Openwifi project
The dawn of the Free/Libre WiFi chip

Xianjun Jiao
IDLab, imec – Gent University, Belgium

What is the openwifi project?

- A free WiFi baseband chip/FPGA design
- 802.11a/g/n (WiFi 4)
- HDL source code is available under AGPLv3
- Tested on FPGA against commercial WiFi chip
- Work in progress: 802.11ax (WiFi 6)
- **https://github.com/open-sdr/openwifi**

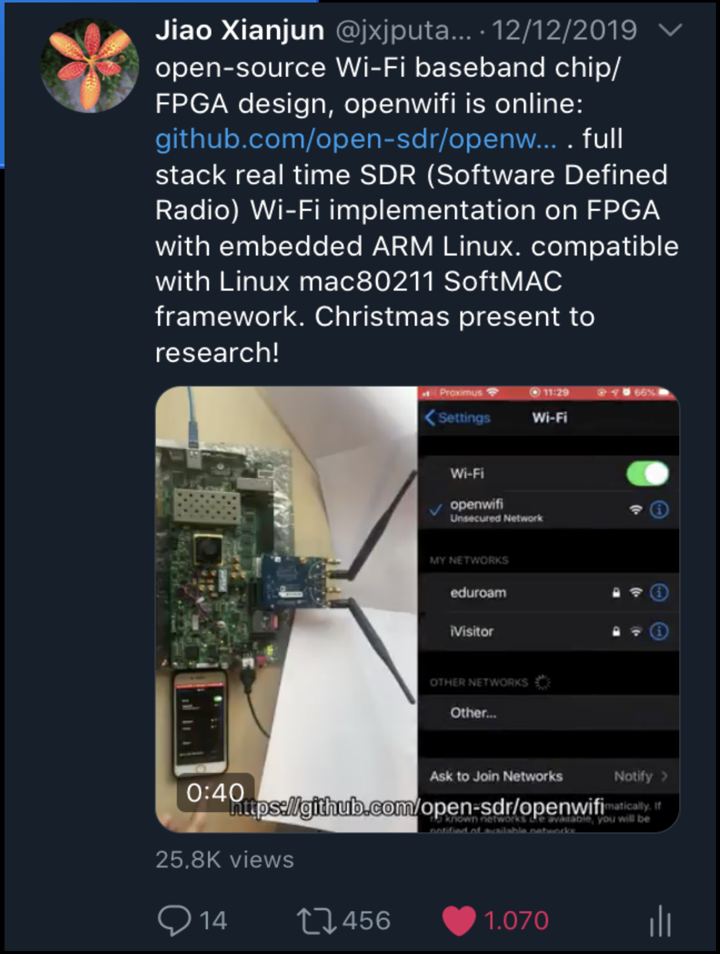
Timeline

2+ years
development

12/12/2019
online!

01/02/2020
FOSDEM

Then ...

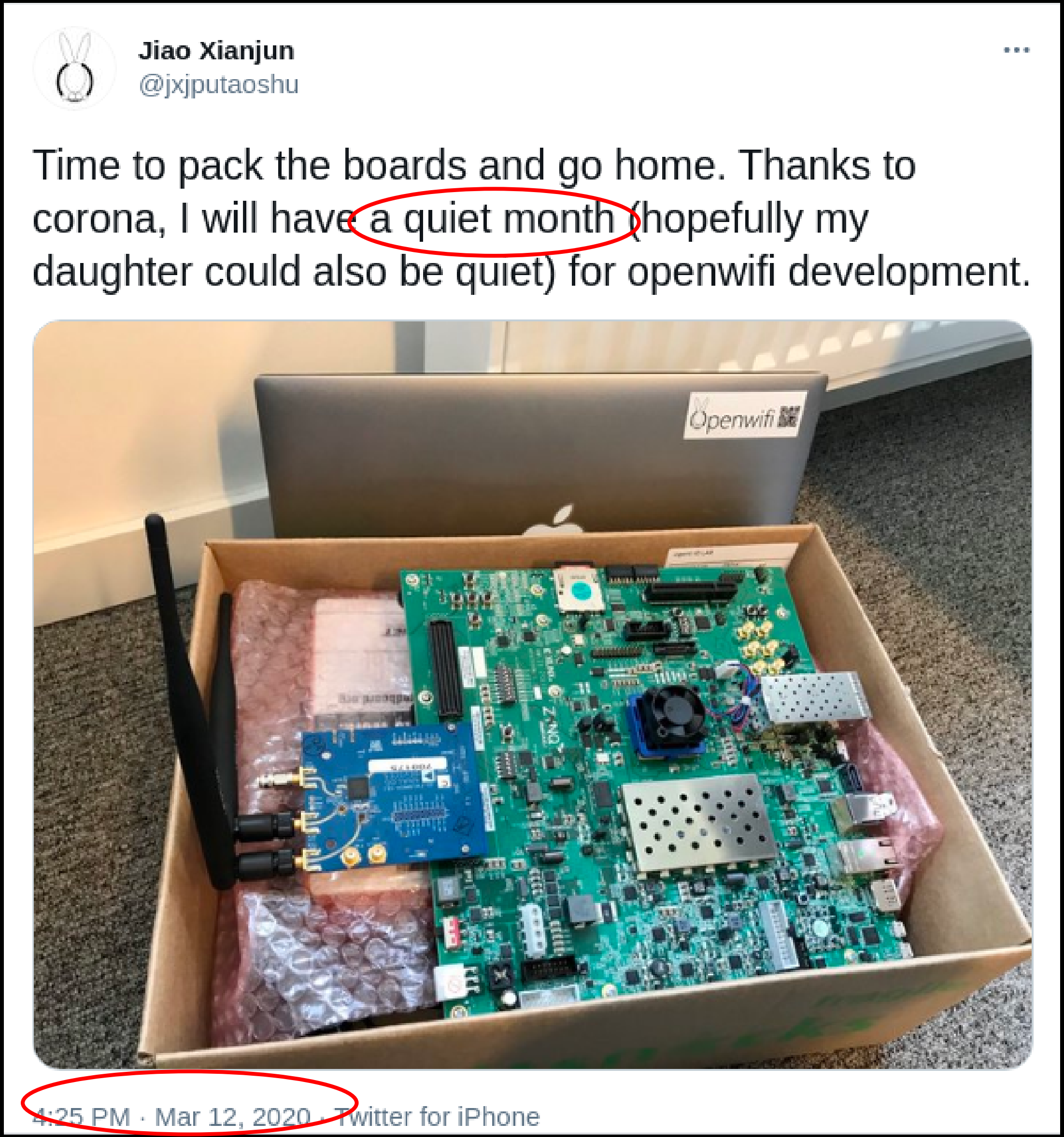


Jiao Xianjun @jxjputa... · 12/12/2019

open-source Wi-Fi baseband chip/ FPGA design, openwifi is online: github.com/open-sdr/openw... . full stack real time SDR (Software Defined Radio) Wi-Fi implementation on FPGA with embedded ARM Linux. compatible with Linux mac80211 SoftMAC framework. Christmas present to research!

25,8K views

14 456 1.070



Jiao Xianjun
@jxjputaoshu

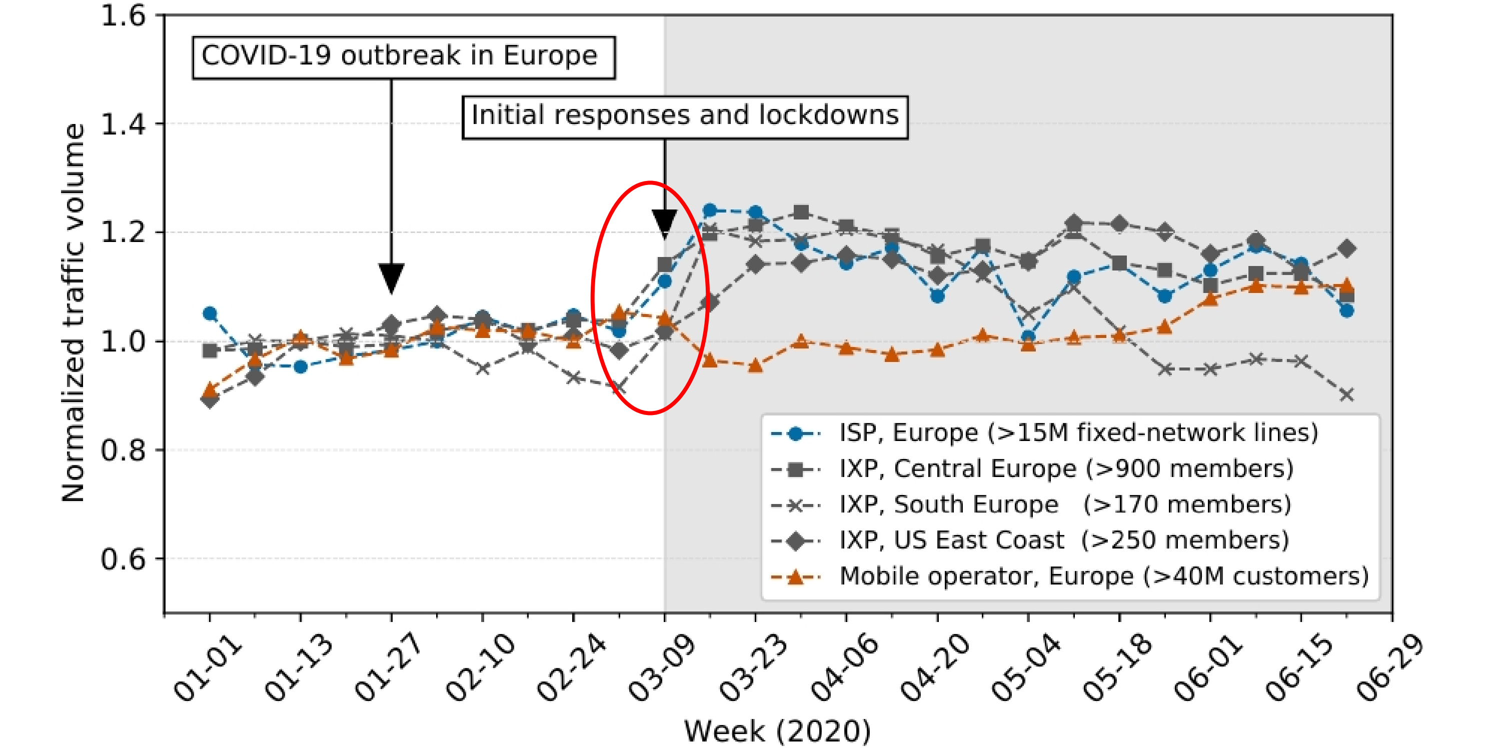
Time to pack the boards and go home. Thanks to corona, I will have a quiet month (hopefully my daughter could also be quiet) for openwifi development.

4:25 PM · Mar 12, 2020 · Twitter for iPhone

2000 YEARS
LATER

Today…
Still …

Internet traffic during the pandemic: https://arxiv.org/pdf/2008.10959.pdf



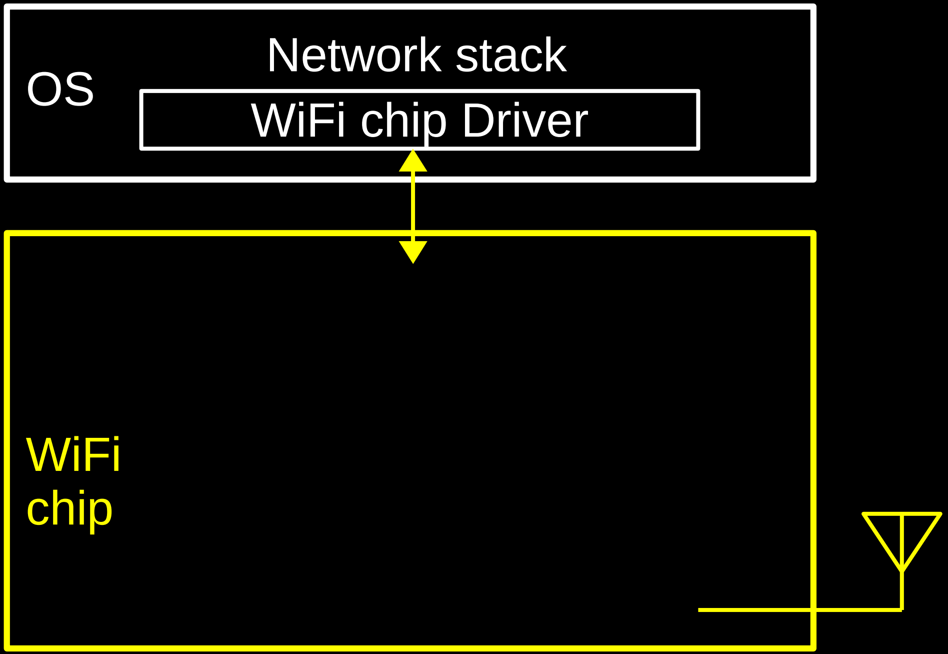
COVID-19 outbreak in Europe

Initial responses and lockdowns

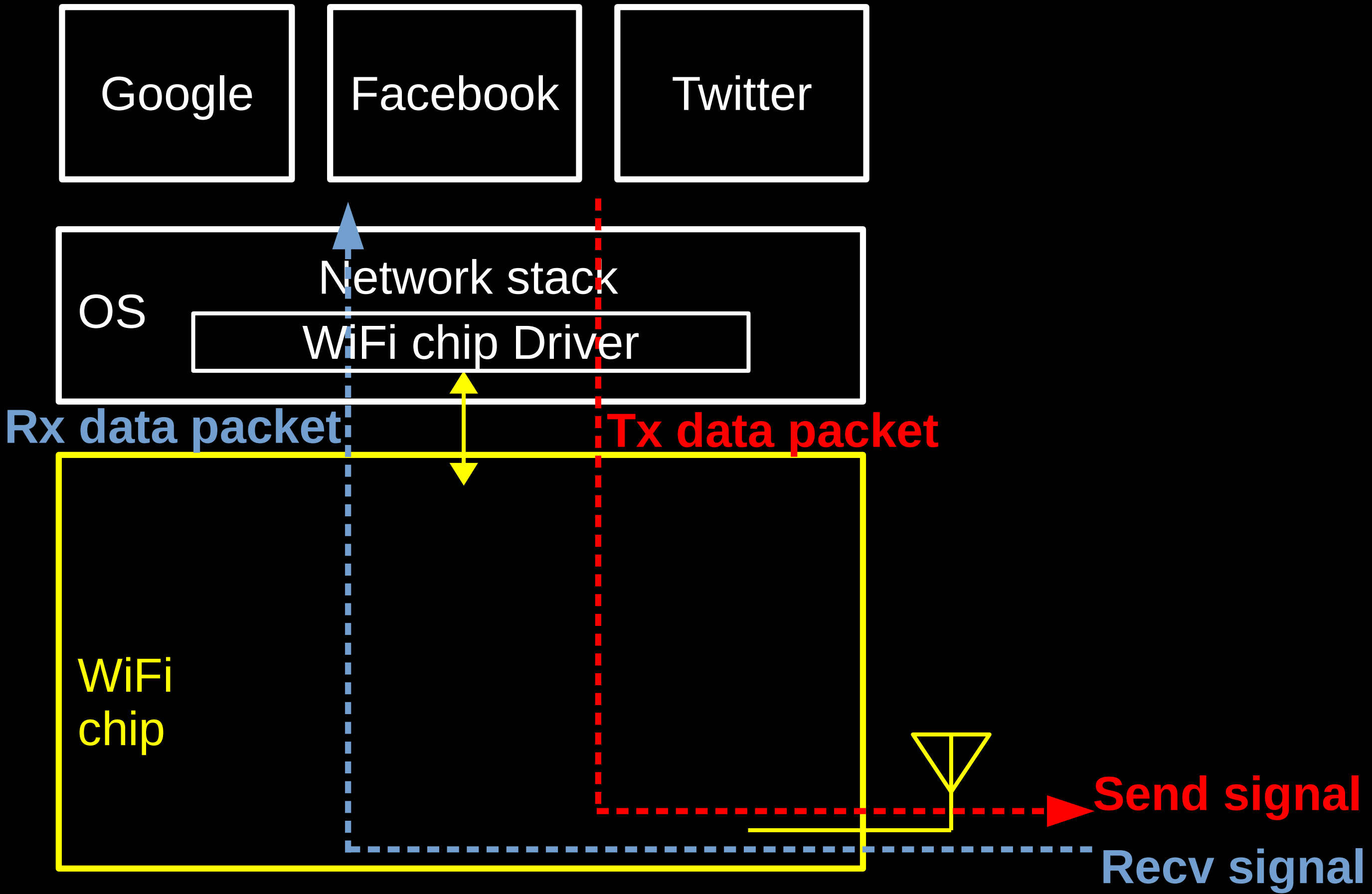
Figure 1: Traffic changes during 2020 at multiple vantage points—daily traffic averaged per week normalized by the median traffic volume of the first up to ten weeks.

Let’s talk about the WiFi chip that handles your daily internet traffic

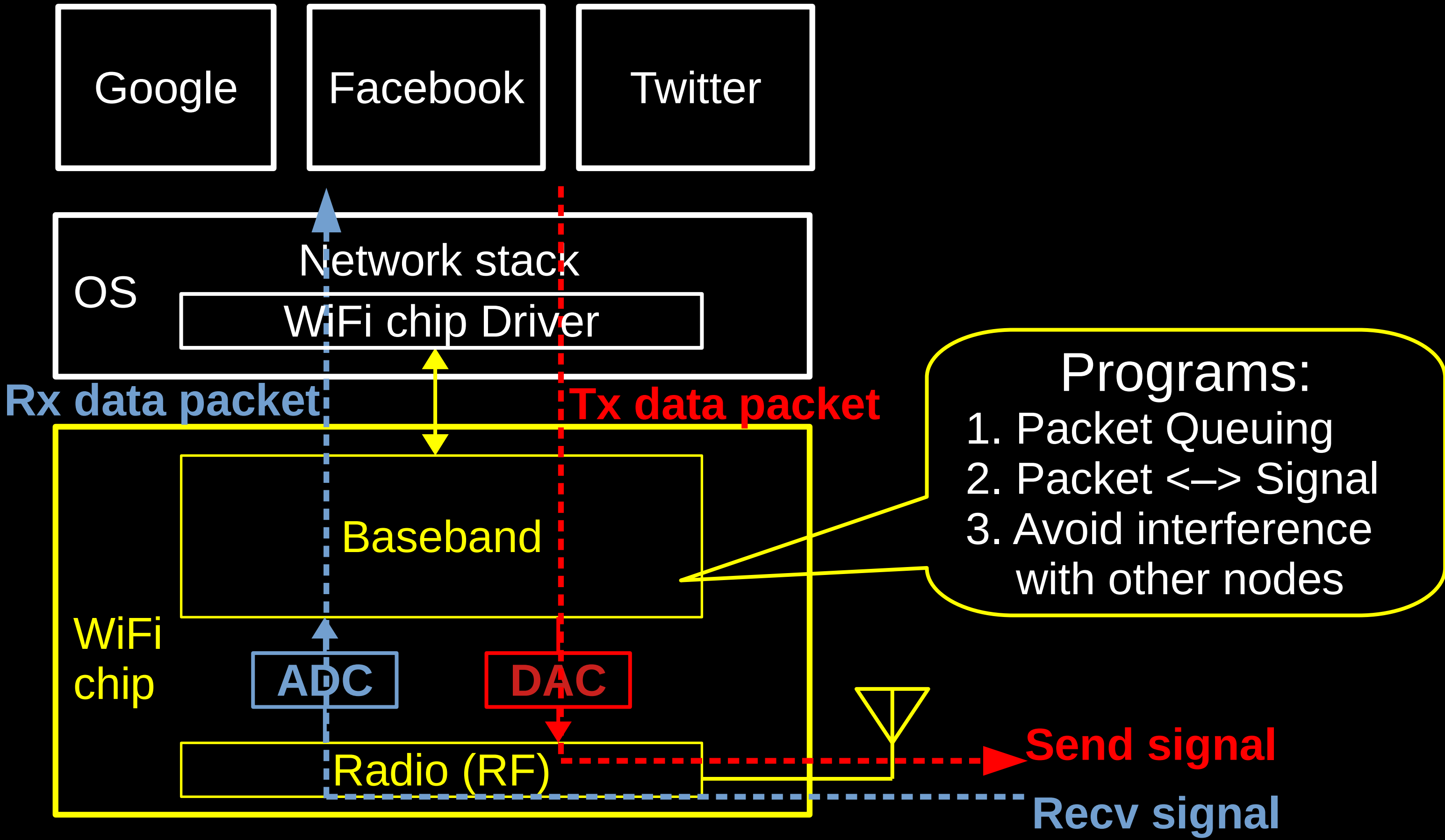
What is a WiFi chip?



How the WiFi chip serve your App



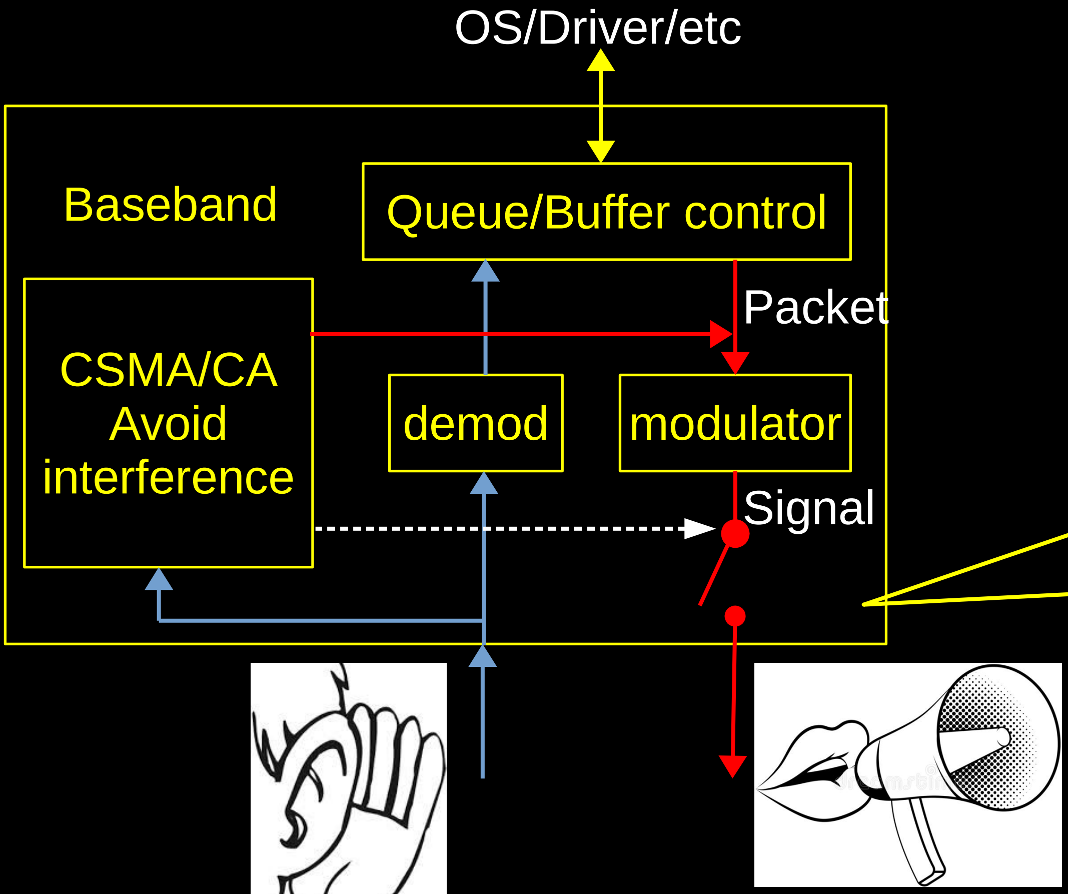
WiFi chip – What are inside?



Programs:

1. Packet Queuing
2. Packet <–> Signal
3. Avoid interference with other nodes

WiFi chip – The baseband



Programs:

1. Packet Queuing
2. Packet <–> Signal
3. Avoid interference with other nodes

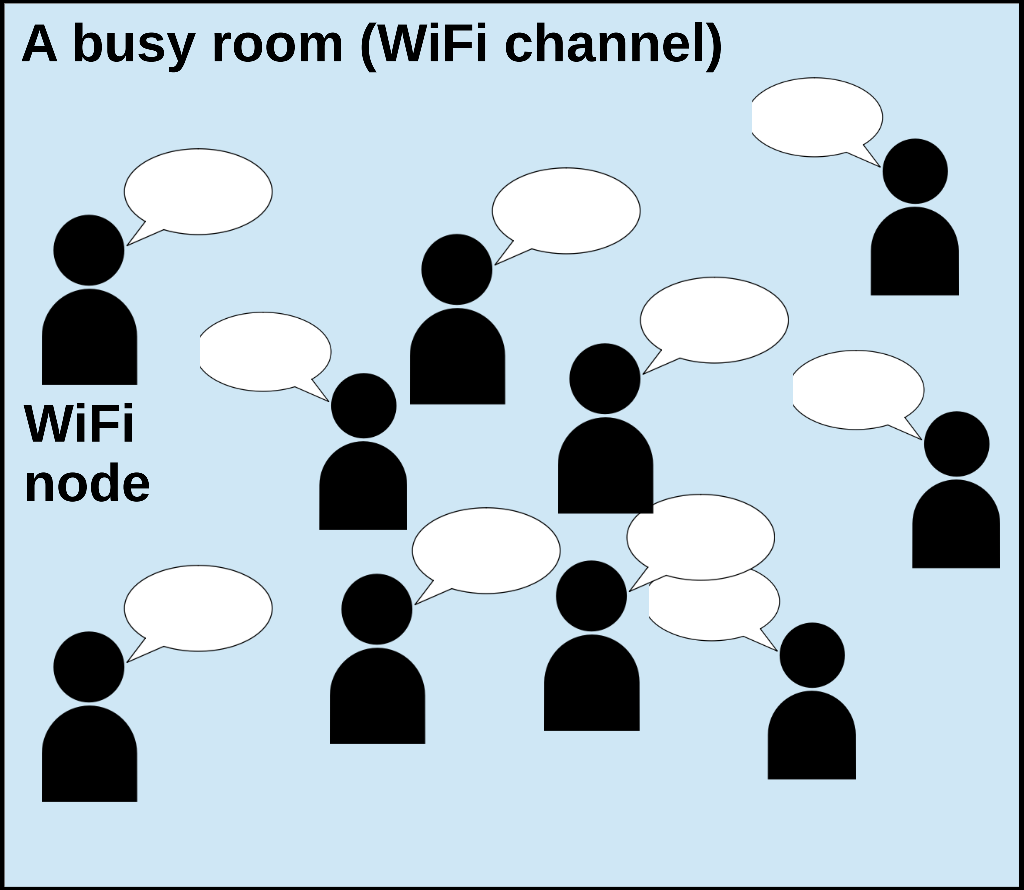
WiFi chip – DCF MAC: CSMA/CA

- Listen Before Talk
- Fast **ACK** to release the channel

- Wait for random time after
  - Channel is released
  - You are interrupted

- Grab the channel by
  - Talking
  - Announcement your plan (**RTS/CTS**)

- Shut Up if
  - Other is talking
  - Other announce occupation for next XX seconds

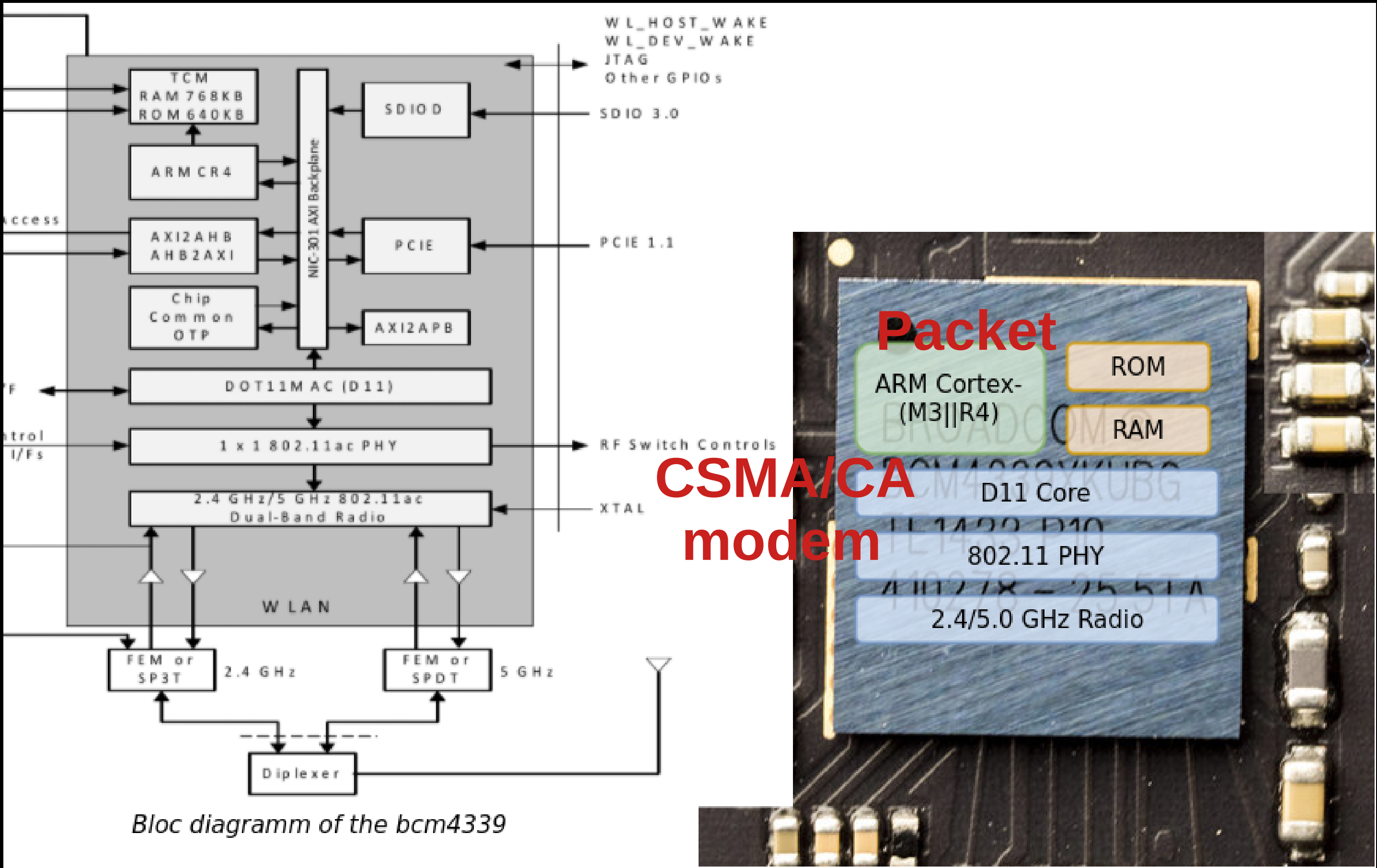


WiFi chip – Real example bcm4339

https://blog.quarkslab.com/reverse-engineering-broadcom-wireless-chipsets.html

- Reverse engineering
- Non-free blob – ARM
- Non-free microcode – D11 core

D11 core – best kept secret
- microcontroller
- implementations of protocols.
- track evolving IEEE 802.11
- instructions from the microcode Memory
- program counter
- ALU
- two basic branch instructions



Bloc diagramm of the bcm4339

Packet

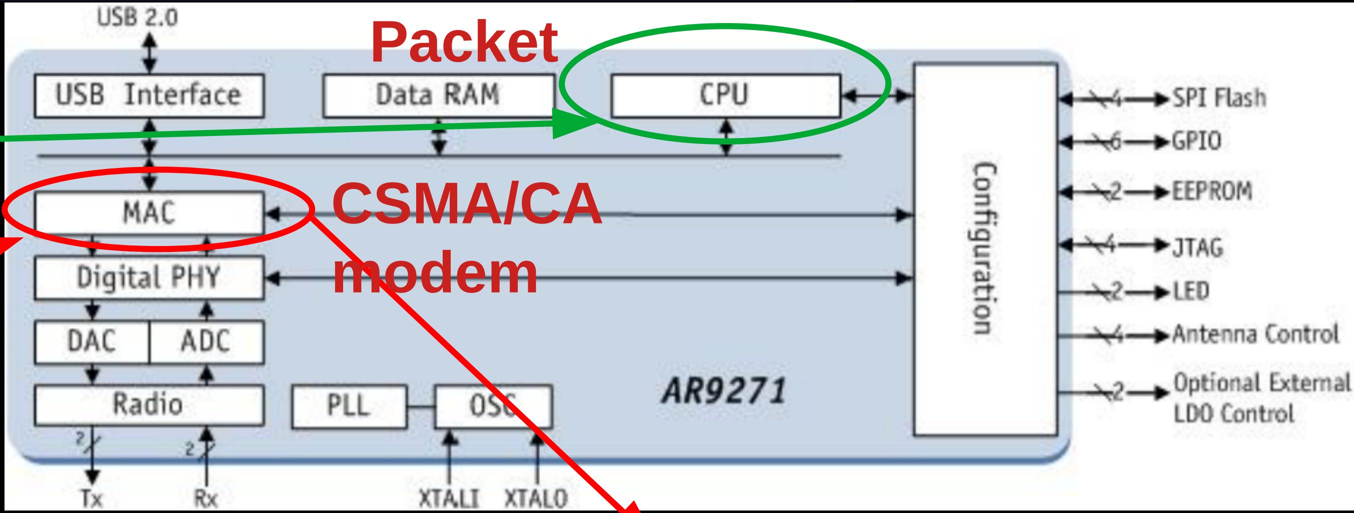
CSMA/CA modem

WiFi chip – Real example AR9271

https://www.phoronix.com/scan.php?page=news_item&px=MTMyNTY

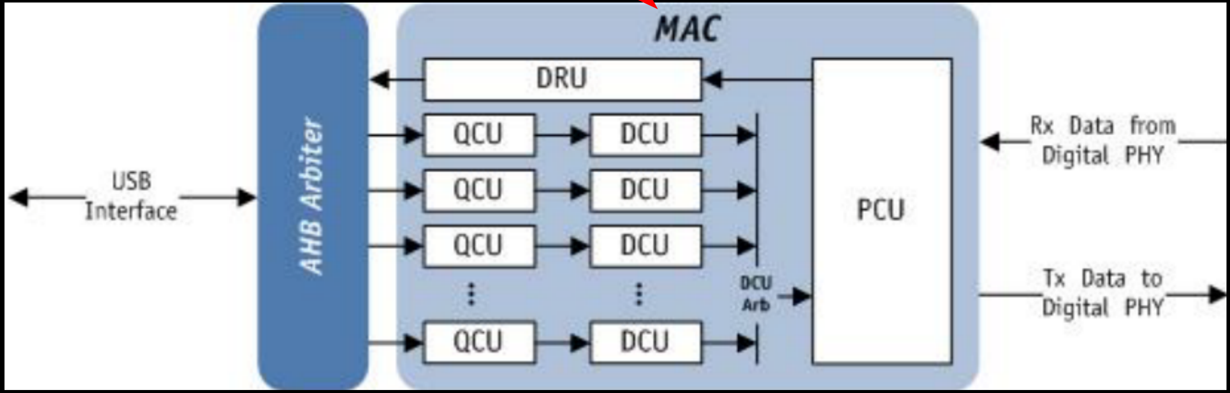
- Free firmware from vendor

- Non-free microcode in MAC cores – best kept secret
  - QCU: Queue Control Unit
  - DCU: DCF Control Unit
  - DRU: DMA Rx Unit
  - PCU: Protocol Control Unit



Packet

CSMA/CA modem



WiFi chip – Community activity

- (Free) hardware projects/boards use COTS WiFi chip.
  - BL602, ESP32, ESP8266, Arduino
  - Raspberry PI, OpenWRT, PINE64
  - RISC-V: PicoRio, BeagleV, etc
- To do more on the COTS chip, read driver code and reverse engineering the firmware.
- WiKi: Comparison of open-source wireless drivers
  - Most of vendors offer source code of WiFi chip driver
  - No vendor offer source code of firmware, **except AR9271 (Discontinued)**
  - No vendor offer source code of low level program (below the firmware, like D11 core in the Broadcom WiFi chip)

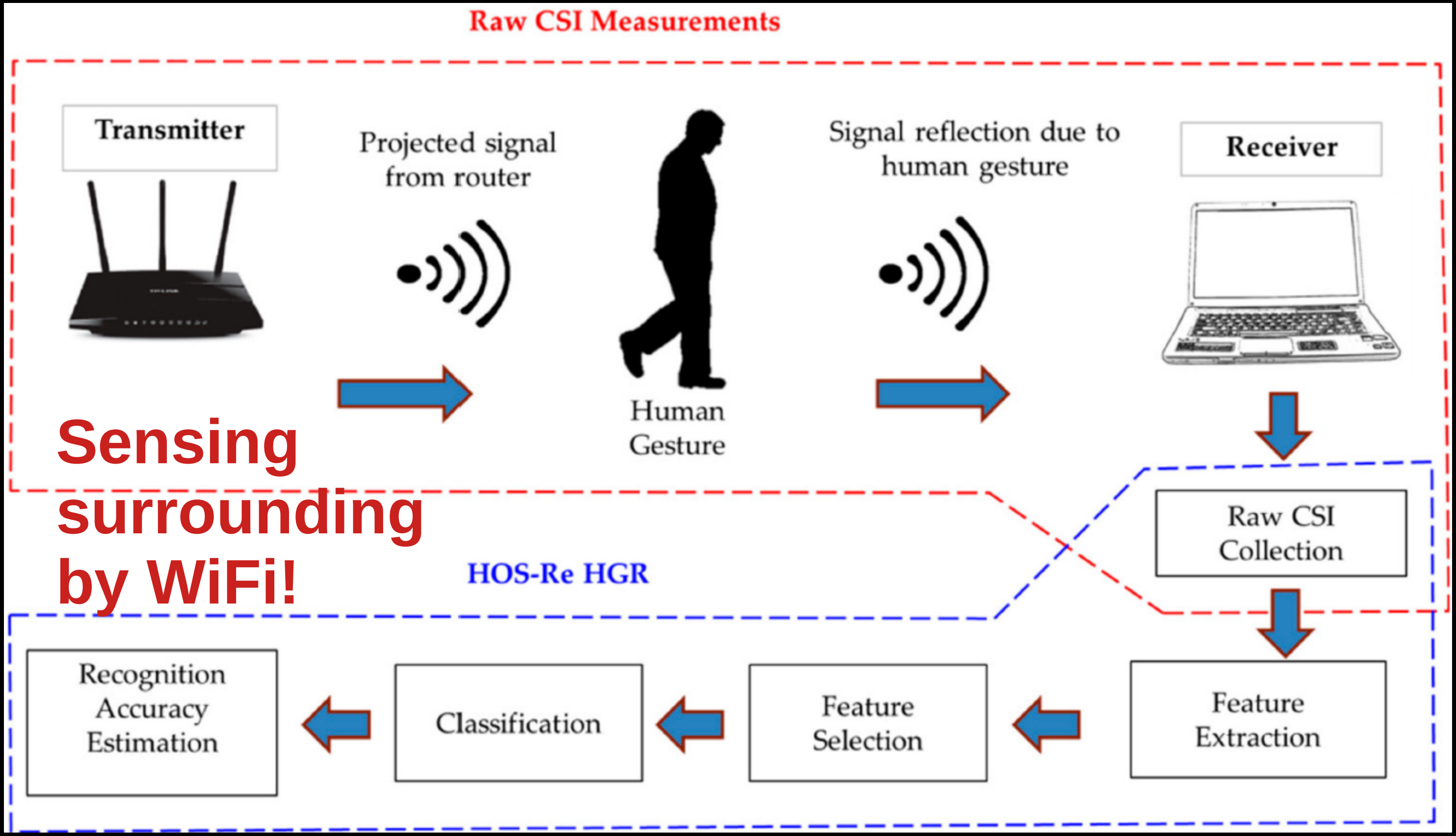
WiFi chip – Sensing

https://www.extremetech.com/extreme/133936-using-wifi-to-see-through-walls

Seeing Through Walls

– Media Lab, MIT

802.11bf WiFi sensing standardization is ongoing!



Sensing surrounding by WiFi!

https://www.sciencedirect.com/science/article/abs/pii/S0952197619302441

WiFi chip – Quick recap

- Small, cheap, yet complicated
- Program (firmware/microcode) is involved heavily
- Chip and program inside are non-free
- Some type of packet is generated on chip (ACK, RTS/CTS, etc), not by and controlled by APP/user
- The chip can “see”/sense the object around
- People are so used to the COTS chip
  - Live with what is offered: black-box chip and free driver
  - Reverse engineering if people want to do more on the chip

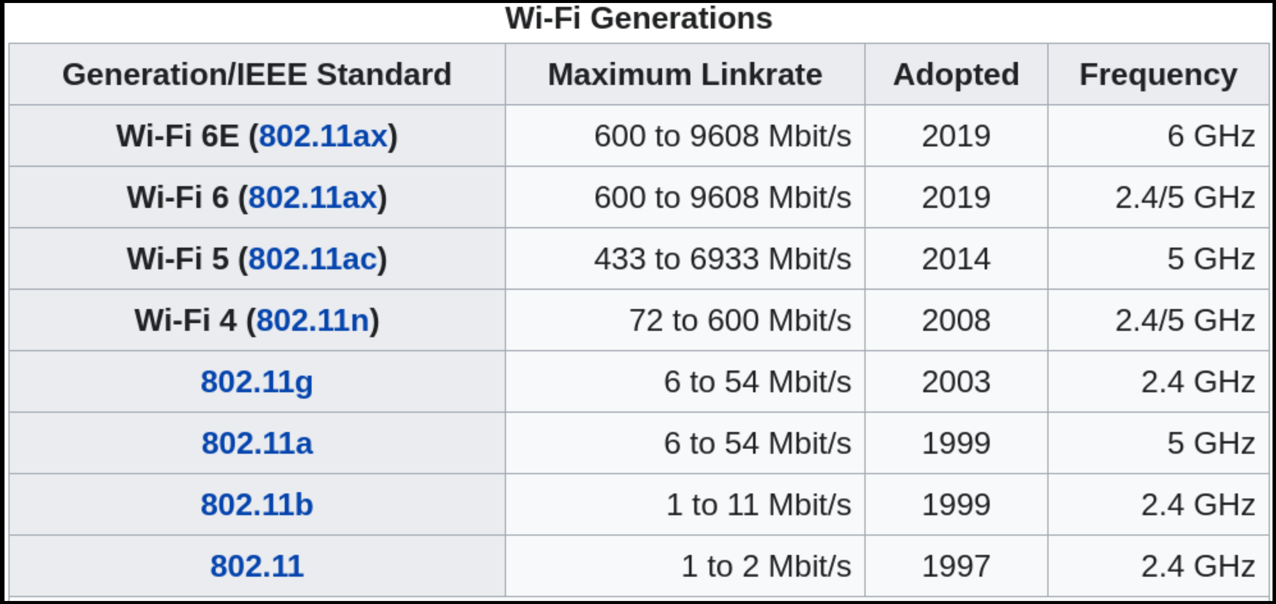
Openwifi: Why do we do it?

- We were not aware of all the above situations before 2020 – our design is different from the COTS WiFi chip

- The initial reason: It is needed by our own research activity and also the broad research community (universities, research institutes)
  - Researchers could implement innovative idea at the driver level and above, but when the idea comes to the chip level, it becomes impossible or very difficult (reverse engineering needs LUCK!)
  - Students learn WiFi knowledge in class room, but never see the devil in the details – design inside a WiFi chip, because no free design available
  - Access the commercial WiFi chip design source code: expensive, with many limitations (NDA, etc).

Openwifi: Could mean more

- After realizing the situation of the non-openness around COTS WiFi chip, we believe that openwifi could mean MORE!
- Openwifi is the 1st free (AGPLv3) chip/FPGA design, 20 years after 802.11a/b/g was released around 2000.



Wi-Fi Generations

Generation/IEEE Standard	Maximum Linkrate	Adopted	Frequency
Wi-Fi 6E (802.11ax)	600 to 9608 Mbit/s	2019	6 GHz
Wi-Fi 6 (802.11ax)	600 to 9608 Mbit/s	2019	2.4/5 GHz
Wi-Fi 5 (802.11ac)	433 to 6933 Mbit/s	2014	5 GHz
Wi-Fi 4 (802.11n)	72 to 600 Mbit/s	2008	2.4/5 GHz
802.11g	6 to 54 Mbit/s	2003	2.4 GHz
802.11a	6 to 54 Mbit/s	1999	5 GHz
802.11b	1 to 11 Mbit/s	1999	2.4 GHz
802.11	1 to 2 Mbit/s	1997	2.4 GHz

Openwifi: Achievement and impact

Openwifi users: +/-50 universities/companies are noticed.

UGent, CUHK, Northeastern university, Stony Brook university, Michigan State university, Trinity College Dublin, University of Massachusetts, Danang University (Vietnam), Tsinghua University, Nanjing University, Wuhan university, BUPT (China), UST Korea, University of Dortmund, unibs (Italy), etc.

On github (3/3/2021)
1.7K stars
230 forks
93 watch
43 issues closed
2 issues still open
external contributors and pull-requests

Openwifi: Achievement and impact

- Initially funded by EU H2020 ORCA project
- 50K€ from NLNET foundation supporting 802.11n/WiFi4 development
- FOSDEM 2020
- FOSDEM 2021
- Lots of discussions on forums/twitters/tech-medias:
  - **cnx-software**, **hackaday**, **nlnet**, **hackster**, **rtl-sdr**
  - **reddit**, **tuxmachines**, **desdelinux**, **opennet**, **abclinuxu**
  - etc.

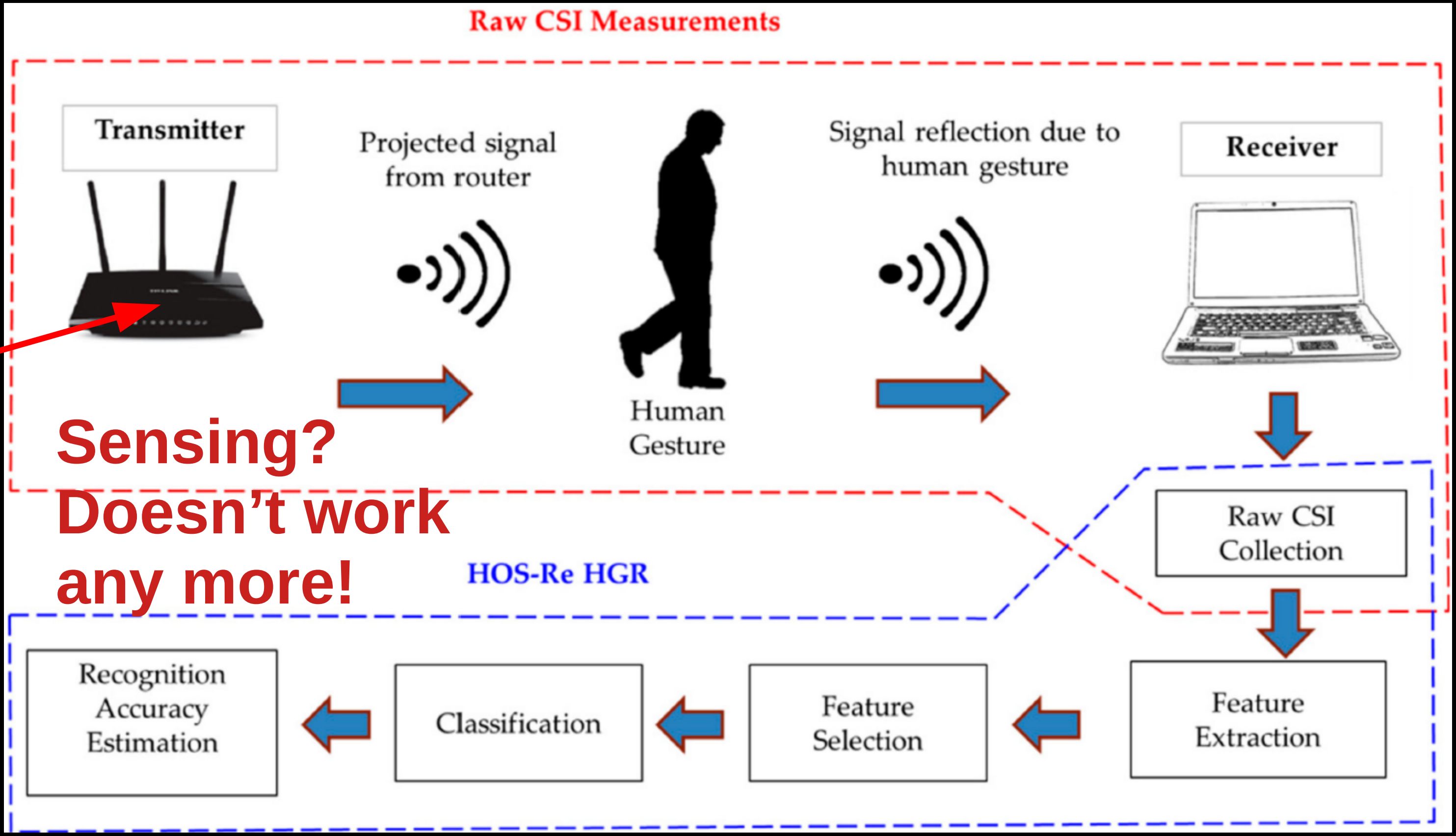
Openwifi: Interesting case from user

CSI – MURDER: https://ans.unibs.it/projects/csi-murder/

Anti-sensing by

Random/Fake CSI generation

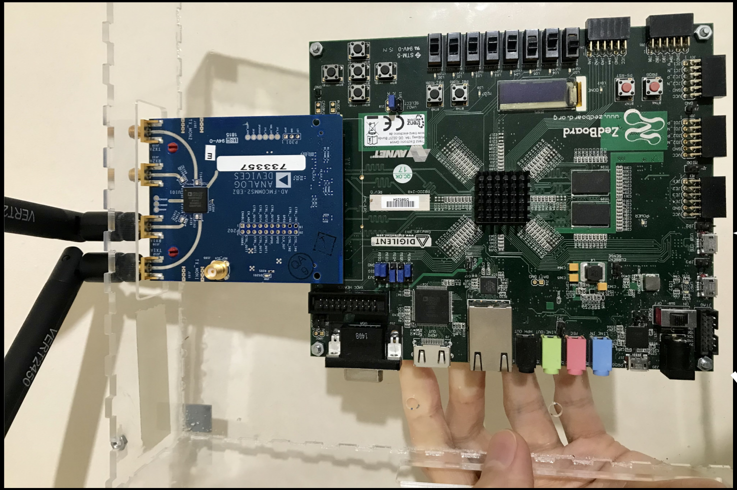
User take control!



Sensing? Doesn’t work any more!

https://www.sciencedirect.com/science/article/abs/pii/S0952197619302441

Openwifi: Your home AP in 3 steps!



(COTS FPGA board. **Not** from us)

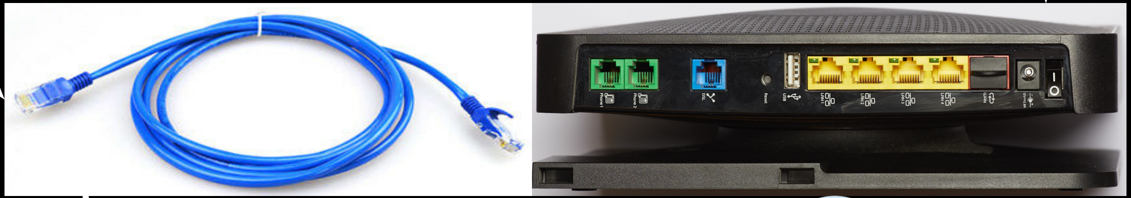
1

Download openwifi img
and flash it to a SD card

Insert

ADSL
Or
Fiber

Connect to your home broadband router



2

3

Power ON!

SSID: openwifi

Openwifi: What’s next?

- FPGA board is flexible, but expensive: 800 ~ 3000+ USD
- Lower the price to the same level as other COTS chip by taping out a real openwifi chip?
  - For the work turning FPGA into a chip. Need **funding**!
  - Game of **volume**! – **go/no-go** decision!
  - Free silicon and firmware – **unique** enough to achieve volume?
- To achieve the volume, need to be adopted by very popular free SW/HW projects – need **your idea/opinion/help**!
  - Raspberry PI sell 7M pcs/year (Commercial-Hobbyist half-half)
  - RISC-V PI? PicoRio, BeagleV, etc. Any other?

Does the world need a free WiFi chip?

Openwifi project

The dawn of the Free/Libre WiFi chip

Xianjun Jiao

IDLab, imec – Gent University, Belgium