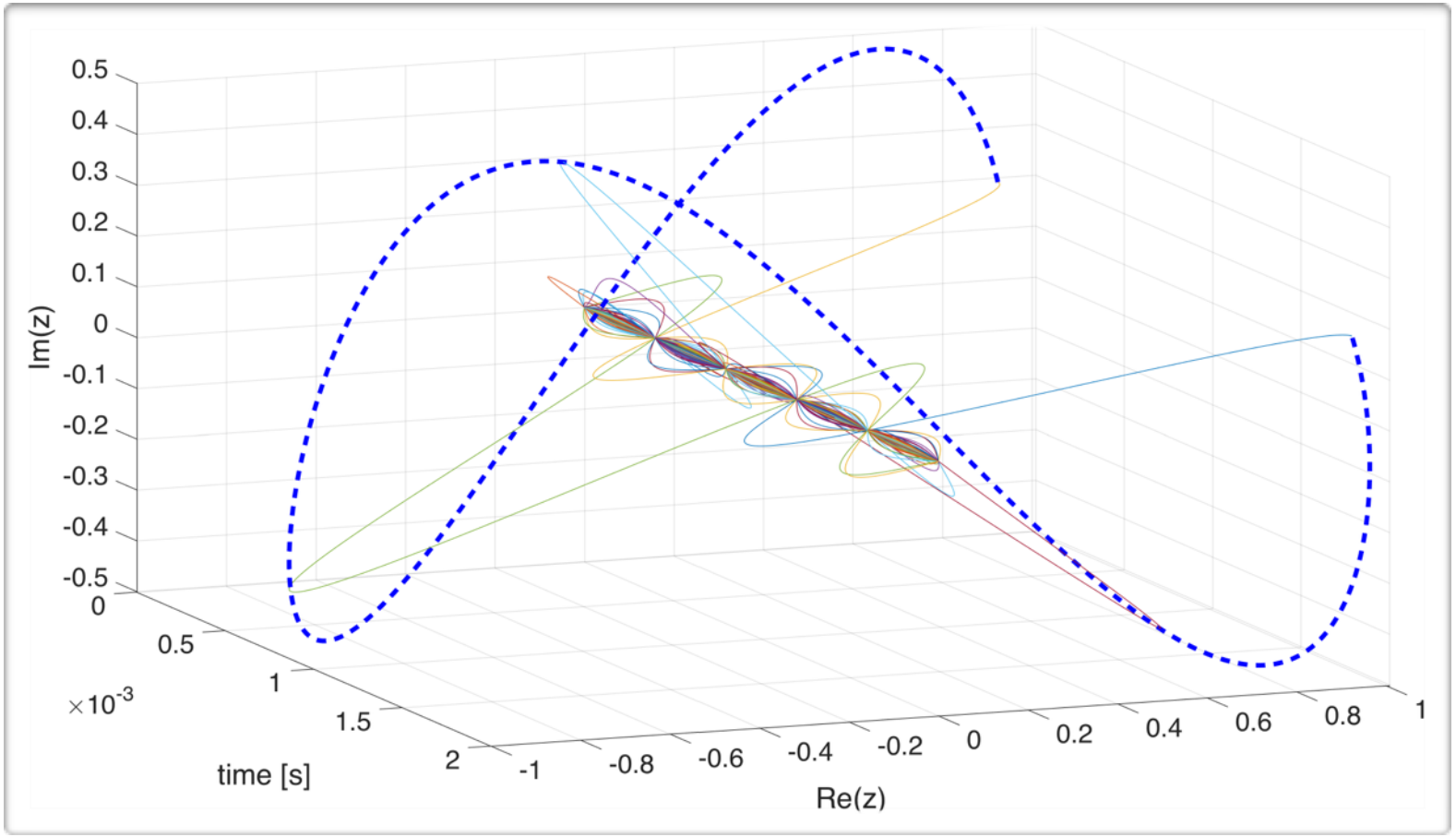
9 kHz -> 1 kHz @ sample rate f_s = 8 kHz

Complex Signal Sampling



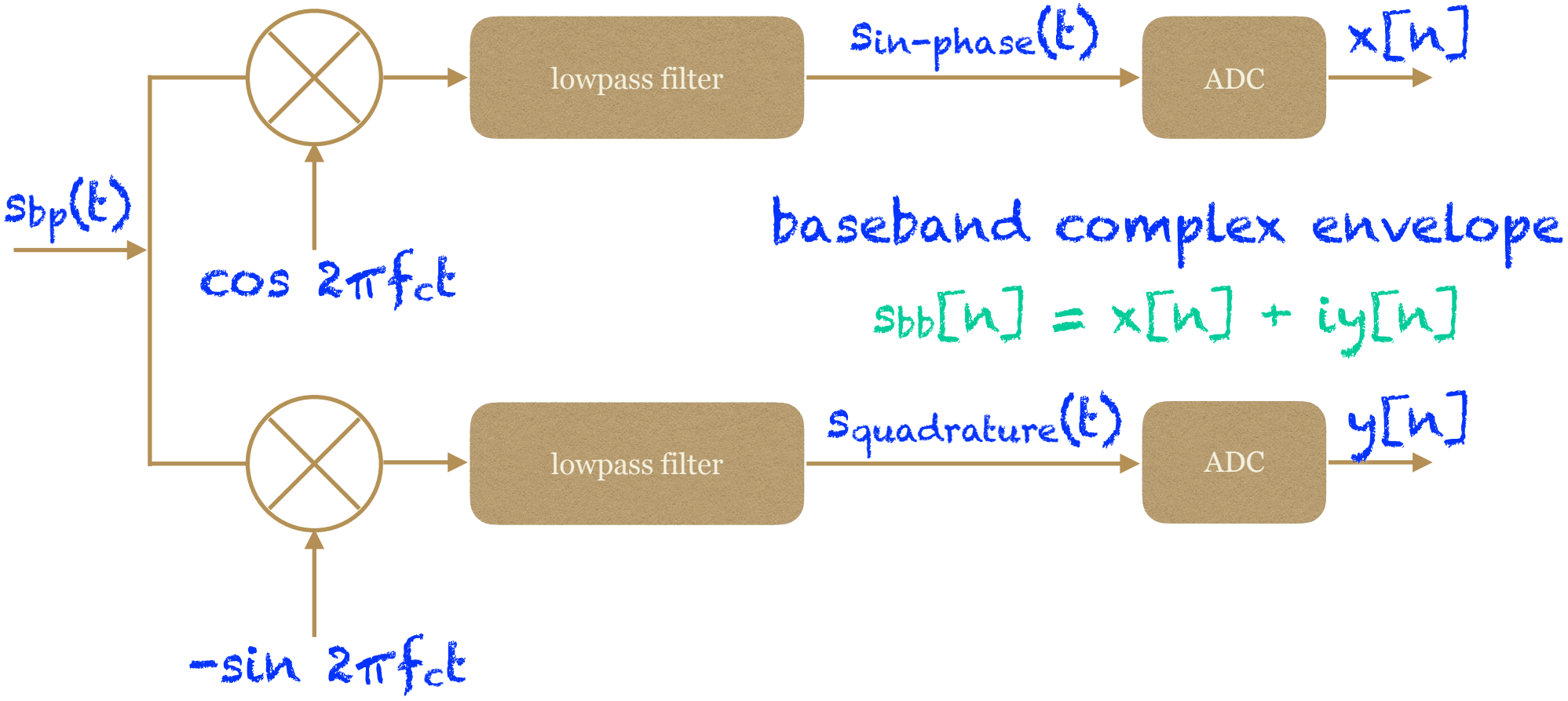
complex signal sampled at f_s = 2.500 kHz

Complex Signal Reconstruction



real and imaginary vector components interpolation
at f_s = 2.500 kHz with finite 30-sample delay

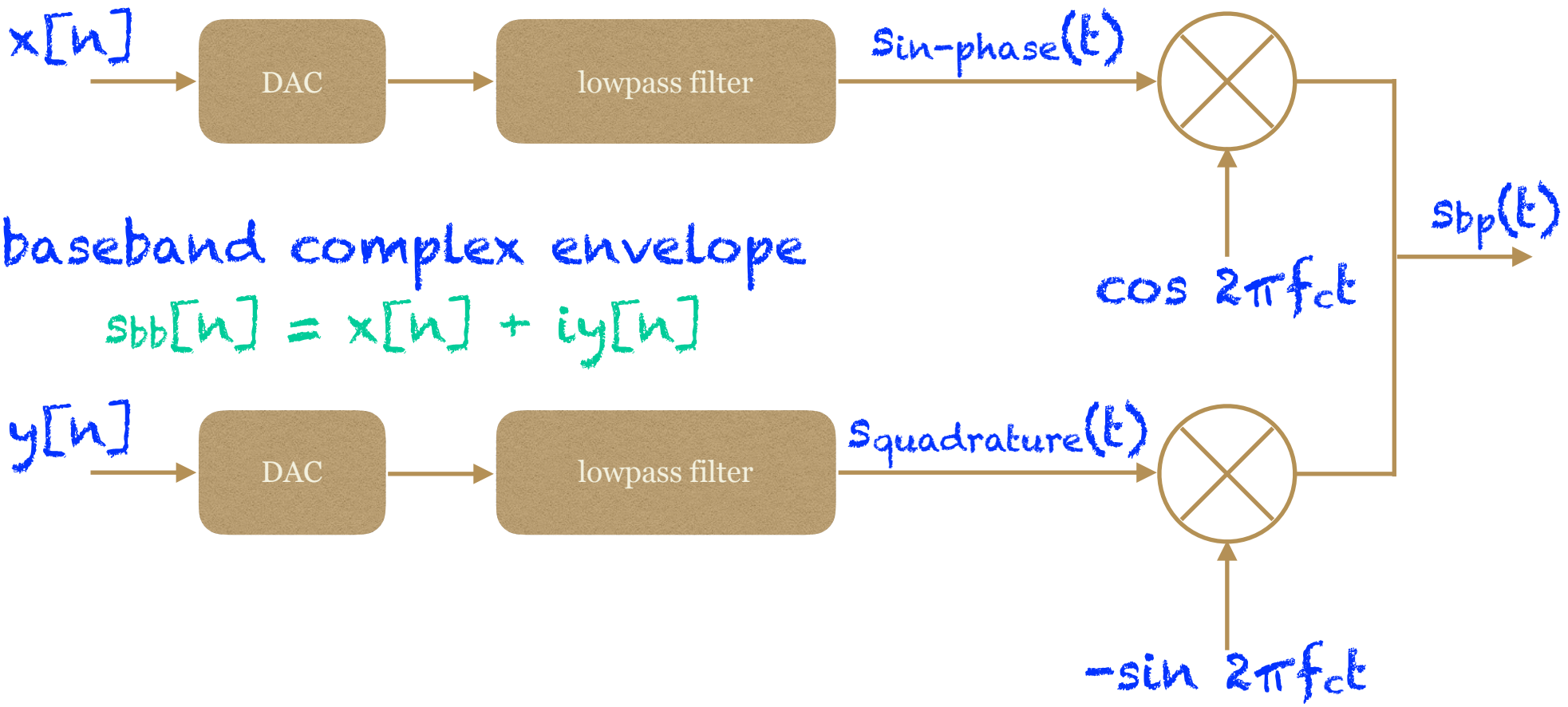
Bandpass Signal Quadrature (Complex) Sampling



bandpass signal complex downconversion ($f_c \rightarrow 0$ Hz)
and sampling at $f_s > B$

cf. [Lyons, 2011] for an excellent, accessible explanation

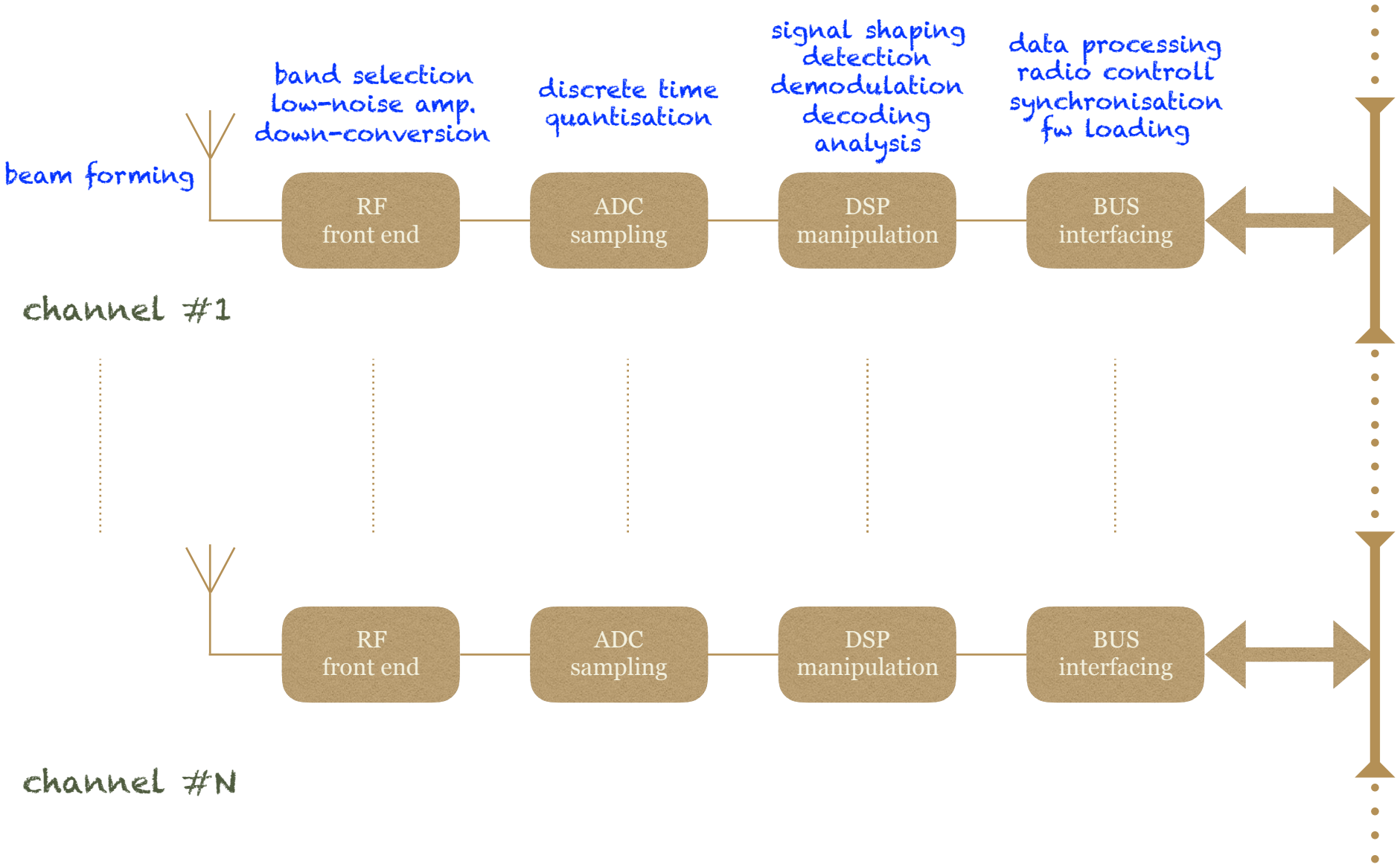
Bandpass Signal Reconstruction (Quadrature Modulation)



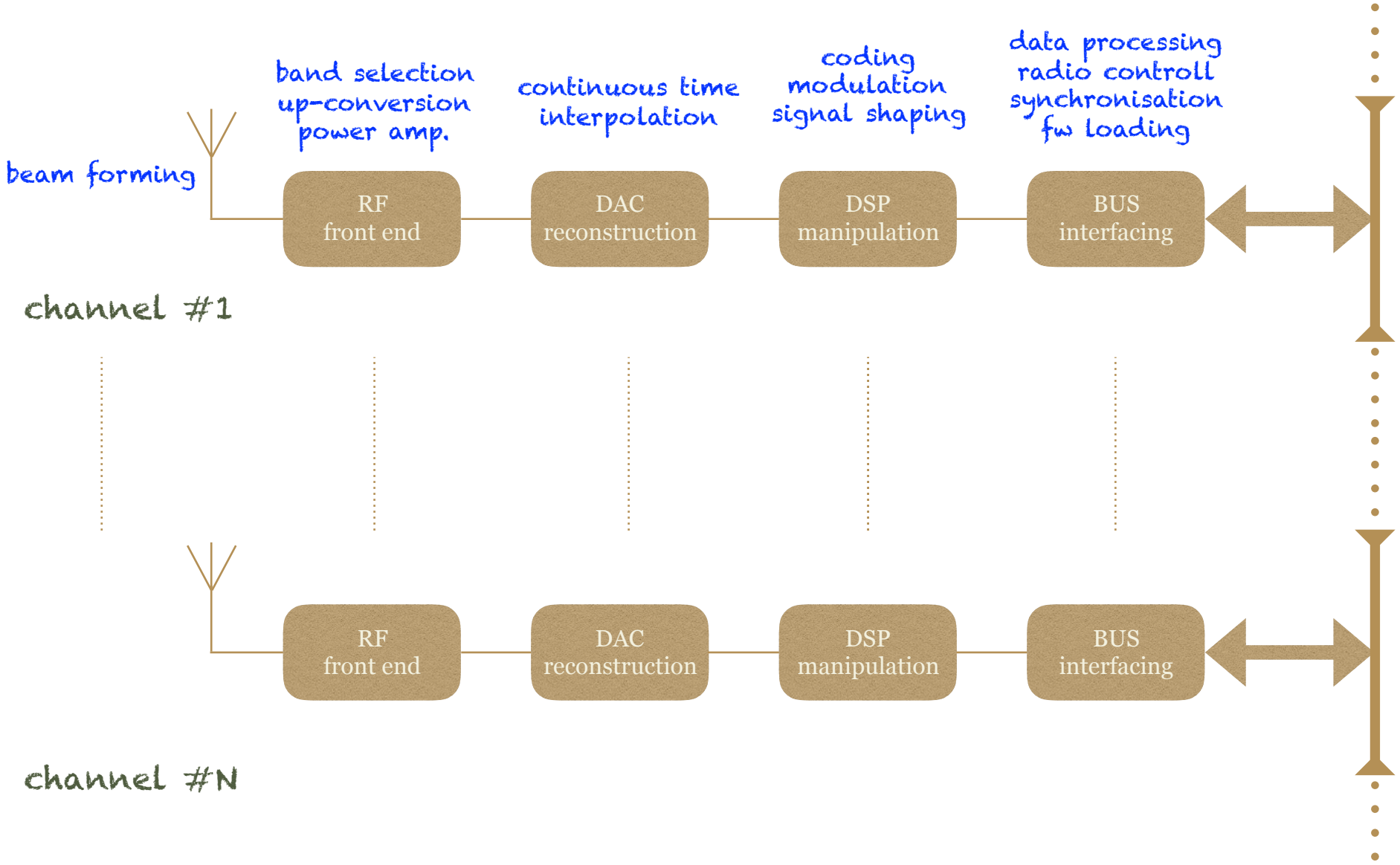
bandpass signal envelope reconstruction from I/Q samples at $f_s > B$ and upconversion to f_c

cf. [Lyons, 11] for an excellent, accessible explanation, [Johnson, Jr. et al., 11] for SDR context, [Holmes, 07] for GNSS applications

SDR Concept - RX Path



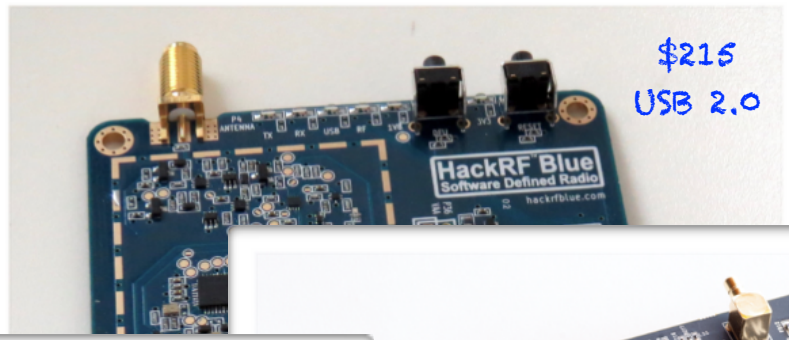
SDR Concept - TX Path



Popular Hacking SDRs

about $20 (NooElec)
RX only

$215
USB 2.0



bladeRF $420 - 1500
USB 3.0

> $1717
1 GigE

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.

RF Front-End Analysis

Due to the physical properties of GNSS satellite signals, it is crucial to understand the role of noise in RF processing circuits

- recall, until after the de-spreading operation, the GNSS signal is hidden below the usual noise floor
- in the front-end, we are therefore focused on processing noise-like signals all the time
- so, we will treat the noise analysis in a higher detail here
- we are going to design our own front-end to be used in chain with the internal front-end (daughterboard) of the particular SDR (e.g. USRP N210 + UBX-40)

Further Relevant Parameters

Besides the basic noise analysis, you may also want to check:

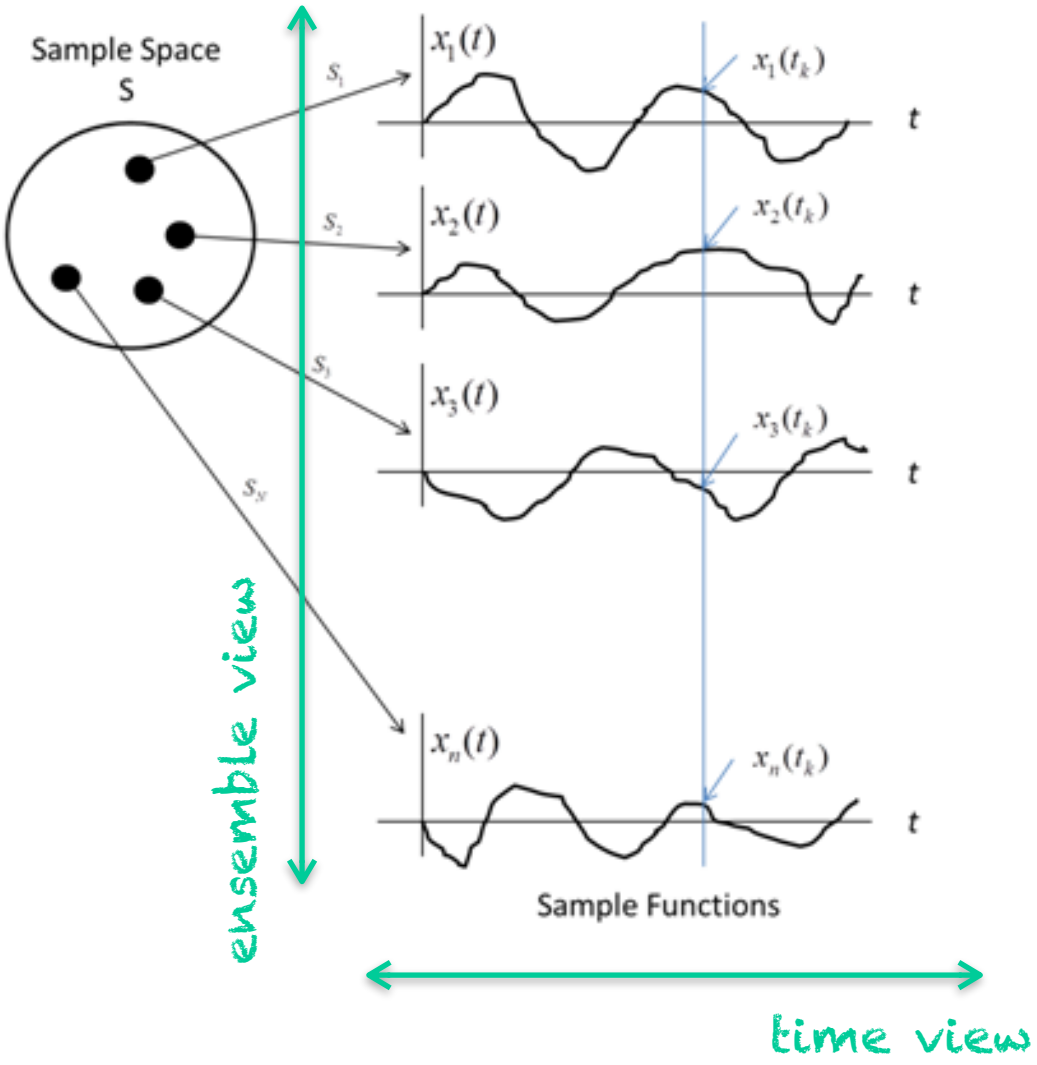
- nonlinear signal distortion, namely the Input Third Intercept Point (IIP3), cf. [Razavi, 12], [Betz, 16], [Nurmi et al., 15], [Samper et al., 09]

  ... this will affect your components selection and limit the gain of their preceding RF stages from above to avoid undesirable interference

- ADC quantization noise and dynamic range, cf. [Betz, 16], [Misra, Enge, 12]

  ... with a well-designed RF front-end, 4 bits of A/D output should be more than enough

Noise in Electronic Circuits



In general, we model such a signal as a realisation of a continuous- (or discrete-) time random process.

That means, we observe successive measurements or projections of a randomly chosen internal state of the system (*time view*).

For a given time instant t_k, $X(t_k)$ is a random variable (*ensemble view*).

We call the process e.g. Gaussian, if $X(t_k)$ has such distribution.

We shall be very careful with mixing time and ensemble views (cf. ergodic process properties).

[van Etten, 05]

Noise Power

We assume a white noise (but not necessarily Gaussian one) signal across the sensed part of the RF band.

Furthermore, we assume an ideal impedance matching in between our circuit components.

That says our noise has a flat *power spectral density* equal to $N_0/2$.

For a real bandpass signal of bandwidth B, we then have the total expected noise power $\boldsymbol{P_{noise} = BN_0}$.

...since the complex power spectrum is symmetric about the frequency origin for a real signal

Something is Missing? N_0, of Course

We define

$$N_0 = kT_{noise} \quad [\mathrm{WHz}^{-1}; \mathrm{JK}^{-1}, \mathrm{K}]$$

where k is Boltzmann constant (1.38 x 10^{-23} J/K) and T_{noise} is the *equivalent noise temperature*.

T_{noise} may (and may not!) correspond to the absolute temperature of the circuit element, see next slides.

The notion of equivalent temperature is introduced to unify the approach to the noise analysis in electronic systems.

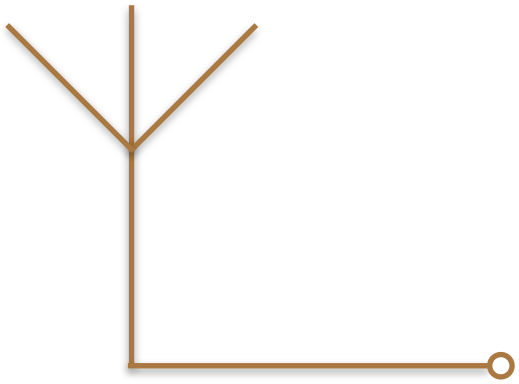
Antenna Temperature

It is an equivalent value, mainly describing the noise power captured by the antenna effective aperture from the sky and partially also from the terrestrial background.

... contains black-bodies radiation sensed via the antenna radiation resistance

... physical temperature of the antenna construction can be neglected, depending on the antenna efficiency (radiation vs. loss resistance)

... in the GNSS user band we can typically assume **T_{ant} = 130 K** [Betz, 16]



$$T_{ant} = 130 \text{ K}$$

$$N_0 = kT_{ant} = 1.794 \times 10^{-21} \text{ WHz}^{-1} = 1.794 \text{ zWHz}^{-1}$$

$$N_{0,dB} = 10 \log \frac{N_0}{10^{-3} \text{ W}} \text{ dBm-Hz} = -177.462 \text{ dBm-Hz}$$

2-Port Equivalent Temperature

In the following, we show how to compute the equivalent noise temperature for passive attenuators and active amplifiers.

... herewith covering all the components we are going to use

Note the equivalent noise temperature T_e here is to be **added to the input, while assuming the rest of the 2-port noiseless.**

... this allows an easy combination with source noise

... leads to Friis formula for cascaded circuits

In Particular

Let T_s be the source noise temperature, T_e the equiv. noise temperature of the device input port, and G its gain.

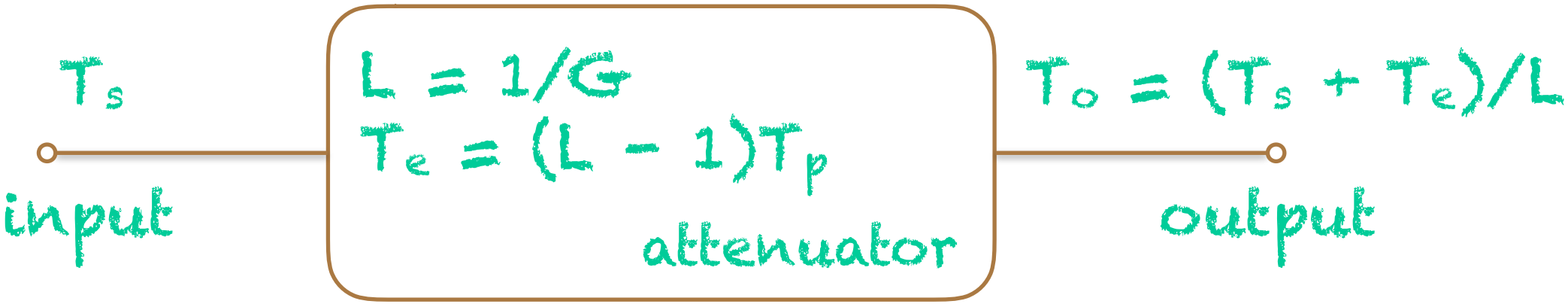
... we will talk about equivalent temperatures, unless stated otherwise

$$N_0 = kT_o = kG(T_s + T_e)$$

Passive Attenuator / Filter / Cable

Its noise temperature directly reflects the physical temperature T_p of the circuit element.

- ... we just need to transform T_p to T_e
- ... we usually use the loss $L = 1/G$ instead of G directly
- ... we shall use direct(!) value of L and G, not in dB



$$N_0 = kT_o = kG(T_s + T_e) = k\frac{(T_s + T_e)}{L} = kT_p + k\frac{(T_s - T_p)}{L}$$

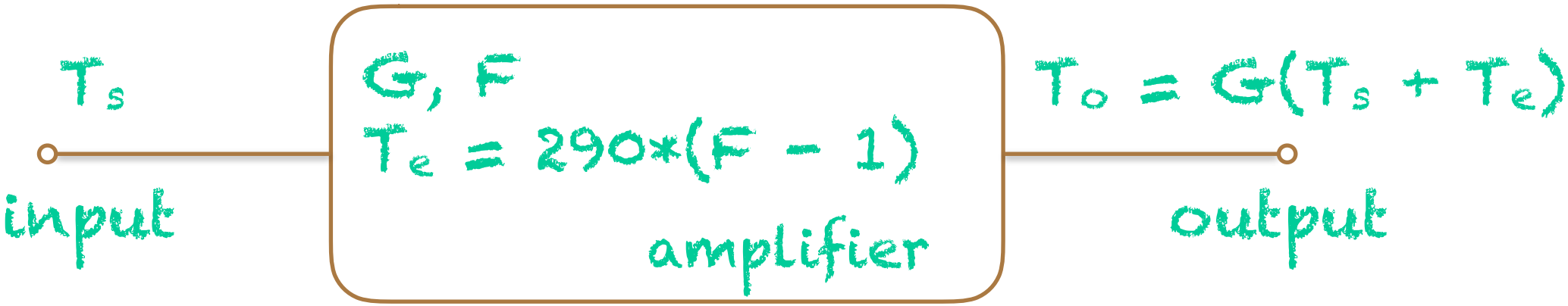
[van Etten, 05, example 6.3]

Active Amplifier

Its equivalent noise temperature is computed from noise figure *F*.

... data-sheet-given proportionality factor with respect to 290 K

... we shall use direct(!) value of *F*, not in dB (usually stated)

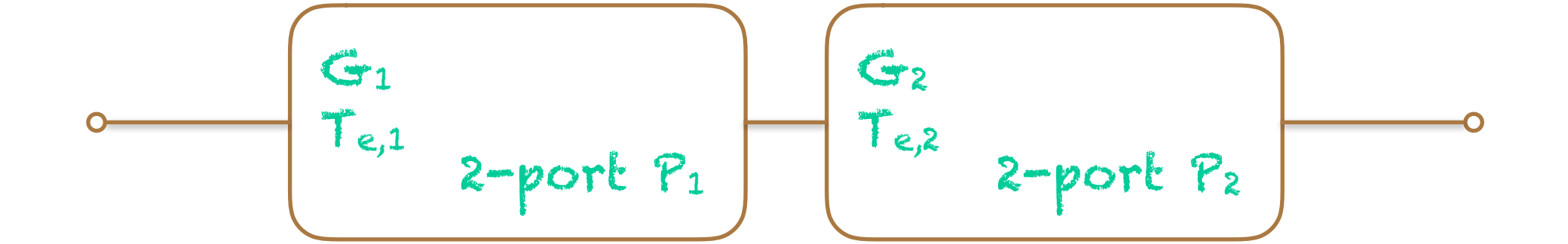


$$N_0 = kT_o = kG(T_s + T_e) = kG(T_s + 290 \times (F - 1))$$

Friis Formula For Noise

Allows computation of total T_e for two chained 2-port components.

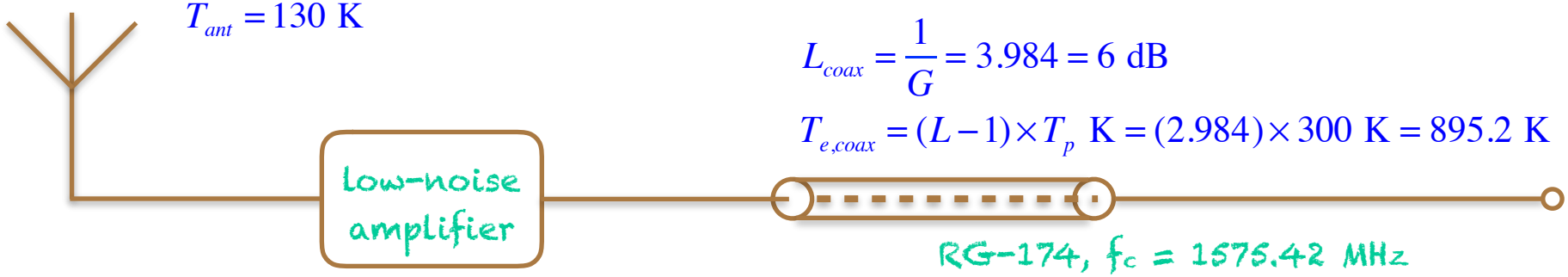
... can be applied recursively to the whole network



$$G = G_1 G_2 , T_e = T_{e,1} + \frac{T_{e,2}}{G_1}$$

$$N_0 = kT_o = kG(T_s + T_e)$$

Antenna-LNA-Coax Example



$T_{ant} = 130$ K

$G_{coax} = -6$ dB $= 0.251$

$L_{coax} = \frac{1}{G} = 3.984 = 6$ dB

$T_{e,coax} = (L-1) \times T_p$ K $= (2.984) \times 300$ K $= 895.2$ K

$G_{LNA} = 27$ dB $= 501.187$

$F_{LNA} = 1.8$ dB $= 1.514$

$T_{e,LNA} = (F-1) \times 290$ K $= (0.514) \times 290$ K $= 149.06$ K

$$G = G_{LNA} G_{coax} = (27-6) \text{ dB} = 21 \text{ dB} = 125.893$$

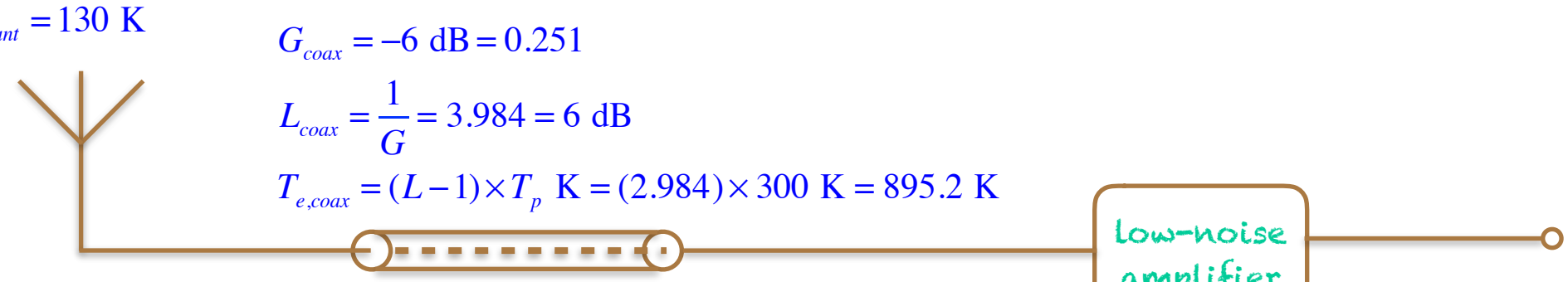
$$T_e = T_{e,LNA} + \frac{T_{e,coax}}{G_{LNA}} = (149.06 + \frac{895.2}{501.187}) \text{ K} = 150{,}846 \text{ K}$$

$$T_i = T_{ant} + T_e = 280.846 \text{ K}$$

$$N_0 = kGT_i = 1.38 \times 10^{-23} \times 125.893 \times 280.846 \text{ WHz}^{-1} = 487.92 \times 10^{-21} \text{ WHz}^{-1} = 487.92 \text{ zWHz}^{-1}$$

$$= -153.117 \text{ dBm-Hz}$$

Antenna-Coax-LNA Example



$$G = G_{coax} G_{LNA} = (-6 + 27)\ \text{dB} = 21\ \text{dB} = 125.893$$

$$T_e = T_{e,coax} + \frac{T_{e,LNA}}{G_{coax}} = (895.2 + \frac{149.06}{0.251})\ \text{K} = 1489.065\ \text{K}$$

$$T_i = T_{ant} + T_e = 1619.065\ \text{K}$$

$$N_0 = kGT_i = 1.38 \times 10^{-23} \times 125.893 \times 1619.065\ \text{WHz}^{-1} = 2.813 \times 10^{-18}\ \text{WHz}^{-1} = 2.813\ \text{aWHz}^{-1}$$

$$= -145.508\ \text{dBm-Hz}$$

Lesson Learnt

Despite having the same total gain (21 dB), the *antenna-LNA-coax* arrangement results in lower total equivalent noise temperature leading to a considerably lower system noise.

As a rule, we shall put the first LNA as close to the antenna as possible to “cover” the noise of the rest of the radio circuits.

... this is also known as the active antenna concept

... especially, we shall use the active antenna in our GNSS receivers whenever possible, even though we employ RF front-ends with a reasonably high gain in themselves

... this usually calls for a bias-T component to empower the active antenna LNA, but this is just a negligible issue

Noise Factor Analysis

In RF electronics, the noise analysis is sometimes almost solely based on working with noise factors F_i of the respective components, instead of their noise temperatures.

When done properly, these two approaches are physically equivalent.

Despite looking simple, the *F*-based approach is full of pitfalls, so we stay with the more robust *T*-based approach here.

... nice elaboration of *F*-based approach in GNSS, including its traps, is given in [Misra, Enge, 12]

OK, what gain is enough?

To minimise the digital word length (≤ 4 bits can be enough), the source signal inside our SDR should swing over the whole ADC input range.

However, because of the L1 C/A power spectrum, we shall **use the expected noise power instead** of the original signal for this estimation.

... like if the noise was all that we want

... we should leave some margin for a possible interference

... also note the noise power is related to a random variable variance, so it is not a direct signal level value

Do not forget to incorporate the gain of your internal SDR front-end (i.e. the daughterboard of USRP, for example).

Example

Let us assume the maximum ADC input level is ±100 mV, corresponding to -10 dBm at 50 ohm input load (for a harmonic signal).

Let the total expected input noise power from the viewpoint of the first LNA embedded in the active antenna (based on aforementioned T_s + T_e concept) be -174.1 dBm-Hz, filtered to 2.046 MHz bandwidth

... this corresponds to the first null-to-null bandwidth of L1 C/A

... it may be uneasy to get such a filter, but let it be for this example

... we get -174.1 + 10 x 6 x Log(2.046) dBm = -174.1 + 63.1 dBm = -111 dBm

The first approximation for the gain is then: 111 - 10 - 3 dB = 98 dB, where the -3 dB is for a safety margin.

... however, Friis formula shows T_e already depends on the gain distribution, so this is in principle an iterative process: guess a scheme and check T_e corresponds with gain

... it is a good idea to leave the final 15 to 30 dB of our gain configurable (for instance, via the internal SDR daughterboard parameters)

... in this example, do not also forget to include the active antenna LNA into the total front-end gain computation

Too High Gain?

Comparing the theoretical gain estimated here, we can see it is somewhat higher than the values used in recent hacking experiments (cf. e.g. [Huang, Yang, 15]).

Well, in general, it is a question of:

- the digital word length used in those experiments, as the ADC bit range can compensate for a weak RF front-end
- the filters bandwidth used in the RF front-end (if any), as a higher bandwidth means higher noise and so a lower gain allowed
- interferences and RF front-end nonlinearities that may have limited the particular experimental setups

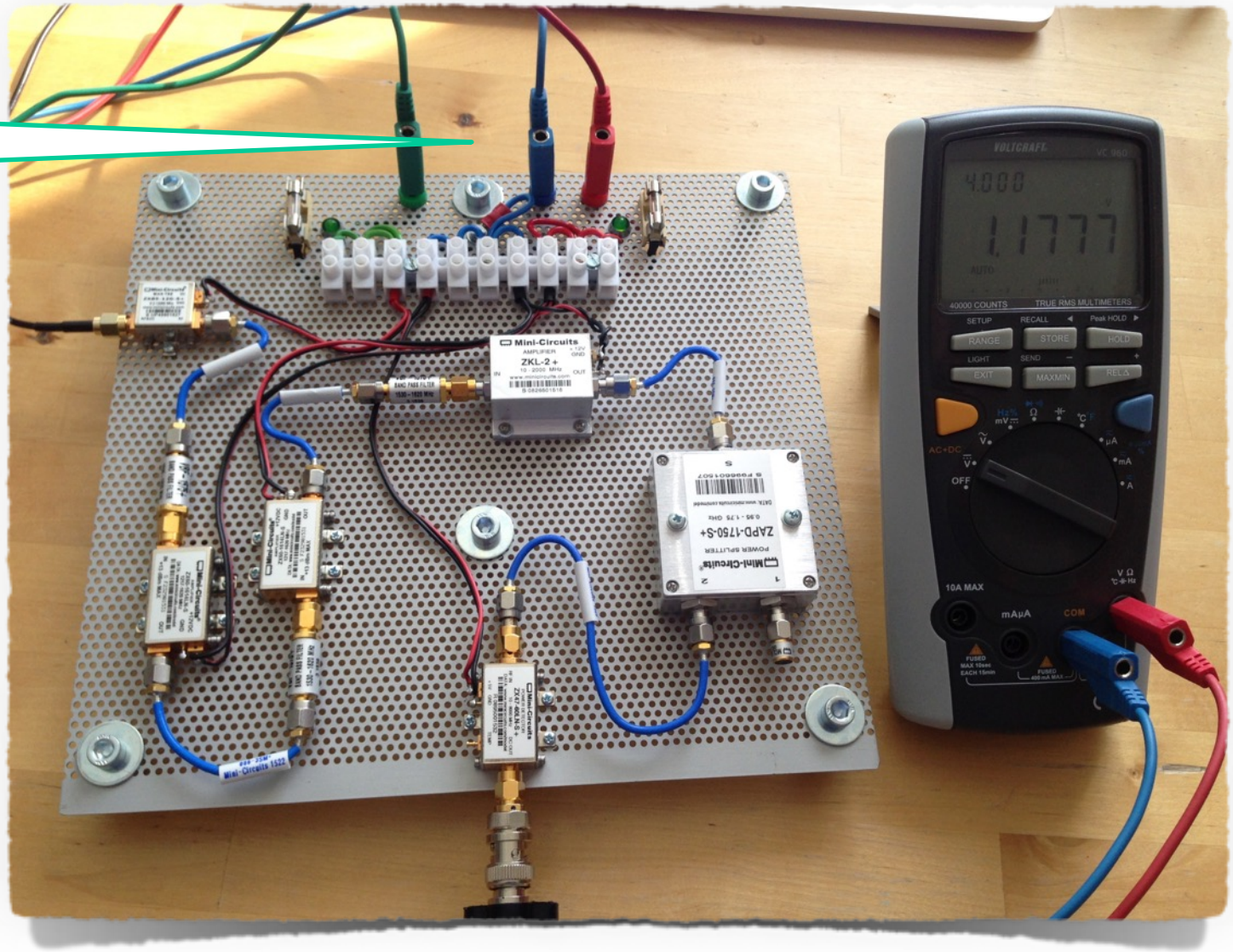
Anyway, this simple theory is just a first approximation for your initial guidance. There is usually a place left for some practical fine-tuning.

RF Front-End Commented Example

5 V and 12 V DC power connection

5 V is required for the active antenna and the RSSI detector (cf. below).

The rest of the circuit uses 12 V.



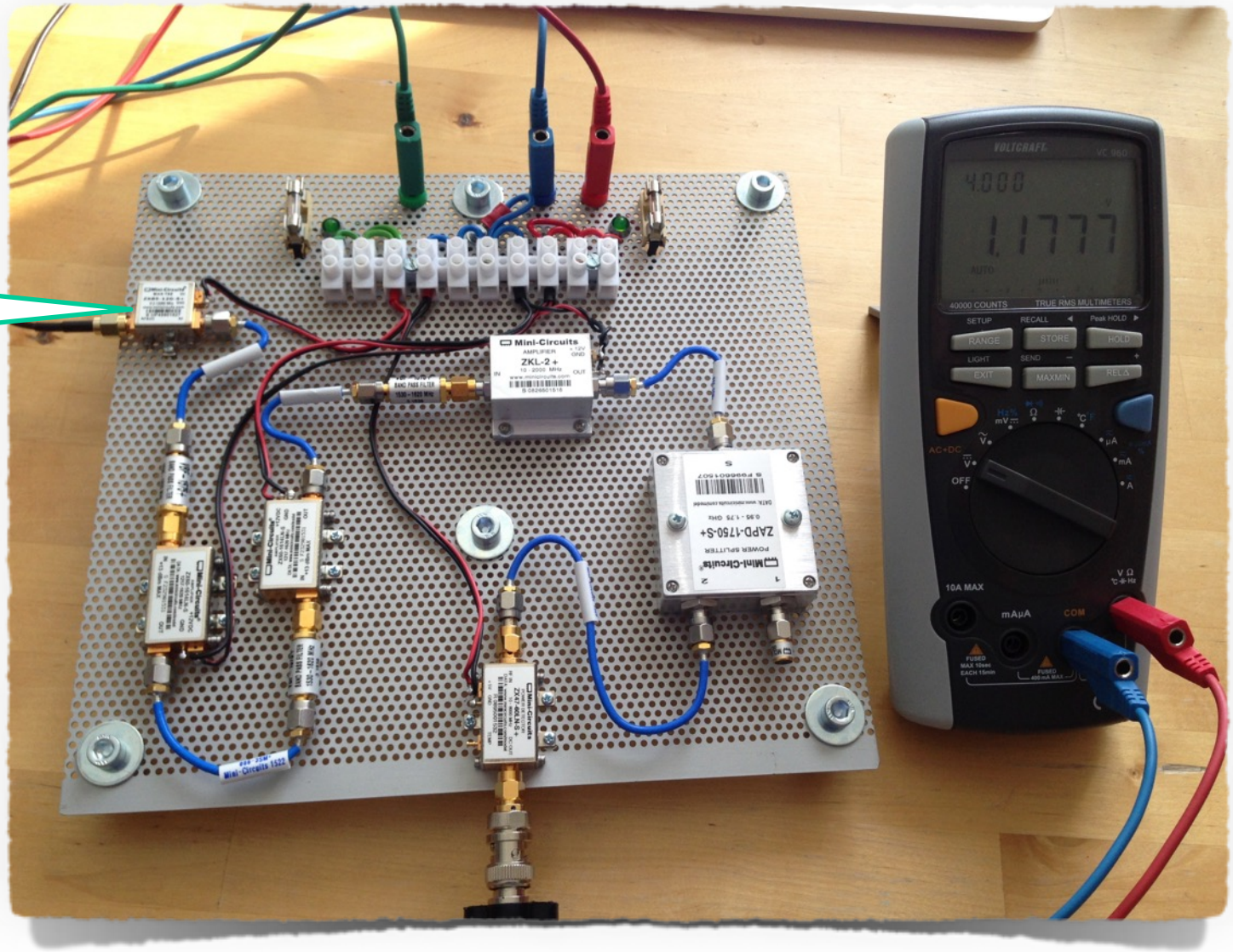
RF Front-End Commented Example

ZX85-12G-S+, bias-tee for empowering the LNA in the active antenna
Ins. loss: 0.6 dB (typ)

Antenna:
1575±3 MHz,
10 MHz BW, RHCP,
4 dBic peak gain,
VSWR max. 1.2

Ant-LNA: G = 27 dB (typ), F = 1.8dB

Cable: 2 m of RG-174

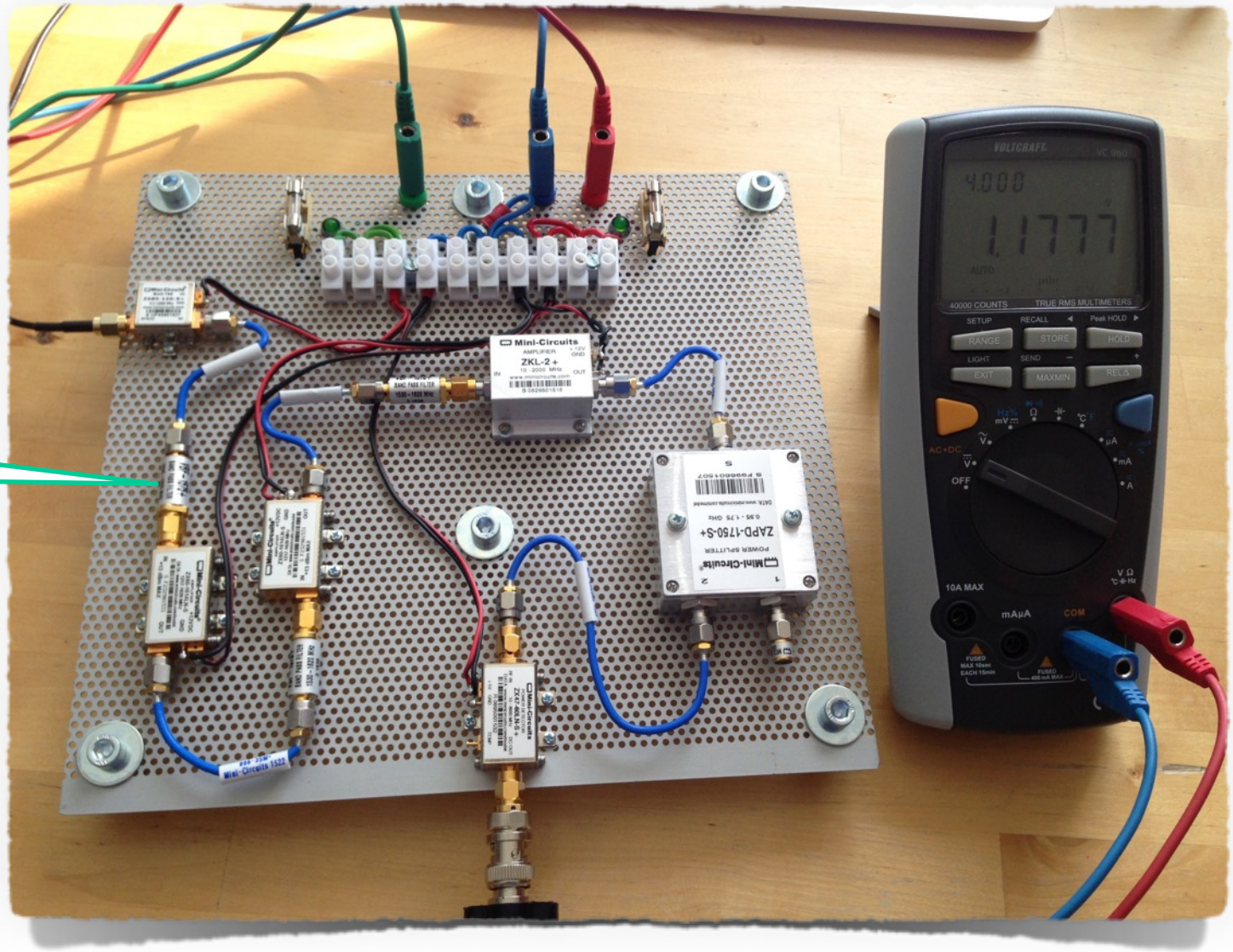


RF Front-End Commented Example

VBF-1575+,
bandpass filter

Passband: 1530 to 1620 MHz, center 1575 MHz.

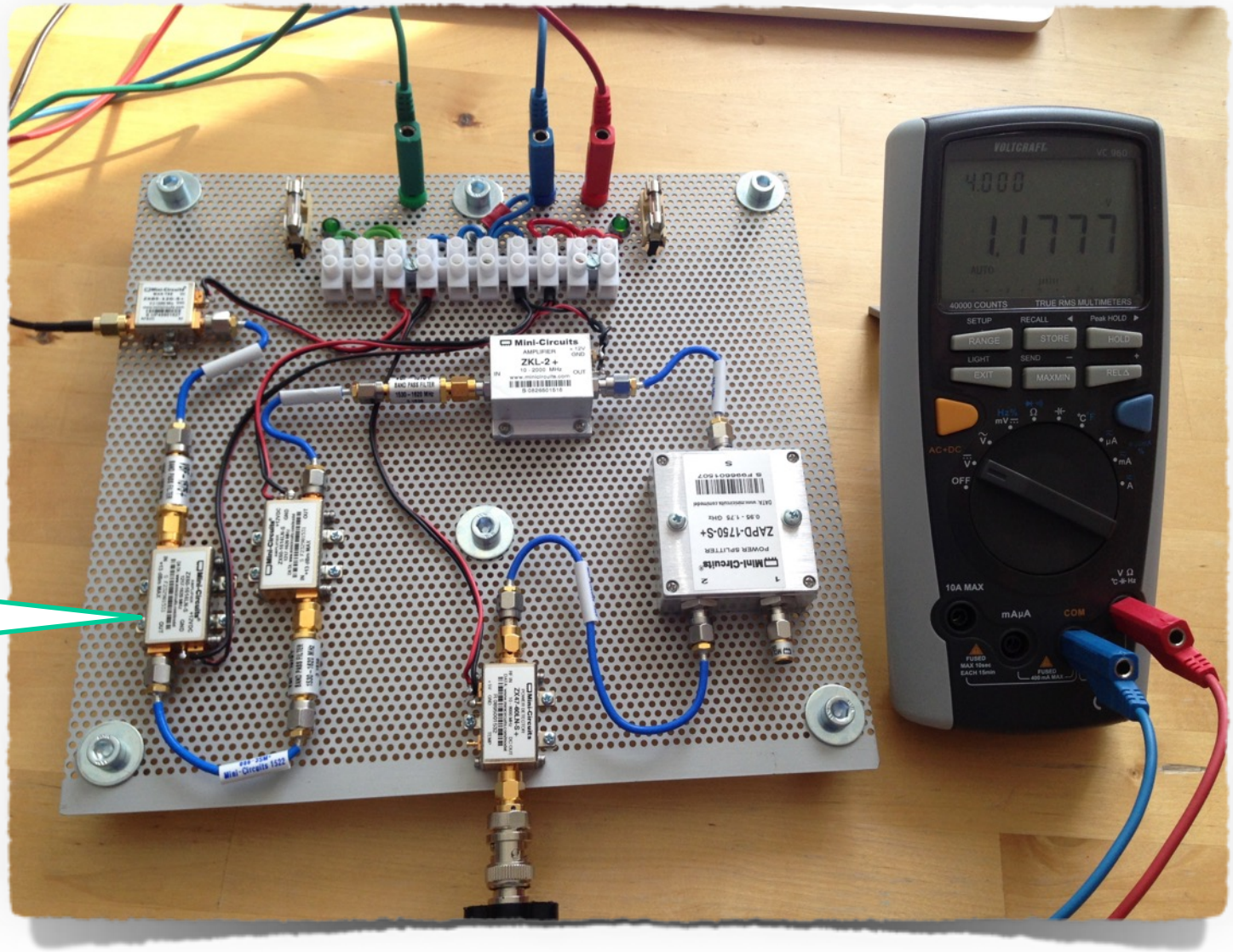
Ins. loss: 3 dB (max)



RF Front-End Commented Example

ZX60-1614LN-S, ultra low noise amplifier

G = 14 dB (typ)
F = 0.5 dB (typ)
IP3 = 30 dBm (typ)
BW: 1217 to 1620 MHz

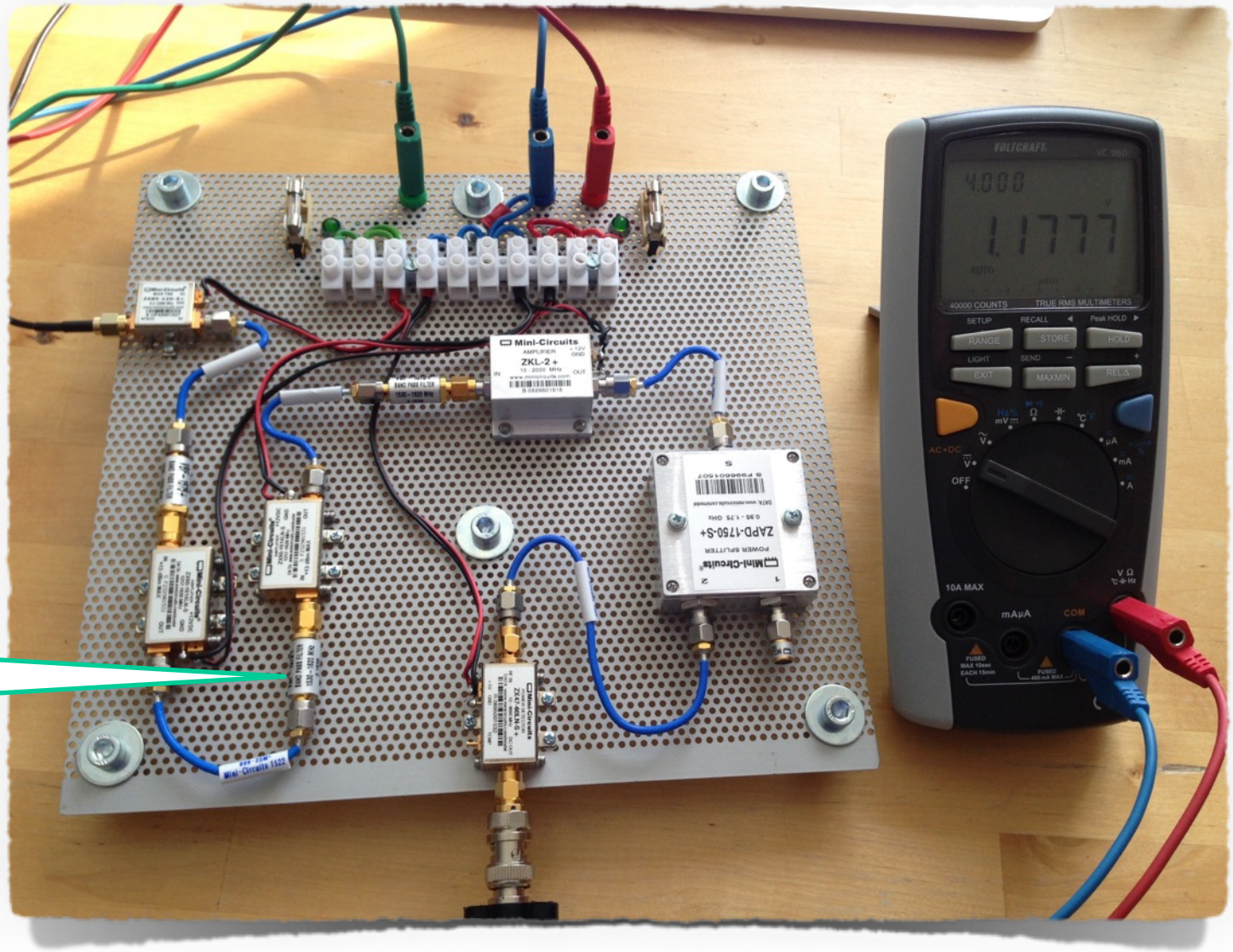


RF Front-End Commented Example

VBF-1575+,
bandpass filter

Passband: 1530 to 1620 MHz, center 1575 MHz

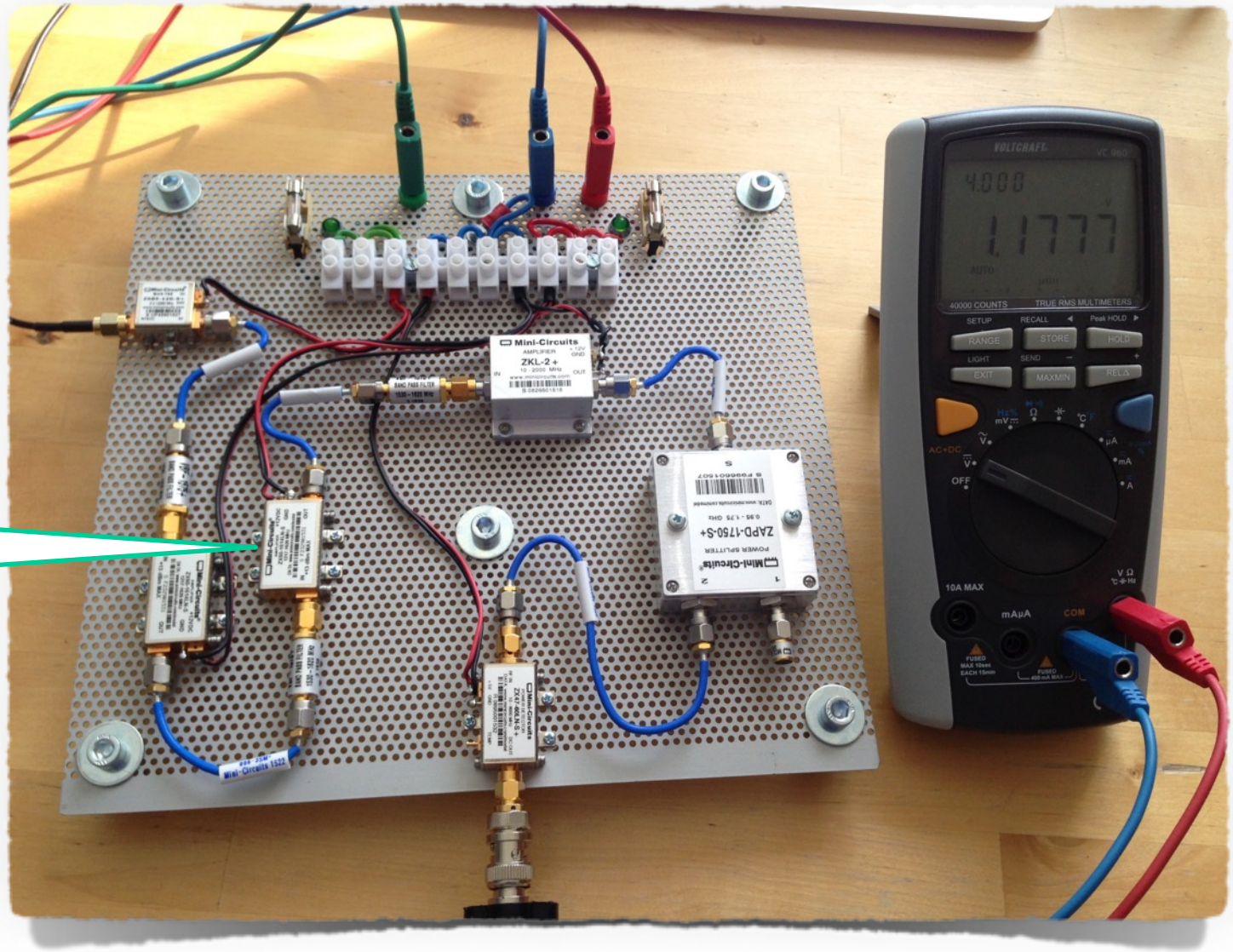
Ins. loss: 3 dB (max)



RF Front-End Commented Example

ZX60-1614LN-S, ultra low noise amplifier

G = 14 dB (typ)
F = 0.5 dB (typ)
IP3 = 30 dBm (typ)
BW: 1217 to 1620 MHz

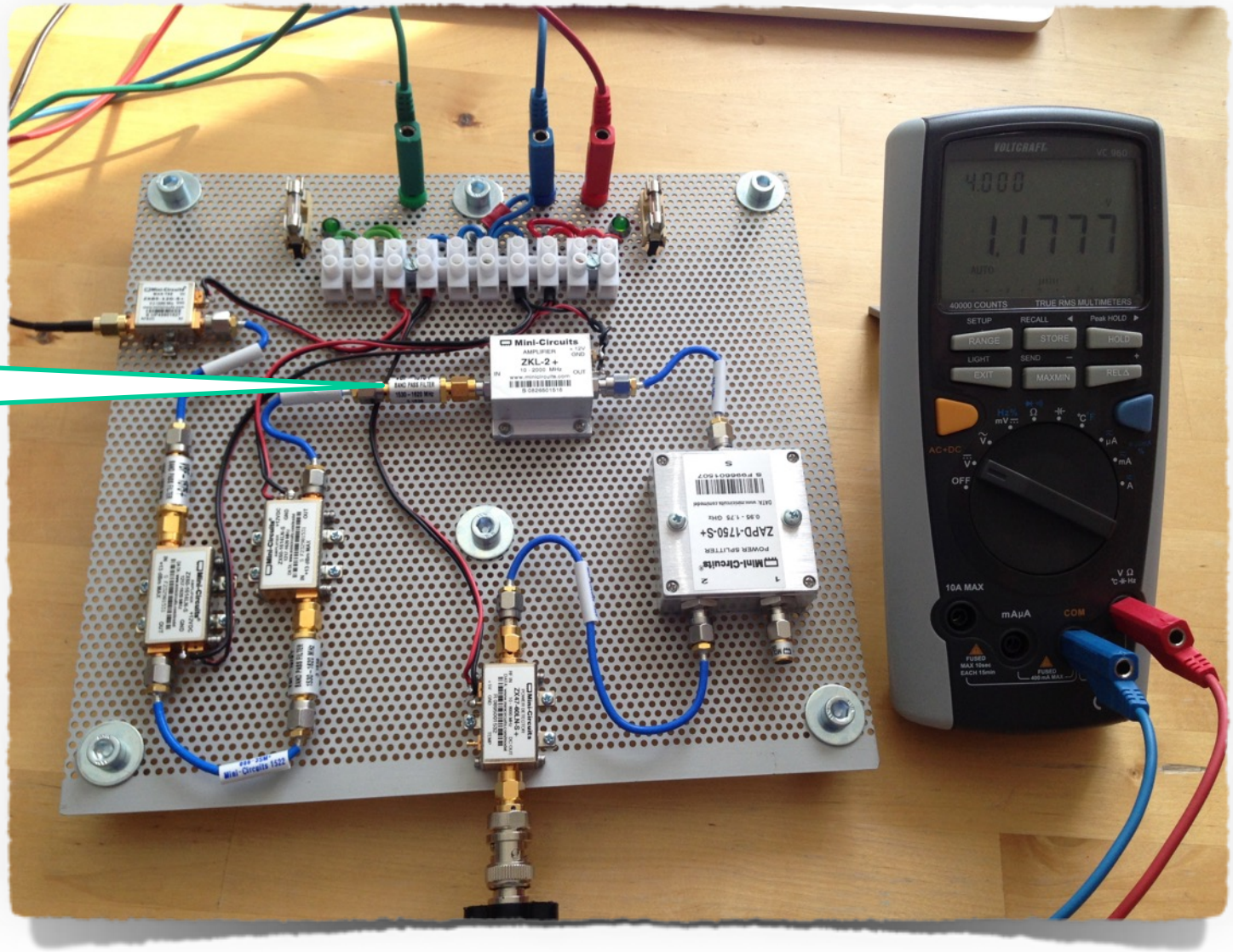


RF Front-End Commented Example

VBF-1575+,
bandpass filter

Passband: 1530 to 1620 MHz, center 1575 MHz.

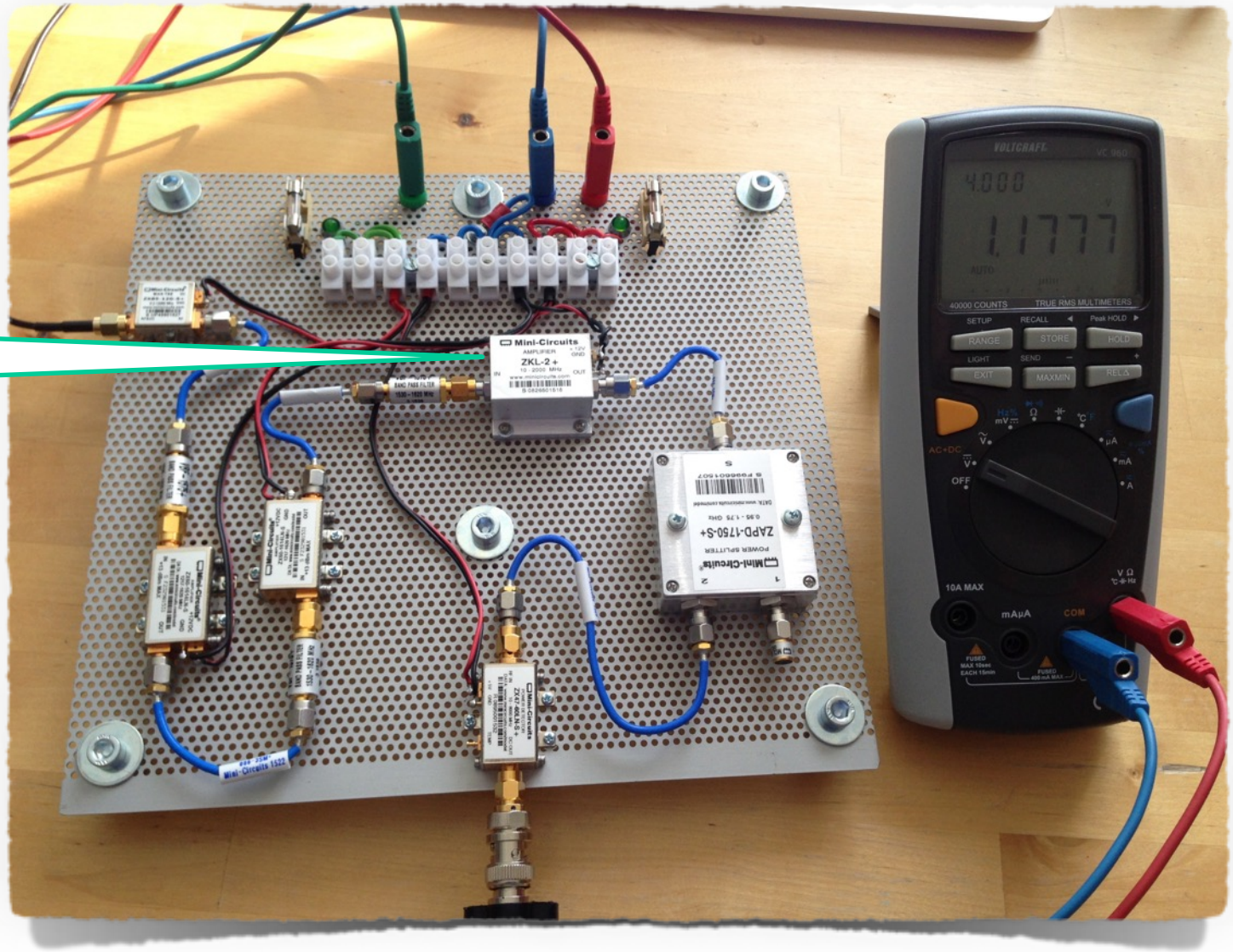
Ins. loss: 3 dB (max)



RF Front-End Commented Example

ZKL-2+, wideband amplifier

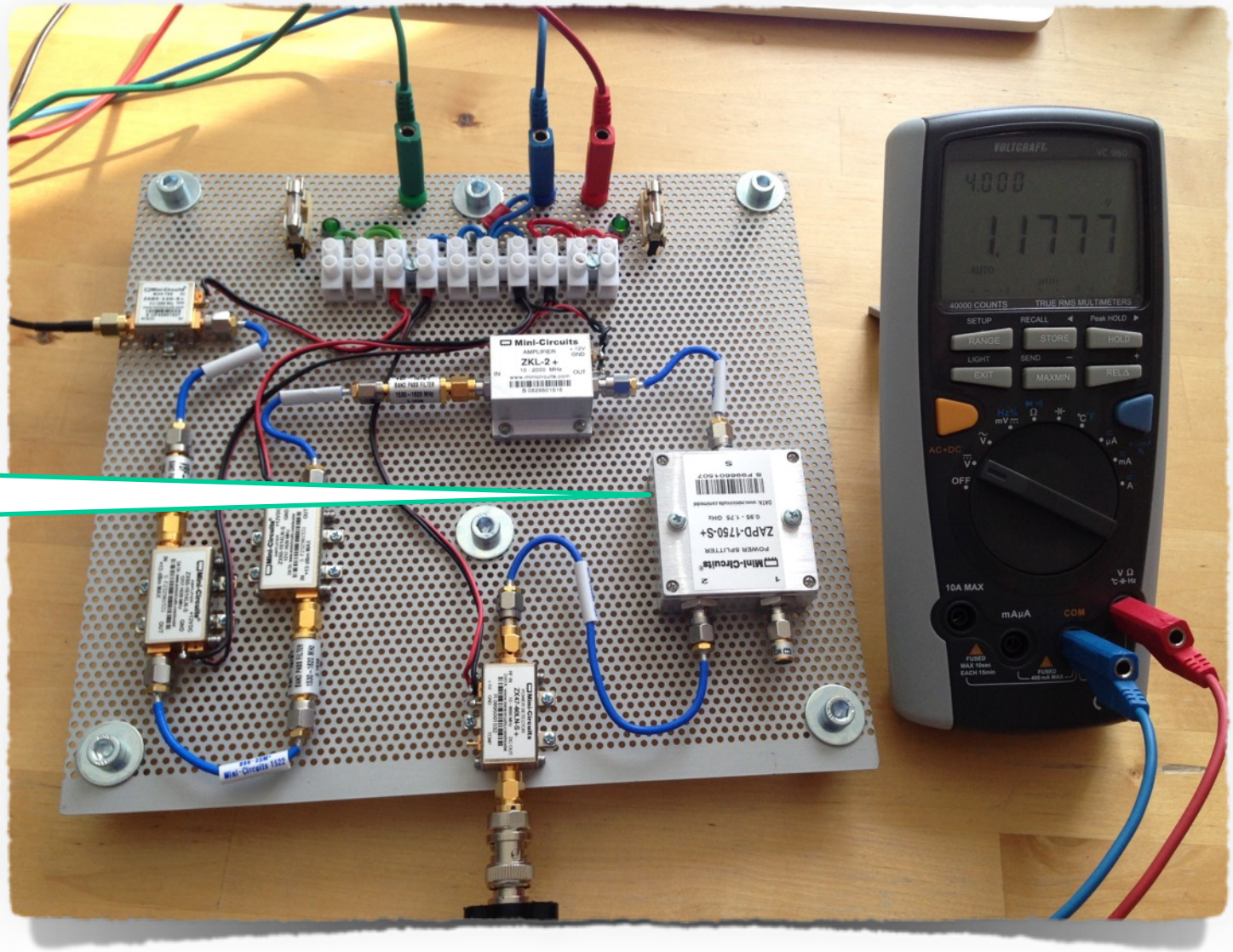
G = 33.5 dB (typ)
F = 4.0 dB (typ)
IP3 = 31 dBm (typ)
BW: 10 to 2000 MHz



RF Front-End Commented Example

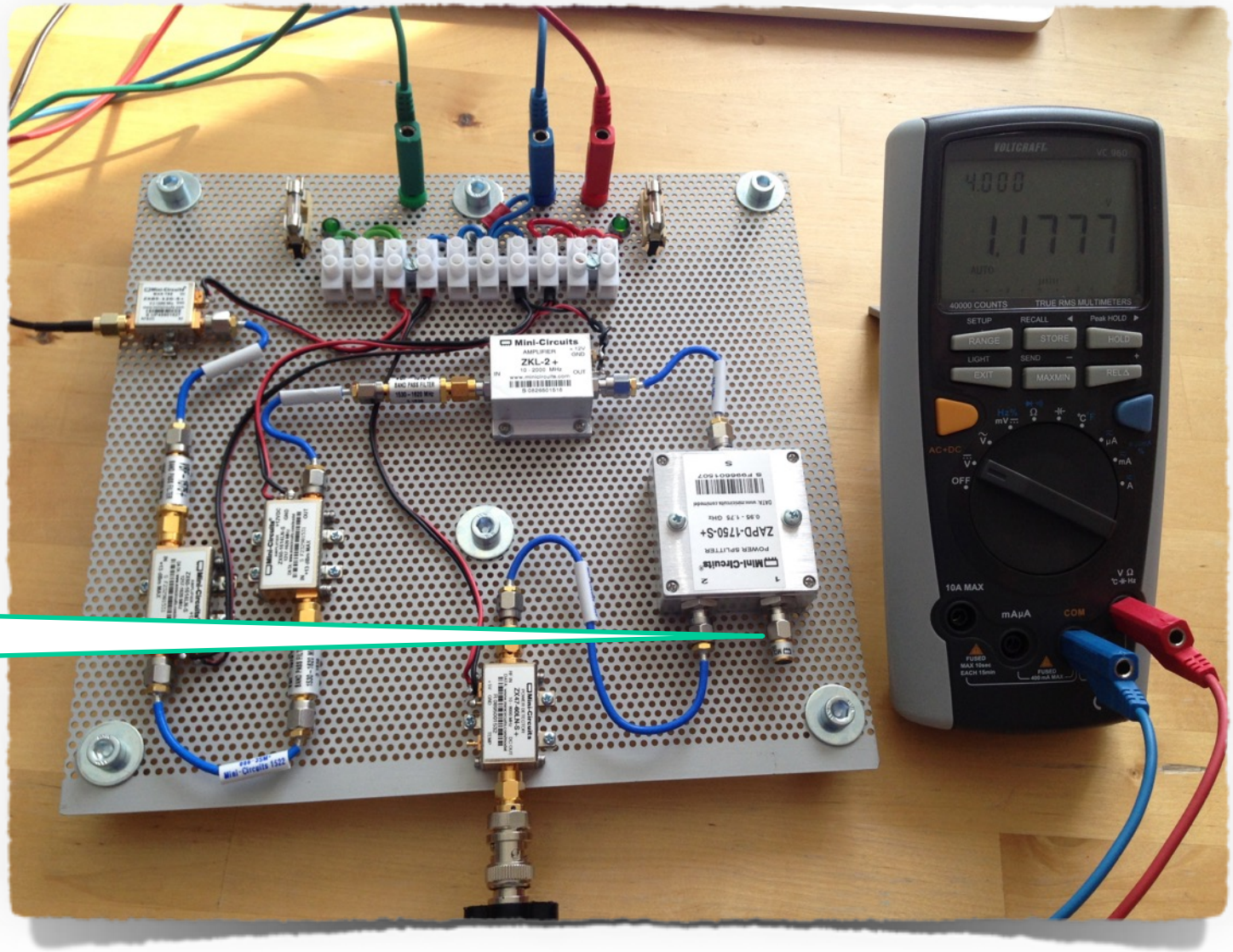
ZAPD-1750-S+,
power splitter/
combiner

Total loss: 3.2 dB (typ)



RF Front-End Commented Example

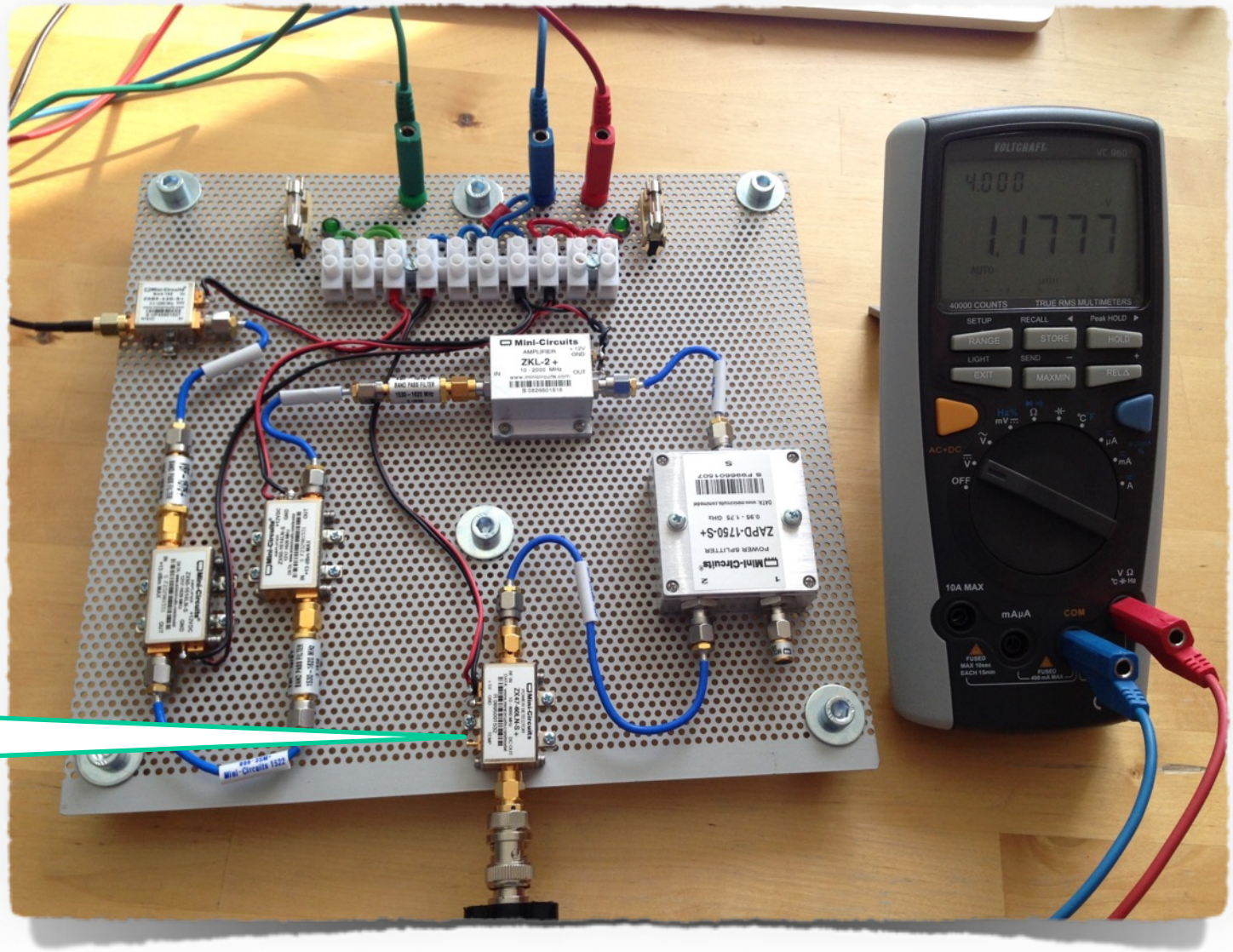
RF front-end output connector. A 50-ohm terminator is used here, now, as to be gentle when no device input is connected.



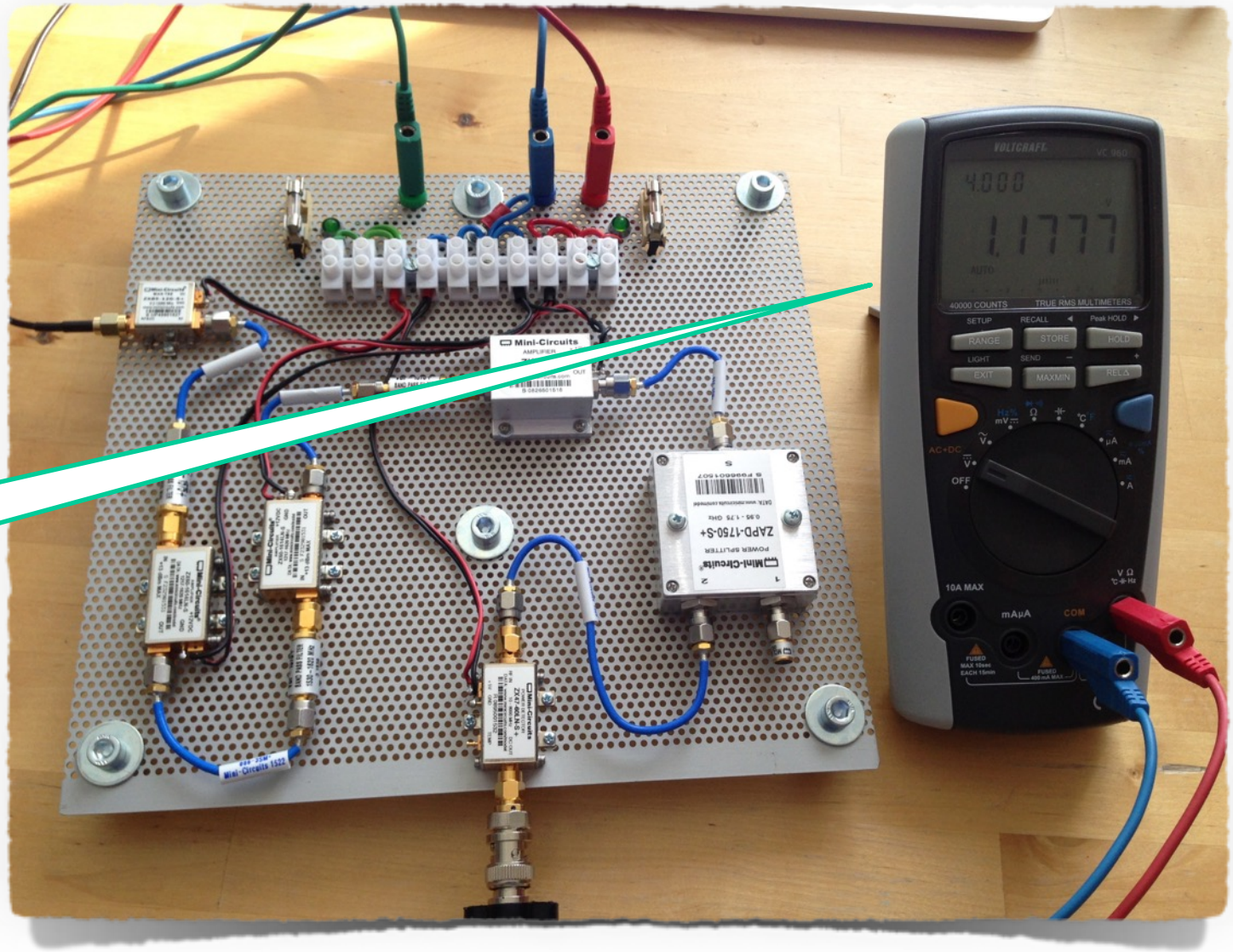
RF Front-End Commented Example

ZX47-60LN-S+,
power detector.
Converts RF power to DC voltage.

Frequency: 10 to 8000 MHz
Power: -60 to +5 dBm
DC out: 2.2 to 0 V, approximately linear with input power.



RF Front-End Commented Example



Voltcraft VC 960, digital multimeter showing DC voltage output of the power detector, herewith serving the role of a simple RSSI monitor.

So, how to use it?

Generally speaking, we need a front-end like this to be put before the internal SDR front-end when we work with the original GNSS signals, namely:

- in record and replay experiments
- in original GNSS processing with e.g. GNSS-SDR toolbox

We can also use its parts, namely the power splitter and RSSI indicator, to quickly check the RF quality of our spoofed signal.

Please see the illustrations below for serving suggestions…

Output Signal Verification

We shall avoid open signal Tx whenever we can.

Get a testing GNSS receiver that allows for an external antenna connection.

Use a direct cable connection in between the SDR output and GNSS receiver input.

... we can also use this method to quickly check our RF front-end (cf. the following example)

It as straightforward as it seems, just pay attention to:

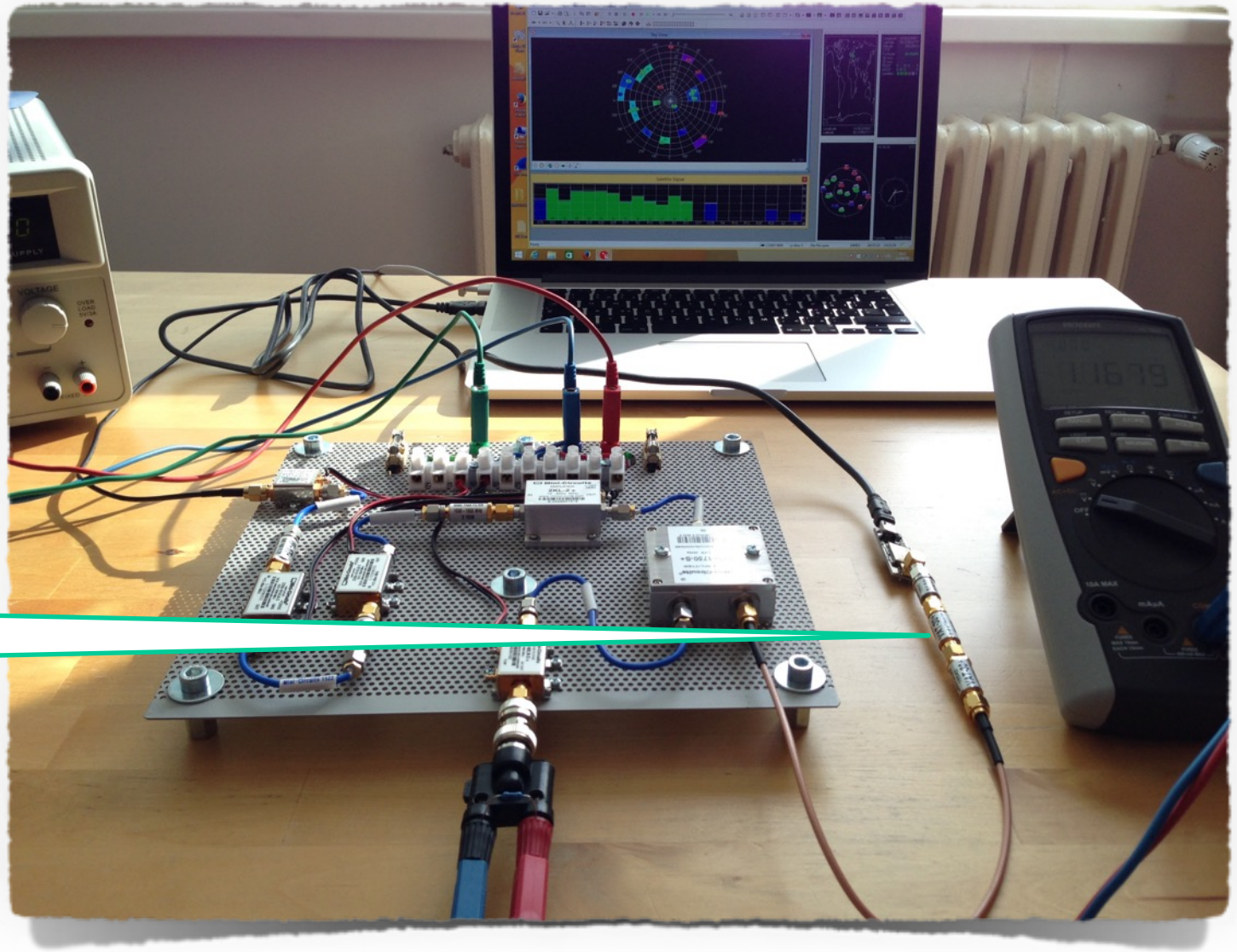
- output/input impedances match
- output power level is in the range expected by the GNSS receiver, possibly use external attenuators
- blocking of possible DC current injected by the GNSS receiver into antenna connector, since it could harm the SDR output

RF Front-End Signal Verification

2x VAT-30+, fixed attenuator

Ins. loss: 30 dB (60 dB in total)
Frequency: DC to 6000 MHz

This roughly compensates the RF front-end gain to get a signal roughly comparable with a standard active antenna output.

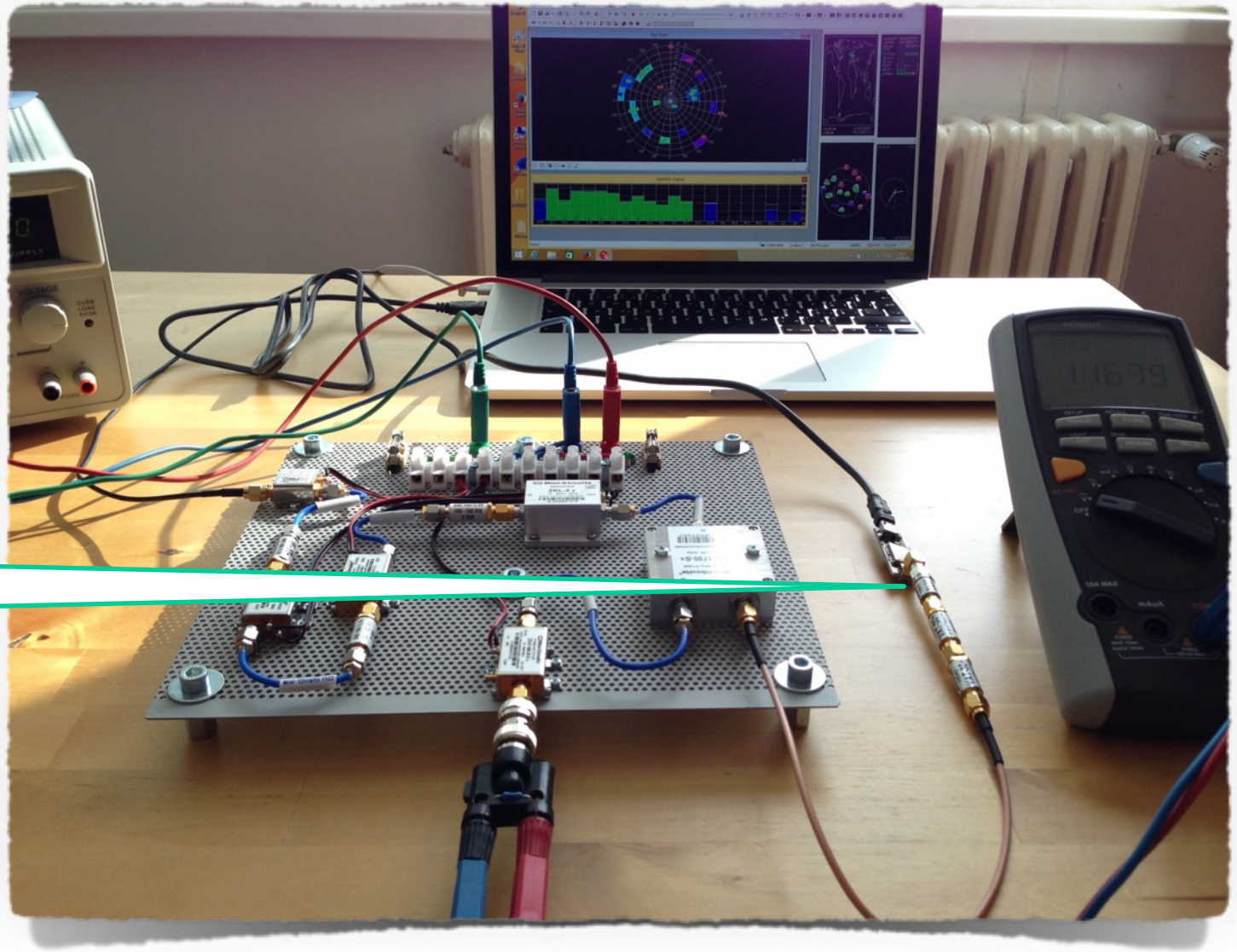


RF Front-End Signal Verification

BLK-18-S+, DC block

Ins. loss: 0.12 dB (typ)
Frequency: 0.01 to 18 GHz

This is a safety circuit for stoping the DC current injected by the ordinary GNSS receiver that implicitly assumes an active antenna at its input.

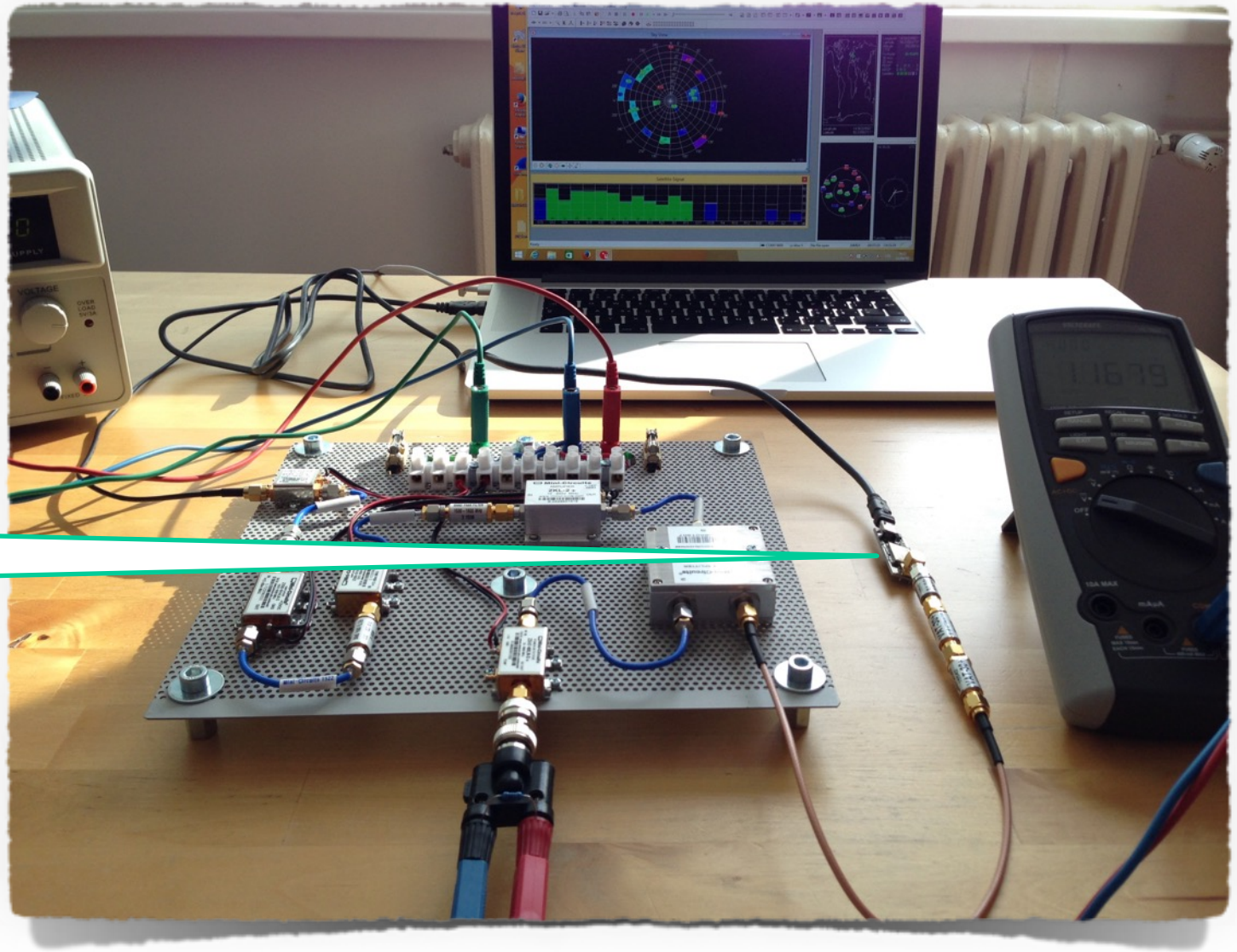


RF Front-End Signal Verification

u-blox NEO-M8N, GNSS receiver board with external antenna and USB connection

It is a breakout board with an industry standard, highly sensitive GNSS receiver.

Works with: GPS/ QZSS, GLONASS, and BeiDou, incl. SBAS (WAAS, EGNOS and MSAS); Galileo ready (fw update required)

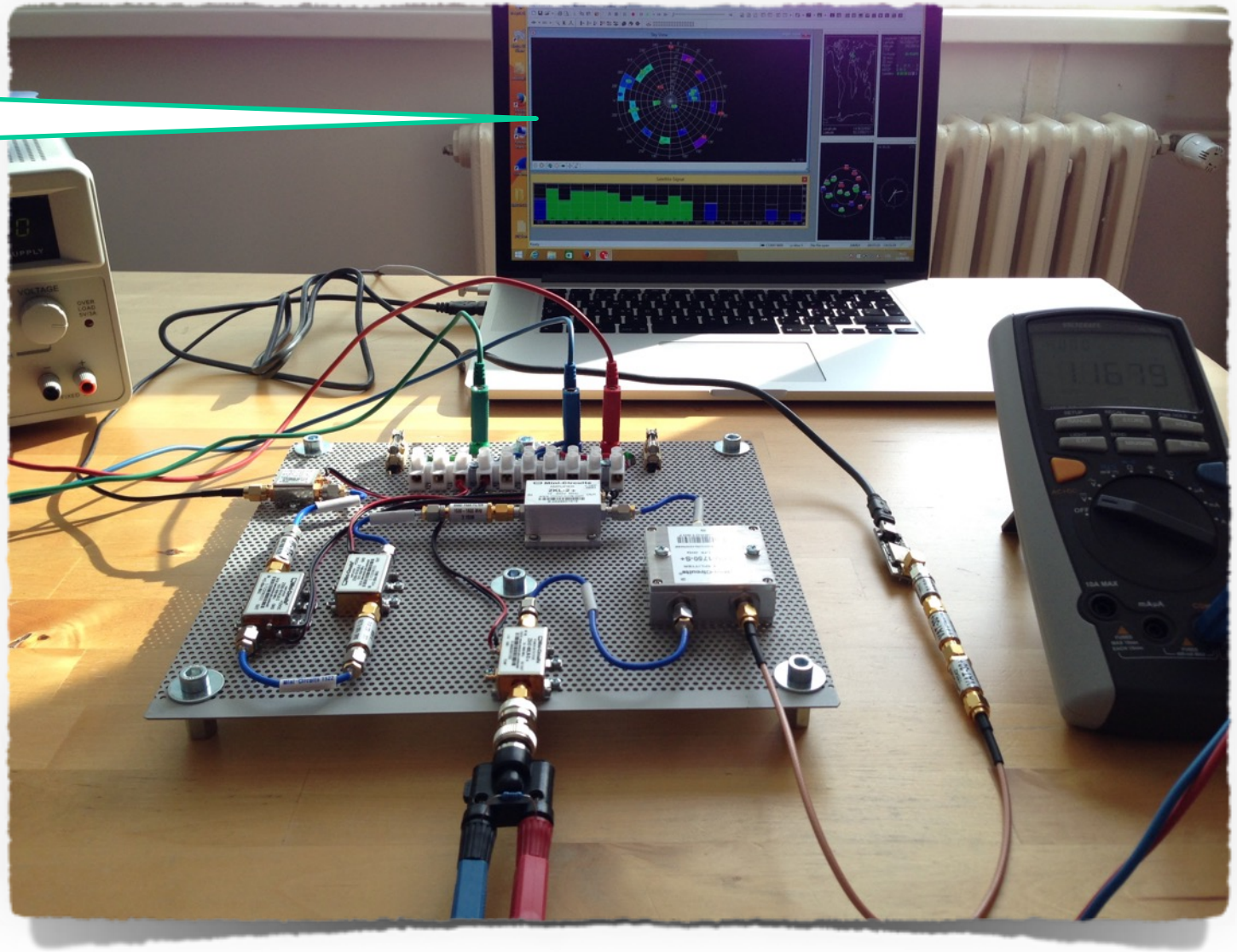


RF Front-End Signal Verification

u-center 8.20, free of charge u-blox GNSS receiver evaluation software

Thanks to the wider bandwidth used (1530 to 1620 MHz), our front-end handled GLONASS L1OF signals as well. (we changed the antenna in the real GLONASS experiment, cf. below)

Galileo E1 signals should also pass.



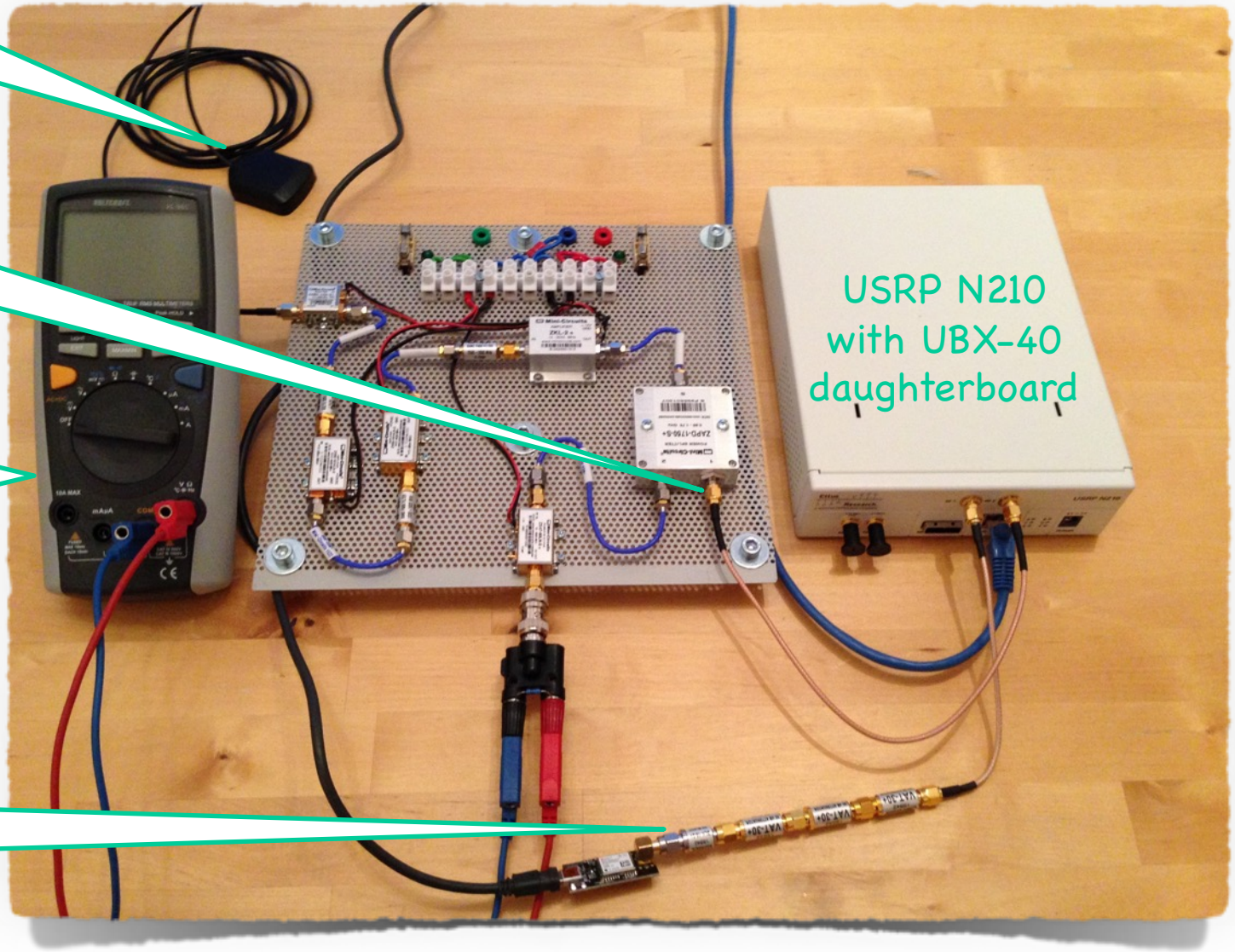
Record & Replay (Meaconing) Setup

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)!

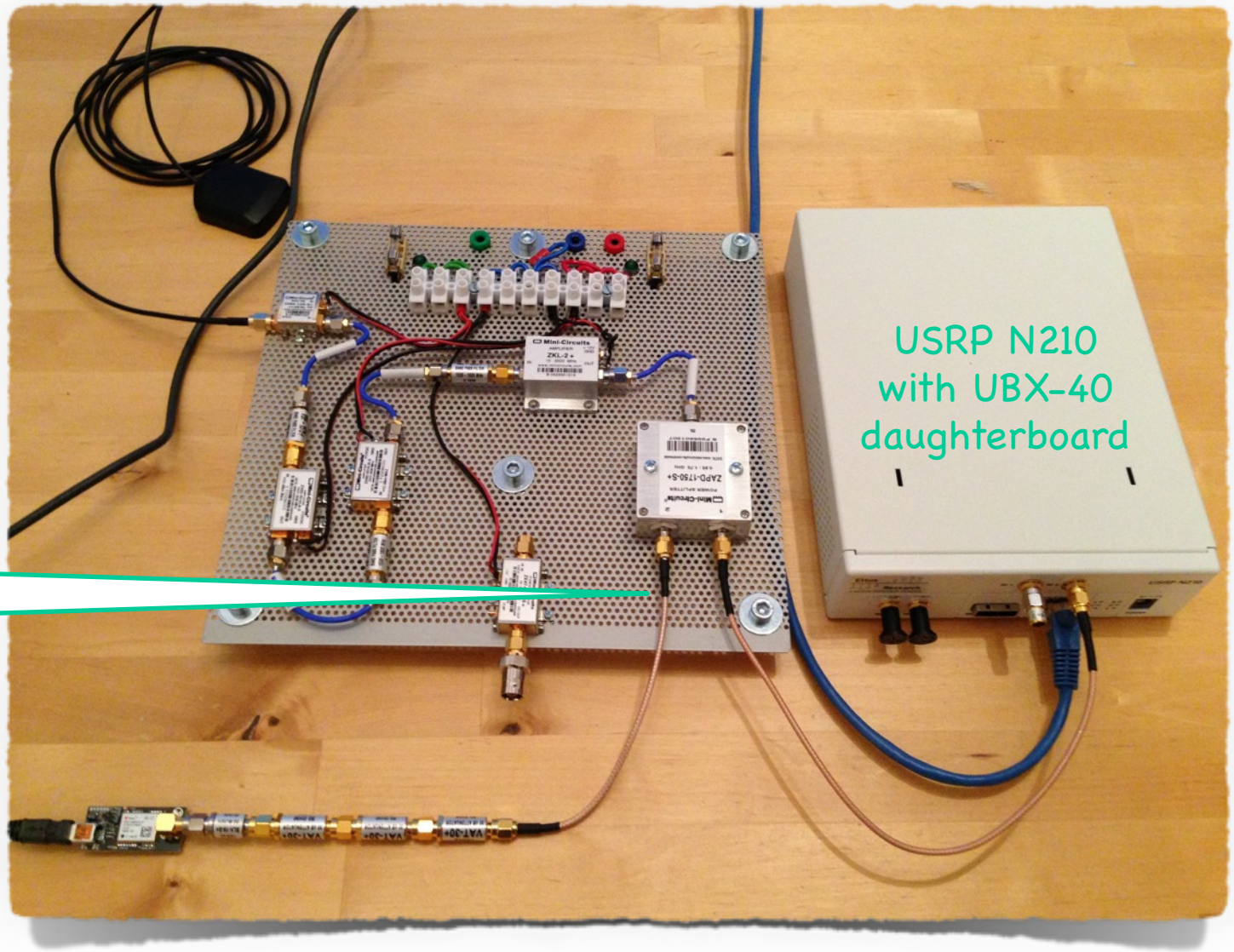


Alternative Scheme During Recording

Instead of the plain RSSI, we can use the power splitter to deliver the RF signal to u-blox receiver directly during rec.

This way, we can monitor the recorded signal much better.

(the attenuation before u-blox shall be adjusted according to our RF gain, this is just an illustration; cf. pls. the verification demo above)



Software Suggested 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, see also [Di, 13] for further possible improvements

... similar radios can have similar standard utilities

We shall carefully balance the sampling rate and word length

... the primary sampling rate shall always correspond with the SDR's internal RF front-end bandwidth to avoid aliasing!

... then we can perform decimation to e.g. 2.5 Ms/s (*with USRP, this is done in its FPGA, so we can directly work at the decimated rate instead*)

... 8-bit (or even 4-bit and less) A/D resolution can be enough under good conditions

... 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 [Chen et al., 13] or even the LabView project at http://www.ni.com/white-paper/13881/en/

In Particular

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

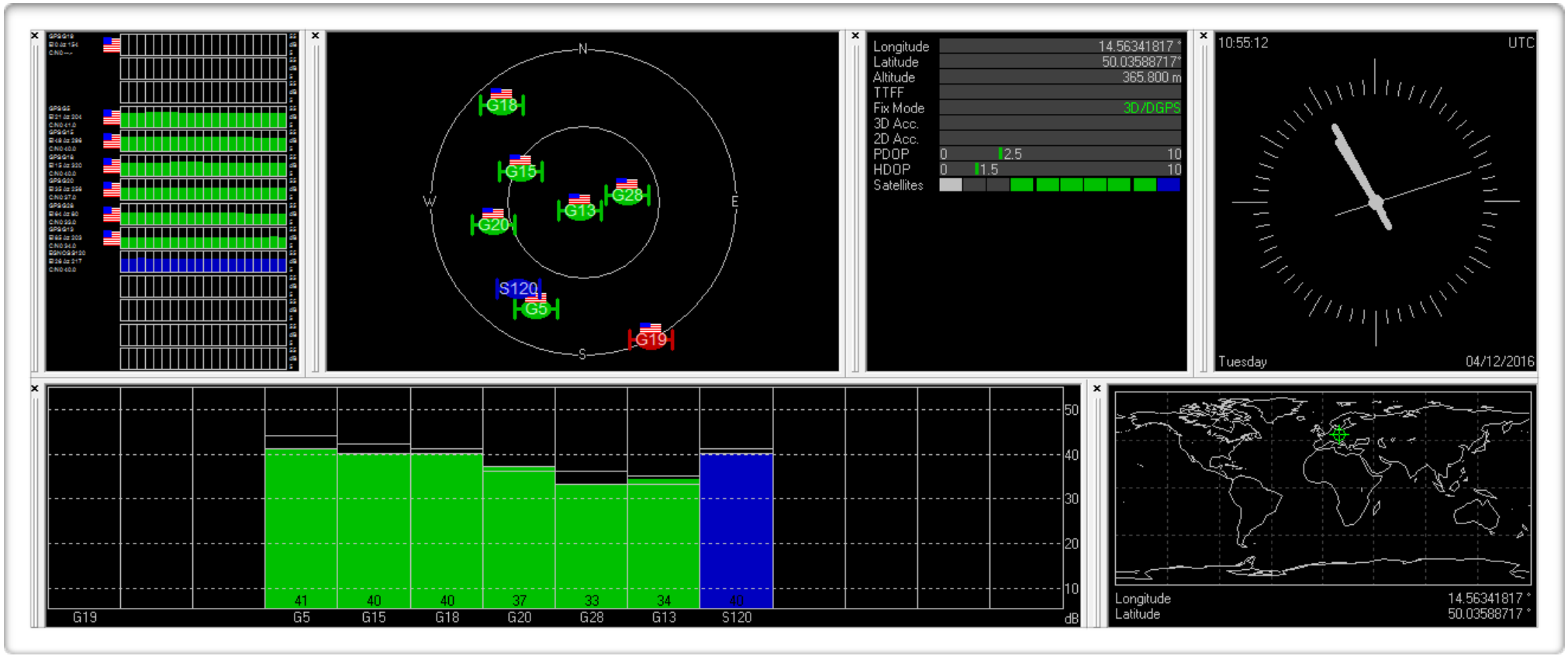
```
$ rx_samples_to_file --type short --duration 300 --spb
  1000000 --rate 2500000 --freq 1575420000 --gain 30
  --progress
```

```
$ 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]

Map View

- Illustrates nicely the core principle of the meaconing (replay) attack
- The smartphone believes it is right at the place where the original signal was captured
- The time derived also corresponds to the recorded original signal time-stamps

[screenshot & idea courtesy by Jiří Buček]

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

... this is distant enough from GPS L1, so it deserves a dual band active antenna (our RF front-end is L1OF capable, as was shown above)

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

... furthermore, the whole FDMA multiplex span is roughly 8.3345 MHz

GLONASS L1OF Signal in Detail

Carrier frequency	L1: 1598.0625 - 1605.375 MHz, spacing by 562.5 kHz (14 carriers)
Minimum received power (GLONASS spc.)	-161.0 dBW = -131 dBm
Polarization	Right-Hand Circular Polarization (RHCP)
Multiple access	Frequency Division Multiple Access (FDMA)
Spreading modulation	BPSK-R(511 kHz)
Tx bandwidth	±511 kHz (first null-to-null BW)
Spreading codes	Common 511 bit m-sequence for all SVs
Data message structure	GLONASS
Data rate	50 bps
Data error control code	Extended (85,81) Hamming code
Data modulation	50 sps biphase modulation
Pilot and data components	100% power data
Overlay code	Meander sequence 101010… @ 100 bps
Multiplexing with other signals	In phase quadrature to L1SF

[Betz, 16], [GLONASS ICD, 08]

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
```

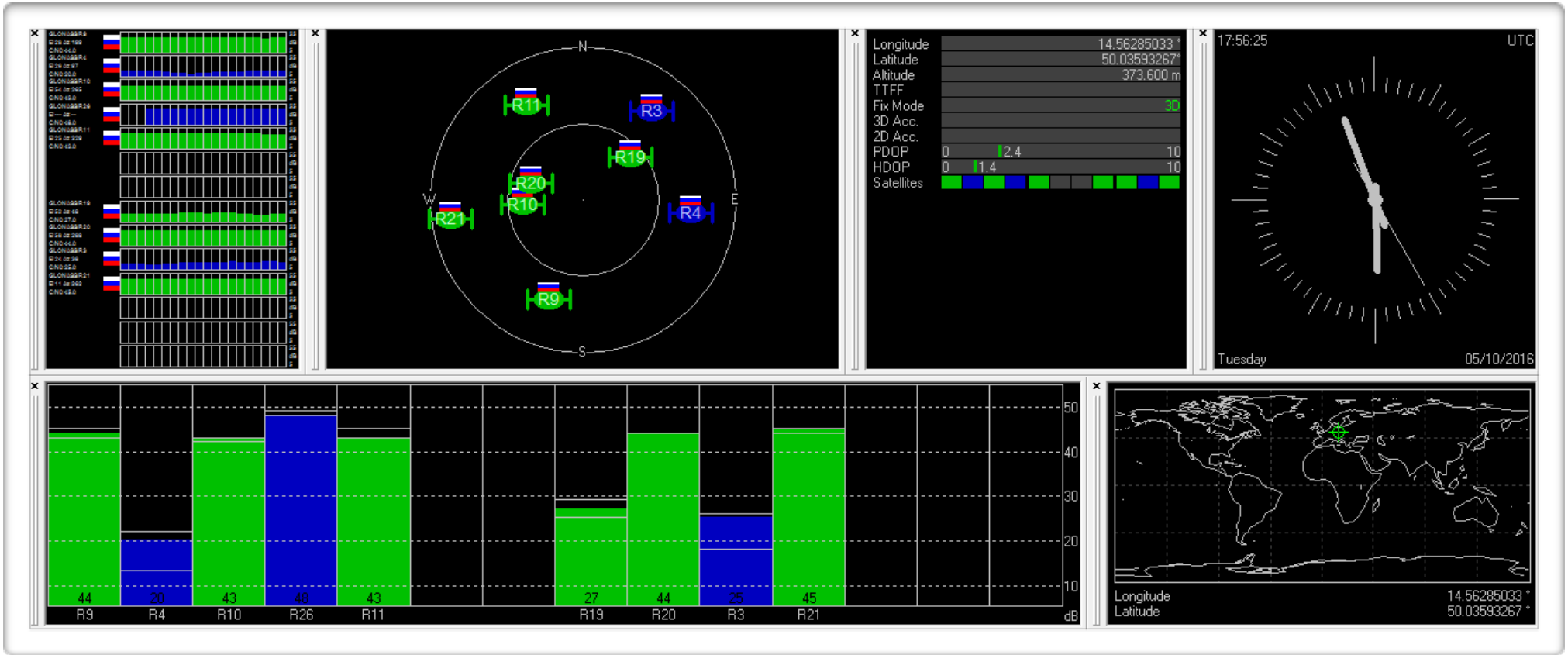
... complex envelope sampling of the whole L1 Open FDMA multiplex signal

... 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 as suggested by [Di, 13]

... for simplicity and safety, we stay with 16-bit I/Q sampling, though this would also deserve optimization if one would decide to alter the original code

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]

Software Suggested 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.

- just go to https://github.com/osqzss/gps-sdr-sim and follow the instructions in `README.md`, including the hints where to get relevant ephemerides files*, cf. also [Wang et al., 15]

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`

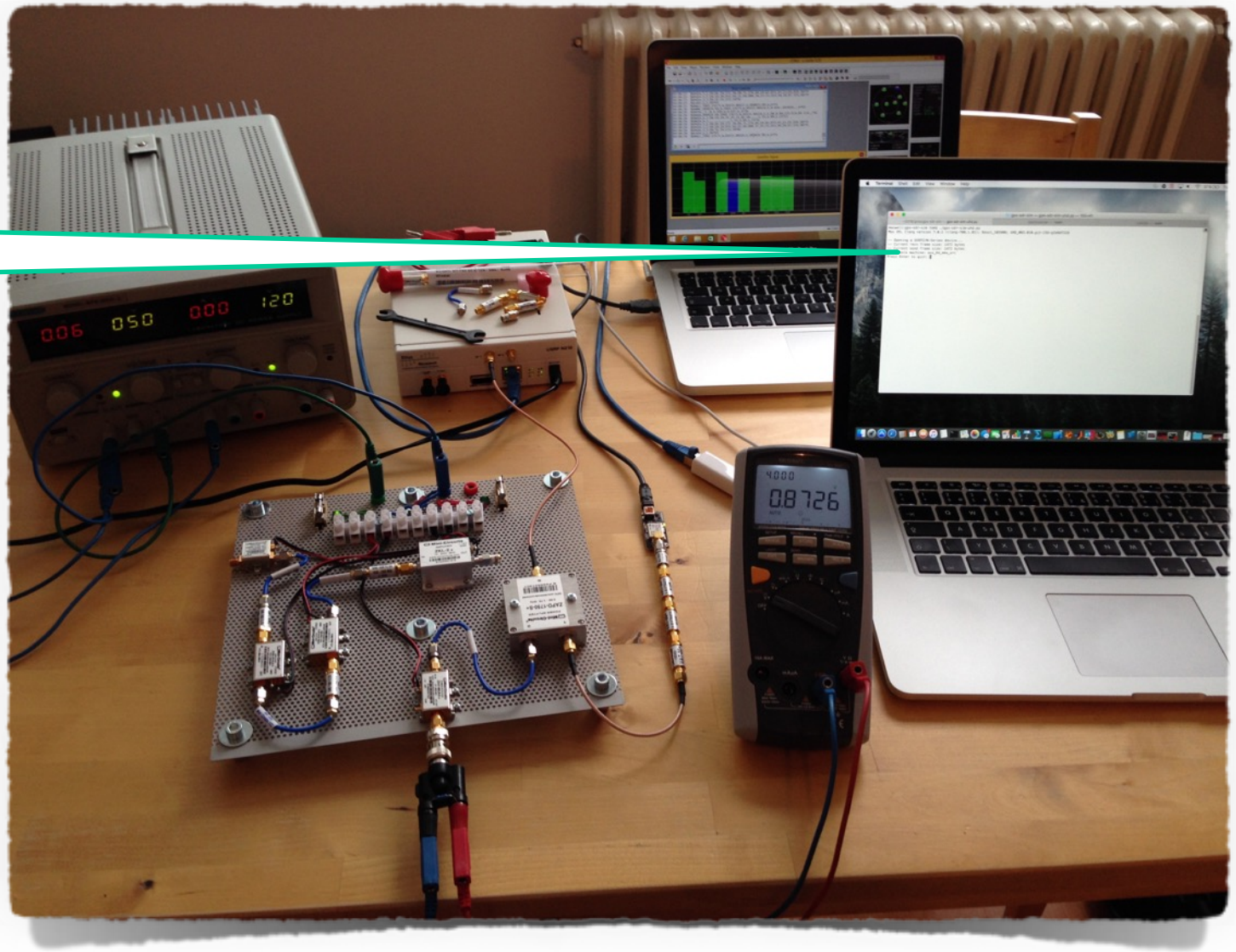
*) These describe the actual orbital motion of GPS satellites. However, you can simply grab the particular file in the NASA archive noted in README.md and pass it on to gps-sdr-sim.

Synthetic Signal Spoofing Demo

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

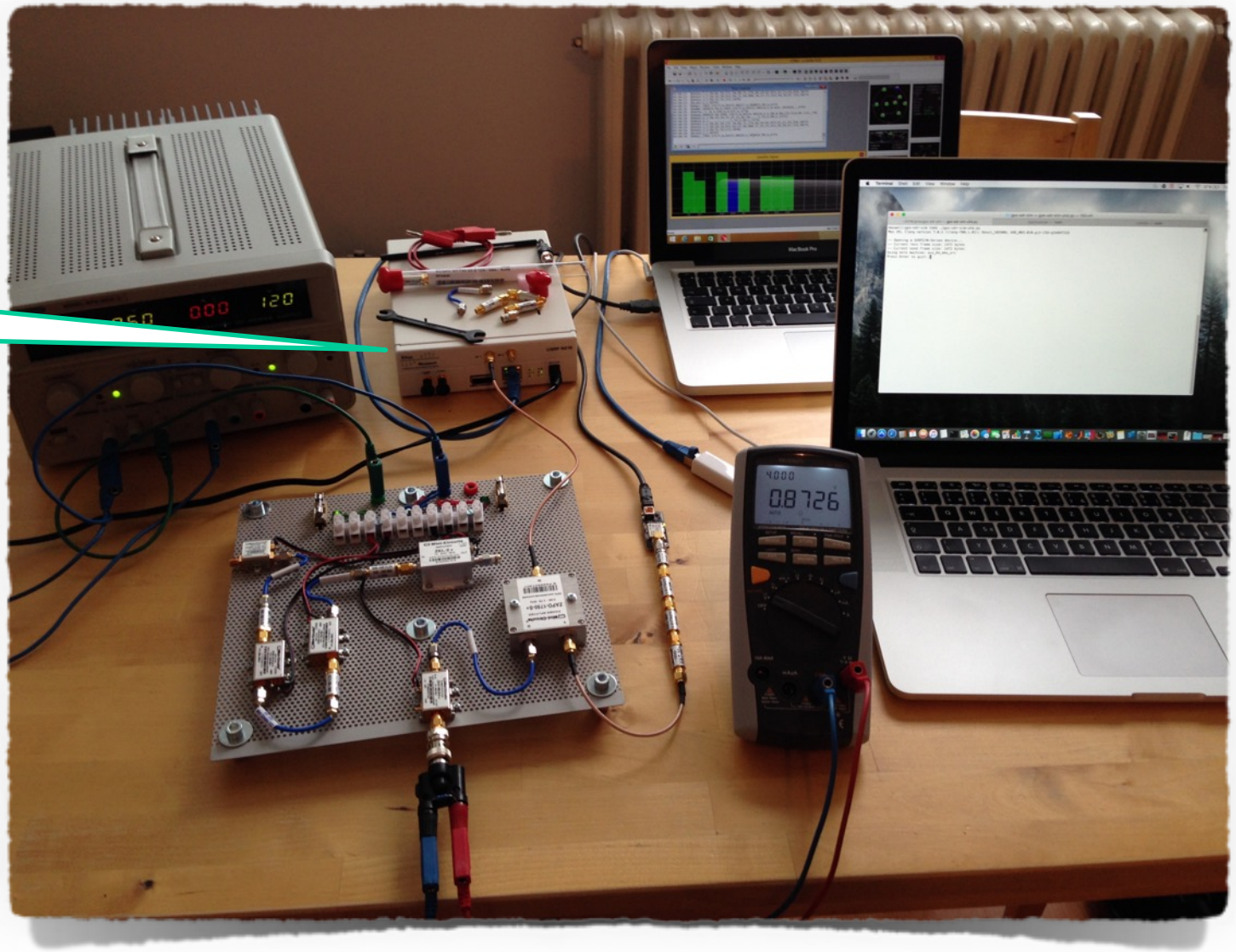
This in turns invokes gnuradio Python framework to transmit the L1 bandpass signal, prepared in the form of I/Q complex envelope samples, through the USRP N210.

This all was running natively on OS X El Capitan (many thanks, MacPorts!).



Synthetic Signal Spoofing Demo

USRP N210 with
UBX-40
daughterboard

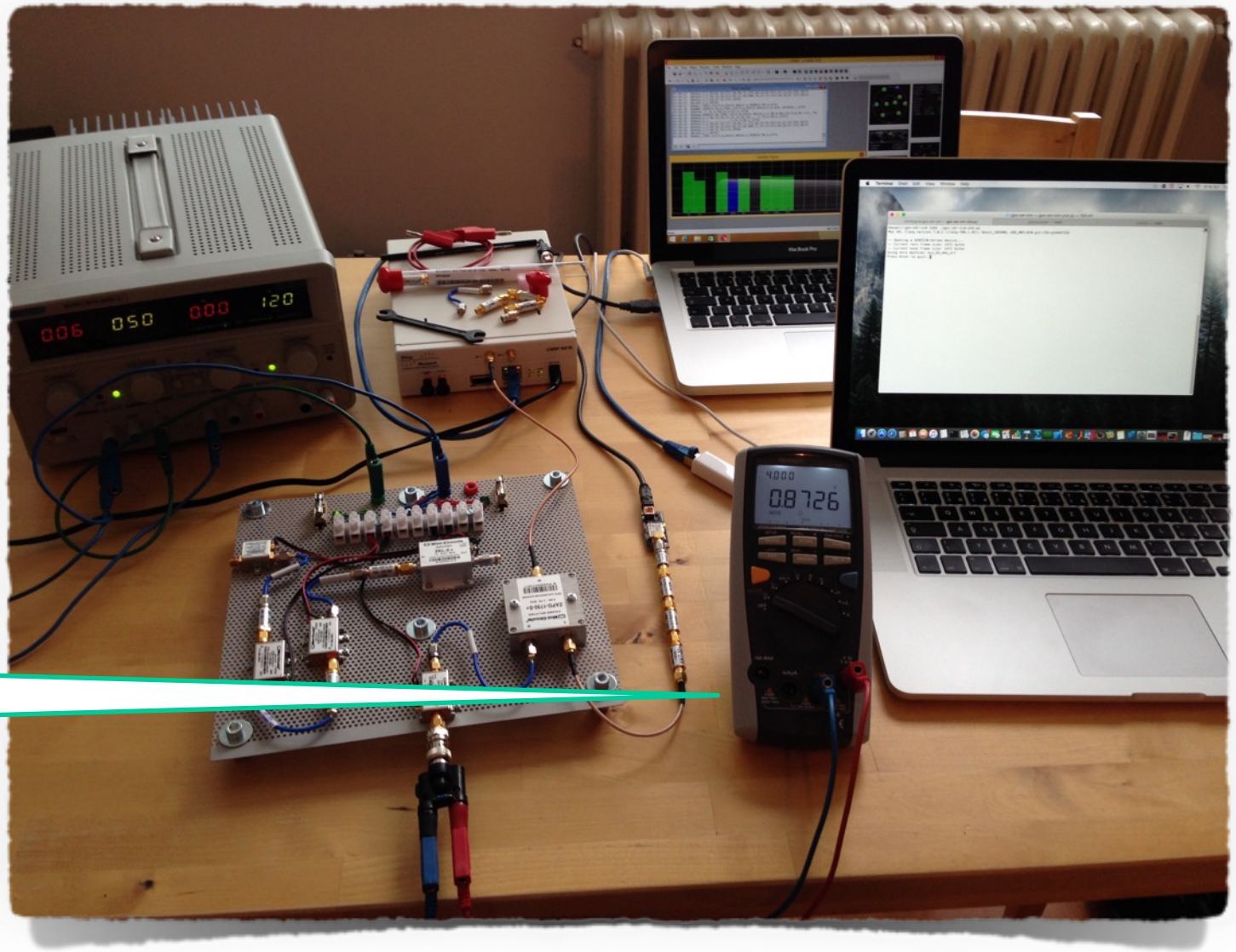


Synthetic Signal Spoofing Demo

The RSSI monitor of our RF front-end was reused to check the Tx output signal.

We get circa -10 dBm from the UBX-40 daughterboard inside USRP N210 for 0 dB output amplifier setting.

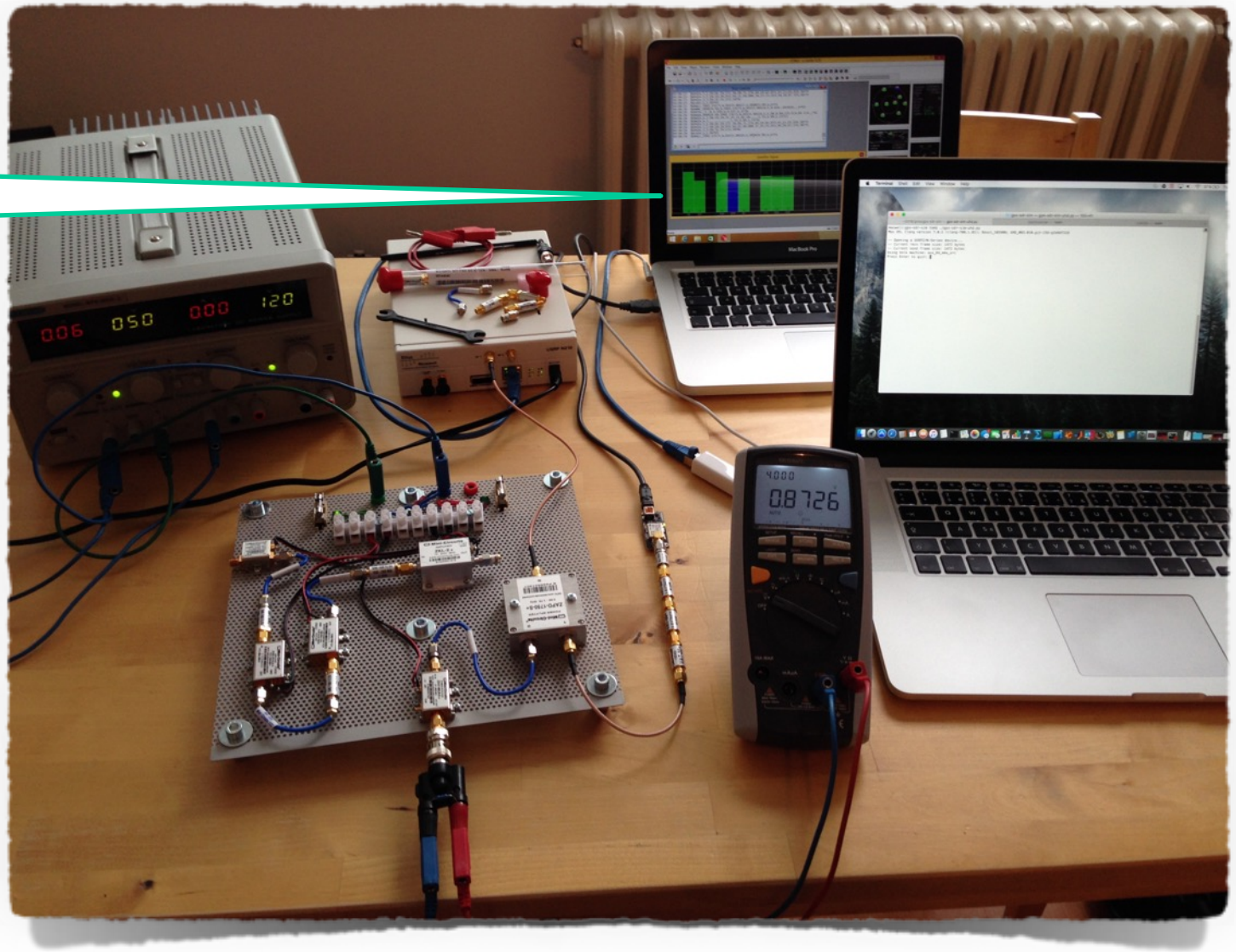
This in turn suggested using 3x30 dB attenuation before the u-blox receiver.



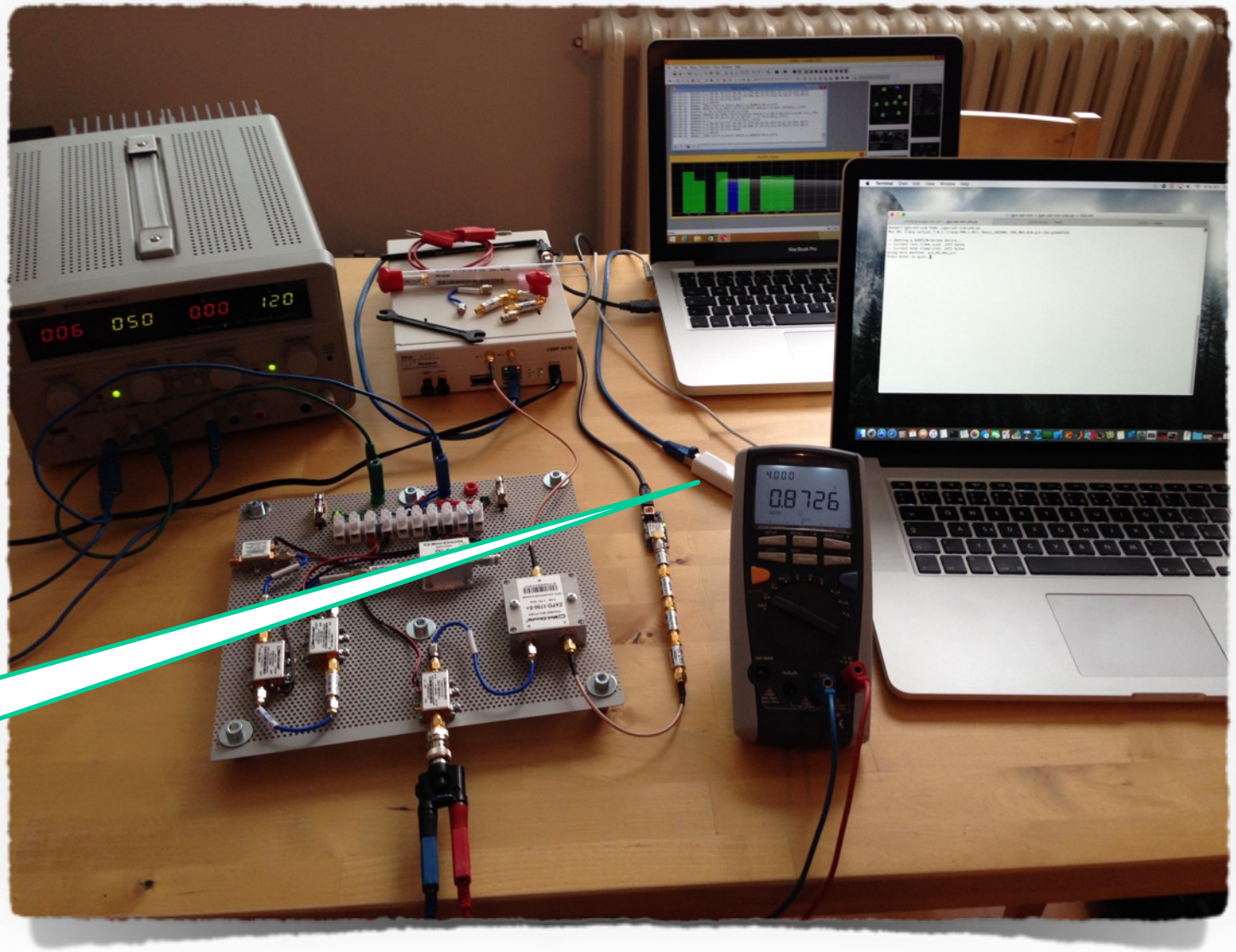
Synthetic Signal Spoofing Demo

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.



Synthetic Signal Spoofing Demo



Macbook special:
1 GigE thunderbolt adapter needed for USRP connection

Map View

…based on the spurious radiation again

[screenshot & idea courtesy by Jiří Buček]

So, you *really* have to *fully* transmit?

Think twice, please!

Consider a well shielded area:

- laboratory (Faraday “tent”)
- civil (cellar, underground parking, bunker, natural cave)

Double check the local safety of you experiment:

- is the original GNSS/GPS signal vanishing there?
- which receivers are nearby and what could they cause (BTS, car alarms, patient monitors, airplanes?!, etc.)?
- use the *Friis transmission equation* to estimate the output power and recognise your electromagnetic footprint

Faraday Tent

Friis Transmission Equation*

Let $P_{rx,dB}$, $P_{tx,dB}$ be the expected received/transmitted power, G_{tx}, G_{rx} the source/target antenna gain in dBi or dBic, f carrier frequency, and d distance.

- for convenience, we directly assume linear polarization for Tx and circular for Rx (implying circa 3 dB loss)
- having neglected the CDMA effect, the following is a first approximation of the far field received power based on total Tx power

$$P_{rx,dB} = P_{tx,dB} + G_{tx,dBi} + G_{rx,dBic} - 3 - 20\log\frac{4\pi f}{c} - 10n\log d$$

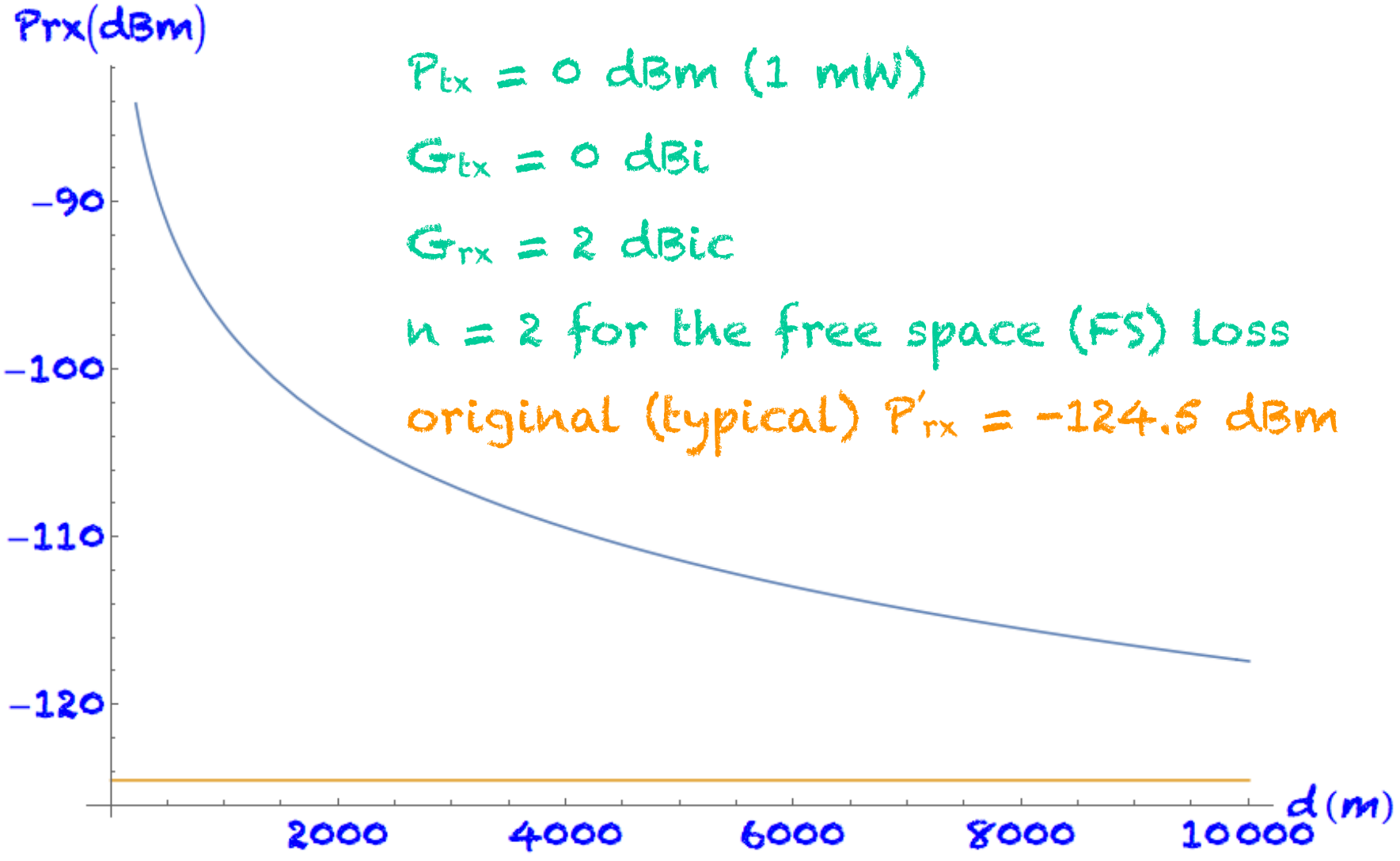
n = 2 for the free space loss

f = 1575.42 MHz for L1

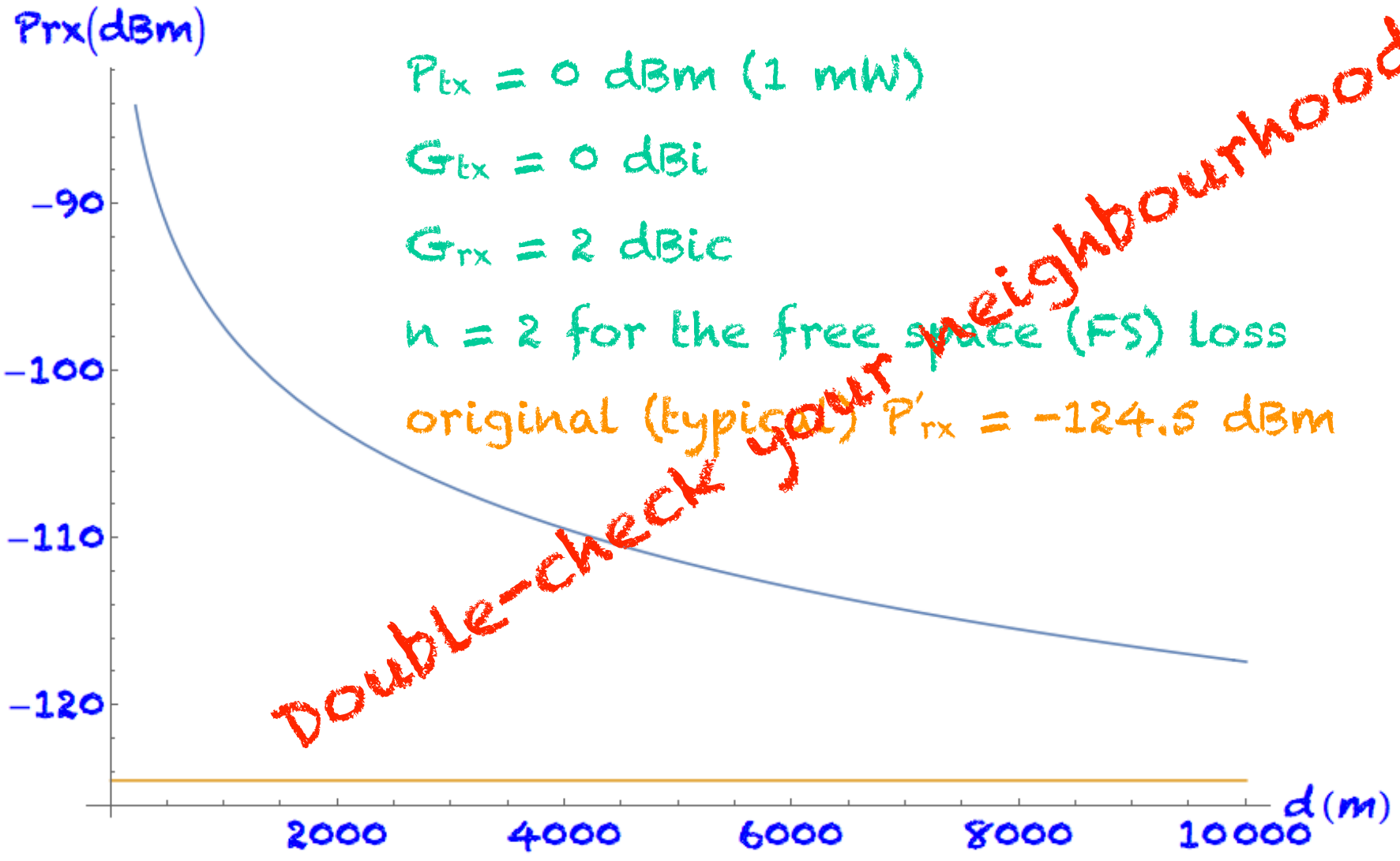
c = 299 792 458 m/s in vacuum

*) pls. note, this is not the same construction as the Friis formula for noise discussed above

Spoofed vs. Original Signal in FS



Spoofed vs. Original Signal in FS



Link Budget

That was a first approximation, you may also want to further check:

- [Richards, 08] for a gentle introduction into the theory of radio wave propagation in general
- [Misra, Enge, 12] for a tailored explanation in the context of GNSS
- [Betz, 16] for a practical approach including building materials attenuation characteristics

OK, so how to transmit?

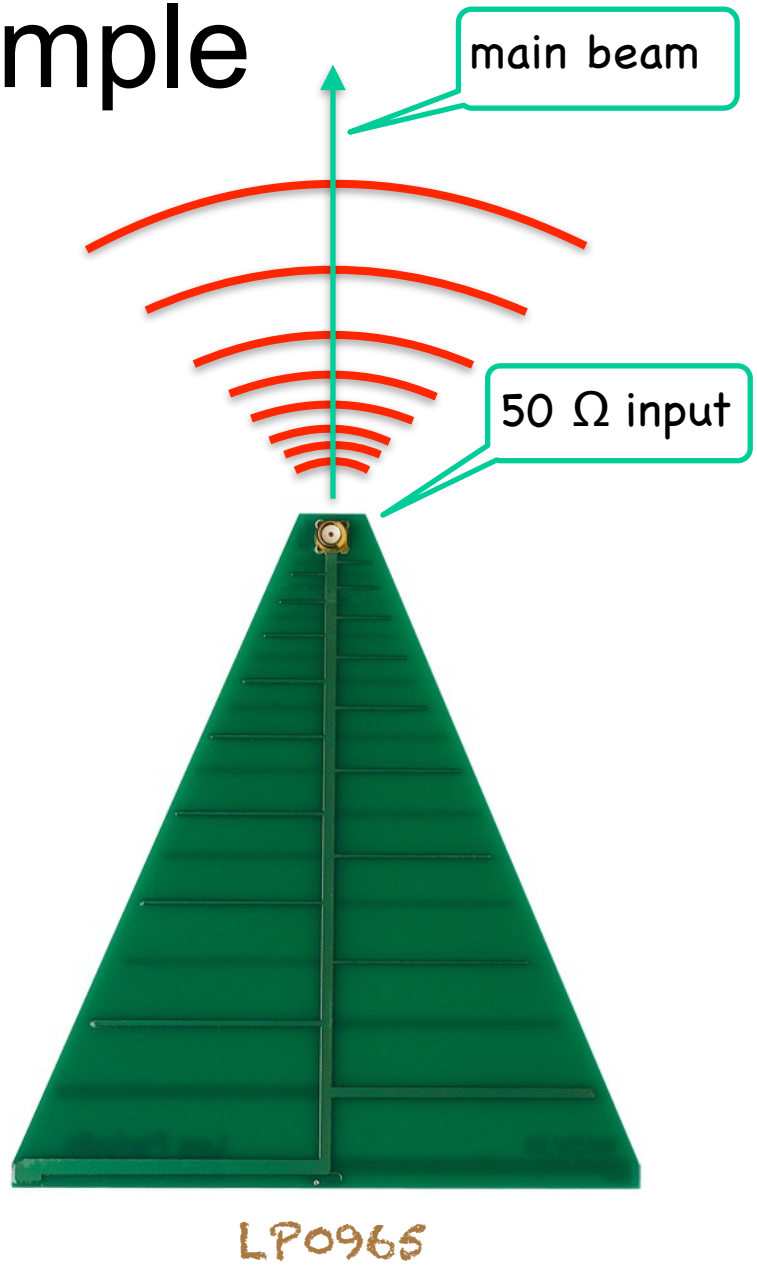
Well, quite simply. Since the usual SDR has enough output power for these experiments (cf. Friis eq. above), all we have to do is to connect an impedance matched antenna to the SDR output.

- ... instead of by the GNSS receiver input, the Tx power will be then consumed by the antenna radiation resistance, herewith emanated as an electromagnetic wave
- ... impedance matching actually means the antenna input should be approximately seen as a real 50 ohm load in the L1 C/A signal band (cf. signal characteristics at the beginning)
- ... sometimes, the antenna matching can be stated as graph of VSWR (Voltage Standing Wave Ratio) vs. frequency; in that case, we should look for VSWR < 2.0 at around 1575.42 MHz
- ... be aware of the antenna cable loss, as the L1 frequency is no longer negligible for common coaxial cables (check the respective data sheet)
- ... on the other hand (again), keep your Tx power as low as possible; recall the original GPS satellites use a few dozens of watts and are over 20 000 km far away from us

Tx Antenna Example

When looking for off-the-shelf components, it may be uneasy to find a suitable antenna, as many of them are active receiving antennas

- ... we can try using the patch antenna that is a part of common active antennas and sometimes also sold separately, provided it can handle the output power; we can get the circular polarization this way
- ... we can also use a **broadband log-periodic antenna**, such as e.g. LP0965 from Ettus/ Kent by WA5VJB; this way we get the linear polarization, but the loss is small and can be accounted for (cf. the elaboration above)
- ... never(!) try to use the active antenna directly (unless you want to destroy the embedded LNA)



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, 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 some recent proclamations of GSA, however, the only "protection" explicitly noted in the OS ICD from November 2015 besides a forward error correction code is simple CRC.

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.

References

Antennas and radio wave propagation

Balanis, C.-A.: *Antenna Theory - Analysis and Design*, Third Edition, Wiley-Interscience, 2005

Kraus, J.-D. and Marhefka, R.-J.: *Antennas For All Applications*, Third Edition, McGraw-Hill, 2003

Richards, J.-A.: *Radio Wave Propagation: An Introduction for the Non-Specialist*, Springer, 2008

Stutzman, W.-L. and Thiele, G.-A.: *Antenna Theory and Design*, Third Edition, Wiley, 2013

RF electronics, DSP, and SDR

Essick, J.: *Hands-On Introduction to LabVIEW for Scientists and Engineers*, Third Edition, Oxford University Press, 2015

Etten, van W.-C.: *Introduction to Random Signals and Noise*, First Edition, Wiley, 2005

Grayver, E.: *Implementing Software Defined Radio*, Springer, 2012

Haykin, S. and Moher, M.: *Communication Systems*, 5th ed., John Wiley & Sons, 2009

Johnson, C.-R., Jr., Sethares, W.-A., and Klein, A.-G.: *Software Receiver Design - Build Your Own Digital Communications System in Five Easy Steps*, Cambridge University Press, 2011

Lathi, B.-P. and Green, R.-A.: *Essentials of Digital Signal Processing*, Cambridge University Press, 2014

Lyons, R.-G.: *Understanding Digital Signal Processing*, Third Edition, Prentice Hall, 2011

Razavi, B.: *RF Microelectronics*, Second Edition, Prentice Hall, 2011

Rutledge, D.: *The Electronics of Radio*, Cambridge University Press, 1999

Schreier, P.-J. and Scharf, L.-L.: *Statistical Signal Processing of Complex-Valued Data: The Theory of Improper and Noncircular Signals*, Cambridge University Press, 2010

Stewart, R.-W., Barlee, K.-W., and, Atkinson, D.-S.-W.: *Software Defined Radio using MATLAB & Simulink and the RTL-SDR*, Strathclyde Academic Media, 2015

References

GNSS theory and practice

Badea, V. and Eriksson, R.: *Indoor Navigation with Pseudolites (fake GPS sat.)*, Joint M.Sc. Thesis, University of Linkoeping, Sweden, 2005

Betz, J.-W.: *Engineering Satellite-Based Navigation and Timing: Global Navigation Satellite Systems*, Signals, and Receivers, IEEE Press, John Wiley & Sons, 2016

Borre, K., Akos, D.-M., Bertelsen, N., Rinder, P., Jensen, S.-H.: *A Software-Defined GPS and Galileo Receiver A Single-Frequency Approach (Applied and Numerical Harmonic Analysis Series),* Birkhäuser Boston, 2007

Diggelen, van F.: A-GPS: *Assisted GPS, GNSS, and SBAS (GNSS Technology and Applications Series)*, First Edition, Artech House, 2009

Doberstein, D.: *Fundamentals of GPS Receivers - A Hardware Approach*, Springer, 2011

European GNSS (Galileo) Open Service (OS), Signal In Space (SIS) Interface Control Document (ICD), Europen Union, November, 2015

Fernández-Prades, C., Arribas, J., and Closas, P.: *Turning a Television into a GNSS Receiver*, In Proc. of ION GNSS, pp. 1492-1507, 2013

GLOBAL NAVIGATION SATELLITE SYSTEM - GLONASS, Interface Control Document, Ed. 5.1, Russian Institute of Space Device Engineering, Moscow, 2008

Holmes, J.-K.: *Spread Spectrum Systems for GNSS and Wireless Communications (GNSS Technology and Applications Series)*, Artech House, 2007

Misra, P. and Enge, P.: *Global Positioning System - Signals, Measurements, and Performance*, Revised Second Edition, Ganga-Jamuna Press, 2012

Montenbruck, O. and Gill, E.: *Satellite Orbits: Models, Methods and Applications*, HAR/CDR edition, Springer, 2011

Navstar GPS Space Segment/Navigation User Interfaces, Interface Specification, IS-GPS-200H, GPS Directorate, 2013

Nurmi, J., Lohan, E.-S., Sand, S., and Hurskainen, H. (Eds): *GALILEO Positioning Technology*, Springer, 2015

Samper, J.-M., Lagunilla, J.-M., and (Author), Perez, R.-B.: *GPS and Galileo: Dual RF Front-end receiver and Design*, Fabrication, & Test, McGraw-Hill Education, 2008

Strang, G. and Borre, K.: *Algorithms for Global Positioning*, Wellesley-Cambridge Press, 2012

Thompson, E.-A., Clem, N., Renninger, I., and Loos, T.: *Software-defined GPS receiver on USRP-platform*, Journal of Network and Computer Applications 35, no. 4 pp. 1352-1360, 2012

Tsui, J.-B.-Y.: *Fundamentals of Global Positioning System Receivers: A Software Approach*, Second Edition, Wiley-Interscience, 2005

Wan, X. and Zhan, X.: *The Research of Indoor Navigation System Using Pseudolites*, Procedia Engineering 15 (2011), pp. 1446-1450, 2011

Woo, K.-T.: *Optimum Semicodeless Carrier–Phase Tracking of L2*, In Proc. of the 1999 International Technical Meeting of the Satellite Division of the Institute of Navigation, also appeared in Navigation 47, no. 2, pp. 82-99, 2000

References

GNSS Jamming, Meaconing, Spoofing, Security

Bonebrake C. and O'Neil, L.-R.: *Attacks on GPS Time Reliability*, IEEE Security & Privacy, May/June 2014, pp. 82-84, 2014

Chen, J., Zhang, S., Wang, H., and Zhang, X.: *Practicing a record-and-replay system on USRP*, In Proc. of the second workshop on Software radio implementation forum, pp. 61-64. ACM, 2013

Di, R.: *A USRP-base Flexible GNSS Signal Recording and Playback System: Performance Evaluation and Study*, M.Sc. Thesis, Miami University, Oxford, Ohio, 2013

Di, R., Peng, S., Taylor, S., and Morton, Y.: A *USRP-Based GNSS and Interference Signal Generator and Playback System*, In Position Location and Navigation Symposium (PLANS) 2012, pp. 470-478, IEEE, 2012

Dong, L.: *IF GPS Signal Simulator Development and Verification*, M.Sc. Thesis, University of Calgary, Alberta, 2003

Dovis, F. (Ed.): *GNSS Interference, Threats, and Countermeasures (Gnss Technology and Applications Series)*, Artech House Publishers, 2015

Hernandez, I.-G., Rodriguez, I., Tobias, G., Calle, J.-D., Carbonell, E., Seco-Granados, G., Simon, J., and Blasi, R.: *Galileo's Commercial Service - Testing GNSS High Accuracy and Authentication*, Inside GNSS, January/February 2015, pp. 38-48, 2015

Huang, L. and Yang, Q.: *GPS Spoofing - Low-cost GPS Simulator*, DEF CON 23, Las Vegas, August 6th - 9th, 2015

Humphreys, T.-E.: *Detection Strategy for Cryptographic GNSS Anti-spoofing,* IEEE Transactions on Aerospace and Electronic Systems, 49(2), pp. 1073-1090, 2013

Humphreys, T.-E., Ledvina, B.-M., Psiaki, M.-L., O'Hanlon, W.-O., and Kintner, P.-M., Jr.: *Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer*, In Proc. of the ION GNSS international technical meeting of the satellite division, vol. 55, p. 56. 2008

Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., Lachapelle, G.: *GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques*, International Journal of Navigation and Observation, 2012

McMilin, E.-B., Chen, Y.-H., De Lorenzo, D.-S., Akos, D.-M., Walter, T.-F., Lee, T.-H., Enge, P.-K.: *Single Antenna, Dual Use: Theory and Field Trial Results for Aerial Applications of Anti-Jam and Spoof Detection*, Inside GNSS, September/October 2015, pp. 40-53, 2015

Nighswander, T., Ledvina, B., Diamond, J., Brumley, R., and Brumley, D.: *GPS Software Attacks*, In Proc. of the 2012 ACM conference on Computer and communications security, pp. 450-461, ACM, 2012

References

GNSS Jamming, Meaconing, Spoofing, Security (cont.)

Perring, A., Canetti, R., Tygar, J.-D., and Song, D.: *The TESLA Broadcast Authentication Protocol*, In CryptoBytes, 5:2, Summer/Fall 2002, pp. 2-13, 2002

Rugamer, A., Stahl, M., Lukcin, I., Rohmer, G.: *Privacy Protected Localization and Authentication of Georeferenced Measurements using Galileo PRS*, In Position, Location and Navigation Symposium-PLANS 2014, 2014 IEEE/ION, pp. 478-486, IEEE, 2014

Shepard, D.-P. and Humphreys, T.-E.: *Characterization of Receiver Response to Spoofing Attack*, In Proc. of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation, p. 2608, 2011

Shepard, D.-P., Humphreys, T.-E., and Fansler, A.-A.: *Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks*, International Journal of Critical Infrastructure Protection 5, no. 3, pp. 146-153, 2012

Tippenhauer, N.-O., Pöpper, C., Rasmussen, K.-B., and Capkun, S.: *On the Requirements For Successful GPS Spoofing Attacks*, In Proc. of the 18th ACM conference on Computer and communications security, pp. 75-86. ACM, 2011

John A. Volpe National Transportation Systems Center: *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System*, Final Report for the Office of the Assistant Secretary for Transportation Policy, U.S. Department of Transportation, August 29, 2001

Wang, K., Chen, S., and Pan, A.: *Time and Position Spoofing with Open Source Projects*, BlackHat EU 2015, November 12th - 13th, 2015

Wesson, K., Rothlisberger, M., and Humphreys, T.: *Practical Cryptographic Civil GPS Signal Authentication*, Navigation, 59(3), pp. 177-193, 2012