Lesson 2: More MISC - Wireless Communication

flagbot (CTF@VIS)

November 7, 2024

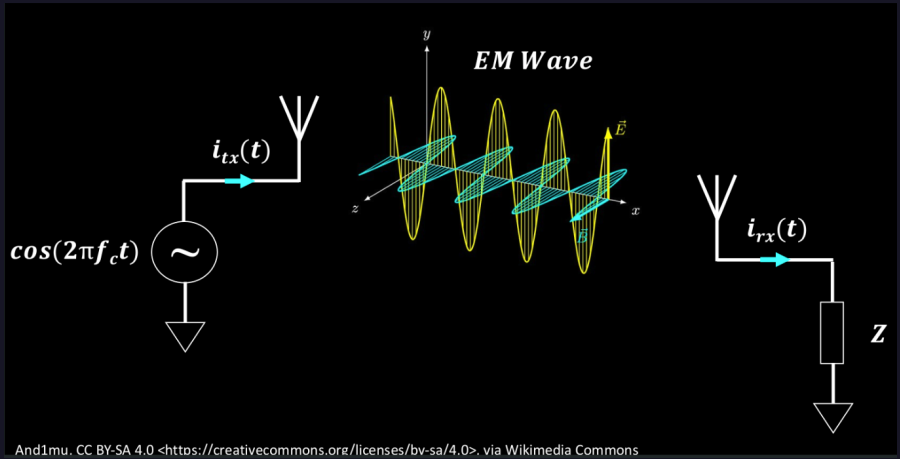
Goals of this Lesson

- Another type of chal usually part of Misc
- What is Wireless Communication? (explanation)
- Intro to Radio Singals & SDRs (explanation)
- Air-berry (challenge)

Discord Invite Link

Wireless Communication - Explanation

Radio Signals



Propagate through space at speed of light

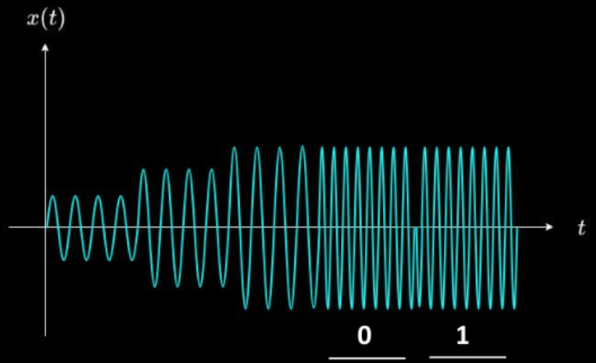
Radio Signals

Intuition

Sinusoidal radio signal (carrier)

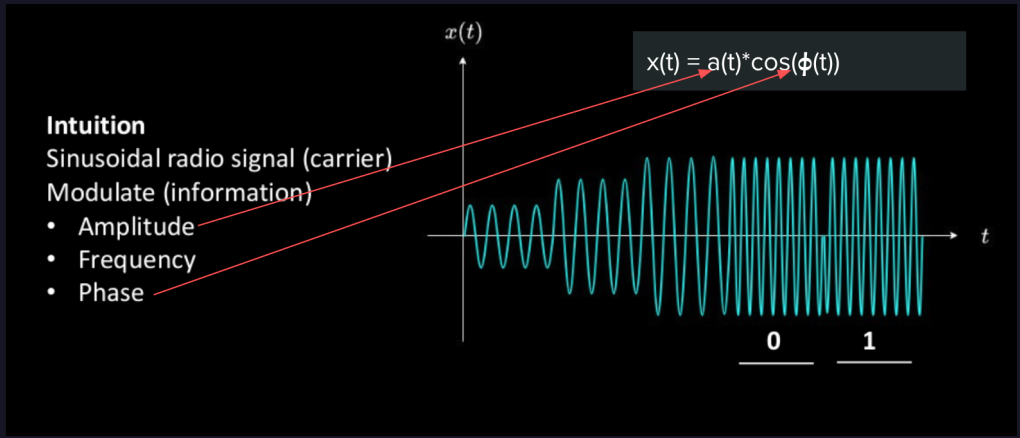
Modulate (information)

- Amplitude
- Frequency
- Phase



Modulated to carry information

Radio Signals

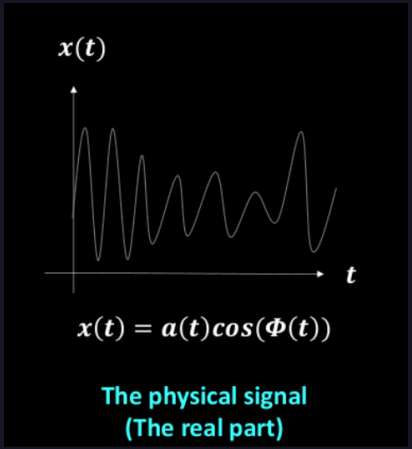


Modulated to carry information

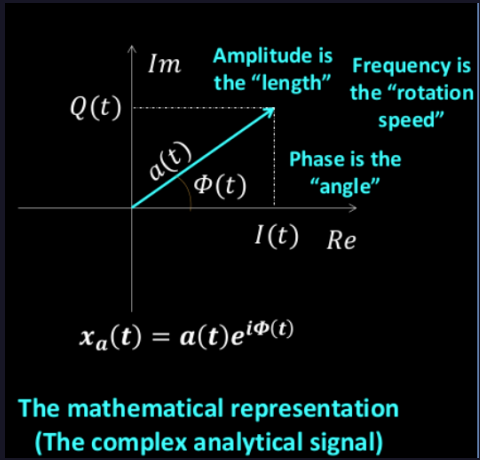
Radio

Digital Signal Processing

Complex representation of real signal allows computers to work on sampled signals:



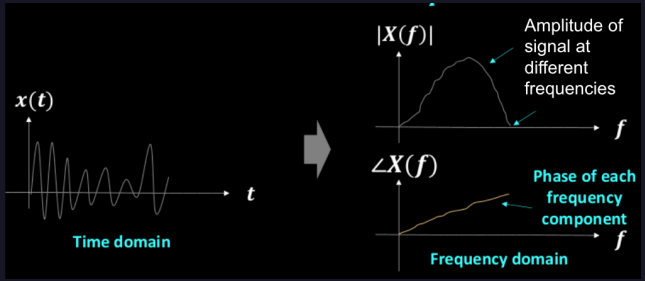
When receiving convert to mathematical repr.



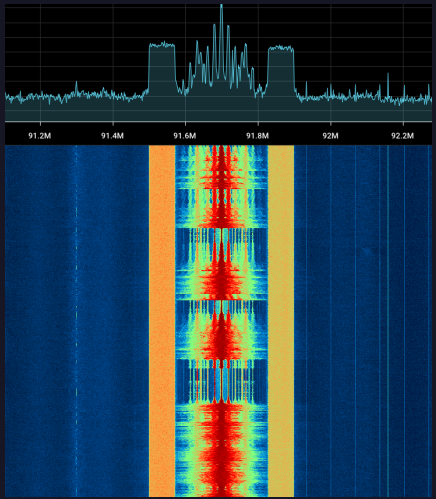
When sending convert to physical signal

Digital Signal Processing

- You get complex samples with an I and a Q-component
- Demodulate RF transmissions directly or you convert it back to the real signal (x(t))
- Also cool useful transformation: **Fourier transform**

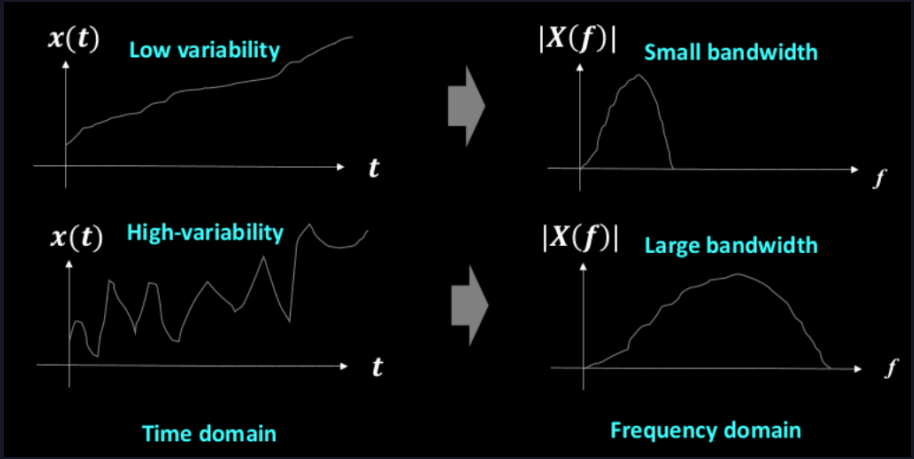


Some basic concepts



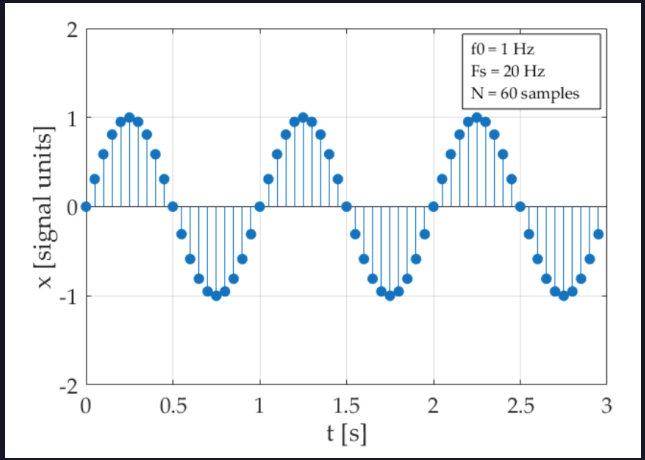
Waterfall diagram - intuitive yet you need to see it

Some basic concepts



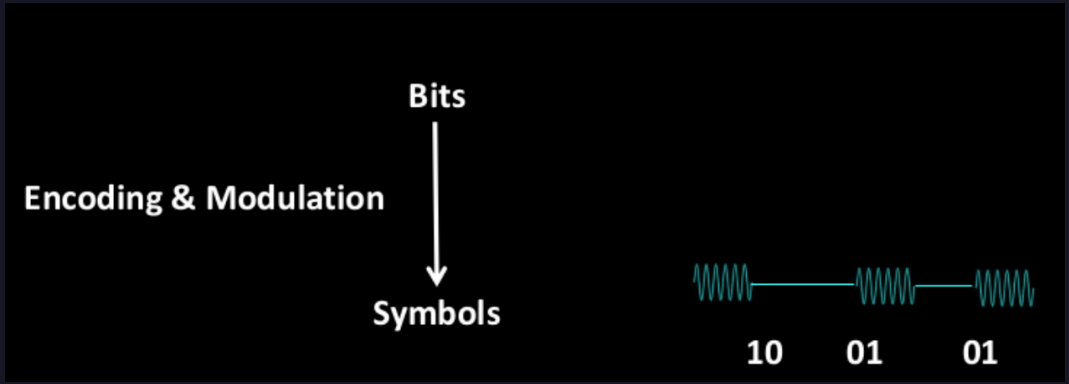
Difference between bandwidths

Some basic concepts



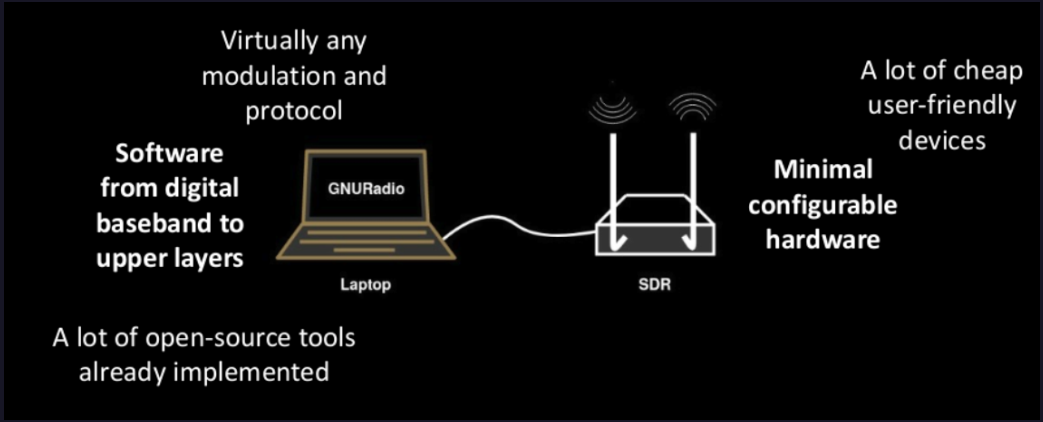
Sampling and Samplerate (=how often/quickly do you sample)

Some basic concepts



On-Off Keying (OOK), FM, PSK, QAM, ODFM = modulating signal amplitude

Software Defined Radios



Software Defined Radios

RTL-SDR

https://www.rtl-sdr.com/

Entry level, simple, only RX, cheap 20 euros

HackRF

https://greatscottgadgets.com/hackrf/

RX/TX, higher bandwidth and range, more expensive

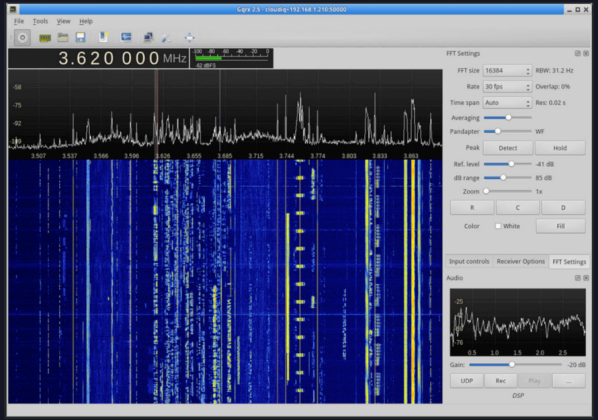
USRP B210

https://www.ettus.com/all-products/ub210-kit/

RX/TX, dual channel, high quality, expensive

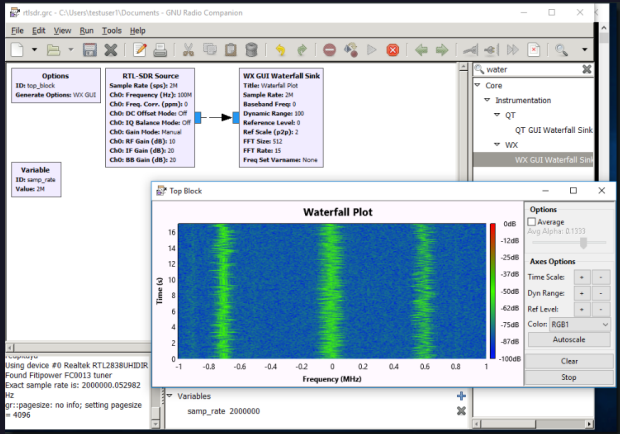
Different hardware exists

Software Defined Radios



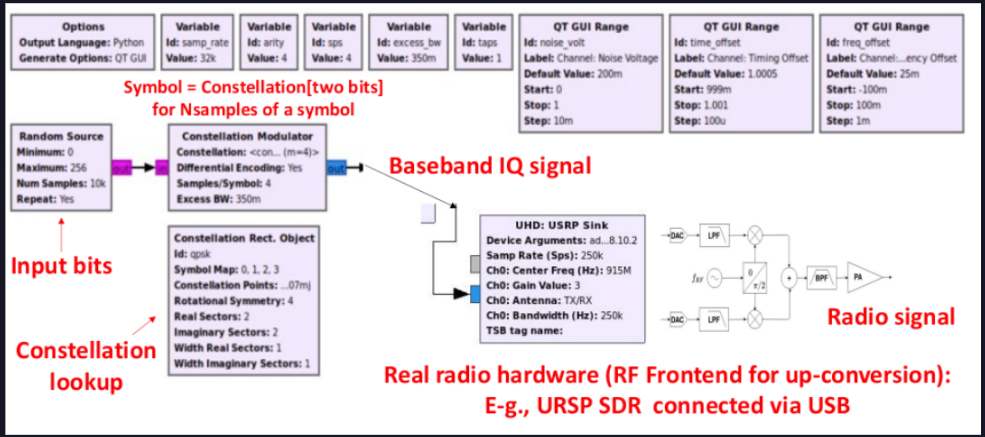
Gqrx: open source, easy to use

Software Defined Radios



GNU radio: steeper learning curve, but powerful and nice

Example RF transmission in gnu radio



Wireless Communication - Challenge

Air-berry

rtl_tcp=10.200.136.50:11234
Wifi: botflag password: miscgang1337

https://cdn.vis.ethz.ch/ctf/air-berry_20230424_102509_432784200_2048000_fc.raw