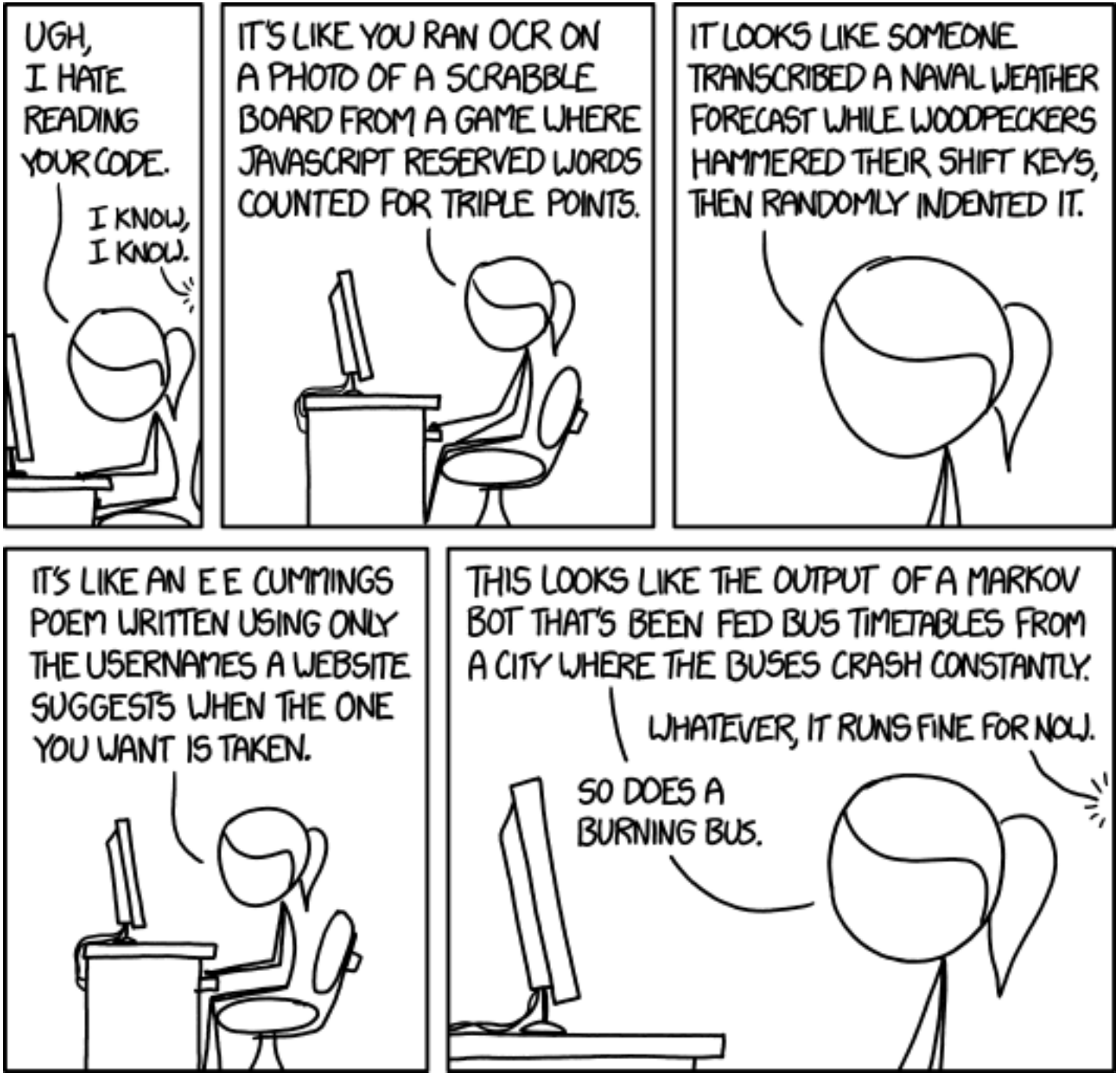


https://xkcd.com/1695/

CS 60:
Computer Networks

Physical layer

Review from last class

Ethernet is the dominant Layer 2 wired protocol

Ethernet frame format:

- Preamble
- dst and src MAC addresses
- Type
- Payload (normally an IP packet)
- CRC

You see 14 header bytes plus payload

NIC strips off preamble and CRC

CRC error detection is more sophisticated than a checksum; it guarantees detection of all burst errors less than r + 1 bits

Switches associate a MAC address with a port when a device transmits

Switch do not (normally) have a MAC address

Does a host need to send to a router for a dst in its subnet? How does it work?

Review: Physical layer moves bits across a Local Area Network

Conceptual network layers

7) Application

Interacts with application programs to send ***messages***
Applications assigned a port, multiple instances can run (many browser pages)
Examples: HTTP, SSH, FTP, SMTP, DNS

4) Transport

Moves ***segments or datagrams***
May provide error control, flow control, application addressing (ports)
Examples: TCP (connection-oriented), UDP (connectionless)
TCP provides sequencing, dropped packet resend, traffic congestion control

3) Network (IP)

Moves ***packets*** between local area networks (routing)
Each computer on the Internet identified by an IP address (IP v4 or v6)
Also called Layer 3 or IP layer (ICMP Ping is here)

2) Link (MAC)

Moves ***frames*** within a local area network (switching)
Each computer identified by a MAC address on its Network Interface Card (NIC)
Also called Layer 2, MAC layer, Data Link layer, or Ethernet layer

Last day for this slide!

1) Physical

How data is physically transmitted

- Transmitter converts logical 1 and 0 ***bits*** to electrical/light pulses or phase/amplitude of radio frequency (RF) and sends down wire or over air
- Receiver converts electrical/light or RF back to logical 1 and 0 bits

https://www.ibm.com/think/topics/osi-model

Agenda



1. Wired physical layer
2. Wireless networks
3. Modulation schemes
4. Wi-Fi

Copper wire is often used for wired connections

Sender

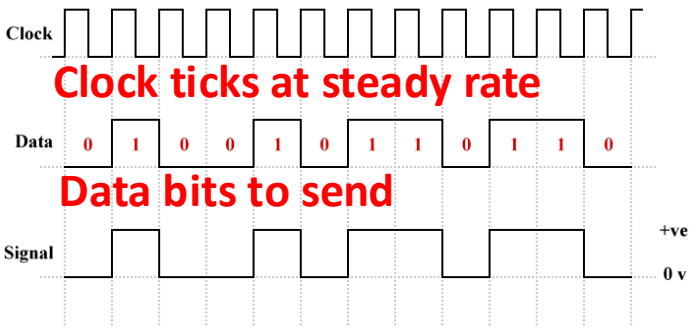
Speeds up to 40 Gbs possible over Cat 8 copper

NRZ = Non-Return to Zero

Receiver

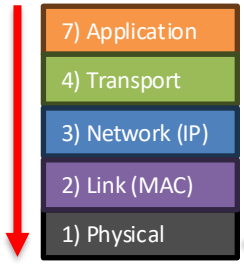


Sender and receiver must get and keep clocks in sync





Bits delivered to Link layer and up the stack to App

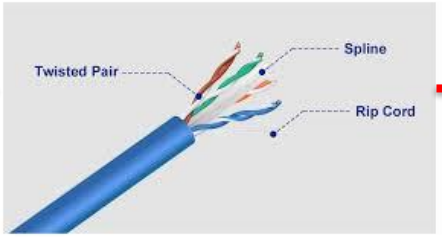


App data goes down the network stack to the physical layer

DAC

Digital to Analog Converter (DAC) At each clock cycle, create electrical pulses

- **1 bit = high**
- **0 bit = low**

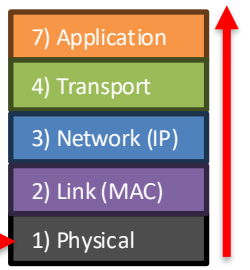


Send electrical pulses over copper wire

ADC

Analog to Digital Converter (ADC) converts electrical pulses into bits

- **High = 1 bit**
- **Low = 0 bit**



Adapted from https://www.technologyuk.net/telecommunications/telecom-principles/line-coding-techniques.shtml

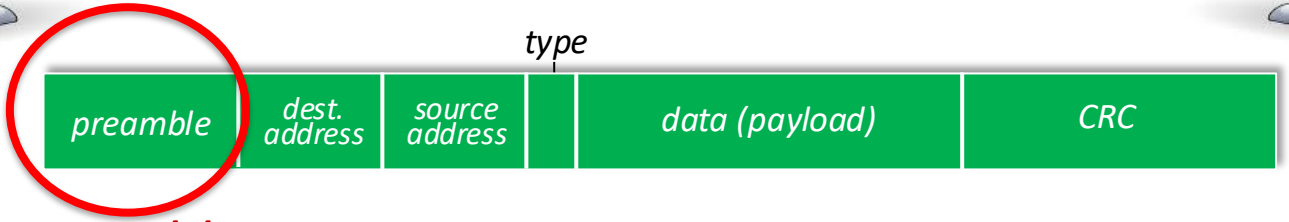
Ethernet preamble keeps sender and receiver's clocks in sync

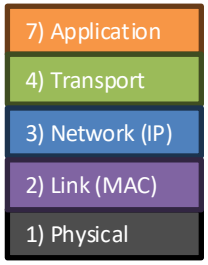
Sender

Receiver

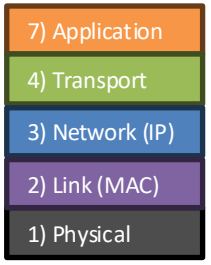


Sending interface adds a preamble to the Link Layer data









Preamble:

- Used to synchronize receiver and sender clocks
- 7 bytes of 10101010 repeated (hey, I'm going to send)
- 1 byte of 10101011 (SFD = Start of Frame Delimiter)
- Receiver knows when frame starts
- Clocks may drift, possible to lose synchronization if many 1's or 0's in a row

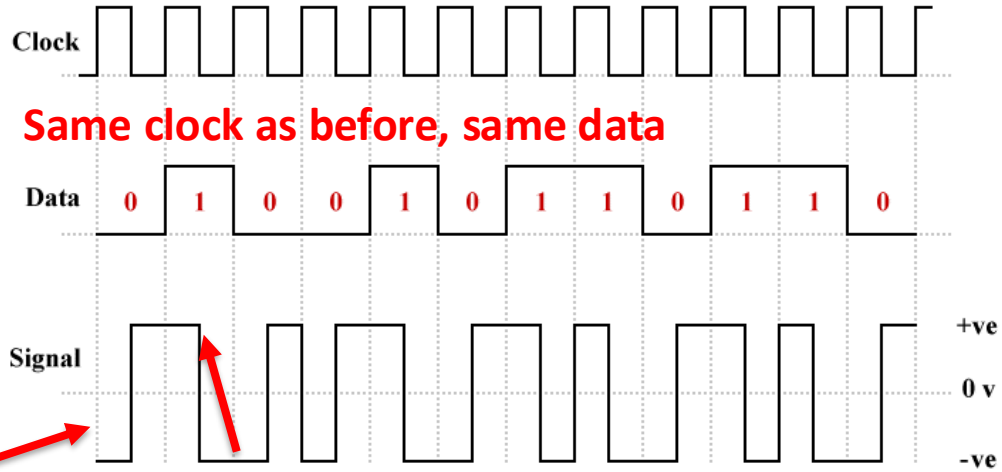
Adapted from https://www.technologyuk.net/telecommunications/telecom-principles/line-coding-techniques.shtml

Manchester encoding can help keep clocks in sync and reduce errors

Sender



7) Application
4) Transport
3) Network (IP)
2) Link (MAC)
1) Physical



Receiver



7) Application
4) Transport
3) Network (IP)
2) Link (MAC)
1) Physical

At each clock cycle always transition

- 0 bit = transition from low to high
- 1 bit = transition from high to low

Transitions keep clocks in sync

There must be an error if no transition during clock cycle

Works better than NRZ in noisy circuits

Adapted from https://www.technologyuk.net/telecommunications/telecom-principles/line-coding-techniques.shtml

Fiber is also common these days

Sender



Two types of fiber

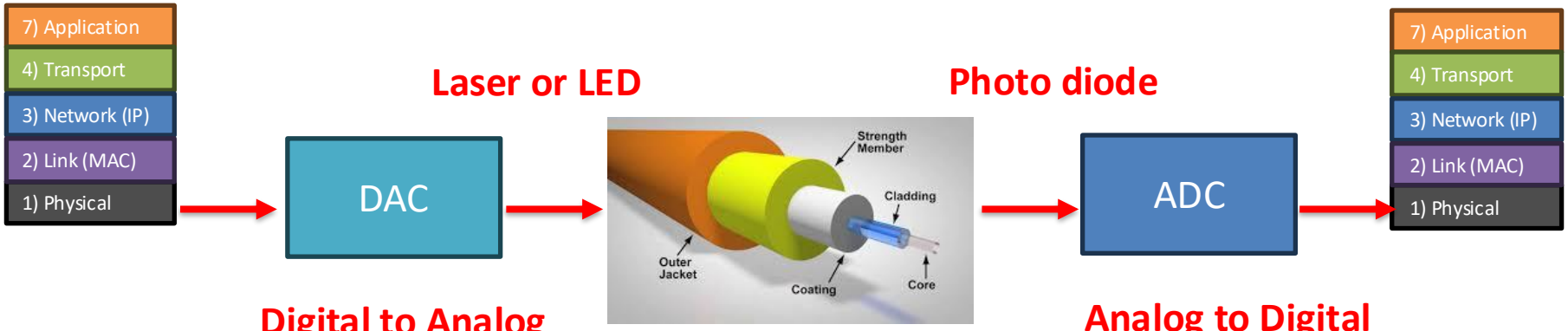
1. Single mode – long range (~40 km without repeaters)
2. Multimode – short range (< 100m)

Petabit speeds theoretically possible

Receiver



Could Manchester encoding be used with fiber? Yes!



Digital to Analog Converter (DAC) At each clock cycle, create light pulses

- **1 bit = laser on**
- **0 bit = laser off**

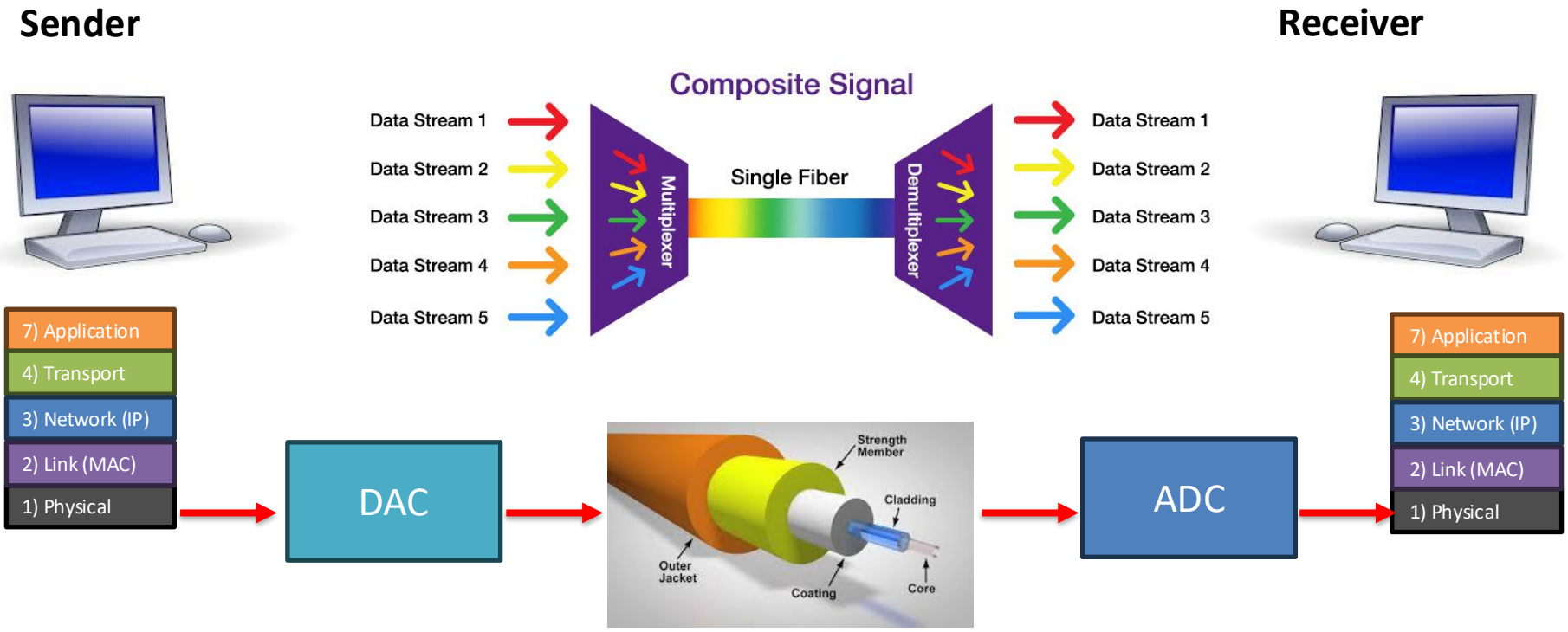
Send light pulses over fiber optic cable

Analog to Digital Converter (ADC) converts light pulses into bits

- **Light = 1 bit**
- **No light = 0 bit**

Adapted from https://www.technologyuk.net/telecommunications/telecom-principles/line-coding-techniques.shtml

Dense Wave Division Multiplexing allows multiple simultaneous streams of data



Dense Wave Division Multiplexing (DWDM)

- Sender gives each data stream a different color of light
- Transmits all colors at once
- Separate colors at receiver

Could you encode multiple frequencies on copper cable
Yes!

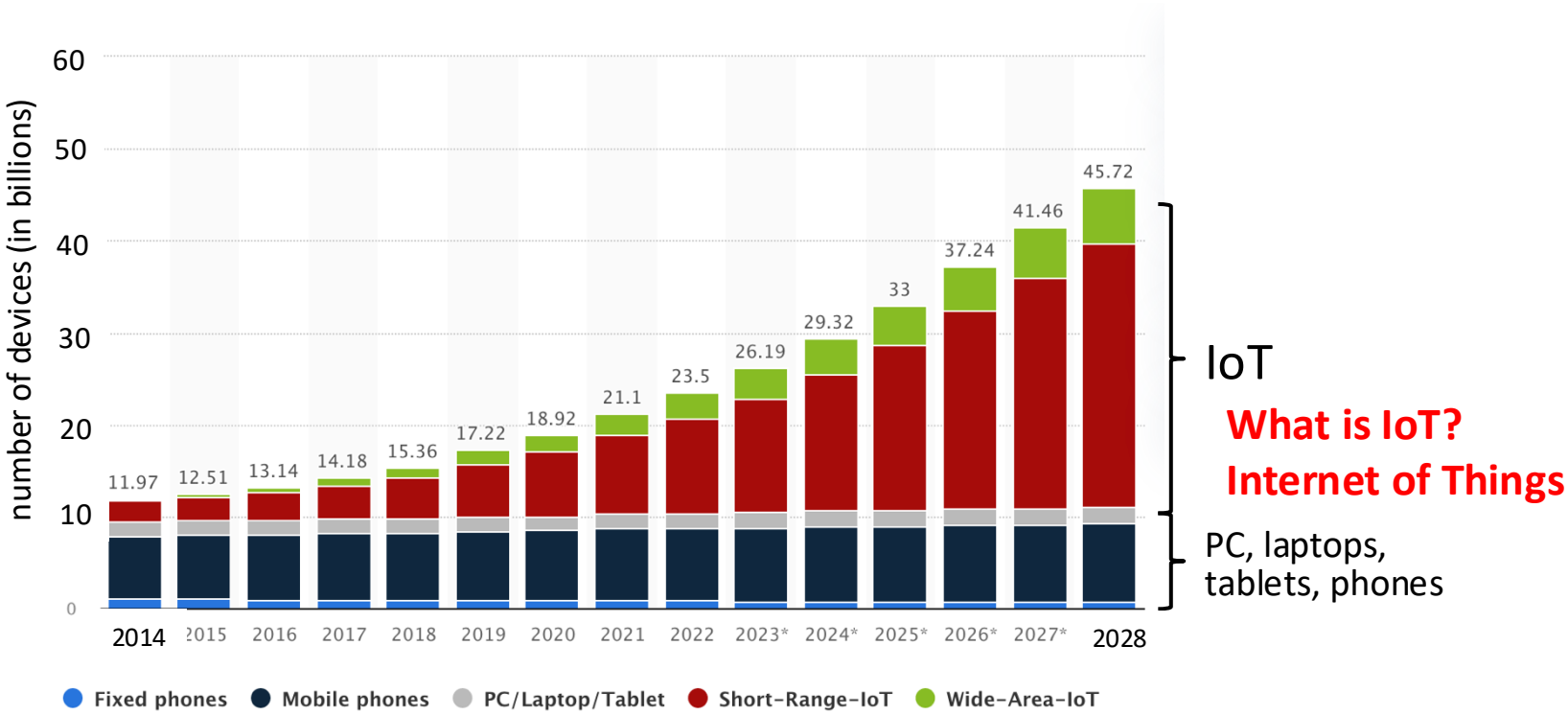
Multiple data streams sent at once (Wi-Fi does this too with RF!)

Adapted from https://www.technologyuk.net/telecommunications/telecom-principles/line-coding-techniques.shtml

Agenda

1. Wired physical layer
2. Wireless networks
3. Modulation schemes
4. Wi-Fi

Lots of connected IoT devices, and more soon!

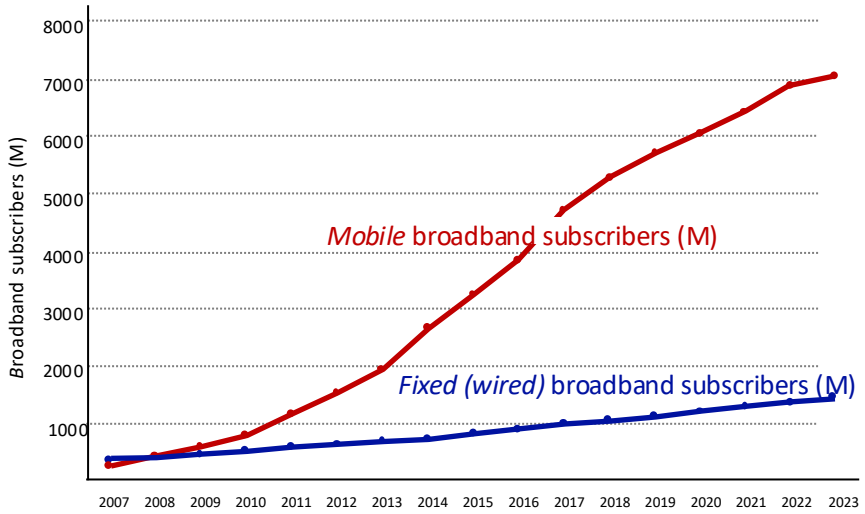


https://www.statista.com/statistics/512650/worldwide-connected-devices-amount/

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

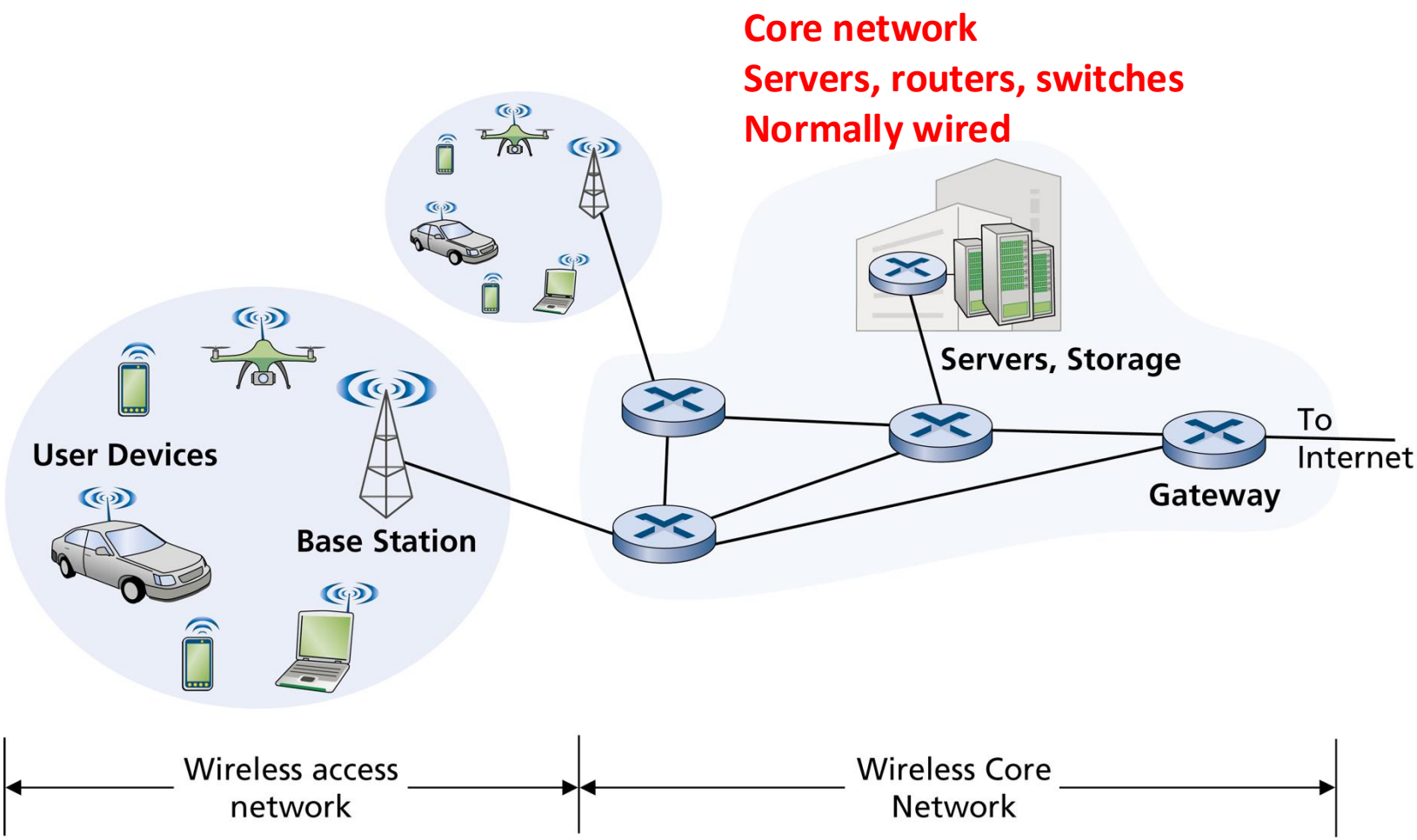
Wireless and Mobile Networks: context

- More mobile-broadband-connected (cellular) devices than fixed-broadband-connected devices (5-1 ratio by 2019)!
  - Wireless connectivity even greater when Wi-Fi users are considered (80% of broadband homes use Wi-Fi)
  - 60% of Internet traffic from major web sites destined to mobile devices



Data source: www.statista.com (1/25)

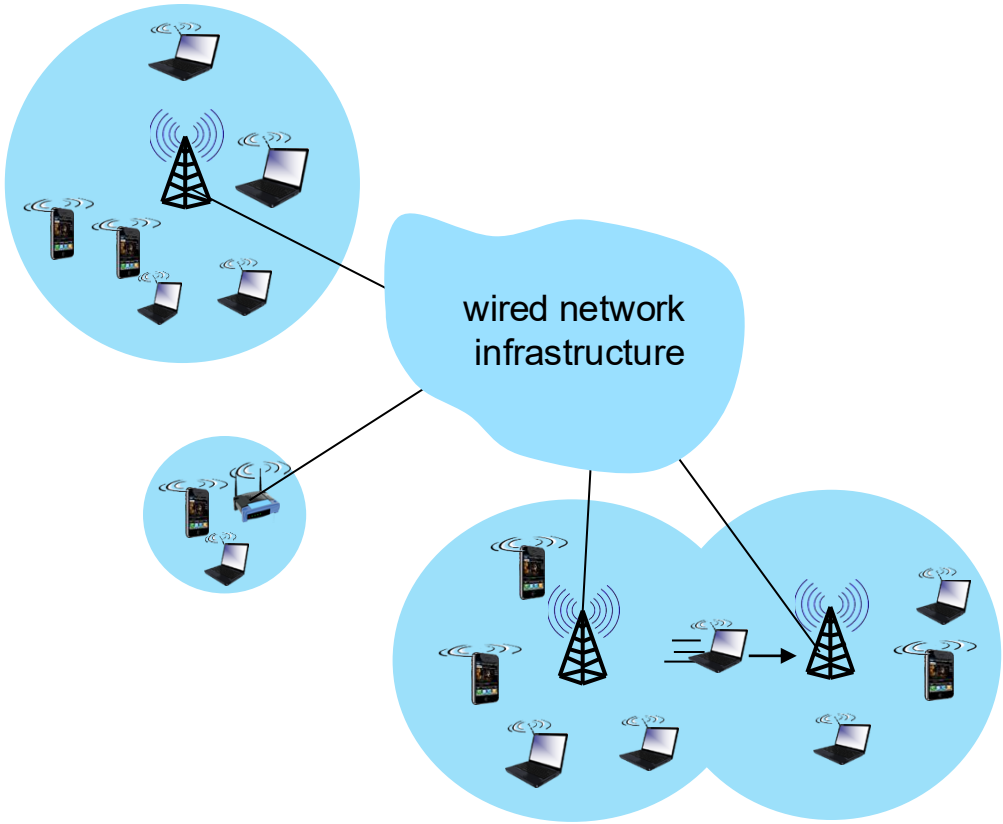
A wireless network comprises an access network and a core network



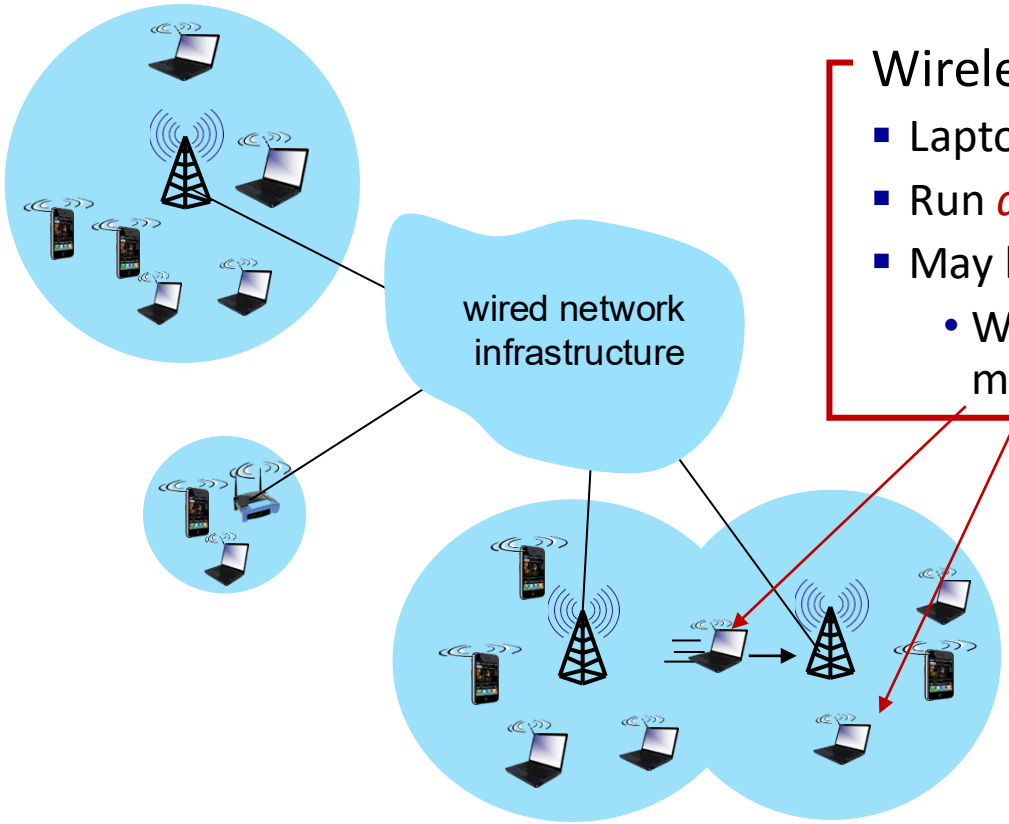
Wireless access network connects devices to larger networks

- **One organization controls access network**
- **Called a Radio Access Network (RAN) or Wireless LAN (WLAN)**

Elements of a wireless network



Elements of a wireless network



Wireless hosts

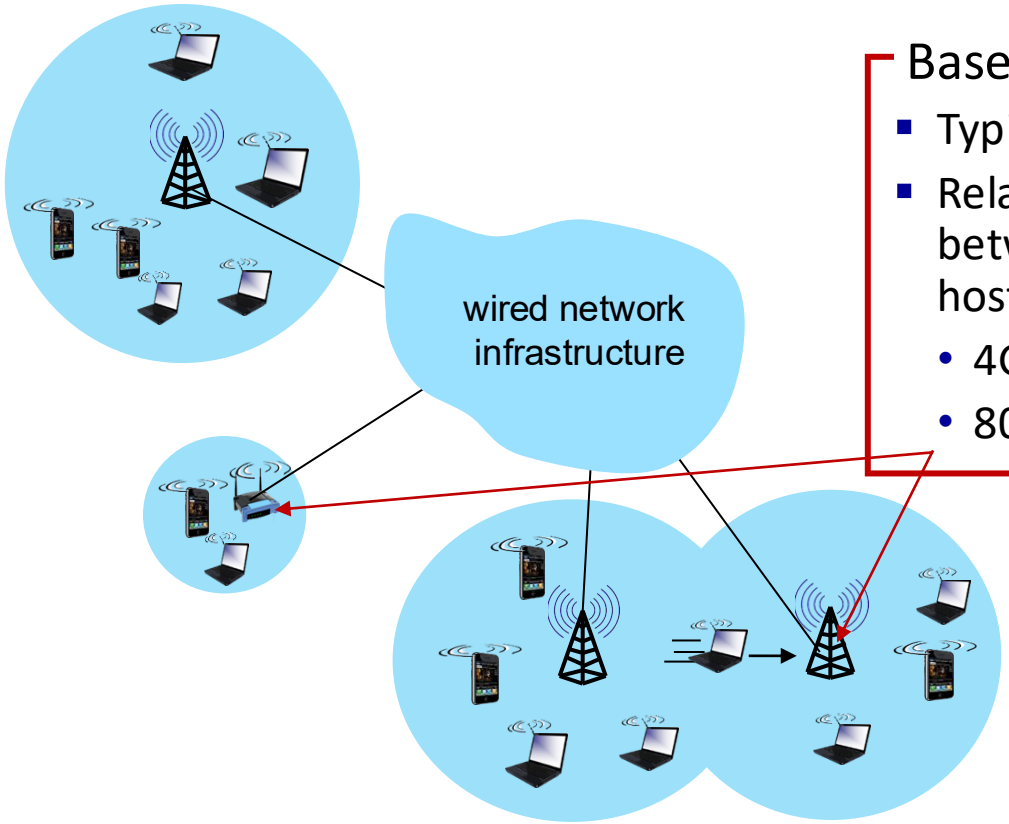
- Laptop, smartphone, IoT



- Run *applications*
- May be stationary (non-mobile) or mobile
  - Wireless does *not* always mean mobility!

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

Elements of a wireless network



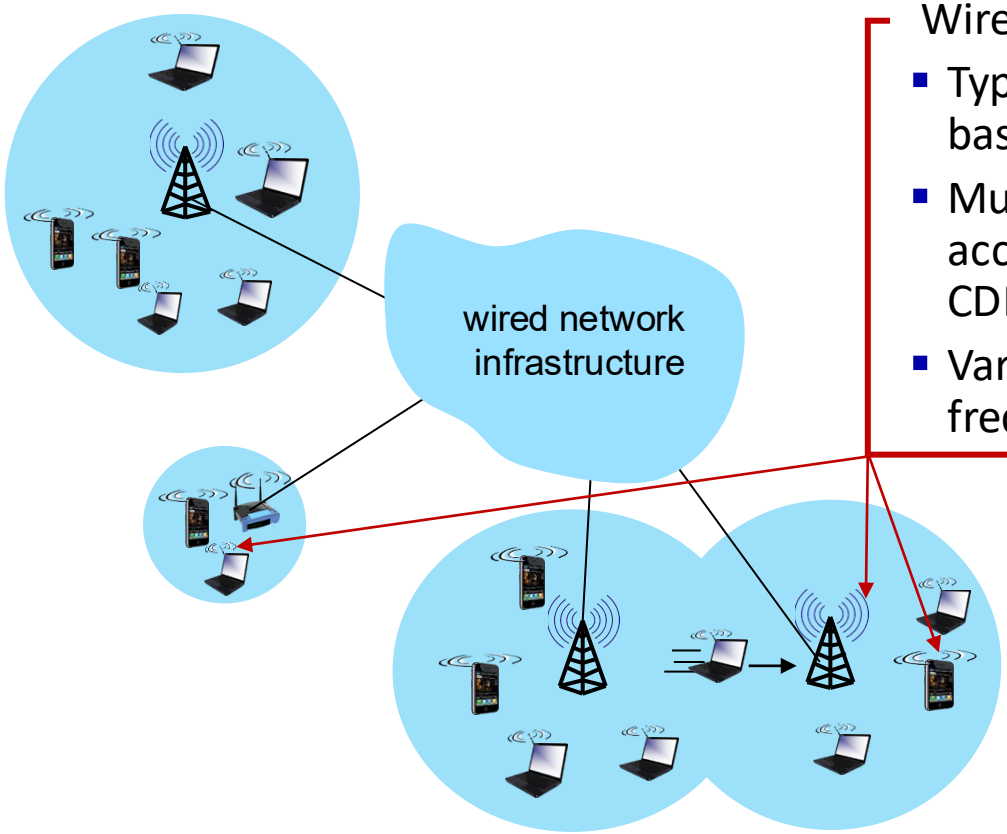
Base station



- Typically connected to wired network
- Relay - responsible for sending packets between wired network and wireless host(s) in its "area"
  - 4G/5G cell towers
  - 802.11 (Wi-Fi) access points (APs)

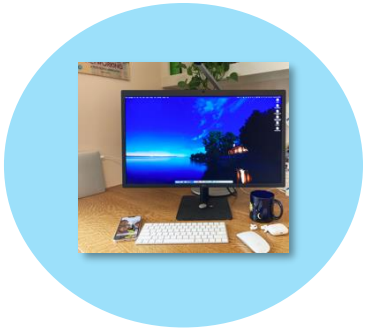
No real counterpart to Base Stations in wired networks

Elements of a wireless network



Wireless link

- Typically used to connect device(s) to base station, also used as backbone link
- Multiple access protocol coordinates link access (random access, FDMA, TDMA, CDMA, polling)
- Various transmission rates and distances, frequency bands

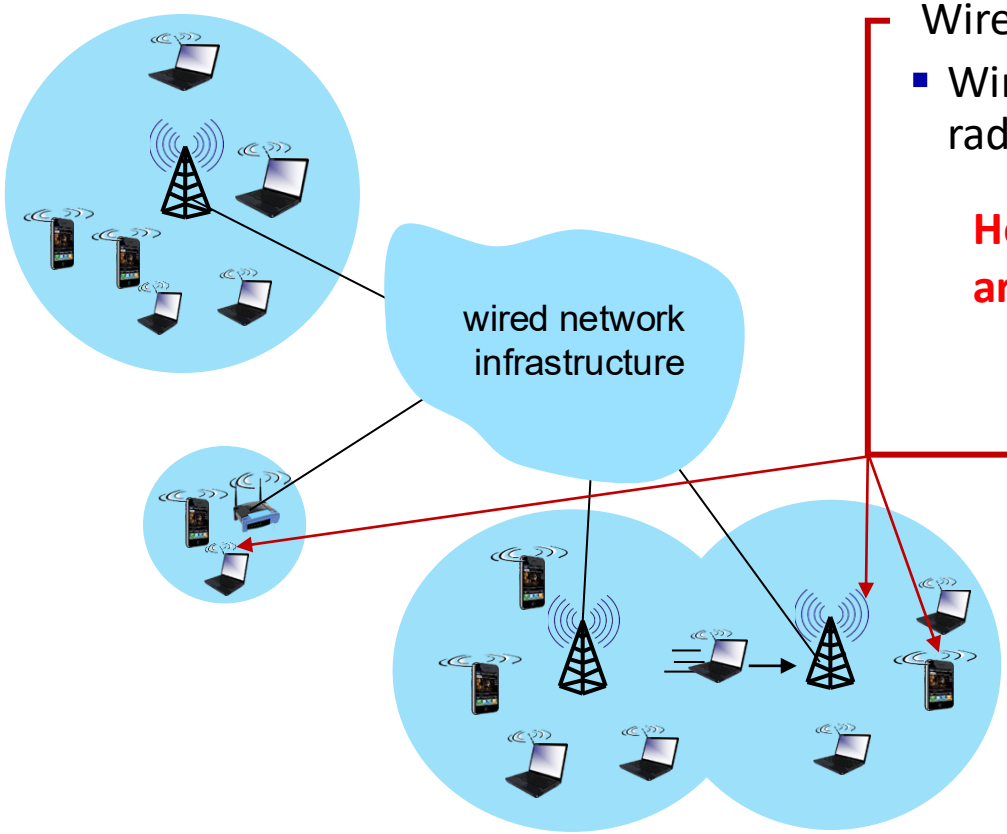


Ad hoc networks: not all wireless networks are connected into a larger network (Bluetooth)

Lab 4 will create ad-hoc communication between devices

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

Elements of a wireless network



Wireless device radio



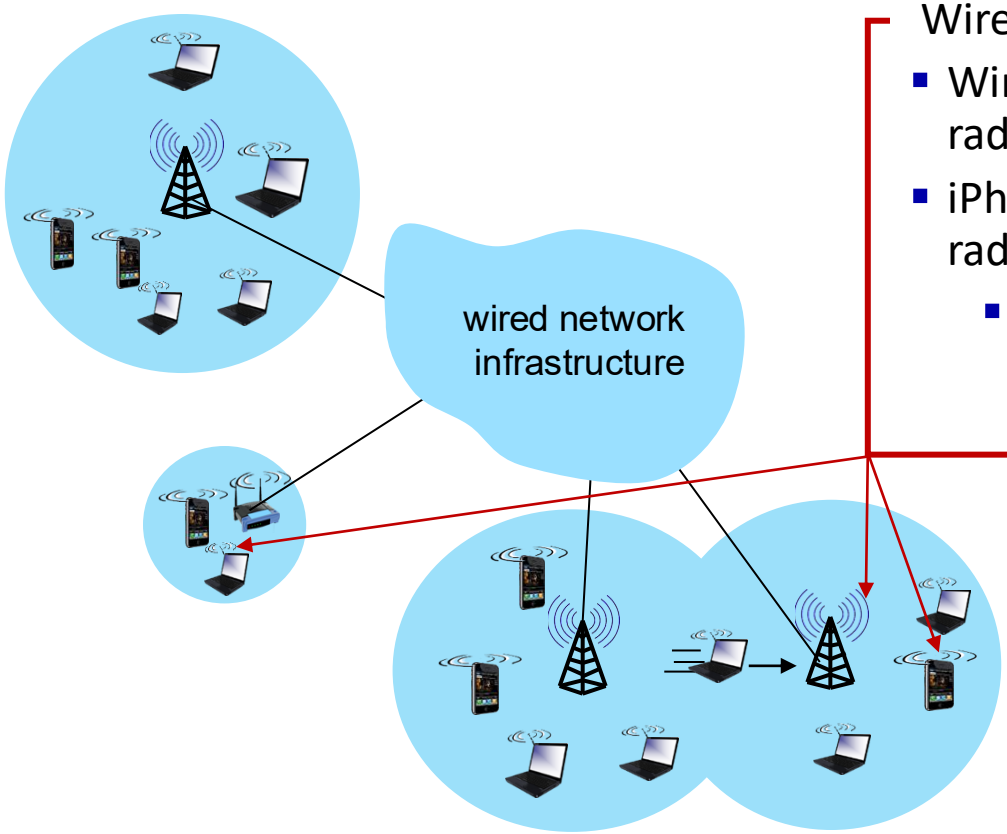
- Wireless devices has different radios for different networks

How many antennas are in an iPhone 16?



Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

Elements of a wireless network

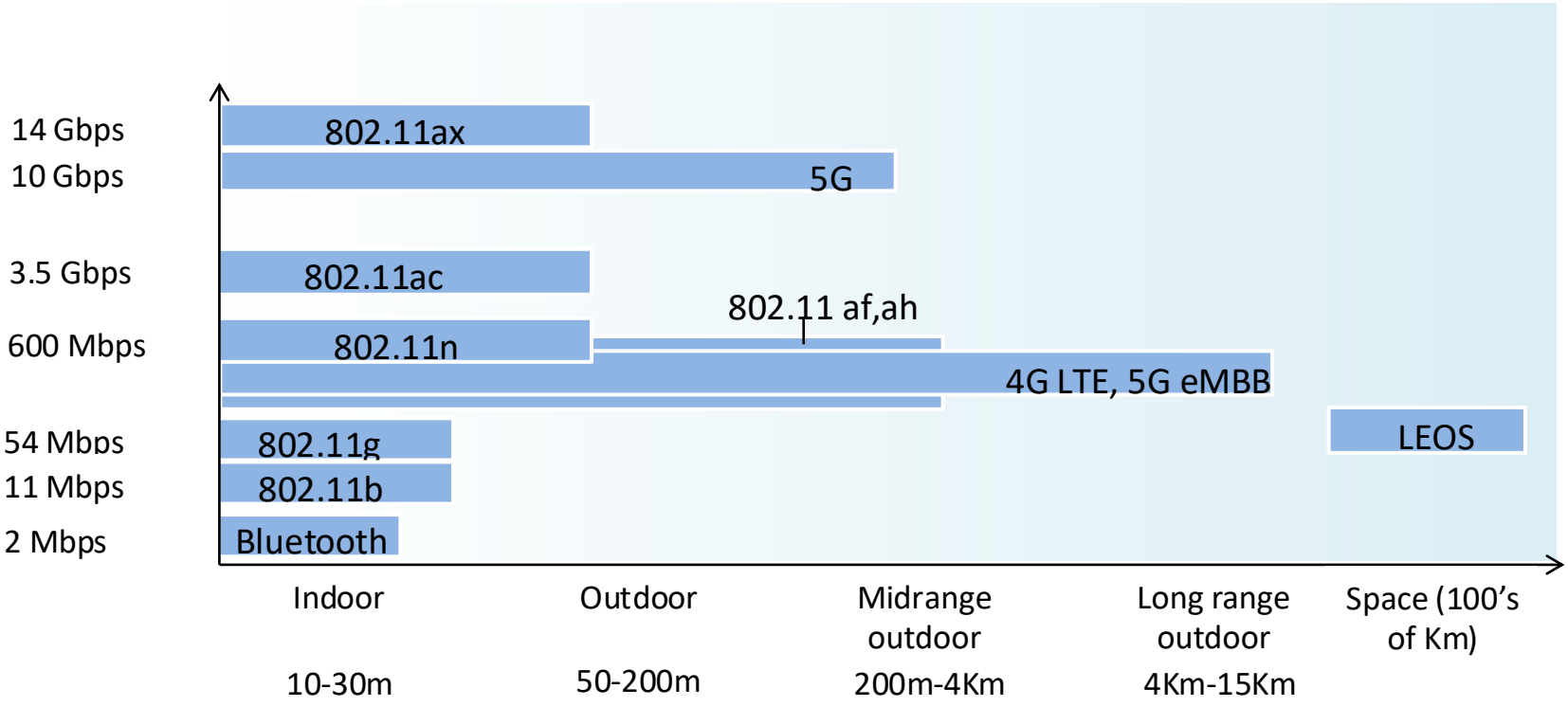


Wireless device radio

- Wireless devices has different radios for different networks
- iPhone16: has ~11 different radios, many antennas
  - 5 different cellular radios, Wi-Fi, Bluetooth, UWB, satellite, NFC, GPS



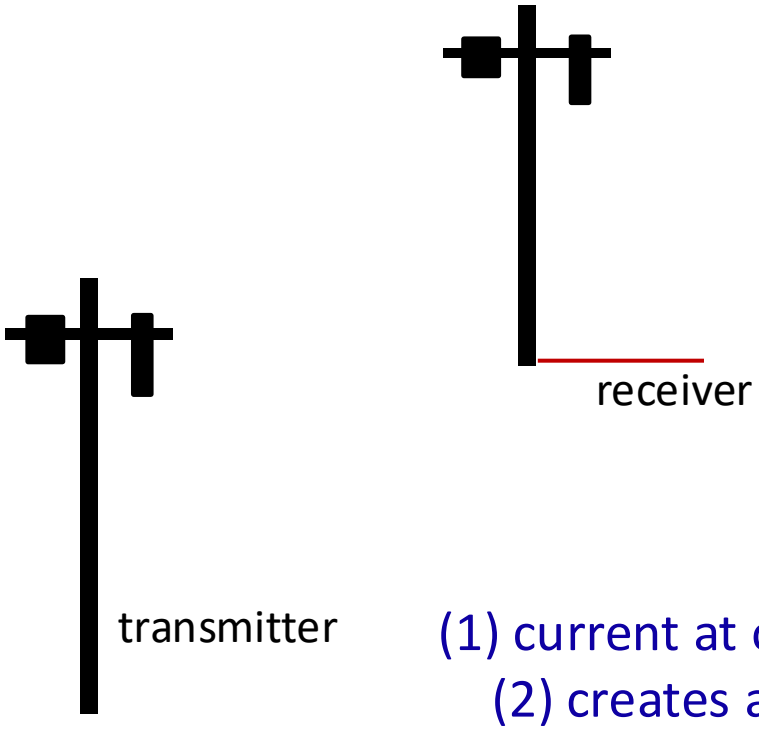
Characteristics of selected wireless links



Generally:
Go fast over short distances
OR
Go slow over long distances

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

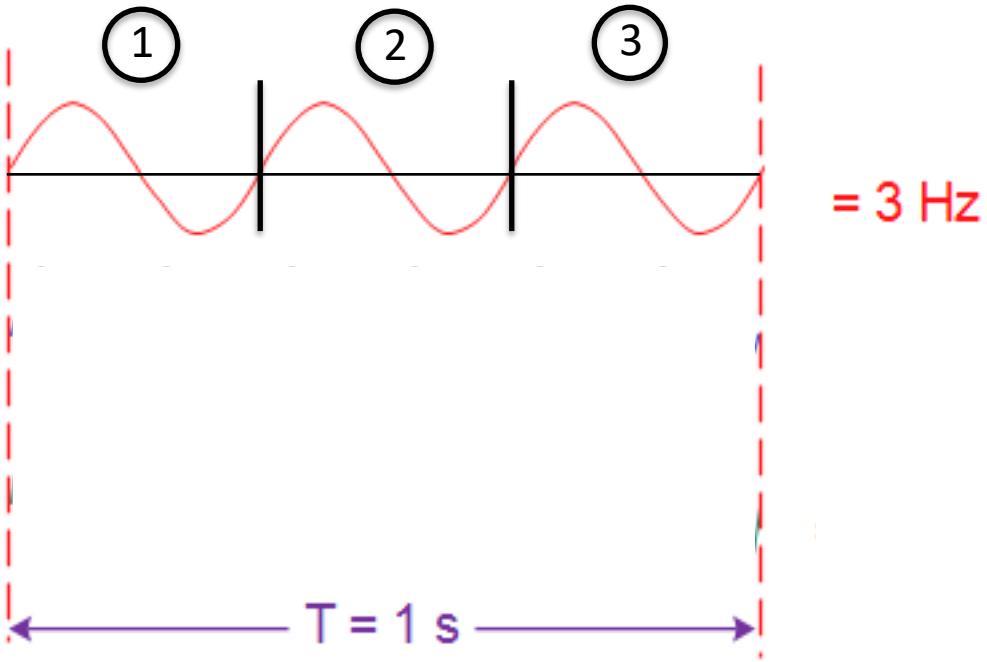
Electromagnetics: enabling communication



(1) current at one location (transmitter) ....
(2) creates an EM field in space ....
(3) induces a current at remote location (receiver)....

slide concept: S. Rangan (NYU)

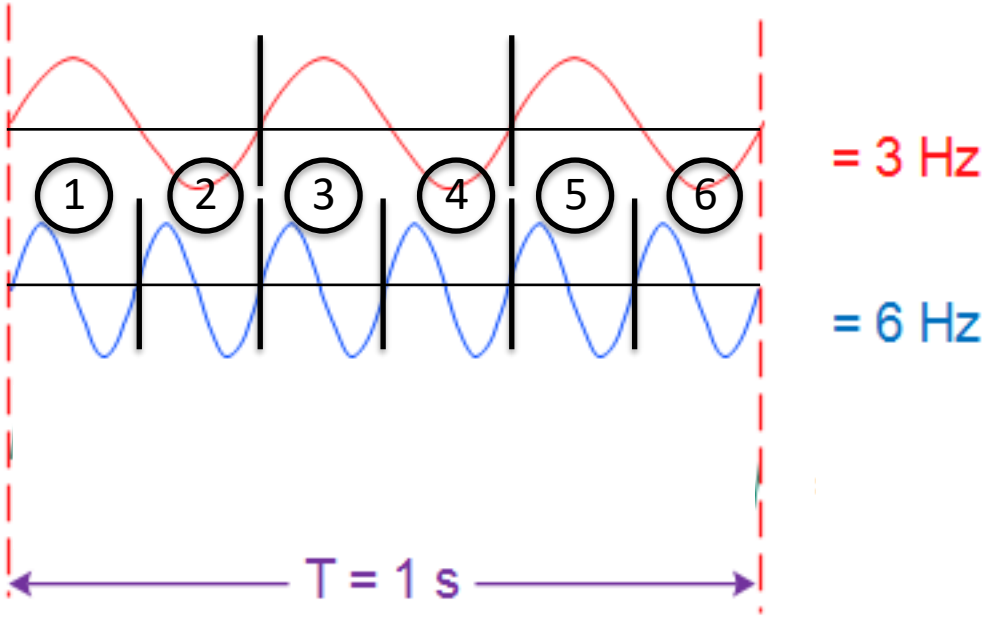
Radio basics: frequency is how many times per second a signal repeats



Frequency is how many times per second a signal repeats

- Measured in Hertz (Hz)

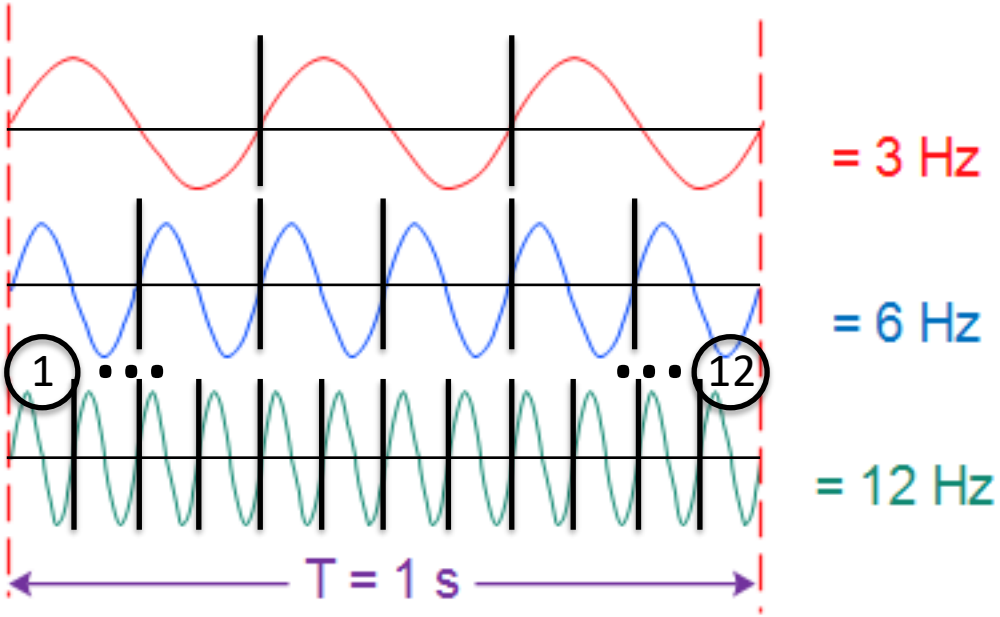
Radio basics: frequency is how many times per second a signal repeats



Frequency is how many times per second a signal repeats

- Measured in Hertz (Hz)

Radio basics: frequency is how many times per second a signal repeats

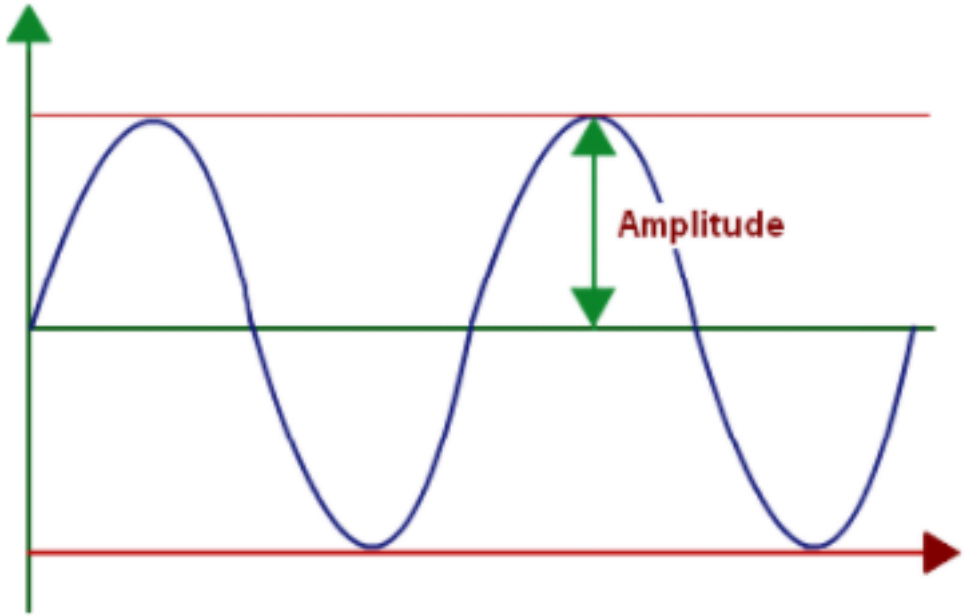


Frequency is how many times per second a signal repeats

- Measured in Hertz (Hz)
- More times a signal repeats per second = higher frequency (12 Hz has 12 repeats in 1 second)
- Fewer times a signal repeats per second = lower frequency (3 Hz signal has 3 repeats in 1 second)

Adapted from https://www.techplayon.com/wavelength-frequency-amplitude-phase-defining-waves/

Radio basics: Amplitude measures the strength of the signal



Amplitude measures signal strength

- Measured from average power to peak
- Not from peak to trough

We will measure signal strength in Lab 4

- **RSSI = Received Signal Strength Indicator**
- **Some Wi-Fi cards will provide this measurement per frame (dongles will)**
- **A few cards provide Channel State Information (gives per subcarrier phase and amplitude)**
- **How might that information be useful?**

Adapted from https://www.techplayon.com/wavelength-frequency-amplitude-phase-defining-waves/

Radio signal characteristics

Power: antenna receive/transmit energy per unit time

- Linear: measured in watts (or milliwatts)
- Logarithmic: measured in decibels (dBm)

$$P_{dBm} = 10 \cdot \log_{10}\left(\frac{P_{mW}}{1mW}\right)$$

- Example:

  P_{mW} = 250 mW (typical max mobile transmit power)

$$P_{dBm} = 10 \cdot \log_{10}\left(\frac{250mW}{1mW}\right)$$

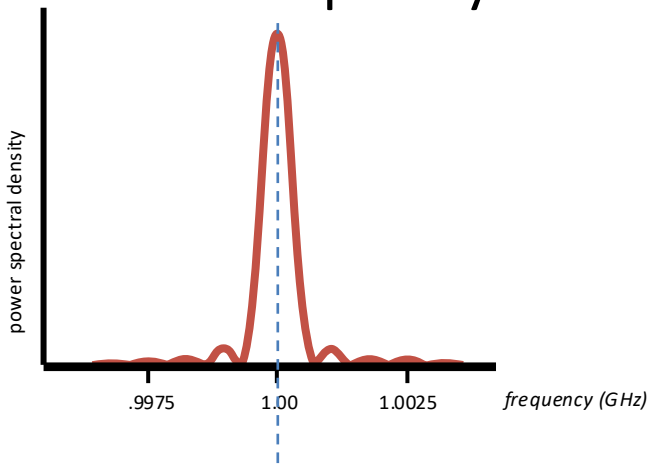
$$= 24 \text{ dBm}$$

Power relative to 1 mW

- **RSSI reports in dBm (Lab 4)**
- **Expected RSSI value?**
- **Wi-Fi normally about -90 to -20 dBm**
- **Don't be alarmed by negative RSSI!**

Power spectral density:

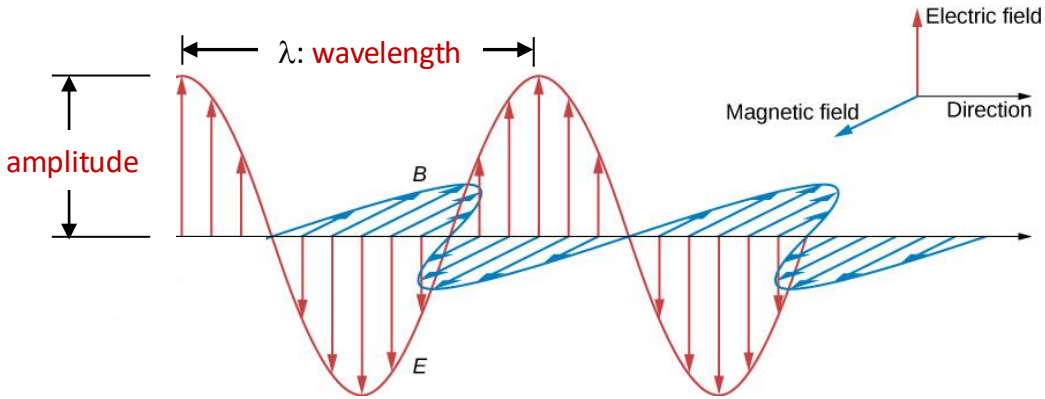
- Power present in signal as a function of frequency



Power density is the amount of energy in an area (e.g., Watts/m^2)
Higher power implies higher signal amplitude
3 dBm increase is roughly a doubling power

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

Radio basics: electromagnetic wave summary



Electromagnetic wave has:

- Wavelength (λ)
- Frequency: speed of light / wavelength = c/λ

Frequency measured in Hertz (cycles/sec)

Wi-Fi wavelength:

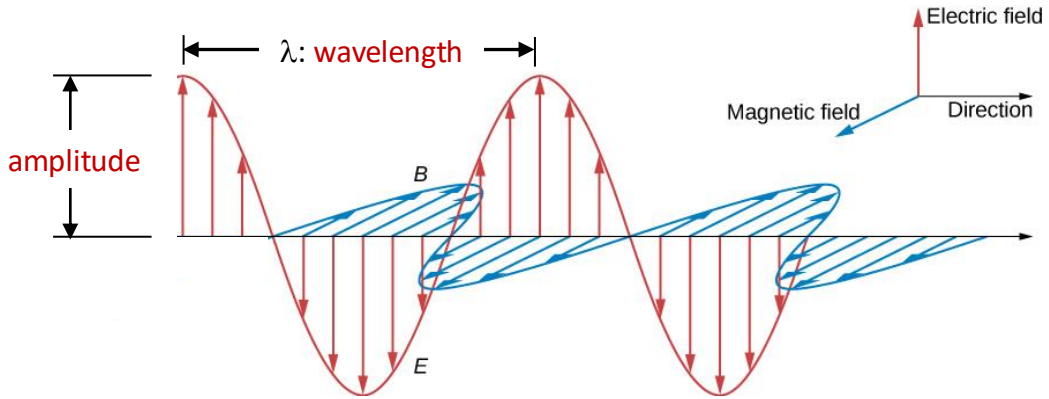
- **~12 cm (2.4 GHz)**
- **~6 cm (5 GHz band)**

Why?

- **Signal moving at speed of light**
- **Frequency gives cycles/sec**
- **Wavelength gives how far signal travels in one cycle**
- **Lower frequency = longer wavelength**
- **Higher frequency = shorter wavelength**

Slide concept: S. Rangan (NYU)

Radio basics: electromagnetic wave summary



wave propagation:

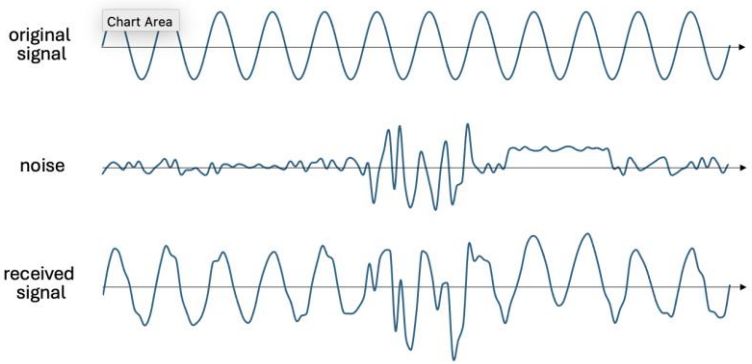
Electromagnetic wave has:

- Wavelength (λ)
- Frequency: speed of light / wavelength = c/λ
- Directionality (of propagation)
- Time-varying amplitude

Slide concept: S. Rangan (NYU)

Signals must be recovered in the presence of noise

- Interference: other transmitters/EM radiaters in same frequency band
  - Hundreds of consumer devices operate in unlicensed 2.4 GHz band (ISM = Industrial, Scientific, and Medical band):
    - Comms: Wi-Fi, Bluetooth, Zigbee
    - Others: Microwave ovens, garage door openers, baby monitors, cordless phones, wireless mics/speakers, radio-controlled drones and toys, amateur radio, ...
- Thermal and electronic noise in receiver:
  - Natural thermal variations, imperfections in electronics



Original signal, noise, and noisy received signal

Received signal is the superposition of the signal plus noise

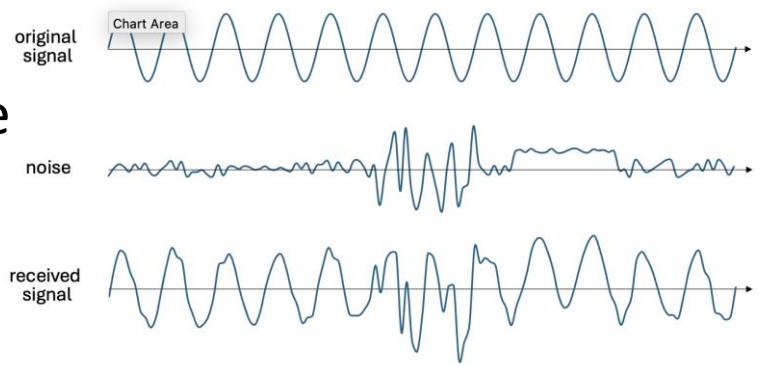
Signal to Noise Ratio (SNR) measures the difference

SNR: ratio of signal power to noise power (often measured in dB)

- Fundamental measure of channel "quality"

$$\text{SNR (dB)} = 10 \cdot \log_{10} \left(\frac{\text{received signal power}}{\text{noise power}} \right)$$

- SNR of 0 implies equal signal and noise
- High (or low) SNR: easy (or hard) to extract signal from signal+noise
- Typical ranges for current radios for good throughput:
  - Lower limit for cellular: -10 to -6 dB
  - Lower limit for Wi-Fi: around 20dB depending on modulation



Original signal, noise, and noisy received signal

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

Signals attenuate (weaken) as they travel

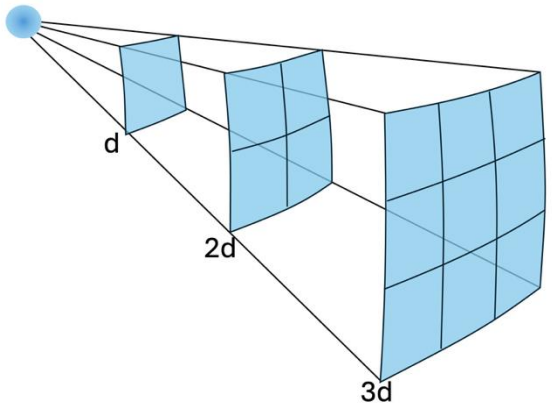
Wireless radio signal attenuates (loses power) as it propagates

Path loss

(aka *fading*) reduction in power density (attenuation) of an electromagnetic wave as it propagates from transmitter to receiver

$$P_r = P_t \cdot G_t \cdot G_r \cdot \left(\frac{\lambda}{4\Pi d}\right)^2$$

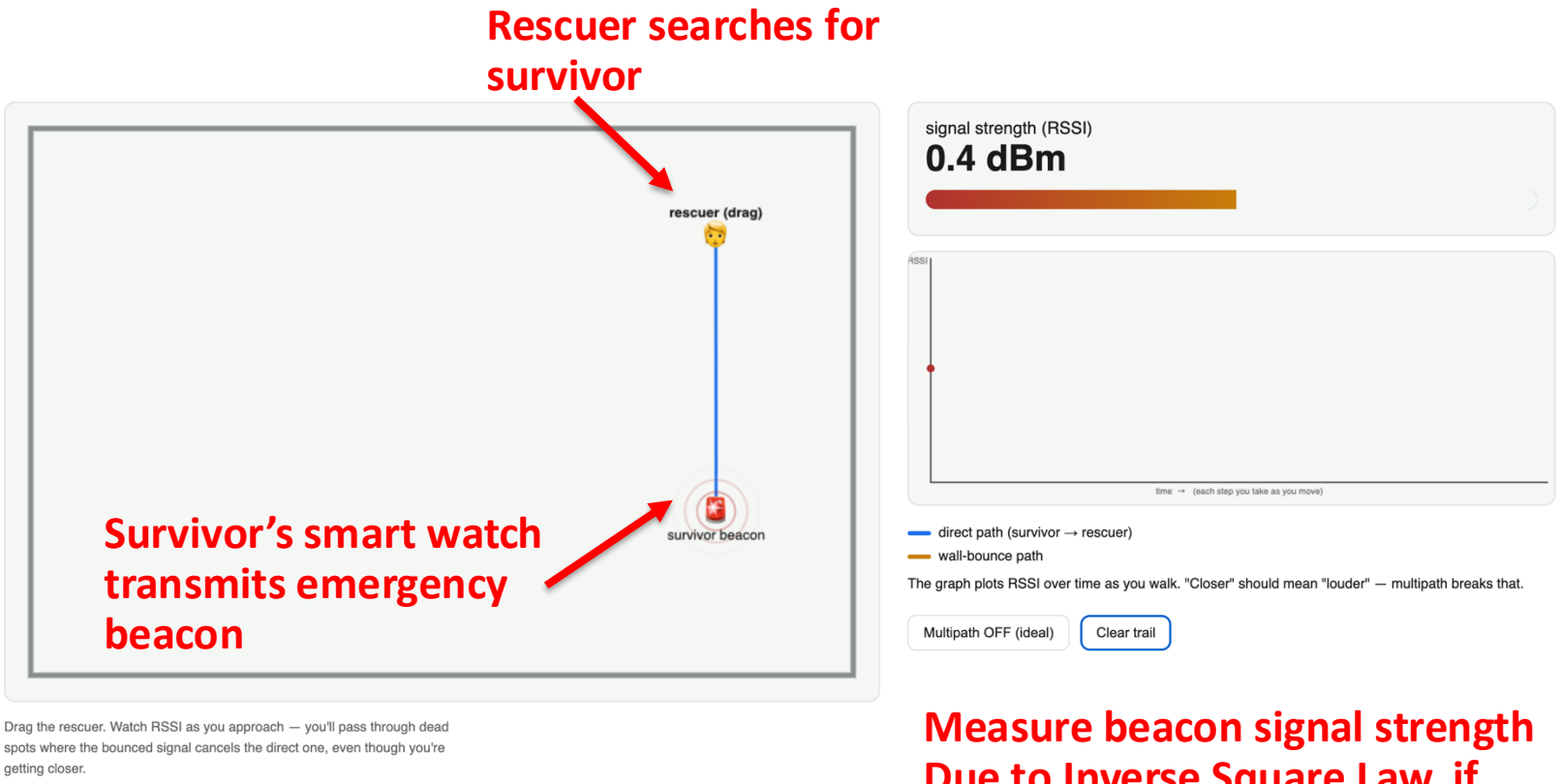
P_r = power received
P_t = power transmitted
G_t = gain of the transmitting antenna
G_r = gain of the receiving antenna
λ = wavelength
d = distance between transmitter and receiver



Inverse Square Law: Signal strength attenuates with the square of distance in free space
Double the distance, means ¼ power

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

Lab 4 uses path loss to rescue survivors in an emergency like an earthquake or fire



Scenario:
After an earthquake survivors are trapped
Suppose a survivor's smart watch sends a Wi-Fi emergency beacon
Rescuers pick up beacon to locate survivor

Measure beacon signal strength
Due to Inverse Square Law, if rescuer is:

- **Moving closer, signal strength *should* increase**
- **Moving farther, signal strength *should* decrease**

https://tjp.cs.dartmouth.edu/cs60/code/day11/rescuer.html

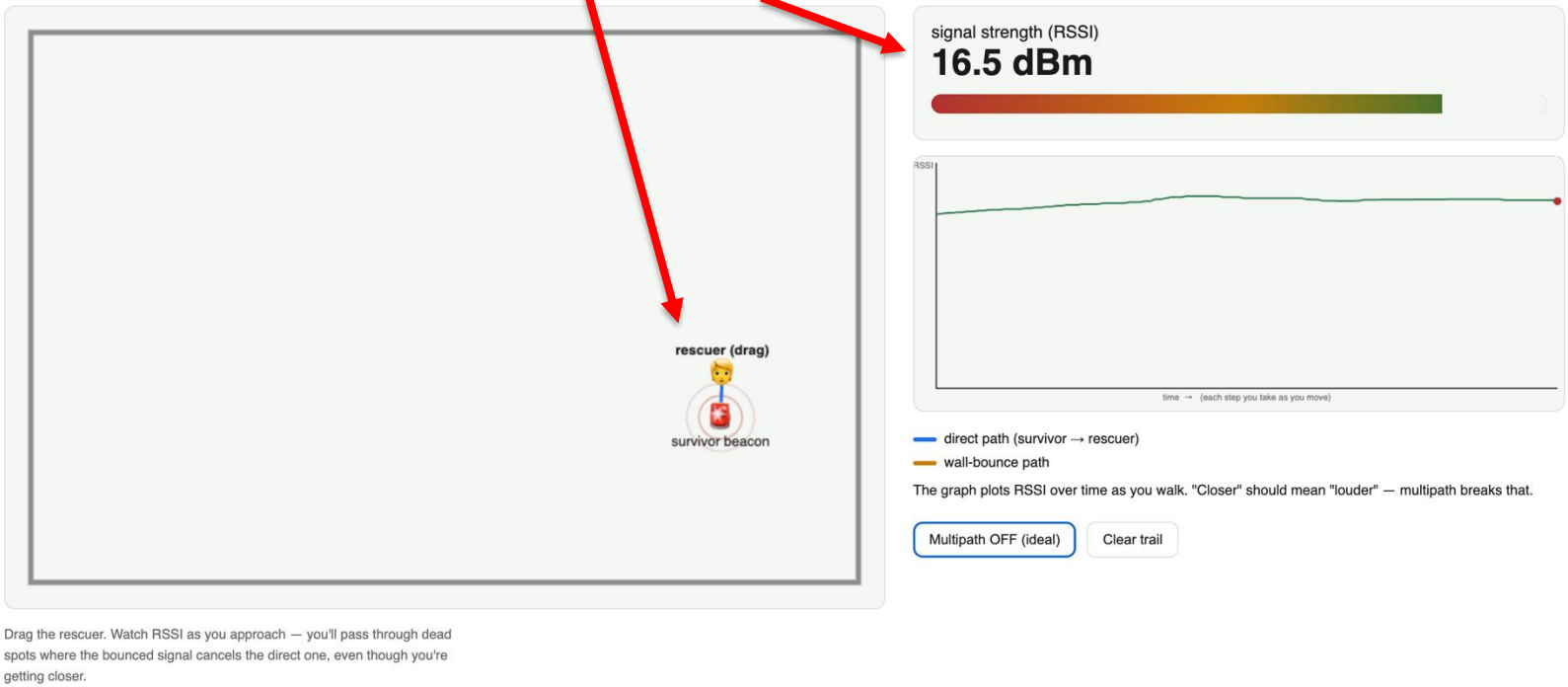
Lab 4 uses path loss to rescue survivors in an emergency like an earthquake or fire



https://tjp.cs.dartmouth.edu/cs60/code/day11/rescuer.html

Lab 4 uses path loss to rescue survivors in an emergency like an earthquake or fire

Move closer
Signal strength increases further



Be careful!

Multipath can cause misleading cues

What is multipath?

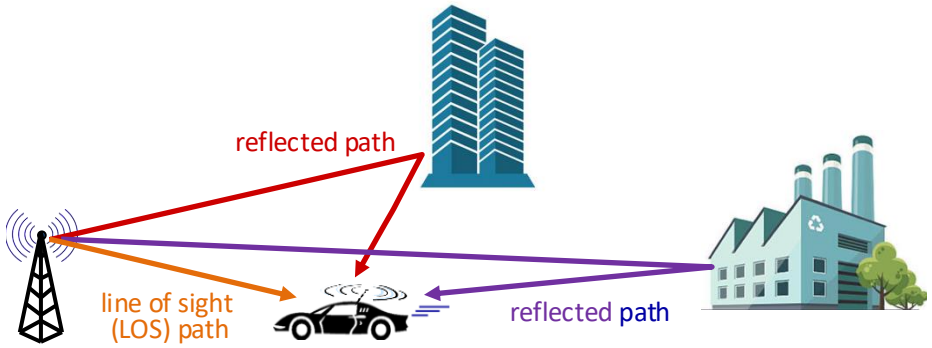
This approach gives a *rough* estimate of whether rescuer is moving closer/farther (but normally works reasonably well)

Try it yourself

https://tjp.cs.dartmouth.edu/cs60/code/day11/rescuer.html

Signals can reflect from object causing multiple paths to the receiver

Multipath propagation: radio signal reflects off objects ground, built environment, arriving at destination at slightly different times



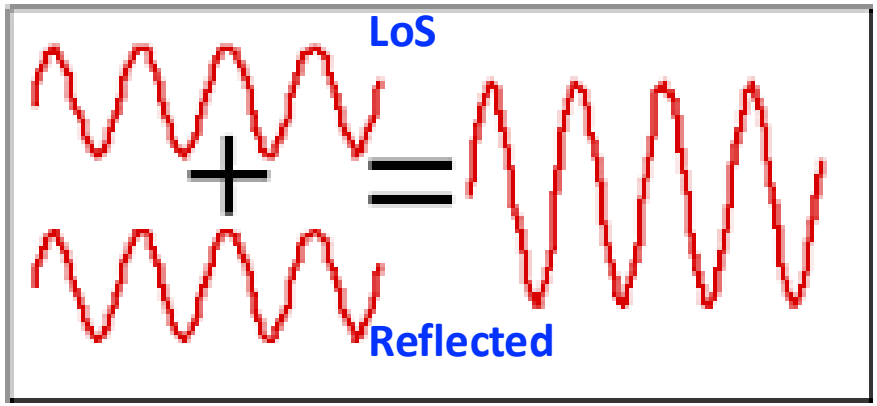
Multipath = multiple copies of the signal arrive at the receiver

- **Line of Sight (LoS) component is usually present unless occluded**
- **Plus, all reflected paths**
- **All paths are superimposed on each other at the receiver**

We will use multipath in Lab 4 to create a secret on two devices

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

Multipath can cause constructive or destructive interference

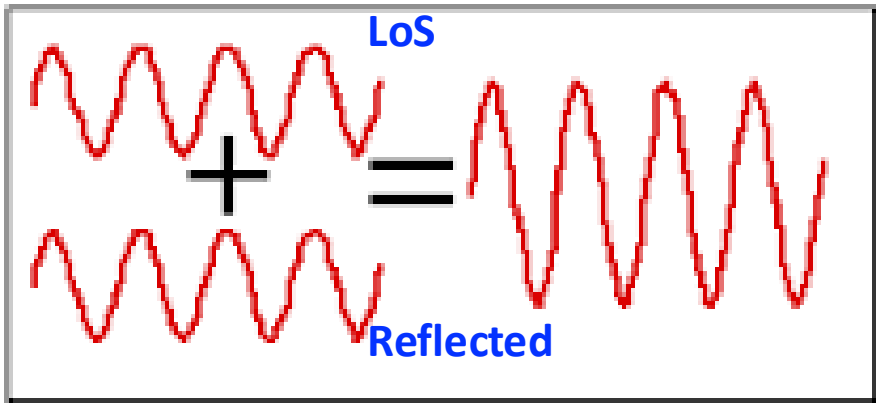


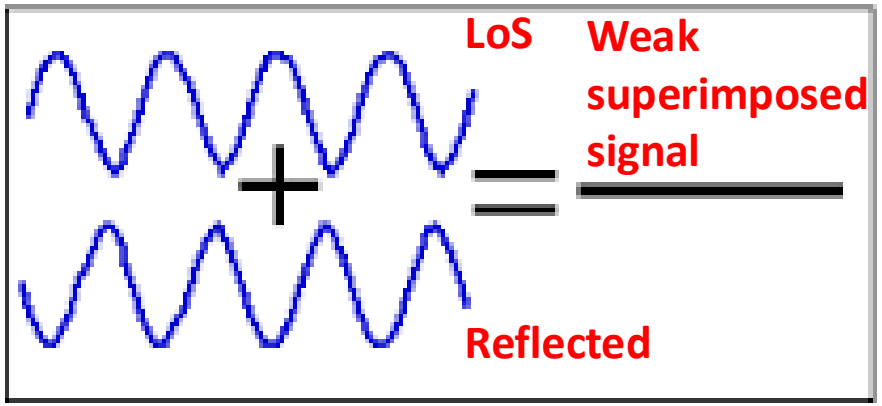
Constructive Interference

If signals that took multiple paths arrive *in phase* with each other

- Waves add up
- Results in greater signal strength than LoS alone
- Called *Constructive* Interference

Multipath can cause constructive or destructive interference





Constructive Interference

If signals that took multiple paths arrive *in phase* with each other

- Waves add up
- Results in greater signal strength than LoS alone
- Called *Constructive* Interference

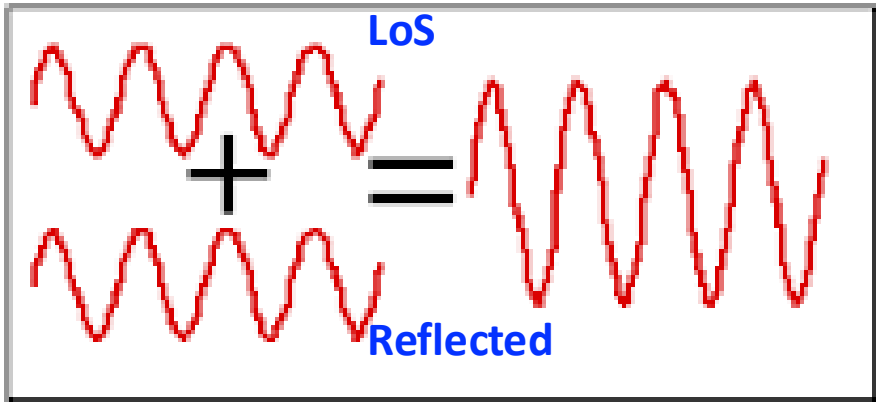
Destructive Interference

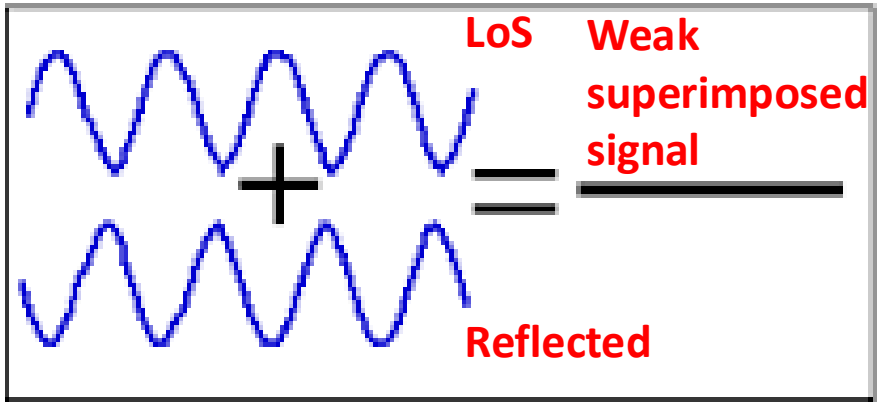
If signals that took multiple paths arrive *out of phase* with each other

- Waves cancel each other
- Results in lower signal strength than LoS alone
- Called *Destructive* Interference

Superimposed signal tends not to cancel completely. Why?

Destructive interference tends not to cancel the signal completely





Constructive Interference

If signals that took multiple paths arrive *in phase* with each other

- Waves add up
- Results in greater signal strength than LoS alone
- Called *Constructive* Interference

Destructive Interference

Superimposed signal at receiver

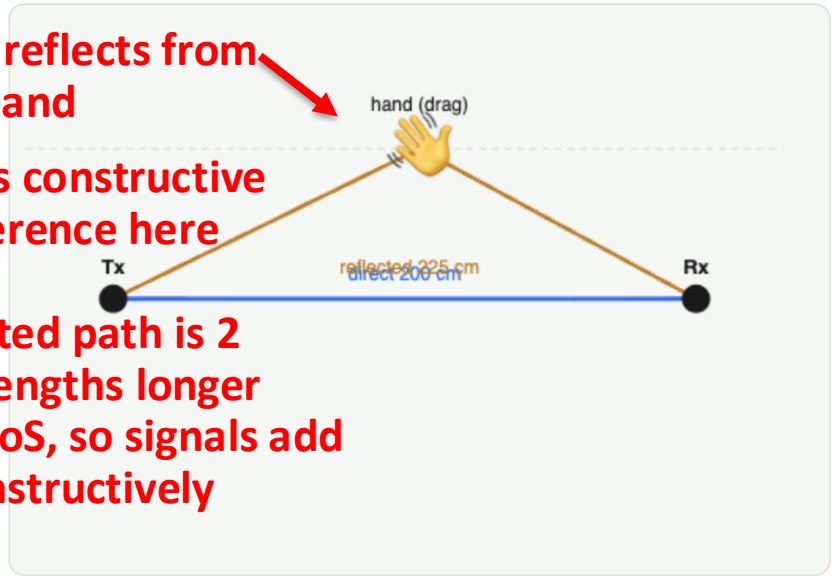
- **LoS signal will travel the shortest distance (straight line between two points)**
- **Multipath signal will attenuate more as it travels further (Inverse Square Law) than LoS**

Lab 4 uses constructive/destructive interference to generate an encryption key

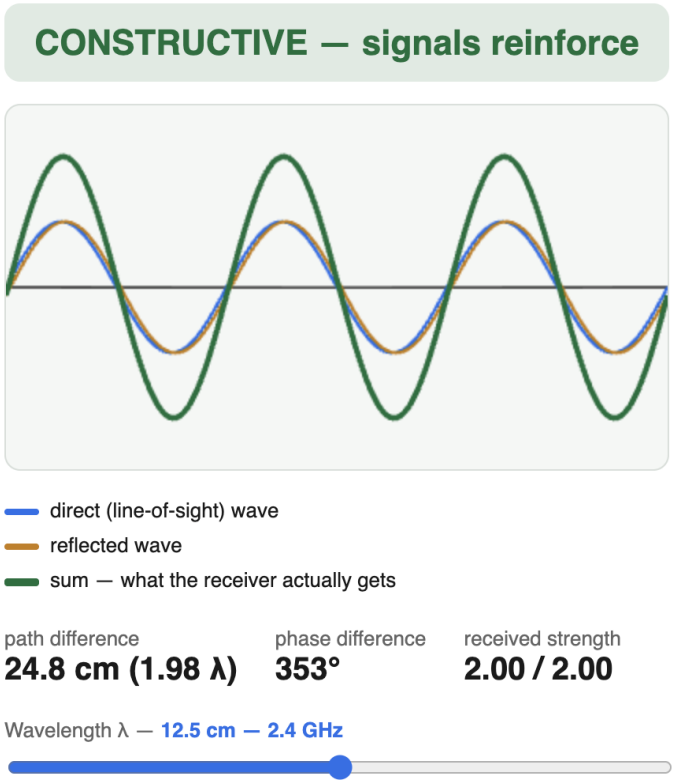
Signal reflects from your hand

Causes constructive interference here

Reflected path is 2 wavelengths longer than LoS, so signals add up constructively



Drag the amber reflector. Moving it changes the bounced path's length, which shifts its phase relative to the direct path.



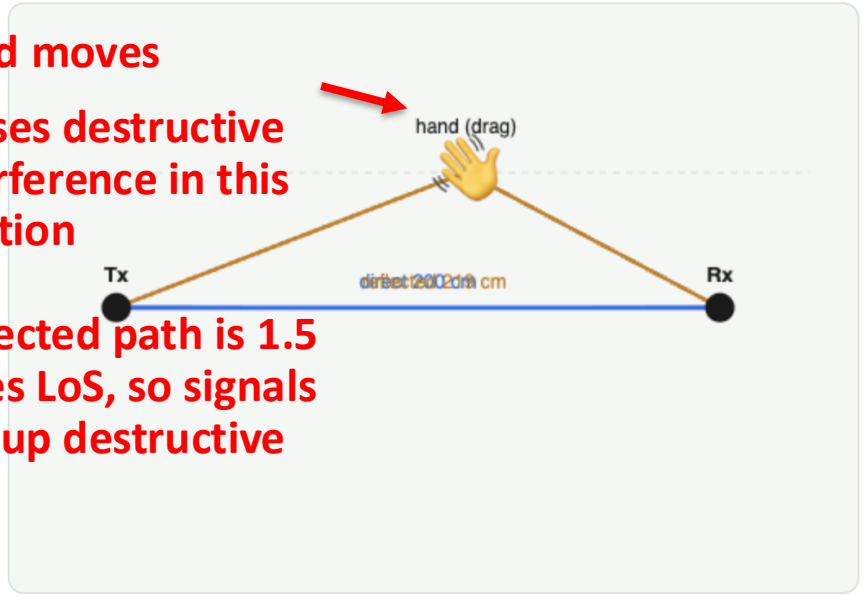
https://tjp.cs.dartmouth.edu/cs60/code/day11/multipath.html

Lab 4 uses constructive/destructive interference to generate an encryption key

Hand moves

Causes destructive interference in this position

Reflected path is 1.5 times LoS, so signals add up destructive



Drag the amber reflector. Moving it changes the bounced path's length, which shifts its phase relative to the direct path.



As you wave your hand near two devices
Each device receives the same pattern of strong or weak signal (constructive or destructive interference)
Each device uses this pattern to independently compute a key it can use for encryption
Dartmouth student's senior thesis
Received U.S. Patent

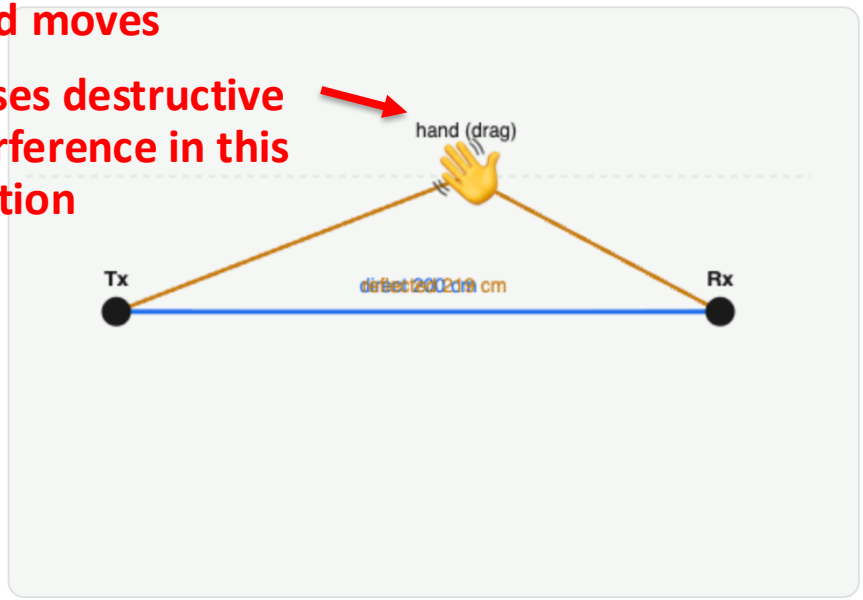
Try it yourself

https://tjp.cs.dartmouth.edu/cs60/code/day11/multipath.html

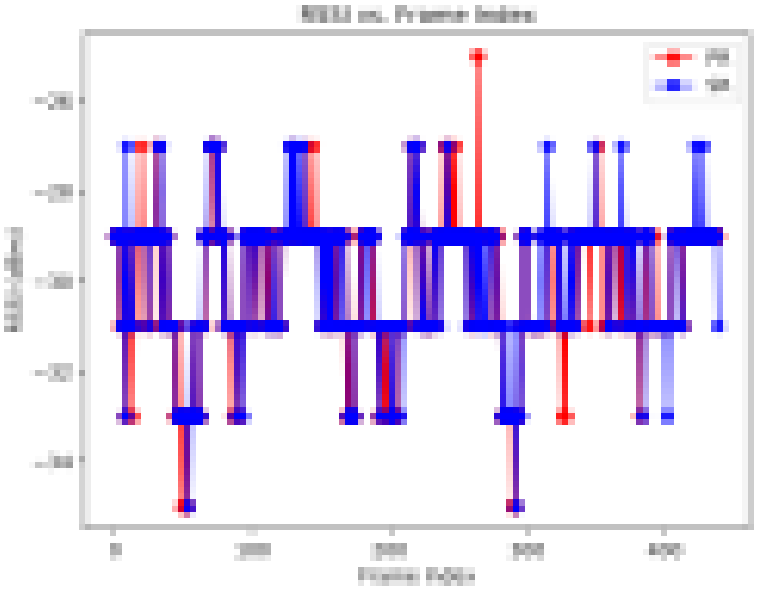
Lab 4 uses constructive/destructive interference to generate an encryption key

Hand moves

Causes destructive interference in this position



Drag the amber reflector. Moving it changes the bounced path's length, which shifts its phase relative to the direct path.



To make a key:
Convert high RSSI into a 1 bit
Convert low RSSI into a 0 bit

As you wave your hand near two devices
Each device receives the same pattern of strong or weak signal (constructive or destructive interference)
Each device uses this pattern to independently compute a key it can use for encryption
Dartmouth student's senior thesis
Received U.S. Patent

Try it yourself

https://tjp.cs.dartmouth.edu/cs60/code/day11/multipath.html

Antennas

MIMO: Multiple input multiple output antenna

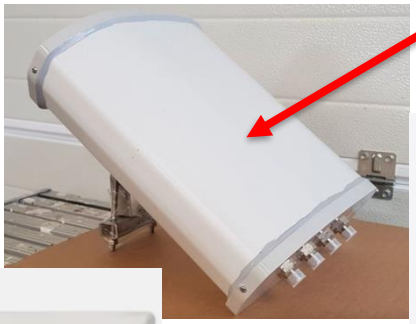
Antennas both transmit and receive radio waves

Single antenna: old school

Multiple antennas: common now in wireless networks



Dipole antenna



Who knows what kind of antenna? Read tech specs to find out



Probably Yagi (maybe Log-Periodic) antenna



Micropatch (others?) antenna

- Gigabit LTE with 4x4 MIMO
- Wi-Fi 6 (802.11ax) with 2x2 MIMO

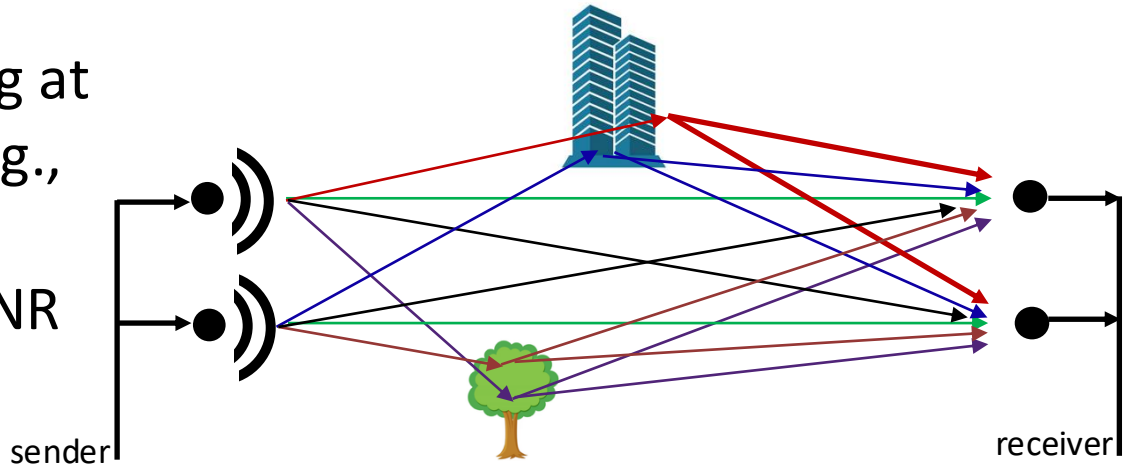
Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

MIMO transmission: single user

Single User MIMO: spatial *diversity*

- Multiple transmit/receive antenna to/at one user at same time
- *Exploit multipath:* use multiple antennas to increase number of paths for transmitted signal between transmitter and receiver

- Multipath: signals arriving at receiver not the same (e.g., some at higher quality)
- Antenna gain: increase SNR by combining multiple signals

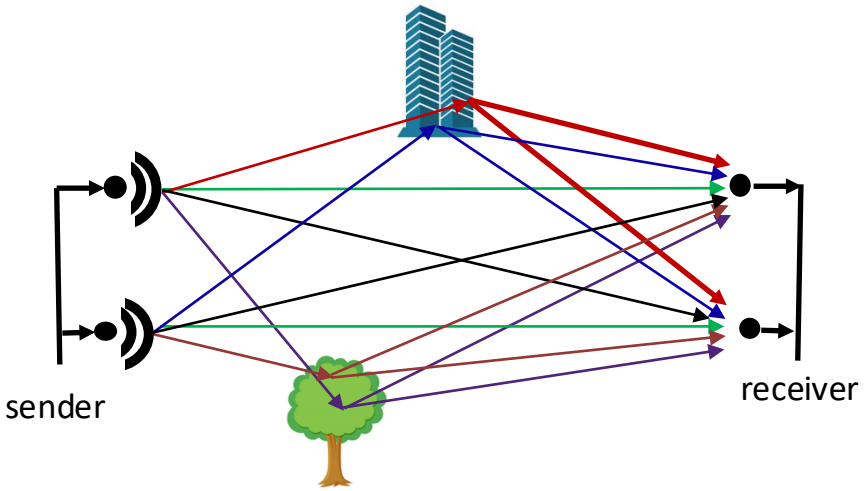


12 signal paths from one sender (with two antennas) to one receiver (with two antennas)

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

MIMO: spatial *diversity*

- Increase reliability, range by sending / receiving *redundant streams of information in parallel* along different spatial paths between transmit and receive antennas



  - *Improved reliability:* unlikely that all paths degraded at same time
  - *Improved range:* multiple antennas gather more signal at receiver

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

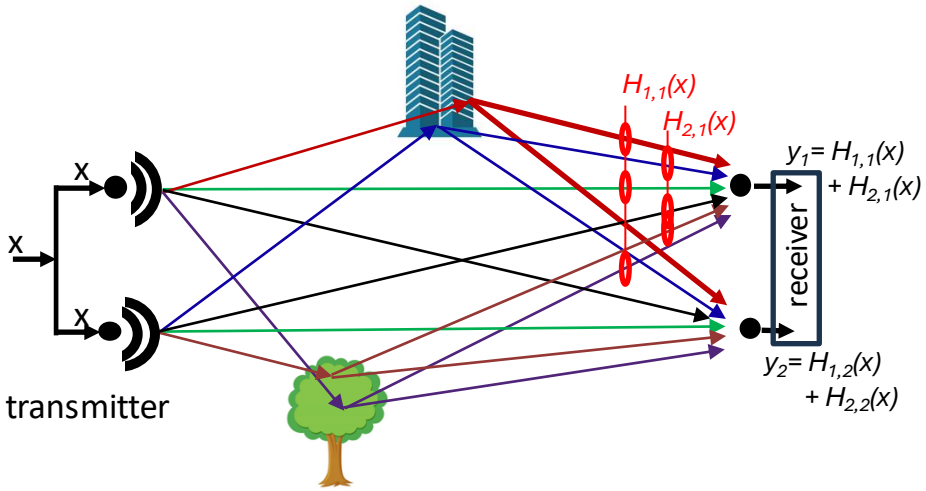
MIMO: spatial *diversity*

x: signal transmitted

y_j: signal received at antenna *j*

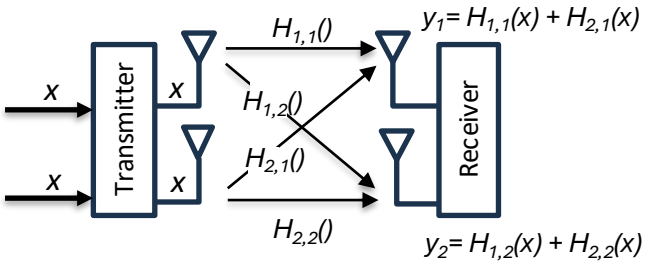
$H_{i,j}(x)$: transformation of signal *x* from transmitter antenna *i* to receiver antenna *j*

- Estimated by receiver (perhaps with preamble)



Signal processing at receiver?

- Don't want to just add y1, y2
- Take stronger or smaller SNR of y1, y2?
- Re-align phases, coherently add

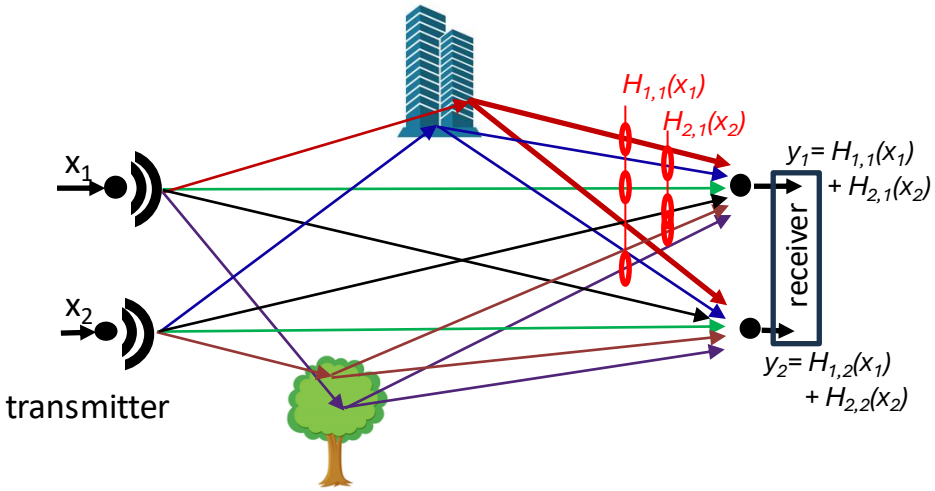


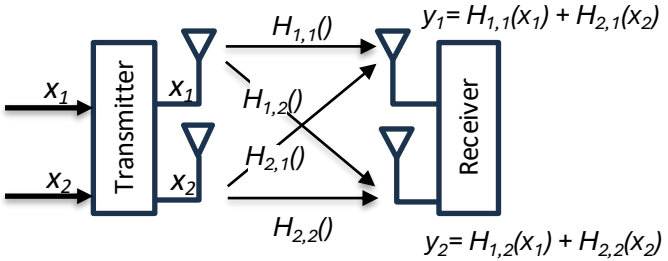
Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

MIMO: spatial *multiplexing*

- Send two *different streams of information,* x_1 and x_2 in parallel along different spatial paths from transmitter to receiver
- Spatial *multiplexing* differs from spatial *diversity*

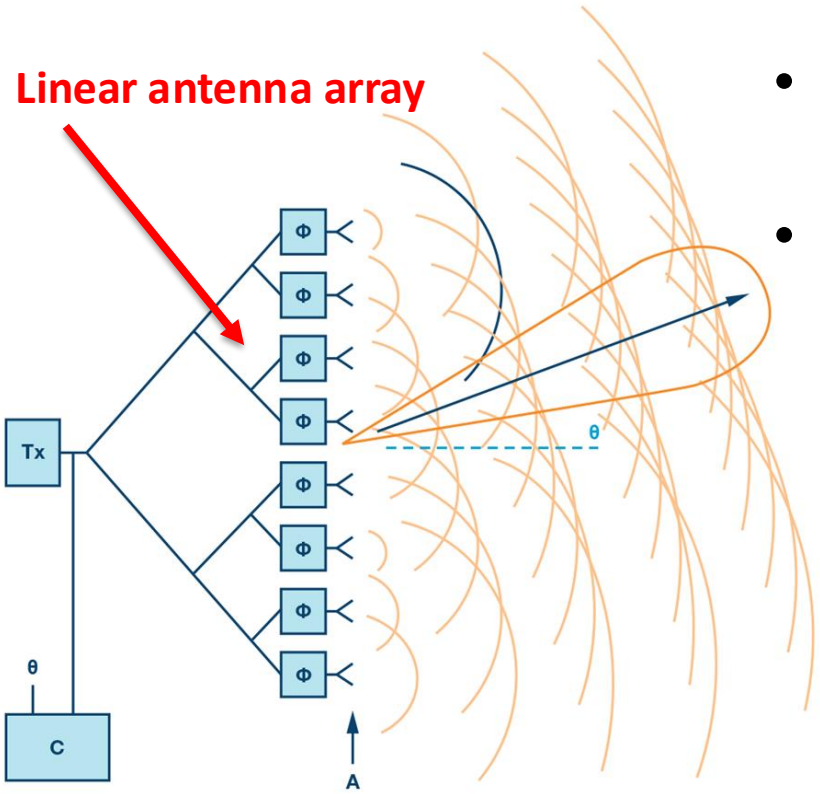
Big idea is more data throughput from multiple streams, not more range or reliability





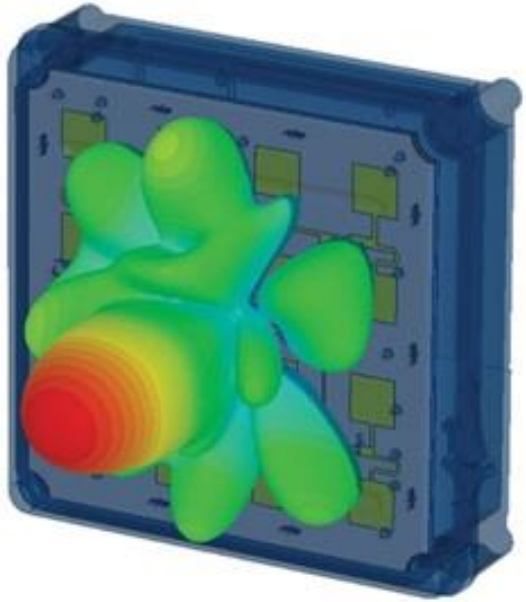
Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

Beamforming with multiple antennas can electronically steer a beam in any direction



Phased array

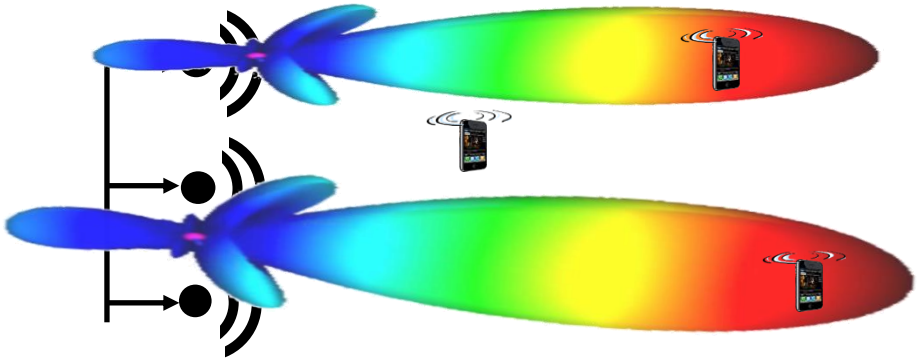
- Physically arrange an array of transmitting antennas
- Change phase for each transmitting antenna
- Can electronically steer the main lobe of the beam in any direction

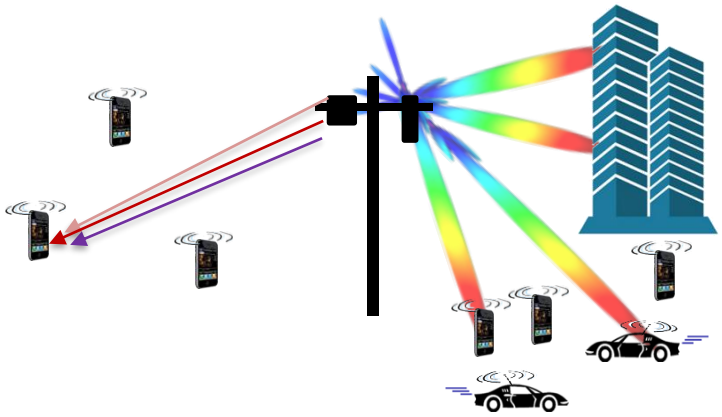


Adapted from https://www.analog.com/en/resources/analog-dialogue/articles/phased-array-beamforming-ics-simplify-antenna-design.html

Beamforming can create Multi-user MIMO

- Multiple transmit antenna send to *different* users at same time
  - "spatial multiplexing"
- *Exploit directional antenna:* send to geographically separated users at same time via beamforming





Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

Fighter jets do something similar to track multiple targets simultaneously

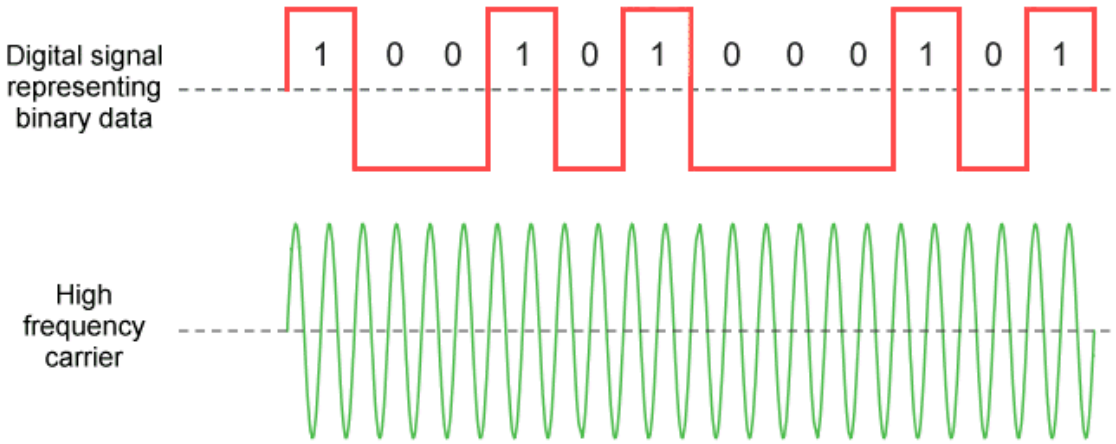


Image: Cophilot, plus beamforming overlay

Agenda

1. Wired physical layer
2. Wireless networks
3. Modulation schemes
4. Wi-Fi

Amplitude and frequency can be used to encode data

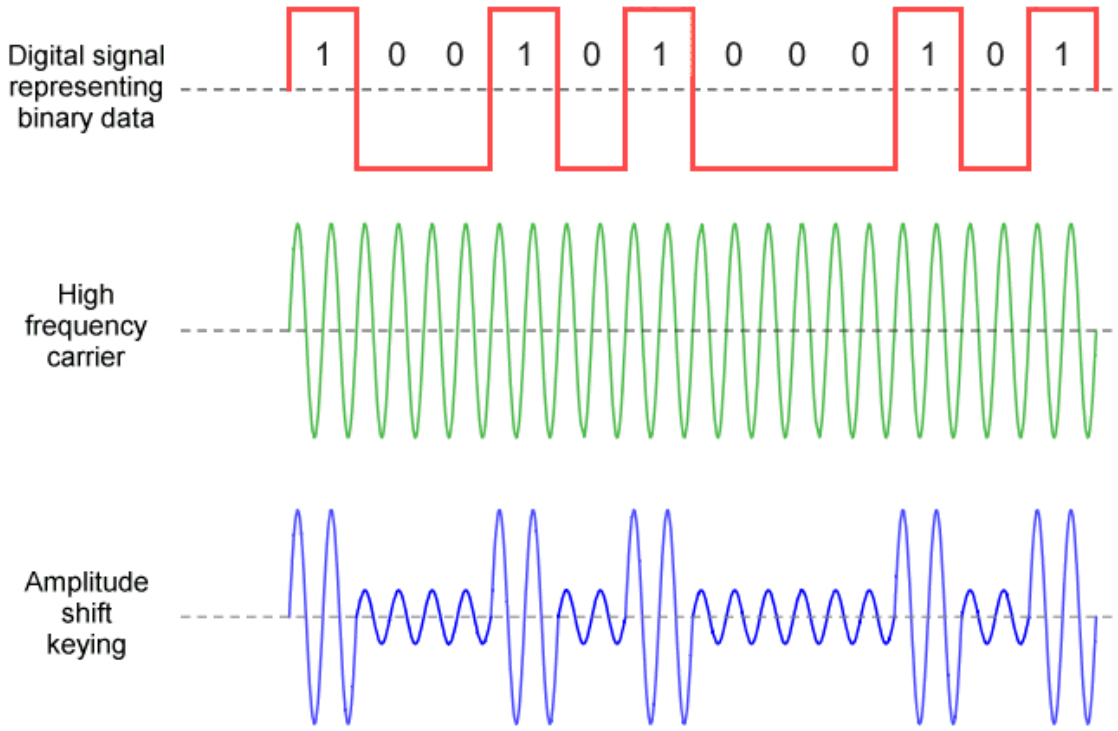


Digital signal to send

We will *modulate* a carrier wave to send data
No data can be received if carrier is not modulated

Adapted from https://www.technologyuk.net/telecommunications/telecom-principles/digital-modulation-part-one.shtml

Amplitude and frequency can be used to encode data



Digital signal to send

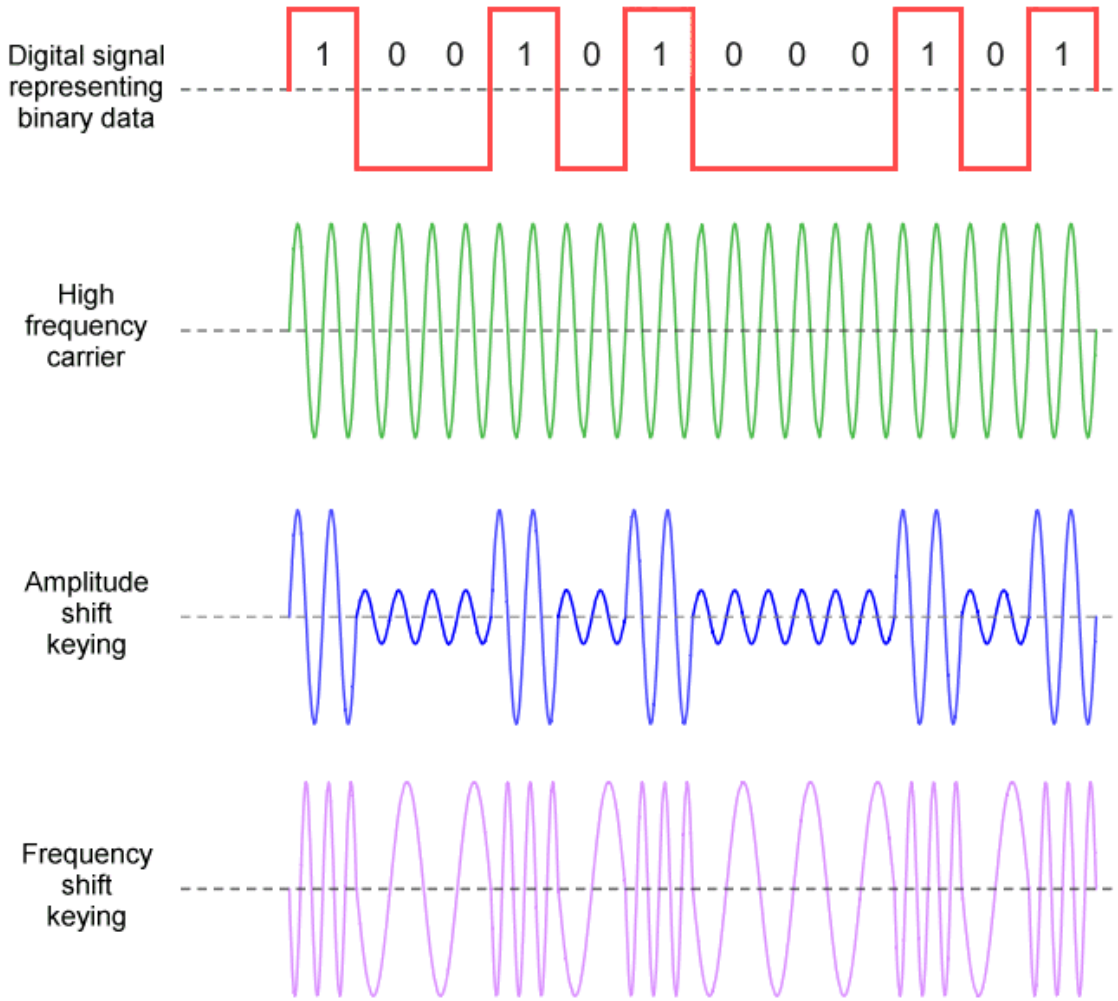
We will *modulate* a carrier wave to send data
No data can be received if carrier is not modulated

Amplitude Shift Keying (ASK)

- **High amplitude = 1 bit**
- **Low amplitude = 0 bit**
- **Simplest is no transmission for low amplitude (On/Off Keying)**

Adapted from https://www.technologyuk.net/telecommunications/telecom-principles/digital-modulation-part-one.shtml

Amplitude and frequency can be used to encode data



Digital signal to send

We will *modulate* a carrier wave to send data
No data can be received if carrier is not modulated

Amplitude Shift Keying (ASK)

- **High amplitude = 1 bit**
- **Low amplitude = 0 bit**
- **Simplest is no transmission for low amplitude (On/Off Keying)**

Frequency Shift Keying (FSK)

- **High frequency = 1 bit**
- **Low frequency = 0 bit**

Adapted from https://www.technologyuk.net/telecommunications/telecom-principles/digital-modulation-part-one.shtml

We can also modulate the phase of the signal to transmit data

Amplitude shift keying (ASK): signal's *amplitude* encodes bits

0: —

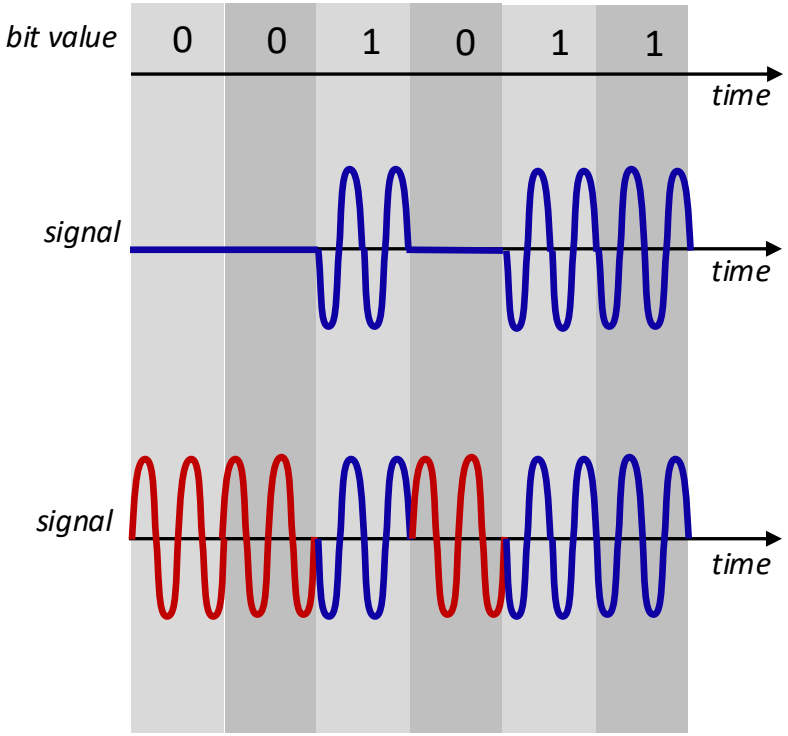
1: 

Binary Phase shift keying (BPSK): signal's *phase* encode bits

0: 

1: 

BPSK: 0 and 1 signals *out of phase* by 180°, but at same carrier frequency

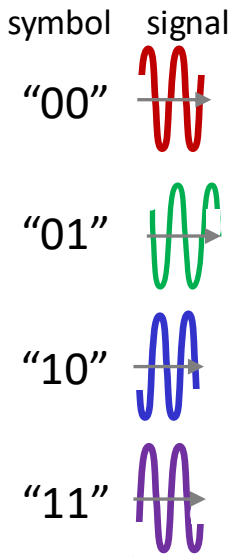


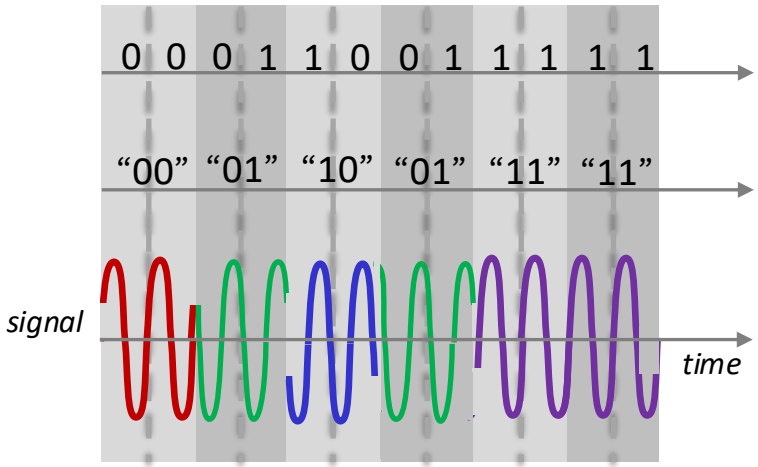
Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

QPSK uses four phases to carry two bits per symbol

Why stop at just two phases?

- Two bits grouped to become one "symbol" (2 bits -> 4 symbols)
- *QPSK: Quadrature Phase Shift Keying:* 4 symbols encoded using 4 phases



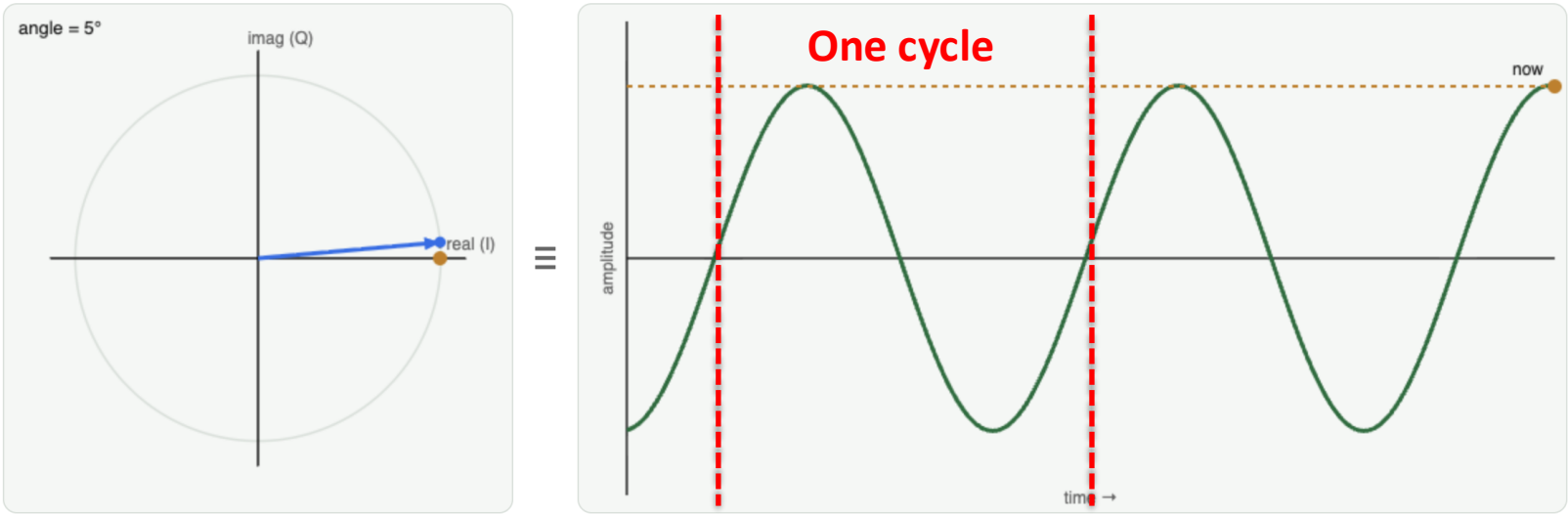


QPSK frequency same as BPSK, but twice the data rate!

Fun interactive QPSK tool: https://www.geogebra.org/m/enkymjtg

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

We can plot the phase and amplitude of a signal in the complex plane



Phase θ — 0°

▶ Resume rotation

Reset θ = 0

Phasor (complex plane): an arrow of fixed length at angle (2πft + θ). It spins counter-clockwise at the signal's frequency.

Wave (time domain): the *horizontal projection* of the spinning arrow, traced out over time — a cosine.

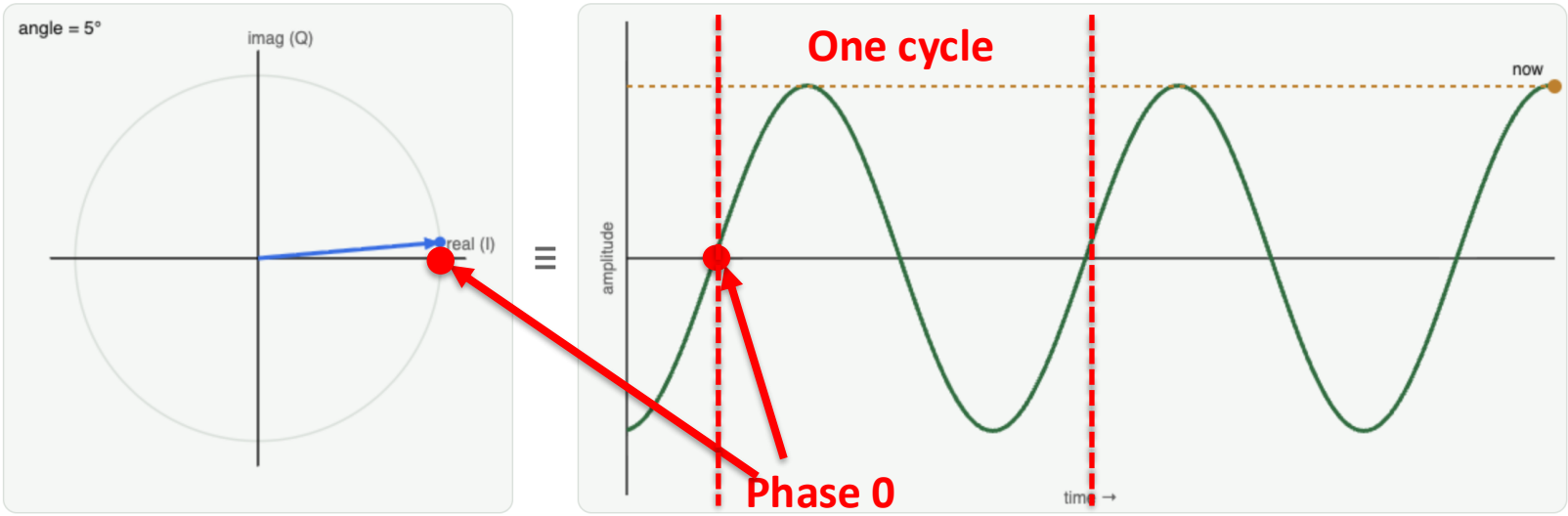
Drag the phase slider: the arrow's starting angle rotates, and the whole wave slides sideways by the same amount. A 90° rotation = a quarter-cycle shift. **Same number, two pictures.** This is exactly what a constellation point encodes.

https://tjp.cs.dartmouth.edu/cs60/code/day11/phase.html

We can plot the phase and amplitude of a signal in the complex plane

In the complex plane:

- **Phase is a rotation around the origin**
- **Amplitude is distance from the origin**



Phase θ — 0°

▶ Resume rotation

Reset θ = 0

Phasor (complex plane): an arrow of fixed length at angle (2πft + θ). It spins counter-clockwise at the signal's frequency.

Wave (time domain): the *horizontal projection* of the spinning arrow, traced out over time — a cosine.

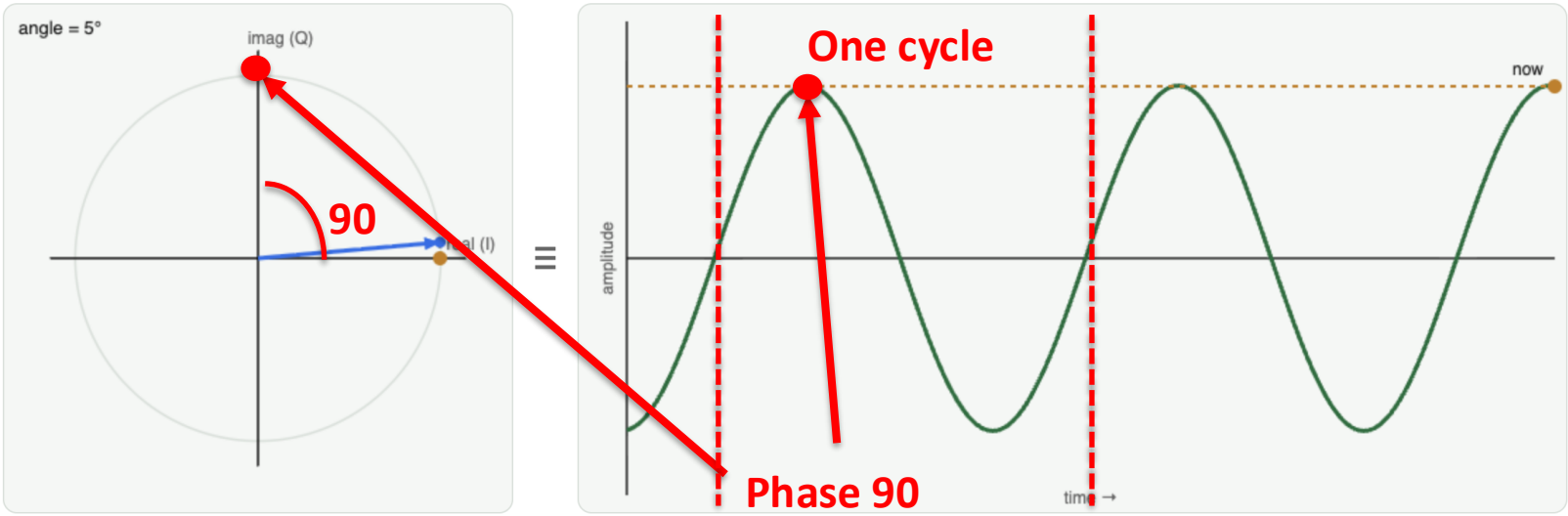
Drag the phase slider: the arrow's starting angle rotates, and the whole wave slides sideways by the same amount. A 90° rotation = a quarter-cycle shift. **Same number, two pictures.** This is exactly what a constellation point encodes.

https://tjp.cs.dartmouth.edu/cs60/code/day11/phase.html

We can plot the phase and amplitude of a signal in the complex plane

In the complex plane:

- **Phase is a rotation around the origin**
- **Amplitude is distance from the origin**



Phasor (complex plane): an arrow of fixed length at angle (2πft + θ). It spins counter-clockwise at the signal's frequency.

Wave (time domain): the *horizontal projection* of the spinning arrow, traced out over time — a cosine.

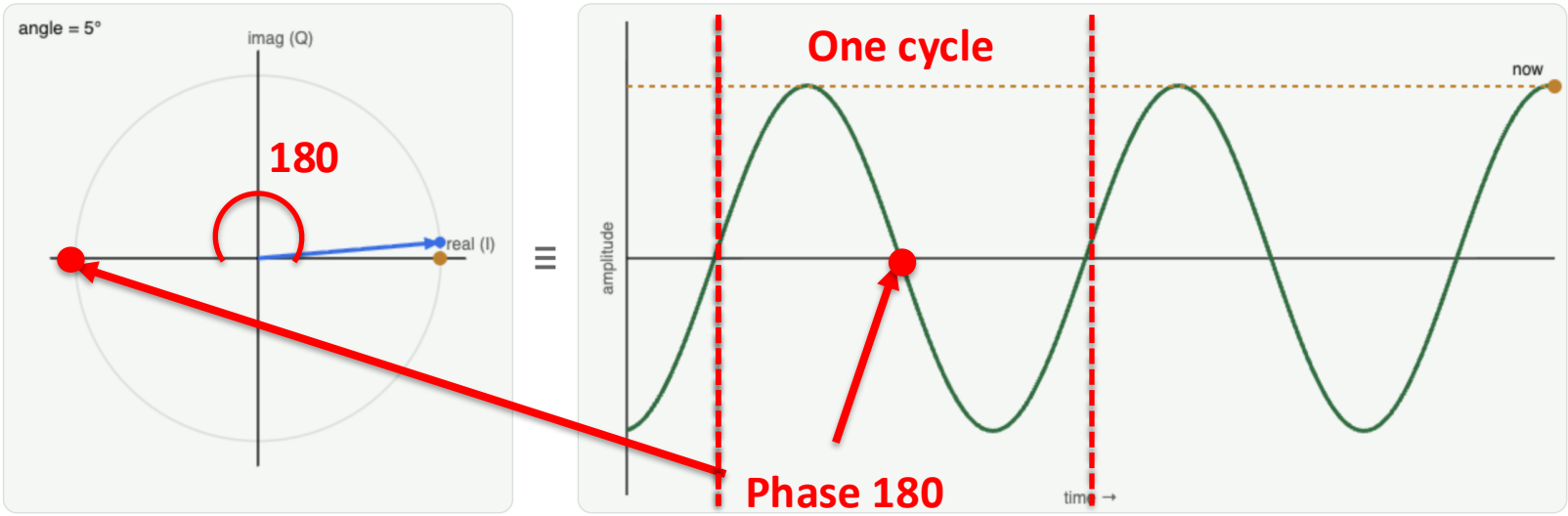
Drag the phase slider: the arrow's starting angle rotates, and the whole wave slides sideways by the same amount. A 90° rotation = a quarter-cycle shift. **Same number, two pictures.** This is exactly what a constellation point encodes.

https://tjp.cs.dartmouth.edu/cs60/code/day11/phase.html

We can plot the phase and amplitude of a signal in the complex plane

In the complex plane:

- **Phase is a rotation around the origin**
- **Amplitude is distance from the origin**



Phasor (complex plane): an arrow of fixed length at angle (2πft + θ). It spins counter-clockwise at the signal's frequency.

Wave (time domain): the *horizontal projection* of the spinning arrow, traced out over time — a cosine.

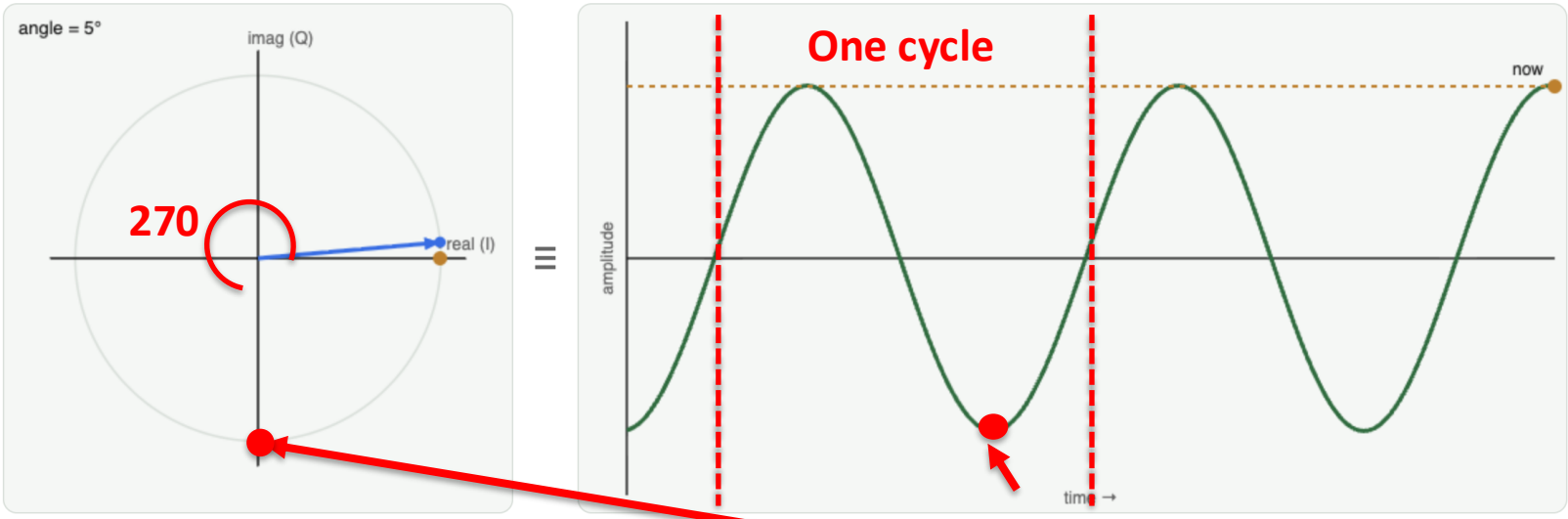
Drag the phase slider: the arrow's starting angle rotates, and the whole wave slides sideways by the same amount. A 90° rotation = a quarter-cycle shift. **Same number, two pictures.** This is exactly what a constellation point encodes.

https://tjp.cs.dartmouth.edu/cs60/code/day11/phase.html

We can plot the phase and amplitude of a signal in the complex plane

In the complex plane:

- **Phase is a rotation around the origin**
- **Amplitude is distance from the origin**



Phasor (complex plane): an arrow of fixed length at angle (2πft + θ). It spins counter-clockwise at the signal's frequency.

Wave (time domain): the *horizontal projection* of the spinning arrow, traced out over time — a cosine.

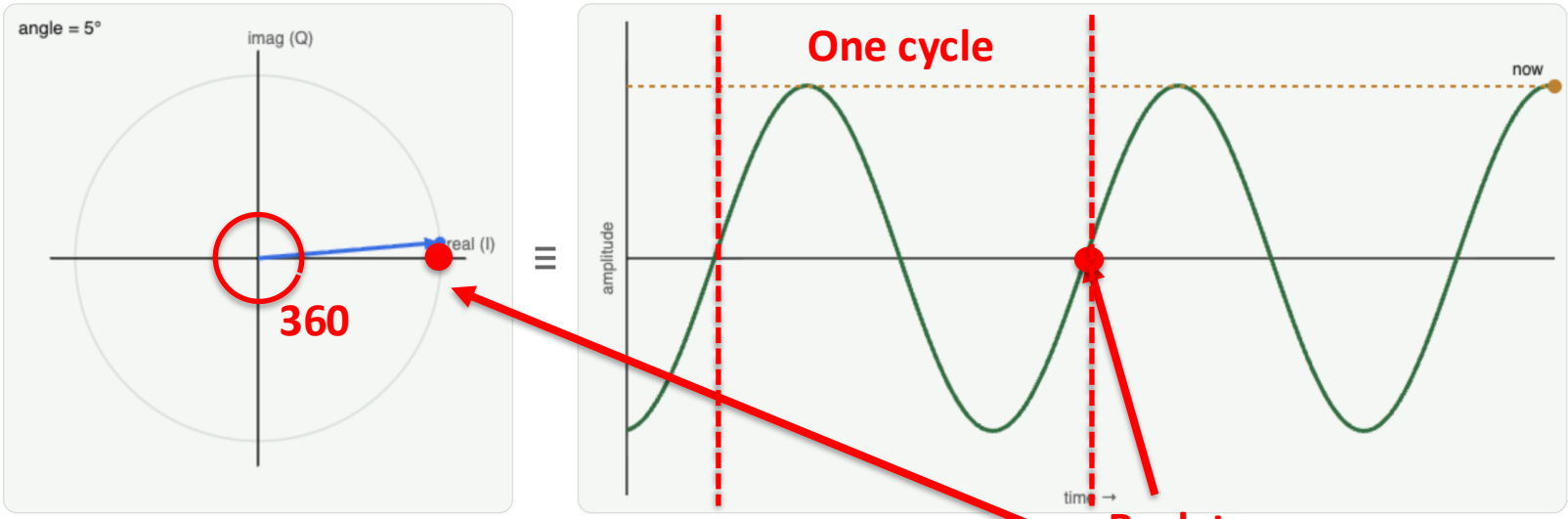
Drag the phase slider: the arrow's starting angle rotates, and the whole wave slides sideways by the same amount. A 90° rotation = a quarter-cycle shift. **Same number, two pictures.** This is exactly what a constellation point encodes.

https://tjp.cs.dartmouth.edu/cs60/code/day11/phase.html

We can plot the phase and amplitude of a signal in the complex plane

In the complex plane:

- **Phase is a rotation around the origin**
- **Amplitude is distance from the origin**



Phasor (complex plane): an arrow of fixed length at angle (2πft + θ). It spins counter-clockwise at the signal's frequency.

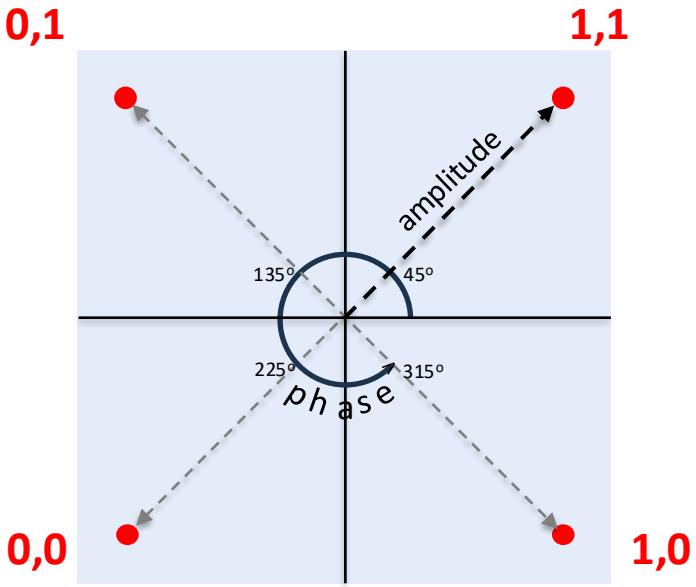
Wave (time domain): the *horizontal projection* of the spinning arrow, traced out over time — a cosine.

Drag the phase slider: the arrow's starting angle rotates, and the whole wave slides sideways by the same amount. A 90° rotation = a quarter-cycle shift. **Same number, two pictures.** This is exactly what a constellation point encodes.

https://tjp.cs.dartmouth.edu/cs60/code/day11/phase.html

Constellation diagrams show phase and amplitude in the complex plane

Graphical characterization of modulation: amplitude, phase of symbols in the complex plane



QPSK constellation diagram

Each constellation point can represent 2 bits

- Point in constellation diagram depicts symbol's phase (degrees counterclockwise from east) and amplitude (distance from origin)
- QPSK constellation diagram: four symbols represented by four signal waveforms:
  - Four different *phases*
  - Identical *amplitude*

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

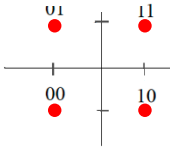
Quadrature Amplitude Modulation uses m phase/amplitude combinations

- Generalizing QPSK
- *m*-QAM: using *m* different amplitude/phase values to encode $\log_2(m)$ bits

Add more phase/amplitude combinations where each represents multiple bits

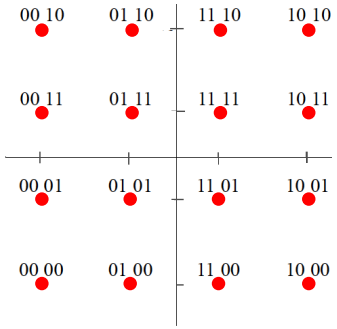
4-QAM

2 bits/symbol
b_0b_1



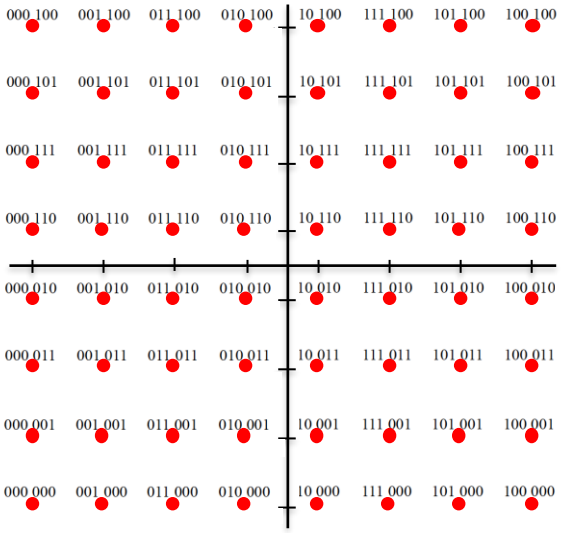
16-QAM

4 bits/symbol
$b_0b_1b_2b_3$



64-QAM

6 bits/symbol
$b_0b_1b_2b_3b_4b_5$

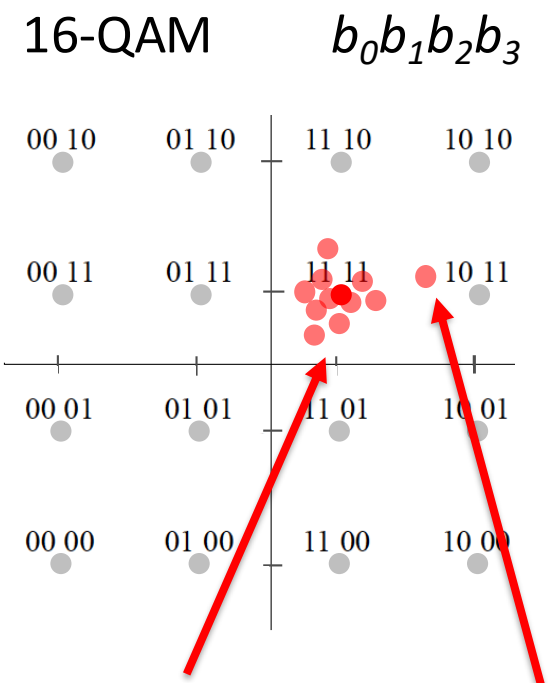


Bit encodings for 4-QAM, 16-QAM, 64-QAM (for Wi-Fi)

More complex modulation schemes carry more data bits per symbol

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

Constellation diagrams: how bit errors occur



Transmitter transmits 12 waveforms for 1111 symbols, sequentially

phase/amplitude of

- transmitted signal
- phase/amplitude of received signals

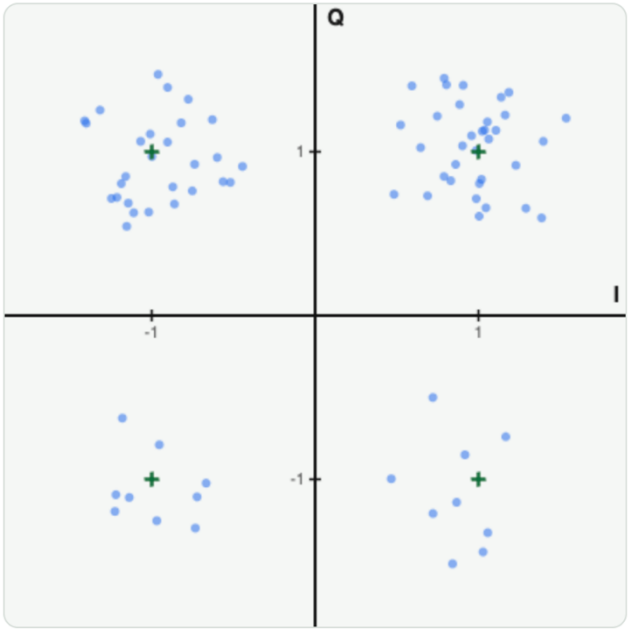
- Receiver measures amplitude, phase of received signal
- Receiver classifies symbol as bit pattern with amplitude, phase closest to received signal amplitude, phase

These received signals are correctly classified as 1111 (received amplitude and phases closest to 1111)

This received signal, is misclassified as 1011 since its amplitude and phase is closer to 1011 than 1111

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

Simple modulation schemes can tolerate noise



ideal symbol received point (color = correctly decoded, red = bit error)

QPSK (4-QAM) tolerates a lot of noise
Why?
Lot of space between constellation points

Modulation

QPSK · 2 bits | 16-QAM · 4 bits | 64-QAM · 6 bits

Signal-to-noise ratio — 12 dB

Decoded message

HELLO CS60 PHY LAYER

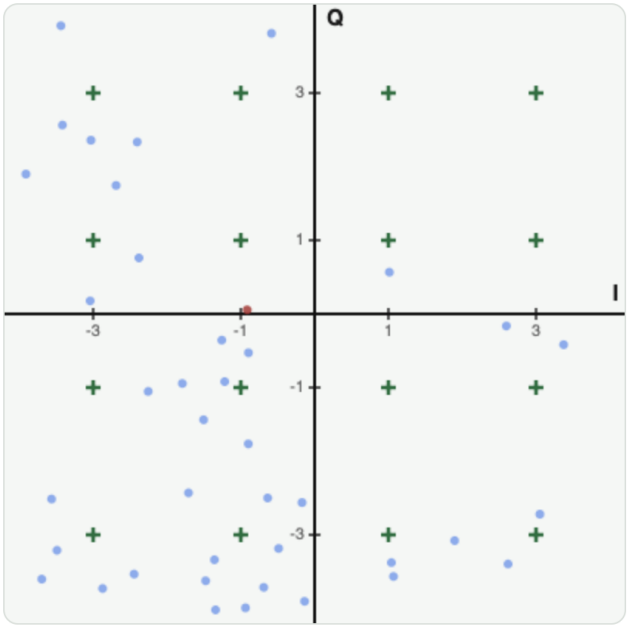
symbols	bits / symbol	bit error rate
80	2	0.0%

No decoding errors, even with low SNR

Clean channel — every point lands near its own symbol, message perfect.

https://tjp.cs.dartmouth.edu/cs60/code/day11/constellation.html

Moderate modulation schemes can tolerate less noise



+ ideal symbol · received point (color = correctly decoded, red = bit error)

16-QAM tolerates less noise but sends 4 data bits per symbol

Modulation

QPSK · 2 bits | **16-QAM · 4 bits** | 64-QAM · 6 bits

Signal-to-noise ratio — **12 dB**

Decoded message

```
HELLO CS60 PHY LAyER
```

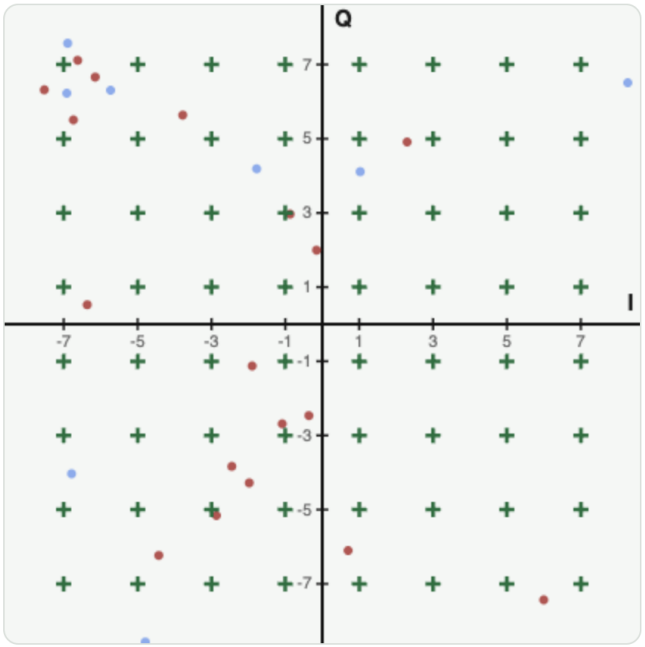
Recovered message has some decoding errors

symbols	bits / symbol	bit error rate
40	4	0.6%

A few points stray, but most symbols still classify correctly. Notice 16-QAM packs points closer, so the SAME noise flips more bits than QPSK would.

https://tjp.cs.dartmouth.edu/cs60/code/day11/constellation.html

Complex modulation schemes can tolerate little noise



+ ideal symbol · received point (color = correctly decoded, red = bit error)

64-QAM struggles with high noise but sends 6 data bits per symbol

Modulation

QPSK · 2 bits | 16-QAM · 4 bits | **64-QAM · 6 bits**

Signal-to-noise ratio — **12 dB**

Decoded message

`LEÄDO`ÃWV0`YLI(HQ·mR`

symbols	bits / symbol	bit error rate
27	6	13.6%

Recovered message has many decoding errors

Noise swamps the spacing between symbols. The receiver is guessing. Notice 64-QAM packs points closer, so the SAME noise flips more bits than QPSK would.

Generally want SNR above 20 dB to use complex modulation schemes

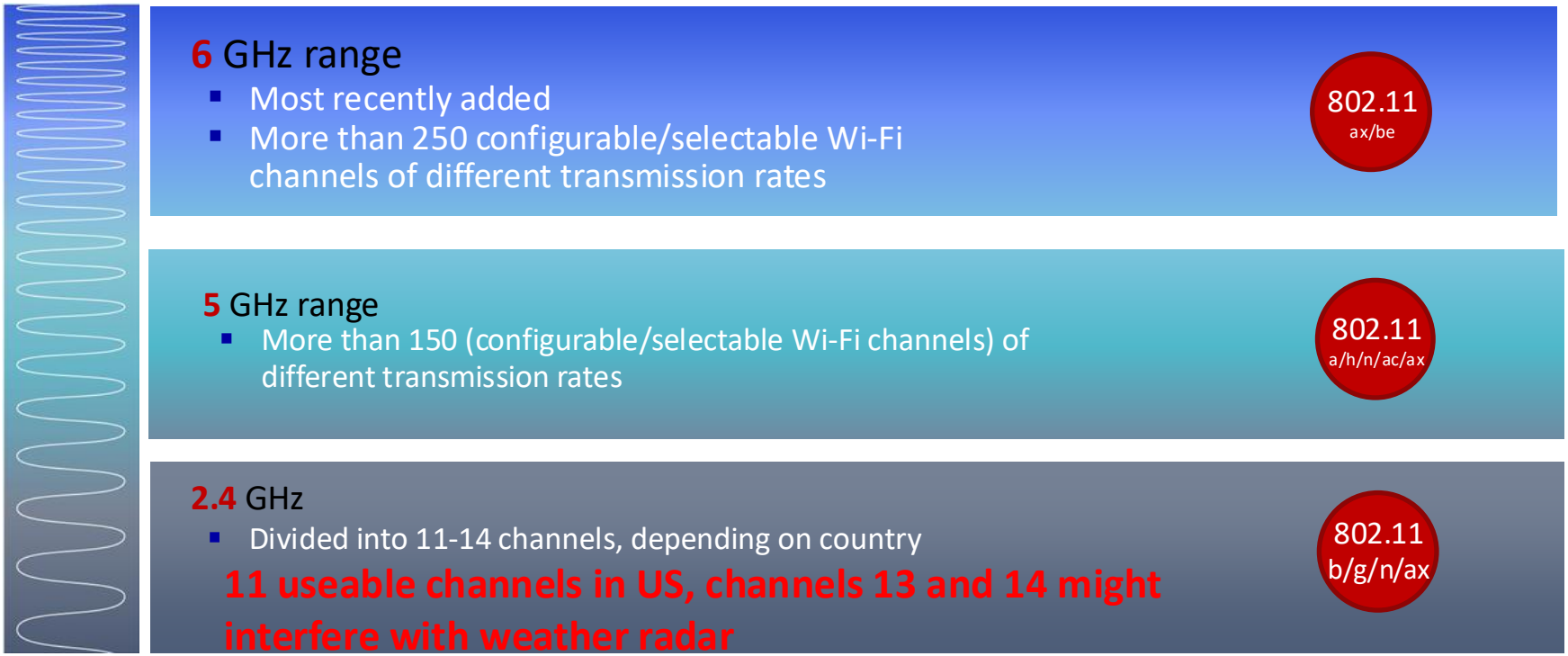
Idea: Change modulation scheme, power on the fly, getting highest data rate possible (at acceptable bit error rate (BER), acceptable energy expenditure), as SNR changes

https://tjp.cs.dartmouth.edu/cs60/code/day11/constellation.html

Agenda

1. Wired physical layer
2. Wireless networks
3. Modulation schemes
4. Wi-Fi

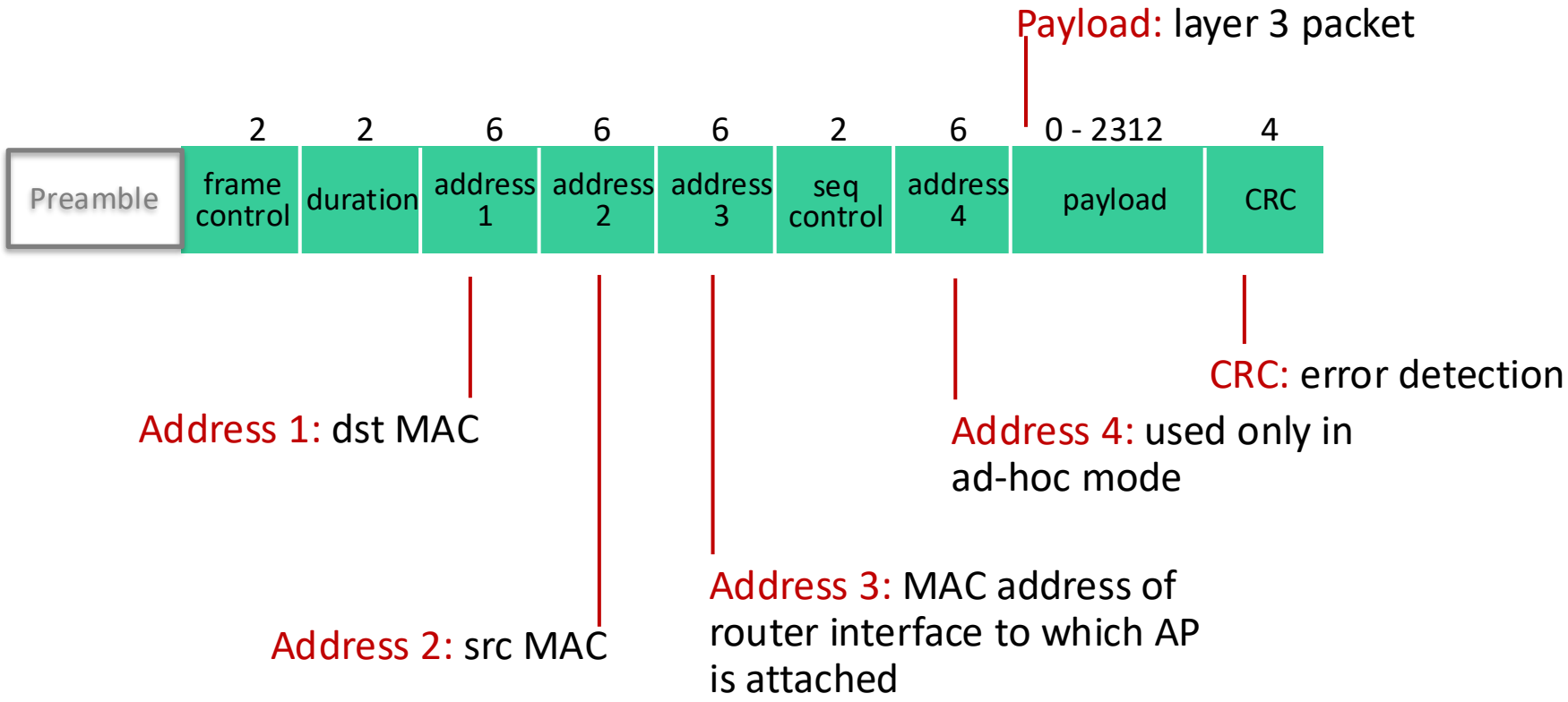
Wi-Fi primarily uses two frequency bands (plus a new third band)



- Other 802.11 Wi-Fi spectrum bands, but not in widespread use

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

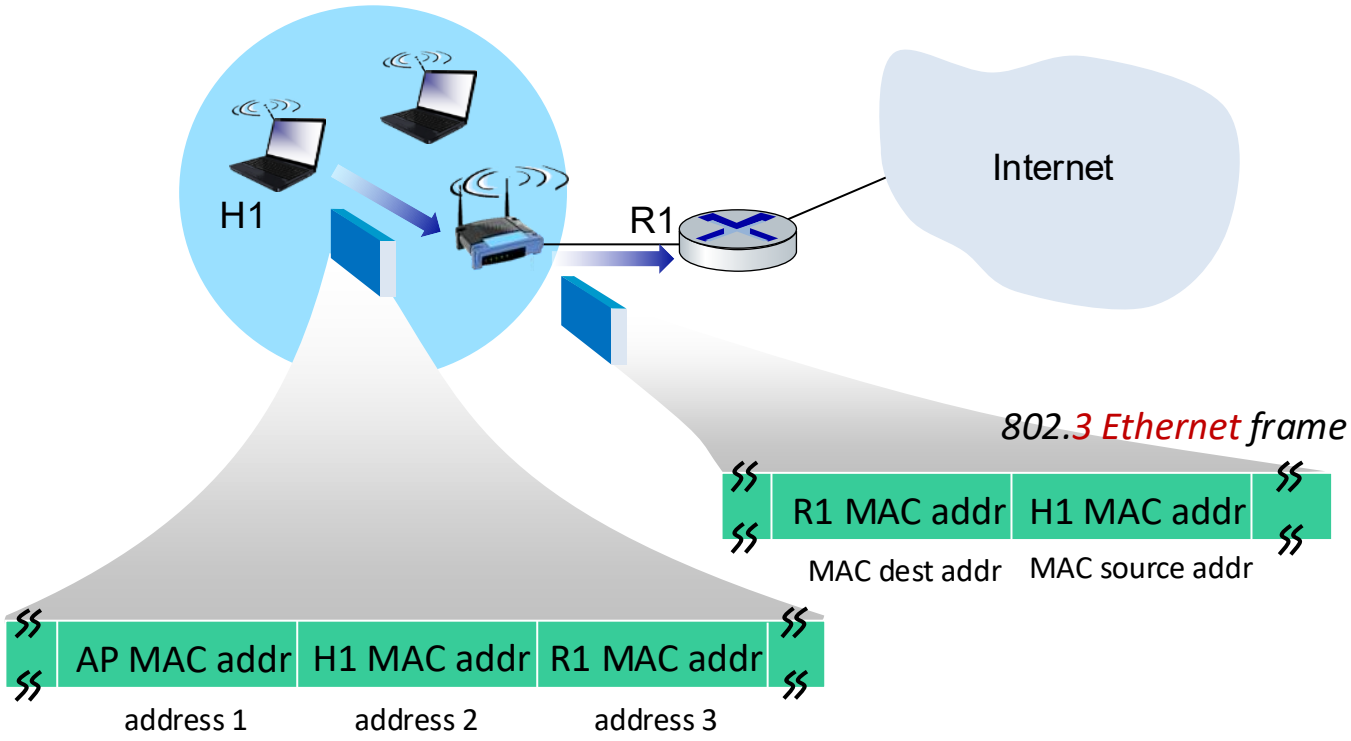
802.11 Layer 2 frame differs from Ethernet



An observer can see src and dst MAC addresses from transmitter, even if not associated with an AP

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

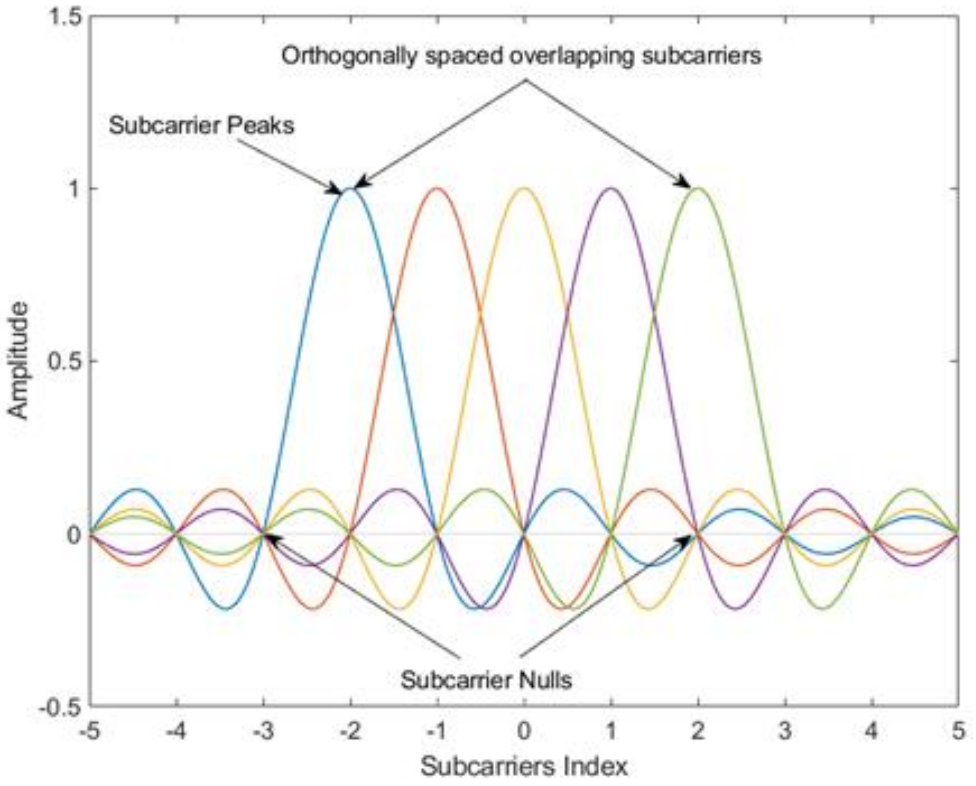
A Wi-Fi Access Point typically converts from Wi-Fi Layer 2 to wired Ethernet



AP receives wireless Wi-Fi bits
Strips Wi-Fi header bits
Adds Ethernet header
Sends to wired network

Adapted from Kurose and Ross: Computer Networking: A Top-Down Approach

OFDM sends data on multiple subcarriers simultaneously

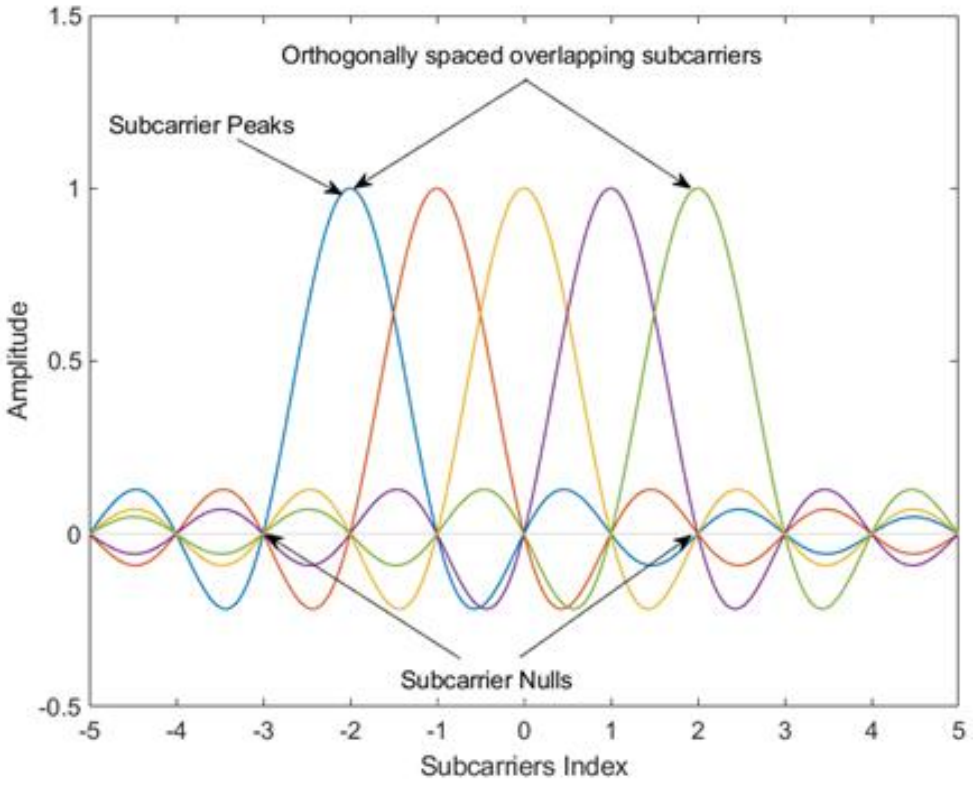


Orthogonal Frequency Division Multiplexing (OFDM)

- Each subcarrier is a different frequency
- Spacing between subcarriers is carefully chosen so the peaks are each subcarrier are at the nulls of neighboring subcarriers (e.g., freqs are orthogonal)
- Each subcarriers carries a data symbol
- Data symbol modulated with BPSK, QPSK, 16 QAM, …
- So, 1, 2, 4, 6, … bits/symbol

Wi-Fi uses 64 subcarriers per 20 MHz channel
Each subcarrier can carry a symbol of up to 10 bits/symbol (QAM 1024)
802.11ax can bond up to 8 channels

OFDM sends data on multiple subcarriers simultaneously



802.11ax max theoretical speed

- 1024-QAM encodes 10 bits per symbol (since $\log_2(1024) = 10$)
- Uses OFDM with:
  - Bits/symbol (Nb) = 10
  - Data subcarriers (Ns) = 1960
  - Coding rate (R) =5/6
  - Streams (S) = 8
  - Symbol duration (Symb): 13.6 µs (including guard interval)

Max theoretical speed

= (Nb * Ns * R * S)/Symb

= (10*1960*5/6*8)/13.6

= 9.6 Gbps

$$\text{Max Theoretical Speed} = 720\ Mbps \times 8 = \boxed{5.76\ Gbps}$$

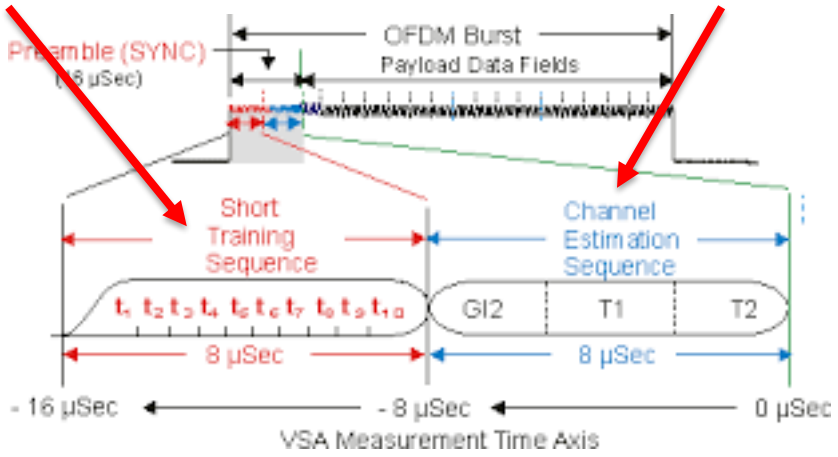
Actual throughput will be much lower!

Wi-Fi uses 64 subcarriers per 20 MHz channel
Each channel can carry a symbol of up to 10 bits/symbol (QAM 1024)
802.11ax can bond up to 8 channels

Use a preamble to deal with attenuation and multipath to make sure data received

STF – get ready here comes a frame

LTF – measure CSI



The phase and amplitude a receiver gets will be different from what the sender transmitted due to attenuation and multipath

Solution:

Add a preamble and transmit at pre-agreed upon phase and amplitude

- Receiver knows what the phase and amplitude the sender used
- Receiver measures phase and amplitude of received signal
- Adds a correction factor to adjust what it received to what it knows the sender transmitted
- Adjustment is called *Channel State Information* (CSI)
- CSI is the change the channel (environment) made to signal

Channel State Information (CSI) from data transmissions can be a side channel

Signal sent to receiver will be modified by the environment

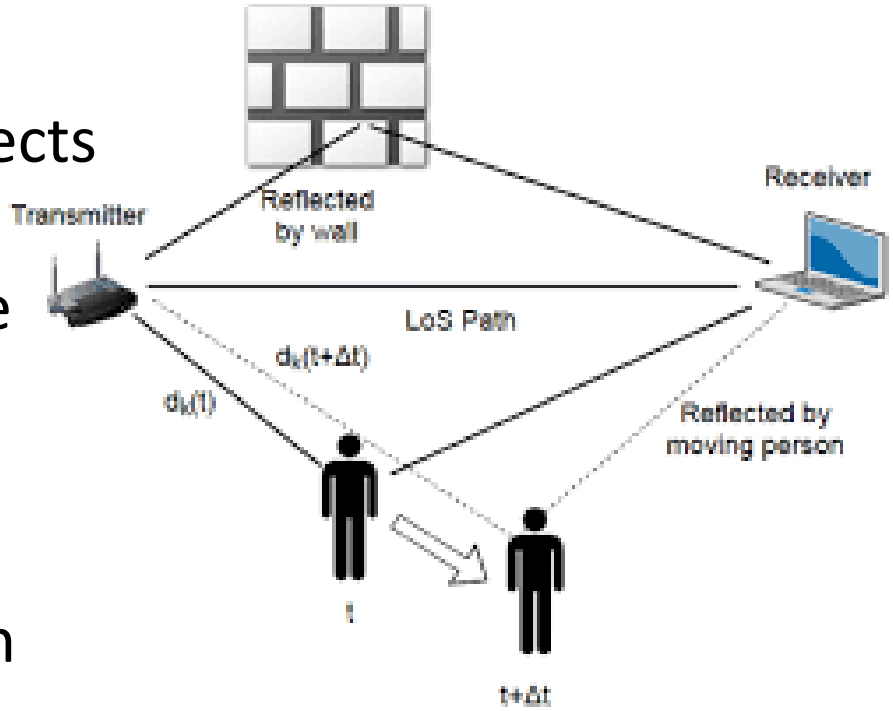
Receiver can estimate channel effects with preamble

Changes caused by channel can be used for[1]:

- Device-free fall detection
- Key presses on keyboard
- Gesture and smoking detection
- Identification

Backscattered background data transmissions can power devices without batteries[2]

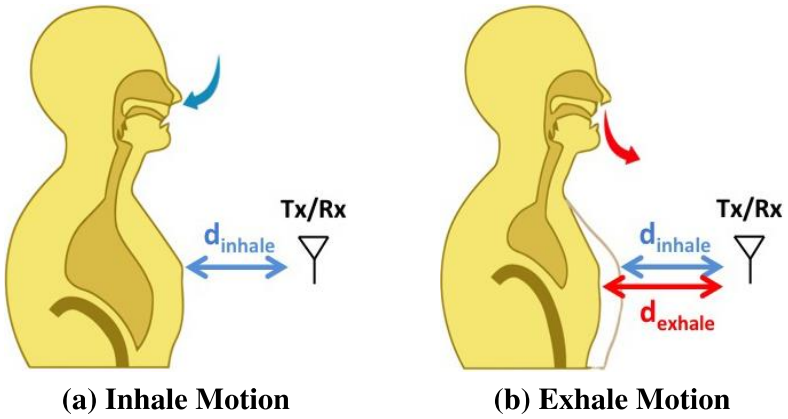
My prediction: many IoT devices go battery-less in the future



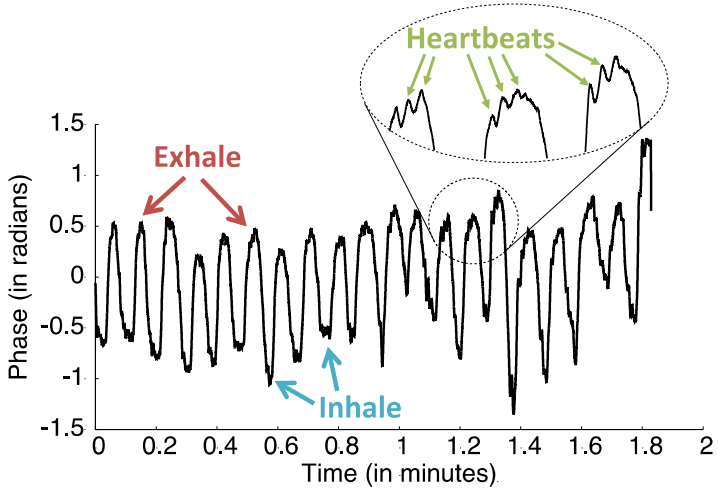
Data transmissions are all around us (all the time)
Intended for info exchange but can be a side channel to infer other things

[1] Ma, Yongsen, Gang Zhou, and Shuangquan Wang. "WiFi sensing with channel state information: A survey." *ACM Computing Surveys (CSUR)* 52.3 (2019): 1-36.
[2] Liu, Vincent, et al. "Ambient backscatter: Wireless communication out of thin air." *ACM SIGCOMM Computer Communication Review* 43.4 (2013): 39-50.

CSI can reveal pulse and respiration rate also!



(a) Inhale Motion (b) Exhale Motion



- Vital-Radio transmits RF signal
- System measures reflection phase changes
- Detects small differences in path length when someone breathes
- Distance change induces phase change
- Also measures heart rate!
- This approach is purposefully trying to collect information with single-purpose transmission
- Newer research collects data from data background Wi-Fi transmissions

Other uses in business setting?

Adib, Fadel, et al. "Smart homes that monitor breathing and heart rate." *Proceedings of the ACM conference on Human Factors in Computing Systems*. 2015.