Openwifi

Open-source WiFi chip progress and future plan

Fosdem 2022, online

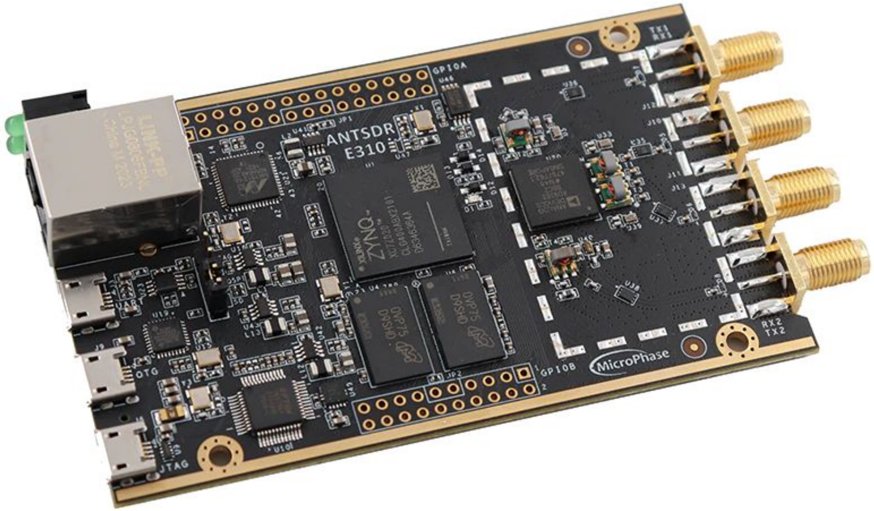
Xianjun Jiao
IDLab, imec - Gent university

What is openwifi?

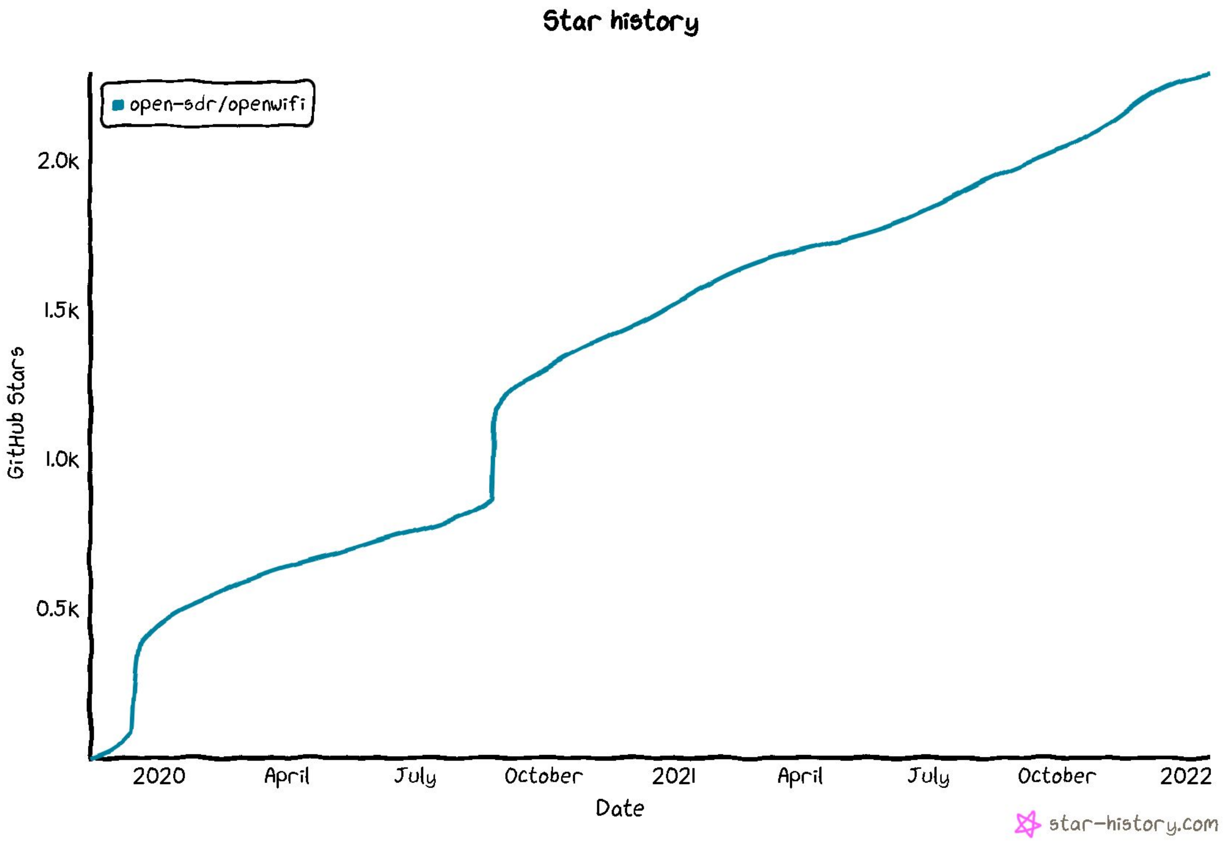
- https://github.com/open-sdr
  - https://github.com/open-sdr/openwifi
  - https://github.com/open-sdr/openwifi-hw
  - https://github.com/open-sdr/openofdm

The open source WiFi chip design.

Already functioning like COTS WiFi chip on FPGA platform.



https://star-history.com/#open-sdr/openwifi&Date



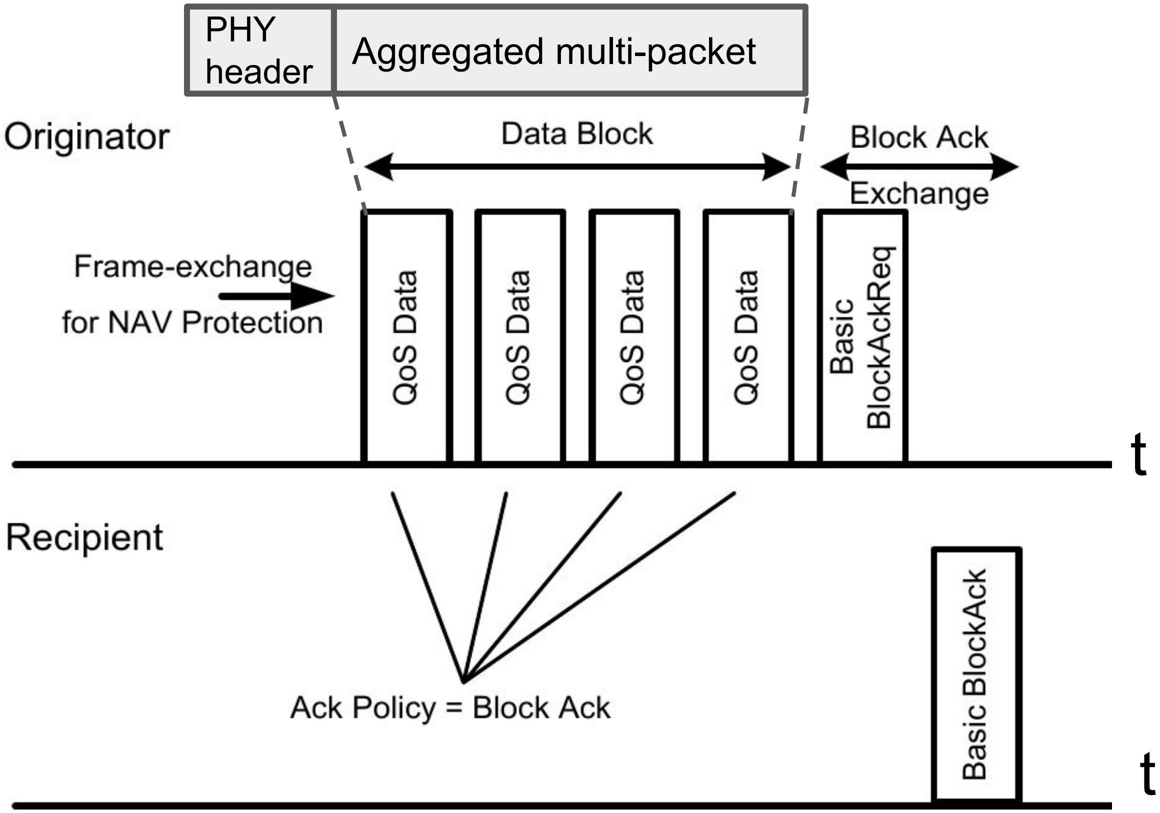
Openwifi project in 2021

- ***Features/optimizations***
- Bug fixes
- RF performance measured by Rohde & Schwarz CMW 270
- Community growth
  - New hardwares
  - New papers/applications
- Current focus
  - Optimization for maturity
  - 802.11ax/WiFi6
- Future plan

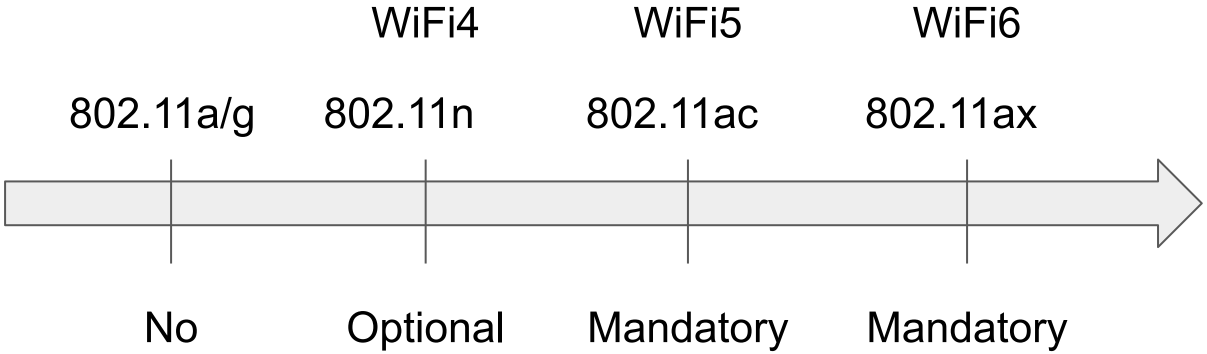
Openwifi features/optimizations 2021

- ***AMPDU and Block ACK***
- Security
  - Ack control in monitor/injection mode (issue 59)
  - CSI fuzzer (app note)
  - Owfuzz (external)
- Simple TX diversity (CSD)
- Enhancements/optimizations
  - FPGA level deep statistics: STF, LTF, header, packet, etc.
  - RF: Full chain (clock/filter/offset-tuning/self-interference-control/etc) optimization
  - PHY RX: Common Phase Error tracking; Sampling Frequency Offset correction.
  - PHY RX: LTF correlation 16->32; Phase rotation steps/precision: 256->512; etc.
  - I/Q capture: Free-running mode; TX I/Q internal loopback

Openwifi features/optimizations 2021: AMPDU, Block ACK

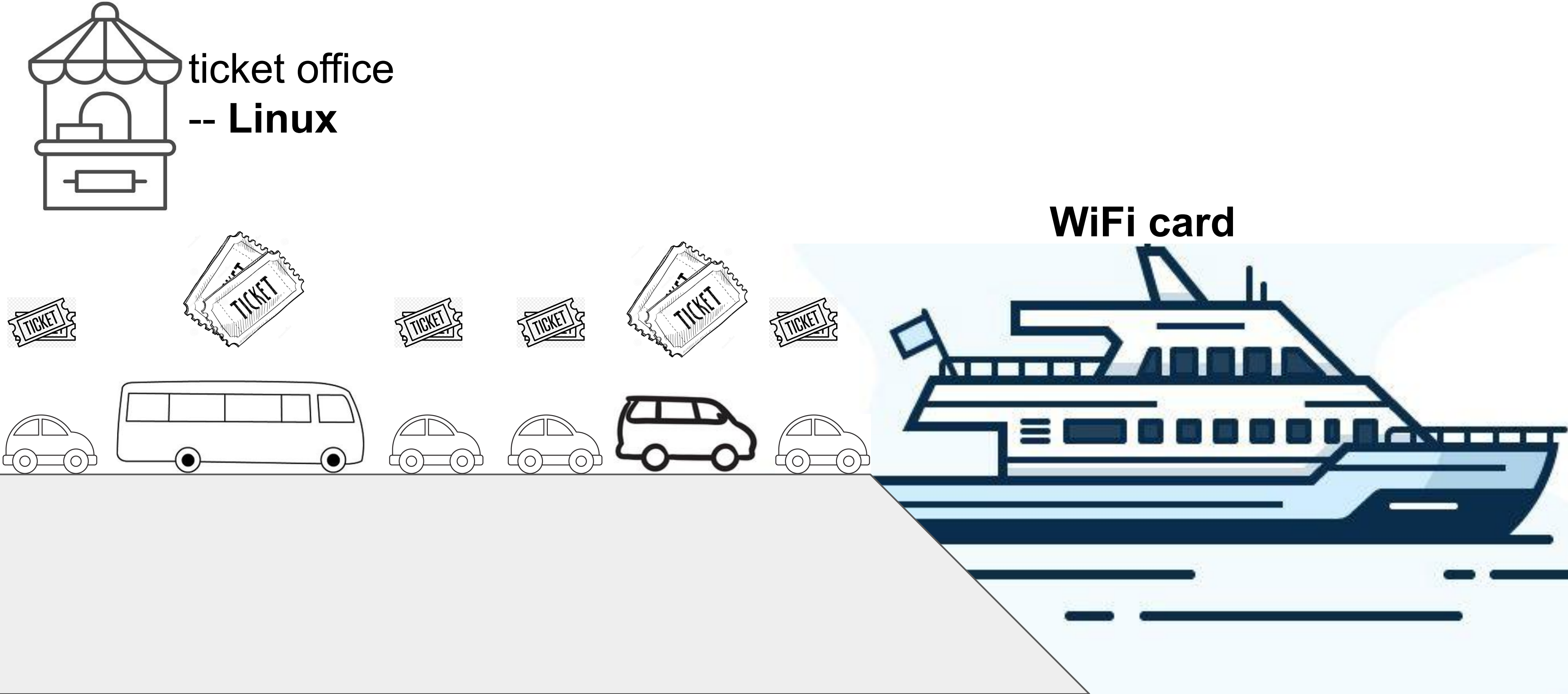


Openwifi features/optimizations 2021: AMPDU, Block ACK



	WiFi4	WiFi5	WiFi6
802.11a/g	802.11n	802.11ac	802.11ax
No	Optional	Mandatory	Mandatory

Openwifi features/optimizations 2021: AMPDU, Block ACK



ticket office
-- **Linux**

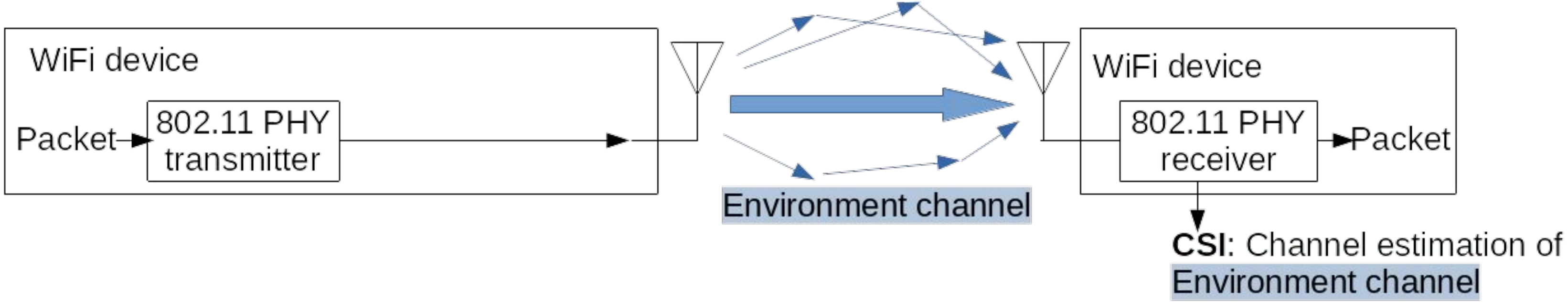
WiFi card

Openwifi features/optimizations 2021

- AMPDU and Block ACK
- Security
  - Ack control in monitor/injection mode (issue 59)
  - ***CSI fuzzer (app note)***
  - Owfuzz (external)
- Simple TX diversity (CSD)
- Enhancements/optimizations
  - FPGA level deep statistics: STF, LTF, header, packet, etc.
  - RF: Full chain (clock/filter/offset-tuning/self-interference-control/etc) optimization
  - PHY RX: Common Phase Error tracking; Sampling Frequency Offset correction.
  - PHY RX: LTF correlation 16->32; Phase rotation steps/precision: 256->512; etc.
  - I/Q capture: Free-running mode; TX I/Q internal loopback

Openwifi features/optimizations 2021: CSI fuzzer

https://github.com/open-sdr/openwifi/blob/master/doc/app_notes/csi_fuzzer.md



WiFi device

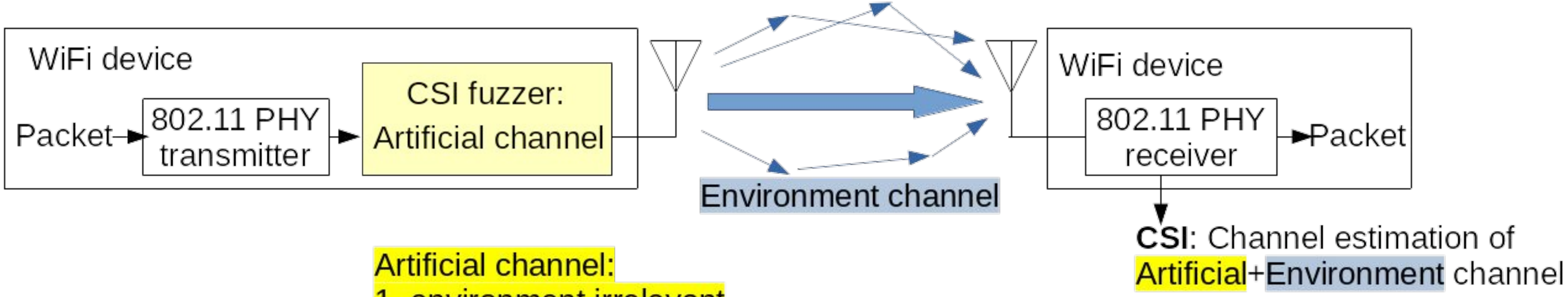
Packet → 802.11 PHY transmitter

Environment channel

WiFi device

802.11 PHY receiver → Packet

CSI: Channel estimation of Environment channel



WiFi device

Packet → 802.11 PHY transmitter → CSI fuzzer: Artificial channel

Environment channel

WiFi device

802.11 PHY receiver → Packet

CSI: Channel estimation of Artificial+Environment channel

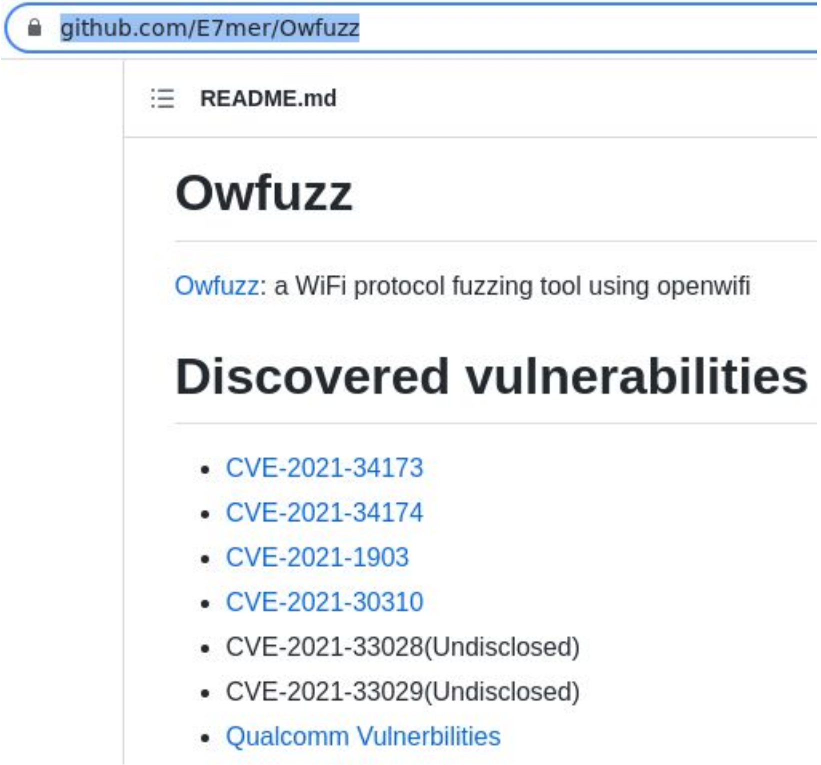
Artificial channel:
1. environment irrelevant
2. unknown to unauthorized receiver!

Openwifi features/optimizations 2021

- AMPDU and Block ACK
- Security
  - Ack control in monitor/injection mode (issue 59)
  - CSI fuzzer (app note)
  - ***Owfuzz (external)***
- Simple TX diversity (CSD)
- Enhancements/optimizations
  - FPGA level deep statistics: STF, LTF, header, packet, etc.
  - RF: Full chain (clock/filter/offset-tuning/self-interference-control/etc) optimization
  - PHY RX: Common Phase Error tracking; Sampling Frequency Offset correction.
  - PHY RX: LTF correlation 16->32; Phase rotation steps/precision: 256->512; etc.
  - I/Q capture: Free-running mode; TX I/Q internal loopback

Openwifi features/optimizations 2021: Owfuzz

https://github.com/alipay/Owfuzz https://github.com/E7mer/Owfuzz



Owfuzz

Owfuzz: a WiFi protocol fuzzing tool using openwifi

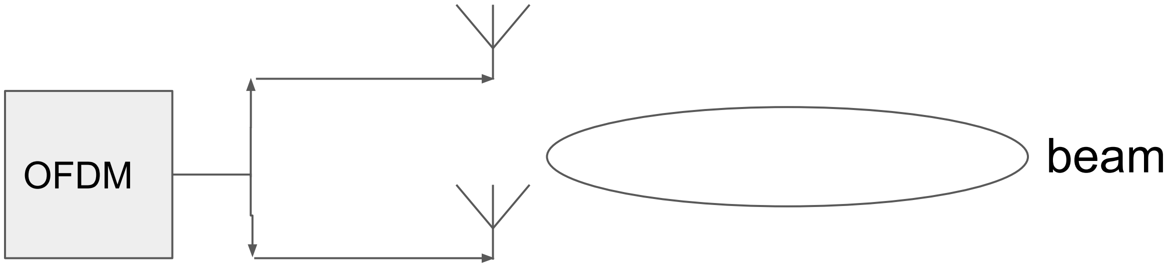
Discovered vulnerabilities

- CVE-2021-34173
- CVE-2021-34174
- CVE-2021-1903
- CVE-2021-30310
- CVE-2021-33028(Undisclosed)
- CVE-2021-33029(Undisclosed)
- Qualcomm Vulnerbilities

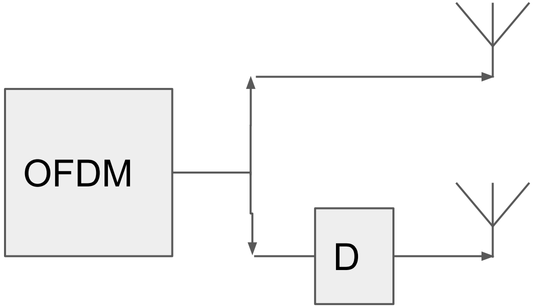
Openwifi features/optimizations 2021

- AMPDU and Block ACK
- Security
  - Ack control in monitor/injection mode (issue 59)
  - CSI fuzzer (app note)
  - Owfuzz (external)
- ***Simple TX diversity (CSD)***
- Enhancements/optimizations
  - FPGA level deep statistics: STF, LTF, header, packet, etc.
  - RF: Full chain (clock/filter/offset-tuning/self-interference-control/etc) optimization
  - PHY RX: Common Phase Error tracking; Sampling Frequency Offset correction.
  - PHY RX: LTF correlation 16->32; Phase rotation steps/precision: 256->512; etc.
  - I/Q capture: Free-running mode; TX I/Q internal loopback

Openwifi features/optimizations 2021: Simple TX diversity



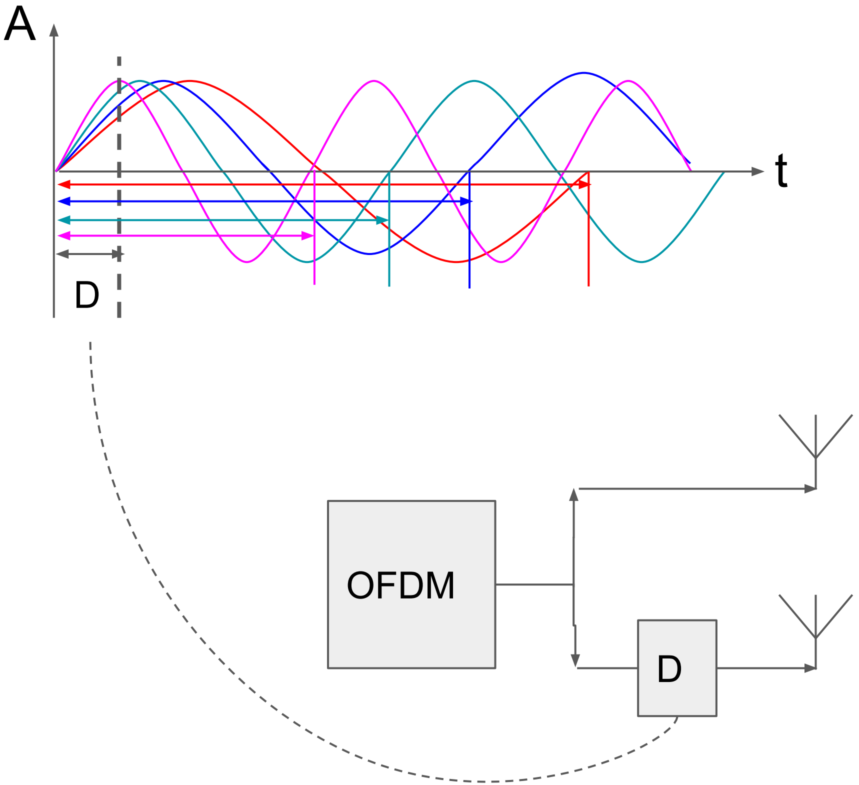
Openwifi features/optimizations 2021: Simple TX diversity



?

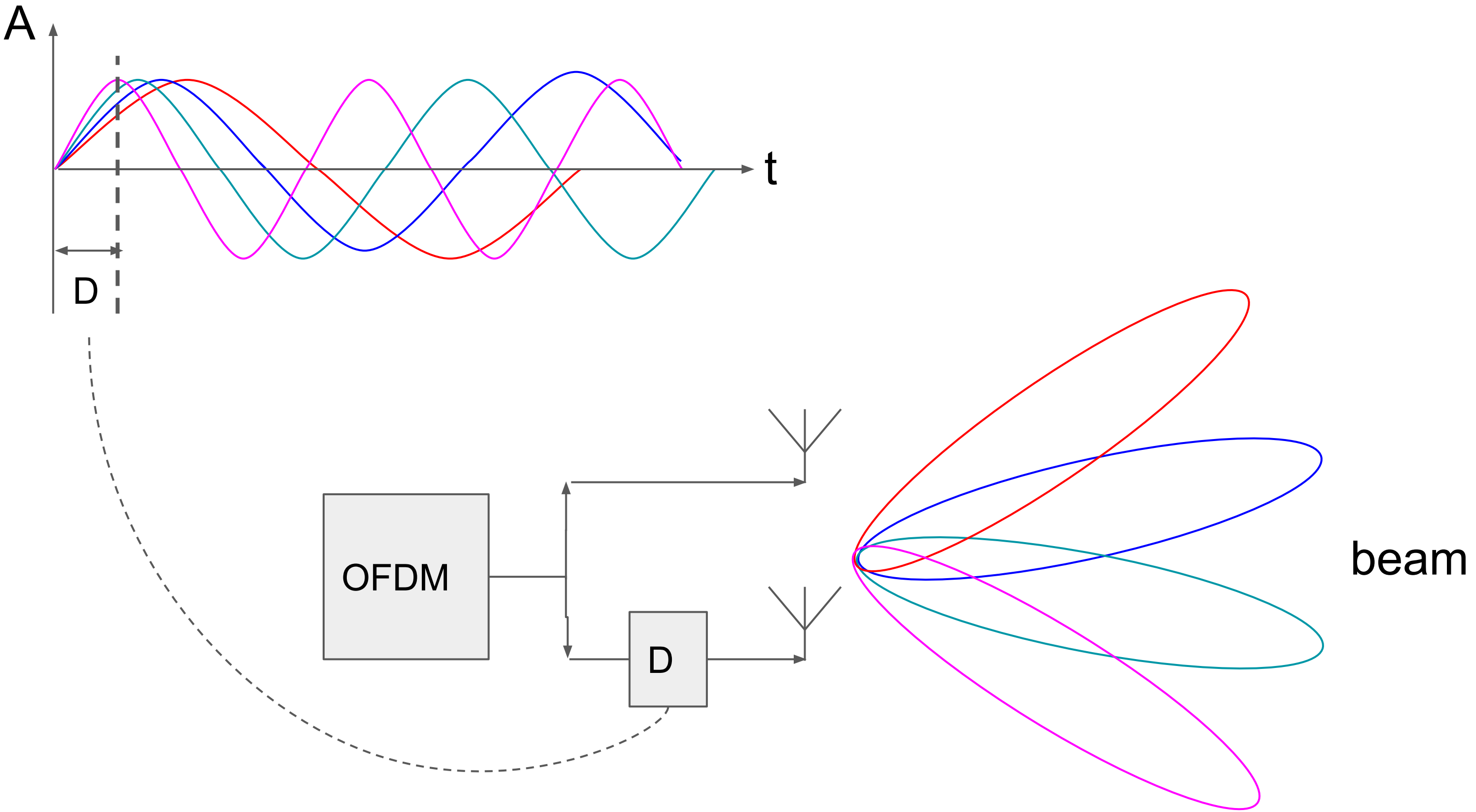
beam

Openwifi features/optimizations 2021: Simple TX diversity



beam

Openwifi features/optimizations 2021: Simple TX diversity

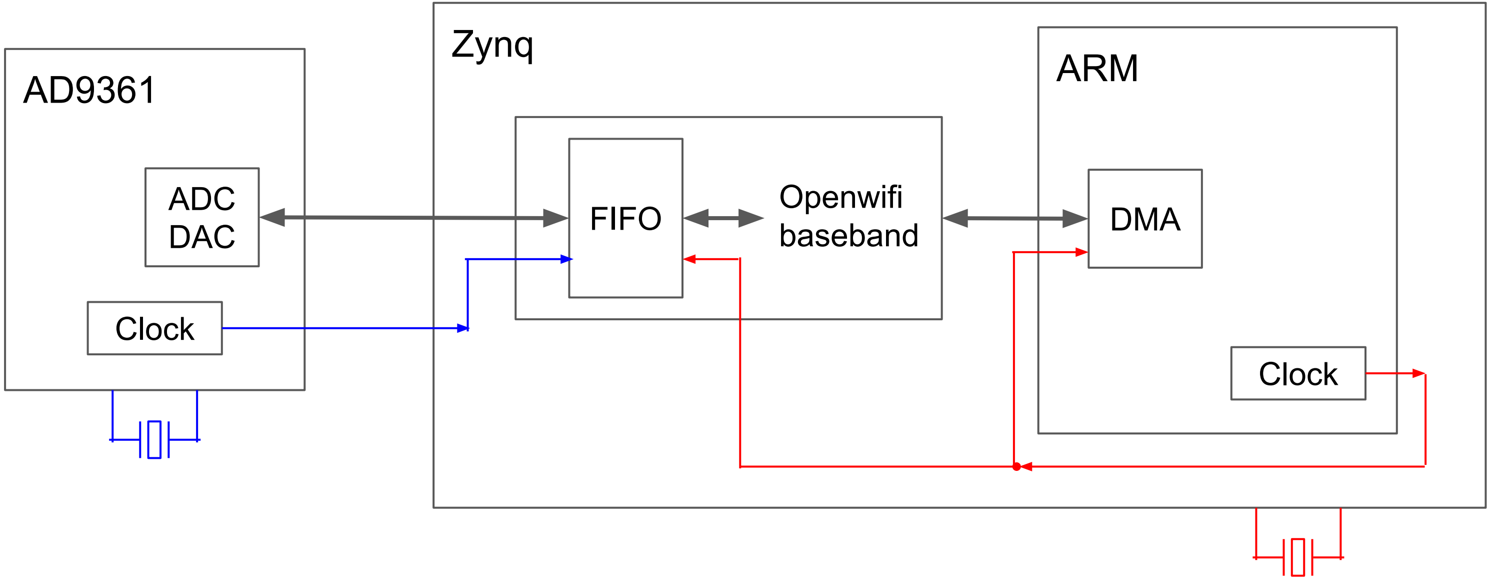


Openwifi features/optimizations 2021

- AMPDU and Block ACK
- Security
  - Ack control in monitor/injection mode (issue 59)
  - CSI fuzzer (app note)
  - Owfuzz (external)
- Simple TX diversity (CSD)
- ***Enhancements/optimizations***
  - FPGA level deep statistics: STF, LTF, header, packet, etc.
  - RF: Full chain (clock/filter/offset-tuning/self-interference-control/etc) optimization
  - PHY RX: Common Phase Error tracking; Sampling Frequency Offset correction.
  - PHY RX: LTF correlation 16->32; Phase rotation steps/precision: 256->512; etc.
  - I/Q capture: Free-running mode; TX I/Q internal loopback

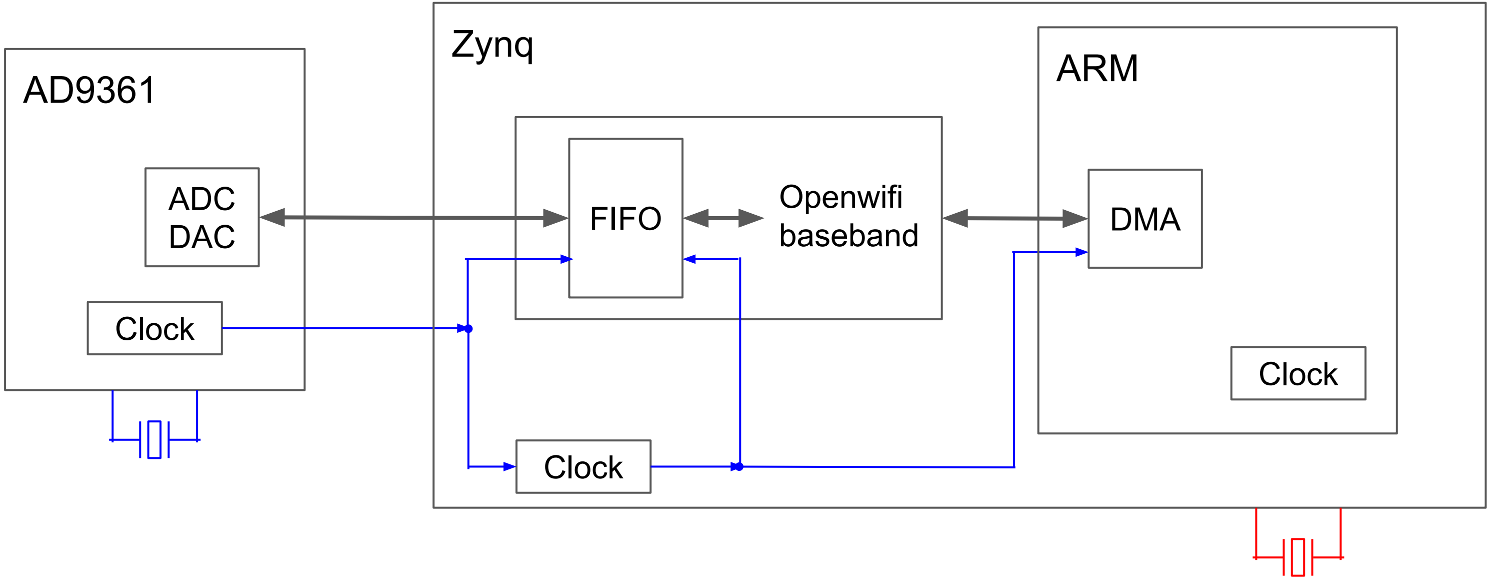
Openwifi features/optimizations 2021: the clock

Before



Openwifi features/optimizations 2021: the clock

Now



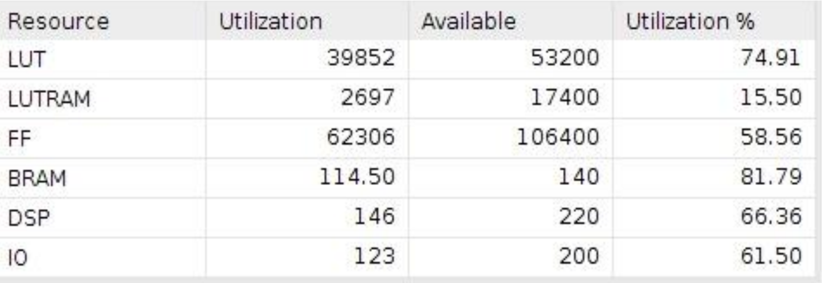
Openwifi features/optimizations 2021

- Improvement for easy project-build and use
  - Less steps for the FPGA project generation by more powerful scripts.
  - Easy setting by user space tool: LBT threshold; TRX antenna; TX power; MCS (HT and non-HT); Short GI; Extra freq-offset;
  - Add test mode driver option for experimental/temporary feature.
  - Etc; etc; etc....

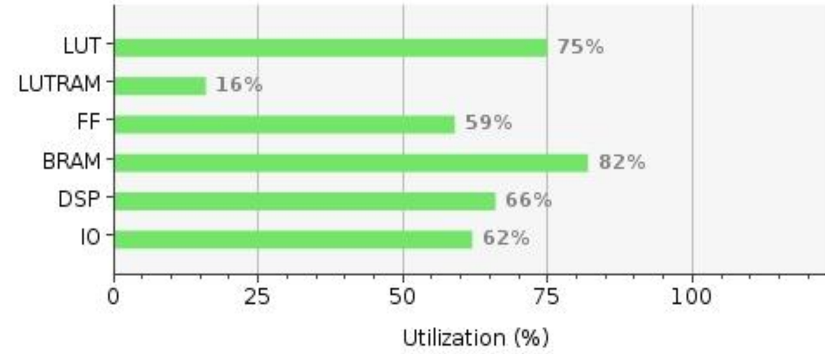
Openwifi features/optimizations 2021

- Less FPGA occupancy, while having more features!

Release **Leuven** (Dec. 2020)

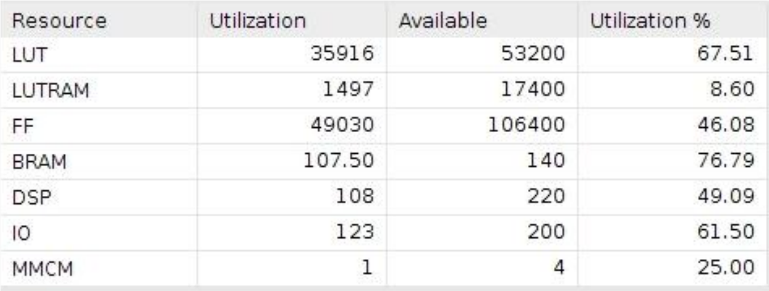


Resource	Utilization	Available	Utilization %
LUT	39852	53200	74.91
LUTRAM	2697	17400	15.50
FF	62306	106400	58.56
BRAM	114.50	140	81.79
DSP	146	220	66.36
IO	123	200	61.50

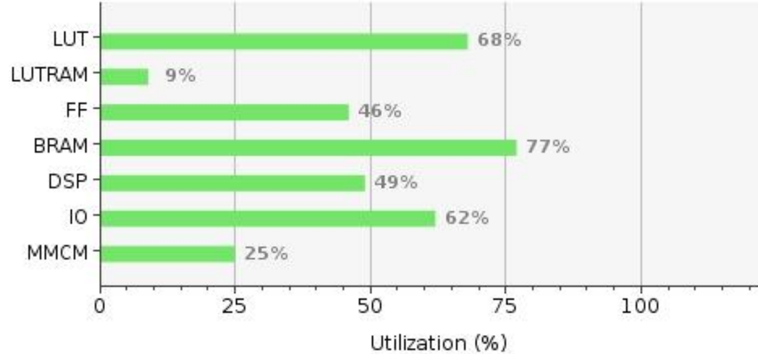


LUT -10%
FF -21%
BRAM -6%
DSP -26%

Release **Wilsele** (Feb. 2022)



Resource	Utilization	Available	Utilization %
LUT	35916	53200	67.51
LUTRAM	1497	17400	8.60
FF	49030	106400	46.08
BRAM	107.50	140	76.79
DSP	108	220	49.09
IO	123	200	61.50
MMCM	1	4	25.00



Openwifi features/optimizations 2021

Wilsele

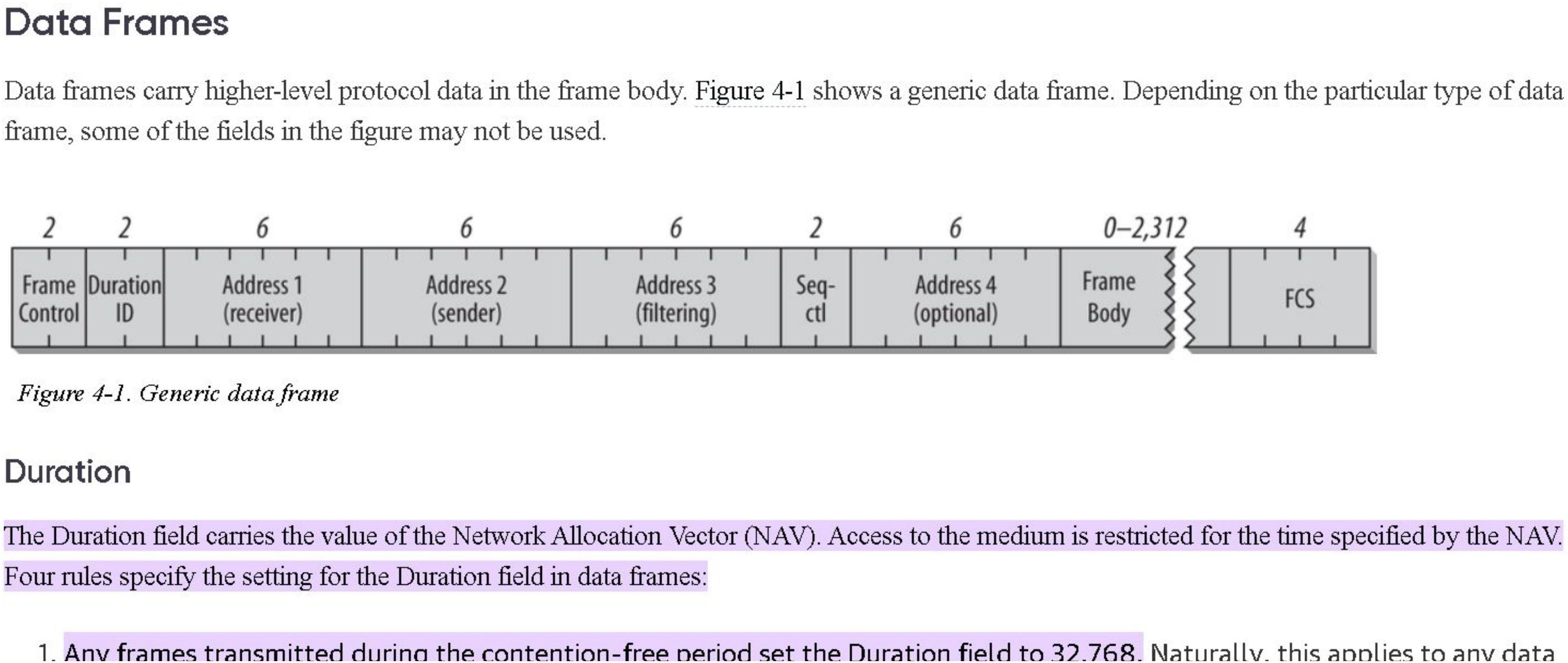
Openwifi project in 2021

- Features/optimizations
- ***<u>Bug fixes</u>***
- RF performance measured by Rohde & Schwarz CMW 270
- Community growth
  - New hardwares
  - New papers/applications
- Current focus
  - Optimization for maturity
  - 802.11ax/WiFi6
- Future plan

Openwifi bug fixes 2021

- ***Duration field of the HT (WiFi4) packet***
  - ***The Linux kernel only do this for 11a/g***
- CW increment mechanism: not by busy, but by actual failed TX
- A new PHY tx is wrongly initiated before the end of previous PHY tx
- Timestamp issue with I/Q capture (issue 122)
- HT STF power level correction
- Bugs around the asynchronous nature of FPGA-CPU interaction
  - FPGA queue <--> ring buffer in the driver <--> Linux mac80211
- Etc.
- Etc.
- Etc.
- ...

Openwifi bug fixes 2021: Duration field for HT (WiFi4)



Data Frames

Data frames carry higher-level protocol data in the frame body. Figure 4-1 shows a generic data frame. Depending on the particular type of data frame, some of the fields in the figure may not be used.

2	2	6	6	6	2	6	0–2,312	4
Frame Control	Duration ID	Address 1 (receiver)	Address 2 (sender)	Address 3 (filtering)	Seq-ctl	Address 4 (optional)	Frame Body	FCS

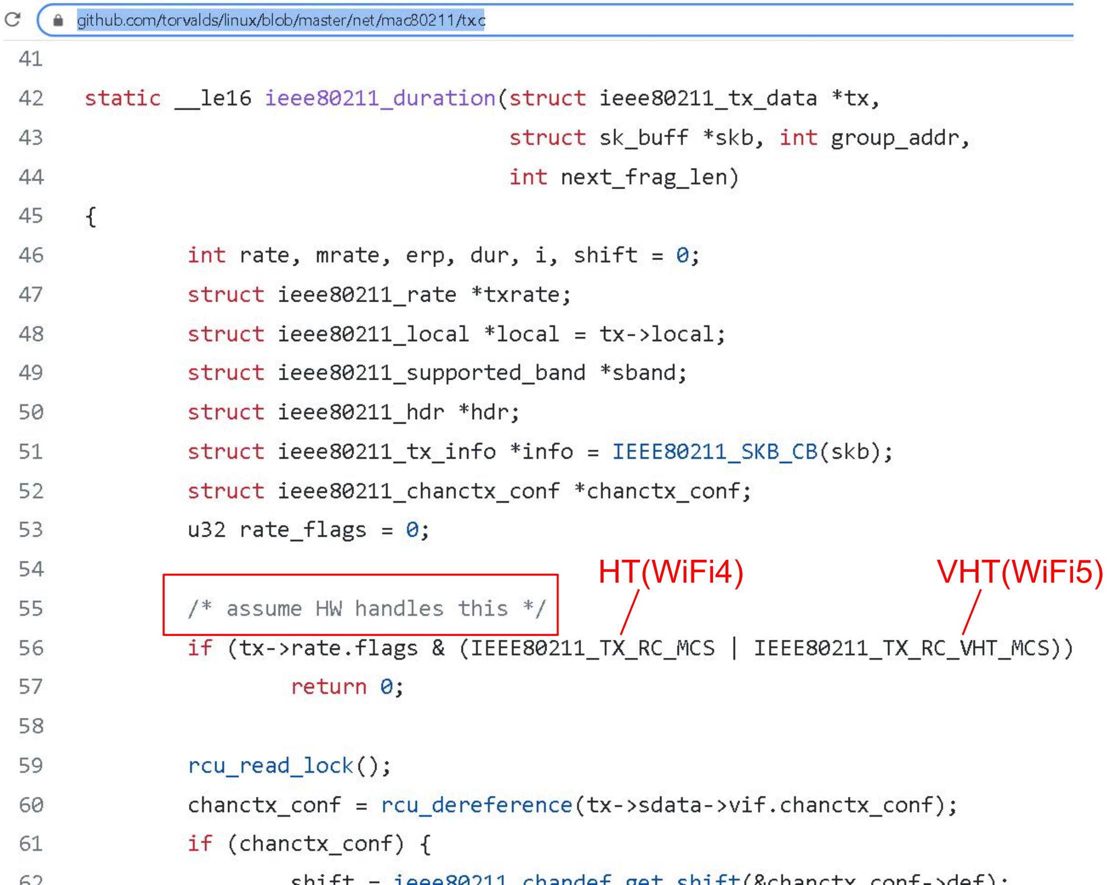
Figure 4-1. Generic data frame

Duration

The Duration field carries the value of the Network Allocation Vector (NAV). Access to the medium is restricted for the time specified by the NAV. Four rules specify the setting for the Duration field in data frames:

1. Any frames transmitted during the contention-free period set the Duration field to 32,768. Naturally, this applies to any data

Openwifi bug fixes 2021: Duration field for HT (WiFi4)



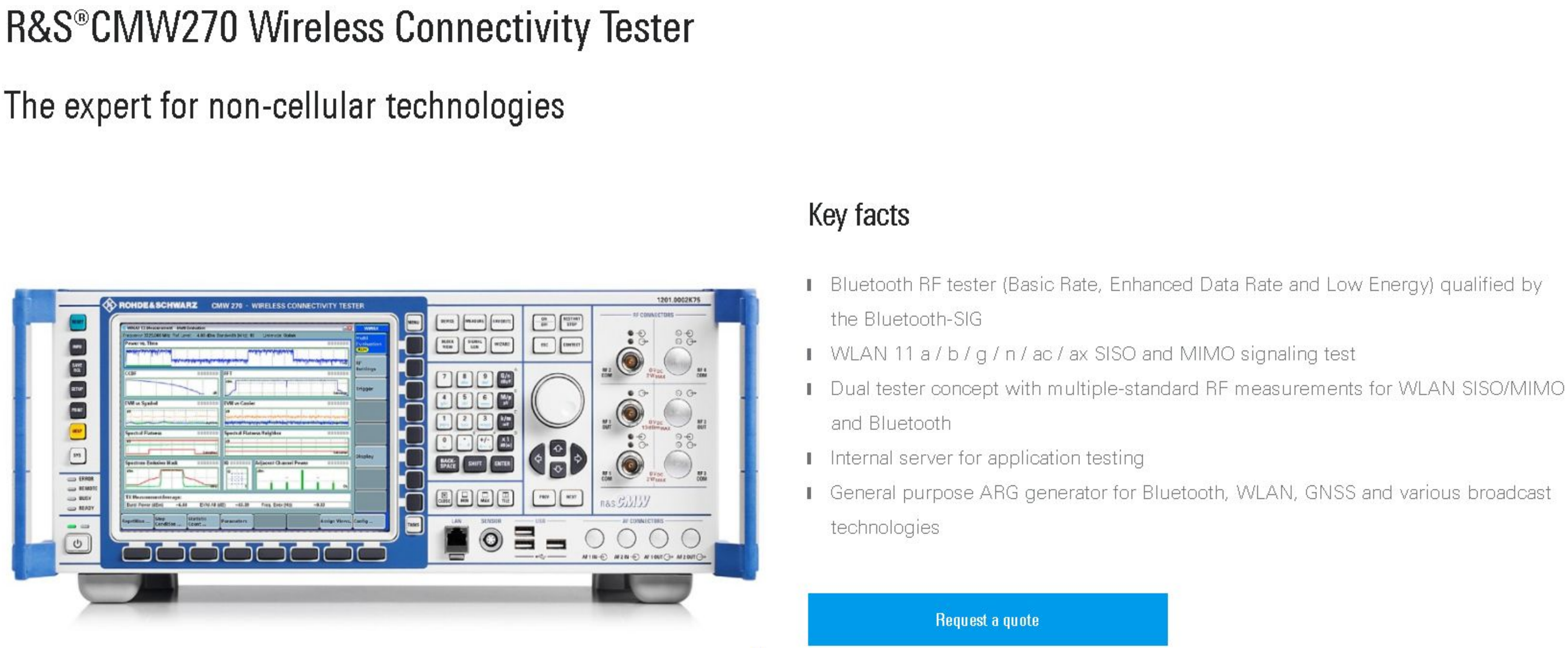
github.com/torvalds/linux/blob/master/net/mac80211/tx.c

```
static __le16 ieee80211_duration(struct ieee80211_tx_data *tx,
                                 struct sk_buff *skb, int group_addr,
                                 int next_frag_len)
{
        int rate, mrate, erp, dur, i, shift = 0;
        struct ieee80211_rate *txrate;
        struct ieee80211_local *local = tx->local;
        struct ieee80211_supported_band *sband;
        struct ieee80211_hdr *hdr;
        struct ieee80211_tx_info *info = IEEE80211_SKB_CB(skb);
        struct ieee80211_chanctx_conf *chanctx_conf;
        u32 rate_flags = 0;

        /* assume HW handles this */
        if (tx->rate.flags & (IEEE80211_TX_RC_MCS | IEEE80211_TX_RC_VHT_MCS))
                return 0;

        rcu_read_lock();
        chanctx_conf = rcu_dereference(tx->sdata->vif.chanctx_conf);
        if (chanctx_conf) {
                shift = ieee80211_chandef_get_shift(&chanctx_conf->def);
```

Openwifi project in 2021

- Features/optimizations
- Bug fixes
- ***RF performance measured by Rohde & Schwarz CMW 270***
- Community growth
  - New hardwares
  - New papers/applications
- Current focus
  - Optimization for maturity
  - 802.11ax/WiFi6
- Future plan

Openwifi RF performance



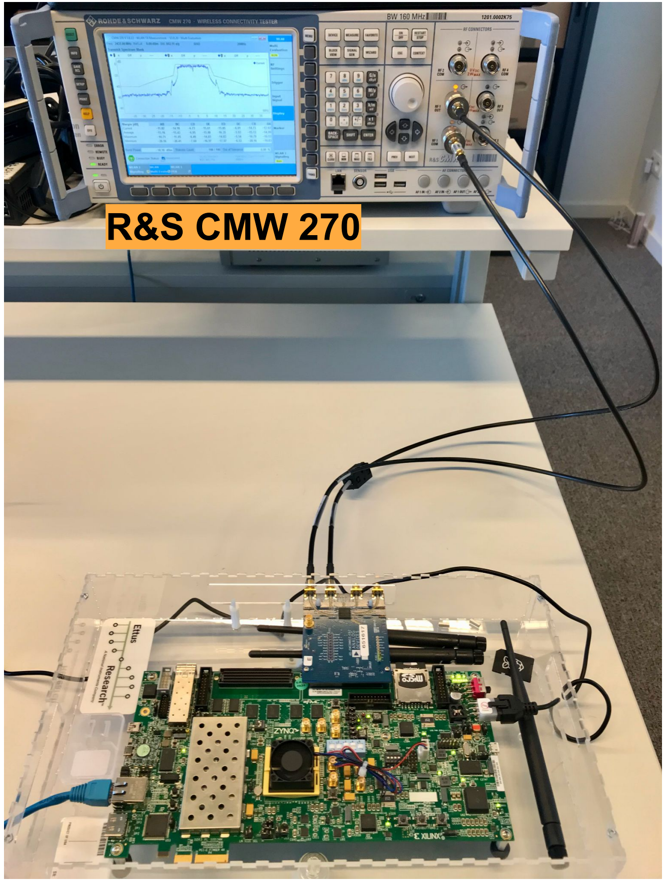
R&S®CMW270 Wireless Connectivity Tester

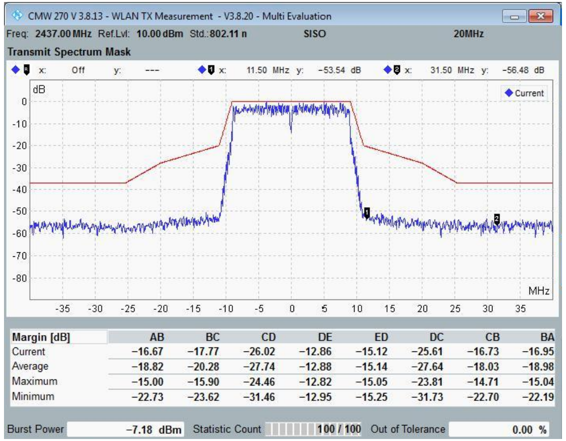
The expert for non-cellular technologies

Key facts

- Bluetooth RF tester (Basic Rate, Enhanced Data Rate and Low Energy) qualified by the Bluetooth-SIG
- WLAN 11 a / b / g / n / ac / ax SISO and MIMO signaling test
- Dual tester concept with multiple-standard RF measurements for WLAN SISO/MIMO and Bluetooth
- Internal server for application testing
- General purpose ARG generator for Bluetooth, WLAN, GNSS and various broadcast technologies

Openwifi RF performance





CMW 270 V 3.8.13 - WLAN TX Measurement - V3.8.20 - Multi Evaluation

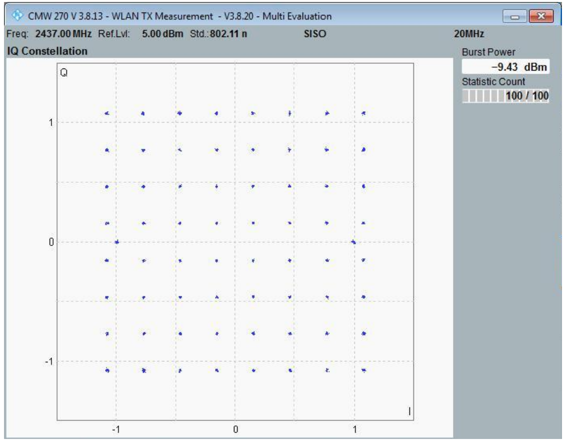
Freq: 2437.00 MHz Ref.Lvl: 10.00 dBm Std.:802.11 n SISO 20MHz

Transmit Spectrum Mask

R x: Off y: --- | 1 x: 11.50 MHz y: −53.54 dB | 2 x: 31.50 MHz y: −56.48 dB

Margin [dB]	AB	BC	CD	DE	ED	DC	CB	BA
Current	−16.67	−17.77	−26.02	−12.86	−15.12	−25.61	−16.73	−16.95
Average	−18.82	−20.28	−27.74	−12.88	−15.14	−27.64	−18.03	−18.98
Maximum	−15.00	−15.90	−24.46	−12.82	−15.05	−23.81	−14.71	−15.04
Minimum	−22.73	−23.62	−31.46	−12.95	−15.25	−31.73	−22.70	−22.19

Burst Power −7.18 dBm Statistic Count 100 / 100 Out of Tolerance 0.00 %



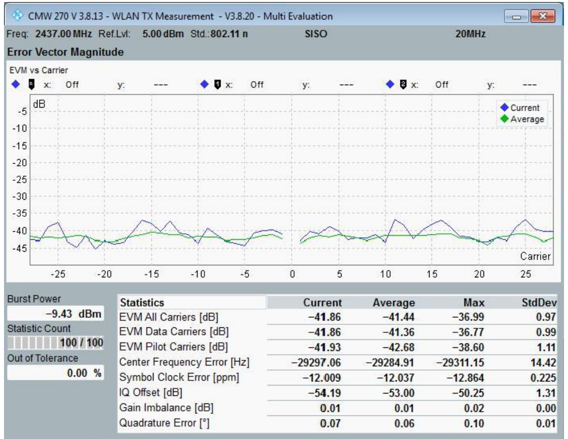
CMW 270 V 3.8.13 - WLAN TX Measurement - V3.8.20 - Multi Evaluation

Freq: 2437.00 MHz Ref.Lvl: 5.00 dBm Std.:802.11 n SISO 20MHz

IQ Constellation

Burst Power −9.43 dBm

Statistic Count 100 / 100



CMW 270 V 3.8.13 - WLAN TX Measurement - V3.8.20 - Multi Evaluation

Freq: 2437.00 MHz Ref.Lvl: 5.00 dBm Std.:802.11 n SISO 20MHz

Error Vector Magnitude

EVM vs Carrier

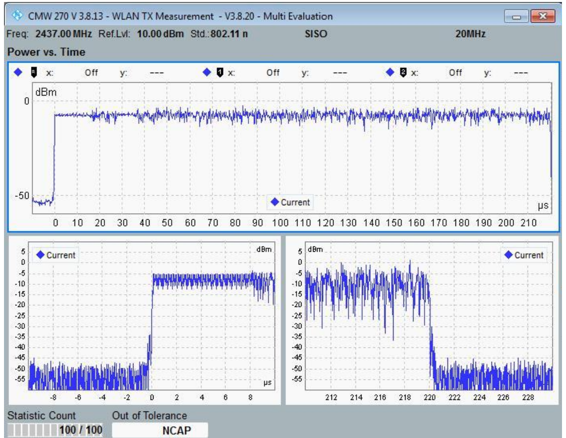
R x: Off y: --- | 1 x: Off y: --- | 2 x: Off y: ---

Burst Power −9.43 dBm

Statistic Count 100 / 100

Out of Tolerance 0.00 %

Statistics	Current	Average	Max	StdDev
EVM All Carriers [dB]	−41.86	−41.44	−36.99	0.97
EVM Data Carriers [dB]	−41.86	−41.36	−36.77	0.99
EVM Pilot Carriers [dB]	−41.93	−42.68	−38.60	1.11
Center Frequency Error [Hz]	−29297.06	−29284.91	−29311.15	14.42
Symbol Clock Error [ppm]	−12.009	−12.037	−12.864	0.225
IQ Offset [dB]	−54.19	−53.00	−50.25	1.31
Gain Imbalance [dB]	0.01	0.01	0.02	0.00
Quadrature Error [°]	0.07	0.06	0.10	0.01



CMW 270 V 3.8.13 - WLAN TX Measurement - V3.8.20 - Multi Evaluation

Freq: 2437.00 MHz Ref.Lvl: 10.00 dBm Std.:802.11 n SISO 20MHz

Power vs. Time

R x: Off y: --- | 1 x: Off y: --- | 2 x: Off y: ---

Statistic Count 100 / 100 Out of Tolerance NCAP

Openwifi RF performance

RX PERFORMANCE -- SENSITIVITY

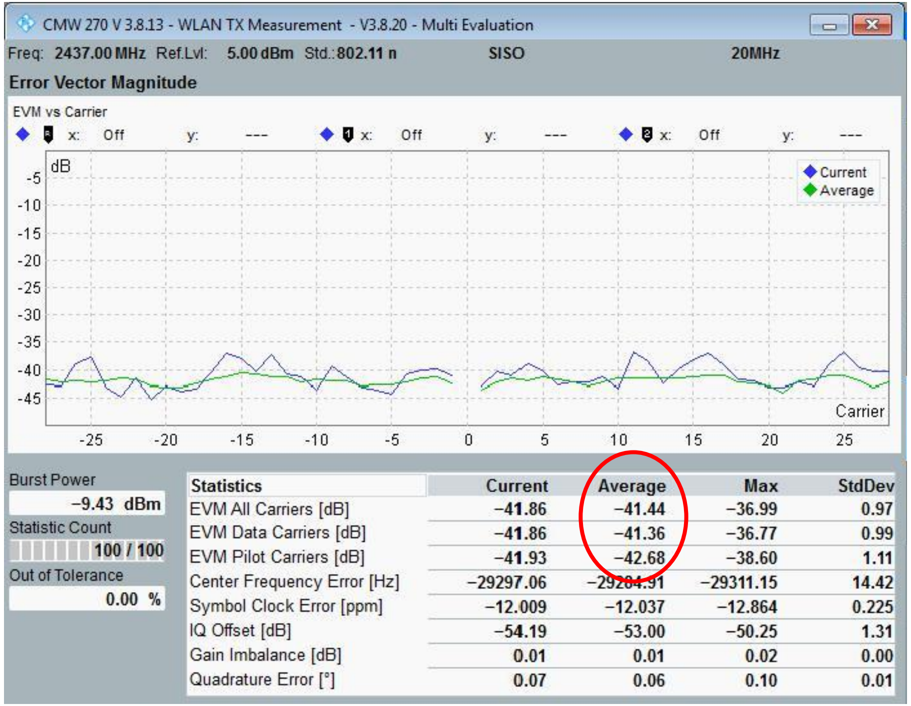
802.11n 2437MHz	CMW270 read	Cable loss (dB)	Openwifi sensitivity (dBm)	Standard need	Openwifi better than standard. (dB)
mcs0	-86	1.8	-87.8	-82	5.8
mcs1	-84.6	1.8	-86.4	-79	7.4
mcs2	-84	1.8	-85.8	-77	8.8
mcs3	-83.4	1.8	-85.2	-74	11.2
mcs4	-81	1.8	-82.8	-70	12.8
mcs5	-76.8	1.8	-78.6	-66	12.6
mcs6	-75	1.8	-76.8	-65	11.8
mcs7	-71.7	1.8	-73.5	-64	9.5

- Sensitivity COTS chip (Qualcomm AR9271 datasheet): -73 ~ -92dBm (LNA2), -70 ~ -89dBm (LNA1)
- Sensitivity Openwifi: -73.5 ~ -87.8dBm without LNA. (AD9361 needs external LNA to boost signal when the RX signal is lower than -62dBm)

Openwifi RF performance

TX PERFORMANCE -- EVM

Standard required: -5dB (BPSK 1/2) ~ -27dB (64QAM 5/6)
Openwifi EVM: -39dB (big spectrum mask margin), -41dB (less margin)



CMW 270 V 3.8.13 - WLAN TX Measurement - V3.8.20 - Multi Evaluation

Freq: 2437.00 MHz Ref.Lvl: 5.00 dBm Std.: 802.11 n SISO 20MHz

Error Vector Magnitude

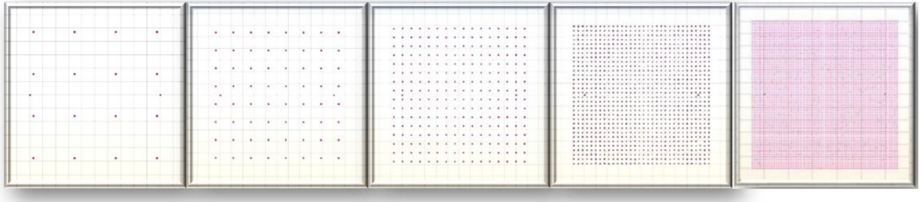
EVM vs Carrier

Burst Power
−9.43 dBm

Statistic Count
100 / 100

Out of Tolerance
0.00 %

Statistics	Current	Average	Max	StdDev
EVM All Carriers [dB]	−41.86	−41.44	−36.99	0.97
EVM Data Carriers [dB]	−41.86	−41.36	−36.77	0.99
EVM Pilot Carriers [dB]	−41.93	−42.68	−38.60	1.11
Center Frequency Error [Hz]	−29297.06	−29284.91	−29311.15	14.42
Symbol Clock Error [ppm]	−12.009	−12.037	−12.864	0.225
IQ Offset [dB]	−54.19	−53.00	−50.25	1.31
Gain Imbalance [dB]	0.01	0.01	0.02	0.00
Quadrature Error [°]	0.07	0.06	0.10	0.01



16 QAM	64 QAM	256 QAM	1024 QAM	4096QAM
-19 dB	-27 dB	-32 dB	**-35 dB**	**-38 dB**

https://www.litepoint.com/wp-content/uploads/2019/05/WiFi_Japan_Seminar_Sept2019_rev2-1.pdf

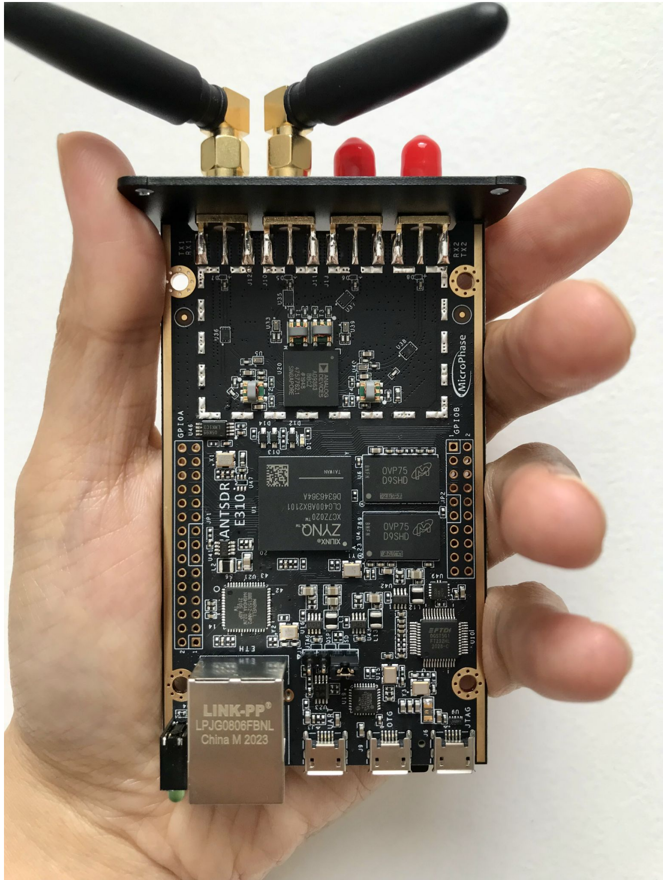
Openwifi is WiFi7 4K QAM capable!

Openwifi project in 2021

- Features/optimizations
- Bug fixes
- RF performance measured by Rohde & Schwarz CMW 270
- ***Community growth***
  - ***New hardwares***
  - New papers/applications
- Current focus
  - Optimization for maturity
  - 802.11ax/WiFi6
- Future plan

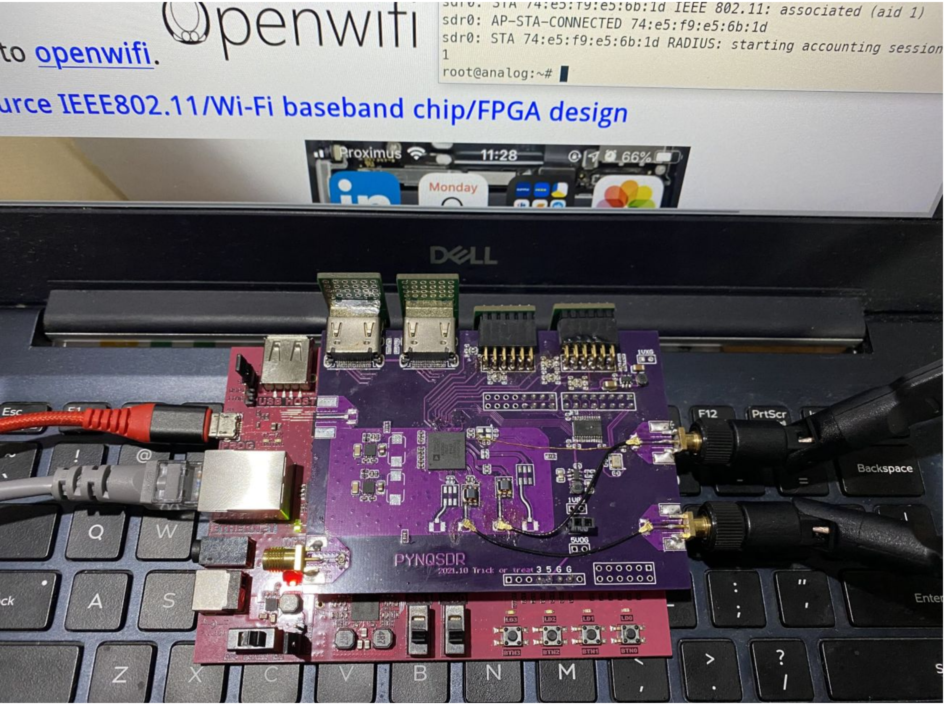
Openwifi community growth 2021: new hardware 1

Antsdr
https://github.com/open-sdr/openwifi/issues/91
The cheapest board so far!
The support is in openwifi mainline now.

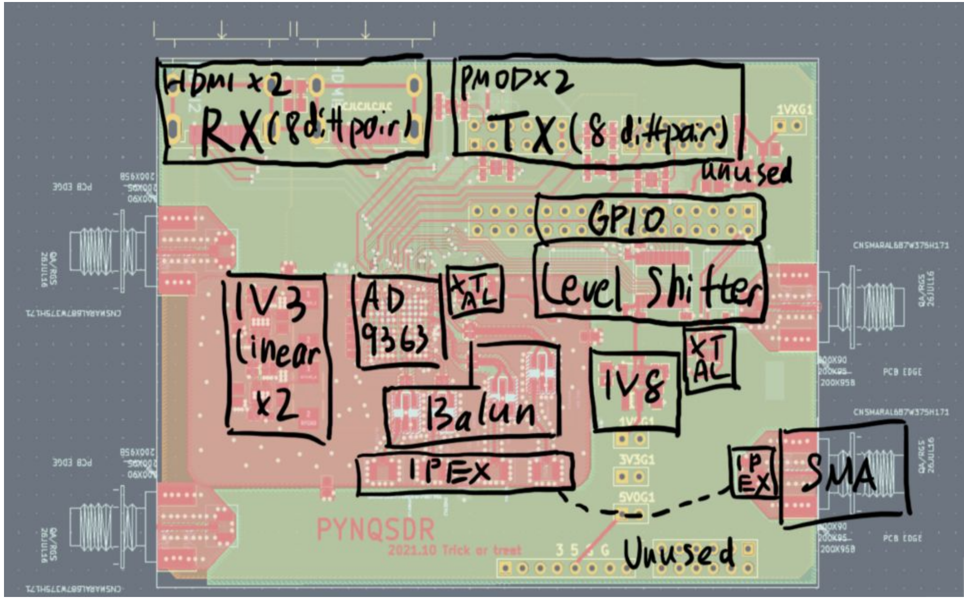


Openwifi community growth 2021: new hardware 2

https://github.com/open-sdr/openwifi/issues/123
An SDR HAT for PYNQ: https://github.com/regymm/PYNQSDR



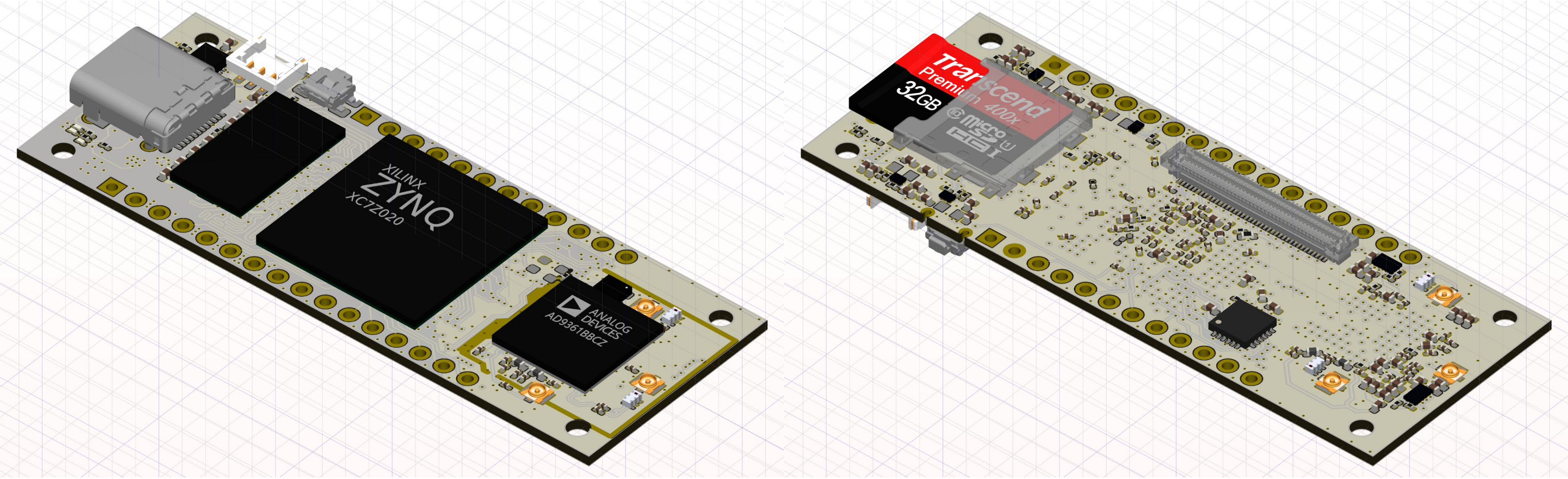
to openwifi.
openwifi
urce IEEE802.11/Wi-Fi baseband chip/FPGA design
sdr0: STA 74:e5:f9:e5:6b:1d IEEE 802.11: associated (aid 1)
sdr0: AP-STA-CONNECTED 74:e5:f9:e5:6b:1d
sdr0: STA 74:e5:f9:e5:6b:1d RADIUS: starting accounting session
1
root@analog:~#
DELL
PYNQSDR
2021.10 Trick or treat



Openwifi community growth 2021: new hardware 3

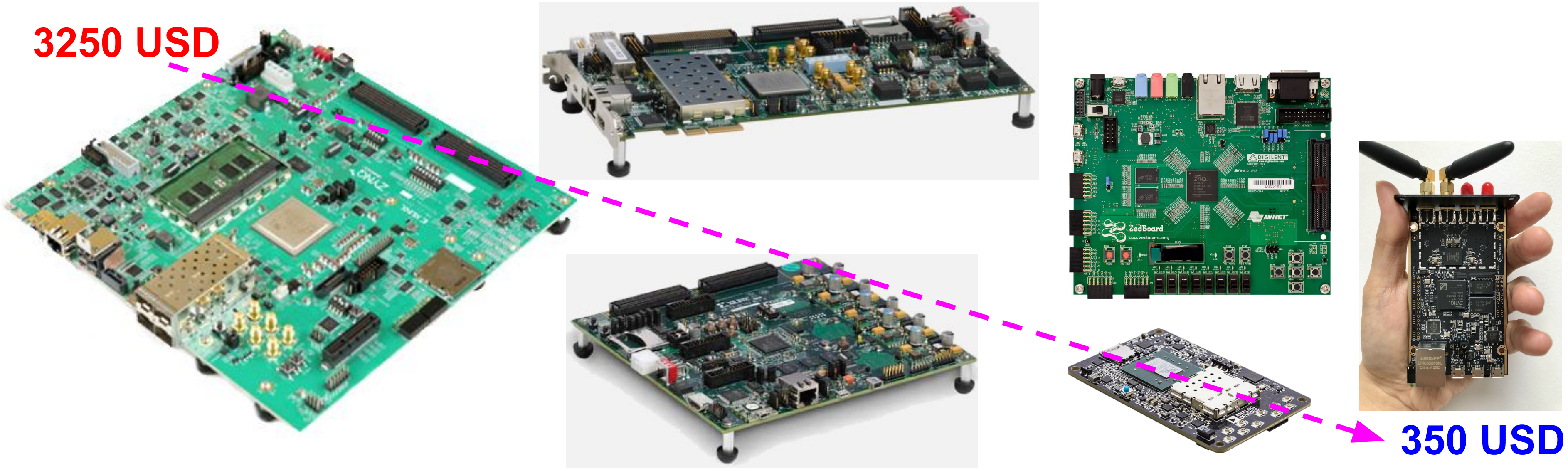
https://github.com/john-luan/SDR-dongle

An openwifi capable small SDR dongle designed by KiCAD!



Openwifi community growth: hardware

Check out all boards we support: https://github.com/open-sdr/openwifi



3250 USD

350 USD

Openwifi project in 2021

- Features/optimizations
- Bug fixes
- RF performance measured by Rohde & Schwarz CMW 270
- ***Community growth***
    - New hardwares
    - ***New papers/applications***
- Current focus
    - Optimization for maturity
    - 802.11ax/WiFi6
- Future plan

Openwifi community growth: papers and applications

Do check out the publications and app notes on the openwifi github:

- https://github.com/open-sdr/openwifi/blob/master/doc/publications.md -- publications
- https://github.com/open-sdr/openwifi/blob/master/doc/app_notes/README.md -- app notes

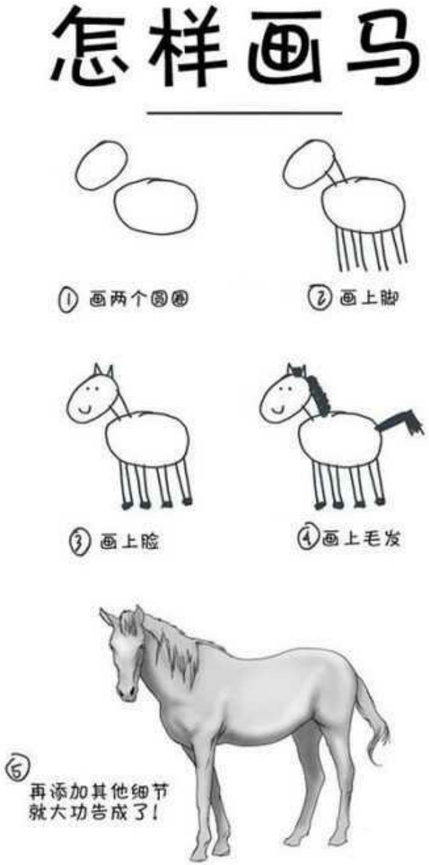
Among them, from users:

- owfuzz: a WiFi protocol fuzzing tool using openwifi. [Vulnerabilities]
- ELSEVIER Computer Networks, 2021. IEEE 802.11 CSI randomization to preserve location privacy: An empirical evaluation in different scenarios
- Blackhat asia 2021, OWFuzz: WiFi Protocol Fuzzing Tool Based on OpenWiFi, [code]
- Arxiv. A Just-In-Time Networking Framework for Minimizing Request-Response Latency of Wireless Time-Sensitive Applications
- MethodsX. A novel method for utilizing RF information from IEEE 802.11 frames in Software Defined Networks
- UGent master thesis 2021. The initial 802.11n 2*2 MIMO and diversity (CSD/Combining) work by Cedric Den Haese
- UGent master thesis 2021. IEEE 802.11 Physical Layer Fuzzing Using OpenWifi by Steven Heijse

Openwifi project in 2021

- Features/optimizations
- Bug fixes
- RF performance measured by Rohde & Schwarz CMW 270
- Community growth
  - New hardwares
  - New papers/applications
- ***Current focus***
  - ***Optimization for maturity***
  - 802.11ax/WiFi6
- Future plan

Openwifi current focus: optimization for maturity



How to draw a horse.

Step1: draw two circles

Step2: draw legs

Step3: draw face and feet

Step4: draw hair

Step5: Add some details

http://youngn.xyz/about/

Openwifi project in 2021

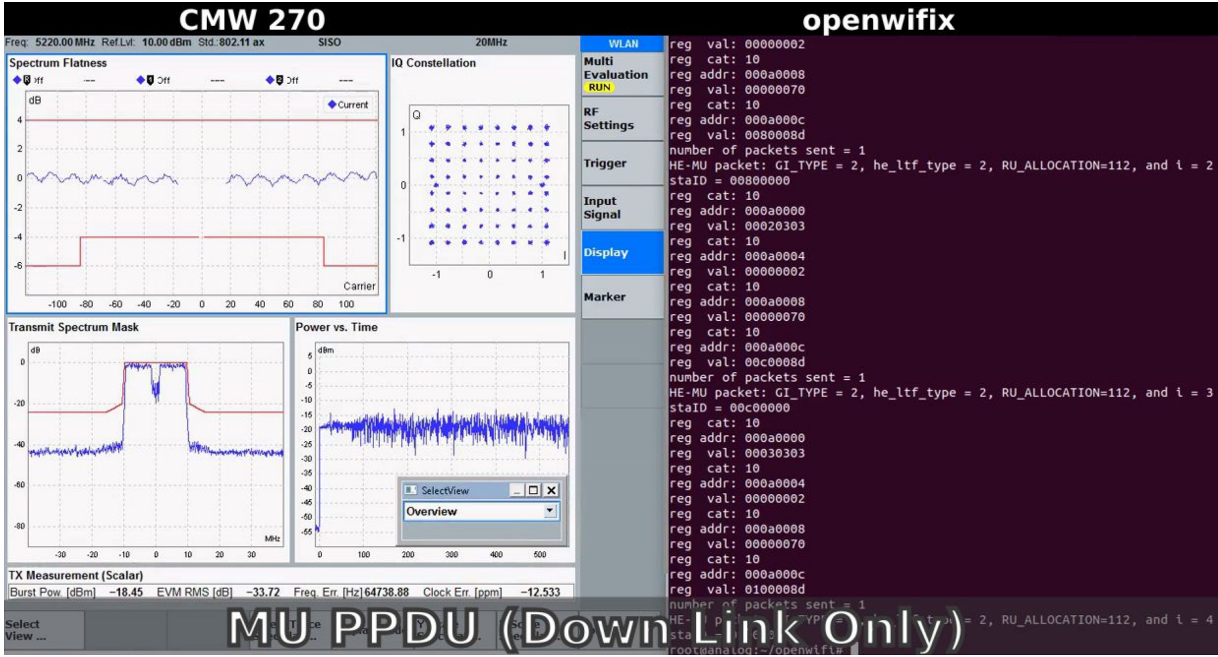
- Features/optimizations
- Bug fixes
- RF performance measured by Rohde & Schwarz CMW 270
- Community growth
  - New hardwares
  - New papers/applications
- ***Current focus***
  - Optimization for maturity
  - ***802.11ax/WiFi6***
- Future plan

Openwifi current focus: 802.11ax/WiFi6

802.11ax TX -- initial version, under testing and optimization

- SU PPDU: Single user UL/DL
- MU PPDU: Multi-user DL to STA
- TB PPDU: Multi-user UL to AP

802.11ax RX and Linux integration -- TODO in 2022



Freq: 5220.00 MHz Ref.Lvl: 10.00 dBm Std.:802.11 ax SISO 20MHz

TX Measurement (Scalar)

Burst Pow. [dBm] −18.45 EVM RMS [dB] −33.72 Freq. Err. [Hz] 64738.88 Clock Err. [ppm] −12.533

```
reg  val: 00000002
reg  cat: 10
reg addr: 000a0008
reg  val: 00000070
reg  cat: 10
reg addr: 000a000c
reg  val: 0080008d
number of packets sent = 1
HE-MU packet: GI_TYPE = 2, he_ltf_type = 2, RU_ALLOCATION=112, and i = 2
staID = 00800000
reg  cat: 10
reg addr: 000a0000
reg  val: 00020303
reg  cat: 10
reg addr: 000a0004
reg  val: 00000002
reg  cat: 10
reg addr: 000a0008
reg  val: 00000070
reg  cat: 10
reg addr: 000a000c
reg  val: 00c0008d
number of packets sent = 1
HE-MU packet: GI_TYPE = 2, he_ltf_type = 2, RU_ALLOCATION=112, and i = 3
staID = 00c00000
reg  cat: 10
reg addr: 000a0000
reg  val: 00030303
reg  cat: 10
reg addr: 000a0004
reg  val: 00000002
reg  cat: 10
reg addr: 000a0008
reg  val: 00000070
reg  cat: 10
reg addr: 000a000c
reg  val: 0100008d
number of packets sent = 1
HE-MU packet: GI_TYPE = 2, he_ltf_type = 2, RU_ALLOCATION=112, and i = 4
sta[illegible]
root@analog:~/openwifi#
```

MU PPDU (Down Link Only)

Openwifi project in 2021

- Features/optimizations
- Bug fixes
- RF performance measured by Rohde & Schwarz CMW 270
- Community growth
  - New hardwares
  - New papers/applications
- Current focus
  - Optimization for maturity
  - 802.11ax/WiFi6
- ***Future plan***

Openwifi future plan

- 802.11ax/WiFi6 receiver by the end of 2022
- Continue to support the user community
  - New ideas, applications
  - New hardware
  - etc.

Openwifi future plan

- Add some details