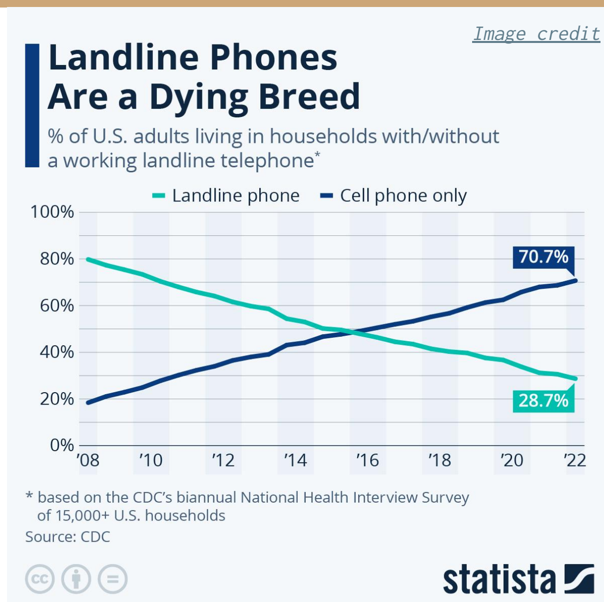
Chapter 7: Physical Layer

WiFi and Cellular

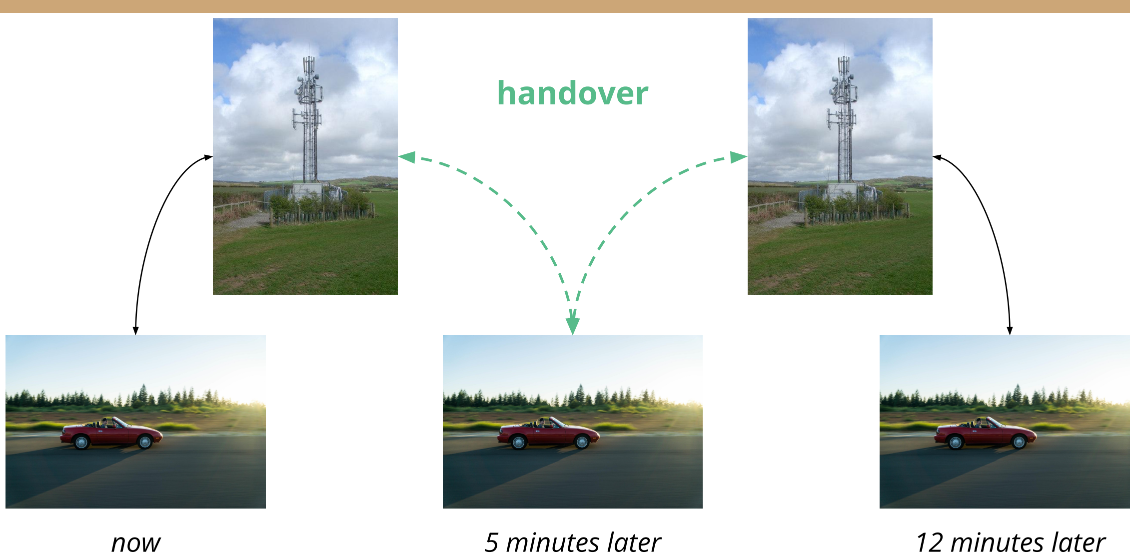
Wireless Connections

- WiFi: 802.11 wireless LANs
  - Wireless Hotspots
- Cellular network: 4G and 5G
- Mobility Management

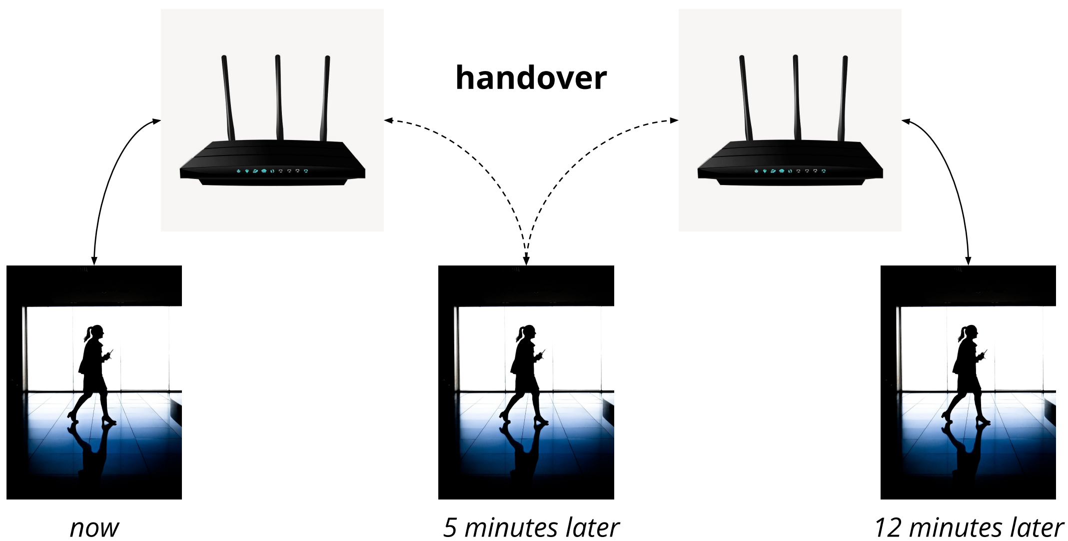
Phones: Landline vs. Mobile Phones



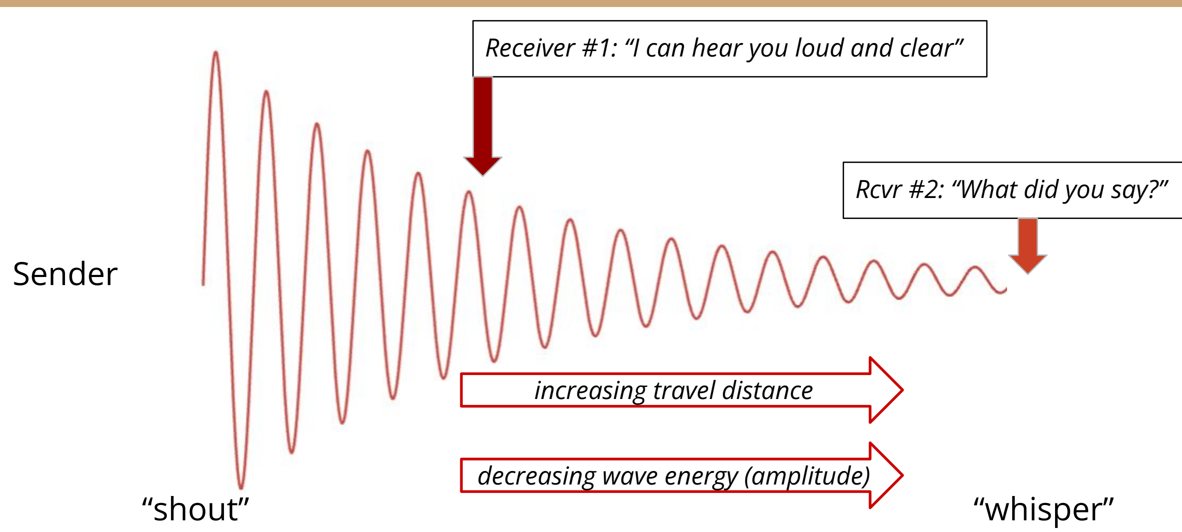
Wireless Connections allow User Mobility



Wireless Connections allow User Mobility



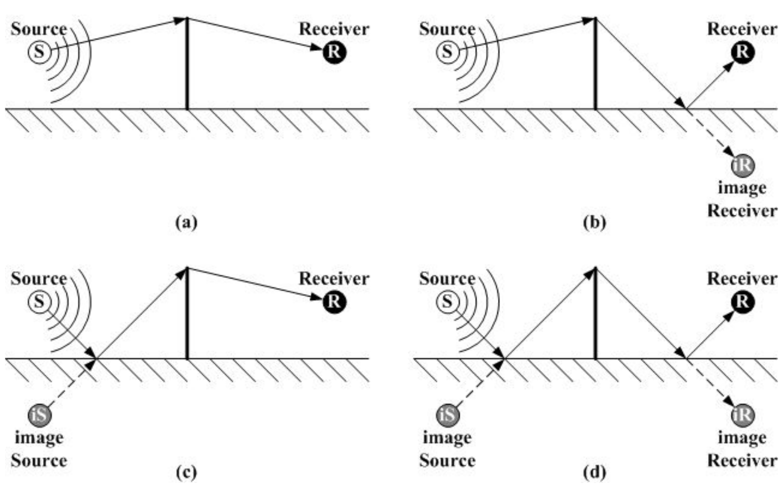
Challenge #1: Wave Energy Dissipation



Solution to Challenge #1

- Use stronger amplifier (expensive hardware, more energy use)
- Use different encoding techniques (software & hardware)

Challenge #2: Multipath Propagation



Multiple "echo" signals (with weaker amplitude) received by R

Solution to Challenge #2

- Rake receivers
  - Use multiple receiver units with increasing delay

Challenge #3: Interference

2.4 GHz WiFi

2.4 GHz Microwave

Solution to Challenge #3

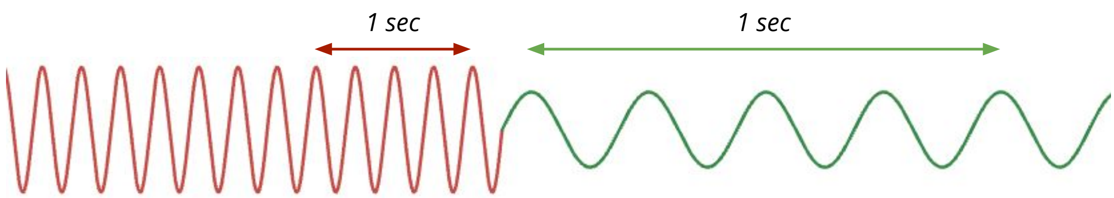
- Use different frequency

Wave Physics Refresher

waveSpeed = waveLength × frequency

- Wave speed is affected only by the medium in which the wave travels
  - speed of sound in air: 343 m/sec
  - speed of sound in water: 1500 m/sec
- Wave frequency is affected by the source of its oscillations
  - When waves travel across different medium, wavelength and speed changes
  - Some of the wave energy may be reflected/conferted/("absorbed"
- Wave energy is proportional to amplitude squared
- Wave energy dissipates
  - over distance (inversely proportional to distance squared)
  - over denser medium

Wave Characteristics



When wave travels from **less dense** to **more dense** medium

- Frequency stays the same (4 Hz in the above illustration)
- Speed increases (wavelength also increases)
- Amplitude decreases ⇒ Lower energy
  - Total energy is conserved
  - Energy loss is due to wave reflection by the more dense medium

Communication Modes in Wireless Network

- In Wireless Infrastructure Mode ⇒ like "Client-Server"
  - Wireless nodes do not talk to each other, they only communicate with the base station
  - Similar concept to "star topology"
- In Adhoc Network Mode ⇒ like "Peer-to-Peer"
  - No base stations
  - Wireless nodes talk to each other (within radius of coverage)
  - Examples:
    - BlueTooth: your laptop with (mouse|keyboard|headphone|earbud|...)
    - File transfer using AirDrop in MacOS
    - Laptop HotSpot connection to a smartphone

Taxonomy

	Single Hop	Multiple Hop
Infrastructure	Nodes connect to base station which connects to the Internet	Nodes may have to relay through several wireless nodes to connect to the Internet
Ad Hoc	No base station ⇒ No connection to larger Internet	No base station ⇒ No connection to larger Internet. May have to relay to reach other nodes

CDMA
Code Division Multiple Access

CDMA vs. (TDMA | FDMA)

	CDMA	FDMA/TDMA
Collision Free	Yes	Yes
Link Utilization	Nodes can use 100% link capacity	Nodes can use 1/N of link capacity

What do hear in this audio recording (of three languages)?

Simultaneous Transmission in Different "Languages"

- The audio recording contains the same message simultaneously spoken in three languages (English, German, Spanish)
- To English speakers: the message in German and Spanish are gibberish
  - Likewise for native speakers in German or Spanish
- "LDMA": *Language Division* Multiple Access
  - Send the message using words which ***make sense only for a particular recipient***
- CDMA: Code Division Multiple Access
  - Encode the message using a code which is *mathematically* make sense only for a particular recipient, but "gibberish"/meaningless for others
  - Concepts from orthogonal vectors

Hadamard/Walsh Matrix

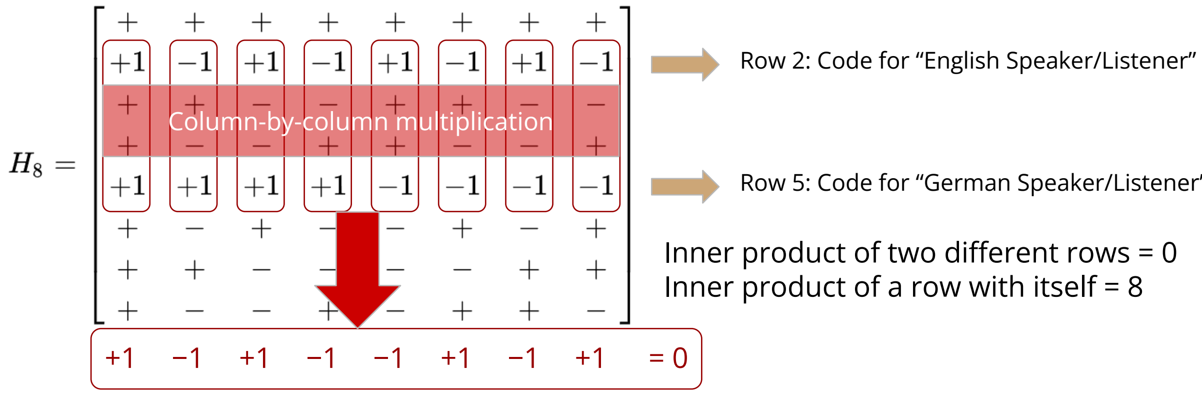
- Is a matrix of size 1x1, 2x2, 4x4, 8x8, ..., $2^k x 2^k$
- The entries are either −1 or +1
- Constructed recursively as follows:

$$H_1 = [1] \qquad H_{2n} = \begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix}$$

$$H_2 = \begin{bmatrix} + & + \\ + & - \end{bmatrix} \quad H_4 = \begin{bmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{bmatrix}$$

$$H_8 = \begin{bmatrix} + & + & + & + & + & + & + & + \\ + & - & + & - & + & - & + & - \\ + & + & - & - & + & + & - & - \\ + & - & - & + & + & - & - & + \\ + & + & + & + & - & - & - & - \\ + & - & + & - & - & + & - & + \\ + & + & - & - & - & - & + & + \\ + & - & - & + & - & + & + & - \end{bmatrix}$$

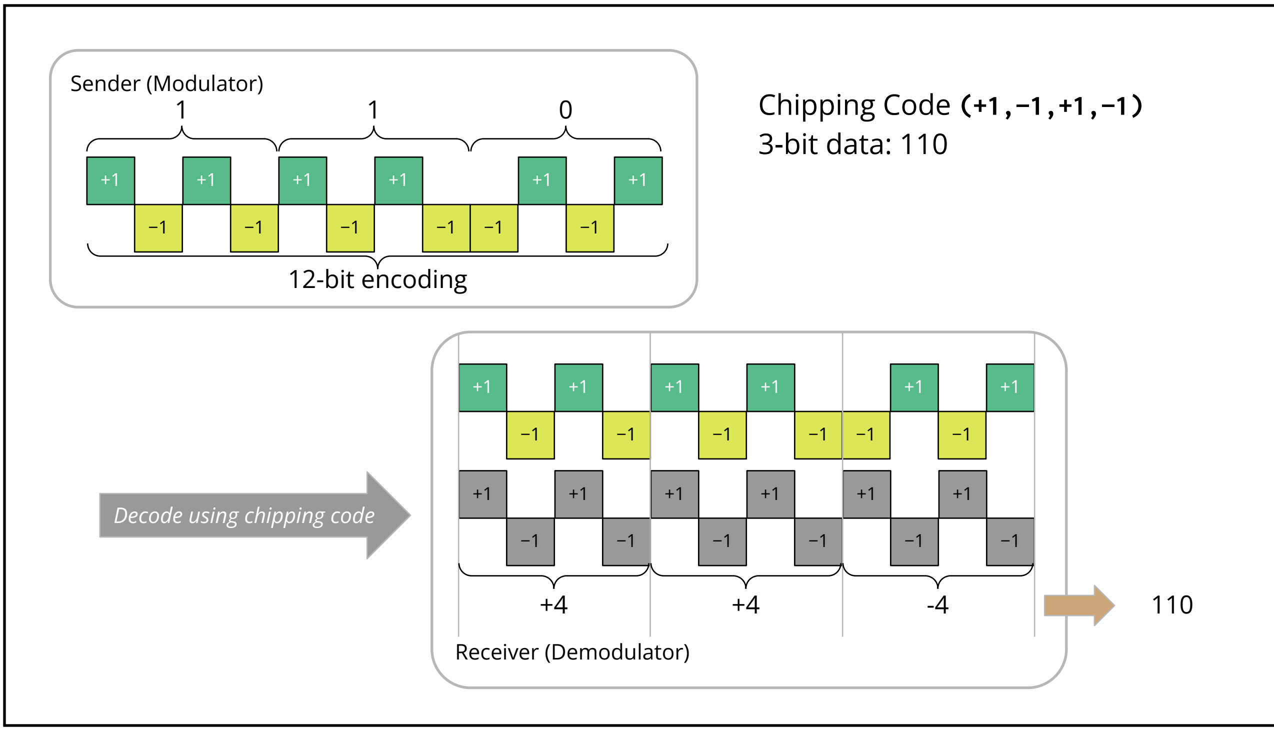
Orthogonal Rows in Hadamard Matrix

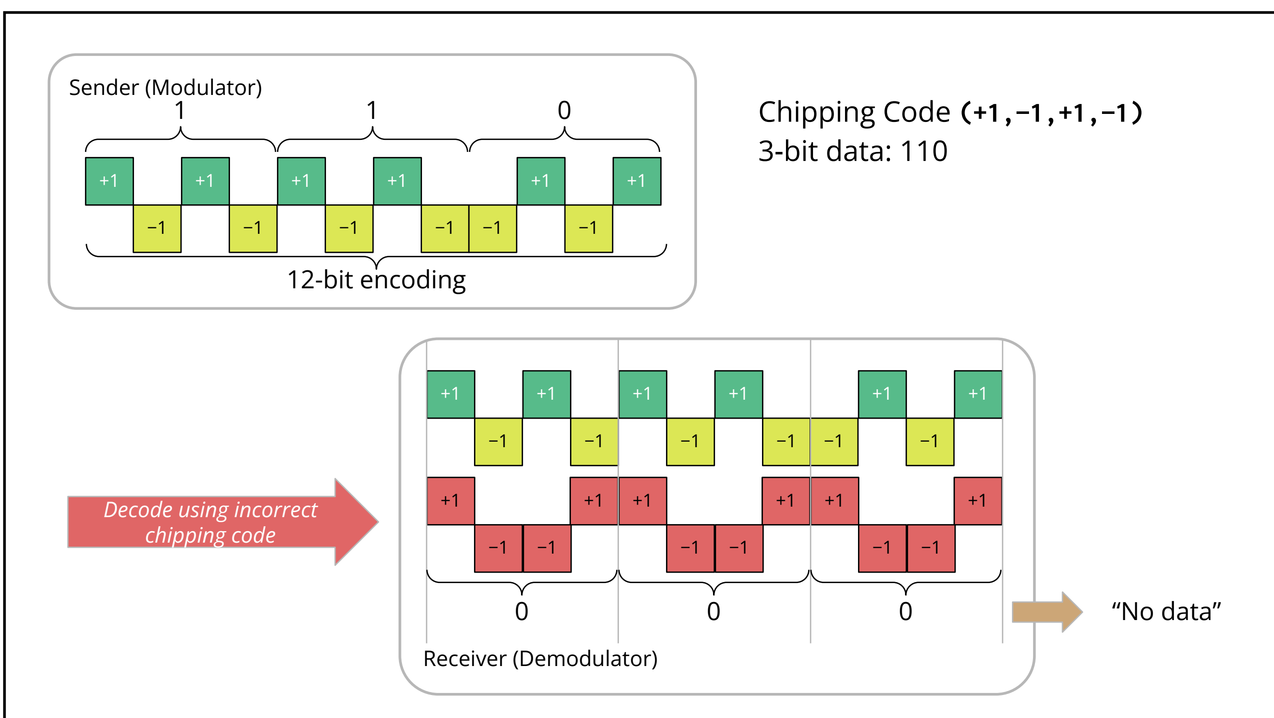


Inner product of two different rows = 0
Inner product of a row with itself = 8

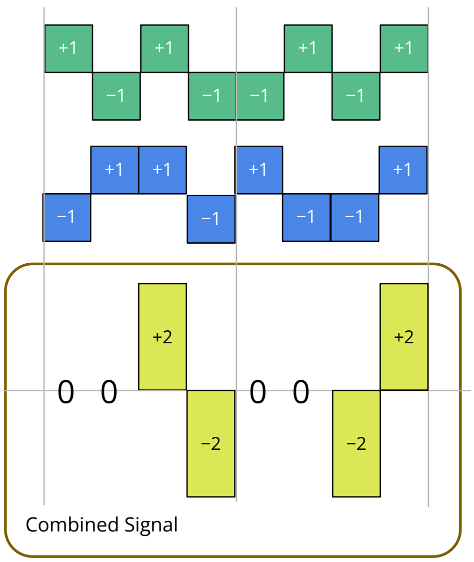
CDMA Data Encoding

- Each sender/recipient must agree on a common N-bit chipping code (C)
  - Taken from one of the rows in the Walsh/Hadamard matrix
- Bit encoding
  - Numeric value −1 represents binary digit 0
  - Numeric value +1 represents binary digit 1
- Each bit of data is encoded using a chipping (“spreading”) code (C)
  - Each bit of data is spread out into N-bit C
  - Bit value 1 is encoded as C
  - BIt value 0 is encoded as −C
  - Side effect: the frequency of the transmitted/encoded signal is N times higher than the original data)
  - Chipping rate is higher than data rate (or viewed from the other perspective: data rate is lower the the signal transmission rate)


Sender (Modulator)
1 1 0
+1 −1 +1 −1 +1 −1 +1 −1 −1 +1 −1 +1
12-bit encoding
Chipping Code (+1,−1,+1,−1)
3-bit data: 110
Decode using chipping code
+4 +4 -4
110
Receiver (Demodulator)


Sender (Modulator)
1 1 0
+1 −1 +1 −1 +1 −1 +1 −1 −1 +1 −1 +1
12-bit encoding
Chipping Code (+1,−1,+1,−1)
3-bit data: 110
Decode using incorrect chipping code
0 0 0
"No data"
Receiver (Demodulator)

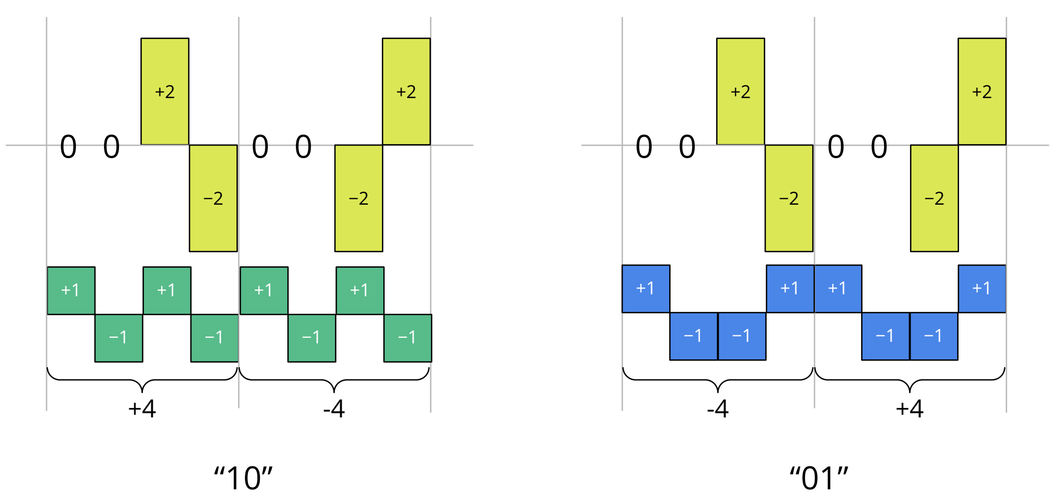
Simultaneous Transmissions by Two Senders



Data1: 10 Code1 **(+1,−1,+1,−1)**

Data2: 01 Code2 **(+1,−1,−1,+1)**

Decoding by Respective Receiver



Mathematical Magic: Orthogonal Vectors

Sender 1 Message $a_0 a_1 a_2 \ldots a_n$ Sender 1 Code : C_1

Sender 2 Message $b_0 b_1 b_2 \ldots b_n$ Sender 2 Code : C_2

$$S_1 = (a_0 C_1, a_1 C_1, a_2 C_1, \ldots, a_n C_1)$$

$$S_2 = (b_0 C_2, b_1 C_2, b_2 C_2, \ldots, b_n C_2)$$

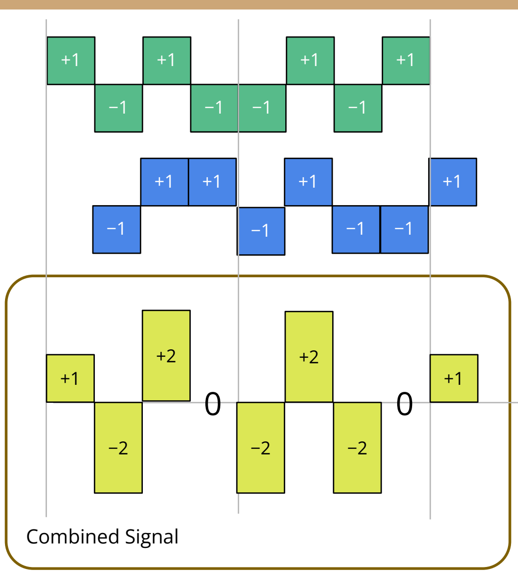
Combined signal

$$S_1 + S_2 = (a_0 C_1 + b_0 C_2, a_1 C_1 + b_1 C_2, \ldots, a_n C_1 + b_n C_2)$$

Decoded using C_1

$$\begin{aligned}(S_1 + S_2) \cdot C_1 &= (a_0 C_1 + b_0 C_2,\ a_1 C_1 + b_1 C_2,\ \ldots\ , a_n C_1 + b_n C_2) \cdot C_1 \\ &= (a_0 \underbrace{C_1 \cdot C_1}_{N} + b_0 \underbrace{C_2 \cdot C_1}_{0},\ a_1 C_1 \cdot C_1 + b_1 C_2 \cdot C_1,\ \ldots\ , a_n C_1 \cdot C_1 + b_n C_2 \cdot C_1) \\ &= (a_0 N, a_1 N, \ldots, a_n N) \\ &= (a_0, a_1, \ldots, a_n) N\end{aligned}$$

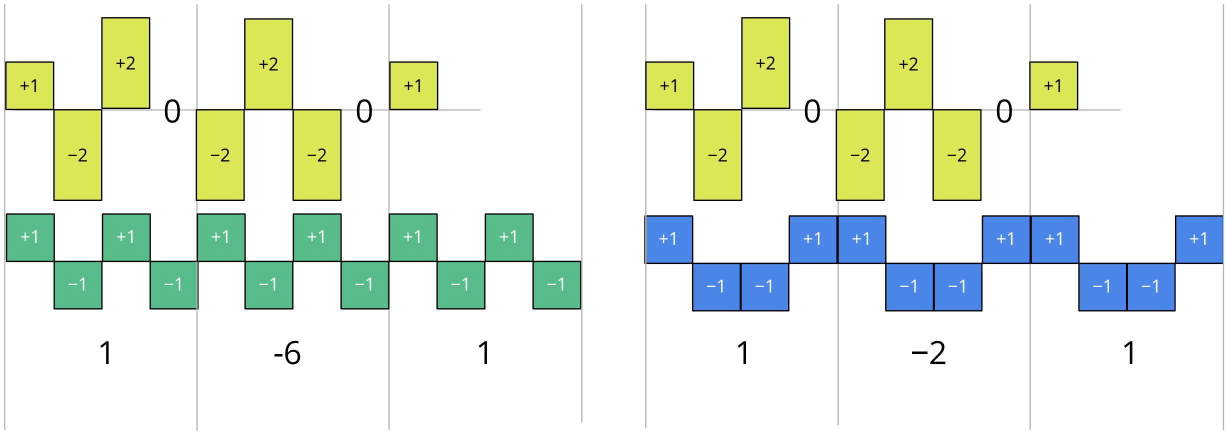
Out of Phase Transmissions by Two Senders



Code1 **(+1,−1,+1,−1)** Data1: 10

Code2 **(+1,−1,−1,+1)** Data2: 01

Decoding Out of Phase Combined Signal



The receiver(s) expect to get -4 or +4

Actual CDMA Implementation

- Use longer code bit
  - 4-bit in the example can only accommodate 16 different senders (receivers)
  - More robust to out-of-phase simultaneous transmissions
    - With 4-bit code, 1-bit shift amounts to 90-degree out of phase
    - With 128-bit code, 1-bit shift amounts only to less than 3-degree out of phase
- Our illustration assumes signal strengths from various users are the same
- The orthogonality principle requires synchronous transmission by all devices. In reality, it is hard to coordinate timing precisely
  - Use asynchronous CDMA, where ***codes are not fully orthogonal***, but ***almost orthogonal***
  - *Inner product of two N-bit user codes is NOT zero but very close to zero*

CDMA Implementations

Standard	Year	Chipping Code	Where Used?
IS-95 ("CDMA One")	1993 (Qualcomm)	64-bit Walsh code	2G Cellular
CDMA 2000	2000	multiple bit lengths (to accommodate different data rates)	2.5G and 3G

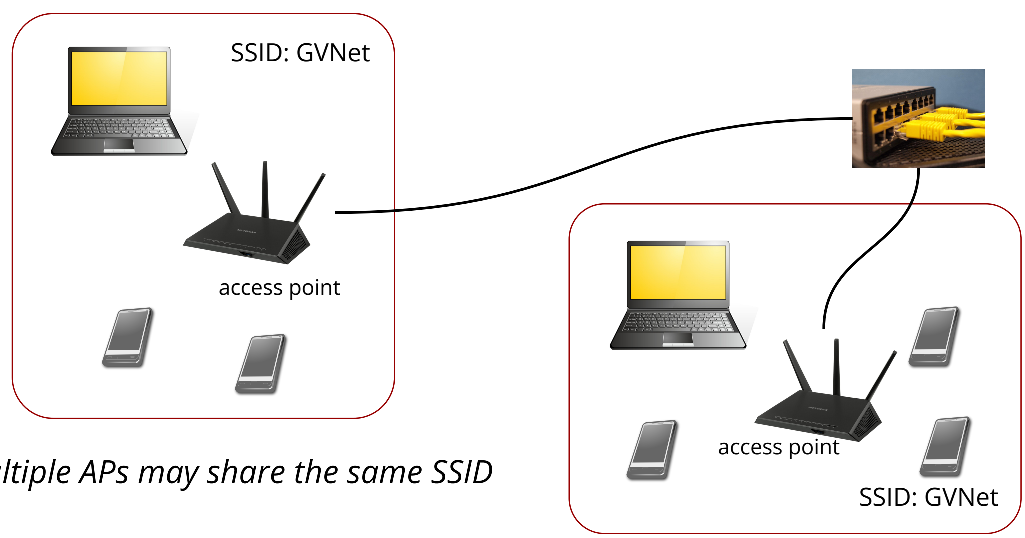
Wifi: IEEE 802.11

Standard	Year	Max Data Rate	Range	Frequency
802.11b	1999	11 Mbps	30 m	2.4 GHz
802.11 g	2003	54 Mbps		
802.11 n	2009	600 Mbps	70m	2.4GHz, 5 GHz
802.11 ac (WiFi 5)	2013	3.47 Gbps		5 GHz
802.11 af	2014	35-560 Mbps	1 km	54-790 MHz
802.11 ah	2017	347 Mbps		900 MHz
802.11 ax (WiFi 6)	2020	14 Gbps	70m	2.4GHz, 5GHz

Connecting to WiFi: Scan-Associate

- Access Points periodically send beacon frames containing
  - SSID = Service Set Identifier (may be shared across several APs)
  - MAC address (unique address per AP)
- Passive Scanning (requires less energy use)
  - A wireless device listens for incoming beacon frames and decide which one to connect/associate to
- Active Scanning (requires more energy use)
  - A wireless initiate a broadcast (request frame broadcast)
  - Then listen for incoming beacon frames
- Authentication (in Chapter 8)
- Configuration: DHCP to obtain IP address

Common Architecture



Multiple APs may share the same SSID

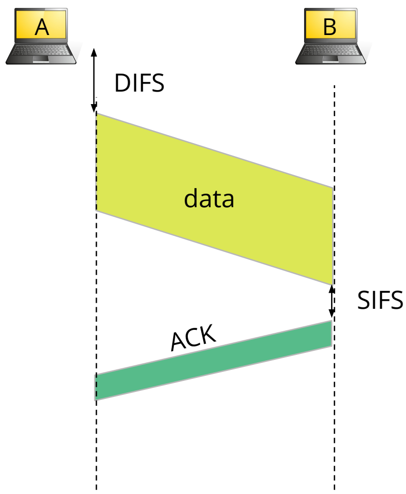
WiFi CSMA with Collision Avoidance

- On wireless connections, the strength of received signal is typically very small ⇒ more expensive hardware needed to detect collisions
- CSMA/CA works with link-layer ACKs
  - Upon receiving a non-corrupted frame (no collision), the receiving device waits from a short period of time (Short Inter-Frame Spacing) and then sends ACK
  - If after a timeout period, the sending node does not receive ACK, it retransmits
  - If after K attempts of retransmissions, no ACKs received, it will stop trying

CSMA/CD vs. CSMA/CA

	CSMA/CD	CSMA/CA
Send packet when channel is idle	Immediate	After DIFS delay
When channel is busy	Continue to listen	Binary Exponential Backoff Wait. Begin countdown after
What if collide?	Stop Transmitting	Not detected. Hence, continue transmitting
Wait for ACKs	No	Yes
Where	Wired connections	Wireless connections

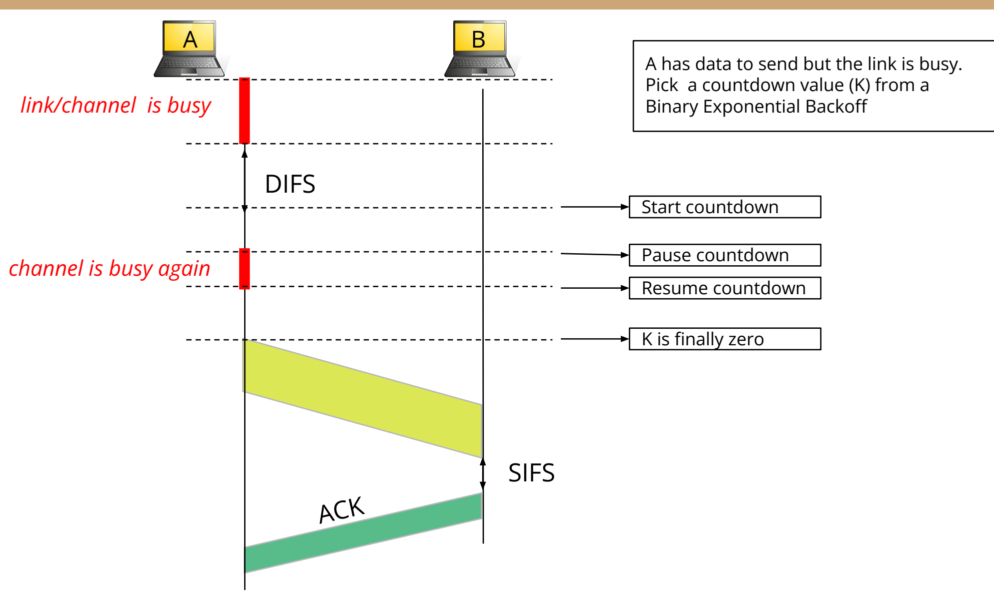
CSMA/CA: Sending Data When Link is Idle



DIFS = DCF Inter-Frame Spacing
DCF = Distributed Coordination Function
SIFS = Short Inter-Frame Spacing

If there is collision, B will not send ACK, causing A to (timeout and) retransmit.

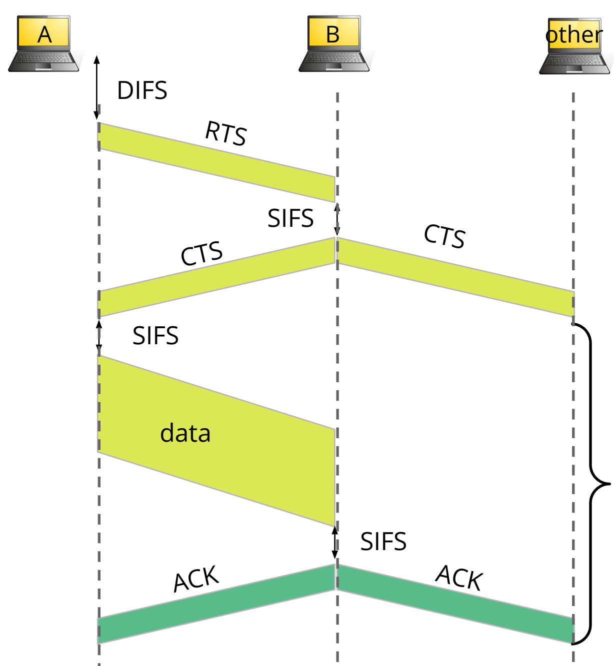
CSMA/CA: Sending Data When Link is Busy



CSMA/CA + Request To Send + Clear To Send

Pilot: "Request Permission to land"

Tower: "Clear to land"

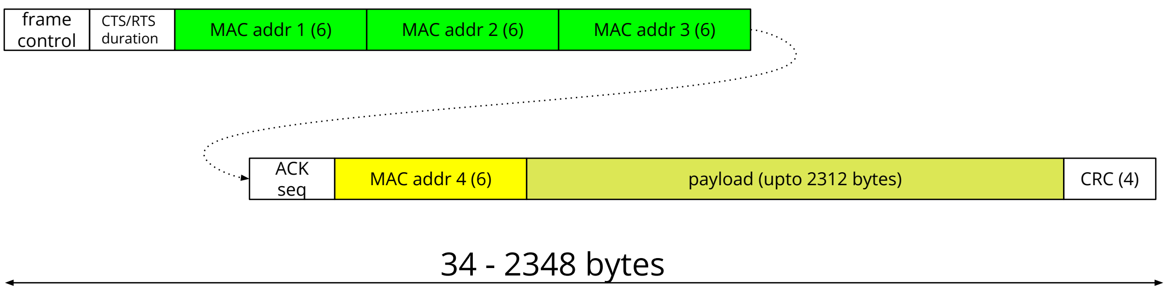


CSMA: Collision Avoidance between A & B

RTSs & CTSs from different hosts may collide but they are only a small packet. <u>Inexpensive</u> collision!

Only A & B are allowed to use the channel

802.11 Frame Format



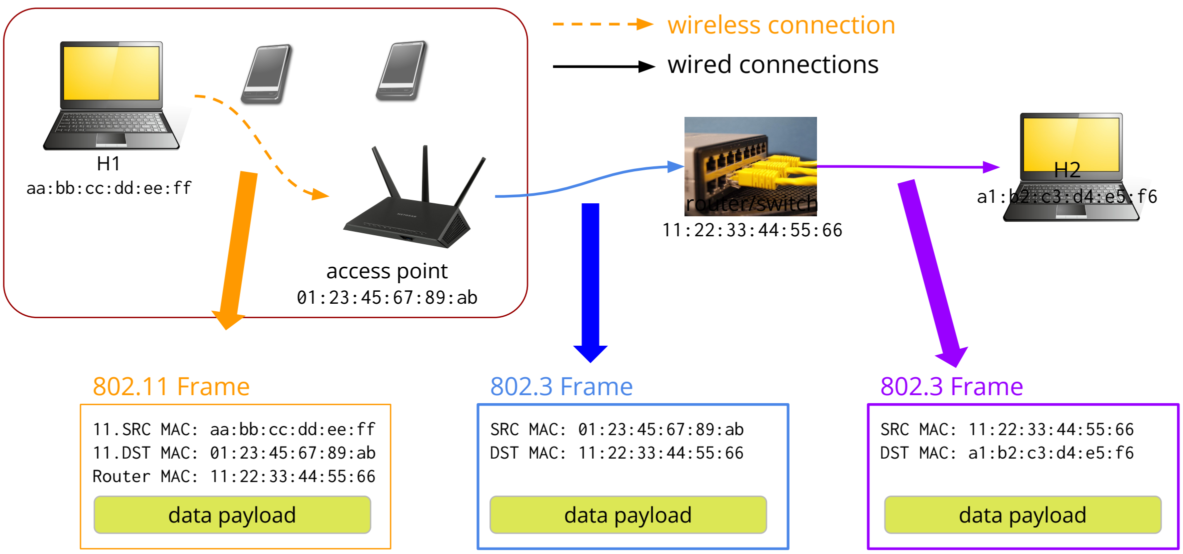
IEEE 802.11 Frame Format

Four address fields, three are important for “infrastructure mode” operations

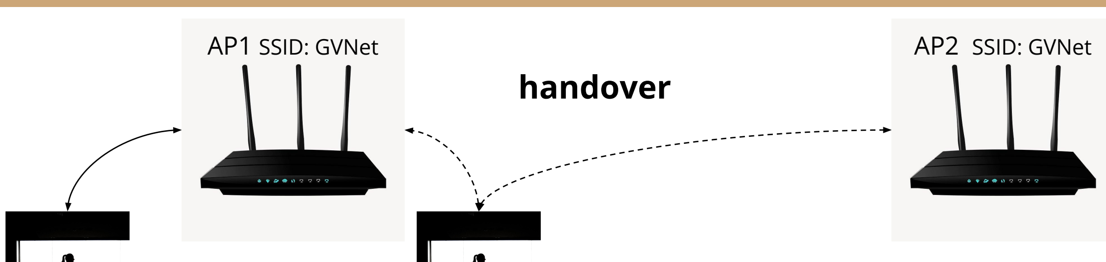
- MAC address #1 of **wireless** sender node or AP
- MAC address #2 of **wireless** recipient node or AP
- MAC address #3 of the router (**wired**) to which AP is attached (*subnet gateway addr*)
- MAC address #4 used only in ad hoc mode

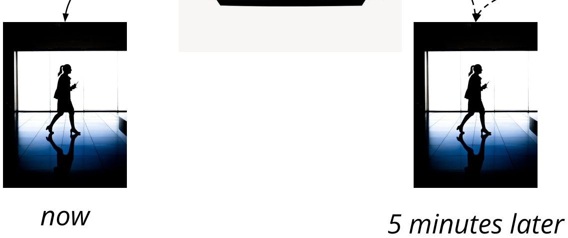
The wireless frame eventually has to go through a wired connection!!!

802.11 (wireless) and 802.3 (wired) Junctions



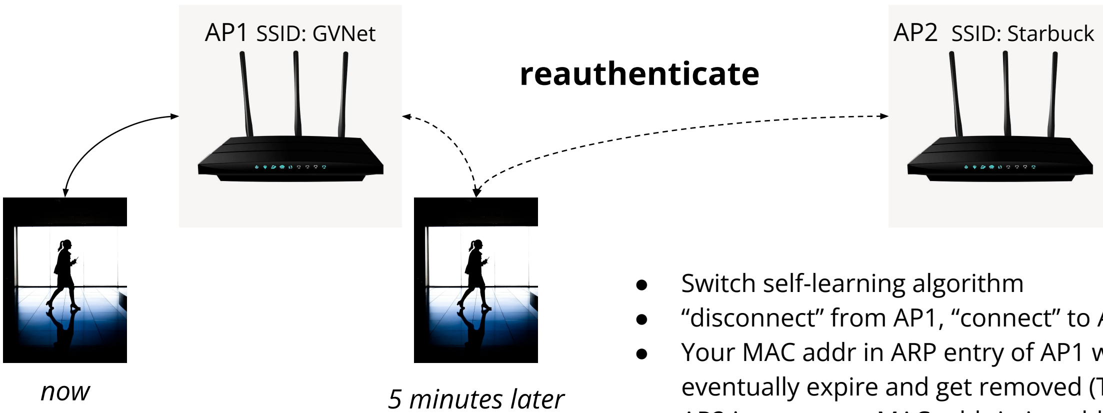
WiFi Handover Across Access Points (same Subnet)





- Switch Self-Learning algorithm naturally handles the hand-off
- “disconnect” from AP1, “connect” to AP2
- Your MAC addr in ARP entry of AP1 will eventually expire and get removed (TTL)
- AP2 inserts your MAC addr in its table

“Handover” Across Access Points (Different Subnets)



- Switch self-learning algorithm
- “disconnect” from AP1, “connect” to AP2
- Your MAC addr in ARP entry of AP1 will eventually expire and get removed (TTL)
- AP2 inserts your MAC addr in its table
- ***New authentication, new DHCP, etc.***

Cellular Networks: 4G and 5G

Cellular Technologies

- AMPS = Advanced Mobile Phone System
- GSM = Global System for Mobile Communications
- GPRS = General Packet Radio Service
- CDMA One
- CDMA 2000
- EV-DO = Evolution-Data Optimized
- EDGE = Enhanced Data Rates for GSM Evolution
- UMTS = Universal Mobile Telecommunications System
- DECT = Digital Enhanced Cordless Telecommunications
- Digital-AMPS = Advanced Mobile Phone System
- iDEN = Integrated Digital Enhanced Network

Major Differences between WiFi and Cellular

	WiFi	**Cellular**
Pay to connect	No	Yes
Device Identity	48-bit MAC Address 64-bit MAC Address (EUI)	Yes (64-bit IMEI/IMSI in SIM Card)
Authentication	Yes (and No)	User Subscription
Network Identity	SSID	Home Network / Foreign Network (Roaming)
Area of Coverage	Meters	Kilometers

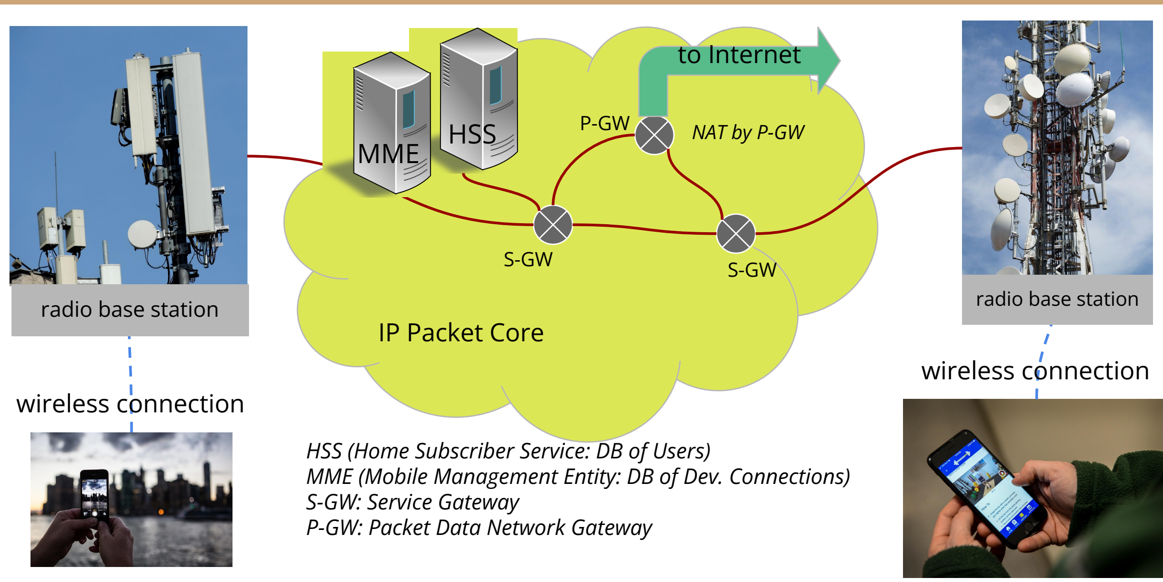
IMEI = International Mobile Equipment Identity
IMSI = International Mobile Subscriber Identity
EUI = Extended Unique Identifier

Cellular History

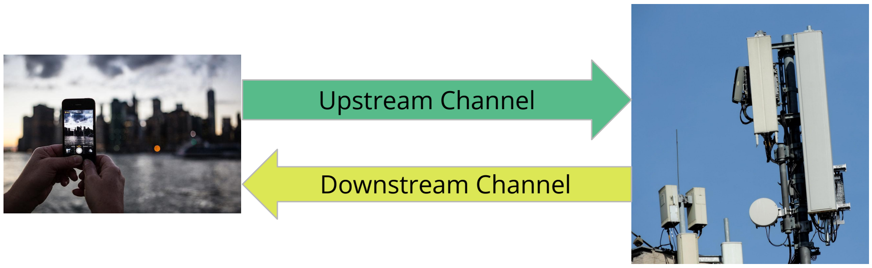
- 1G, 2G, 3G separate voice and data services
  - **Circuit switched network** for voice calls and text
  - **Packet switched network** for data
  - Cellular providers must maintain two separate networks
- 4G LTE and 5G handle all services as IP network

Generation	Commercial Name	Access Method
1G	AMPS	FDMA
2G	GSM, GPRS, EDGE	TDMA
3G	UMTS, EV-DO	CDMA, Wide-CDMA
4G	4G LTE	Orthogonal FDMA

4G LTE Cellular Network (of One Provider)



LTE Radio Access Network



- LTE Frequency Bands
- Orthogonal Frequency Division Multi Access (OFDM)
  - Combination of FDM and TDM
  - “Orthogonal” ⇒ frequency of neighboring channels are chosen to minimize interference
  - TDMA: 500 microseconds time slots

OFDM[A]

- Combines benefits of TDMA and FDMA
- Similar idea to CDMA but operates in the frequency domain
- FDM subdivides the communication link into N channels, each channel use a different (sub) frequency
- OFDM[A] = FDM where each sub frequency is an **integer multiple** of a **fundamental frequency**
- Stream of data bits are spliced into smaller group of bits, each group is encoded using a different frequency
- **Benefits**
  - Subchannels can be packed closer to each other while minimizing interference
  - Efficient implementation using Fast Fourier Transform

Fourier Transform (Fourier Series)

$$X(f) = \int_{-\infty}^{\infty} x(t)\, e^{-i2\pi f}\, dt$$

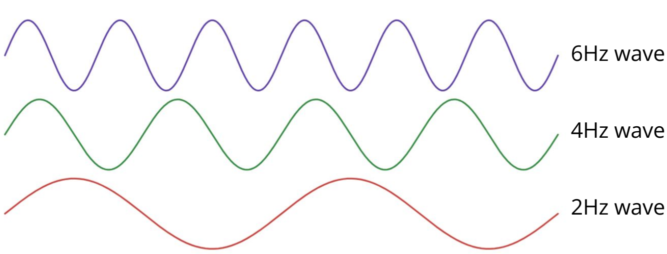
$x(t)$ function in time domain
$X(f)$ function in frequency domain

Joseph Fourier (1807): a function can be expressed as an infinite sum of sine and cosine functions of various frequencies

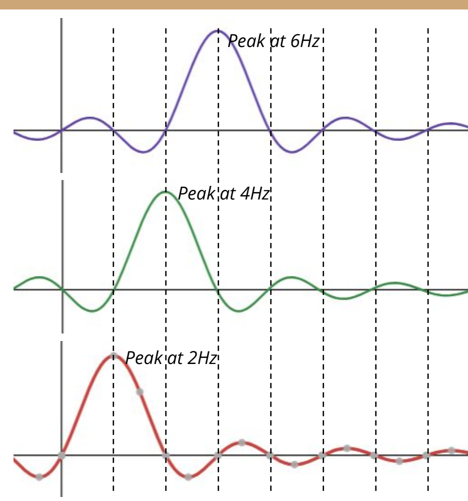
Moog synthesizer (1964)

3Blue1Brown: Drawing Joseph Fourier using Fourier Series

OFDMA: Multiple of Fundamental Frequency



Finite Signals in Time Domain

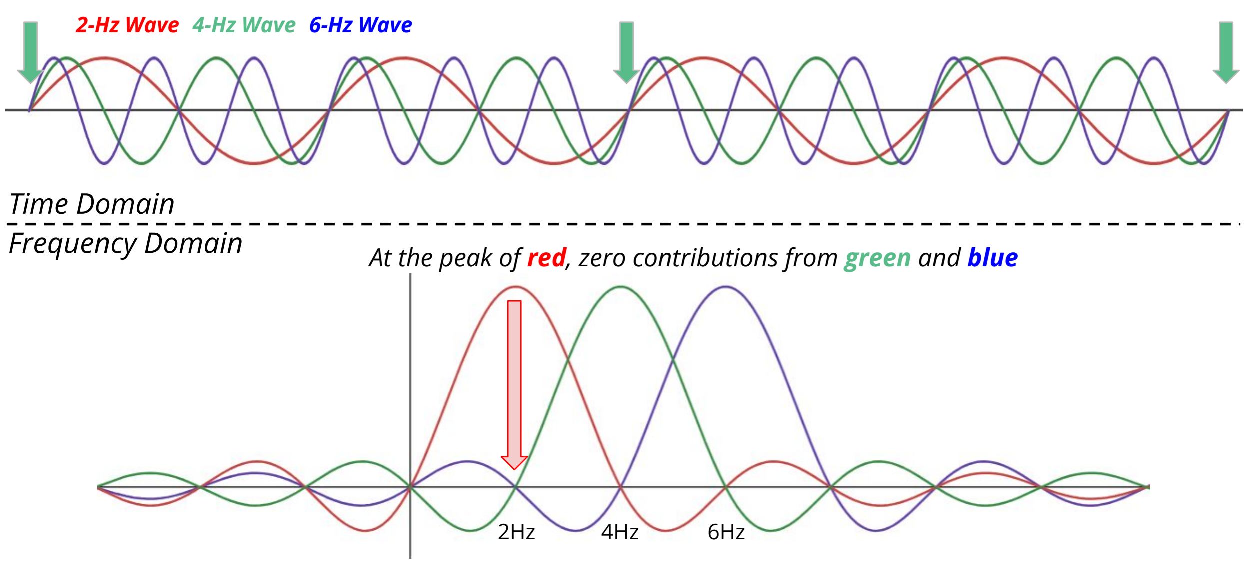


Frequency Spectrum

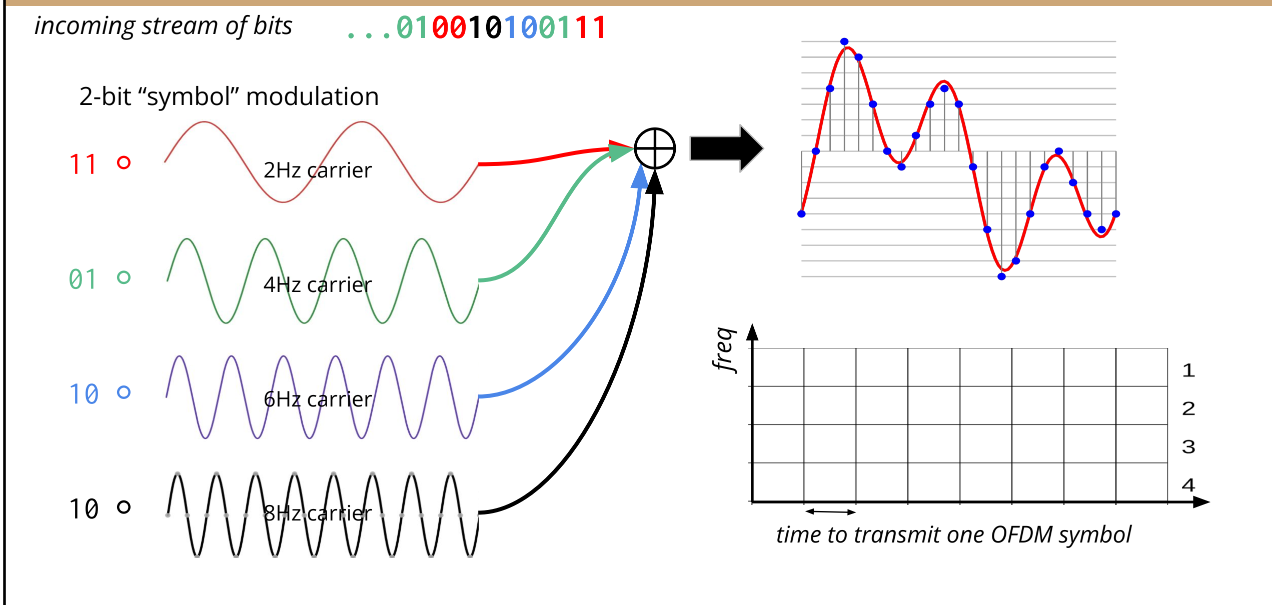
Live Demo:

Online Pitch Detector

OFDMA: Multiple of Fundamental Frequency



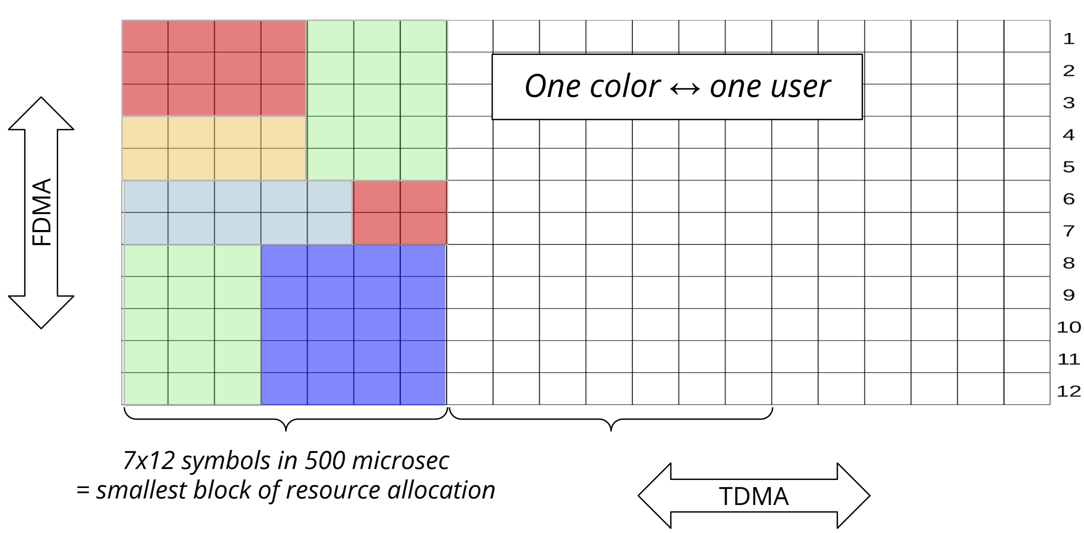
OFDMA Data Encoding / Modulation



LTE OFDMA Implementation

- 12 sub channels, each sub frequency is a multiple of 15 KHz (F_c)
  - 15KHz, 30 KHz, 45 KHz, …
- Duration of symbols is $1/F_c$ seconds = 66.67 microseconds
  - Resistant to relatively long multipath propagation delay
  - For instance, 6 microseconds (1.8 kilometers) contributes only to 10% time shift
  - **7 symbols (per channel) can be transmitted in a 500-millisecond block**
  - 7x12 symbols can be transmitted in a 500-millisecond block across all 12 channels

LTE OFDMA Implementation



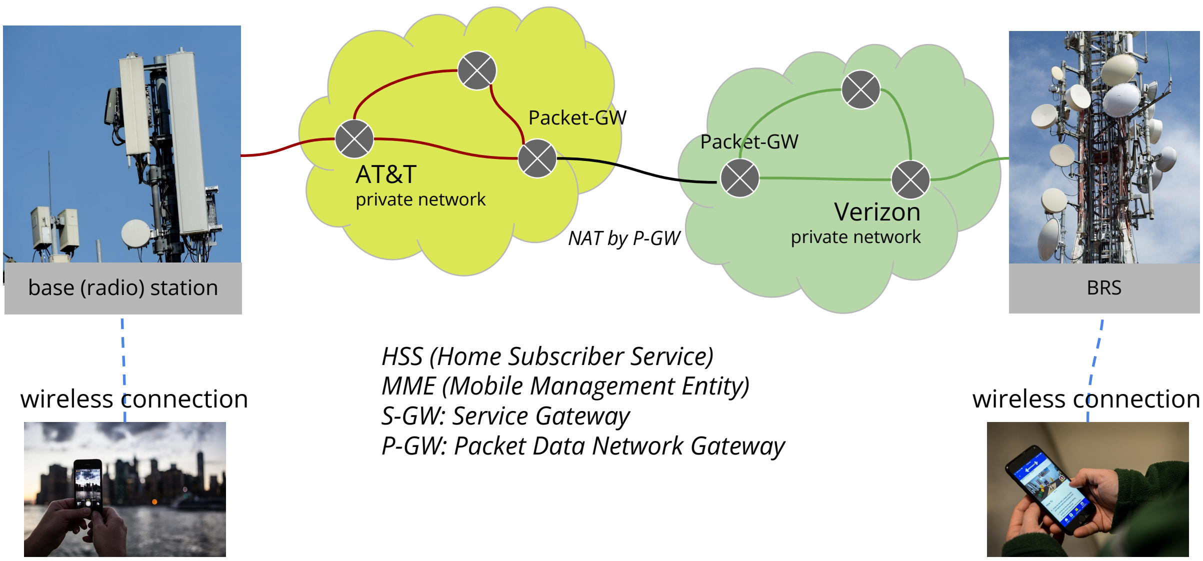
Specialized "Servers" in 4G LTE Network

- Mobility Management Entity ("Mobility Management Service")
  - Manages **live data of the connections**
  - Authentication: Device-to-Network, Network-to-Device
  - Device handover between cells
  - Path setup (tunneling) from mobile device to Packet-Gateway
  - Tracking device location ⇒ *Has been used as Forensic Evidence in Criminal cases*
- Home Subscriber Service
  - Manages **static data of the subscribers**
  - DB of mobile subscribers
    - Billing info
    - Plan details (data limit, text/voice limits, etc.)

Specialized Routers in 4G LTE Network

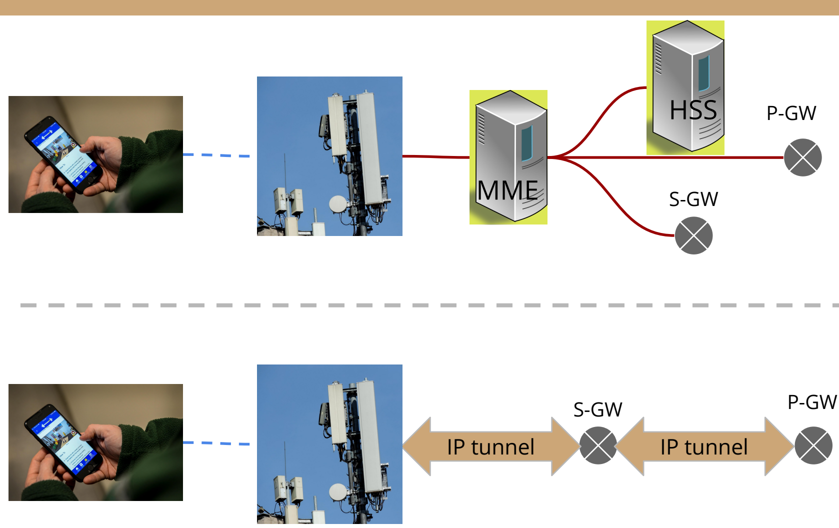
- Service Gateway (S-GW)
  - Entry point from the base station to the Packet Core
- Packet Data Network Gateway (P-GW)
  - "Outgoing" gateway
  - The last LTE element that pushes IP datagram from a mobile device to the Internet
  - Provide Network Address Translation Services
    - Most providers use private IP address within their "home network"

4G LTE Cellular Network (Cross Providers)



HSS (Home Subscriber Service)
MME (Mobile Management Entity)
S-GW: Service Gateway
P-GW: Packet Data Network Gateway

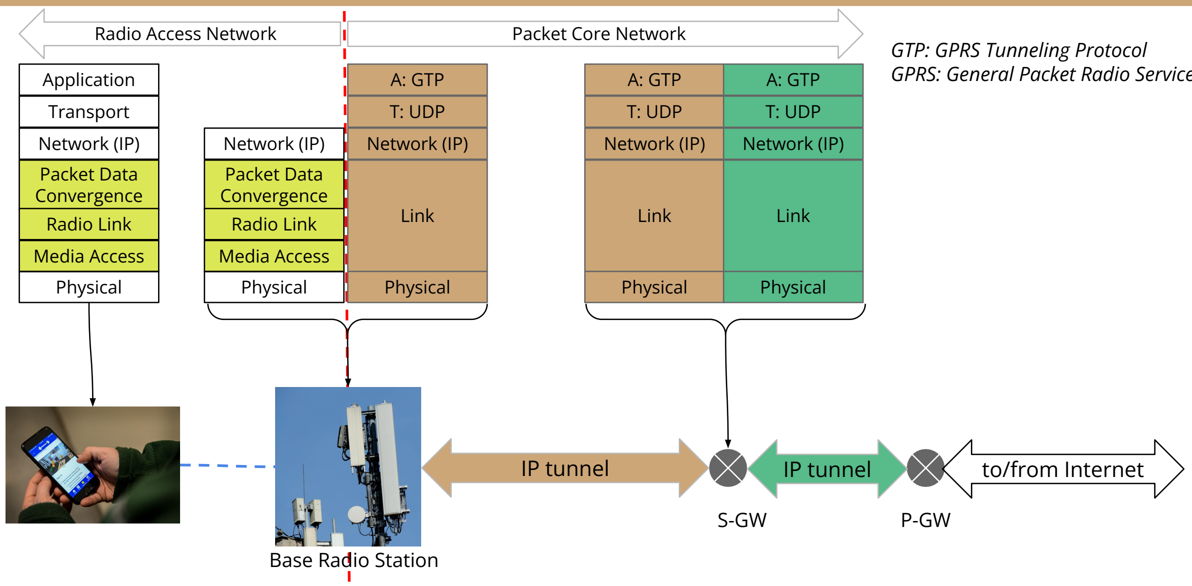
Cellular Control Plane & Data Plane



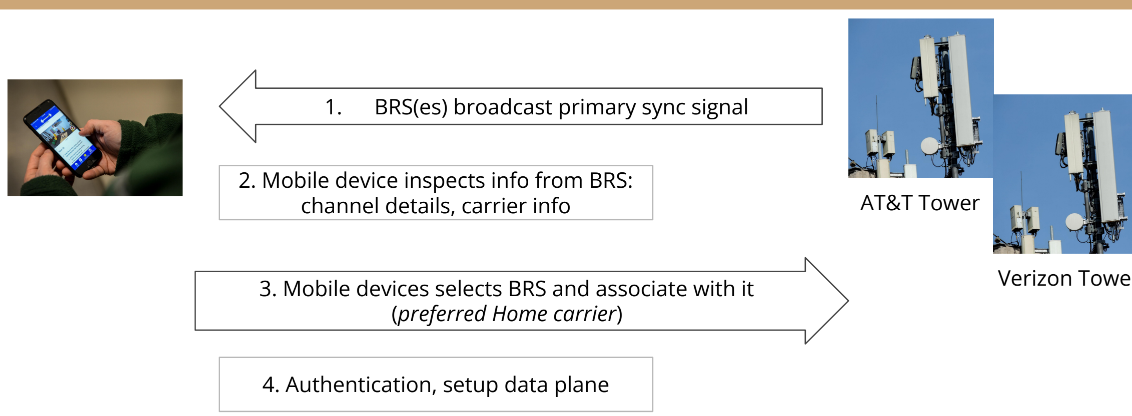
Control Plane: authentication, security, mobility management

Data Plane relies on *IP tunnels* for transporting mobile IP payload over wired IP core

LTE Data Plane Protocol Stack



Associating with a Base Radio Station

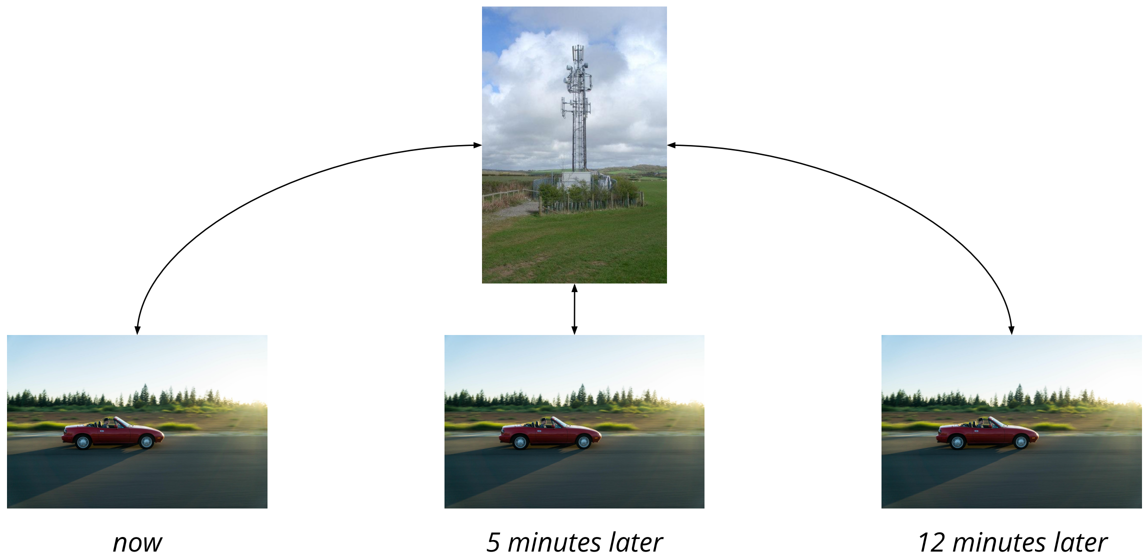


4G LTE vs. 5G

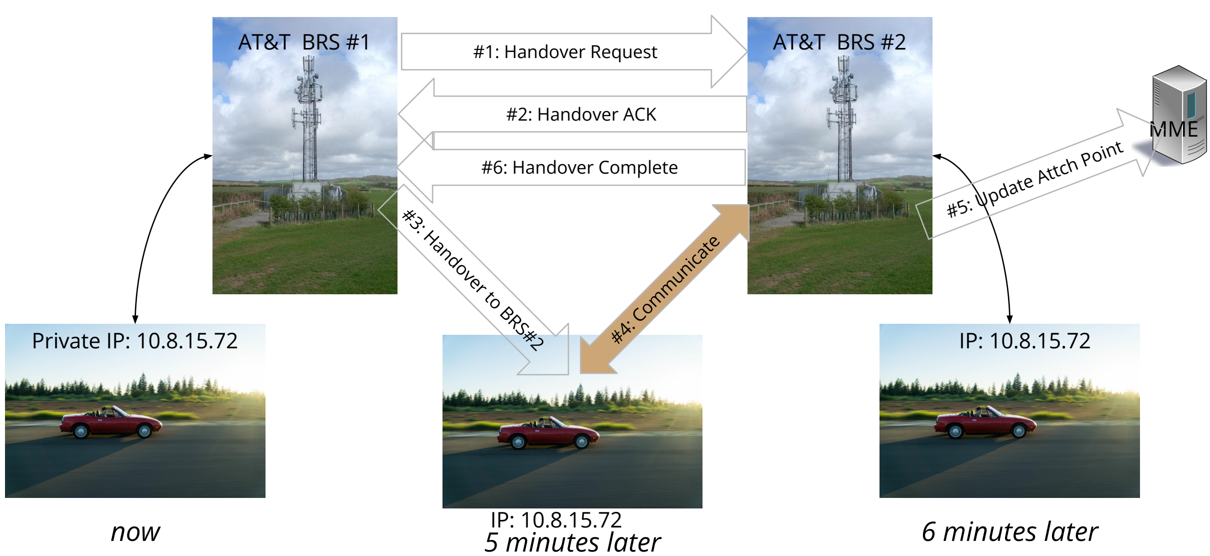
	4G LTE	5G
Frequency Band(s)	< 6 GHz	low band: < 1GHz medium band: 1-2.6 GHz, 3.5-6 GHz high band: 24-40 GHz (millimeter waves)
Data rate	lower	higher
Coverage	longer distance (kilometers)	shorter distance (10-100m)
Cellular structure	Less dense cells	More dense “pico cells”

User/Device Mobility

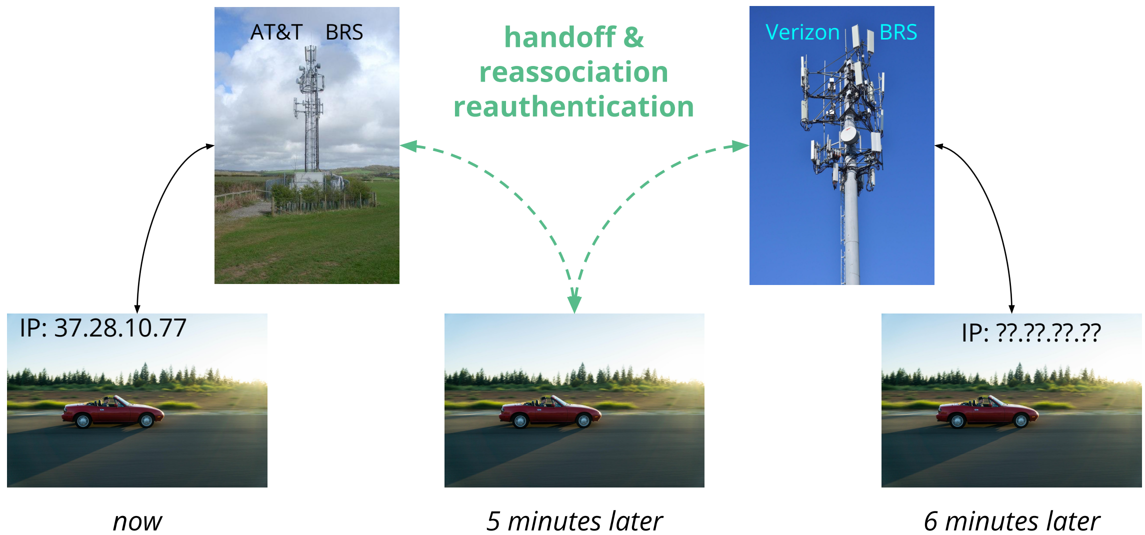
Low Mobility: Stay Connection to One BRS



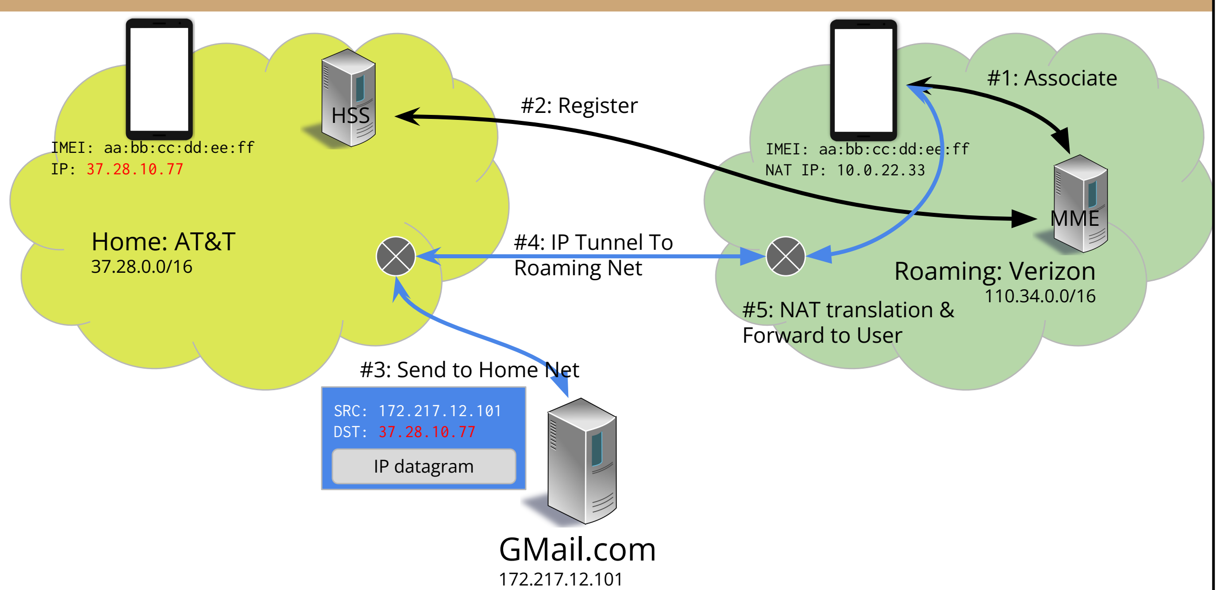
Medium Mobility: Stay Within One Provider



High Mobility: Across Multiple Providers



High Mobility: Indirect Routing



High Mobility: Direct Routing