CS4222 Cheatsheet AY24/25 —— @JasonYapzx

- **Wavelength:** of sinusoidal waveform travelling at speed v, freq f is $\lambda = \frac{v}{f}$
- EM waves travelling in free space, speed of light ($c \approx 3 \times 10^8$ m/s)

Relationship between antenna size and frequency

Antenna size is **inversely proportional** to frequency of radio wave

- Higher frequency, smaller antenna size, Lower frequency, larger size
- Dipole: length of conductor is $\frac{1}{2}$ of wavelength of radio wave
- Half-Dipole: length of conductor is $\frac{1}{4}$ of wavelength of radio wave

Performance of an antenna

- **Gain of antenna:** Dimensionless ratio (unitless in linear form), commonly expressed in decibels (dB) or dBi. It measures the ability of an antenna to focus energy in a particular direction compared to a reference.
  - **dBi**: Gain referenced to a theoretical isotropic antenna (uniform radiation in all directions)
  - **dBd**: Gain referenced to a half-wave dipole antenna ($dBd = dBi - 2.15$)
- **Units:**
  - Linear gain (G) is unitless
  - Logarithmic gain (G_{dB} or G_{dBi}) is in decibels (dB)
  - Convert: $G_{\text{dB}} = 10\log_{10}(G_{\text{linear}})$ and $G_{\text{linear}} = 10^{G_{\text{dB}}/10}$
- **When to convert:**
  - Use **linear gain** in physical formulas (e.g., Friis, $G = \frac{4\pi A_e}{\lambda^2}$)
  - Use **dBi/dB** when doing link budget calculations (additive terms with power in dBm, FSPL in dB, etc.)
- $\uparrow$ gain $\Rightarrow$ more directional transmission/reception $\Rightarrow$ narrower beamwidth

$$\boxed{G = \frac{4\pi A_e}{\lambda^2} = \frac{4\pi f^2 A_e}{c^2}}$$

- G = antenna gain (unitless)
- A_e = effective aperture area (m^2)
- f = carrier frequency (Hz)
- c = speed of light 3×10^8 m/s
- λ = carrier wavelength (m)

- **Effective area:** Related to the physical size and shape of the antenna—larger A_e typically yields higher gain.
- Power output evaluated in a direction, relative to isotropic antenna output.
- Relationship between gain and number of elements in an array: $G_{\text{array}} = G_{\text{single element}}(\text{dBi}) + 10\log_{10}(N)$, where N is the number of antenna elements; $10\log_{10}(N)$ is the array factor.

Choosing Beamwidth: Tradeoffs

- **Narrow beamwidth**: Offers higher directivity and longer range due to increased gain, making it suitable for point-to-point links.
- **Broader beamwidth**: Covers a larger area but has lower directivity and range due to lesser gain, making it suitable for broadcast applications.

Attenuation and Gain: Decibel (dB) unit

- **Attenuation:** Loss of energy when signal traverses through a medium
- **Gain:** $\uparrow$ in energy $\rightarrow$ devices employed to improve signal strength
- $\boxed{dB = 10\log_{10}\frac{P_2}{P_1}}$ (where P_1 is input power, P_2 is output power)
- e.g. supposed signal travels through transmission medium, power $\downarrow$ to $\frac{1}{2}$ original value, meaning $P2 = \frac{1}{2}P1$.
- $10\log_{10}\frac{P_2}{P_1} = 10\log_{10}\frac{0.5P_1}{P_1} = 10\log_{10}0.5 = 10(-0.3) = -3dB$
- Effectively, loss of $3dB$ is equivalent fo losing half of the signal power

Unit of power of a signal: dBm (decibel milliwatt)

- Decibel (dBm) is a measure of signal power, calculated as $10\log 10(P_m)$ where P_m is power in milliwatts (mW)
- $0\ dBm$ represents a transmit power of $1mW$ $\rightarrow$ common reference point in communication systems
- $30\ dBm$ which corresponds to transmit power of $1W$ is often the maximum permissible output power for devices operating in unlicensed frequency bands, e.g. those in Wi-Fi and other wireless communication technologies.

Estimating received signal strength and range: Friis propagation model

$$\boxed{P_r = G_r G_t \left(\frac{c}{4\pi f_c d}\right)^a P_t}$$

(in dBm)

- f_c center frequency in Hertz
- c = speed of light
- d = distance btw transmitter/receiver
- a = path loss component
- G = antenna gain

Environment	Path Loss Exponential (α)
Free Space	2
Urban area cellular radio	2.7 to 3.5
Shadowed urban cellular radio	3 to 5
In building LOS	1.6 to 1.8
Obstructed in building	4 to 6
Obstructed in factory	2 to 3

Free Space Path Loss — $FPSL(\textbf{linear}) = \frac{4\pi df}{c}^2$

- Loss of power by signal as it transmits from the transmitter to receiver
- d is the distance between the transmitter and receiver antennas (in meters),
- f is the frequency of signal (in Hertz), c is speed of light in a vacuum
- $\boxed{FPSL = 20\log_{10}(d) + 20\log_{10}(f) + 20\log_{10}(\frac{4\pi}{c})}$ — in dB always

Total link gain in wireless communication

- net amplification/attenuation of EM signal along the communication path
  - Antennas, FSPL, any other system component is also included:

$$\boxed{(\text{dB}) = G_{Tx} + G_{Rx} - L_{Path} - L_{Misc}}$$

  - G_{Tx} = Transmitter antenna gain (dB)
  - G_{Rx} = Receiver antenna gain (dB)
  - L_{Path} = Path loss (dB), including free-space loss
  - L_{Misc} = misc losses (dB), (atmospheric/cable losses/interference)

Link Budget and Total Link Gain

- Calculation that takes into account all gains/losses to determine received signal strength of wireless signal in a communication system
- Total Link Budget (P_{rx}) = $P_{tx}+$ Total Link Gain
- **Total Link Budget** $\boxed{P_{Rx} = P_{Tx} + G_{Tx} + G_{Rx} - L_{Total}}$
  - P_{Tx} = Transmit power in dBm.
  - G_{Tx} = Transmit antenna gain in dBi.
  - G_{Rx} = Receive antenna gain in dBi.
  - L_{Total} = Total losses (e.g., free space path loss, cable losses) in dB.
  - P_{Rx} = Received power in dBm.

dB, dBm and dBi operations

- db (Decibel): log unit for ratios (gain/loss), dimensionless
- dBm: absolute power reference to $1mW$, $0dBm = 1mW$
- dBi: Antenna gain relative to isotropic radiator. Measures directionality
- **Adding dB values:**
  - If 2 components contribute gain/loss, we add their dB values
  - e.g. 2 amplifiers with +10dB and +5dB gain
- **Adding dBi to dBm to get EIRP**
  - Effective Isotropic Radiated Power (EIRP): total output power including antenna gain: $EIRP = P_{TX}(dBm) + G_{antenna}(dBi)$
- **Subtracting Losses (dB) from Power (dBm)**
  - Losses (cable/FPSL) can be subtracted from transmitted power
- **Subtracting dBm values to get dB diff.:** Used to compare 2 power EIRP
- You cannot add dBm values directly as dBm represents absolute power, log values cannot be added directly
  - Must convert to linear scale e.g. $10dBm = 10mW + 20dBm = 100mW$, Total power = $110mW = 10\log_{10}(110) = 20.4dBm$

Operations with dB, dBm, and dBi

Operation	Valid?	Explanation
dBm + dBm	×	Log scale absolute powers can't be added directly
dBm + dBi	✓	EIRP calculation: antenna gain added to transmit power
dBm - dB	✓	Used to subtract path/cable losses
dB + dB	✓	Gains/losses (ratios) are additive in log scale
dBm to linear (mW)	✓	$P_{mW} = 10^{P_{dBm}/10}$
Linear (mW) to dBm	✓	$P_{dBm} = 10\log_{10}(P_{mW})$
dBm + dBm (via linear)	✓	Convert to mW, sum, then log: $P_{total} = 10\log_{10}(P_1 + P_2)$

Modulation

Amplitute modulation

- Change amplitude of carrier signal according to the message signal

$$\boxed{s(t) = [A_c + A_m \cdot m(t)] \cdot (2\pi f_c t)}$$

  - A_c Carrier Amplitute
  - A_m Baseband signal amplitude
  - $m(t)$ Message signal
  - f_c Carrier Frequency
- **Modulation Index**
  - For amplitude modulation $\mu(modulation\ index) = A_m/A_c$
    - A_m = Peak amplitude of modulating/baseband signal
    - A_c = Peak amplitude of carrier signal
    - $\mu < 1$: under-modulated (weak signal, no distortion); $\mu = 1$: fully modulated; $\mu > 1$: over-modulated (distortion, clipping)

Frequency modulation

- Change frequency of carrier signal according to the message signal
- Advantages over AM: resilient to interference, spectrum efficiency
- Remains widely used for radio broadcast, also computer communication
- Bandwidth of frequency modulated signals

$$\boxed{s(t) = A_c cos(2\pi f_c t + 2\pi k_f \int m(t)dt))}$$

  - A_c Carrier Amplitute, f_c Carrier Frequency
  - k_f Frequency sensitivity of modulator (how much carrier freq. changes in response to amplitude of modulating signal)
  - $m(t)$ Modulating signal
- **Modulation Index**
  - $\beta(modulation\ index) = \triangle f/fm$
  - Given by Carson's rule, bandwidth is $2(\triangle f + fm)$
  - $\triangle f$ = Peak frequency deviation (how much carrier frequency changes)
  - f_m = Maximum frequency of the modulating signal
  - $B < 1$: Narrow band signal, $B > 1$ Wideband signal, better noise immunity, signal quality, FM broadcast

What is a phase

- Represents position of point on waveform cycle, an offset from starting position of sine wave
- Complete cycle of sine wave is 360 degress / 2 π radian

$$\boxed{s(t) = A\cos(2\pi ft + \phi)}$$

  - A = Amplitude of signal
  - f = Frequency of signal
  - ϕ Phase (phase contstant / offset)

- ϕ determines where in its cyclewave is (begins at $t = 0$)
- Changing phi shifts waveform left or right in time
- **Impact of phase shifts on waves (summation)** (interference)
  - *Constructive:* 2 waves with same phase add tgt to form larger amplitude
  - *Destructive:* 2 waves out-of-phase (e.g. 180deg apart), cancel each other

Phase modulation

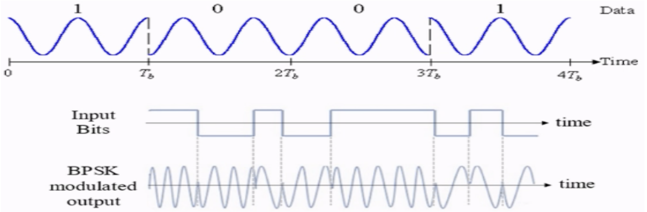
- Change phase of carrier signal according to the message signal
- Integral part of modern communcation standards: Wifi/Television
- Advantages over FM: Better SNR and spectral efficiency
- Uses different phase shifts to represent digital data

$$\boxed{s(t) = A\cos(2\pi f_c t + 2\pi k_p m(t))}$$

  - A = Amplitude of signal
  - f_c = Carrier frequency
  - k_p = Phase sensitivity (rad / unit amplitude)
  - $m(t)$ = modulating signal

Binary Phase Shift Keying

- simple form of phase modulation where phase is shifted between 2 values
- *Bit 0* $\rightarrow$ 0 degrees ($A\sin(2\pi f_c t)$)
- *Bit 1* $\rightarrow$ 180 degrees ($A\sin(2\pi f_c t + \pi)$)



Quadrature Binary Phase Shift Keying

- extends BPSK with 4 distinct phase states, allow encoding of 2 bits/symbols
- *Bit 00* $\rightarrow$ 45 degrees ($A\sin(2\pi f_c t + \pi/8)$)
- *Bit 01* $\rightarrow$ 90 degrees ($A\sin(2\pi f_c t + \pi/4)$)
- *Bit 10* $\rightarrow$ 135 degrees, *Bit 11* $\rightarrow$ 225 degrees
- We are *doubling the bit rate* for the same bandwidth

Digital equivalent of AM FM and PM modulation

- Vary analog signal according to digital bits
  - ASK: amplitute/FSK: frequency/PSK: phase shift keying
- Digital variants relevant when we talk about computer communication

Link Quality Metrics:

- **Packet Delivery Ratio (PDR)**: ratio of successfully received packets to transmitted packets. $\boxed{PDR = \frac{Received\ Packets}{Transmitted\ Packets} \times 100}$
  - $\uparrow =$ better link quality, $\downarrow =$ congestion/interference or poor connectivity
- **Bit Error Rate (BER):** Ratio of bits received in error to the total transmitted bits. Indicates transmission quality at the physical layer
  - $\boxed{BER = \frac{Errored\ Bits}{Total\ Bits\ Transmitted} \times 100}$
  - $\downarrow =$ fewer errors + better link perf. $\uparrow =$ data corruption / retransmissions
  - Wired Ethernet: 10^{-12}, Wireless Wifi: 10^{-6} to 10^{-3}, Poor cxn $= 10^{-2}$
- **Signal-to-Noise Ratio (SNR):** Ratio of signal power to background noise, often measured in decibels. $\boxed{SNR = 10\log_{10}(\frac{P_{signal}}{P_{noise}}) \text{ — if } P \text{ in } W}$
  - Else $P_{signal} - P_{noise}$ in dBm
  - $\uparrow =$ stronger signal, fewer errors. $\downarrow =$ more packet loss.
- **Expected Transmission Count (ETX):** Measures expected number of trasmissions (including re-trasmission) required for packet to successfully received. Used in routing algorithms $\boxed{ETX = \frac{1}{P_{forward} \times P_{reverse}}}$
  - Lower ETX means fewer transmission and better efficiency, higher leads to increased latency and power consumption

Understanding Channel Capacity & Link Quality

- **Definition:** Maximum rate at which information can be transmitted over a communication channel without error.
- Channel capacity is measured in the unit of **bits/second**.
- How does channel capacity relate to link quality?
  - Higher **SNR** usually leads to a higher capacity.
  - Recall bandwidth is the frequency range over which the signal is transmitted; a wider bandwidth can support higher data rates.
  - Factors that reduce link quality: **Fading, interference**, reducing channel capacity.
- Channel Capacity and Link Quality — Shannon Perspective:

$$C = B \times \log_2(1 + \frac{S}{N})$$

  - C Channel capacity in bits per second (bps)
  - $B =$ Bandwidth of the channel in Hertz (Hz)
  - S/N Signal-to-noise ratio (SNR) expressed as linear ratio

Processors, Memory, Contiki

- Microcontroller (μC) small computer on single integrated circuit on simple CPU with peripheral devices (I/O, timers, memories)
- Low power, often include sleep mode that dramatically reduces the power consumed to micro or even nanowatts

ISA and Realization

- **Instruction set architecture:** definition of instructions that processor can execute and certain structural constraints (such as word size) that realizations must share
- **Processor, Realization Chip:** Piece of silicon sold by vendor which is realization of the ISA
- A ISA may appear in many different chips often made by different manufacturers with widely varying performance profiles

Digital Signal Processor

- Deal with large amounts of information, Sample in time/space/both
- Sophisticated mathematical operations like filtering, frequency analysis
- Digital signal processor are class of processors optimized for such mathematically intensive tasks

Random access memory

- Fast, temp storage where individual bytes/words can be read/written quickly

- **SRAM (static RAM):**
  - Faster, more reliable
  - Uses more silicon area per bit
  - Data remains as long as power is maintained
- **DRAM (dynamic RAM):**
  - Uses less area/bit (higher density)
  - Requires periodic refresh cycles to maintain data, can introduce access time variability and potential stalling

Non-volatile memory

- Retains data when power is lost, essential for firmware/persistent user data
- **ROM (Read-Only Memory / Mask ROM)**
  - Fixed content programmed during manufacturing
  - Suitable for mass-produced firmware that does not change
- **EEPROM (Electrically-Erasable Programmable ROM)**
  - Can be reprogrammed in the field, longer write times, limited write cycles
- Flash Memory
  - **NOR Flash:** Accessible like RAM but slowe erase/writes
  - **NAND Flash:** Cheaper, faster erase/write time, data access in large blocks (hundreds to thousands of bits)
  - **Disk memories:** large capacities, involve mechnical parts (spinning disks), leading to slower variable access time

SRAM (RAM) versus Flash (ROM)

- Size and time difference between non-volatile and volatile memory is *significantly* reduced from traditional computing
  - Non-volatile store 2–10x larger than volatile
  - Single-cycle RAM. Maybe two-cycles to Flash (to read)
- Major difference: energy and writability
  - SRAM is low-energy to read and write (no refresh needed)
  - Flash is lowish-energy to read, but very high energy to write
- Hierarchical structure is not enforced
  - Same address space for RAM and Flash (very different from traditional)
  - Run instructions right inside of Flash
  - Keep variables in RAM (or const variables in Flash)

Memory Map

- how processor addresses correspond to physical memory and the peripherals
- size of memory map constrained by processors address width
- 32 bit processor has 2^{32} locations or 4 GB of memory Accessible
- e.g. ARM Cortex-M3
  - Separation of address spaces: distinct regions for program memory (flash), data memory (SRAM, DRAM) and peripheral devices
  - Havard architecture: Separates instructions (program memory) from data (data memory) to allow simultaneous fetches, improving throughput

Sensors

Eyes and ears for an embedded device. Sense environment and help to understand physical world. Sensor is an electronic component that measures a physical phenomenon.

Models of sensors

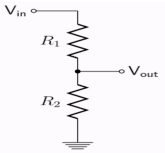
- Many sensors can be modelled approximately as an affine function
- $f : R \rightarrow R$
  - $x(t)$: Physical Quantity reported by sensor at the time instance t
  - $f(x(t))$: Value reported by sensor for the particular physical quantity
  - Function f is linear if there exists proportionality constant $a \in R$ and a bias $b \in R$ s.t. $\forall x(t) \in R$, $f(x(t)) = ax(t) + b$
- **Proportionality constant** a: represents the sensitivity of a sensor, specifies degree to which sensor reading changes in correspondence to the change in the physical quantity
- No sensor truly *realizes an affine function*, range of sensor, set of values of a physical quantity that it can measure is always limited
- Outside that range, an affine function model is no longer valid
- Physical quantities outside this range typically *saturate*
  - These quantities yield a max or min reading outside their range
- When we talk about embedded systems, we focus on *passive sensing* as it is much cheaper and lower energy consumption

Sensors transform phenomenon into electrical signals

- Ohm's Law: voltage (V) = Current (I) × Resistance (R)
- By altering one of the variables, in response to changes in the phenomenon, a sensor generates an analog signal that corresponds with the phenomenon
  - e.g. Resistivity ρ: materials with higher ρ create more resistance for same length/area. $R = \frac{\rho L}{A}$ Sensitive to physical conditions:
    - ∗ Temperature: Many conductors have higher resistivity at higher temps
    - ∗ Light: materials (photoresistors) change resistivity exposed to light
    - ∗ Strain: e.g. strain gauges increase in resistivity when stretched
- ***Temperature*** sensing using resistivity changes
  - Thermistor is a sensor which varies in resistance based on temperature
    - ∗ **Advantages:** cheap and easy to use , low cost
    - ∗ **Disadvantages:** non-linear transfer function
- ***Light*** sensing using resistivity changes
  - Photocell change resistance with light (non-linear)

Voltage Dividers

- $V_{out} = \frac{R_2}{R_1+R_2} \times V_{in}$
  - V_{in} is a voltage source and R_1 and R_2 are resistors
- If $R_1 == R_2$, $V_{out} = \frac{V_{in}}{2}$
- Smaller R_1 means larger V_{out}, V_{out} approaches V_{in}



ADC: Bridging analog and digital worlds — Analog Digital Converter

- ADCs convert analog signals, which have a continuous range of values, into digital signals, which have discrete numerical representations. This is essential for digital devices to process real-world analog inputs.
- **What are the various parameters of the ADC?**
  - **Resolution:** Determined by the number of bits the ADC uses to represent the analog value. More bits mean higher resolution and finer granularity in the output.
  - **Sampling Rate:** The frequency at which the ADC samples the analog signal. Higher sampling rates can capture more detail and are necessary to comply with the Nyquist theorem. It also means higher power consumption.
  - **Accuracy:** The closeness of the ADC's output to the true input value. It includes factors such as linearity, noise, and error rate.

Digital Sensors

- Some sensors incorporate ADC within their circuits to provide digitized signals, which can then be read by a microcontroller.
- **Dynamic Range:** Digital sensors are unable to distinguish between two closely spaced values of the physical quantity. The precision p of a sensor is the smallest absolute difference between two values of a physical quantity whose sensor readings are distinguishable.
  - $D \in R+$ of a digital sensor is the ratio
  - $p =$ represents the precision of the sensor: $D = \frac{H-L}{p}$, where H and L are limits of range in (often expressed as units of decibels)
  - $D_{dB} = 20\log_{10}(\frac{H-L}{p})$, $p = \frac{H-L}{2^{ADL}-1}$, where we take -1 because we usually do not use 0 to represent

Quantization of sensor readings

- Digital sensors represent a physical quantity through a n-bit number
- n is a typically small number, and thus there are 2^n numbers
- Actual physical quantity represented by a real number $x(t) \in R$
- Digital sensor picks **one of the** 2^n distinct numbers to represent it, thus sensor readings are quantized

Ideal digital sensor what should be n and p

- **Ideal digital sensor:** 2 physical quantities that differ by the precision p are represented by digital quantites that differ by 1 bit
- Precision and quantization become intertwined

Sensor Distortion Function

- Defines the output of a sensor as a function of input: $f : R \rightarrow \{0, 1, \cdots, 7\}$
- For sensors with output similar to above, has precision given by following formula $p = \frac{H_L}{2^n}$

Sampling through analog to digital converter

- Physical quantity $x(t)$ is a function of time t
- A digital sensor will sample the physical quantity at any particular points in time to create a discrete signal
- Uniform sampling, there is a fixed time interval T between samples
- T is called the sampling interval
- The resulting signal may be modelled as function $s : Z \rightarrow R$ $\forall n \in Z, s(n) = f(x(NT))$
- Physical quantity $x(t)$ is observed only at times $t = nT$

How does this related to ADCs

- The smaller the sampling interval T, the more costly it becomes to provide more bits in an ADC
- Same cost, faster ADCs typically produce fewer bits and hence have either higher quantization error or smaller range

Noise in sensors and measurement

- Part of signal which we do not want. If we want to measure $x(t)$ and we ended up measuring $x'(t)$ the noist $n(t) = x'(t) - x(t)$
- Noise is the side effect of sensor not measuing exactly what it is supposed to measure: e.g. by sensor imperfection, quantization errors etc

Motion sensing: accelerometers

- measures proper acceleration, sensor circuit measures the position of fixed mass in frame
- mass moves in any direction, gets displaced and results in displacement of mass used to determine acceleration
- Measures usually in gs, where $1g$ = Earth's gravity

Measuring rotation using gyroscope

- Not affected by graviational field
- Bulk rotating devices, or more modern MEMs (microelectromechanical systems) levering optical / electromagnetic properties to detect minute changes in orientation of device

Measuing magnetic field

- Measures the magnetic field, usually used in devices such as compasses
- Satellites also often use these magnetometers for localization

Active sensing: Ultrasound sensor

- Emits high freqency sound waves from sesor which bounces from objects present in the environment
- Estimates distance, proximity by measuring time taken for sound waves to bounce back and propagate back to ultrasound device
- Power conusming, though can be used on IoT devices
- Common applicaiton: Robotics, obstacle detection, water level sensing

Passive Infrared sensor (PIR)

- Detect movement in the environment by detecting change in IR levels
- Often come with plastic lens cover to improve field of view and range

Power management, Energy Efficiency

Battery capacity

- Watt-hour (Wh) = unit of energy equivalent to 1 Watt of power expended for 1 hour of time
- Ampere-hour (Ah) is unit of electric charge equal to charge transferred by steady current of 1A flowing for 1 hour
- Typically wireless devices consume more power than batteried devices

Smart phone power consumption

- Wifi state transition for beacon communication is faster
- However state transition for data communications is still slow due to driver/software overhead

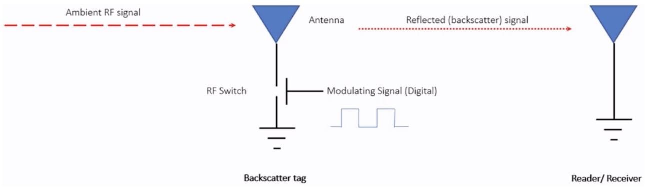
Transmission states for wireless networking

- Device **rarely** transmit continuously
- Having different power states allow power consumption to be reduced

Low-power transmission

Backscatter communication

- Vary between absorbing or reflecting signal to modulate data
  - Wireless transmission at microwatts of power draw (10000x energy savings)
  - Frequency bands: 400MHz, 900MHz 2.4GHz



Communication using inductive coupling

- Shared magnetic field created between 2 devices
- $\triangle$ current through one induces current charge on other
- Device can vary load to transmit
- Very low frequency bands (135 KHz, 13.56 MHz), transmit through materials like skin, but sensitive to metal

Near Field Communication

- Inductive Coupling concept (13.56 MHz): attached to powered + capable device, $10 - 20$cm range, Data range $100 - 400$ kbps
- Can act as tag or reader (smart phone can power a tag if needed, and act like a card to respond to reader)

Wireless communcation through Light

Light Fidelity (LiFi)

- **Advantages:** Illuimination, Energy and Communication
- **Disadvantages:**
  - Cannot propagate through physical boundaries, good for privacy but limited deployable locations for IoT devices

Communication Layers

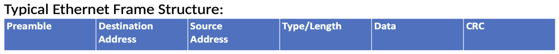
Layers define how data travels from one system to another across networks. A standardized approach to networking ensures interoperability, efficiency, and reliability

- Simplifies complexity: Each layer focuses on specific functions
- Facilitates interoperability: Layers are standardized and interoperable between different systems
- Allows easier troubleshooting: Issues are isolated within a specific layer
- Promotes modularity: Layers can evolve independently without impacting the entire system

Duty Cycles: Active Time / Total Time
Avg Power Consumption: (Active Power Consumption × Duty Cycle) + (Idle Power Consumption × (1 - Duty Cycle))

Open System Interconnection Model

1. *Application Layer:* Interacts with user applications (e.g., HTTP, FTP, email protocols)
2. *Presentation Layer:* Formats or translates data into an appropriate form (e.g., encryption/decryption, data compression)
3. *Session Layer:* Manages communication sessions between applications (establishes, maintains, and terminates sessions)
4. *Transport Layer:* Ensures efficient communication between objects
   - TCP (Transmission Control Protocol):
     - Connection-oriented
     - Guarantees data integrity through acknowledgments and retransmission
     - Ideal for email, file transfers, web browsing
   - UDP (User Datagram Protocol):
     - Connectionless, fast delivery without guaranteed delivery or order
     - Ideal for streaming media or gaming applications
5. *Network Layer:* determines how data moves through interconnected networks
   - IP (Internet Protocol):
     - Assigns unique addresses (IP addresses) to devices
     - Routes packets efficiently from source to destination
     - Supports both IPv4 (32-bit addresses) and IPv6 (128-bit addresses)
6. *Data Link Layer:* responsible for packaging data into frames, managing direct communication between adjacent network devices, handling error detection and correction, and coordinating access to shared media (e.g., Ethernet, WiFi)
   - Framing:
     - Groups bits into structured "frames".
     - Adds headers and trailers for addressing and error-checking
     - Ensures data integrity through checksums (CRC - Cyclic Redundancy Check)



Typical Ethernet Frame Structure:

Preamble	Destination Address	Source Address	Type/Length	Data	CRC

   - Logical Link Control (LLC):
     - Manages communication flow between sender and receiver
     - Handles error detection, correction, and acknowledgments
   - Media Access Control (MAC):
     - Regulates device access to shared media (wired or wireless)
     - Ensures orderly transmission of data

- Protocols:
  - Ethernet defines how devices format data into frames for wired local networks, managing frame structure, addressing, and media access (MAC).
  - WiFi (IEEE 802.11) protocols similarly manage framing, addressing, error detection, and media access for wireless communication.
- Wireless Considerations:
  - **Robustness:**
    - Frames require additional control data to handle physical layer variations (e.g., varying signal strength and interference)
    - Different modulation rates might be used for different packet segments (headers might be transmitted at lower rates to enhance reliability)
  - **Explicit Routing Information:**
    - Supports multi-hop wireless networks (e.g., mesh networks)
    - Ensures packets follow a defined route for optimal reliability
- Error Detection and Recovery:
  - Error Detection:
    - Techniques such as CRC and checksums
    - Quickly identifies corrupted data for retransmission
  - Error Recovery:
    - Automatic Repeat Request (ARQ) mechanisms
    - Retransmits corrupted data or missing packets
  - Significance for Wireless:
    - Wireless communication experiences higher error rates due to environmental factors
    - Efficient recovery strategies are essential to reduce costly retransmissions
- Medium Access Control (MAC): handles device access to shared communication channels to prevent collisions + efficient utilization
  - Wired (ETH), MAC ensures orderly data transmission on shared cable
  - Wireless, MAC coord transmissions to avoid interference + collisions

MAC for wireless

- Wired networks are constant, reliable, and physically isolated
  - Ethernet has the same throughput minute-to-minute
  - Bits sent through Ethernet or USB are (usually) received
- Lack of wires introduces variability, unreliability, and vulnerability to interference compared to wired communication
- Wireless networks are variable, error-prone, and shared
  - WiFi throughput changes based on location and walls
  - Signals from nearby devices interfere with your signals
  - Individual bits might flip or never be heard at all
  - Wireless signals degrade with distance, obstacles, and interferences
- Increasing **network capacity** is challenging
  - Wired networks just add more wires, buses are many signals in parallel to send more data
  - Wireless networks, adding more links increases interference, need expand to diff frequencies

Channelization Protocols

FDMA — Frequency Division Multiple Access

- Separate transmissions by placing then at diff freq.
- Technically, each device can use a separate, fixed frequency
  - One example can be walkie-talkies (mostly separate), $\uparrow$ throughput and reliability, spatial diversity
  - **Disadvantages:** If devices are not always transmitted, that part of the spectrum is not being used — inefficient use of the entire spectrum

Multi Channel MAC Protocols

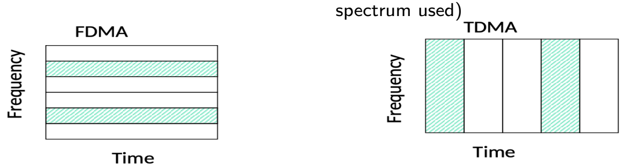
- Control channel: default, time syncrhonization for control/msg exchange
- Nodes switch to different channel for data communication
- All channels used for comm. , node switches channel when link quality bad

TDMA — Time Division Multiple Access

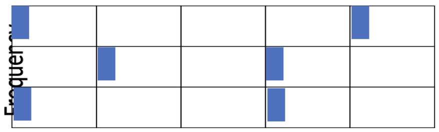
- Split transmission in time, devices share same channel
- Splits time into fixed-length windows: each device assigned 1 or more window, can build priority system here with uneven split among devices
- Requires syncrhonization between devices
  - Often devices must listen periodically to resynchronize
  - Less efficient use of slots reduce synchronization
  - Large guard windows e.g. 1.5 second slot for 1 second trans.

Orthogonal Frequency Division Multiplexing — OFDM

- FDM: entire frequency spectrum is dedicated to carry data from a single source
- OFDM: data divided into many (slower) bit streams and multiple subcarriers (each with smaller spectrum used)

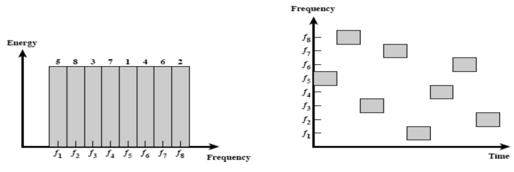


In practical systems, TDMA is often combined with FDMA



Frequency and Time leads to Spread Spectrum (SS)

- Spread-spectrum techniques are methods by which a signal is deliberately spread in the frequency domain, resulting in a signal with a wider bandwidth
- Such techniques can be used to establish secure communications, increase resistance to natural interference, jamming and to prevent detection
- **Advantages:**
  - Resistant to narrowband interference
  - Signals are difficult to interpret – appears as if increase in background noise
  - Can share frequency band with others with minimal interference


Energy
5 8 3 7 1 4 6 2
f_1 f_2 f_3 f_4 f_5 f_6 f_7 f_8
Frequency
Frequency
f_8 f_7 f_6 f_5 f_4 f_3 f_2 f_1
Time

(a) Channel assignment (b) Channel use

FHSS increase resistance to a) natural interference b) jamming c) detection

Spectral Efficiency

- Spectral efficiency (in bits/s/Hz) determines how efficiently devices utilize allocated bandwidth, depending on the modulation scheme
- Different modulation schemes provide different spectral efficiency:
  - Simple modulation (e.g., FSK) $\approx$ 1 bit/s/Hz
  - Advanced modulation (e.g., QPSK, QAM) higher bits/s/Hz (2–8 bps/Hz).

Random Access Protocol

- Networks are increasingly wireless and dynamic:
  - Rapid proliferation of mobile devices, sensors, and IoT nodes
  - Devices join or leave networks unpredictably; traffic patterns not always regular predictable
- Fixed scheduling is challenging or impractical:
  - Pre-allocating transmission slots becomes inefficient when traffic is bursty/unpredictable
  - Scheduled transmissions waste resources if nothing to send during allocated slots
  - RAPs an efficient, lightweight solution for managing sporadic, unscheduled, low-rate data transmissions

Aloha

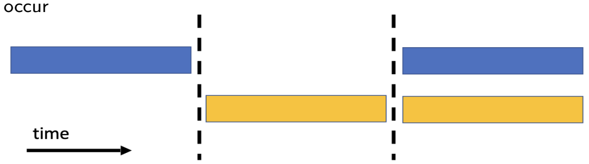
- Devices transmit whenever data is available, without explicit coordination, no prior scheduling or channel sensing; purely random transmissions
- Rules:
  1. If you have data, transmit immediately
  2. After transmission, wait a certain time to receive acknowledgment (ACK)
  3. If ACK is received, transmission successful; if no ACK, wait a random time interval and retransmit (exponential backoff recommended)
- Collision Problem:
  - If ≥ 2 nodes transmit simultaneously, collision occurs, results in lost data
  - Nodes do not listen before transmitting (no channel sensing)

Packet collisions are bad, we need to avoid them

- Each packet transmission has a window of vulnerability
  - If two nodes transmit within one packet-duration interval, collision occurs
  - The time duration is the on-air duration of a packet
  - Competing transmissions during the packet are bad

  - Competing transmissions before packet can also be bad

- Slotted Aloha:
  - Slotted ALOHA reduces collision windows by aligning transmissions to predefined slots
  - Requires synchronization: Every device must know slot boundaries, adding complexity to the implementation and device
  - Real world Analogy: Speaking during predefined time slots in a conference
  - Slotted throughput is double because the “before” collisions can no longer occur



Why Use Random Access if Efficiency is Limited

- *Simplicity and low overhead:*
  - RAPs do not need complex synchronization or scheduling mechanisms
  - Suitable for resource-constrained IoT or sensor networks
- *Efficiency in low-load scenarios:*
  - Collisions are rare when network load is low
  - Random access can achieve low latency for intermittent or bursty transmissions
- *Real-world usage examples:*
  - BLE beaconing: Short, random broadcasts to discover devices
  - LoRaWAN: Simplicity and battery efficiency preferred over maximizing throughput
  - Satellite and RFID networks: Sporadic data transmission scenarios

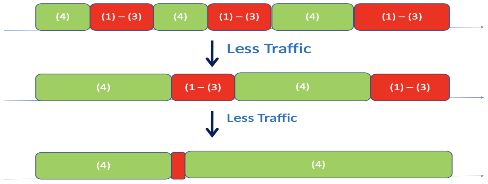
Carrier Sense Multiple Access w/ Collision Avoidance (CSMA/CA)

- Carrier Sense Multiple Access with Collision Avoidance is a medium access control protocol widely used in wireless networks (especially WiFi)
- Nodes sense the medium to check if it's busy before attempting transmission, but collisions are actively avoided rather than detected after occurrence
- Why is Collision Avoidance necessary:
  - Wireless networks have difficulty reliably detecting collisions directly due to signal fading, interference, and hidden nodes.
  - Collision Avoidance proactively reduces the probability of collisions occurring
- Algorithm:
  1. *Listen first (Carrier Sensing):* Nodes listen (sense) the channel before transmission. If the channel is busy, the node waits.
  2. *Random Backoff (Collision Avoidance):* Once the channel becomes idle, nodes don't transmit immediately. Instead, they wait for a random time interval (random backoff period) before transmitting
  3. *Transmit Data:* After the random wait, if the medium remains idle, the node transmits its data
  4. *Acknowledgment (ACK):* Successful reception is confirmed through an ACK from the receiving node. Lack of ACK implies potential collision or error, triggering retransmission
- Choosing W_{max}
  - Intuitively, W_{max} should be small when there is lower chance of collision and vice versa
  - W_{max} varies according to the Binary Exponential Backoff (BEB) algorithm.
  - Set “slot time” to 2 times the max. propagation delay on the channel
  - If this is the first transmission, sends immediately
  - If there is a collision, after i-th collision, pick W_{max} randomly between 0 and $2^i - 1$ time slots.
- Binary Exponential BAckoff (BEB)
  - If collisions occur, waiting intervals adaptively increase to further reduce future collision probability
  - Each successive collision indicates higher channel contention
    1. Initial attempt: Small waiting period (randomized within a small range).
    2. After each collision: The range (window size) for the random backoff doubles (exponential increase), reducing collisions progressively:
       ∗ 1st collision: Wait between $0 - (2^1 - 1)$ slots
       ∗ 2nd collision: Wait between $0 - (2^2 - 1)$ slots
       ∗ After i-th collision: Wait between $0 - (2^i - 1)$ slots
- Trade-offs:
  - More aggressive (smaller W_{max}) – more likely to achieve higher channel utilization, but also more likely to collide
  - Less aggressive – lower channel utilization, less likely to collide
  - **Utilization vs Delay:** Overly aggresive or conservative can increase delay
  - **Optimal point depends:** no. of stations/nodes contenting + traffic load
- CSMA with RTS/CTS
  - Occurs when two transmitters cannot sense each other's transmissions but interfere at a common receiver
  - RTS/CTS Mechanism:
    ∗ Request to Send (RTS): Short control frame sent by transmitter requesting access
    ∗ Clear to Send (CTS): Receiver replies if it's ready, informing nearby nodes to remain silent temporarily
  - A partial solution
    ∗ When channel is idle, transmitter sends a short (RTS)
    ∗ Receiver will send a Clear To Send (CTS) to only one node at a time
    ∗ RTS collisions are faster, less wasteful than hidden terminal collisions
    ∗ Downside: overhead is high for waiting for CTS when contention is low

Medium Access Control for Internet of Things

- General wireless MAC protocols typically optimize for:
  - Low Latency
  - High Channel Utilization
  - Fairness (all nodes have equal chance to communicate)
- However, IoT has unique requirements:
  - Extremely low power consumption
  - Typically, low and intermittent channel utilization
- Priority shift for IoT MAC protocols:
  - Energy conservation becomes the primary design goal
  - MAC protocols must minimize power usage to prolong battery life

“Life Cycle” of MAC Protocols



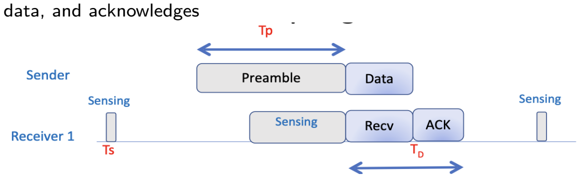
As traffic load decreases, the proportion of energy consumed by idle listening increases significantly. This makes idle listening the dominant source of wasted energy in low-load IoT networks.

- Idle listening consumes significant energy, especially at low load:
  - Measurements show idle listening can consume between 50% to 100% of the energy needed for actual receiving
- Dilemma clearly presented: If nodes turn off their radios to save power, how will they detect incoming transmissions?
- Solution: Duty cycling—periodically waking up briefly to sense transmissions, then returning to sleep mode
  - Nodes sleep when inactive, drastically reducing idle listening time
  - Periodically “wake up” to sense channel activity

- Challenges:
  - ∗ Determining the optimal wake-up schedule is critical
  - ∗ Coordination required to ensure nodes wake at the right time to detect transmissions

ALOHA with Preamble Sampling

- Determining the optimal wake-up schedule is critical
- Coordination required to ensure nodes wake at the right time to detect transmissions
- Algorithm:
  - Sender transmits a long preamble to "wake up" receiver
  - Receiver periodically wakes briefly to sense for preambles
  - Once a preamble is detected, receiver stays awake, receives the actual data, and acknowledges

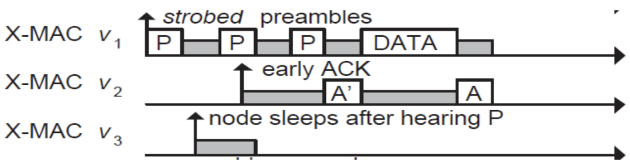


- **Advantages:** Reduces idle listening significantly, saving power, simple to implement async
- **Disadvantages:** Preamble wastes energy at sender and slightly increases latency

B-MAC: Asynchronous Medium Access Control

- Implements preamble sampling concept.
  - Nodes independently choose wake-up intervals (asynchronous).
- Operational Steps:
  1. Sender transmits a long preamble
  2. Receivers periodically sample the channel
  3. If a preamble is detected, the receiver stays awake for data transmission
- Key Parameters:
  - Channel sampling interval: Determines energy usage
  - Long preamble: Duration matches sampling interval to ensure detection
- Pros: Energy-efficient, simple, asynchronous operation
- Cons: Long preamble introduces latency and unnecessary overhead

B-MAC improvements with X-MAC



- Sender transmits many "probes" with gaps between probes. Each probe contains address of intended receiver
- Receiver checks address embedded in probe, sends acks if it is the destination during the gap period between probes
- Sender transmits DATA, receive replies with Ack to complete data transfer

Synchronous MAC

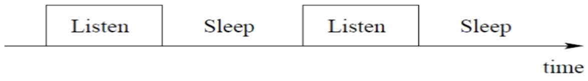


Fig. 1. Periodic listen and sleep.

- Nodes agree to wake up simultaneously at predetermined intervals
- Each interval split into active (listen period) and inactive (sleep period)
  1. 10% duty cycle: 10% of the time nodes listen; 90% sleep.
  2. For example: nodes listen for 100 ms, then sleep for 900 ms.
- **Advantages:** Predictable and coordinated, easier to manage communication during listening
- **Disadvantages:** Requires synchronization overhead, less flexible compared to asynchronous schemese (X-MAC, B-MAC)

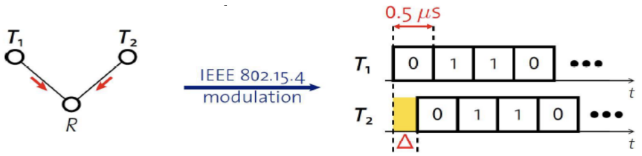
Collisions are not always bad

- Occurs when multiple nodes transmit simultaneously, yet the receiver successfully decodes the strongest signal
- In some scenarios, collisions do not always cause complete failures
- Receiver receives the strongest signal, ignoring weaker interfering signals
- Enhances performance in certain scenarios (dense IoT deployments)

Flooding

- Goal: get information to all nodes, problem of data dissemination
- Problem: difficult in Mesh topologies: packet loss, retransmission delays
- But broadcast transmission do not reach far enough to cover entire mesh

Synchronous Transmissions



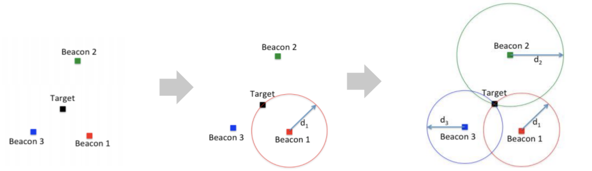
- Multiple nodes transmit same packet at same time
- R can receive packet with high probability if $\triangle$ is small
- May even improve probability of reception (more energy at receiver)
- 500 ns is $1/32$ of a symbol for $802.15.4$ (chip duration)

Wireless Localization

- Localization systems determine the physical coordinates of an electronic device such as IoT nodes, drones, mobile phones or a subject
- Types of the Target's Physical Coordinates
  - **Global (absolute) coordinates:** defined using an external reference system (e.g., GPS), meaning coordinates are absolute and universally understood.
    - ∗ Global coordinates: (37.7749° N, 122.4194° W)
  - **Relative coordinates** defined with respect to another coordinate system, using transformation like rotation, reflection, or translation
    - ∗ E.g., locating an AirTag indoors, for example, inside a room

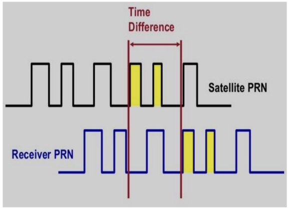
GPS — Global Positioning System

- Satellites placed in Medium Earth Orbit (Altitude 20,000 KM)
- Orbit twice a day, $\geq$ 4 satellites visible from anywhere on Earth at all times
- Steps of GPS positioning:
  1. GPS satellites broadcast their positions and time
     - Position: Global coordinates of the satellite
     - Time: A precise timestamp of when the signal was sent (Time of Transmission)
  2. The GPS receiver (e.g., phone) receives signals from multiple satellites
     - It logs the exact timestamp (Time of Arrival) when each signal arrives
  3. The GPS receiver calculates the distance from each satellite
     - Time of flight = Time of Arrival - Time of Transmission
     - Distance = time of flight × speed of light
     - Speed of light: 3.0×10^8 m/s
  4. Using trilateration, your device computes your exact location
     - With dist. measurements from each beacon, we determine the position
     - Goal: find intersection point of circles(2D)/spheres (3D)



- GPS requires at least 4 satellites
  - 3D scenario: with 3 satellites, trilateration results in two possible locations
  - If the targe device is on the ground, the incorrect point can be easily eliminated.
  - ***However***
    - ∗ Not all targets are on the ground, e.g., aircraft
    - ∗ Clock (time) drift in GPS receivers, e.g., mobile phone

GPS receiver (e.g. phone): Determining distance



Distance = time of flight X speed of light

- Each satellite periodically sends a unique pseudo-random no. sequence
  - Receivers also locally generate the same sequence in synchronized fashion
- Receivers measure time of arrival of the sequence
- Transmission includes time of transmission of the sequence and the location of the satellite at that time
  - Allows receiver to calculate Time of Flight and distance
- Satellites have very accurate (expensive) clocks, and all satellites are precisely synchronized.
- Receivers have less accurate clock, e.g., mobile phone, much cheaper.
- The 4th satellite helps solve for the receiver's clock error `latitude, longitude, altitude, clock drift`

Physical layer of GPS

- Frequency: 1.2GHz and 1.5GHz, $10-15$MHz
- Receiver needs to know additional information:
  - Current time, position of each satellite
- GPS transmission has this data layered on top (50bps)
- Listening for (up to) 30 seconds gets time and this satellite's position
  - Known as ephemeris, valid for up to 4 hours
- Listening for 12.5 minutes gets all satellites' positions
  - Known as almanac, valid for up to two weeks

Assisted GPS

- Cell phone GPS is so quick as only downloads almanac from the internet
- Bootstraps location information, cell towers give coarse position, enables devices to know which satellites are overhead

Beacon Nodes (e.g., GPS satellites)

- Necessary to localize a network in a global coordinate system, also they can be used for finding relative coordinates
- At a minimum
  - Three (non-collinear) beacons required to define a global coordinate system in two dimensions
  - Four non-coplanar beacons for 3-D coordinates
- Beacon Placement
  - Significant impact on localization
  - If the beacons are spread out around the target area instead of being clustered together, we get more accurate positioning
  - Adding an extra beacon somewhere centrally can also improve results

Ways to measure distances

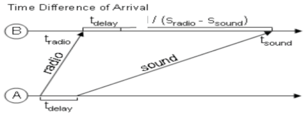
Time of flight — time of arrival (ToA)

- Determine distance by knowing:
  - Exact position of infrastructure
  - Transmit time
  - Receive time
  - Signal velocity (i.e. speed of light)
- Infrastructure transmits and device listens
  - Can happen all the time, but devices only listen when they want a position
- Requires time synchronization between infrastructure and device
  - Synchronization must be good: 1μ s $= 300$ meters
- Important Considerations:
  - Speed of signal propagation, Distance to be measured, Clock accuracy
- Example:
  - Speed of light $(c) \approx 3 \times 10^8$ m/s
  - Distance travel in 1ms = 300m
  - Clock accuracy needed for meter accuracy $(1/c) \approx 3$ns

Time difference of arrival — (TDoA)

- (Target) Device transmits and infrastructure (beacon) listens transmission
  - Multiple infrastructure nodes receive at different times based on distance
- Determine distance by knowing
  - Exact position of infrastructure
  - Time of arrival at two different locations
  - Signal velocity (i.e. speed of light)

- Does not require synchronization with infrastructure!
  - Still requires synchronization between infrastructure nodes
  - Does require device to transmit "loud" enough for infrastructure to hear it
- With different mediums:
  - $\frac{d}{S_{sound}} - \frac{d}{S_{Radio}} + t_{delay}$, Works well in LOS environment
  - Requires additional hardware but works better with calibration


Time Difference of Arrival

Ultrasound

- **Advantages**
  - Solves the barrier problem
    - Human spaces already designed to contain sound
  - Easier to get high-accuracy results
    - Sound is ~1,000,000x slower than light
    - Less synchronization is needed to get same accuracy
- **Disadvantages**
  - More energy to transmit, Slower update rate (still sub-second), Limited range, Pets can hear it

Received Signal Strength Indicators (RSSI)

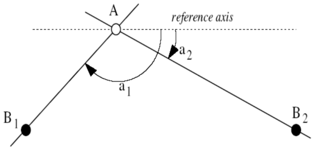
- RSSI measures signal strength to estimate distance
- In theory, RSSI varies with $1/d^{\alpha}$
  - Where α depends on the wireless environment (typically 2 or 3)
  - Common assumption: closer nodes receive stronger RSSI than those further away
- In practice, RSSI ranging measurements contain noise on the order of several meters, highly non-uniform
  - Radio propagation differs over different surface (water, grass, asphalt etc.)
  - Obstacles such as wall, furniture etc.
- **Problem:** Pathloss is NOT only due to distance

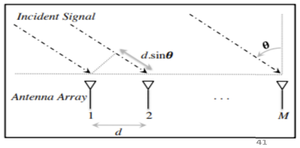
Fingerprinting using RSSI

- Shifts from trilateration to mapping
- Uses RSSI patterns from known locations to determine position
- Phase 1 – Setup
  - Measure signal strength from multiple Access Points at various locations
  - Record measurement in a database – mapping signal strengths to specific locations
- Phase 2 - Localization
  - A device measures real-time signal strength from surrounding APs
  - The system compares these readings to the database to determine the most likely location
- **Wi-Fi Fingerprinting**
- – Repurpose existing infrastructure for localization (e.g. Wifi points)
  - Benefits: localization with unmodified hardware, no extra infra
- **Challenges**
  - Efforts to create database: manual measurements at locations
  - Non-static environment: signal strength changes with obstacles, needs to periodically re-measure and update database
  - Measurements might vary between devices (how you hold it, antennas of devices etc)
- **Variations:**
  - Measurements can be used by several access points simultaneously, improves accuracy quite a bit
  - May not have to be Wi-Fi base dat all, cellular networks do the fingerprinting, deploying your own BLE beacons
- **Accuracy:**
  - State-of-the-art: median accuracy of 0.5-1.5 meters
  - Barrier problems depend on walls

Angle of arrival (AoA)

- Measures direction of incoming signal using antenna array
- By using 2 anchors (B1 and B2), A can determine its position
- BLE 5.1 includes AoA localization
- Leveraging antenna arrays, measures differences in arrival time ($\triangle t$) across the antenna elements
- d is known, antenna spacing, $\triangle t \times$ speed of light $= d \sin\theta$
- $\sin\theta =$ speed of light $\times \frac{\triangle t}{d}$





Sensor Networks

- Once deployed, sensors have to initiate neighbour discovery
- Discover neighbours to connect with one another
- **Naive approach**
  - Node A continously listens its neighbour to transmit signals until hears transmission from Node B
  - Problem is that Node A has to wake up and constantly listen during period, battery drained **quickly**

Synchronous Neighbour Discovery

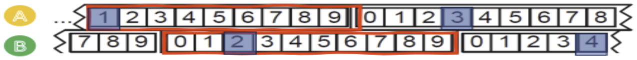
- **All nodes synchronized** to same clock/time
- Nodes scheduled to wake up periodically at same time to transmit/receive
- deterministic approach — provide guarantee bounds on discovery latency
- **Disadvantages**
  - Synchronization overhead, consumes significant power
  - Slow discovery process to detect all nodes

Asynchronous Neighbour Discovery

- **No clock synchronization needed**
- Each device uses its own clock to divide its timeline into time slots
- Each node independently wakeup for TX/RX at random time slots
- No restrict wake-up schedules → much lower average discovery latency

Birthday Protocol - Asynchronous neighbor discovery

Easy to implement + Good average discovery latency but unbounded worst case



1. Nodes have repeating periods (like birthdays repeat every 365 days)
2. Each period has 10 time slots
3. Node randomly pick wake-up slots – shaded boxes

Model probability of birthday paradox

- Two nodes randomly choose to wakeup k time slots (shaded boxes) out of a total n slots (periods). What is the probability that they wakeup at the same time slot at least once?
- Probability (Q) can be written down as:
  - (Duty-cycle: 1%) $n = 100$, $k = 1$, $Q(100, 1) = 0.01$
  - (Duty-cycle: 5%) $n = 100$, $k = 5$, $Q(100, 5) = 0.23$
  - (Duty-cycle: 1%) $n = 1000$, $k = 10$, $Q(1000, 10) = 0.096$
  - (Duty-cycle: 5%) $n = 1000$, $k = 50$, $Q(1000, 50) = 0.928$
- $Q(n,k) = 1 - \frac{\binom{n-k}{k}}{\binom{n}{k}}$ — Drawbacks – probabilistic bound for discovery time, some nodes may take very long sometimes

DISCO - Asynchronous deterministic neighbor discovery

- Scheduling wake-up timeslots at multiples of prime numbers to ensure deterministic discovery
- Nodes can have different duty cycles
- **Version 0:** Node i picks a prime number p_i and wakes up every p_i time slots
  - The duty cycle is $(1/p_i)$
  - In the worst case, two nodes p_i and p_j will meet after $(p_i * p_j)$ timeslots
- **Problem:** what if both nodes pick the same prime number?
- **Improved Version:**
  - Each node picks two prime numbers p_{i1} and p_{i2}
  - Node **wakes up every** p_{i1} **and** p_{i2} **time slots** to ↑ discovery chances
  - The duty cycle is $(1/p_{i1} + 1/p_{i2})$
  - If both nodes pick the same pair of prime numbers:
    - Duty cycle $\approx (p_{i1} + p_{i2})/p_{i1}p_{i2}$, Worst Case time $\approx p_{i1}p_{i2}$

Routing

If all N nodes are connected to each other, there will be $N(N-1)$ or $O(N^2)$ uni-directional links

Structure of wired networks

- Hierarchical and structured
- Use *switches* and *routers* for managing connections and route data
  - Switch connects multiple devices within a local network (e.g., at home or in an office)
  - Router connects different networks together (e.g., your home network to the Internet)
- Adding more switches/routers reduces the number of direct links needed and allows network to scale efficiently

Structure of wireless networks

- Wireless network are typically single-hop: All stations/devices communicate directly with base stations or (Access Points)
  - Example: WiFi, Cellular Network, LoRa
- **Multi-hop**
  - Extends network reach/coverage for the same number of base stations
  - Provides more routes, potentially more robust

Factors (routing metrics) to consider

- Energy efficiency
- Reliability: ensure packets successfully delivered (e.g., ETX)
- Hop Count
- Delay: how long it takes for data to reach the destination
- Other factors: network congestion / throughput

Energy Consumption

- Free space model: $P_r = CP_t/d^{\alpha}$
  - C is a constant — α is an exponent, typically 2 or 3
- Transmission over a total distance d, minimum received power P_0
- **Single-hop** transmission to cover distance d, calculate transmission power (P_1):
  - $P_0 = CP_1/d^{\alpha}$ or $P_1 = P_0/C * d^{\alpha}$
- **Multiple-hop** (N) transmissions to cover distance d, calculate transmission power (P_N) per hop:
  - $P_0 = CP_N/(d/N)^{\alpha}$ or $P_N = P_0/C * (d/N)^{\alpha}$
  - Total transmission power is $NP_N = NP_0/C * (d/N)^{\alpha}$

Reliability

- Ensure packets successfully delivered, minimize packet loss
- Routing Metric: "expected number of transmissions" to successfully transmit a packet, so called ETX
- Measure link quality over time to determine each link's reliability
  - Link quality varies between nodes
  - Fewest hops might not be the "most reliable" path

Measure Packet reception ratio (PRR)

- A transmitter sends S packets over a period of T seconds
- During T sec, the receiver records the number of packets successfully received, denoted as R
- $PRR = R/S$

Overheads of Measuring PRR

- Trade-off between communication cost and reaction time
- Assume ZigBee radio is used (250Kbps), each transmission takes 1ms (~250bits, ~30bytes) and link measurement probes should not collide
- If T=1s, S=100
  - Measurement takes up 10% of bandwidth 1 node
  - If there are 10 nodes, 100 probes need to be transmitted in 1 sec (100% of bandwidth used only for measurement!)
- If T=100s, S=10
  - Measurement takes up very little bandwidth
  - Is S too small?
  - If there is a change in link quality, how long does it take to notice?

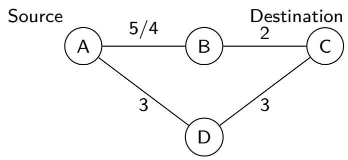
Calculate Expected number of transmissions: ETX

- ETX (expected transmissions) is a commonly used routing metric
- Using Packet reception ratio (PRR): $ETX = 1/PRR$

Routing

Routing using the shortest path algorithm

- Many practical routing algorithms are based on the notion of shortest path between two nodes
- Each link is assigned a positive number called its length
- A shortest path routing algorithm routes each packet along the minimum length (or shortest) path between the source and destination
- If length is always 1, then shortest path becomes minimum hop routing
- By defining the length using metrics like ETX, energy, delay etc, other paths can be obtained



Classification of Routing Protocols

- **Proactive (Routing Table based):** when a packet needs to be forwarded, the best route is already known (stored in the routing table)
- **Reactive (Demand-based):** Determine the best route only when there is data to send

Proactive Routing

- Periodically query for the possible routes in the network
  - Save all routes that are important (maybe just all routes?)
  - Also determine routes whenever topology changes (nodes join/leave)
- **Upside:** when a packet arrives, route to destination is already known
- **Downside:** requires more memory and effort on part of routers
  - Wastes some network bandwidth on checking for route changes

Reactive Routing

- Build up a map of the routes through a network
  - Hopefully the "optimal" routes
- Map routes in reaction to a packet arrival
  - Sensor devices are slow and limited
  - Most likely to resend to same prior address
  - Discover a route when it is needed, then cache for next time

Ad-hoc Networks

- What if the nodes are not static but mobile?
- A Mobile Ad hoc Network (MANET) is an autonomous system of mobile nodes (MS) (also serving as routers) connected by wireless links
- No infrastructure exists in a MANET
- Network's wireless topology may change dynamically in an unpredictable manner since nodes are free to move, each node has limited transmitting power
- Assumption: Due to node mobility, routing path may be available but needs to be "discovered"

Ad-hoc On-demand Distance Vector Routing (AODV)

- **Ad-hoc:** dynamic and temporary networks
- **On-demand:** Construct routes only when needed
- **Distance vector:** routing metric is the number of hops a packet has to pass (Hop Count)

AODV Routing Table

- Store the next hop towards a destination, instead of storing a full path
  - All routers along the path must also have Destination→Next mappings
- Also keep hops-to-destination and last-seen-destination-sequence-number
  - Destination-sequence-number is an indicator of route freshness

AODV Route Discovery

- Upon demand: check table
- If not cached send Route Request (RREQ) via broadcasting
  - Route is unknown, so broadcasting is needed

AODV Route Requests (RREQs)

Request ID	Source Address	Destination Address	Source SeqNo	Destination SeqNo	Hop Count

- Request ID identifies this RREQ
  - Used to discard duplicates during flooding
- Sequence Numbers are per-device, monotonically increasing
  - Used as a notion of "how recently" device has been seen
  - Source SeqNo is the source's most recent sequence number
  - Destination SeqNo is the most recently seen from the destination by the source (Defaults to zero)
- Hop Count is the number of hops this request has taken
  - Starts at 1 and incremented by each transmitter along the path

AODV Route Response (RREP)

Source Address	Destination Address	Destination SeqNo	Hop Count

- Reply is sent unicast back to the source via newly constructed route
  - Each node along the way already knows the route back
- Includes recent destination sequence number as a sense of recency
  - No need for source sequence number anymore

Route maintenance in AODV

- If a link in the routing table breaks, all active neighbors are informed with Route Error (RERR) messages
  - After some number of retransmissions and timeouts
  - RERR contains destination address that broke
- Nodes receiving RERR can start RERQ for destination address
  - Which lets them find a new path through the network
  - And updates everyone's cached next-hops

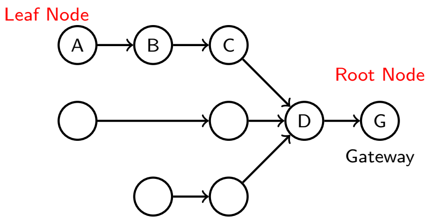
Tradeoffs for reactive routing

- **Upside:** no transmissions unless there is demand
  - Routes might appear, disappear, reappear, but no need to update if no one actually wants to transmit anything
- **Downside:** large, variable delay when actually sending a packet
  - Full RREQ/RREP protocol before data can actually be sent
  - Route might have broken at some point
    - ∗ So data will be sent based on cached information
    - ∗ RERR will occur, RREQ/RREP will occur
    - ∗ Then data will be sent again

Load Balancing in Wireless Network

Many-to-one Sensor Networks

- Data collection follows a spanning tree
  - All data is collected on a single node (gateway)
- Routing is simple:
  - Each device only needs to remember hop to gateway
  - If gateway wants to send message back, it must include a full hop path
- **Power consumption for each node**
  - Per-node power consumption for data transmission and reception grows exponentially from the leaves to the root of the tree
  - Power consumption increases at least linearly when nodes are closer to the sink
  - Typical case is much worse
  - Consequence: the power sources of the nodes close to the sink (gateway) deplete faster.



In-network data aggregation

- To mitigate cost of forwarding, compute relevant statistics along the way: mean (A, B, C), max, min, median etc.
  - E.g., Node C sends mean of (A, B, C)
  - Send one value, instead of three separate messages
- Forwarding nodes aggregate the data they receive with their own and send one message instead of relaying multiple messages
  - Prevents exponentially growing number of messages
- **Issues:**
  - Location-based information is lost
  - Distributed computation of statistics
    - ∗ mean: node needs to know both the mean values and the sizes of samples to aggregate correctly
    - ∗ median: only an approximated computation is possible
- **Applications:**
  - Especially useful in a query-based data collection system
  - Queries regard a known subset of nodes
  - Aggregation function can be specified

Wifi

- Designed for high-speed communication over short indoor ranges
  - Typical range: approximately 10 to 30 meters
  - Primary use: connecting devices like laptops, mobile phones etc.

Basic WiFi network

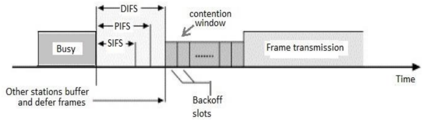
- Star topology network
- A Basic Service Set includes:
  - Access point(s) - AP
  - Multiple connected clients
- Service Set ID (SSID)
  - Identifies network
  - Broadcast by access point in beacons

Random Backoff in WiFi

- Carrier Sense Multiple Access
- Listen for activity
  - If free:
    - ∗ Wait for Inter Frame Spacing (IFS)
    - ∗ If still free, transmit
  - If busy:
    1. Randomly select a number of backoff slots
    2. Count down slots whenever medium is not busy
    3. If busy when backoff completes:
       - ∗ Increase maximum backoff slots
       - ∗ Repeat
- Slot time: basic time unit for protocol
  - Total time of: switch from Rx to Tx, plus processing time, plus propagation delay

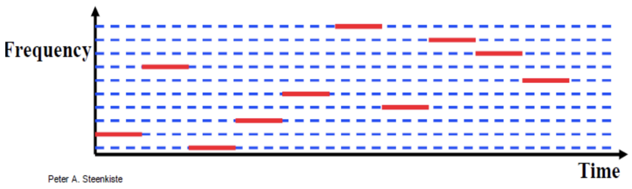
Prioritizing packets with varying IFS

- Tiered Contention Multiple Access (TCMA)
  - Idea: assign different inter-frame spacing based on traffic class
  - Inherently prioritizes communication
- Acknowledgements sent with Short IFS (SIFS)
  - Will always transmit before new data clears CSMA check
- Regular data sent with DIFS
- SIFS ¡ PIFS ¡ DIFS



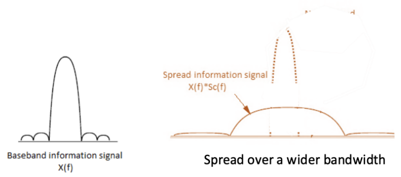
FHSS

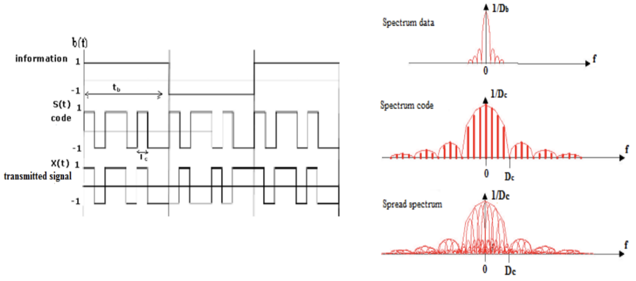
- Frequency Hopping Spread Spectrum
- Frequency hopping over 80 channels (1 MHz each)
- Have the transmitter hop between a seemingly random sequence of frequencies
- Spreading pattern shared by pairs of sender and receiver
- FHSS is one type of *Spread Spectrum technique*



Direct Sequence Spread Spectrum (DSSS)

- Each bit of information is coded so that it uses a larger bandwidth
- Essentially, each bit is multiplied by a sequence of bits with a much higher data rate


Spread information signal
X(f)*Sc(f)
Baseband information signal
X(f)
Spread over a wider bandwidth



DSSS properties

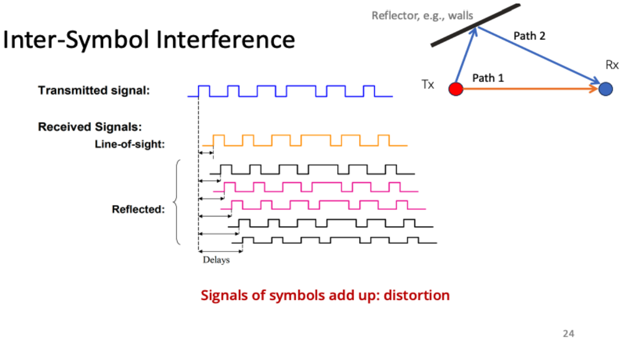
- DSSS increases bandwidth of a signal
  - Beyond what is needed for the data
  - Energy is smeared across the frequencies
- More robust against interference
  - Data can be recovered from partial code
- Data Rate better than FHSS
  - DSSS transmits continuously over a wide band
  - FHSS has to switch frequencies, introducing delays during each hop
- Cost: using a lot of bandwidth for only a little data
- GPS uses DSSS

Spread Spectrum Summary

- Spreading out the signals over a wide channel
  - FHSS (multi-frequency hops)
  - DSSS (single frequency)
- Spread Spectrum:
  - Add Redundancy in frequency domain
  - Spread transmission much wider spectrum band than needed for the intended bit rate
  - Key idea: traffic of other users looks like noise
- Cellular 3G (CDMA) builds on spread spectrum
  - Each pair of the TX and RX must coordinate so RX can apply the same code to decode the data

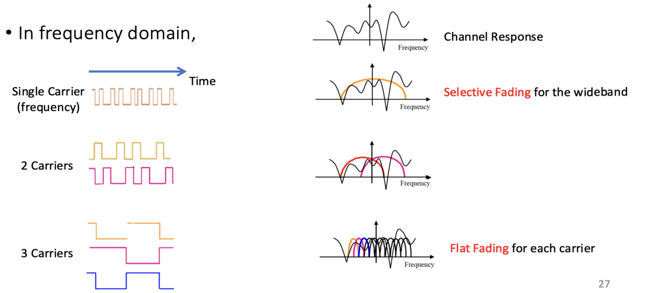
OFDM

- **OFDM:** orthogonal frequency division multiplexing
- **Channel Impact - Multipath:**
  - **Key Issues:**
    - ∗ Frequency selective fading: Induces significant impact at high data rates and on wide-band channels
    - ∗ Inter-symbol interference (ISI): As rates increase, symbol duration shrinks, making ISI effects more pronounced
  - Caused by signal reflection from objects (e.g., walls) creating multiple paths
  - **Solution needed:** An encoding/modulation solution to mitigate multipath effect


Inter-Symbol Interference

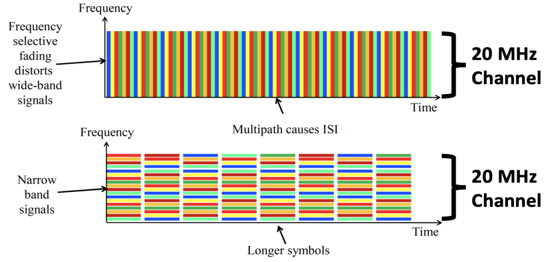
Signals of symbols add up: distortion

Key Idea — Frequency Division Multiplexing


- In frequency domain,

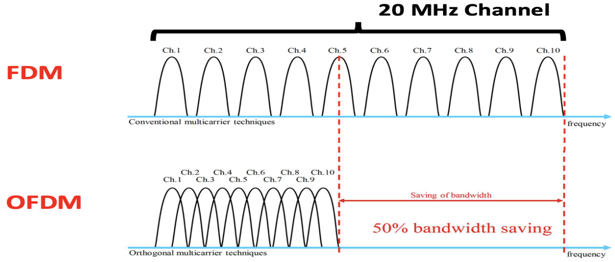
- Each subcarrier is a narrow-band signal with a different center frequency
- Symbol duration increases with number of carriers, more resistance to ISI
- **Implementation:**
  - Distribute bits over N subcarriers that use different frequencies over the band with B bandwidth
  - Each signal uses ∼ B/N bandwidth
  - Multi-carrier modulation
- **Benefits:**
  - Since each subcarrier only encodes 1/N of the bit stream, each symbol can take N times longer in time
  - Since signals are narrower in spectrum, frequency-selective fading is mitigated

FDM Illustration



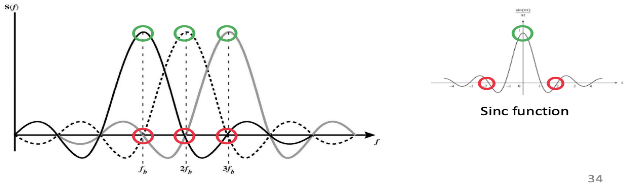
Why Orthogonal in OFDM

OFDM Illustration



- **Goal:** To achieve even higher data rate
- **Challenge:** How to pack multiple subcarriers very densely?
  - Need to support 48 or more subcarriers
  - Must avoid interference between subcarriers
  - Traditional FDM uses guard bands between adjacent subcarriers
- **Solution:** Orthogonal subcarriers
  - Allows denser packing of subcarriers without interference
  - More efficient use of available bandwidth compared to traditional FDM

Orthogonal Subcarriers



- Peaks of spectral density of each carrier falls exactly at the zeros of the other carriers
- Carriers can be packed densely with minimal interference

OFDM enables higher throughput

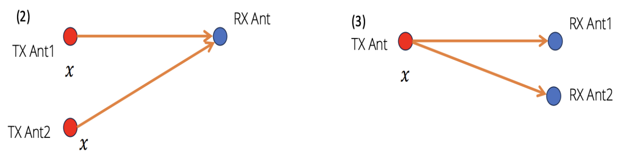
- **Evolution:** Replace DSSS with Orthogonal Frequency Division Multiplexing
- **OFDM Approach:**
  - Split band into a number of narrow subcarriers
  - Subcarriers are spaced so that they don't interfere
  - Transmit on multiple subcarriers at once to increase throughput
- **Implementation:**
  - Receivers collect signal from entire channel
  - Can split it apart to gain data on each subcarrier
  - Process: Frequency-Domain QAM → IFFT → Time-Domain Signal → FFT → Recovered QAM Data
- **Advantages:**
  - Higher spectral efficiency through dense subcarrier packing
  - Parallel transmission across multiple subcarriers
  - Better handling of multipath effects
- **Tradeoffs:**
  - Benefits: more throughput, still robust against narrowband interference
  - Costs: more complicated and sensitive radio design

802.11a - First WiFi with OFDM

- **Implementation (1999):**
  - Applied OFDM techniques on the 5 GHz band
  - Enabled more data throughput 54 Mbps (compare to 11 Mbps for 802.11b)
- **Multiple rates available:**
  - BPSK/QPSK/QAM over OFDM
  - Quadrature Amplitude Modulation (QAM)
- **Channel Structure:**
  - Several 20 MHz channels with no overlap
  - Big increase from "three" channels of 2.4 GHz
  - Various regional rules on number of different channels
  - Needs to avoid frequencies in use by existing radar deployments
- Never reached widespread adoption
  - Regulatory hurdles in some regions

- More complicated hardware delayed it

Use multiple antennas to increase throughput



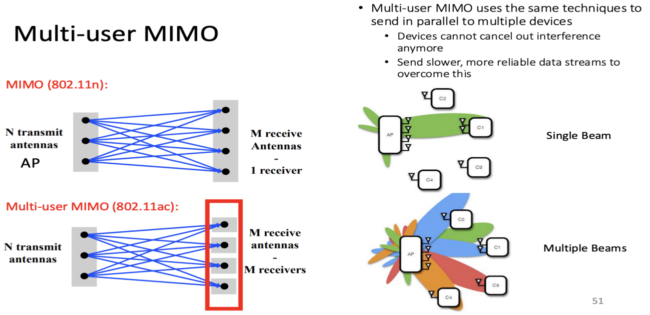
- **Multiple Antenna Benefits:**
  - Receive multiple copies of the same signal
  - Combine copies to improve signal quality (e.g., stronger, clearer)
  - More robust performance in noisy environments
  - Better signal allows for faster data transmission
    - Enables higher data rates without extra bandwidth
- **Multiple Antenna Configurations:**
  - Multiple transmitters to single receiver (2→1)
  - Single transmitter to multiple receivers (1→2)
  - Each configuration provides different benefits for signal quality and reliability

MIMO - Multiple Input Multiple Output

- **Architecture:**
  - N transmit antennas communicate with M receive antennas
  - Creates $N \times M$ subchannels for simultaneous data transmission
- **Benefits:**
  - Huge boost in data throughput
  - Antenna diversity adds to reliability as well
- **Signal Processing:**
  - The signals may interfere with each other
  - But receiving all of them allows the data to be recovered
- **Beamforming:**
  - Use interactions between array of antennas to focus energy on the receiver

802.11n - Wider channels and MIMO

- **Channel Width (2009):**
  - OFDM allows many subcarriers within a channel to be used at once
  - Throughput scales with the amount of bandwidth available
  - Allow larger 40 MHz channels to be used
- **Dual-band Support:**
  - Supports OFDM and MIMO on 2.4 GHz and 5 GHz
  - Supports 20 MHz and 40 MHz channels
  - Easier to create large channels in 5 GHz band
- **Compatibility:**
  - Backwards compatible with 802.11g (tries not to be with 802.11b)
  - Wildly successful
    - Still the 2.4 GHz band protocol (802.11ac is 5 GHz only)
    - A little less than half of the networks visible are still 802.11n



Multi-user MIMO

- Multi-user MIMO uses the same techniques to send in parallel to multiple devices
  - Devices cannot cancel out interference anymore
  - Send slower, more reliable data streams to overcome this

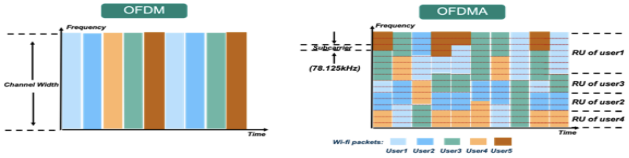
802.11ac - Enhanced MIMO and wider channels

- **Implementation (2013):**
  - Update for 5 GHz band only
  - Supports Downlink MU-MIMO (from AP to device)
  - Supports channel widths up to 160 MHz
  - Engineering updates: up to 256-QAM
- **Deployment Strategy:**
  - Routers apply 802.11ac to 5 GHz and 802.11n to 2.4 GHz

WiFi 6 - Focus on Network Efficiency

- **Primary Goal:** Improve total throughput across all devices in the network
- **Context:**
  - For point-to-point, WiFi is "(more than) fast enough"
  - Now the problem is the quantity of devices in a single space
    - Desktop, laptop, tablet, smartphone, smartwatch, IoT devices, etc.
- **Solution Approach:**
  - Insight: Bring established cellular techniques to WiFi
  - Focus on managing multiple concurrent connections efficiently

OFDMA - Efficient Multi-user Access



- **OFDM vs OFDMA:**
  - OFDM: split channel into subcarriers and transmit on those
  - OFDMA: allocate subcarriers to a device for an amount of time
- **Key Innovation:**
  - Turns OFDM into an access control mechanism
  - Complicated question: which device gets which subcarriers at which time?
- **Benefits:**
  - More efficient use of available bandwidth
  - Multiple users can transmit simultaneously
  - Reduced latency for small data transfers

802.11ax (WiFi 6) - 6 GHz Band Extension

- **Standard Timeline:**
  - Standard approved on February 9th 2021
  - First devices started supporting it in 2019 (WiFi 6)
- **6 GHz Band (WiFi 6E):**
  - 1.2 GHz of bandwidth (5.925-7.125 GHz)
  - 2020: US FCC made band available for unlicensed use
  - EU followed in March 2021
- **OFDMA Implementation:**
  - MAC scheduling variant of OFDM
  - Schedule devices based on time and subcarrier allocations

Feature	FDMA	TDMA	OFDM
Channel Access	Divides channel into frequency bands, each user assigned a specific frequency	Divides channel into time slots, each user assigned a specific time slot	Uses multiple orthogonal subcarriers simultaneously
Collision Handling	No collisions within allocated frequency bands	No collisions within allocated time slots	Minimizes collisions through orthogonal frequency division
Efficiency	Medium: Bandwidth may be wasted if user has no data to send	Medium-High: Time slots may be wasted if user has no data to send	High: Efficient spectrum usage through parallel transmissions
Interference	Vulnerable to narrowband interference	Less vulnerable to frequency-specific interference	Resistant to narrowband interference and multipath fading
Synchronization	No tight synchronization needed	Requires precise time synchronization	Requires frequency synchronization
Best Used In	Simple constant-bit-rate applications, analog systems	Digital cellular systems, satellite communications	Modern wireless networks (Wi-Fi, 4G/5G), high-speed data transmission

Feature	Aloha	Slotted Aloha	CSMA
Channel Access	Transmits immediately when data is ready without checking channel status	Transmits only at beginning of predetermined time slots	Listens to the channel before transmitting (sense-before-send)
Collision Handling	Collisions occur frequently due to uncoordinated transmissions	Reduced collisions compared to pure Aloha, but still occur	Significantly reduces collisions by avoiding transmission when channel is busy
Retransmission	Random backoff time before retrying after collision	Random waiting time before retrying, synchronized to slots	Uses various backoff algorithms (e.g., exponential) to reduce subsequent collisions
Efficiency	Very low: 18% of channel capacity	Low-Medium: 36% of channel capacity	Medium-High: Up to 80% in optimal conditions
Collision Avoidance	None; simply retransmits after collision	None; retransmits at next available slot	Various mechanisms like RTS/CTS and collision detection depending on variant
Best Used In	Simple, very low-traffic networks	Networks with predictable traffic patterns	Wireless and wired LANs with variable traffic loads

Feature	ALOHA with preamble	B-MAC	X-MAC
Channel Access	Sends a preamble before data transmission to announce intent	Uses Low Power Listening (LPL) with long preambles	Uses shortened preambles with target address
Collision Handling	Reduced collisions compared to pure Aloha	Collisions reduced through channel sensing	Improved collision avoidance through early acknowledgment
Power Efficiency	Low: Continuous listening	Medium: Periodic channel sampling	High: Early acknowledgment reduces overhearing
Latency	Medium	High due to long preamble	Reduced compared to B-MAC
Adaptability	Limited adaptability to traffic patterns	Configurable sleep intervals	Adaptable to varying traffic patterns
Best Used In	Simple networks with low power constraints	Wireless sensor networks with low duty cycles	Energy-constrained sensor networks with variable traffic