Over-The-Air Radiometer (ORM)

ORM is a software and hardware solution that captures and analyzes radio signals in real-time to assist telco specialists with deep technical details to monitor the traffic. For non-technical users ORM can be used as “the best radio spot” meter to detect a better radio quality receiving location

Possible protocols are: 4G LTE, 5G NR, WiFi (802.11). Current v1.0.0 is specialized at 4G LTE only.

Glossary

HW	Hardware
eNB	4G LTE eNodeB base station
SDR	Software Defined Radio [HW]
UE	User Equipment (mobile phones, IoT devices etc.)
DL	Downlink (from eNB to UE)
UL	Uplink (from UE to eNB)
RF	Radiofrequency
I/Q	In-phase & quadrature numbers of digitized radio wave
L1 PHY	Physical layer of radio signal
L3 RRC	Radio resource control layer of radio signal
RSRQ	Reference signal received quality of UE
FDD	Frequency division duplex requires different RF on DL and UL

For whom and why?

- Radio Frequency Service
  - One of main KPI: technical quality control of radio communication and TV broadcasting

- Telecommunication Operators
  - Troubleshooting & monitoring radio traffic

- Construction Companies with own RF infra
  - Monitoring radio traffic, UE heatmap data

- Market business
  - UE heatmap data per time, density of potential customers in specified location

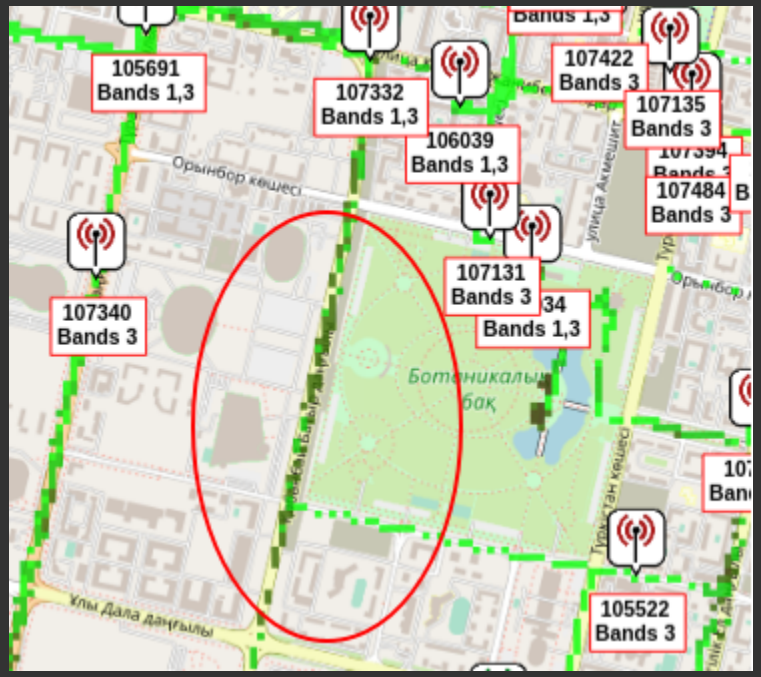
Product advantages

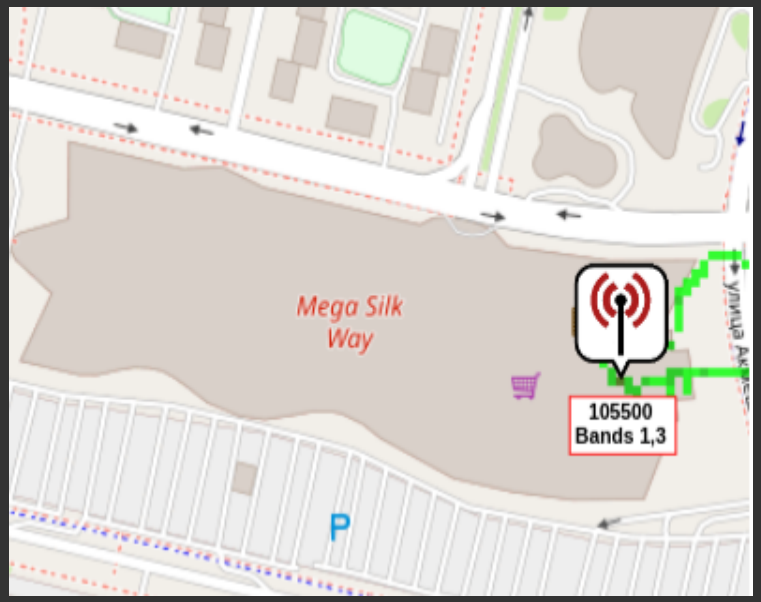
- Subject complexity: radio and 4G LTE in particular is a complex, advance subject to deal with (ORM is not the innovation, but rather a simpler solution of complex subject)
  - only few world competitors can actually decode radio traffic, especially in real-time

- Cost: ORM's HW components which are SDR, analog components' net cost is much lower than competitors' black-box solution

- Flexibility: ORM HW components can operate as radiometer, eNB or UE emulator with variety of supported radio protocols

Problem





How to know the reasons for a bad radio signal and improve it in the current location?

- get closer to eNB in the hope of getting a better radio signal quality
- request Telco support to mount a new eNB closer to the location
- request Telco to give higher bandwidth to improve data rate

What about if there is an eNB in close proximity in crowded places like malls and RSRQ is excellent but the data rate is slow?

Solid solution in 3 words:
capture, decode, analyze

Over-The-Air Radiometer (ORM)

for 4G LTE communications

1

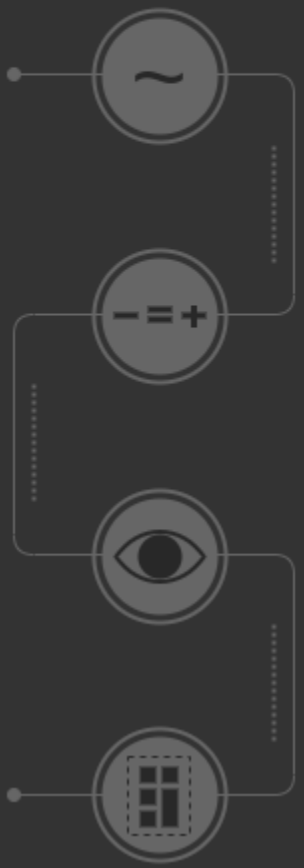
OTA Capture

Capture DL, UL via SDR in real-time on fixed RF

2

Decoding

Demodulation & L1-L3 decoding of UE control & data channels with all tech detailed information



3

Monitoring

Dashboard with deep technical details per UE each 1 ms - 10 ms, correlated with graphs

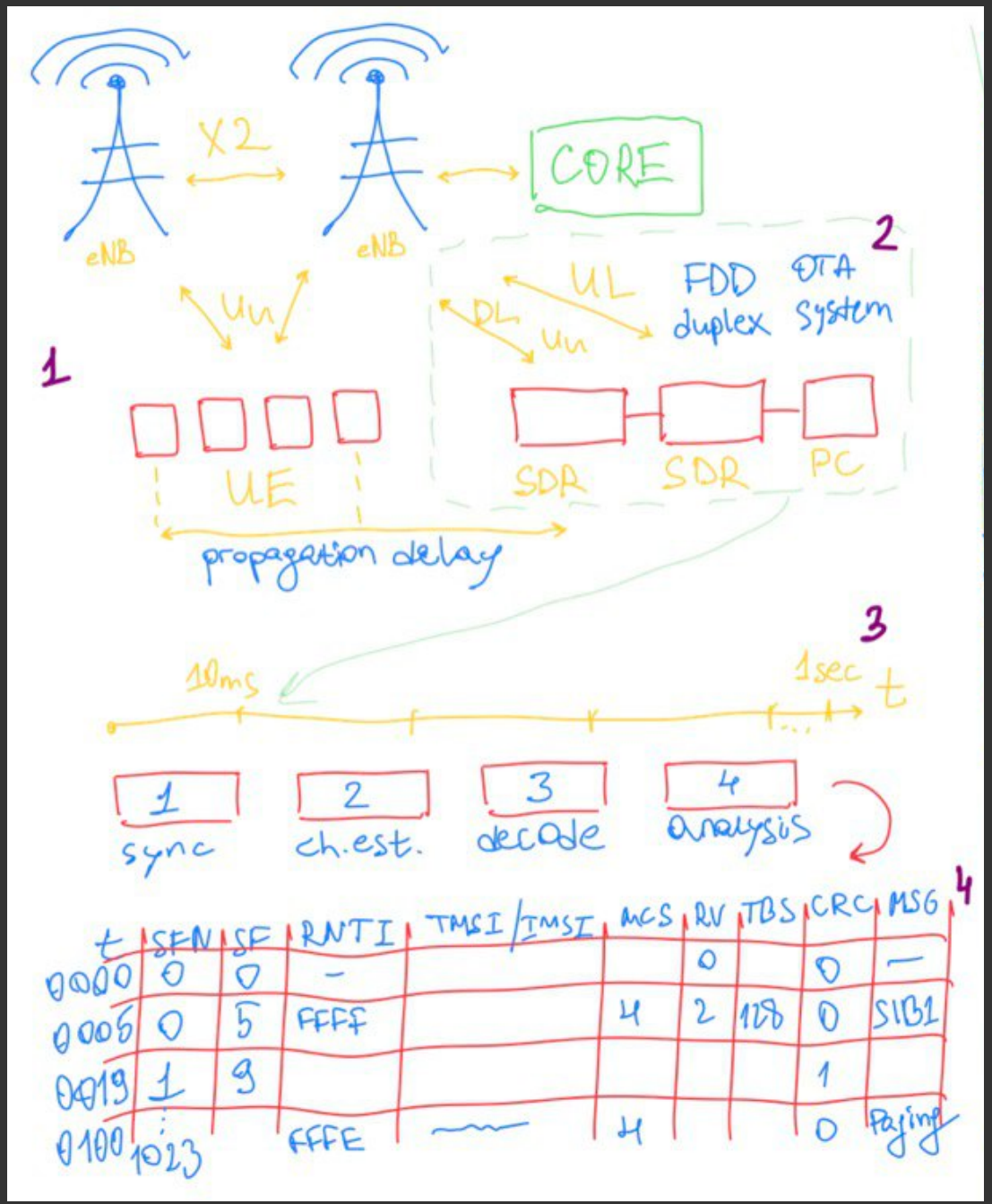
4

Statistics

Provide number of UEs, calculate their data rate and RSRQ, Rx etc.

v1.0.0

How does ORM work?



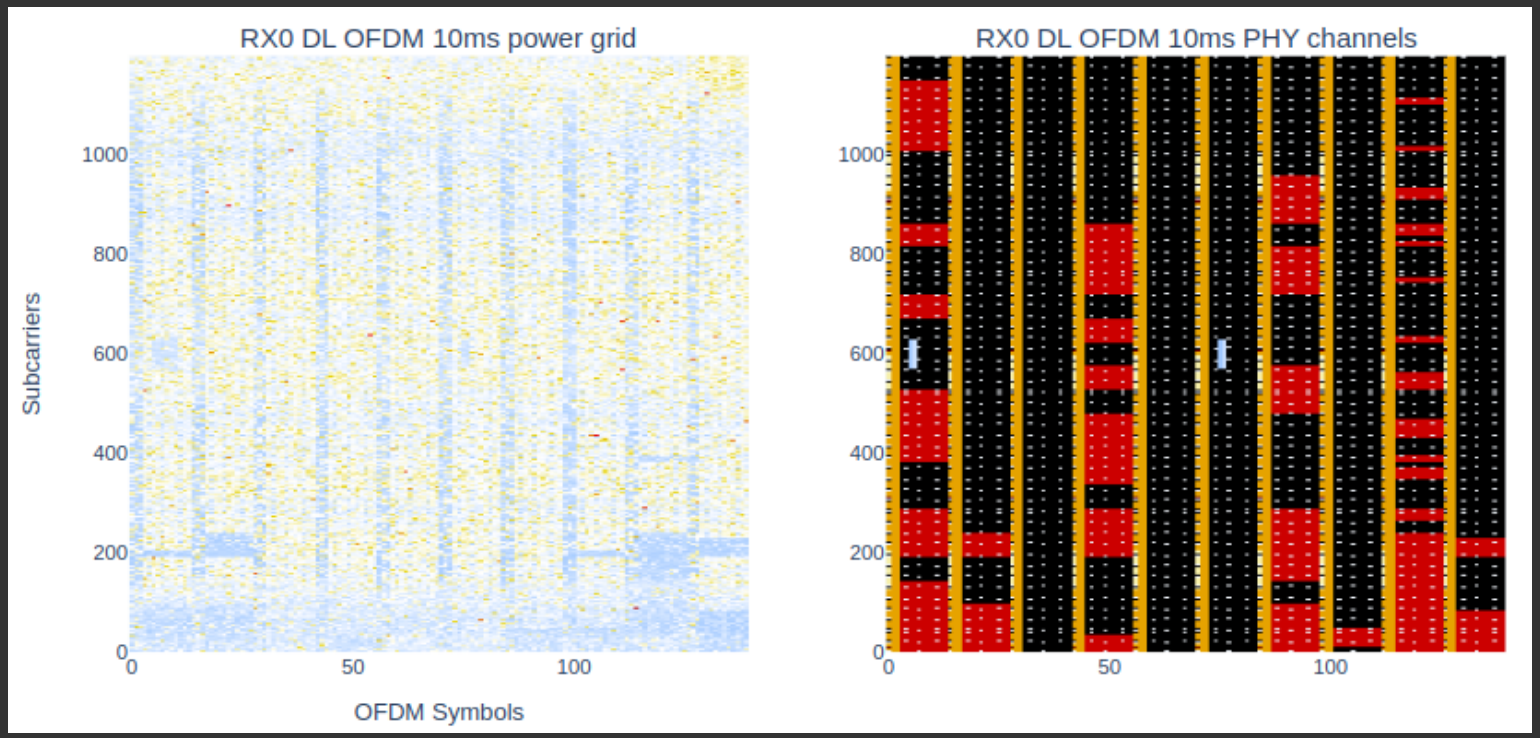
1. Standard E-UTRAN 4G architecture, where several eNB stations communicate with each other via X2 interface and receive and transmit radio traffic Uu.

2. In FDD duplex mode, ORM system uses a separate SDR for DL and for UL frequencies. Scalable up to 2x2, 4x4 MIMO. Propagation delay and obstacles between distances of ORM SDR and UEs affect decoding results.

3. Real-time process of captured signal with freq. and time sync up to decoded L1 PHY and L3 RRC protocol analysis.

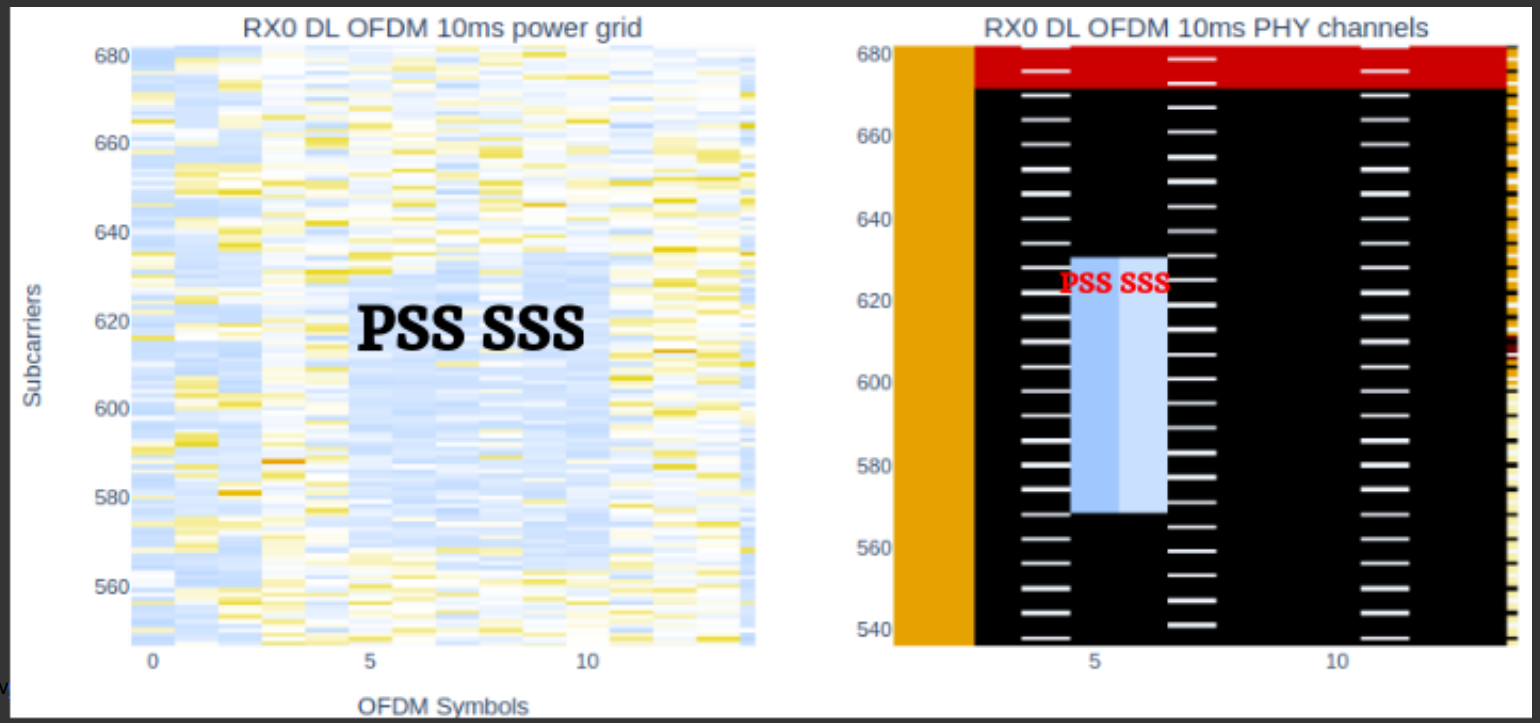
4. Monitoring dashboard with complete technical details for statistics and analysis.

Monitoring traffic load



Stored data can be replayed for analysis.

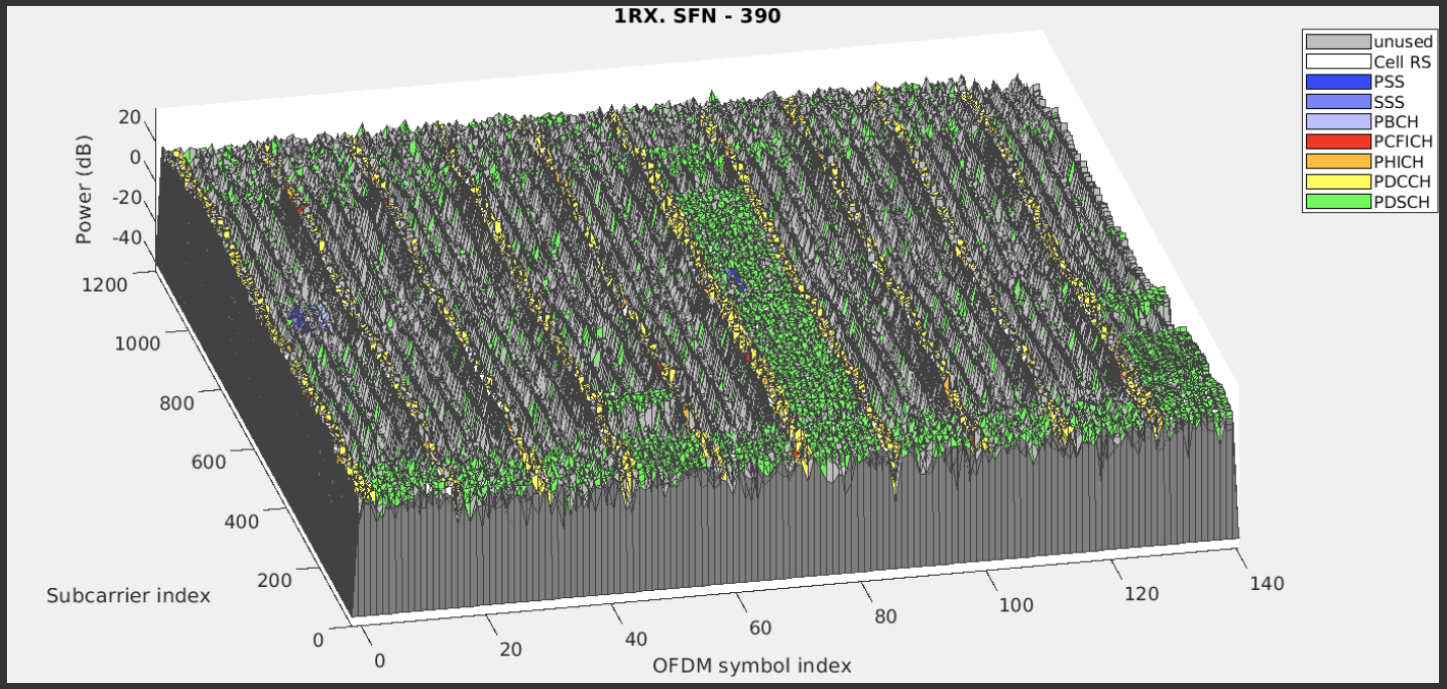
In the 1st picture blue regions show higher Power in dB, meaning the most data is transmitted there.



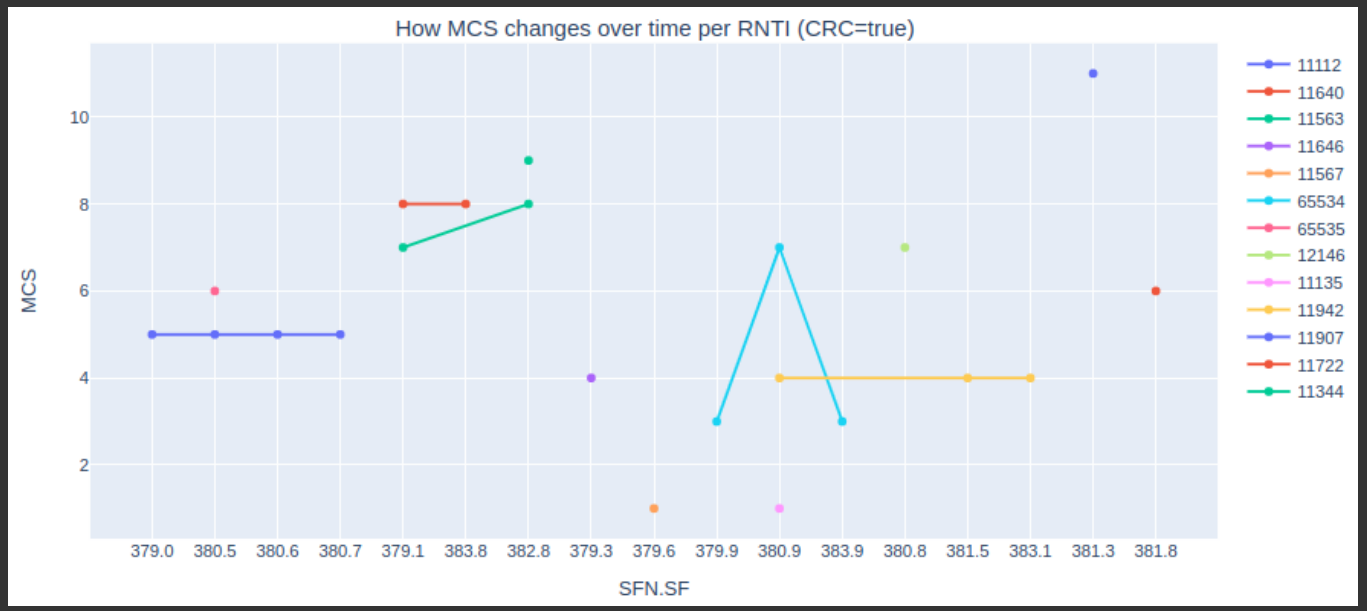
Zoom in to the tiniest 1x1 cell in a 10 ms matrix.

Easily monitor specific PHY channels like PDSCH, PDCCH, PCFICH etc.

Monitoring your traffic from 1 ms to 1 second

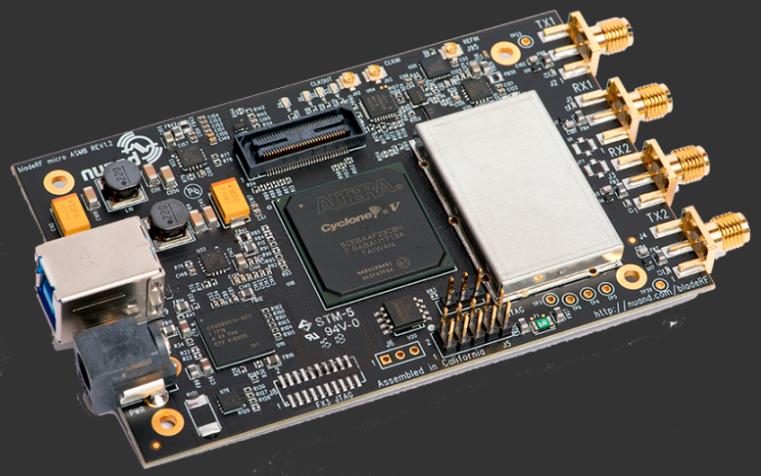


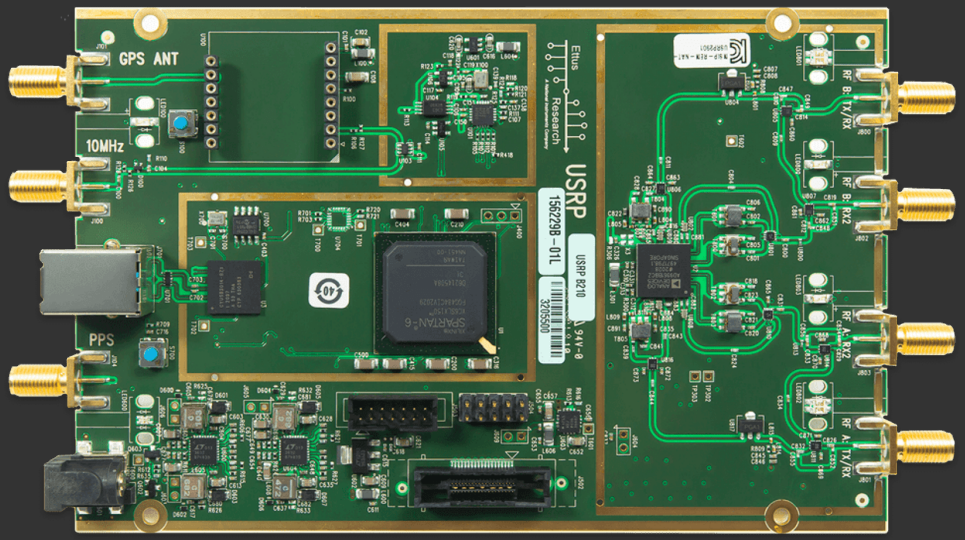
Here another view of power grid with PHY channels in a single picture



v1.0.0

Current solution - DL only





- SDR Nuand bladeRF 2.0 micro xA9. 2x2 MIMO. Costs $860 (personal)
  or
  SDR Ettus USRP B210. 2x2 MIMO. Costs $2100 (borrowed)

- Lenovo Thinkpad X1 Carbon Gen6 with i7-8650U, 1.90GHz

- Due to Kazakhstan has only FDD type 4G LTE, DL and UL have different frequencies. Listed SDRs have 1x local oscillator (LO) to capture in 1 or 2 Rx antennas a fixed frequency. Current ORM v1.0.0 can capture only DL frequency from eNB and decode L1 to L3 protocols in real-time for fixed transmission modes (TM). There is no information about what UEs transmits to eNB, meaning we can't "hear" what users are actually saying.

Why are only fixed TMs supported for v1.0.0?

Because there are MIMO features that require UE feedback, e.g. you can not decode DL without knowing UE selected configuration that's transmitted to eNB in the UL channel.

Which means that if you can capture both DL & UL and decode them, ORM can support TM1-10 types, e.g. all UEs in the current location are captured.

v1.0.0

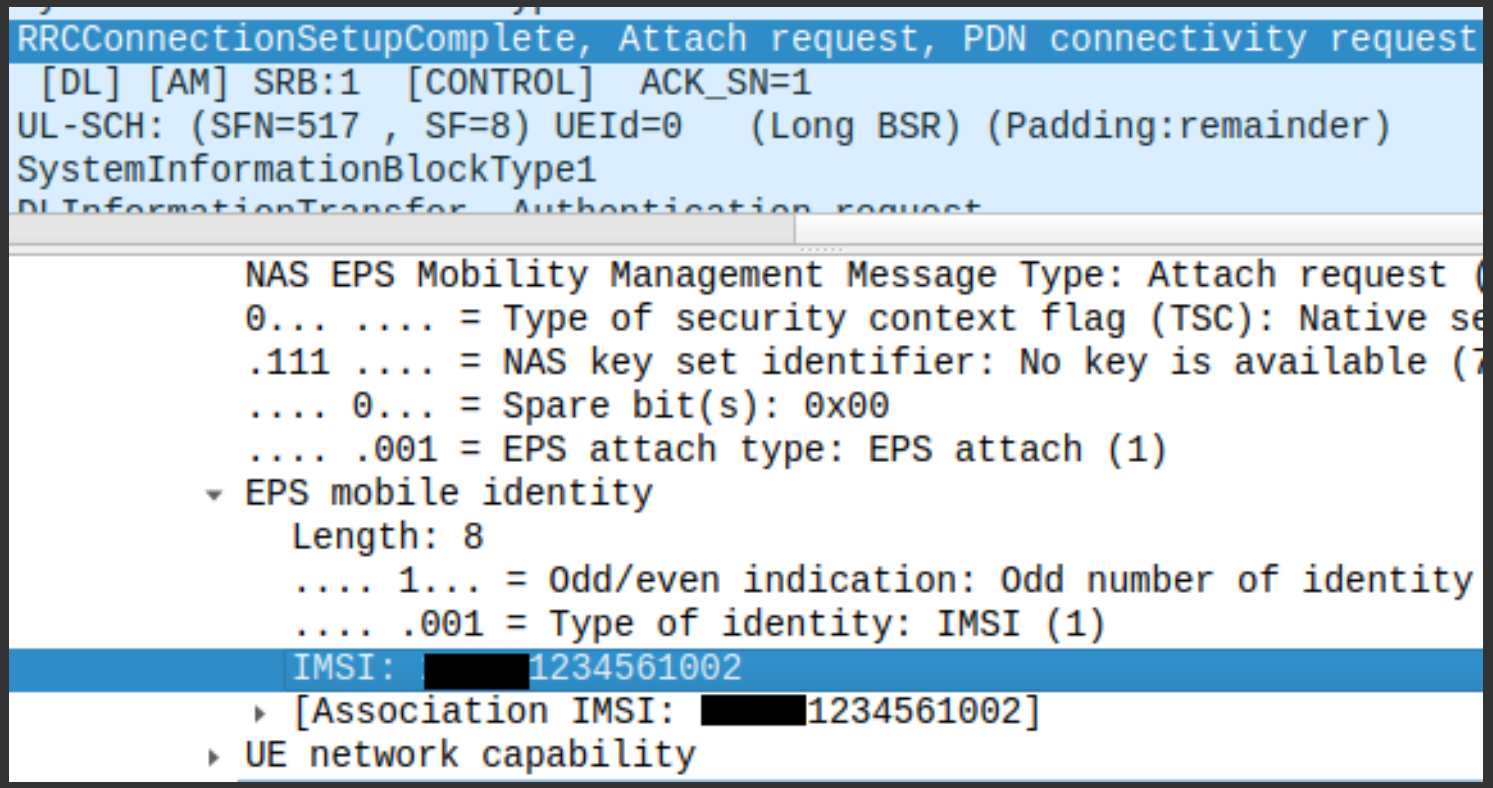
What's required to do full DL & UL decoding?

1. 2x bladeRF for DL & UL
   - Need external analog GPSDO module to sync them
   - Costs: 2 x $860 + 1 x $3325 = $5045
2. 2x USRP B210 for DL & UL
   - Also need an external GPSDO module to sync
   - Costs: 2 x $2101 + 1 x $3325 = $7527
3. 1x USRP X310 with 2x LO that can capture DL & UL at the same time
   - No external GPSDO module
   - Outperforms 2x USRP B210 due to frontend capabilities
   - Costs: 1 x $9353 = $9353

	BW	Frequency range	LO	Rx SMA ports	Need GPSDO	Cost
bladeRF micro xA9	56 MHz, 14-bit 122 MHz, 8-bit	47 MHz - 6 GHz	1	2	Yes	$5045
USRP B210	56 MHz, 14-bit	70 MHz - 6 GHz	1	2	Yes	$7527
USRP X310	160 MHz	70 MHz - 6 GHz	2	2	No	$9353

What are the benefits of UL decoding?

- UE capabilities profiling
- UE CSI reports (feedback), e.g. UE sends its channel state, SINR from eNB etc.
- All L3 RRC messages (MIB, SIB1/2/x, Attach Req/Resp, Auth Req/Resp etc.)
- C-RNTI -> TMSI -> IMSI mapping
- UE Kc session's SRAND for decryption
    - note that without Kc stored on UE SIM card it's impossible decrypt UE data



SDR for 4G LTE AND for 5G NR

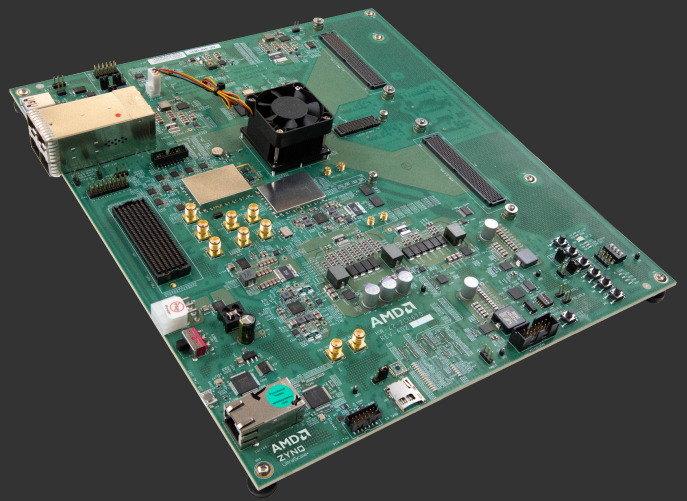
If you see this project (ORM) can grow to 5G NR with 100 MHz bandwidth, where 4G LTE has 20 MHz in a single carrier, and 4G LTE-Advanced with 5x20 MHz carriers aggregated.

5G NR has 2 frequency ranges:

- FR1 - also known as sub-6GHz frequency range
- FR2 - also known as mmWave, for example, 27.4 - 27.8 GHz (400 MHz bandwidth)

We've seen USRP X310 is suitable for 100 MHz bandwidth for 5G NR FR1.

Xilinx RFSoC (where ADC/DAC are in single SoC) is revolutional method to process 4G, 5G signals. There are variations of them with different characteristics but ZCU670 can do FR1 and FR2. Note that for FR2 additional analog front-end are required.

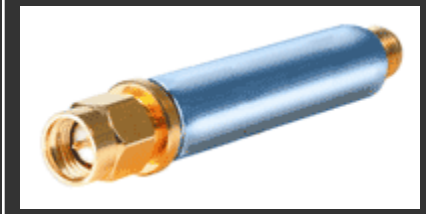


Xilinx RFSoC DFE ZCU670 devboard: $12954

- 8x ADC with direct-RF 7.125 GHz bandwidth
- 400 MHz iBW (for FR2)
- Target applications:
  - 5G massive-MIMO, mmWave
  - Aerospace & defense
  - Test & measurement

v1.0.0

Additional analog improvements

	bandpass filter (BPF)	allow signals within a specific frequency range to pass through while attenuating signals outside of that range.
	Low noise amplifier (LNA)	amplify weak signals without adding significant noise. The "Low Noise" part of the name emphasizes that the primary design criterion for the amplifier is to keep its own internally-generated noise as low as possible.
	Mixer + synthesizer	multiply two signals, which in the RF world typically results in the generation of sum and difference frequencies. This is used to translate signals from one frequency to another.

Additional idea - ORM as eNB, UE emulation

For lab & testbed purposes, eNB and UE can be emulated via SDR receiving Rx and transmitting Tx data.

In other words, build your own test eNB and test UE to perform tests and measurements.

Summary

Current:

- ORM v1.0.0 is capable of capturing, decoding in real-time 4G LTE DL only
  - Software is implemented via C/C++
- TM1 (SISO), TM2 (TxDiversity) are supported
- Decoded L2 MAC, L3 RRC layers in PCAP
- Script to visualize features of decoded data

What's required to do:

- Support 4G LTE UL with additional or improved SDR
- Support 4G LTE all transmission modes if business is required. TM1 - TM10
- Support 4G LTE Carrier Aggregation if business is required
- Support ORM for 5G NR
  - Implement software for capturing, decoding in C/C++
  - Alternative way to implement some logics on FPGA due to high-bandwidth