PHY FUNDAMENTALS II

Wireless Signal Propagation

©2020 Mahbub Hassan

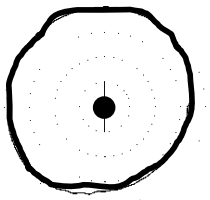
Overview

1. Antenna
2. Reflection, Diffraction, Scattering
3. Fading, Shadowing, Multipath
4. Inter-symbol Interference
5. Path loss model (Frii's, 2-ray)
6. MIMO (Diversity, Multiplexing, Beamforming)
7. Orthogonal Frequency Division Multiplexing (OFDM)
8. Orthogonal Frequency Division Multiple Access (OFDMA)
9. Effect of Frequency

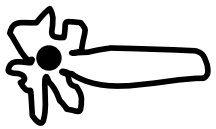
©2020 Mahbub Hassan

Antenna

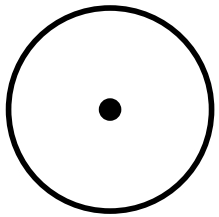
- Transmitter converts electrical energy to electromagnetic waves
- Receiver converts electromagnetic waves to electrical energy
- Same antenna is used for transmission and reception
- Omni-Directional: Power radiated in all directions
- Directional: Most power in the desired direction
- Isotropic antenna: Radiates in all directions *equally*
- Antenna Gain = Power at particular point/Power with Isotropic
  Expressed in dBi ("decibel relative to isotropic")



Omni-Directional



Directional



Isotropic

©2020 Mahbub Hassan

Example

Question: How much stronger a 17 dBi antenna effectively receives (transmits) the signal compared to the isotropic antenna?

Solution

Let

Power of isotropic antenna = P_{iso}

Power of 17 dBi antenna = P

We have

$17 = 10\log_{10}(P/P_{iso})$

Thus $P/P_{iso} = 10^{1.7} = 50.12$, i.e., the 17 dBi antenna will *effectively* receive (transmit) the signal 50.12 times stronger than the isotropic antenna albeit using the same *actual* transmit power.

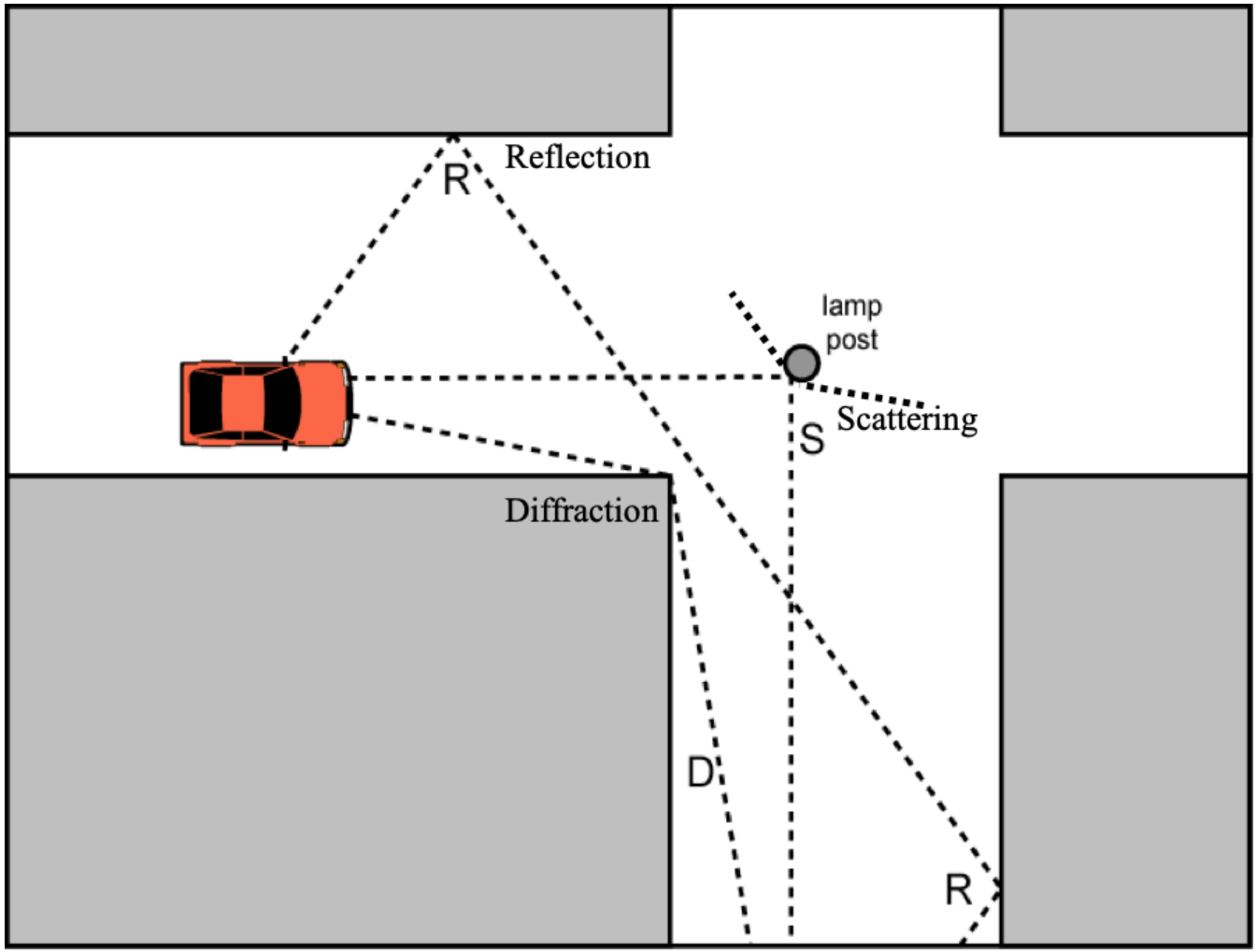
©2020 Mahbub Hassan

Relationship between antenna size and frequency

- Antennas are designed to transmit or receive a specific frequency band
  - Cannot use a TV antenna for wireless router, or vice-versa (why?)
- End-to-end antenna length = ½ wavelength
  - So that electrons can travel back and forth the antenna in one cycle
- If dipole (two rods), each rod is ¼ wavelength

©2020 Mahbub Hassan

Reflection, Diffraction, Scattering



©2020 Mahbub Hassan

Reflection, Diffraction and Scattering (Cont)

- **Reflection**: Surface large relative to wavelength (λ) of signal
  - May have phase shift from original
  - May cancel out original signal or increase/strengthen it at receiver
- **Diffraction**: Edge of impenetrable body; large relative to λ
  - Receiver may receive signal even if no line-of-sight (LOS) to transmitter
- **Scattering**
  - Obstacle size on order of wavelength. Lamp posts etc.
  - Reflection/diffraction are more directional; scattering in many directions
- If LOS, diffracted and scattered signals not significant (LOS dominates)
  - Reflected signals may be significant
- If no LOS, diffraction and scattering are primary means of reception

©2020 Mahbub Hassan

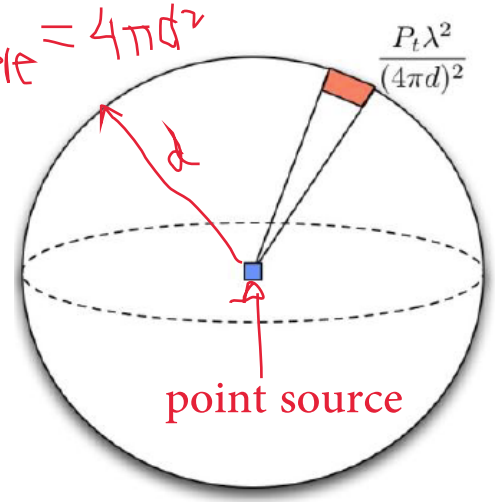
Path Loss

- Received power (P_R) at a particular location is only a fraction of the total power used by the transmitter to transmit the signal (P_T)
- Path loss = $P_T - P_R$
  - Depends on distance/separation between Tx-Rx
- Need to estimate path loss to design wireless links
- How to estimate path loss?
- There are well-known path loss models
  - Frii's model: designed for free-space (no reflections); frequency dependent
  - 2-Ray model: reflections considered, but frequency-independent (antenna heights are important)

©2020 Mahbub Hassan

Free Space Path Loss (Frii's Law)

$A_{sphere} = 4\pi d^2$



- Power density at shpere surface = $\frac{P_T}{4\pi d^2}$

$A_{ant} = \frac{\lambda^2}{4\pi}$

- Tx and Rx placed in *empty space*
  - No absorbing/reflecting obstacles
- Received power (P_R) decreases as *inverse square of distance (d^{-2} law)*

$$P_R = P_T G_T G_R \left(\frac{\lambda}{4\pi d}\right)^2$$

  - *Where G_T= Tx antenna gain, G_R = Rx antenna gain*
  - *For isotropic antennas, G_T=G_R=1 ("unit gain antennas" or 0 dBi)*

- For isotropic antennas: $P_R = P_T\left(\frac{c}{4\pi df}\right)^2$

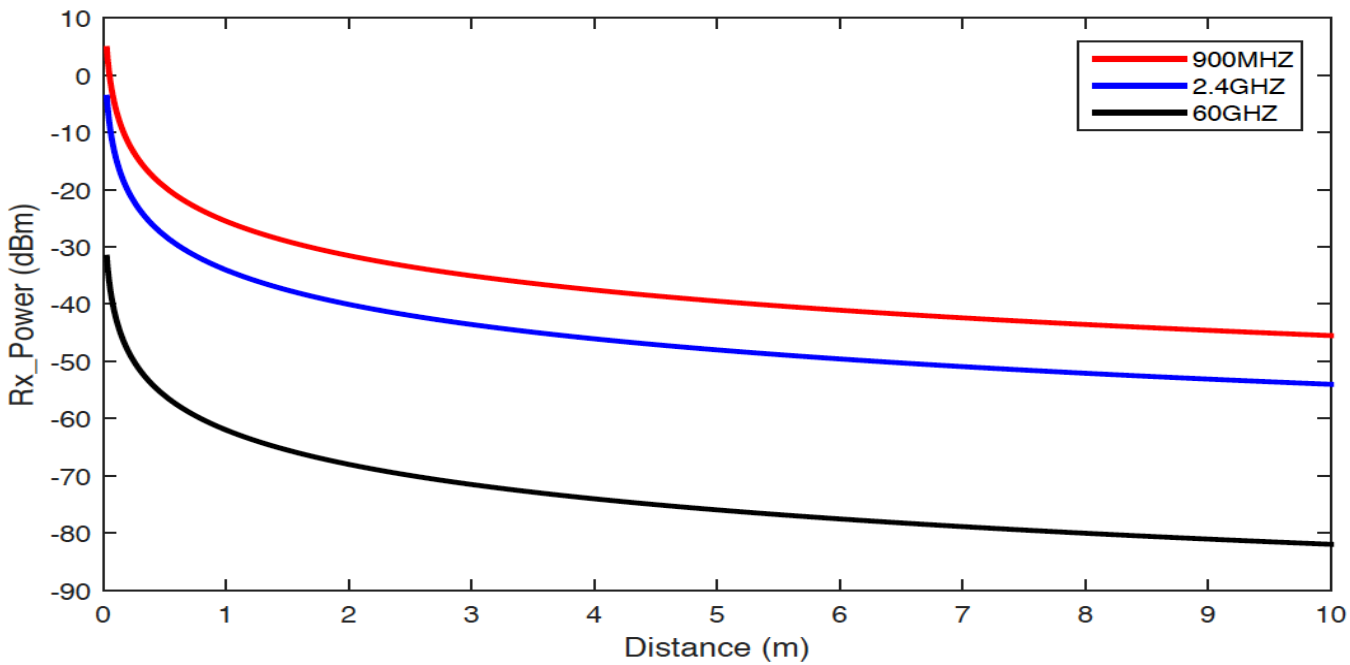
P_R = Power density x A_{ant}

©2020 Mahbub Hassan

Free-space path loss (cont)

- A factor of 10 increase in distance → 20dB more path loss (20dB/decade)
  - 2.4 GHz path loss at 1 meter = 40.04dB, 10 meter = 60.04dB
- The higher the frequency, the greater the path loss at fixed distance
  - At 10 meter, 2.4GHz = 60.04dB, 5GHz = 67.25dB

20dB diff



©2020 Mahbub Hassan

Example

Question: If 50W power is applied to a 900 MHz frequency at a transmitter, find the receive power at a distance of 100 meter from the transmitter (assume free space path loss with unit antenna gains).

huge power loss!!

Solution

Unit antenna gain means: G_T=G_R=1.

We have d=100m, f=900x10^6 Hz, P_T=50W, c=3x10^8 m/sec, and $\pi = 3.14$

$$P_R = P_T \left(\frac{c}{4\pi f d}\right)^2 = 3.5\mu W$$

linear formula

©2020 Mahbub Hassan

Example

Question: What is the received power in dBm at 10 meter from a 2.4GHz WiFi router transmitting with 100mW of power (assume free space path loss and isotropic antennas).

Solution

For isotropic antennas: G_T=G_R=0dBm.

We have d=10m, f=2.4x10^9 Hz, P_T=100mW=20dBm, c=3x10^8 m/sec, and $\pi = 3.14$

log formula

$$Pathloss(dB) = 20log_{10}\left(\frac{4\pi f d}{c}\right) dB = 40\ dB \text{ (approx.)}$$

From π & c

Or, we can use the other path loss expression as follows:

$$\mathrm{PL_{dB}} = 20log_{10}(d) + 20log_{10}(f) - 147.55 = 40 \text{ dB (approx.)}$$

100 mW = 20 dBm

$$P_R = P_T - pathloss = 20 - 40 = -20dBm \text{ (approx.)}$$

©2020 Mahbub Hassan

Receiver Sensitivity

- The received power (received signal strength or RSS) has to be greater than a threshold for the receiver to decode information correctly (with low error probability)
  - To achieve a minimum signal-to-noise ratio (SNR)
- Different hardware/standard/equipment specify different values
  - Depends on channel bandwidth and receiver noise figure (and temperature)
  - Larger bandwidth → larger minimum power (and vice versa)
  - Larger receiver noise → larger minimum power (and vice versa)
- Examples (for room temperature)
  - LTE: -52 dBm [roughly]
  - Bluetooth: -70 dBm [roughly]

©2020 Mahbub Hassan

Example

- To increase the coverage with low transmit power, a manufacturer produced Bluetooth chipsets with a receiver sensitivity of -80 dBm. What is the maximum communication range that could be achieved for this chipset for a transmit power of 1 mW? Assume Free Space Path Loss with unit antenna gains.

Bluetooth frequency f = 2.4 GHz, P_T= 1 mW, P_R=-80 dBm=10^{-8} mW

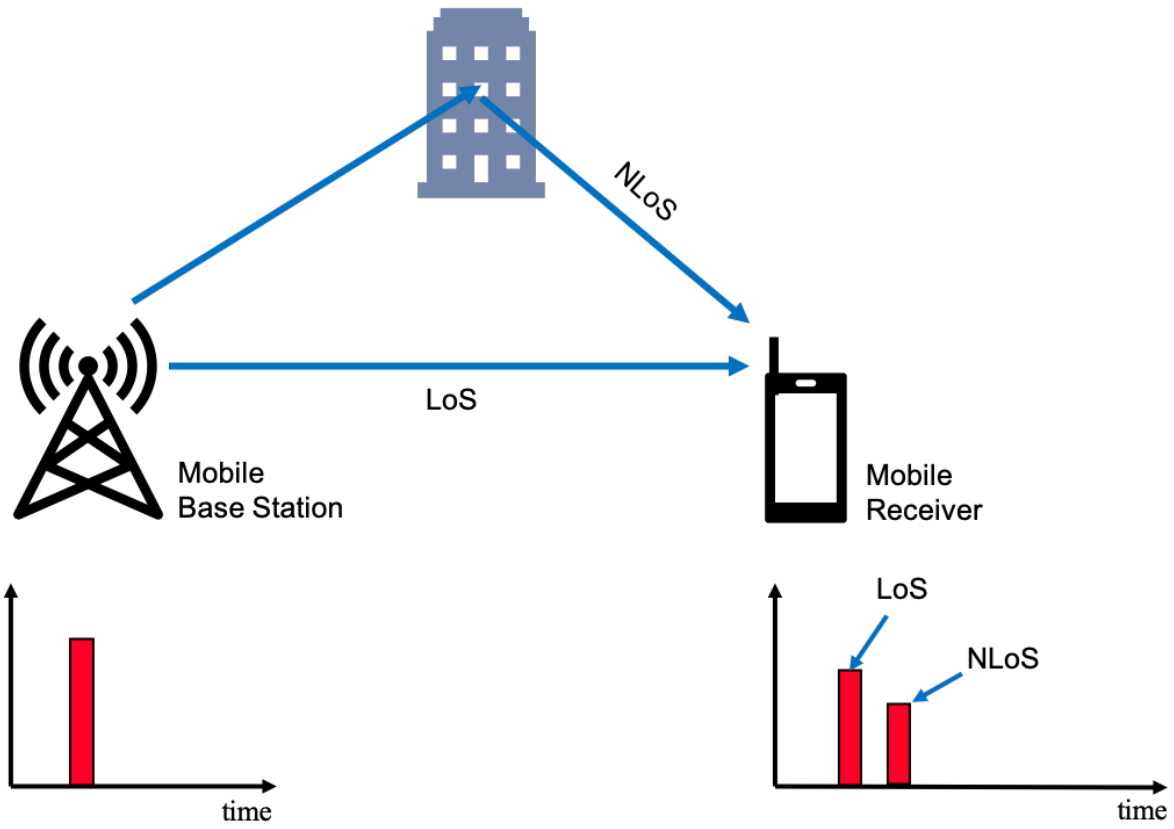
We have $$P_R = P_T\left(\frac{c}{4\pi d f}\right)^2$$

Or, $$d = \frac{c}{4\pi f}\sqrt{P_T / P_R}$$

= 99.5 meter

©2020 Mahbub Hassan

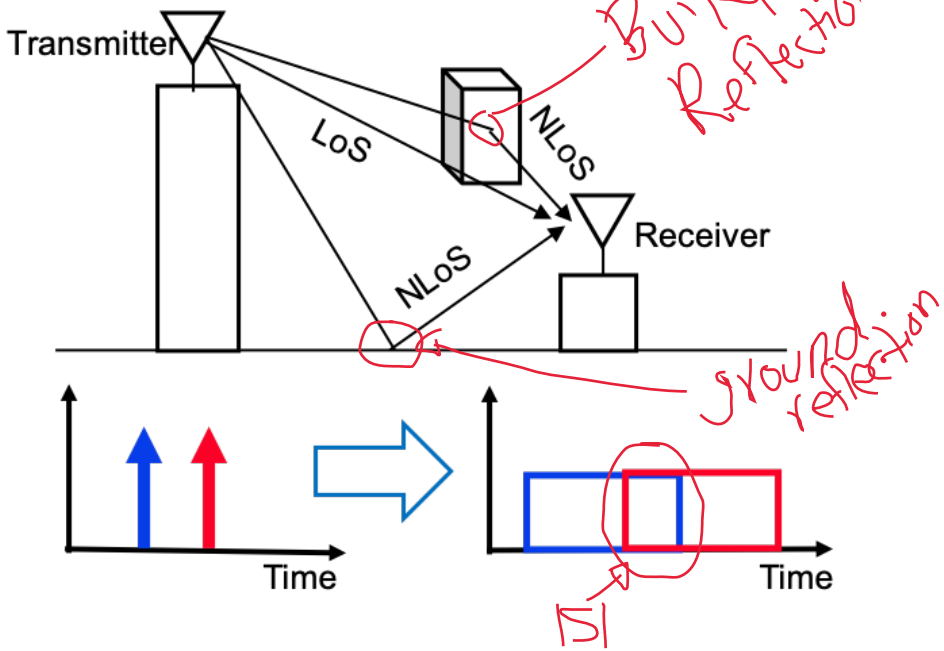
Multipath



- Multiple copies of the signal received (LoS+reflected NLoS)
- The LoS signal reaches the receiver first followed by the NLoS copy (NLoS has longer path length compared to the LoS path)
- RSS(LoS) > RSS(NLoS). NLoS signal travels further and hence attenuates more compared to the LoS.

©2020 Mahbub Hassan

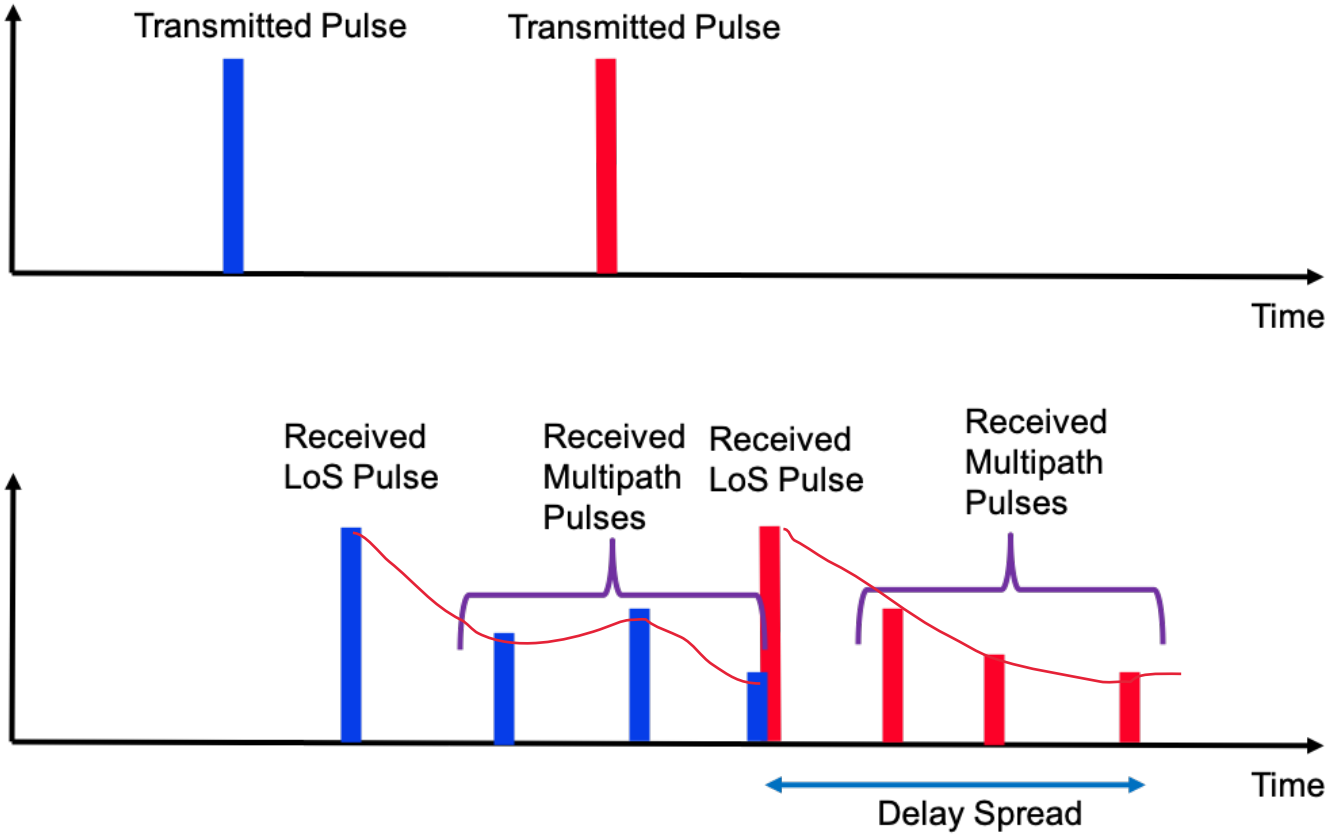
Inter-Symbol Interference



- Multipath effect: receiver continues to receive the signal (its reflections) even after the transmitter completes symbol transmission
- As a result, symbols become wider; two consecutively transmitted symbols overlap and interfere with each other
- Longer bit intervals or symbol lengths are required to avoid ISI
  - Limits the number of bits/s (data rate *inverse* of symbol length)

©2020 Mahbub Hassan

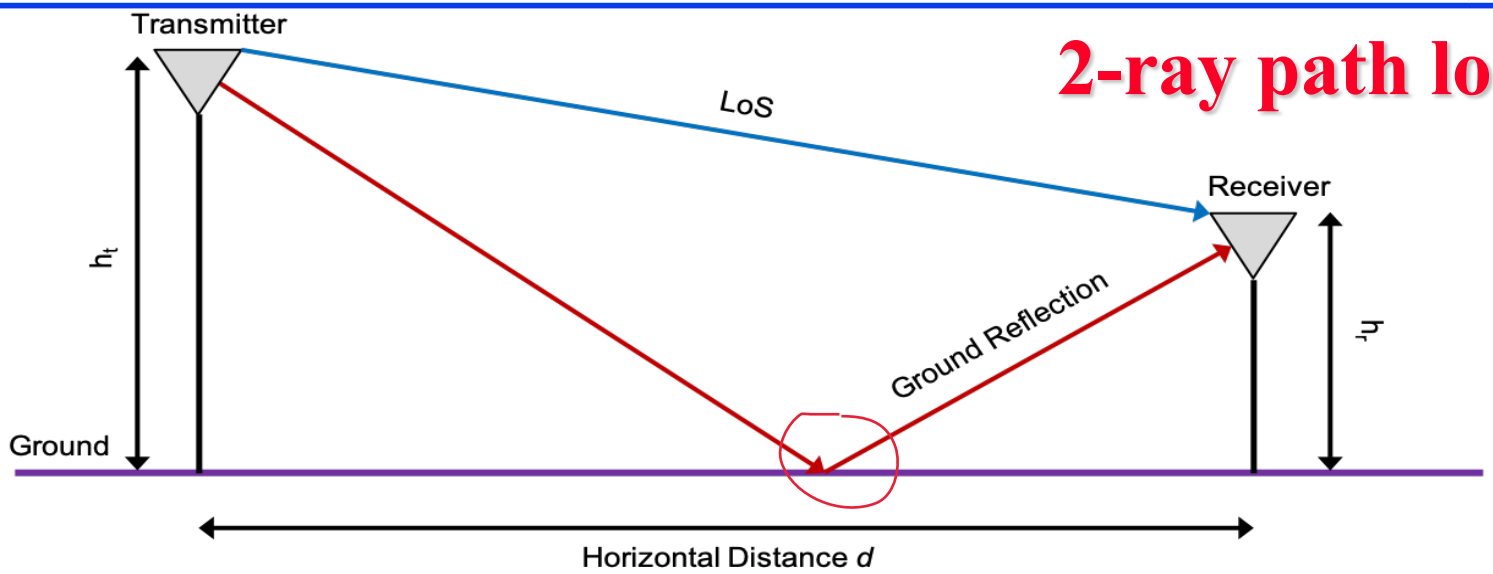
Delay Spread



- How long to wait to avoid ISI?
- RSS of late arrivals fluctuate, but consistently diminish on average
- Delay Spread = Time between the first (LoS) and the last copy of NLoS
  - RSS(last copy of NLoS) < $RSS_{threshold}$ (so next symbol can still be decoded)

©2020 Mahbub Hassan

2-ray path loss model



$$P_R = P_T G_T G_R \left(\frac{h_t h_r}{d^2}\right)^2$$

- pathloss (dB) = $40log_{10}(d) - 20log_{10}(h_t h_r)$ [unit gain antenna]
  - Where, h_T and h_R are heights of transmit and receive antennas
  - 1 LoS ray and 1 reflected from the ground
- It is valid for distances larger than $d_{\text{break}} = 4h_T h_R/\lambda$ far field
- Note that the received power becomes *independent of the frequency*.
- Higher the transmit antenna, better the signal at receiver (explains why BSs are installed at a higher location than the ground)

©2020 Mahbub Hassan

Example

Question: A 2m tall user is holding his smartphone at half of his height while standing 500m from a 10m high base station. The base station is transmitting a 1.8GHz signal using a transmission power of 30dBm. What is the received power (in dBm) at the smartphone? Assume *unit gain* antennas.

We have h_t = 10m, h_r=2m, d=500m, f=1.8x10^9 Hz, P_T=30dBm, c=3x10^8 m/sec

$$d_{break} = 4\left(\frac{h_t h_r f}{c}\right) = 480m$$ far field

This means that the 2-ray model can be applied to estimate the pathloss at 500m.

$$pathloss = 20log_{10}\left(\frac{d^2}{h_t h_r}\right) = 81.94dB$$

The received power = 30 – 81.94 = -78.94dBm

©2020 Mahbub Hassan

Path loss exponent

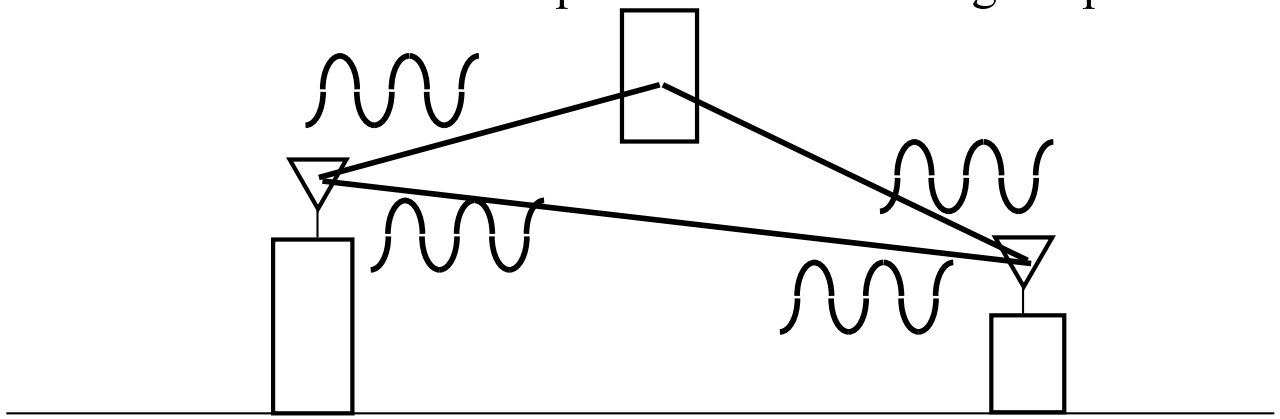
- Empty/free space (no reflector) → d^{-2} law (Frii's)
  - $PL(dB) = 10\log_{10}(d^2) + C = 10x2x\log_{10}(d) + C$ (a straight line with slope = 2)
- 2-ray model → d^{-4} law
  - $PL(dB) = 10\log_{10}(d^4) + C = 10x4x\log_{10}(d) + C$ (a straight line with slope = 4)
- Measurements in real environments → d^{-n} (n = 1.5 to 5.5, typically 4)
  - $PL(dB) = 10\log_{10}(d^n) + C = 10n\log_{10}(d) + C$ (a straight line with slope = n)

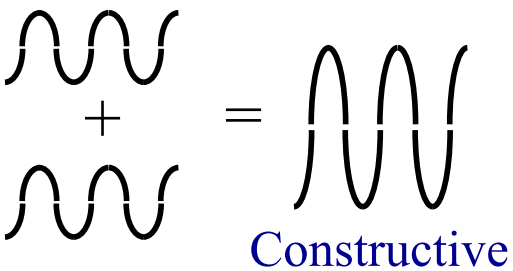
C is a constant; frequency related (Free-space) or antenna height related (2-ray)

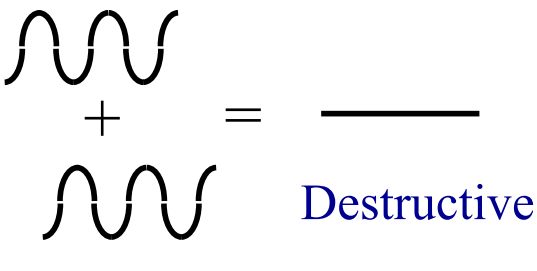
©2020 Mahbub Hassan

Small Scale Fading

- Multipath has phase change (due to reflection and different path to travel)
- Fading: the signal amplitude can change significantly by moving a *few centimeters* (called *small scale fading*: fluctuates in small time scale): *half-wavelength path distance can cause 180 degree phase shift!*
  - **Constructive:** increased amplitude due to alignment of phase
  - **Destructive:** reduced amplitude due to misaligned phase



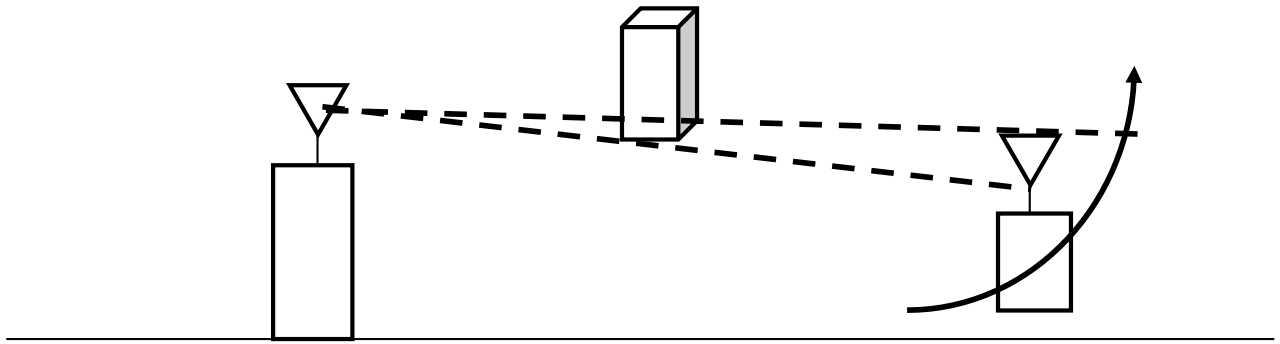


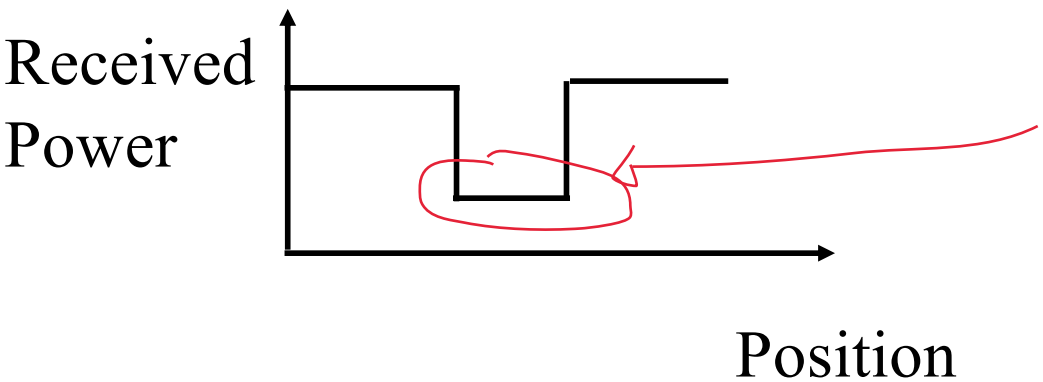


©2020 Mahbub Hassan

Shadowing (large scale fading)

- Shadowing gives rise to *large scale* fading
  - Mobile may be in the *shadow* of a building (fading) for *several meters*
  - RSS drops when in shadow

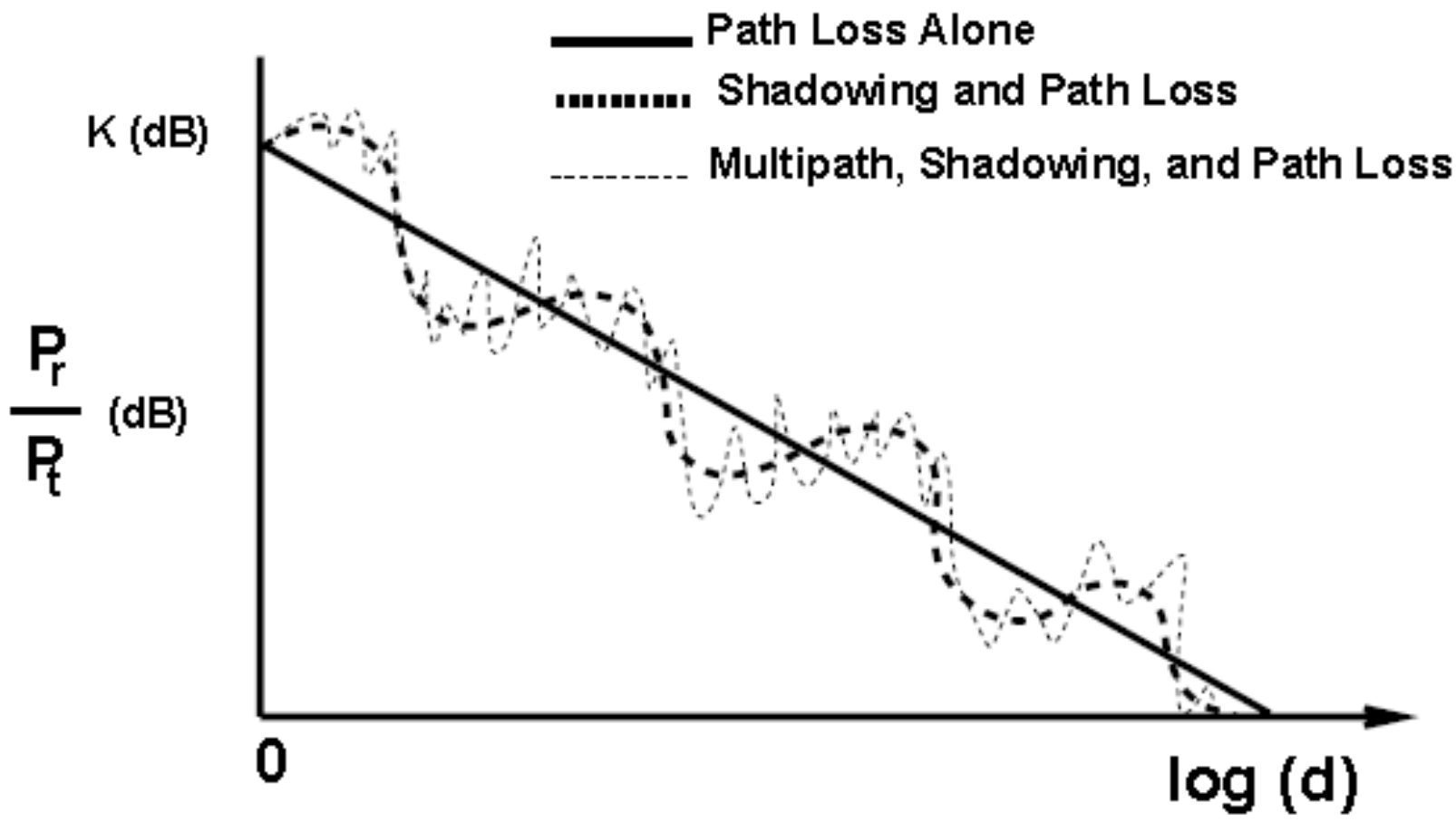




Shadow of the building

©2020 Mahbub Hassan

Total Path Loss



©2020 Mahbub Hassan

MIMO

- Traditionally, single antennas were used
- Multiple antennas are increasingly being used to boost quality/reliability and capacity of wireless communications
  - E.g., most recent WiFi routers have multiple antennas
- Multiple input (multiple antennas at the *transmitter*)
- Multiple output (multiple antennas at the *receiver*)
- MIMO – multiple input multiple output

©2020 Mahbub Hassan

MIMO Antenna Configurations

- SISO – single input (1 Tx antenna) single output (1 Rx antenna)
- SIMO – single input (1 Tx antenna) multiple output (>1 Rx antenna)
- MISO – multiple input (>1 Tx antenna) single output (1 Rx antenna)
- MIMO – multiple input (>1 Tx antenna) multiple output (>1 Rx antenna)
  - 2x2 MIMO – 2 input & 2 output (2 Tx antennas & 2 Rx antennas)
  - 4x2 MIMO – 4 input & 2 output (4 Tx antennas & 2 Rx antennas)
  - 1000x2 MIMO – 1000 input & 2 output (1000 Tx antennas & 2 Rx antennas)

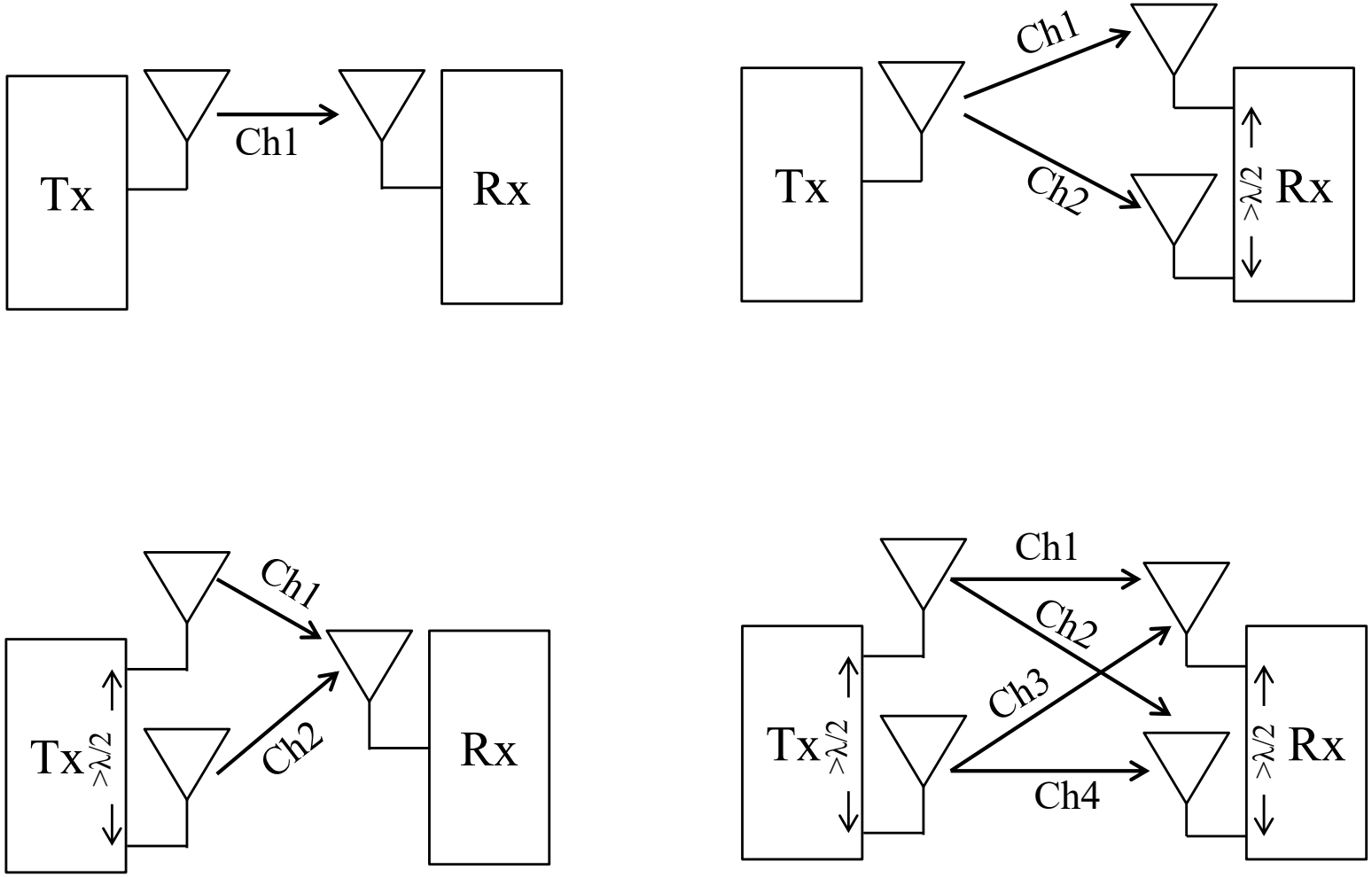
©2020 Mahbub Hassan

Why Multiple Antennas Can Improve Performance?

- Multi-path scenario: if antennas are spaced >λ/2 apart, multipath signals for different antennas can be uncorrelated
  - multiple (*spatial*) channels using the same frequency!
  - More channels means opportunity to improve *signal quality* and *data rate*
- Line-of-Sight (LOS) scenario: multiple antennas at the transmitter can be used to realize *virtual directional antennas* (beamforming)
  - Increase *coverage* and *signal strength* at a particular direction of choice

©2020 Mahbub Hassan

Spatial Channels



©2020 Mahbub Hassan

MIMO Techniques

- Spatial Diversity (a.k.a. Diversity)
  - Improve *reliability* by exploiting spatial channels
- Spatial Multiplexing (a.k.a. Multiplexing)
  - Improve *data rate* by exploiting spatial channels
- Beamforming
  - Increase *coverage* and *signal strength* by exploiting multiple Tx antennas to focus the beam at a narrow angle

©2020 Mahbub Hassan

Diversity

- Total # of *independent* paths = N_T x N_R
  - N_T = # of transmit antenna, N_R = # of receive antenna
- Send same data (copied) over N_T x N_R redundant paths
- Increases reliability – probability that all paths will suffer bad fading at the same time is low
  - SNR at receiver can be improved (*diversity gain*)

©2020 Mahbub Hassan

Example

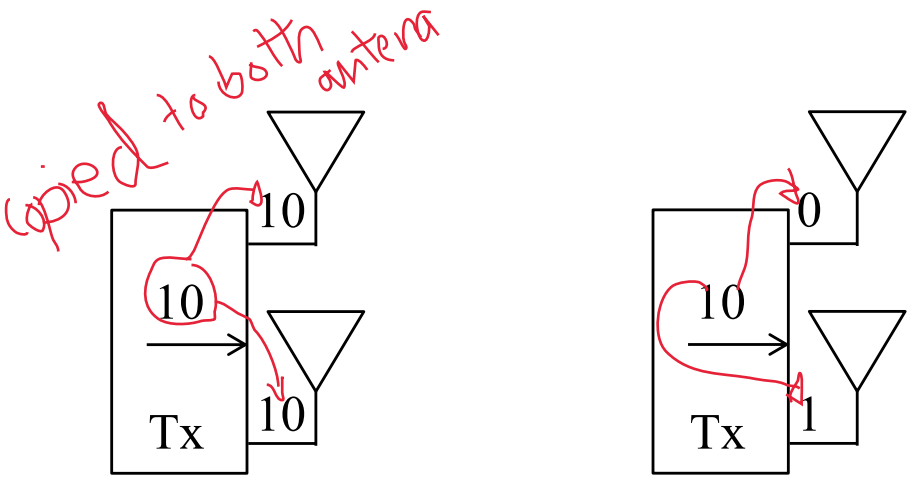
- A base station is equipped with an *antenna array* consisting of 100 elements. What is the maximum number of spatial channels that could be created from this base station to an ordinary mobile device equipped with a *single* antenna?

Answer: It is a 100x1 MIMO. 100 spatial channels are possible.

©2020 Mahbub Hassan

Multiplexing

- Send different bits of the data on different channels
- The combined data rate is increased due to multiplexing
- Overall multiplexing gain is limited by *degrees of freedom*
- Degrees of freedom = $\min(N_T, N_R)$



Diversity Multiplexing

©2020 Mahbub Hassan

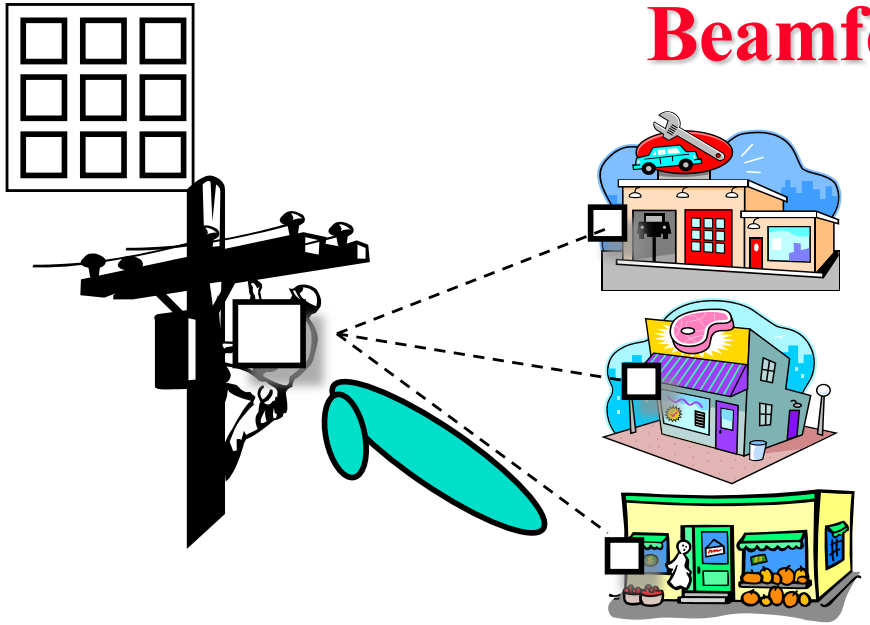
Example

- What is the *degrees of freedom* for an 802.11ac WiFi system with the access point having 8 antennas and communicating to a laptop equipped with 2 antennas?

- Answer: degrees of freedom = min(8,2) = 2

©2020 Mahbub Hassan

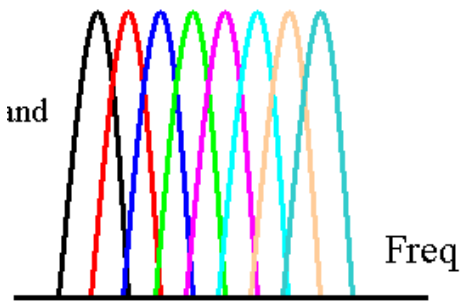
Beamforming



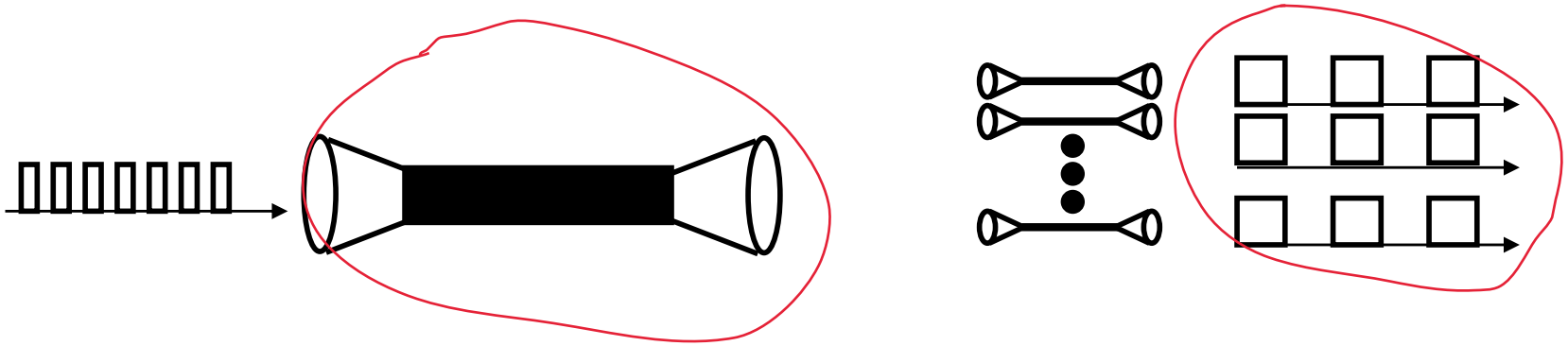
- Phased Antenna Arrays:
  Transmit the same signal using multiple antennas
- By phase-shifting various signals ⇒ Focus on a narrow directional beam (increased SNR and long-distance coverage)
- Receiver does the same, i.e., focus its reception from a particular BS
- Used when LOS

©2020 Mahbub Hassan

OFDM



- **O**rthogonal **F**requency **D**ivision **M**ultiplexing
- Ten 100 kHz channels are better than one 1 MHz Channel

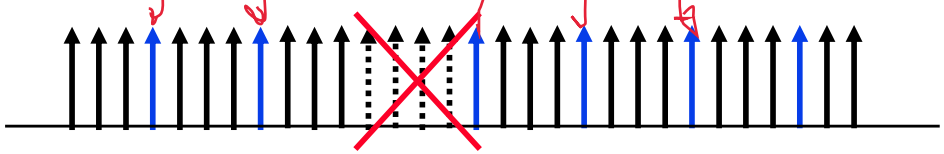


- Frequency band is divided into 256 or more sub-bands.
  - Orthogonal: Peak of one at null of others
- Each carrier is modulated indecently with a BPSK, QPSK, 16-QAM, 64-QAM etc. depending on the fading in the channel (frequency selective fading means different channel has different fading and requires different modulation and coding)
- Used in newer generation of WiFi and 4G/5G

©2020 Mahbub Hassan

Advantages of OFDM

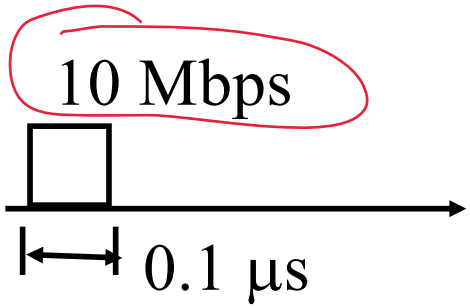
- Robustness against frequency selective burst errors
- Allows adaptive modulation and coding of subcarriers
- Robust against narrowband interference (affecting only some subcarriers)
- Allows pilot subcarriers for channel estimation



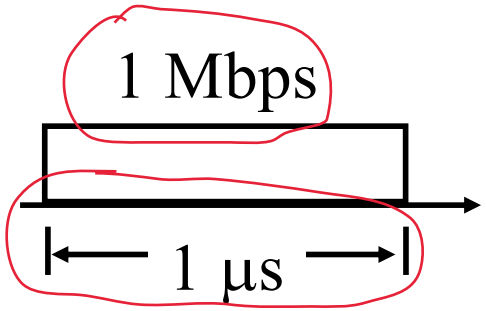
©2020 Mahbub Hassan

OFDM: Design considerations

- Subcarrier spacing = Frequency bandwidth/Number of subcarriers
- Large number of carriers ⇒ Smaller data rate per carrier ⇒ Larger symbol duration ⇒ Less inter-symbol interference
- Reduced subcarrier spacing ⇒ Increased inter-carrier interference due to Doppler spread in mobile applications



Small # of carriers
Shorter symbol durations
Higher data rates per carrier



Large # of carriers
Longer symbol durations
Lower data rates per carrier

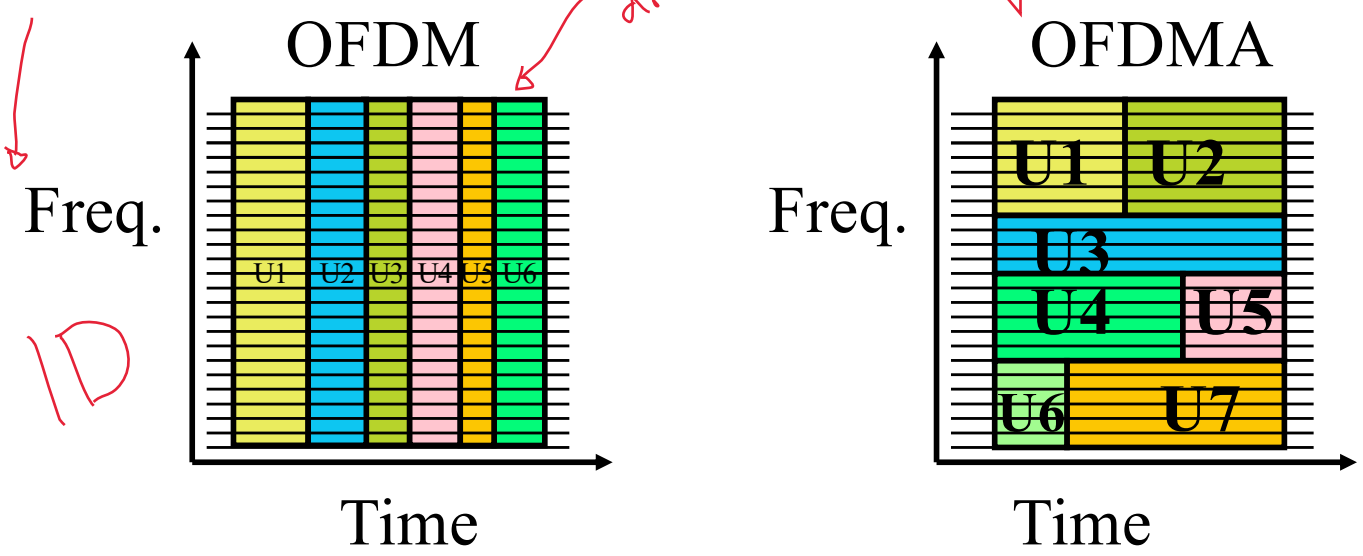
©2020 Mahbub Hassan

OFDMA

- Orthogonal Frequency Division Multiple Access
- Each user has a subset of subcarriers for a few time slots
- OFDM systems use TDMA (e.g., in WiFi)
- OFDMA allows Time+Freq DMA ⇒ 2D Scheduling

OFDM subcarriers

all subcarriers are used



1D

©2020 Mahbub Hassan

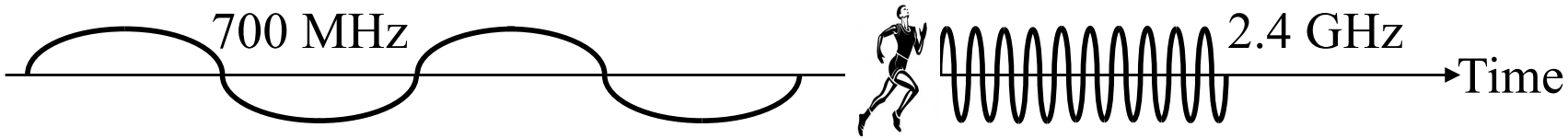
Example

- *With a subcarrier spacing of 10 kHz, how many subcarriers will be used in an OFDM system with 20 MHz channel bandwidth?*

Number of subcarriers = channel bandwidth/subcarrier spacing
$= 20x10^6/10x10^3 = 2000$

©2020 Mahbub Hassan

Effect of Frequency



- Higher Frequencies have higher attenuation,
  e.g., 18 GHz has 20 dB/m more than 1.8 GHz
- Higher frequencies need smaller antenna
  Antenna $\geq$ Wavelength/2, 800 MHz $\Rightarrow$ 6”
- Higher frequencies are affected more by weather
  Higher than 10 GHz affected by rainfall
  60 GHz affected by absorption of oxygen molecules
- Higher frequencies have more bandwidth and higher data rate
- Higher frequencies allow more frequency reuse
  They attenuate close to cell boundaries. Low frequencies propagate far.

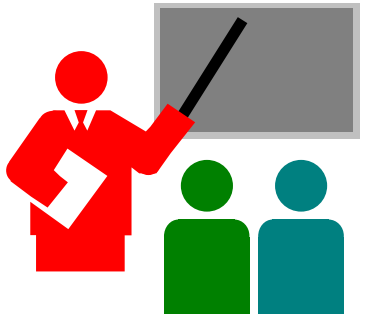
©2020 Mahbub Hassan

Effect of Frequency (Cont)

- Lower frequencies have longer reach
  ⇒ Longer Cell Radius
  ⇒ Good for rural areas
  ⇒ Smaller number of towers
  ⇒ Longer battery life
- Lower frequencies require larger antenna and antenna spacing
  ⇒ MIMO difficult particularly on mobile devices
- Lower frequencies ⇒ Smaller channel width
  ⇒ Need aggressive MCS, e.g., 256-QAM
- Doppler shift = vf/c = Velocity × Frequency/(speed of light)
  ⇒ Lower Doppler spread at lower frequencies
- Mobility ⇒ Below 10 GHz

©2020 Mahbub Hassan

Summary



1. Path loss increases at a power of 2 to 5.5 with distance.
2. Fading = Changes in power with changes in position
3. Multiple Antennas: Receive diversity, transmit diversity, multiplexing, and beamforming
4. OFDM splits a band into many orthogonal subcarriers. OFDMA = FDMA + TDMA

©2020 Mahbub Hassan

Acronyms

- BPSK — Binary Phase-Shift Keying
- BS — Base Station
- dB — DeciBels
- dBi — DeciBels Intrinsic
- dBm — DeciBels milliwatt
- DFT — Discrete Fourier Transform
- DMA — Direct Memory Access
- DSP — Digital Signal Processing
- DVB-H — Digital Video Broadcast handheld
- FDMA — Frequency Division Multiple Access
- FFT — Fast Fourier Transform
- IDFT — Inverse Discrete Fourier Transform
- IFFT — Inverse Fast Fourier Transform
- ISI — Inter-symbol interference
- kHz — Kilo Hertz
- LoS — Line of Sight

©2020 Mahbub Hassan

Acronyms (Cont)

- MHz — Mega Hertz
- MIMO — Multiple Input Multiple Output
- MS — Mobile Station
- OFDM — Orthogonal Frequency Division Multiplexing
- OFDMA — Orthogonal Frequency Division Multiple Access
- QAM — Quadrature Amplitude Modulation
- QPSK — Quadrature Phase-Shift Keying
- RF — Radio Frequency
- SNR — Signal to Noise Ratio
- SS — Subscriber Station
- STBC — Space Time Block Codes
- TDMA — Time Division Multiple Access

©2020 Mahbub Hassan

PHY FUNDAMENTALS I

Coding and Modulation

©2020 Mahbub Hassan

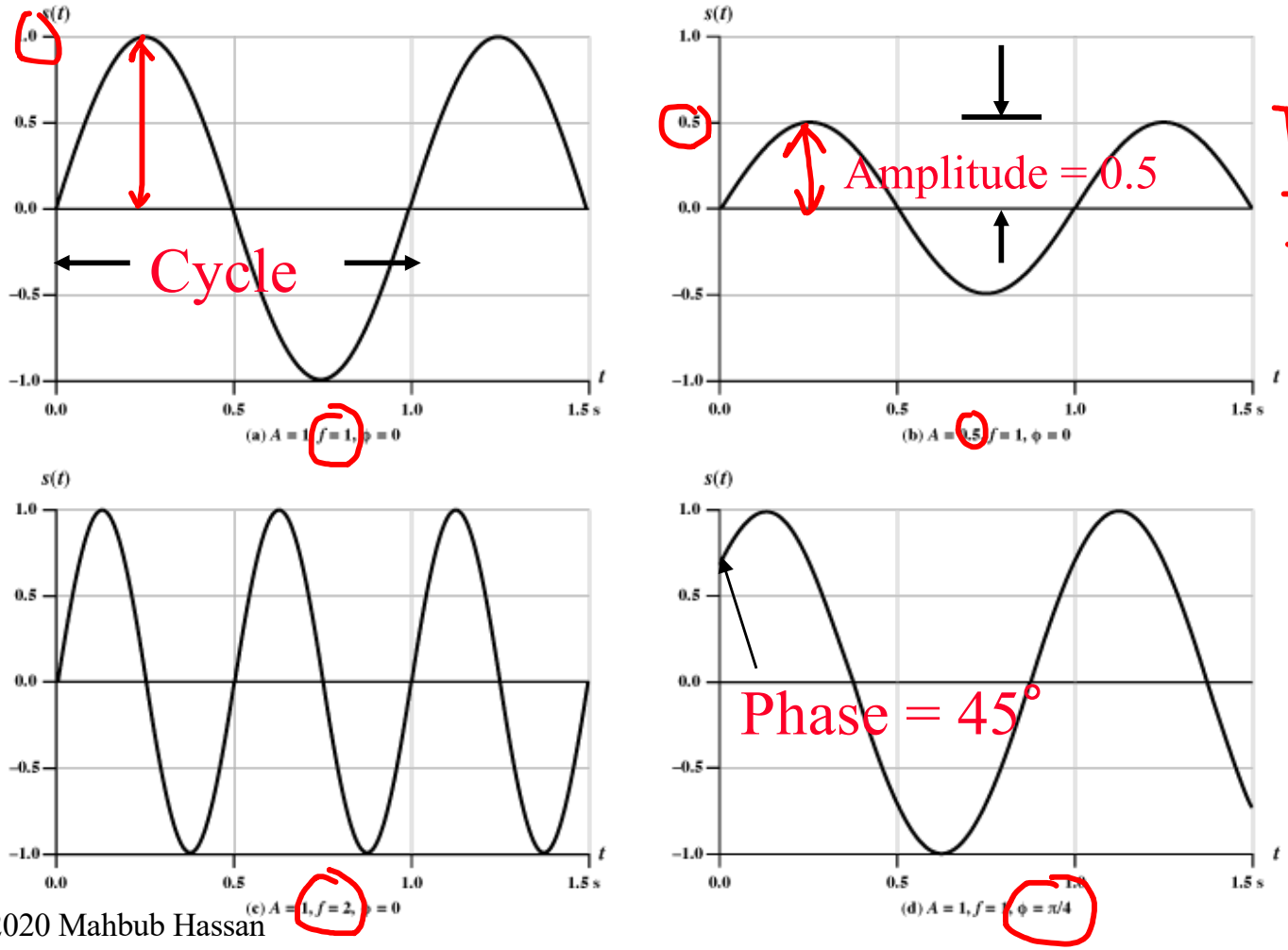
Overview

1. Frequency, Wavelength, Amplitude, and Phase
2. Electromagnetic Spectrum
3. Time and Frequency Domains
4. Decibels
5. Coding and modulation
6. Channel Capacity (Nyquist's and Shannon's Theorems)
7. Hamming Distance and Error Correction
8. Multiple Access Methods (TDMA, FDMA, CDMA)
9. Spread Spectrum (Frequency Hopping and Direct Sequence)
10. Doppler Shift, Doppler Spread, Coherence Time
11. Duplexing

©2020 Mahbub Hassan

Frequency, Period, and Phase

- A Sin(2πft + ϕ), A = Amplitude, f=Frequency, ϕ = Phase, Period T = 1/f,
  Frequency is measured in Cycles/sec or **Hertz**



$\pi = 180°$

$\frac{\pi}{2} = 90°$

$\frac{\pi}{4} = 45°$

©2020 Mahbub Hassan

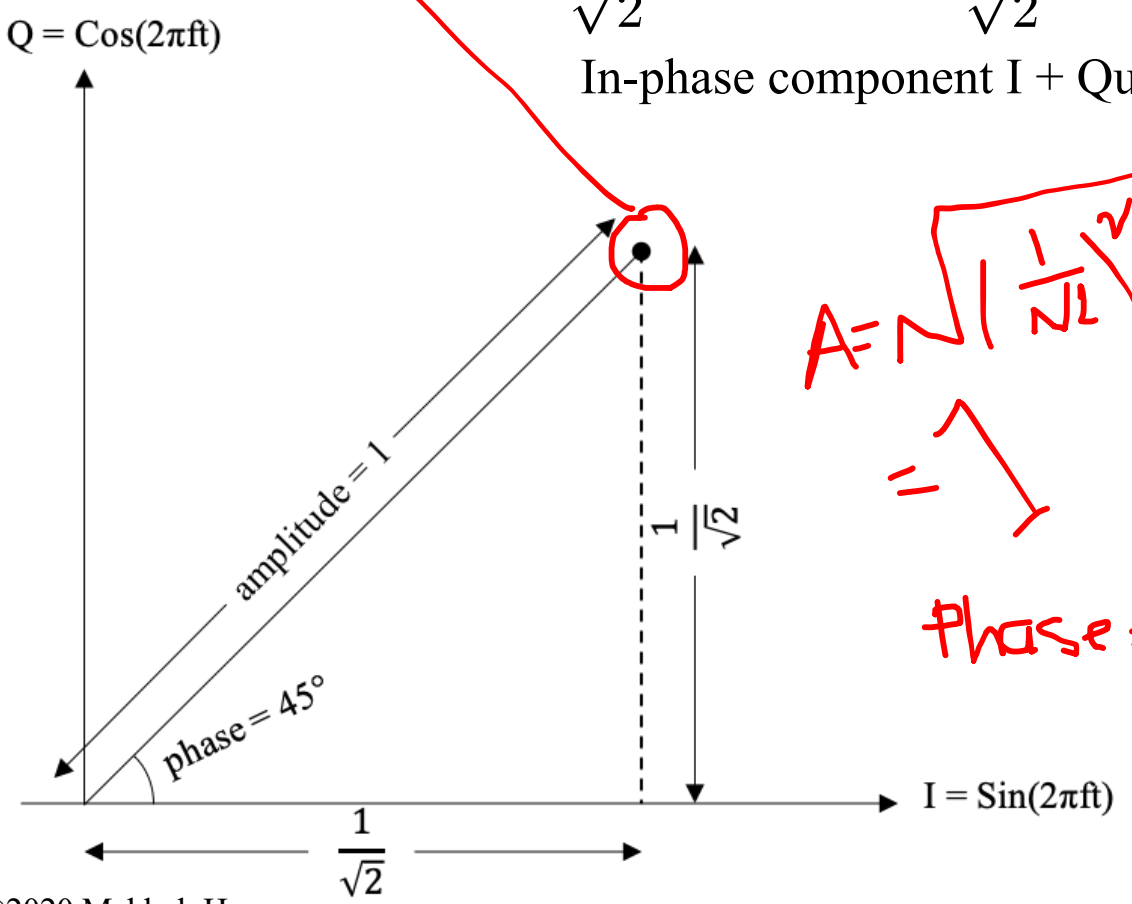
Phase and Amplitude: 2D Representation

- Sine wave with a phase of 45°

$$A=1 \quad \sin(2\pi ft + \frac{\pi}{4}) = \sin(2\pi ft)\cos(\frac{\pi}{4}) + \cos(2\pi ft)\sin(\frac{\pi}{4})$$

$$= \frac{1}{\sqrt{2}}\sin(2\pi ft) + \frac{1}{\sqrt{2}}\cos(2\pi ft)$$

In-phase component I + Quadrature component Q

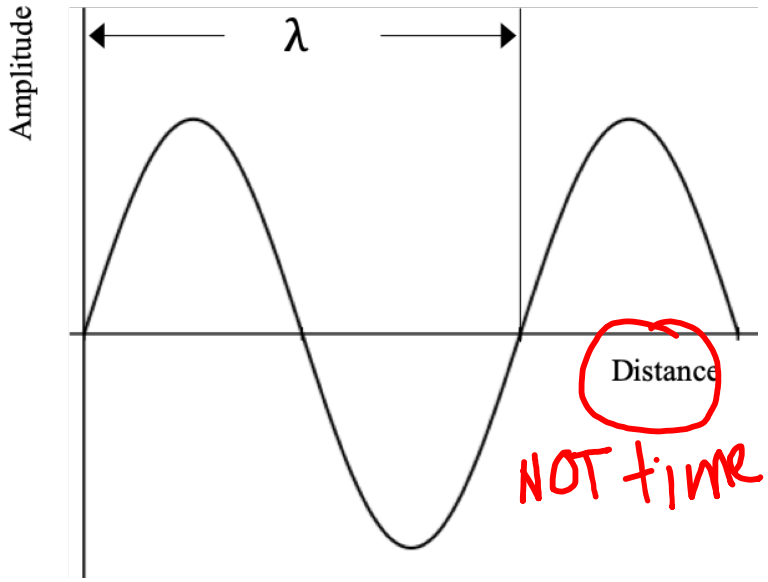


$$A = \sqrt{\left(\frac{1}{\sqrt{2}}\right)^2 + \left(\frac{1}{\sqrt{2}}\right)^2} = 1$$

$$\text{Phase} = \tan^{-1}\left(\frac{\frac{1}{\sqrt{2}}}{\frac{1}{\sqrt{2}}}\right) = \tan^{-1}(1) = 45^\circ = \frac{\pi}{4}$$

©2020 Mahbub Hassan

Wavelength



- Distance occupied by one cycle
- Distance between two points of corresponding phase in two consecutive cycles
- Wavelength = λ
- Assuming signal velocity v
  - $\lambda = vT$
  - $\lambda f = v$
  - c = 3×10^8 m/s (speed of light in free space) = *300 m/μs*

©2020 Mahbub Hassan

Example: converting frequency to wavelength

- Frequency = 2.5 GHz

$$\begin{aligned} \text{Wavelength} = \lambda &= \frac{c}{f} \\ &= \frac{300\ \text{m}/\mu\text{s}}{2.5 \times 10^9} \\ &= 120 \times 10^{-3} = 120\ \text{mm} = 12\ \text{cm} \end{aligned}$$

©2020 Mahbub Hassan

Example: converting wavelength to frequency

- Wavelength = λ = 5 mm

Frequency = f = c/λ

= $(3 \times 10^8 \text{ m/s}) / (5 \times 10^{-3} \text{ m})$

= $(300 \times 10^9) / 5 = 60$ GHz

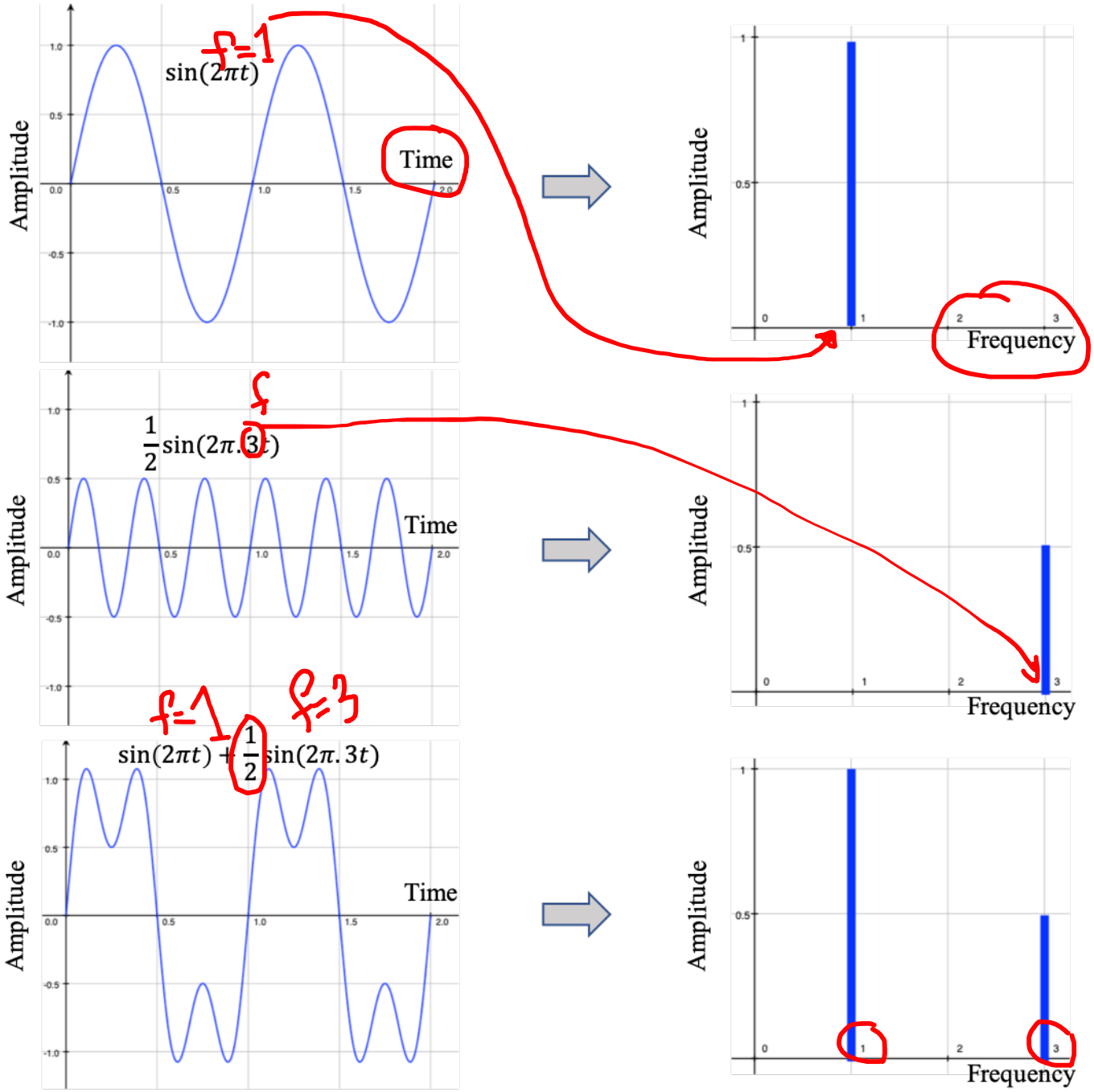
©2020 Mahbub Hassan

Well-known frequencies & wavelengths

- The higher the frequency, the smaller the wavelength
- 900 MHz has a wavelength of 33.33 cm
- 2.4 GHz has a wavelength of 12.5 cm
- 60 Ghz has a wavelength of only 5 mm (this technology is called *millimeter wave or mmWave*)

©2020 Mahbub Hassan

Time and Frequency Domains



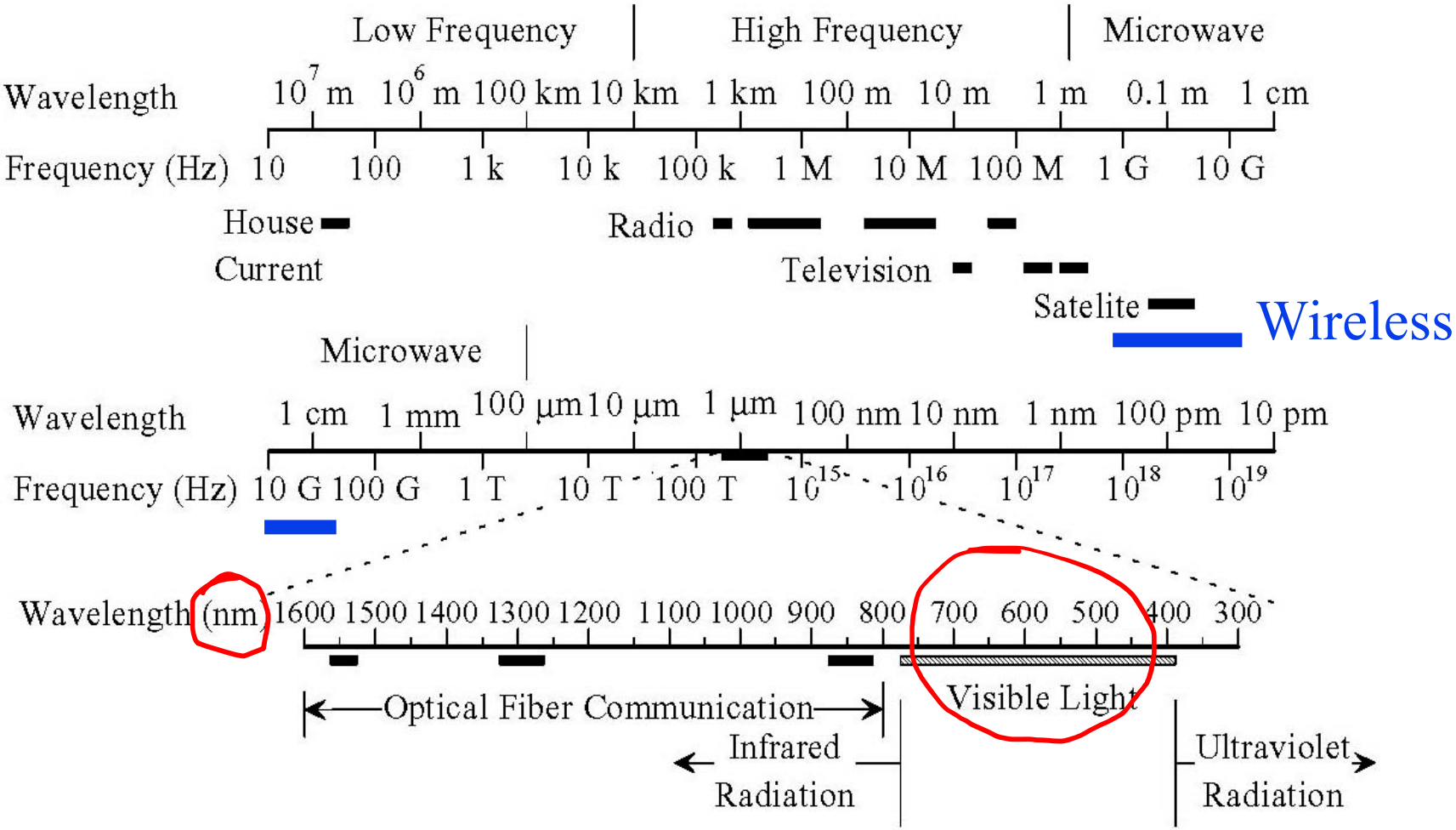
©2020 Mahbub Hassan

Electromagnetic Spectrum

- Wireless transmissions use the airwaves
  - Airwaves are radio frequencies
- Useful frequencies constitute the Spectrum
- Spectrum is 'virtual'
  - We cannot touch and feel
- A gift from nature (the force field)
  - Has been there ever since earth was created
- A (limited) natural resource

©2020 Mahbub Hassan

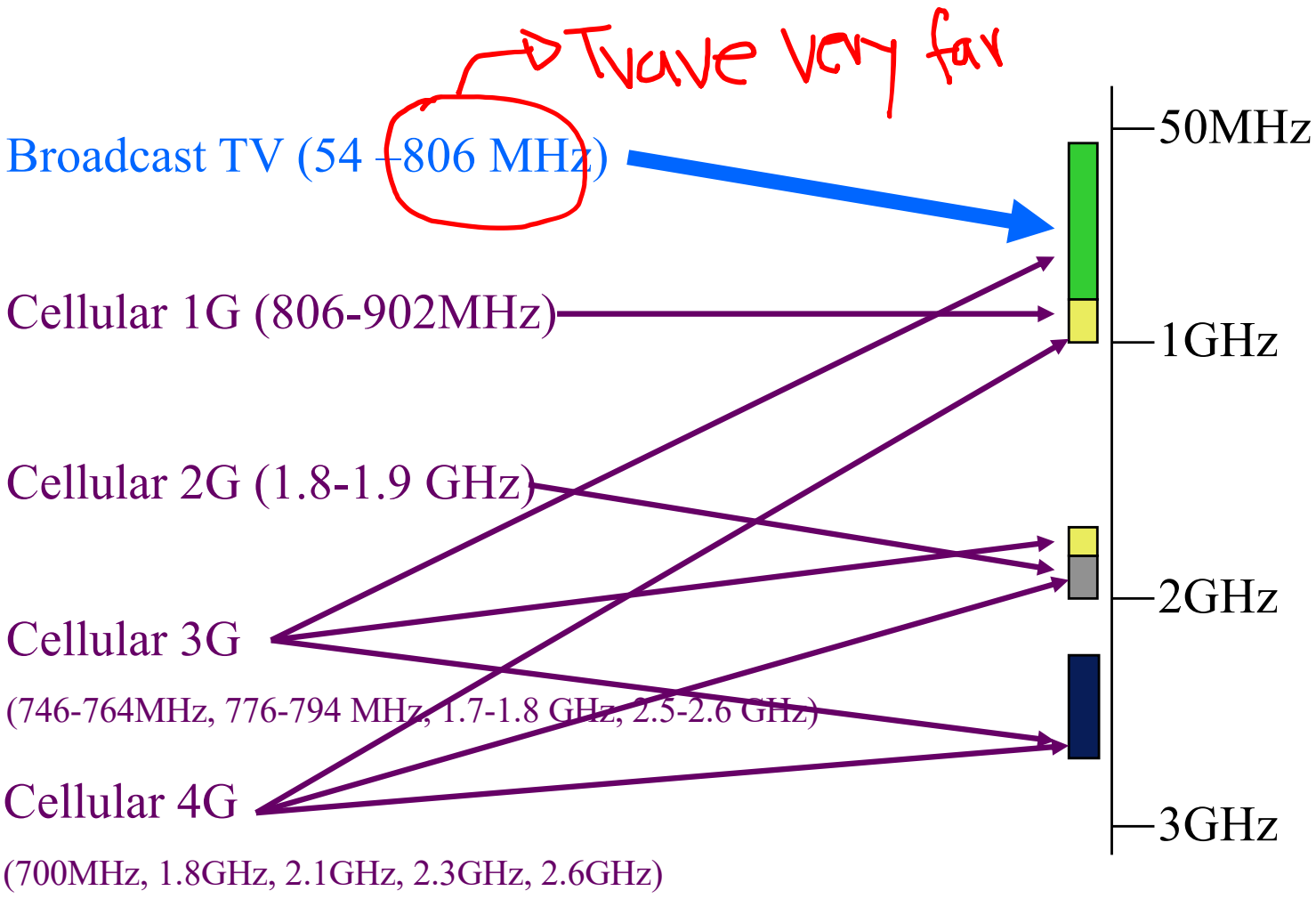
Electromagnetic Spectrum



- Wireless communication mostly uses 100 kHz to 6 GHz
- > 6 GHz are currently being explored and 60 GHz is used in some latest WiFi products

©2020 Mahbub Hassan

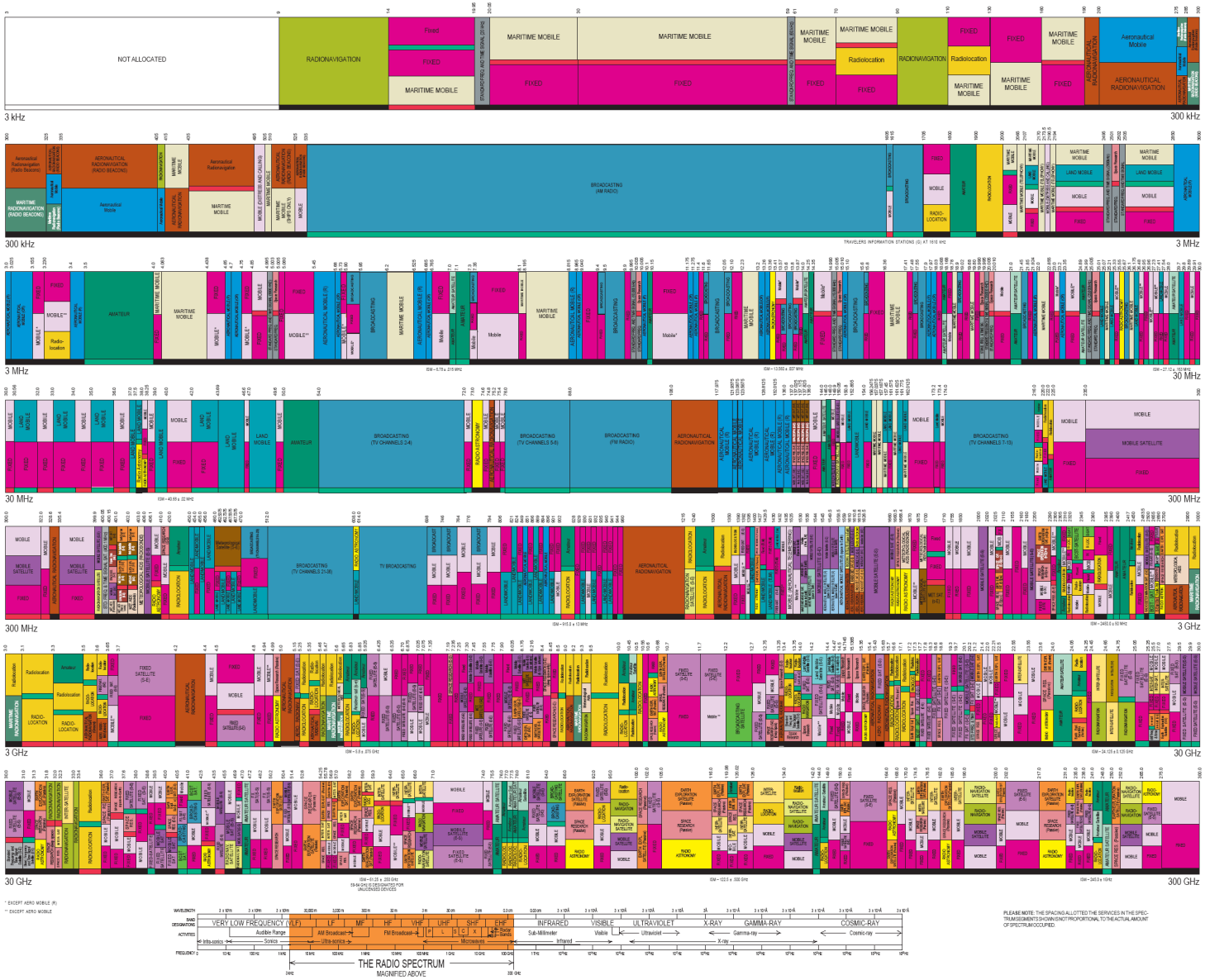
Spectrum use by TV and cellular services



©2020 Mahbub Hassan

UNITED STATES FREQUENCY ALLOCATIONS

THE RADIO SPECTRUM



©2020 Mahbub Hassan

Spectrum regulation and licensing

- Many users use the same airspace
  - Recipe for collision
  - No one would get anything useful done
- Spectrum use is highly regulated
  - By govt. authorities (eg FCC in the USA)
- Spectrum is often licensed
  - By big companies, eg Telstra
  - Gives exclusive rights to certain freq. bands
  - Interference avoidance by regulation

©2020 Mahbub Hassan

Spectrum allocation

- Bulk of it reserved for government use
  - Scientific exploration
  - Public safety
  - Military
- Some for commercial services
  - TV broadcast
  - Mobile phone
- Some for free-to-use
  - High-speed wireless local area network (WiFi)
  - Cordless phone handsets at home
  - Can you name a few more?

©2020 Mahbub Hassan

Key principles of spectrum allocation

- Maximize spectrum utilization
- Spectrum made available to new technologies and services
  - Adapt to new market needs
- Fair licensing
- Promote competition
- Ensure spectrum availability for public safety, health, defense, scientific experiments…

©2020 Mahbub Hassan

Free/unregulated/license-exempt spectrum

- Not subject to license
- Has rules for products (eg *power limitation*)
- More frequencies are being released as license-exempt
- Some current license-exempt frequencies
  - 900 MHz
  - 2.4 GHz ISM band (WiFi, Microwave etc.)
  - 5.2/5.3/5.8 GHz (WiFi, Cordless phone etc.)
  - Can you identify more?

©2020 Mahbub Hassan

Decibel

- Tx_power for practical mobile systems vary by many orders of magnitude
  - 100kW or kilowatt (FM radio station)
  - 500mW or milliwatt (cellular phone tx power)
  - 2.5mW (Bluetooth with ~10m range)
  - 100pW or picowatt (typical WiFi rx threshold)
  - Femto watt? (nanosensor communication)
  - 1 W = 10^3 mW = 10^6 μW = 10^9 nW = 10^{12} pW
- Decibel is a more convenient (logarithmic scale) unit to compare these powers, which are many orders of magnitude apart
- Also path loss (attenuation) can be many orders of magnitude
  - Path loss therefore is usually expressed in decibels

©2020 Mahbub Hassan

Decibel (dB) Formula

- In Honour of Graham Bell
- The number of decibels is ten times the logarithm to base 10 of the ratio of two power quantities ($dB = 10\log_{10}(P_1/P_2)$)
  - The quantity "Bel" would be $\log_{10}(P_1/P_2)$, but not used
- Decibel can be used for different purposes
  1. Path Loss: To express path loss or attenuation: [P_1 = transmit power; P_2 = receive power]
  2. SNR: To express signal (P_1) to noise (P_2) ratio at the receiver
  3. Signal Power: To express signal power (P_1), which can be either transmit or receive power, to a reference power (P_2)

©2020 Mahbub Hassan

Decibel Examples for Path Loss

- **Example 1**: $P_t = 10$ mW, $P_r = 5$ mW (power reduced by half)
  Attenuation (path loss) = $10 \log_{10} (10/5) = 10 \log_{10} 2 = 3$ dB

- **Example 2**: $P_t = 100$ mW, $P_r = 1$ mW (power reduced by a factor of 100)
  Attenuation = $10 \log_{10} (100/1) = 10 \log_{10} 100 = 20$ dB

Power Ratio	dB
10,000,000,000 (ten billion times)	100 (10 x 10)
1,000,000 (1 million times)	60 (10 x 6)
10 (ten times)	10 (10 x 1)
0.001 (10^{-3})	-30 (10 x -3)
0.0001 (10^{-4})	-40 (10 x -4)

©2020 Mahbub Hassan

Decibel Examples for Signal-to-Noise Ratio

- **Example 1**: P_{signal} = 1 mW (received signal strength), P_{noise}= 100 μW

  SNR = 10 $\log_{10}$ (1000/100) = 10 $\log_{10}$ 10 = 10 dB

- **Example 2**: Received signal strength is measured at 10 mW. What is the noise power if SNR = 10 dB?

  SNR = 10 dB = 10 $\log_{10}$ (10mW/P_{noise})

P_{noise} = 1 mW

©2020 Mahbub Hassan

Expressing Power in dBm

m stands for milliwatt

- dBm is in reference to 1 milliwatt
- First, express power in milliwatt
- Then apply the following formula to obtain dBm

Power in dBm = 10 log (power in milliwatt)

©2020 Mahbub Hassan

Conversion to dBW

- dBW is in reference to 1 watt
- First express power in watt
- Then apply the following formula to obtain dBW

Power in dBW = 10 log (power in watt)

©2020 Mahbub Hassan

Relationship between dBm & dBW

- Note that 1 W = 1000 mW
- This gives us following relationship
  - Note log(axb) = log(a)+log(b)

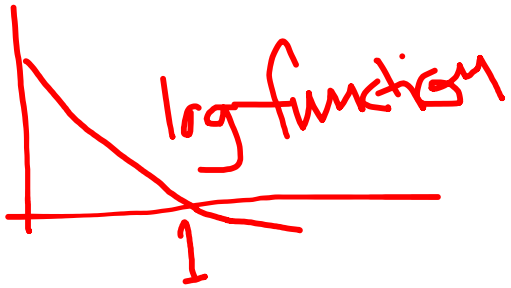
$$dBm = dBW + 30$$

If you've calculated a power in dBW, you can simply derive the equivalent dBm by adding 30 to dBW, and vice versa.

©2020 Mahbub Hassan

Examples for converting Watt to dBm/dBW

- Example 1: Express 1 mW power in units of dBm



$$10 \log (1) = 10x0 = 0 \text{ dBm}$$

So, ZERO dBm does not mean there is no power !

©2020 Mahbub Hassan

Example (2)

- Example 2: Express 50 W in
  - (a) dBW
  - (b) dBm

$$\text{(a) } P(\text{dBW}) = 10 \log (50) = 17 \text{ dBW}$$

$$\text{(b) } P(\text{dBm}) = 10 \log (50\text{x}1000) \text{ dBm}$$

$$= 10 \log (50) + 10 \log (1000) \text{ dBm}$$

$$= 17 + 30 = 47 \text{ dBm}$$

©2020 Mahbub Hassan

Coding Terminology

- **Symbol:** **the smallest element of a signal with a given amplitude, frequency, and phase that can be detected**

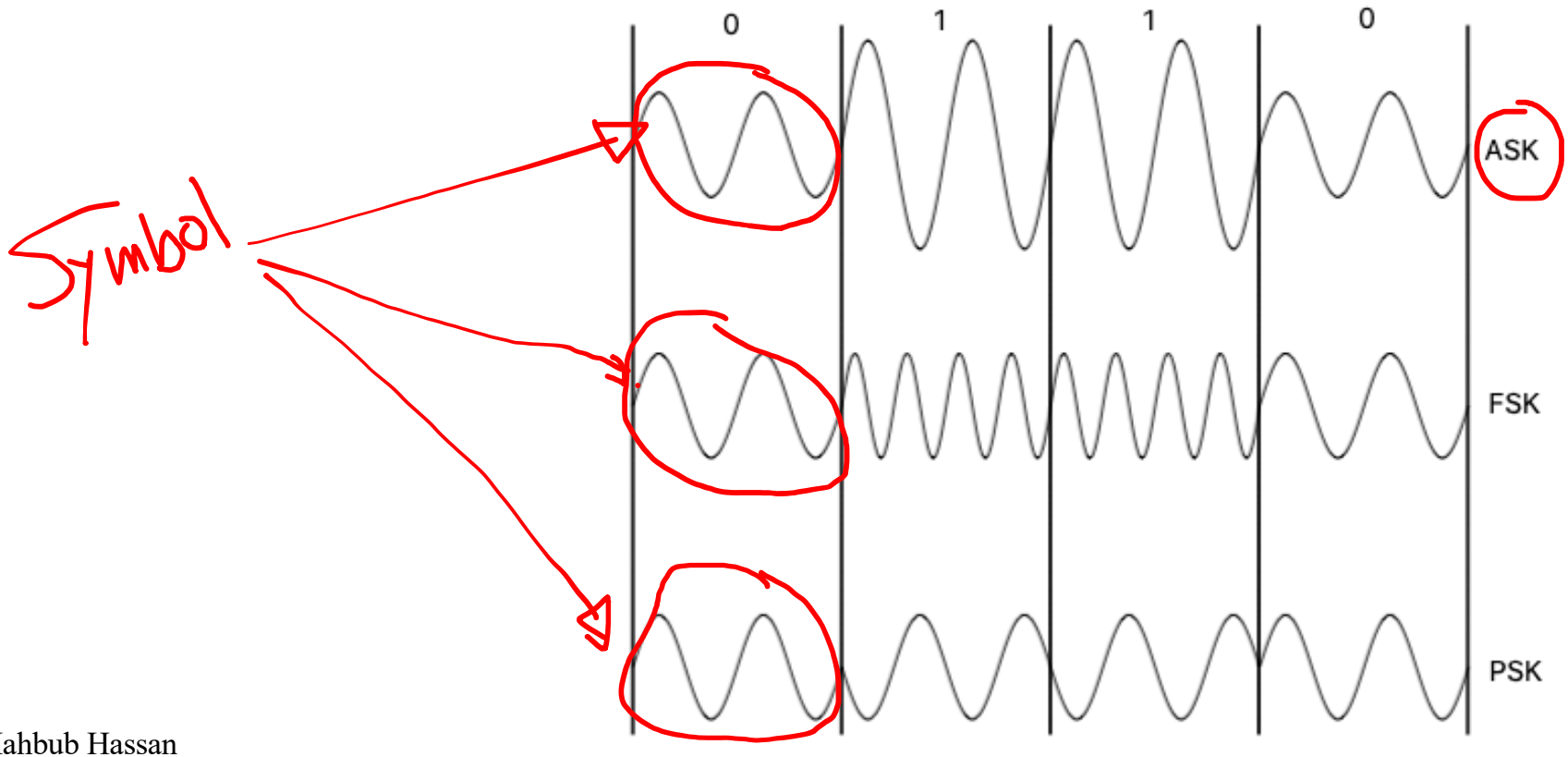
1 0

- **Modulation Rate**: = 1/symbol_duration = Baud rate (or symbol rate)
- **Data Rate**: Bits per second (bps)
- A symbol may carry multiple bits
  - A binary signal with only two different symbols would carry 1 bit per symbol (baud rate = data rate)
  - For an M-ary signal, data rate = baud rate x $\log_2(M)$

©2020 Mahbub Hassan

Modulation

- Digital version of modulation is called **keying**
  - **Amplitude Shift Keying (ASK)**
  - **Frequency Shift Keying (FSK)**
  - **Phase Shift Keying (PSK):** Binary PSK (BPSK)



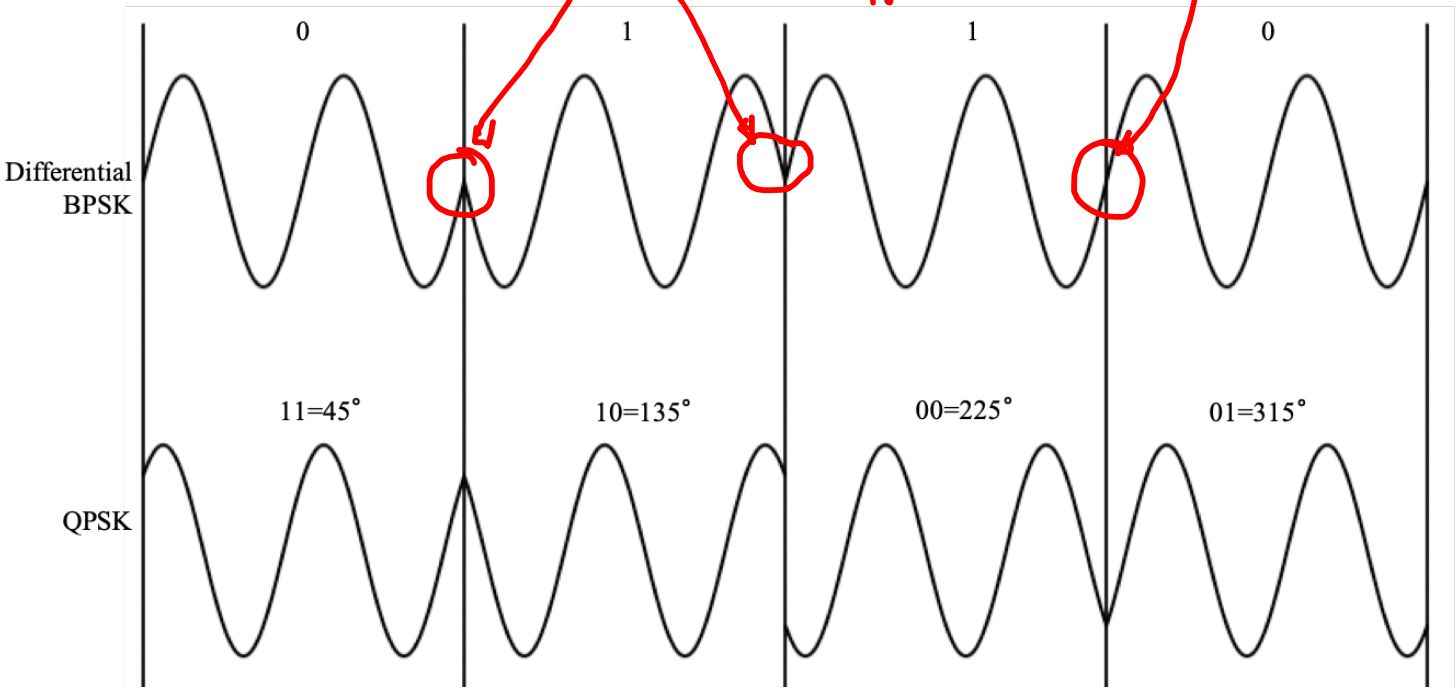
©2020 Mahbub Hassan

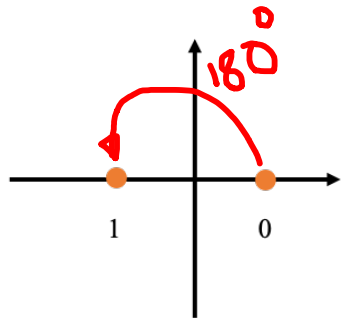
Modulation (Cont)

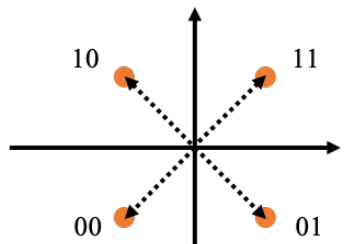
- **Differential BPSK:** Does not require reference signal
- **Quadrature Phase Shift Keying (QPSK)**

Phase difference

No difference





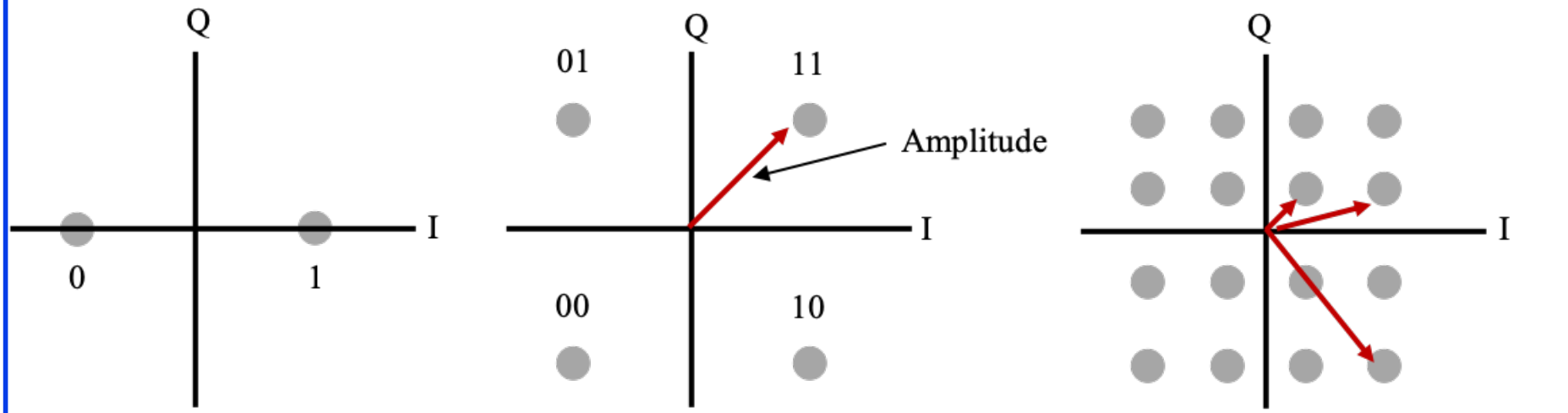


Constellation

©2020 Mahbub Hassan

QAM

- Quadrature Amplitude and Phase Modulation
- 4-QAM, 16-QAM, 64-QAM, 256-QAM, …
- Used in DSL and wireless networks
- Constellation diagram (shows combinations of amplitudes and phases)



Binary (1 amplitude, 2 phases) 4-QAM (1 amplitude, 4 phases) 16-QAM (3 amplitudes, 12 phases)

- 4-QAM ⇒ 2 bits/symbol, 16-QAM ⇒ 4 bits/symbol, …

©2020 Mahbub Hassan

QAM in Action

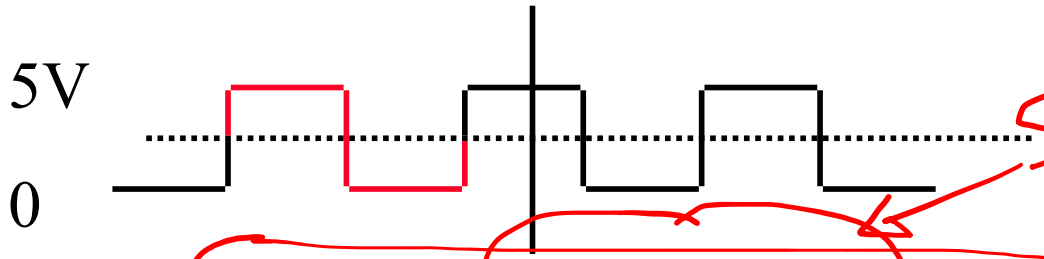
Wireless Technology	QAM Supported
4G	256 QAM
5G	1024 QAM
WiFi 802.11n	16 QAM, 64 QAM
WiFi5 802.11ac	256 QAM
WiFi6 802.11ax	1024 QAM

10 bits per symbol

©2020 Mahbub Hassan

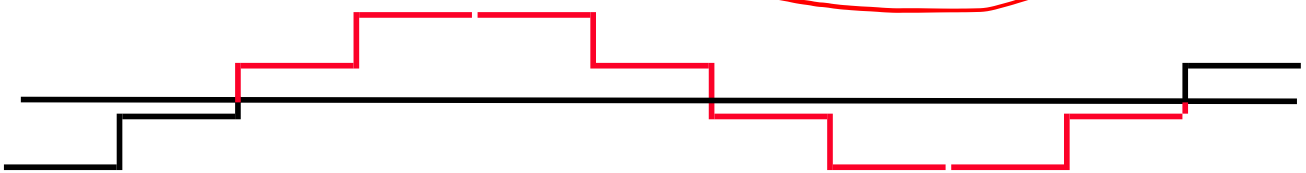
Channel Capacity

- Capacity = Maximum data rate (bps) for a channel
- **Nyquist Theorem (noiseless channel)**: Bandwidth = B Hz
  Baud rate $\leq$ 2 B
- Bi-level Encoding: Max. Data rate = 2 × Bandwidth



Symbol Rate

- Multilevel: Capacity = 2 × Bandwidth × $\log_2 M$
  M = Number of levels



Example: M=4, Capacity = 4 × Bandwidth

©2020 Mahbub Hassan

Example

Assume that you have discovered a novel material that has negligible electrical noise. What is the maximum data rate that this material could achieve over a phone wire having a bandwidth of 3100 Hz if data was encoded with 64-QAM?

Solution

We have B= 3100 M = 64

$$\text{Data rate} = 2 \times 3100 \times \log_2 64 = 37{,}200 \text{ bps}$$

©2020 Mahbub Hassan

Shannon's Theorem (noisy channel)

- Bandwidth = B Hz
  Signal-to-noise ratio = S/N
- Maximum number of bits/sec = $B \log_2 (1+S/N)$ [error free communication]
- Example: Phone wire bandwidth = 3100 Hz

$$S/N = 30 \text{ dB}$$

$$10 \text{ Log}_{10} S/N = 30$$

$$\text{Log}_{10} S/N = 3$$

$$S/N = 10^3 = 1000$$

$$\text{Capacity} = 3100 \log_2 (1+1000) = 30{,}894 \text{ bps}$$

©2020 Mahbub Hassan

Hamming Distance

- Hamming Distance between two sequences = Number of bits in which they disagree
- Example: 011011
  110001

  Difference 101010 $\Rightarrow$ Distance = 3

©2020 Mahbub Hassan

Error Correction Example

- 2-bit words transmitted as 5-bit/word

Data	Codeword
00	00000
01	00111
10	11001
11	11110

Received = 00100 ⇒ Not one of the code words ⇒ Error

Distance (00100,00000) = 1 Distance (00100,00111) = 2

Distance (00100,11001) = 4 Distance (00100,11110) = 3

⇒ Most likely 00000 was sent. Corrected data = 00

b. Received = 01010 Distance(…,00000) = 2 = Distance(…,11110)
Error detected but cannot be corrected

c. Three-bit errors will not be detected. Sent 00000, Received 00111.

©2020 Mahbub Hassan

Multiple Access Methods

Time Division Multiple Access

(communicating groups are taking turns)

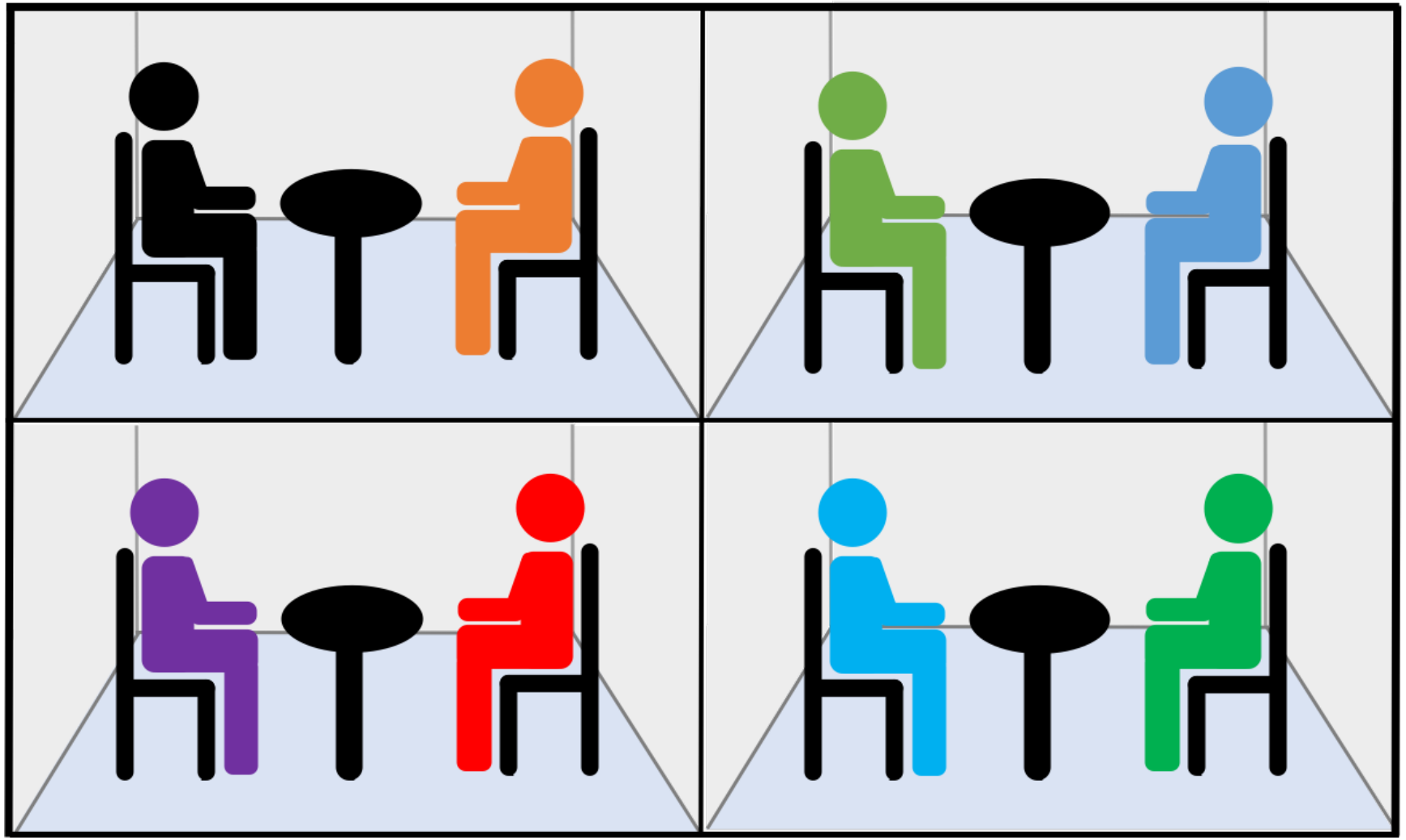
Code Division Multiple Access

(all communicating groups are talking at the same time)

©2020 Mahbub Hassan

Multiple Access

FDMA (frequency division multiple access)



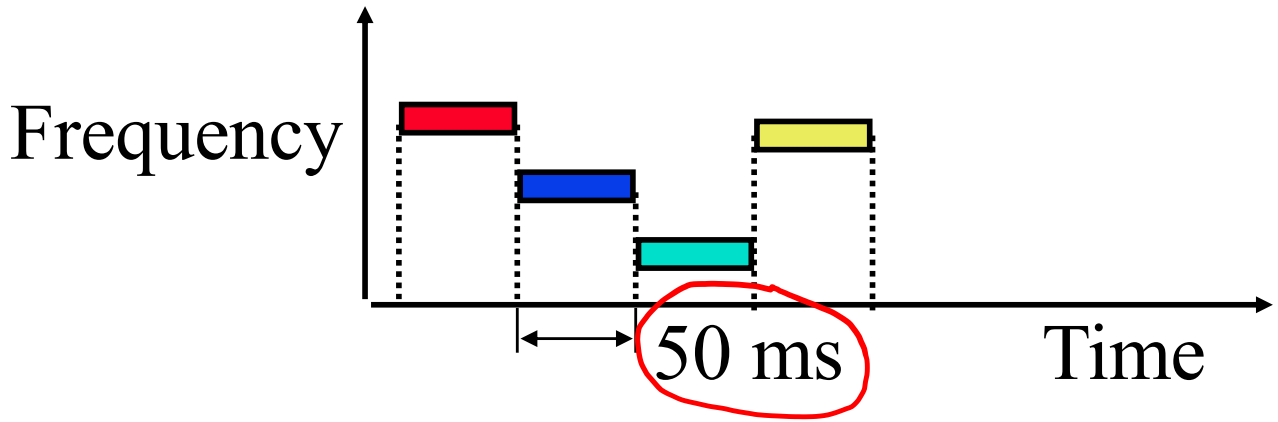
©2020 Mahbub Hassan

CDMA

- Each communicating group is using a different "code"
- You can understand a conversation only if you know the code used in that conversation
- Much like a *multilingual party*, where people from different languages are all talking at the same time (code = language)
- Two popular coding methods for CDMA
  - Frequency hopping spread spectrum (FHSS)
  - Direct sequence spread spectrum (DSSS)

©2020 Mahbub Hassan

Frequency Hopping Spread Spectrum



- Transmit over a narrowband, but continuously switch (hop) frequency over a wide spectrum
  - Spreads the transmission (power) over a wide spectrum
    ⇒ Spread Spectrum
- Pseudo-random frequency hopping (both transmitter and receiver use the same pseud-random number sequence = code)
  - Developed initially for military
  - Patented by actress Hedy Lamarr (idea came while playing a piano; tone changes continuously)

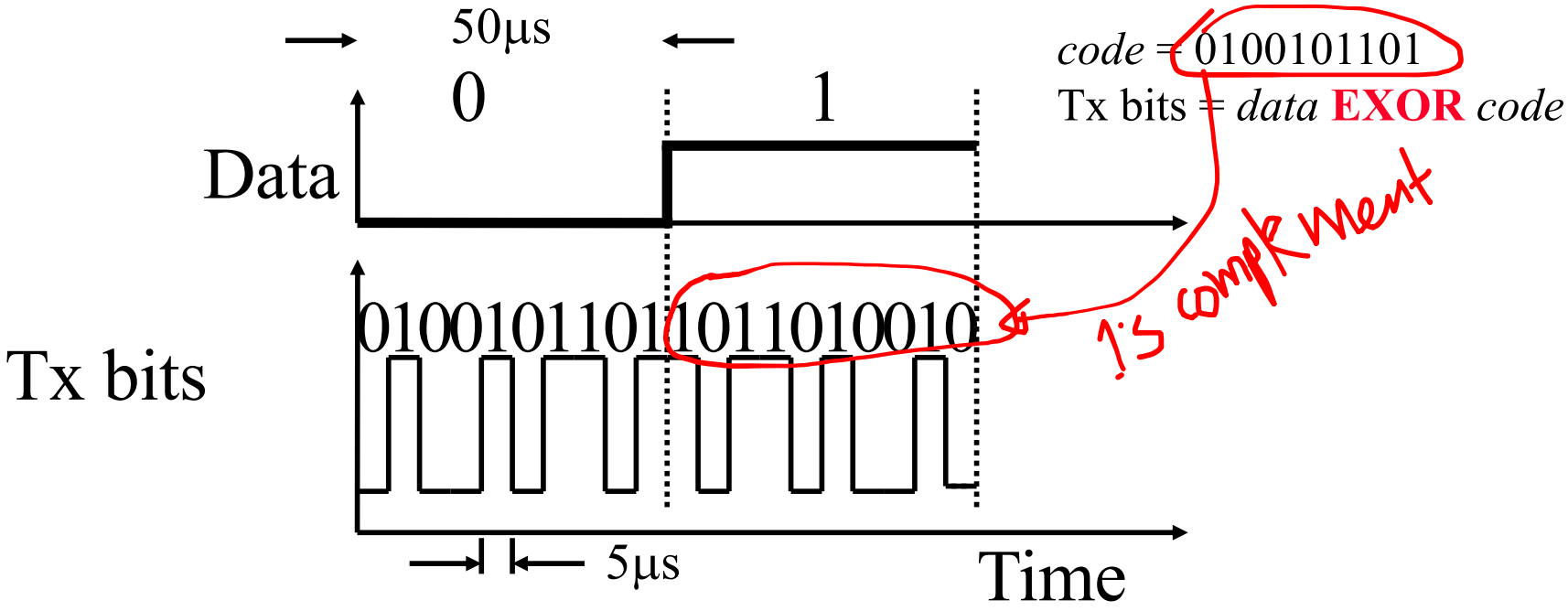
©2020 Mahbub Hassan

FHSS Advantages and Disadvantages

- Advantages
  - Difficult to intercept (appears as random ‘blips’)
  - Narrowband interference can't jam
- Disadvantages
  - Requires increased bandwidth (ability to randomly hop between 1000 frequencies → 1000 more bandwidth)
  - Both time and frequency synchronization

©2020 Mahbub Hassan

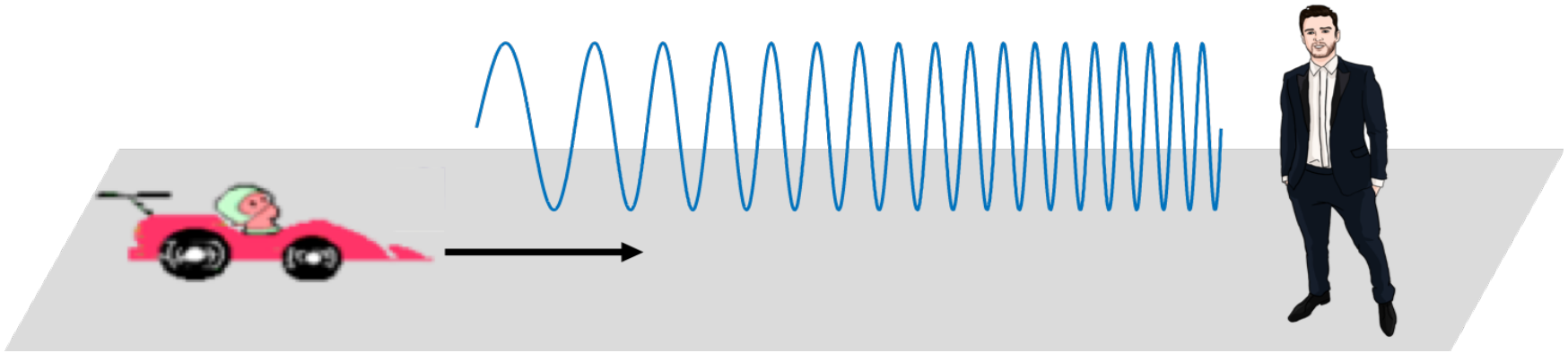
Direct-Sequence Spread Spectrum



- Many bits are transmitted for each data bit
- Spreading factor = Code bits/data bit, 10-100 commercial (Min 10 by FCC), 10,000 for military
- Signal bandwidth >10 × data bandwidth
- Code sequence synchronization
- Correlation between codes ⇒Interference (Orthogonal to avoid interference)

©2020 Mahbub Hassan

Doppler Shift



- If the transmitter or receiver or both are mobile the frequency of received signal changes
- Moving towards each other ⇒ Frequency increases
- Moving away from each other ⇒ Frequency decreases

Frequency difference = velocity/Wavelength = $v/\lambda = vf/c$

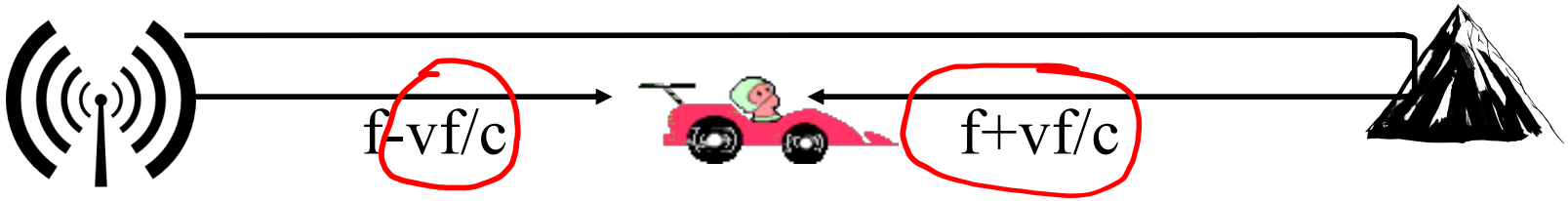
Example: 2.4 GHz ⇒ $\lambda = 3\text{x}10^8/2.4\text{x}10^9 = 0.125\text{m}$

v = 120km/hr = 120x1000/3600 = 33.3 m/s

Freq diff (Doppler shift) = 33.3/0.125 = 267 Hz

©2020 Mahbub Hassan

Doppler Spread and Coherence Time



- Two rays will be received (*original+reflection*)
- **Doppler Spread** = 2vf/c = 2 × Doppler shift
- They will add or cancel-out each other as the receiver moves
- **Coherence time**: Time during which the channel response is constant = 1/Doppler spread = $c/2vf = \lambda/2v$

©2020 Mahbub Hassan

Example

- What is the *coherence time* for a 2.4 GHz wifi link connecting a car travelling at 72 km/hr?

V=(72 x 1000)/3600 = 20 m/s

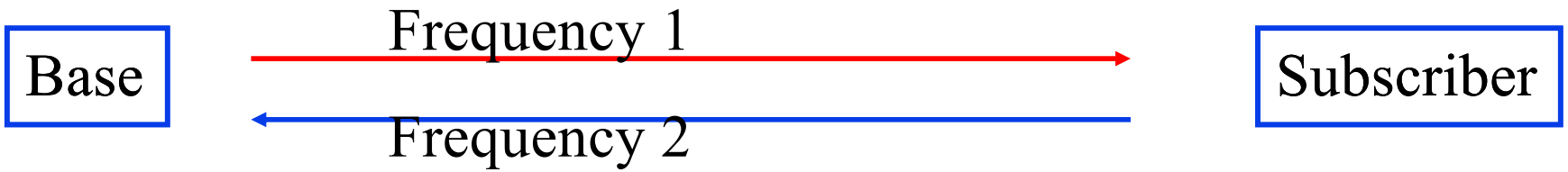
Doppler spread = $2vf/c$ = $(2 \times 20 \times 2.4 \times 10^9)/(3 \times 10^8)$ = 320 Hz

Coherence time = 1/320 = 0.003125 s = 3.125 ms

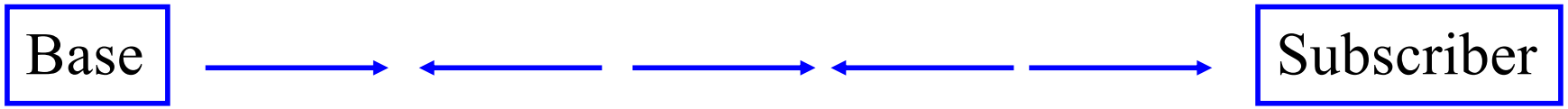
©2020 Mahbub Hassan

Duplexing

- Duplex = Bi-Directional Communication
- Frequency division duplexing (FDD) (Full-Duplex)



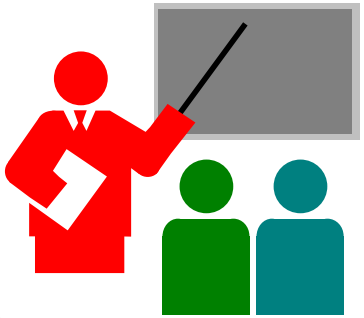
- Time division duplex (TDD): Half-duplex



- Many LTE deployments will use TDD.
  - Allows more flexible sharing of DL/UL data rate
  - Does not require paired spectrum
  - Easy channel estimation ⇒ Simpler transceiver design
  - Con: All neighboring BS should time synchronize

©2020 Mahbub Hassan

Summary



1. Electric, Radio, Light, X-Rays, are all electromagnetic waves
2. Wavelength and frequency are inversely proportional (wavelength = c/f)
3. Historically, wireless communications mostly used frequencies below 6 GHz, but beyond 6 GHz is actively explored in modern wireless networks.
4. Hertz and bit rate are related by Nyquist and Shannon's Theorems
5. Nyquist's theorem explains capacity for noiseless channels
6. Shannon's capacity takes SNR into consideration
7. By spreading the original signal bandwidth over a much wider band, spread spectrum can provide better immunity against interference and jamming as well allowing multiple parties to communicate over the same frequency at the same time.
8. FHSS and DSSS are two fundamental methods of realizing spread spectrum
9. Doppler effect explains the shift in frequency experienced by mobile objects
10. Doppler spread is twice the Doppler shift
11. Channel coherence time is inversely proportional to doppler spread
12. FDD and TDD are two fundamental methods of resource allocation between the transmitter and the receiver so they both can exchange information with each other

©2020 Mahbub Hassan

Wireless LAN I

IEEE 802.11 Basics

©2020 Mahbub Hassan

Overview

1. IEEE 802.11 vs. WiFi
2. IEEE Standards Numbering System
3. Key features of 802.11
4. 802.11 Bands and Channels
5. Hidden Node Problem and 4-Way Handshake RTS/CTS)
6. 802.11 MAC (inter-frame space, PCF, DCF)
7. 802.11 Architecture and Addressing
8. 802.11 Frame Format
9. 802.11 Power Management

©2020 Mahbub Hassan

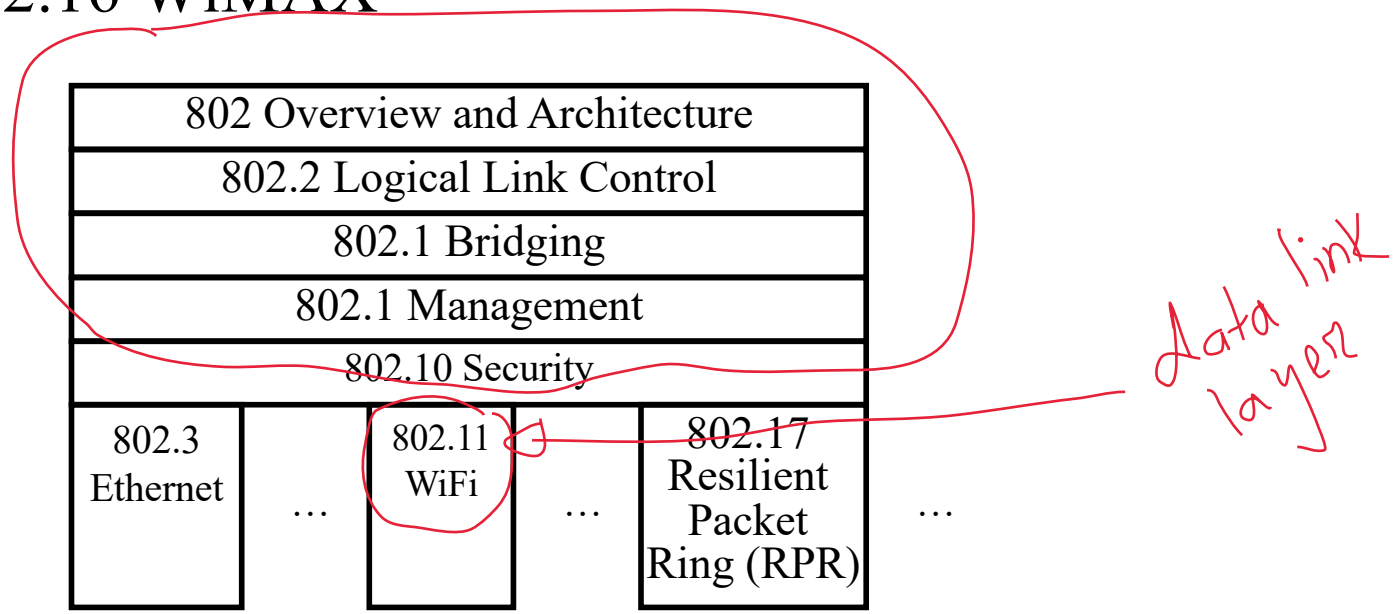
IEEE 802.11 vs. WiFi

- IEEE 802.11 is a standard
- WiFi = "Wireless Fidelity" is a trademark
- Fidelity = **Compatibility** between wireless equipment from different manufacturers
- WiFi Alliance is a non-profit organization that does the compatibility testing (WiFi.org)
- 802.11 has many options and it is possible for two equipment based on 802.11 to be *incompatible*.
- All equipment with "WiFi" logo have selected options such that they will **interoperate**.

©2020 Mahbub Hassan

IEEE Standards Numbering System

- IEEE 802.* and IEEE 802.1* standards (e.g., IEEE 802.1Q-2011) apply to all IEEE 802 technologies:
  - IEEE 802.3 Ethernet
  - IEEE 802.11 WiFi
  - IEEE 802.16 WiMAX



©2020 Mahbub Hassan

Lettered vs. Numerical Versions

- IEEE 802.11 uses *letters* to name the versions
  - E.g., 802.11a/b (1999), 802.11g (2003), 802.11n (2009), 802.11ac (2013), and so on
- WiFi Alliance proposes numbers to simplify
  - E.g., WiFi 4 (802.11n), WiFi 5 (802.11ac), WiFi 6 (802.11ax) … 7

©2020 Mahbub Hassan

IEEE 802.11 Features

- Data rate (a.k.a. *speed*)
  - Original IEEE 802.11-1997 was at 1 and 2 Mbps.
  - Newer versions at 11 Mbps, 54 Mbps, 108 Mbps, 1.2 Gbps, …
- Spectrum licensing
  - All versions use *license-exempt* spectrum

do not have to pay for spectrum use

- PHYs:
  - Spread spectrum (in old versions)

FHSS
DSSS

  - OFDM (in new versions)

voip
video
game
Zoom

- Supports multiple priorities (time-critical and data traffic)
- Power management allows a node to `doze off'
  - Longer battery life

one coin cell battery for 10 years for some sensors

©2020 Mahbub Hassan

IEEE 802.11 Physical Layers

- Issued in several stages
- First version in 1997: Legacy IEEE 802.11 (no longer used)
  - 3 physical layer specifications (2 in 2.4-GHz, 1 in infrared)
  - All operating at 1 and 2 Mbps
- Amendments in 1999:
  - IEEE 802.11a-1999: 5-GHz band, 54 Mbps/20 MHz, **OFDM**
  - IEEE 802.11b-1999: 2.4 GHz band, 11 Mbps/22 MHz (spread spectrum)
- Amendment in 2003:
  - IEEE 802.11g-2003 : 2.4 GHz band, 54 Mbps/20 MHz, **OFDM**

©2020 Mahbub Hassan

ISM Bands

- **I**ndustrial, **S**cientific, and **M**edical bands. **License exempt**

From	To	Bandwidth	Availability
6.765 MHz	6.795 MHz	30 kHz	
13.553 MHz	13.567 MHz	14 kHz	Worldwide
26.957 MHz	27.283 MHz	326 kHz	Worldwide
40.660 MHz	40.700 MHz	40 kHz	Worldwide
433.050 MHz	434.790 MHz	1.74 MHz	Europe, Africa, Middle east, Former Soviet Union
902.000 MHz	928.000 MHz	26 MHz	America, Greenland
2.400 GHz	**2.500 GHz**	**100 MHz**	**Worldwide**
5.725 GHz	**5.875 GHz**	**150 MHz**	**Worldwide**
24.000 GHz	24.250 GHz	250 MHz	Worldwide
61.000 GHz	61.500 GHz	500 MHz	
122.000 GHz	123.000 GHz	1 GHz	
244 GHz	246 GHz	2 GHz	

Ref: http://en.wikipedia.org/wiki/ISM_band

©2020 Mahbub Hassan

main stream

WLAN/WiFi Bands

WLAN/WiFi Standard	Frequency Band
802.11b/g/n	**2.4 GHz**
802.11a/n/ac/ax	**5 GHz**
802.11p (car-to-car)	5.9 GHz (licensed band)
802.11ah (IoT)	900 MHz
802.11af (Rural)	700 MHz (unused TV channels)
802.11ad/ay (Multi Gbps wireless applications: e.g., cable replacement, VR, …)	60 GHz

niche

©2020 Mahbub Hassan

WiFi Channels

- The entire *band* is divided into several individual *channels*
- An AP operates over a **single channel** at any given time
- Different nearby APs can operate over different channels of the same band
  - Avoid congestion and interference
- Each channel is usually 20 or 22 MHz wide
- With newer WiFi versions, it is possible to combine two or more channels to get a wider channel
  - More bandwidth for higher data rates

only make sense when there is less interference from nearby AP (less densely populated wifi area)

©2020 Mahbub Hassan

2.4 GHz WiFi Channel Frequencies

- A total of 14 channels (not all channels available in all countries)
- Centre frequencies are 5 MHz apart (except channel 14)
- Each channel is 22 MHz wide

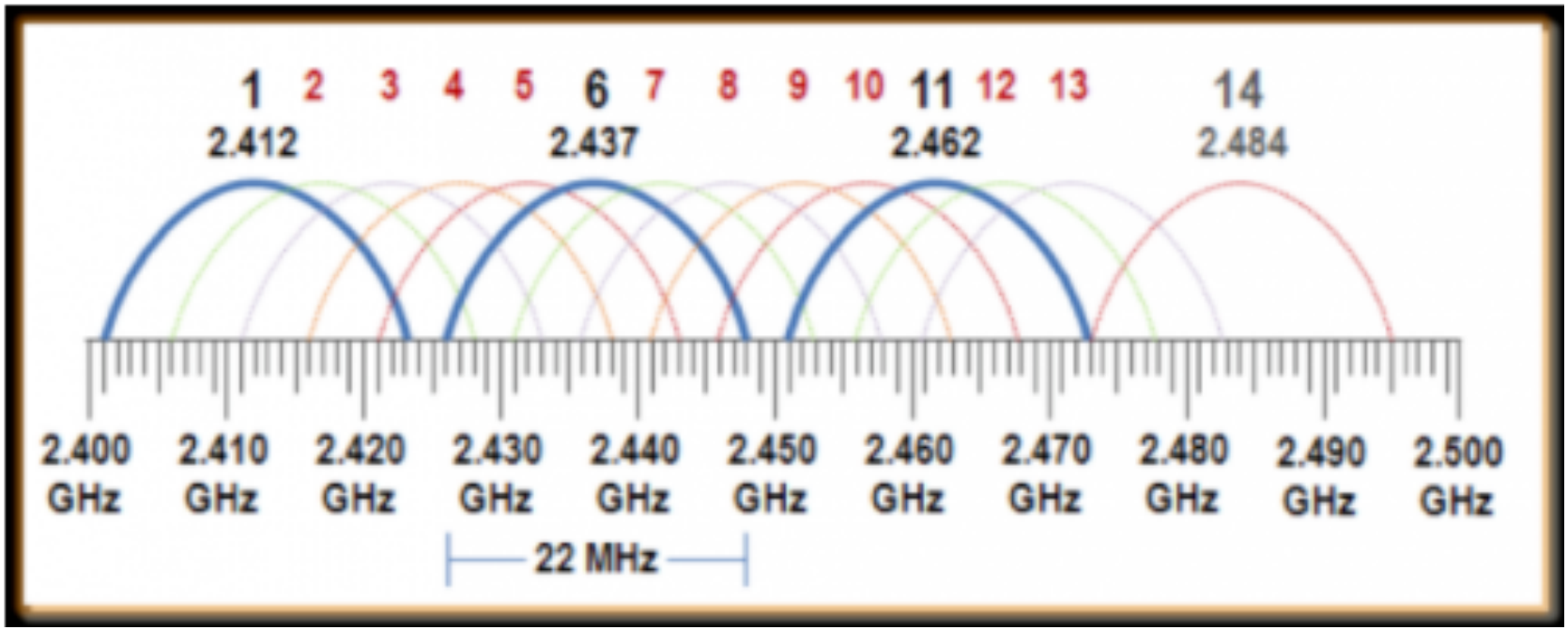
CHANNEL NUMBER	LOWER FREQUENCY MHZ	CENTER FREQUENCY MHZ	UPPER FREQUENCY MHZ
1	2401	2412	2423
2	2406	2417	2428
3	2411	2422	2433
4	2416	2427	2438
5	2421	2432	2443
6	2426	2437	2448
7	2431	2442	2453
8	2436	2447	2458
9	2441	2452	2463
10	2446	2457	2468
11	2451	2462	2473
12	2456	2467	2478
13	2461	2472	2483
14	2473	2484	2495

From http://www.radio-electronics.com/info/wireless/wi-fi/80211-channels-number-frequencies-bandwidth.php

©2020 Mahbub Hassan

2.4 GHz Channel Overlaps

- Most channels in 2.4 GHz band overlap
- Maximum of three non-overlapping channels are possible
- 1-6-11 are most widely used non-overlapping channels (6 is usually default)
  - E.g., if three are three nearby APs in an enterprise, they are usually set to 1-6-11



From http://boundless.aerohive.com/experts/WLAN-Channels-Explained.html

©2020 Mahbub Hassan

Channels in 5 GHz Band

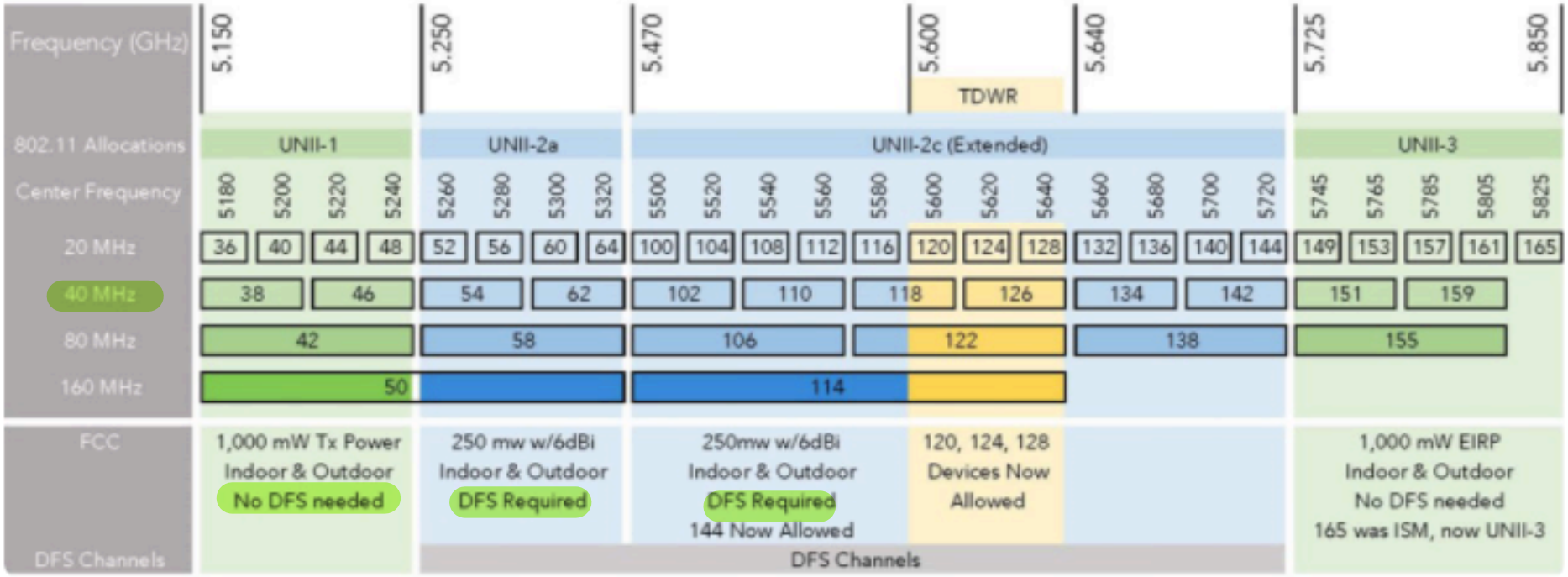
- 20 MHz channels (c.f. 22 MHz in 2.4 GHz band)
- Non-overlapping (c.f., mostly overlapping in 2.4 GHz)
- Two types of channels
  - Always available
  - Channels used by **radar** (requires DFS)
- Dynamic Frequency Selection (DFS): WiFi AP monitors radar channels and vacate them (switch to another channel) if radar is detected
  - May cause connection drop for clients

wifi protocol has mechanisms for AP to notify the client that a channel switch is imminent

©2020 Mahbub Hassan

5GHz Channel Structure

5 GHz Channel Allocations

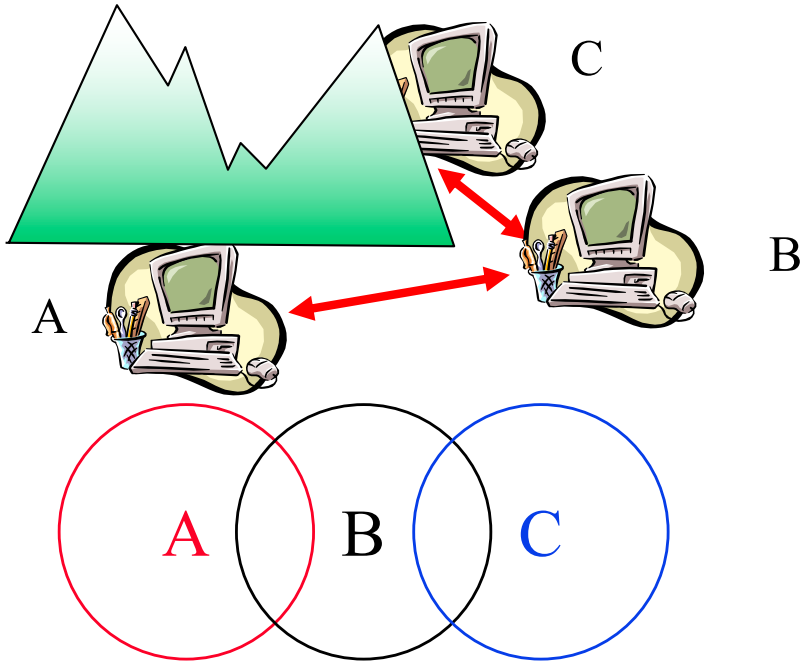


Source: Wireless LAN Professionals

Source: https://www.ekahau.com/blog/channel-planning-best-practices-for-better-wi-fi/ (accessed 15 June 2020): this structure is probably for the US; radar channels may vary with countries

©2020 Mahbub Hassan

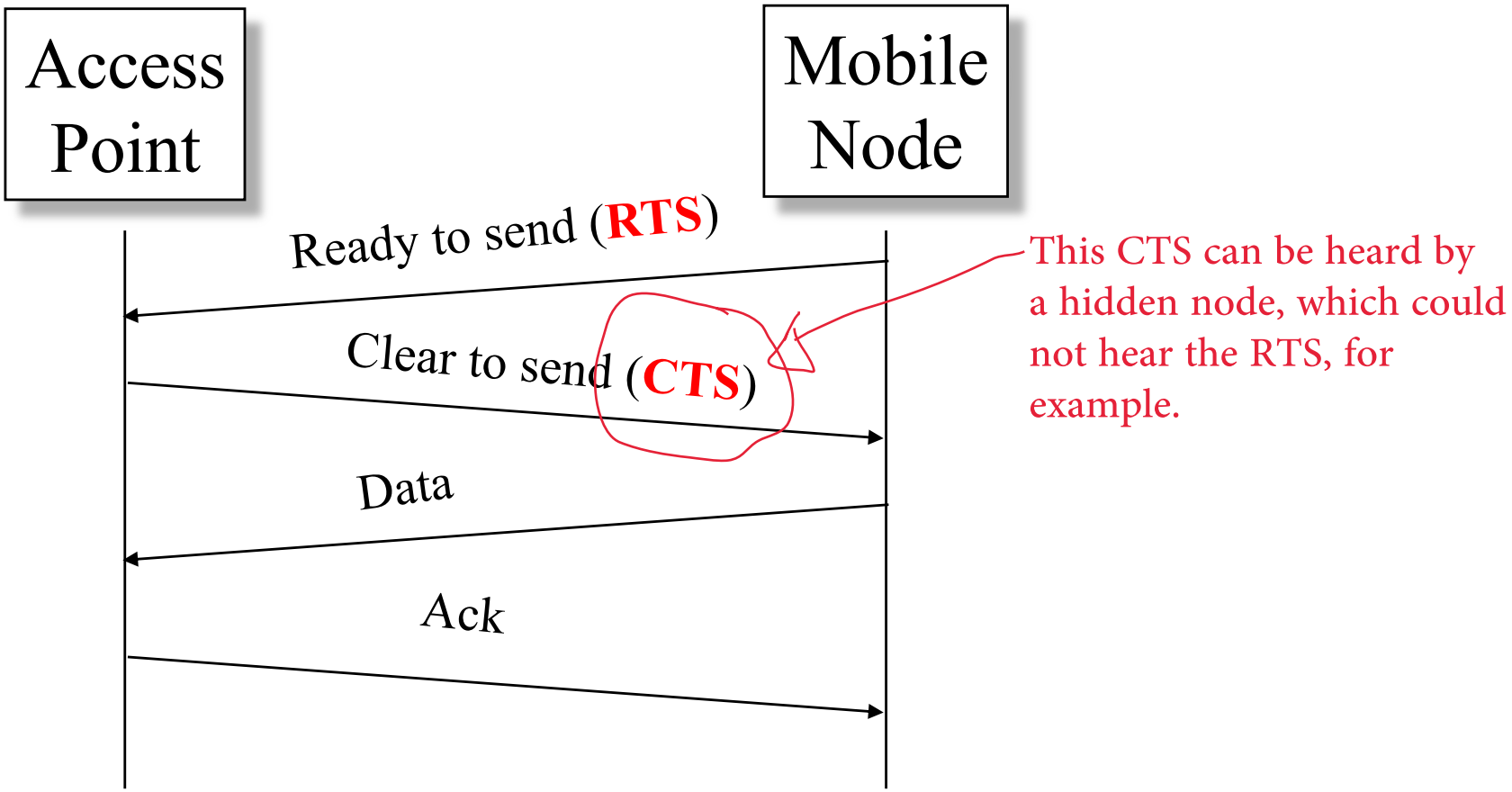
Hidden Node Problem



- A can hear B, B can hear C, but C cannot hear A (C and A are *hidden* from each other)
- C may start transmitting while A is also transmitting → collision at B!
  - A and C (wireless transmitters) can't detect collision (why?).
- CSMA/CD is not possible (CD = collision detection; CD used in Ethernet)
  → in WLAN, only the receiver can help *avoid* collisions
- 4-way handshake needed to implement CA (*collision avoidance*) in WLAN

©2020 Mahbub Hassan

4-Way Handshake



©2020 Mahbub Hassan

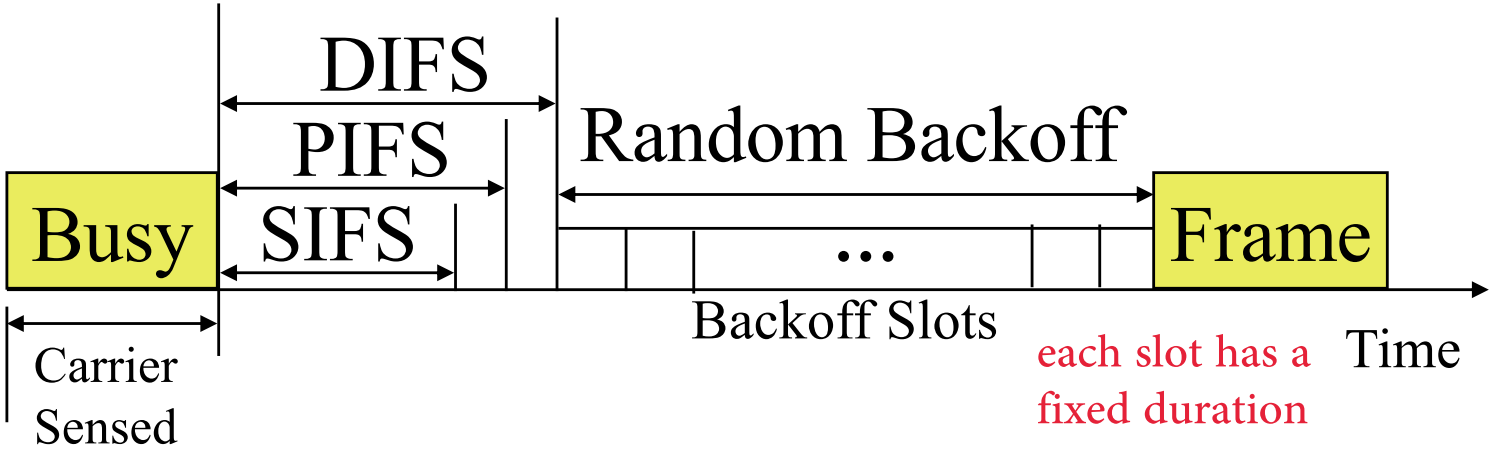
IEEE 802.11 MAC

- Carrier Sense Multiple Access with Collision Avoidance (**CSMA/CA**)
- Listen before you talk. If the medium is busy, the transmitter backs off for a random period.
- Avoids collision by sending a short message:
  Ready to send (**RTS**)
  RTS contains dest. address and duration of message.
  Tells everyone to backoff for the duration.

  for the entire 4-way handshake, i.e., end of the ACK.
- Destination sends: Clear to send (**CTS**)
  Other stations set their network allocation vector (**NAV**) and wait for that duration
- Cannot detect collision, hence each packet is acked.
- MAC-level retransmission if not acked.

©2020 Mahbub Hassan

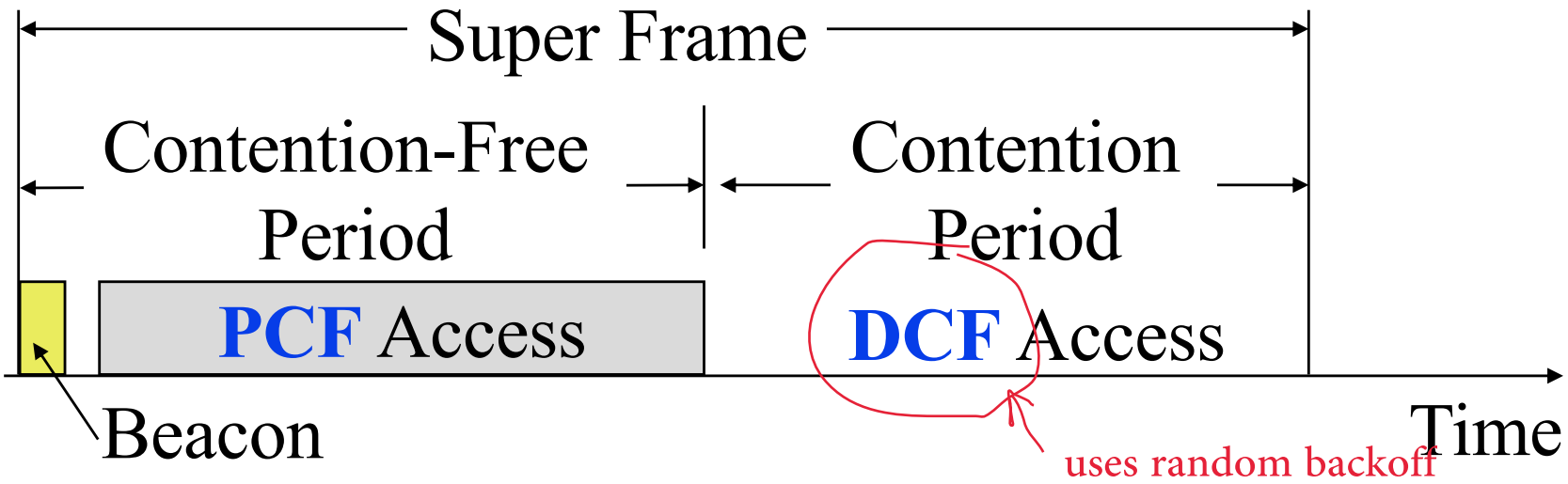
IEEE 802.11 Priorities with Inter-frame space



- 802.11 has different priorities for **control**, **data**, and **time-critical** packets
- Achieve priorities by using different amounts of interframe space (IFS)
- Highest priority frames, e.g., Acks, use short IFS (**SIFS)**
- Medium priority time-critical frames use "Point Coordination Function IFS" (**PIFS**)
- Asynchronous data frames use "Distributed coordination function IFS" (**DIFS**)

©2020 Mahbub Hassan

Time Critical Services



- Timer critical services use **Point Coordination Function**
- The point coordinator allows only one station to access
- Coordinator sends a beacon frame to all stations.
  Then uses a polling frame to allow a particular station to have contention-free access
- Contention Free Period (CFP) varies with the load.

©2020 Mahbub Hassan

IEEE 802.11 DCF Backoff

- MAC works with a single FIFO Queue
  - Focuses on transmitting the packet at the head of the queue
- Three variables:
  - Contention Window (CW)
  - Backoff count (BO)
  - Network Allocation Vector (NAV)
- If a frame (RTS, CTS, Data, Ack) is heard, NAV is set to the duration in that frame. Stations sense the media after NAV expires.
- If the medium is idle for DIFS, and backoff (BO) is not already active, the station draws a random BO in [0, CW] and sets the backoff timer.
  - CW is in units of *slot time* (slot time varies with 802.11 standards)
- If the medium becomes busy during backoff, the timer is paused and a new NAV is set. After NAV, back off continues.

©2020 Mahbub Hassan

IEEE 802.11 DCF Backoff (Cont)

if you increase CW, BO will choose a random number from a wider interval

- BO = *random*(0,CW)
- Initially and after each *successful* transmission:

$$CW = CW_{min}$$

- After each *unsuccessful* attempt

$$CW = \min\{2CW + 1, CW_{max}\}$$

©2020 Mahbub Hassan

Example

- Assume that we have CWmin=3 and CWmax=127 configured for a given WLAN. What would be the values of CW if there were 8 successive unsuccessful attempts after initalizing the network?

After initialization, CW = CWmin = 3

3x2+1

After 1st unsuccessful attempt, CW = min(7,127) = 7

7x2+1

After 2nd unsuccessful attempt, CW = min(15,127) = 15

Then on, 31, 63, 127, 127, 127, …

at 5th attempt you reach the maximum

©2020 Mahbub Hassan

Parameter Values: interframe space and contention window

WLAN	Slot-time (µs)	SIFS (µs)	CWmin	CWmax
11a	9	16	15	1023
11b	20	10	31	1023
11g	9 or 20	10	15 or 31	1023
11n (2.4 GHz)	9 or 20	10	15	1023
11n (5 GHz)	9	16	15	1023
11ac	9	16	15	1023

- PIFS = SIFS + 1 slot time
- DIFS = SIFS + 2 slot times = PIFS + 1 slot time

Slot time: basic unit of backoff algorithm

©2020 Mahbub Hassan

Example

- What is the duration of PIFS and DIFS for IEEE 802.11b?

Slot time = 20 μs

SIFS = 10 μs

PIFS = SIFS + slot time = 10+20 = 30 μs

DIFS = SIFS + 2 x slot time = 10 + 40 = 50 μs

©2020 Mahbub Hassan

Virtual Carrier Sense

does not consume battery (unlike physical)

- Every frame has a "Duration ID" which indicates how long the medium will be busy.
  - RTS has duration of RTS + SIF + CTS + SIF + Frame + SIF + Ack
  - CTS has duration of CTS + SIF + Frame + SIF + Ack
  - Frame has a duration of Frame + SIF + ACK
  - ACK has a duration of ACK
  - A station has to estimate the durations of RTS/CTS/ACK
- All stations keep a "**Network Allocation Vector (NAV)**" timer in which they record the duration of each frame they hear.
- Stations do not need to sense the channel until NAV becomes zero (conserve power)

©2020 Mahbub Hassan

Example

SIFS = 10 micro sec

- Consider an 802.11b WLAN. A station estimates the transmission times of RTS, CTS, and ACK as 10 μs, 10 μs, and 25 μs, respectively. What would be the value of the Duration field in the RTS header if the station wants to send a 250 μs long data frame ?

802.11b has a SIFS duration of 10 μs.

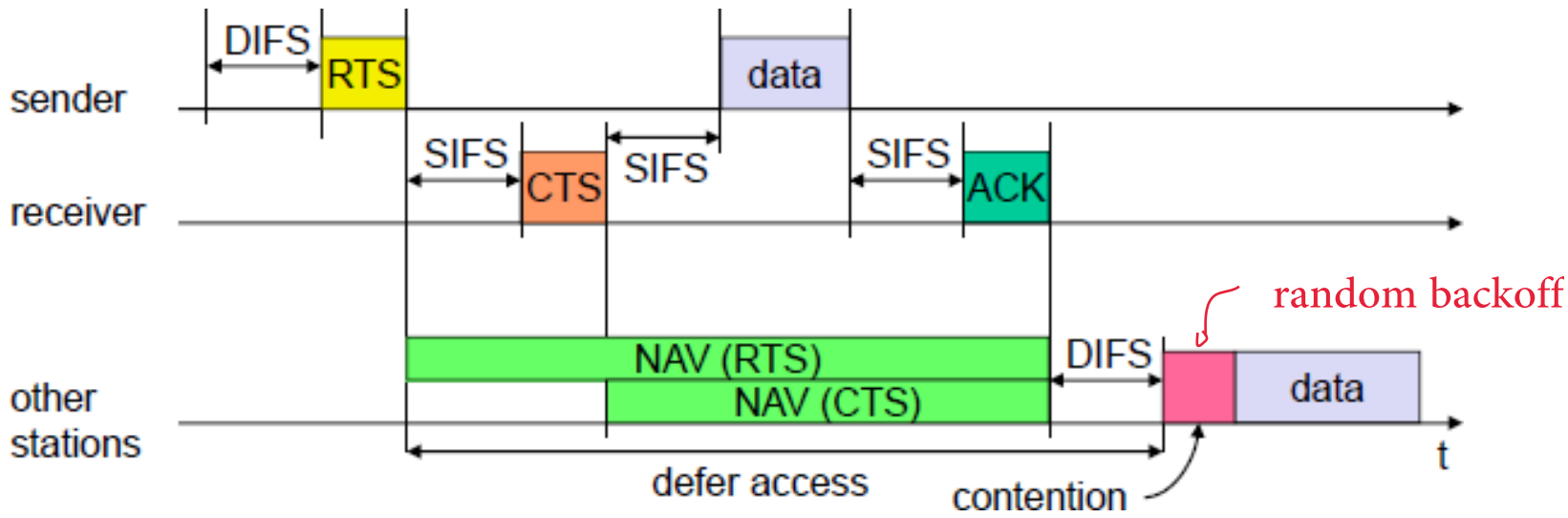
Duration field in RTS = RTS_time + CTS_time + ACK_time + data_time + 3xSIFS

= 10+10+25+250+3x10 = 325 μs

©2020 Mahbub Hassan

802.11 with RTS/CTS

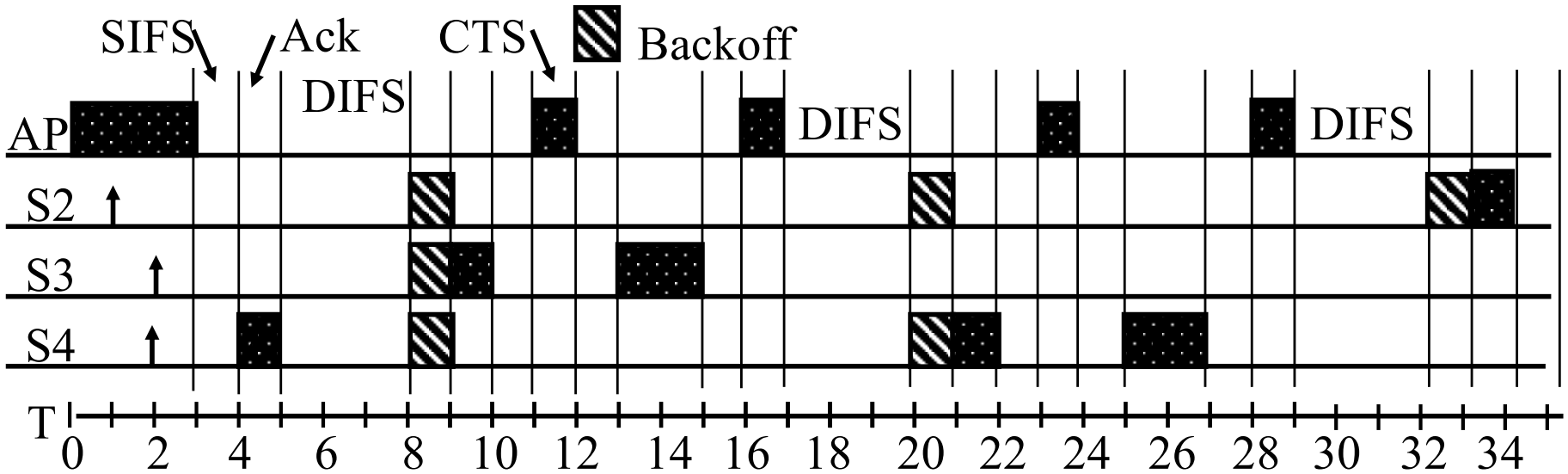
When a node is sensing the channel, it must be free for DIFS period. SIFS is used as the wait time between the RTS, CTS, DATA and ACK frames. SIFS < DIFS means that another node cannot incorrectly determine that the channel is idle during the 4-way handshake between two other nodes.



©2020 Mahbub Hassan

DCF Example

- Example: Slot Time = 1, CWmin = 5, DIFS=3, PIFS=2, SIFS=1
- T=1 Station 2 wants to transmit but the media is busy
- T=2 Stations 3 and 4 want to transmit but the media is busy
- T=3 Station 1 finishes transmission. AP
- T=4 Station 1 receives ack for its transmission (SIFS=1)
  Stations 2, 3, 4 set their NAV to 1.
- T=5 Medium becomes free
- T=8 DIFS expires. Stations 2, 3, 4 draw backoff count between 0 and 5. CWmin
  The counts are 3, 1, 2

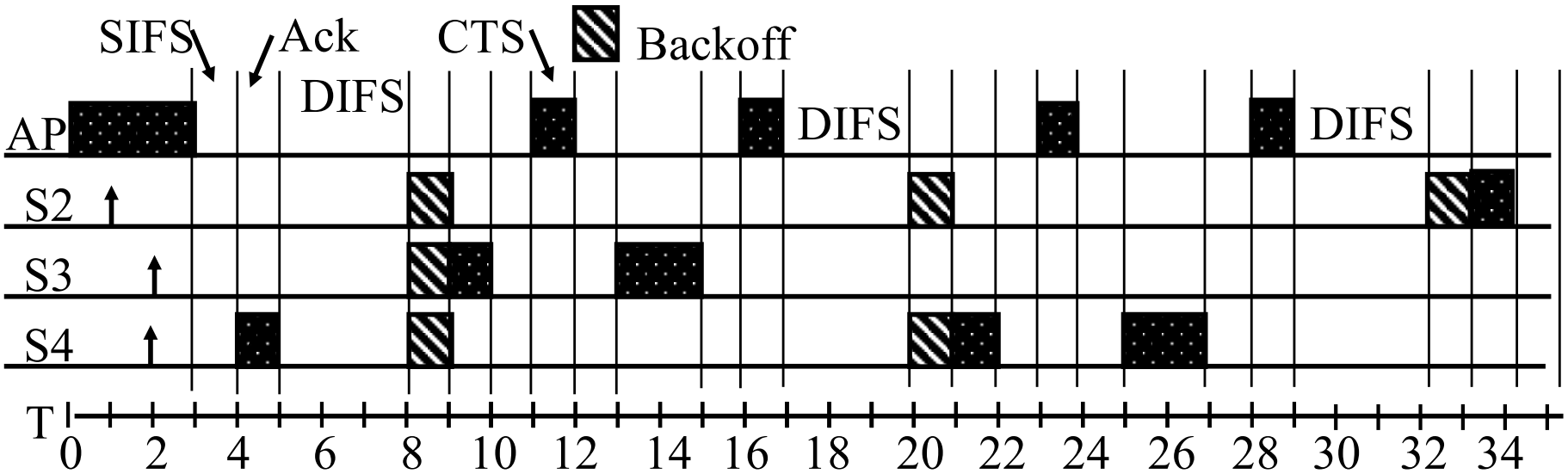


©2020 Mahbub Hassan

DCF Example (Cont)

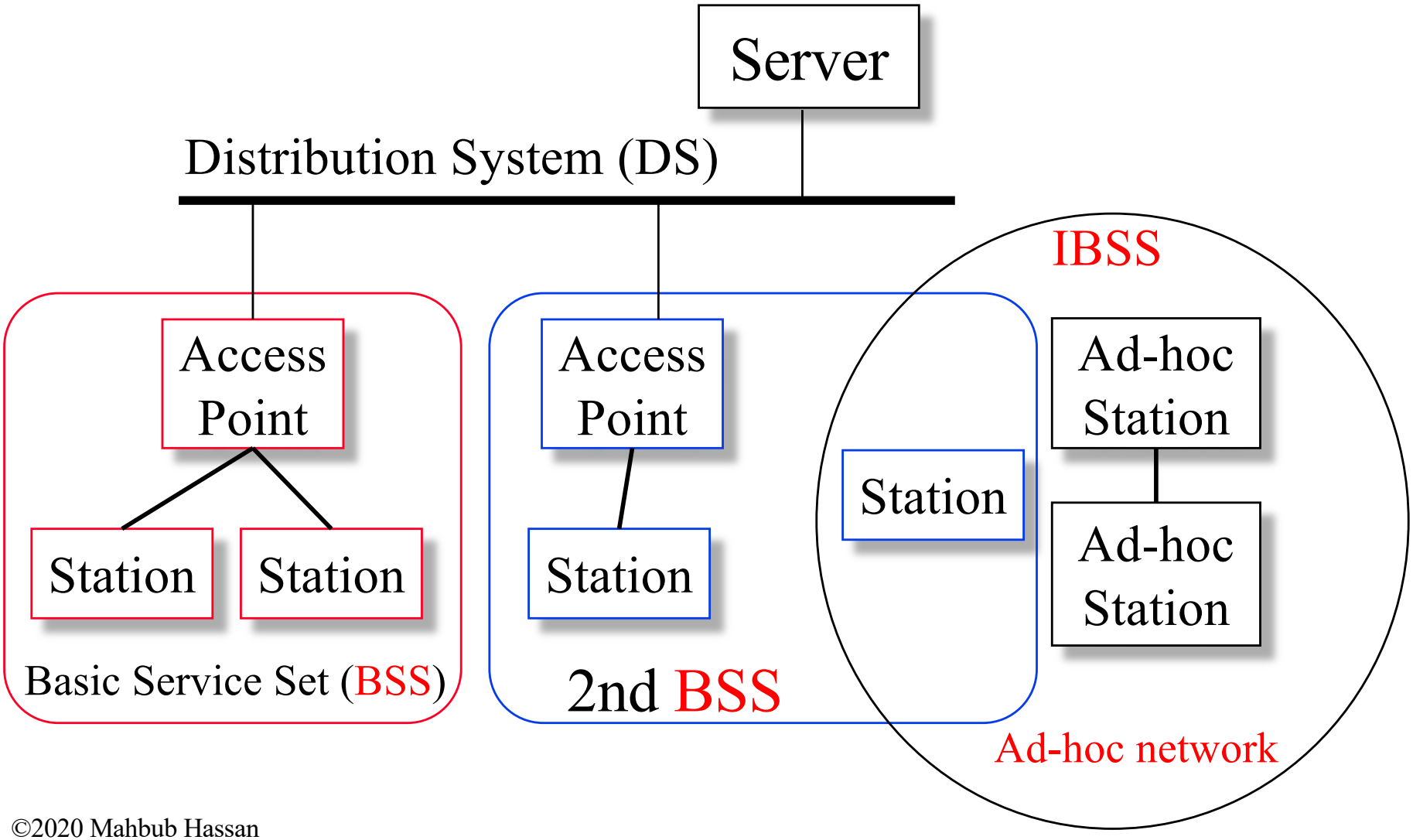
- T=9 Station 3 starts transmitting. Announces a duration of 8 (RTS + SIFS + CTS + SIFS + DATA + SIFS + ACK). Station 2 and 4 pause backoff counter at 2 and 1 resp. and wait till T=17 9+8 = 17
- T=15 Station 3 finishes data transmission
- T=16 Station 3 receives Ack.
- T=17 Medium becomes free
- T=20 DIFS expires. Station 2 and 4 notice that there was no transmission for DIFS. Stations 2 and 4 start their backoff counter from 2 and 1, respectively. resume backoff with the remaining values
- T=21 Station 4 starts transmitting RTS

backoff ends for station 4



©2020 Mahbub Hassan

IEEE 802.11 Architecture



©2020 Mahbub Hassan

IEEE 802.11 Architecture (Cont)

- **Basic Service Set (BSS)**
  = Set of stations associated with one AP
- **Distribution System (DS)** - wired backbone
- **Independent Basic Service Set (IBSS)**: Set of computers in **ad-hoc mode**. May not be connected to wired backbone.
- Ad-hoc networks coexist and interoperate with infrastructure-based networks
- BSSID: 48-bit MAC address of the AP radio
- IBSSID: randomly generated address
  - 2 bits are fixed, 46 bits are generated randomly
- All-1s BSSID/IBSSID is used for broadcast

©2020 Mahbub Hassan

Frame Format

Frame Control	Duration/ ID	Adr 1	Adr 2	Adr 3	Seq Control	Adr 4	Info	CRC
16b	16b	48b	48b	48b	16b	48b		32b

Prot. Ver.	Type	Sub type	To DS	From DS	More Frag.	Retry	Power mgt	More Data	WEP	Order
2b	2b	4b	1b	1b	1b	1b	1b	1b	1b	1b

- Type: Control, management, or data
- Sub-Type: Association, disassociation, re-association, probe, authentication, de-authentication, CTS, RTS, Ack, Power-Save Poll (PS-POLL) …
- Retry/retransmission
- Power mgt: Going to Power Save mode
- More Data: More buffered data at AP for a station in power save mode
- WEP: Wireless Equivalent Privacy (Security) info in this frame
- Order: Strict ordering

©2020 Mahbub Hassan

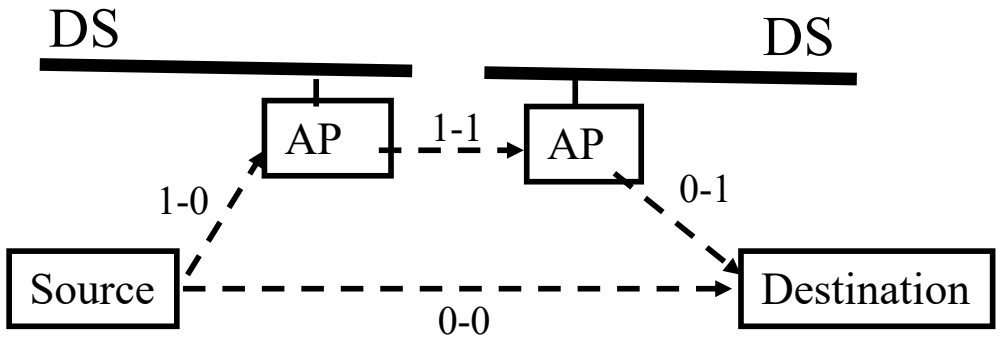
MAC Frame Fields

- **Duration/Connection ID**:
  - If used as duration field, indicates time (in μs) channel will be allocated for successful transmission of MAC frame. Includes time until the end of Ack
  - In some control frames, contains association or connection identifier
- **Sequence Control**:
  - 4-bit fragment number subfield
    - For fragmentation and reassembly
  - 12-bit sequence number
  - Number frames between given transmitter and receiver

©2020 Mahbub Hassan

802.11 Frame Address Fields – data frames

- Source/Destination: ultimate network devices that prepare and decode the frame for network layer
- Transmitter(Tx)/Receiver(Rx): Could be the source/destination, or intermediate radio devices, e.g., access point (AP)
- 4 address fields; defined by 2 DS bits

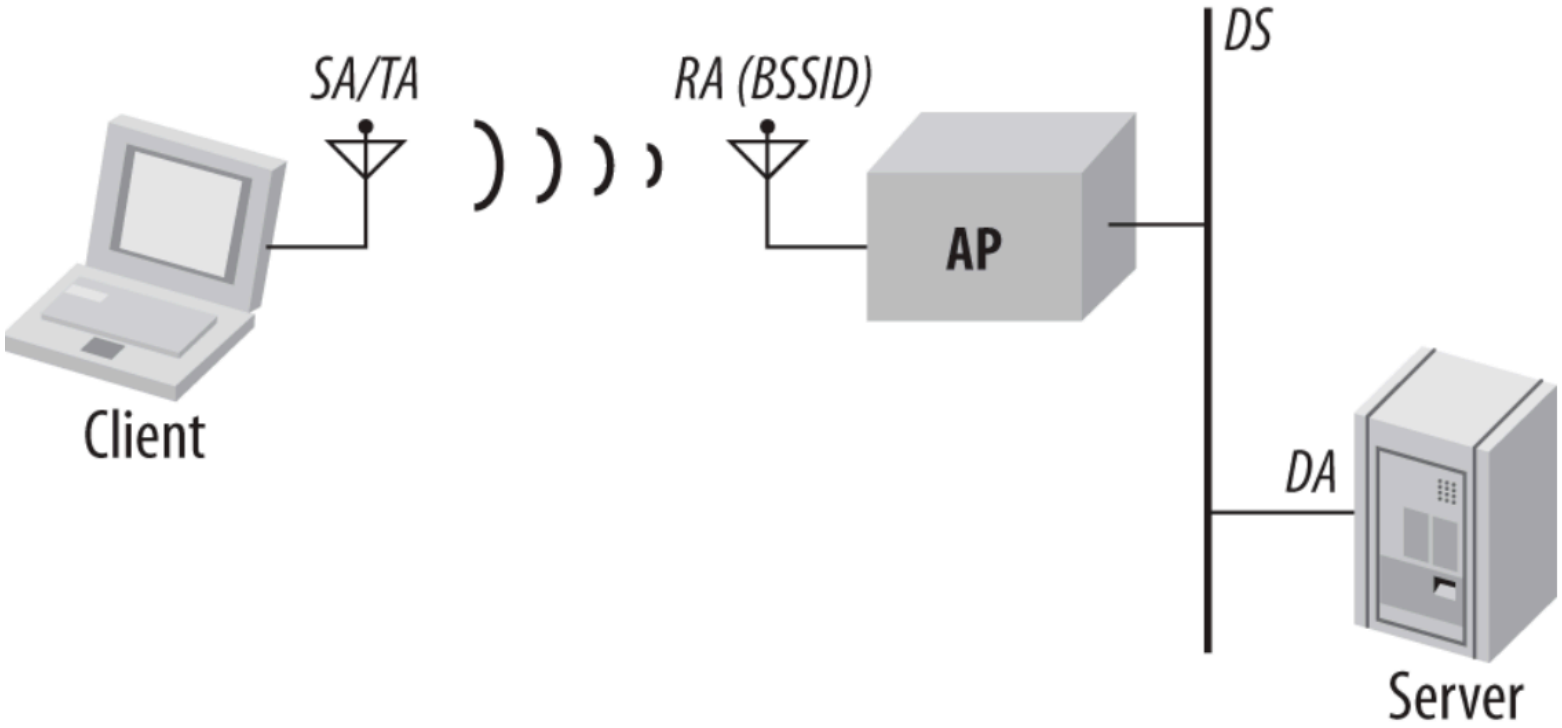


"WiFi Address Table"

Purpose	ToDS	FromDS	ADR1 (Rx)	ADR2 (Tx)	ADR3	ADR4
IBSS	0	0	DA	SA	IBSSID	N/A
From AP (from infra.)	0	1	DA	BSSID	SA	N/A
To AP (to infra.)	1	0	BSSID	SA	DA	N/A
AP-to-AP (W'less Brdg)	1	1	RxA	TxA	DA	SA

©2020 Mahbub Hassan

Example 802.11 Addressing: Wireless Client to Server



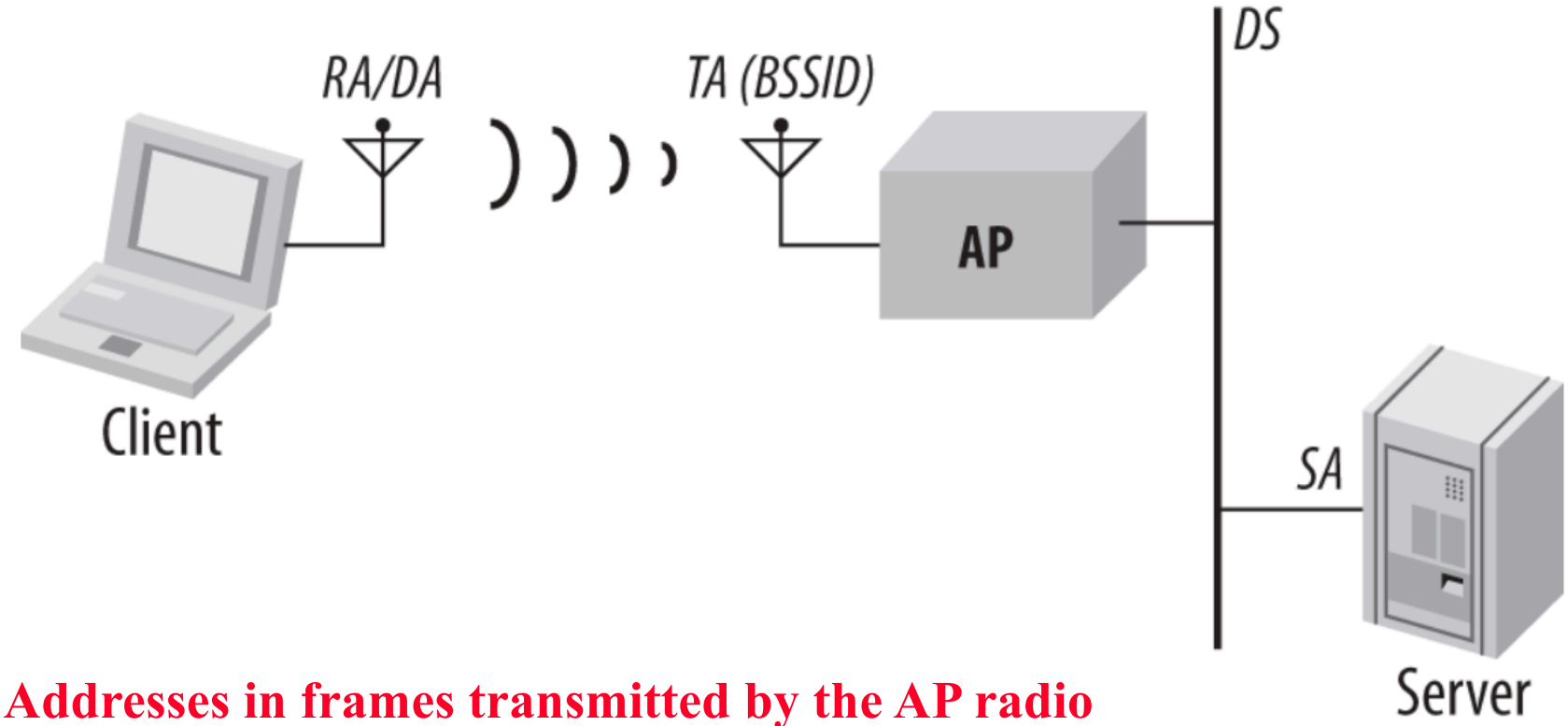
Addresses in frames transmitted by the client radio

ADR1: AP MAC address (BSSID)
ADR2: Client MAC address (source address)
ADR3: Server MAC address (destination address)
ADR4: Not applicable

From Row3 of "WiFi Address Table" shown in previous slide

©2020 Mahbub Hassan

Example 802.11 Addressing: Server to Wireless Client



Addresses in frames transmitted by the AP radio

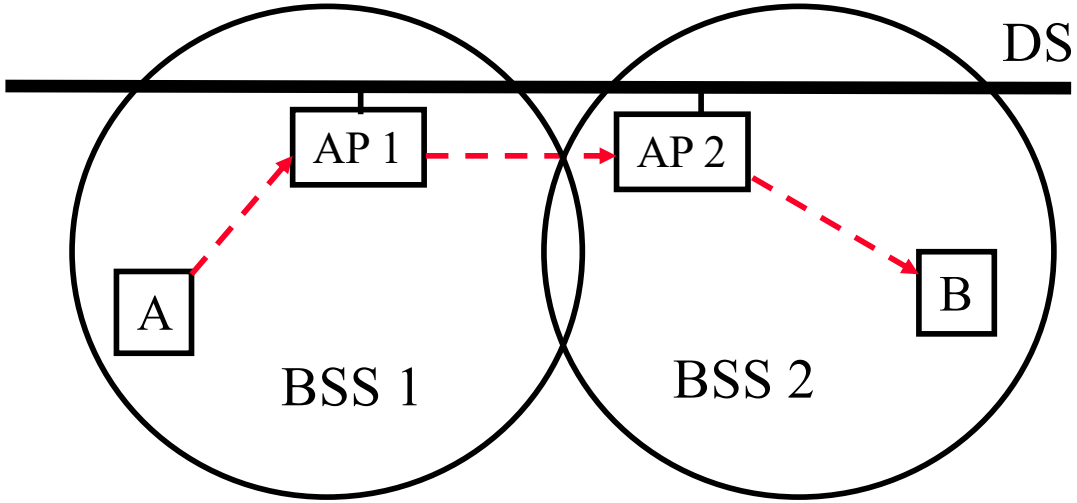
ADR1: Client MAC address (destination address)
ADR2: AP MAC address (BSSID)
ADR3: Server MAC address (source address)
ADR4: Not applicable

From Row2 of "WiFi Address Table"

©2020 Mahbub Hassan

Example 802.11 addressing

- Consider the example WLAN in the figure where two BSSs are connected via a distribution system. What is the content of the Address 3 field when Station A wants to send a packet to Station B via AP 1?



- In this case (To DS=1, From DS=0), Address 3 field should contain the address of the destination station. Therefore, it should be the address of B.

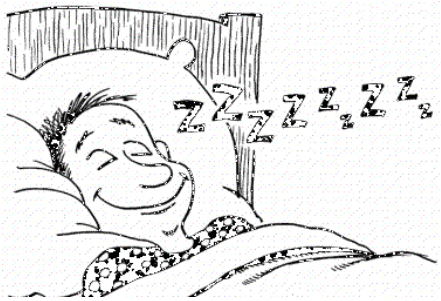
©2020 Mahbub Hassan

Power Saving

- Extending the battery life of portable devices is one of the main challenges of wireless networks.
- Mechanisms must be devised to let the device sleep as much as possible and wake up only when it needs to transmit or receive.
- If there are no packets to be received, a receiver could go to sleep and save battery power.
- To facilitate this kind of power saving, IEEE 802.11 has a power management function.

©2020 Mahbub Hassan

802.11 Power Management



- Station tells the base station its mode:
  Power saving (PS) or active
  - Mode changed by Power Mgmt bit in the frame control header.
- All packets destined to stations in PS mode are buffered (at AP)
- AP broadcasts list of stations with buffered packets in its beacon frames: Traffic Indication Map (TIM)
- When a station wakes up, it waits for the beacon; sends a PS-Poll message to AP if its bit is turned on in TIM; AP then sends one frame with buffered data and sets the More Data bit in the header if more data in the buffer (station does not go back to sleep after receiving one frame if More is set).

©2020 Mahbub Hassan

Traffic Indication Map (TIM)

- A bit map inside a beacon
- 2008 bits; each bit represents an Association ID (one associated client)
- If packets are buffered in the AP for a given Association ID, its corresponding bit is set to ‘1’, ‘0’ otherwise

©2020 Mahbub Hassan

Summary

1. 802.11 PHYs: Spread spectrum in earlier versions, but OFDM in new versions
2. 2.4 GHz channels (22 MHz) are mostly overlapped, but 5 GHz channels (20 MHz) are non-overlapped, but some are shared with the radar service
3. High speed applications can be supported by combining multiple adjacent channels into single channel with higher bandwidth
4. 802.11 uses SIFS, PIFS, DIFS for priority
5. WLAN frames have *four* address fields
6. 802.11 supports power saving mode

©2020 Mahbub Hassan

Acronyms

- Ack — Acknowledgement
- AP — Access Point
- APSD — Automatic Power Save Delivery
- BO — Backoff
- BSA — Basic Service Area
- BSS — Basic Service Set
- BSSID — Basic Service Set Identifier
- CA — Collision Avoidance
- CD — Collision Detection
- CDMA — Code Division Multiple Access
- CFP — Contention Free Period
- CRC — Cyclic Redundancy Check
- CSMA — Carrier Sense Multiple Access
- CTS — Clear to Send
- CW — Congestion Window
- CWmax — Maximum Congestion Window

©2020 Mahbub Hassan

Acronyms (Cont)

- CWmin — Minimum Congestion Window
- DA — Destination Address
- DCF — Distributed Coordination Function
- DIFS — DCF Inter-frame Spacing
- DS — Direct Sequence
- ESA — Extended Service Area
- ESS — Extended Service Set
- FH — Frequency Hopping
- FIFO — First In First Out
- GHz — Giga Hertz
- IBSS — Independent Basic Service Set
- ID — Identifier
- IEEE — Institution of Electrical and Electronics Engineers
- IFS — Inter-frame spacing
- ISM — Instrumentation, Scientific and Medical
- LAN — Local Area Network

©2020 Mahbub Hassan

Acronyms (Cont)

- MAC Media Access Control
- MHz Mega Hertz
- MIMO Multiple Input Multiple Output
- NAV Network Allocation Vector
- OFDM Orthogonal Frequency Division Multiplexing
- PCF Point Coordination Function
- PHY Physical Layer
- PIFS PCF inter-frame spacing
- PS Power saving
- QoS Quality of Service
- RA Receiver Address
- RTS Ready to Send
- SA Source Address
- SIFS Short Inter-frame Spacing

©2020 Mahbub Hassan

Acronyms (Cont)

- SS Subscriber Station
- TA Transmitter's Address
- TIM Traffic Indication Map
- WiFi Wireless Fidelity
- WLAN Wireless Local Area Network

©2020 Mahbub Hassan

WiFi Part II

IEEE 802.11 Evolution
b→a→g→n→ac→ax

©2020 Mahbub Hassan

Overview

1. Chronology of IEEE 802.11 Amendments
2. Maths of WiFi Data Rates | Modulation and Coding Scheme
3. 802.11a/b/g
4. 802.11n: Channel Bonding, Aggregation
5. 802.11ac: Multi-User MIMO
6. 802.11ax: OFDMA

©2020 Mahbub Hassan

WiFi Evolution: Key 802.11 Amendments

5.5x

- **802.11-1997:** 2 Mbps Legacy WiFi in 2.4GHz (now extinct!)
- **802.11b-1999**: Higher speed modulation in 2.4GHz (11Mbps)
- **802.11a-1999**: Higher speed PHY (OFDM) in 5GHz (54Mbps)
- **802.11g-2003**: Higher speed PHY (OFDM) in 2.4GHz (54Mbps)
- **802.11n-2009**: Enhancements for higher throughput: 2.4/5GHz (600 Mbps)
- **802.11ac-2013**: Very high throughput: 5GHz (~7 Gbps)
- **802.11ax-2020 (expected)**: High efficiency: 2.4/5GHz (~9.6Gbps, but particularly efficient for *short packets* and *dense deployments*)

4.9x

11.1x

special

1.36x 11.6x

©2020 Mahbub Hassan

Basics of WiFi Data Rates

- Each WiFi version supports a range of specific data rates
  - E.g., 802.11b → 11 Mbps,
  - 802.11a → 6,9,12,18,24,36,48,54 (Mbps)

8 different data rate options!

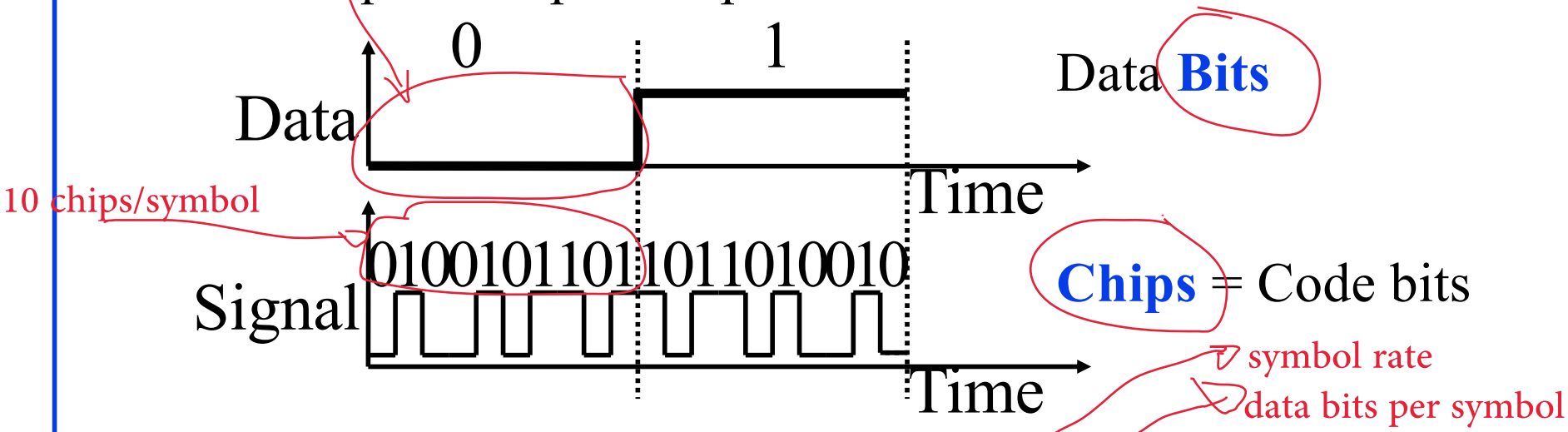
- **Data rate = symbol rate x data bits per symbol**
- Symbol rate = number of symbols per second
- Symbol rate calculation depends on PHY
  - Direct sequence spread spectrum (802.11b)
  - OFDM (802.11a/g/n/ac/ax)
- Data bits per symbol depends on modulation and coding
- WiFi with MIMO can have more than one independent data **stream** => *increases data rate linearly with number of such available streams*

©2020 Mahbub Hassan

IEEE 802.11b-1999

could be an example of a binary modulation

- Direct Sequence Spread Spectrum:



- **Complementary Code Keying (CCK)**: Multi-bit symbols with appropriate code to minimize errors
- IEEE 802.11-1997: ½ rate binary convolution encoder, 2 bit/symbol, 11 chips/symbol, DQPSK = ½ × 22 × 1/11 × 2 = **2 Mb/s** using 22 MHz
- IEEE 802.11b-1999: ½ rate binary convolution encoder, 8 bit/symbol, 8 chips/symbol, CCK = ½ × 22 × 1/8 × 8 = **11 Mb**/s using 22 MHz

Ref: P. Roshan and J. Leary, "802.11 Wireless LAN Fundamentals," Cisco Press, 2003, ISBN:1587050773, Safari book

©2020 Mahbub Hassan

Example

- A WLAN standard is employing a spread spectrum coding with only ½ rate, which produces chips at a rate of **½ chips per Hz**. It uses **8 chips to code a symbol** and 16 QAM modulation to modulate the symbol stream. What would be the data rate for 22 MHz channels?

Chip rate = ½ x 22 = 11 Mcps (cps = chips per second)

Symbol rate = 11/8 = 1.375 Msps (sps = symbols per second)

Bits per symbol = $\log_2(16) = 4$ [16 QAM produces 4 bits per symbol]

Data rate = symbol rate x bits per symbol = 1.375 x 4 = 5.5 Mbps

©2020 Mahbub Hassan

Symbol Rate for OFDM

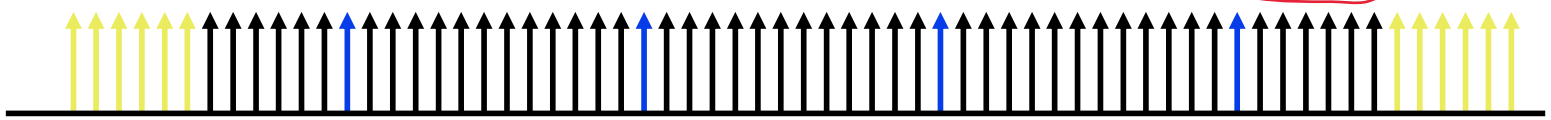
- OFDM adopted from 802.11a onwards
- OFDM symbol rate = 1/(symbol-interval)
- Symbol interval = data interval + guard interval
- Only the data interval contain the actual symbol
- Guard interval contains no data; it is used to protect against *inter symbol interference*
  - More multipath → longer delay spread → longer guard interval → reduced symbol rate

©2020 Mahbub Hassan

Bits per symbol - OFDM

- Bits per symbol in OFDM depends on *modulation order* and *subcarrier structure*
- Total # of subcarriers in a WiFi channel = channel-bandwidth/subcarrier-spacing
  - Subcarrier spacing 312.5 kHz in 802.11a/g/n/ac
  - Subcarrier spacing 78.125 kHz in 802.11ax
- Total subcarriers are divided into three categories: data subcarriers + pilot subcarriers + guard subcarriers
  - Only data subcarriers carry data
  - Pilots estimate the wireless channel
  - Guards protect against interference from adjacent channels
- Each OFDM symbol is carried over all data subcarriers in parallel
- M-ary modulation → $\log_2 M$ bits per data subcarrier for the symbol
  - E.g., 16-QAM yields 4 bits per data subcarrier
- Number of **raw (coded)** bits per symbol = $\log_2 M$ ✘ #-of-data-subcarriers

this multiplier is for OFDM



OFDM subcarrier structure: Black: *Data*, Blue: *Pilot*, Yellow: *Guard*

©2020 Mahbub Hassan

Impact of error coding on *data bits per symbol* in OFDM

- Error coding is often applied to original data to detect/correct bit errors during transmission
- Coded bit stream = original data bits + code bits
  - E.g., with ¾ code, 4 bits are transmitted for 3 data bits
  - With 2/3 code = 3 bits are transmitted for 2 data bits, and so on
  - ¾, 2/3, etc. are referred to as *coding rate*
- **Data bits per symbol** = *coding rate* ✘ $\log_2 M$ ✘ *#-of-data-subcarriers*

raw (coded) bits per symbol

©2020 Mahbub Hassan

Example

Question: What is the data rate of an OFDM WiFi applying 64-QAM and a coding rate of ¾ to its 48 data subcarriers? Assume a symbol interval of 4μs.

includes guard interval

Answer:

$Log_2M = log_2 64 = 6$

Coded bits per symbol = log_2M ✘ #-of-data-subcarriers = 6x48 = 288

Data bits per symbol = coding rate x 288 = ¾ x 288 = 216

Symbol rate = 1/symbol-interval = ¼ Msps (0.25 million symbols per sec.)

Data rate = symbol rate x data bits per symbol = 216 x ¼ Mbps = **54 Mbps**

©2020 Mahbub Hassan

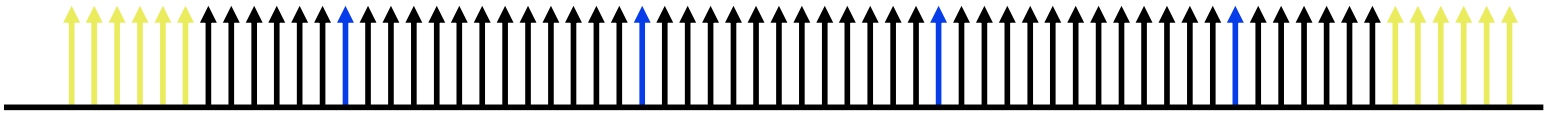
5 Key Parameters affecting WiFi data rates

1. Modulation (affects number of bits per symbol)
   - Usually multiple options available
2. Coding (error correction overhead)
   - Usually multiple options available
   - MCS (integer number) defines combination of modulation and coding
3. Guard interval (affects symbol rate)
4. Channel width → # of OFDM data subcarriers
   - Channel width can be increased via *bonding* from 802.11n onwards
5. MIMO streams (number of independent data streams that can be sent in parallel)
   - MIMO available from 802.11n onwards

©2020 Mahbub Hassan

IEEE802.11a-1999

- To increase the data rate, 802.11a uses OFDM.
- 20 MHz divided into 64 subcarriers (20000/312.5=64). 6 subcarriers at each side are used as guards and 4 as pilot, which leaves 48 for data.



- Each OFDM symbol is carried over 48 subcarriers in parallel.
- 802.11a OFDM has a symbol interval of 4μs → 0.25 M symbols/s
  - 3200ns (data pulse) + 800ns (guard interval) = 4000ns = 4μs
- With a binary modulation (e.g., BPSK) , there will be 1 coded bit per subcarrier for each OFDM symbol, or 48 coded bits per OFDM symbol in total (over 48 subcarriers)
- Data rate depends on the combination of *modulation* and *coding*
- 802.11a supports 4 different modulations: BPSK, QPSK, 16QAM, 64QAM
- 802.11a supports three coding rates, ½, 2/3, and ¾
- 802.11a supports 8 different data rates, 6 Mbps up to 54 Mbps, by selecting a combination of modulation and coding scheme (MCS)

©2020 Mahbub Hassan

IEEE802.11a-1999 Data Rates

MCS #	Modulation	Coding Rate	Coded bits per subcarrier	Coded bits per symbol	Data bits per symbol	Data Rate (Mbps)
0	BPSK	1/2	1	48	24	**6**
1	BPSK	3/4	1	48	36	**9**
2	QPSK	1/2	2	96	48	**12**
3	QPSK	3/4	2	96	72	**18**
4	16-QAM	1/2	4	192	96	**24**
5	16-QAM	3/4	4	192	144	**36**
6	64-QAM	2/3	6	288	192	**48**
7	64-QAM	3/4	6	288	216	**54**

©2020 Mahbub Hassan

IEEE 802.11g-2003

- 802.11a was great at max. data rate of 54Mbps, but
  - Only operates at 5GHz and not backward compatible with 11b
- 802.11g achieved 54Mbps at 2.4GHz using OFDM
  - And could fall back to 11b rates with CCK modulation
  - Was cheaper than 11a (2.4GHz radio had economy of scale)
- OFDM data rates are identical with 11a:
  - 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- CCK data rates:
  - 1, 2, 5.5, 11 Mbps

©2020 Mahbub Hassan

IEEE 802.11n-2009

©2020 Mahbub Hassan

MIMO in WiFi

1. **First WLAN to use MIMO** (Multi-input Multi-Output)
2. **MIMO** (Multi-input Multi-Output) Multiplexing:
   $n \times m{:}k \Rightarrow n$ transmitters, m receivers, ***k* streams**
   $k = degrees\ of\ freedom = \min(n,m)$
   $\Rightarrow k$ times more throughput
   E.g., $2 \times 2{:}2$, $2 \times 3{:}2$, $3 \times 2{:}2$, $4 \times 4{:}4$, $8 \times 4{:}4$
3. The AP is expected to have more antennas than the mobile device

©2020 Mahbub Hassan

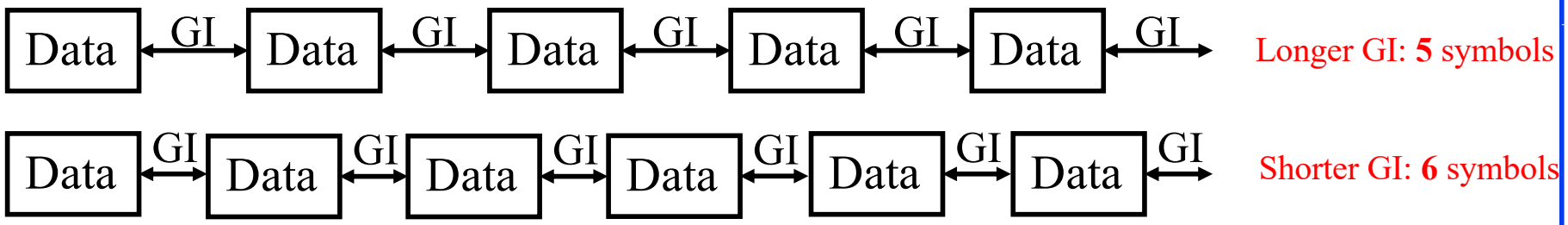
Other New Features of IEEE 802.11n-2009

1. **Frame Aggregation**: Pack multiple input frames inside a frame ⇒ Less overhead ⇒ More throughput
2. **Reduced Inter-Frame Spacing** (SIFS=2 μs, instead of 10 μs)
3. **Greenfield Mode**: Optionally eliminate support for a/b/g (shorter and higher rate preamble)
4. **Dual Band**: 2.4 and 5 GHz
5. **Lower FEC Overhead**: 5/6 instead of ¾ — new coding rate (not available in previous WiFi)
6. **Channel Bonding**: Combine two 20MHz channels to achieve 40MHz
7. **Shorter Guard Interval**: 400 ns instead of 800 ns
8. **More OFDM subcarriers**: Shorter GI in *time domain* enables less guard carriers in *frequency domain*
   - 4 instead of 6 guard carriers on either side of data carriers
   - 52 instead of 48 data carriers with 20 MHz legacy channels
   - 108 data carriers with 40MHz (no guard between two legacy channels)

52x2+4 = 108

©2020 Mahbub Hassan

Guard Interval



- Rule of Thumb: Guard Interval = 4 × Multi-path delay spread
- Initial 802.11a design assumed 200ns delay spread
  ⇒ 3200ns data + 800ns GI ⇒ 20% overhead (800/4000=0.2)
- Most indoor environment have smaller delay spread ~50-75ns
- So if both Tx-Rx agree, 400ns GI can be used in 802.11n
  ⇒ 3200ns data + 400ns GI ⇒ 11.11% overhead (400/3600=11.11)

Ref: M. Gast, "802.11n: A Survival Guide," O'Reilly, 2012, ISBN:978-1449312046, Safari Book

©2020 Mahbub Hassan

Example: 11n data rate improvement

- Compared to 802.11a/g, 802.11n has higher coding rate, wider channel bandwidth, lower coding overhead, and reduced guard interval. On top of this, 802.11n uses MIMO multiplexing to further boost the data rate. Given that 802.11a/g has a data rate of 54 Mbps, can you estimate the data rate for 802.11n that uses 4 MIMO streams (assume 64 QAM for both of them, i.e., there is no improvement in modulation)?

54 Mbps is achieved with ¾ coding for 3200 Data+800 GI for a/g, which basically uses a single stream (no MIMO).

802.11n has the following improvement factors:

- Streaming factor = 4
- Coding factor = (5/6)/(3/4) = ~1.11
- OFDM subcarrier (plus wider bandwidth) factor = (108/48) = 2.25
- Guard interval factor = (3200+800)/(3200+400) = ~1.11
- Total improvement factor = 4x1.11x2.25x1.11 = ~**11.1**

Improved data rate for 802.11n =

$$4 \times [(5/6)/(3/4)] \times (108/48) \times [(3200+800)/(3200+400)] \times 54 \Rightarrow \mathbf{600\ Mbps}$$

©2020 Mahbub Hassan

Example: 802.11n maximum data rate

Question: Calculate the maximum achievable data rate for 802.11n

Answer:

Minimum guard interval: 400ns (data interval=3200ns) → 3.6μs symbol interval

Maximum modulation: 64 QAM

Maximum coding: 5/6

Maximum # of MIMO streams: 4 (4x4 MIMO)

Maximum # of data carriers: 108 (for 40MHz bonded channels)

Coded bits per symbol = $\log_2 64$ ✘ #-of-data-subcarriers = 6x108 = 648

Data bits per symbol = coding rate x 648 = 5/6 x 648 = 540

Symbol rate = 1/symbol-interval = 1/3.6Msps

Data rate (single MIMO stream) = symbol rate x data bits per symbol = 1/3.6 x 540 Mbps = **150 Mbps**

Data rate with 4 streams = 4 x 150 = 600 Mbps

©2020 Mahbub Hassan

802.11n Data Rates (Single Stream)

MCS index	Spatial streams	Modulation type	Coding rate	Data rate (Mbit/s)			
				20 MHz channel		40 MHz channel	
				800 ns GI	400 ns GI	800 ns GI	400 ns GI
0	1	BPSK	1/2	6.5	7.2	13.5	15
1	1	QPSK	1/2	13	14.4	27	30
2	1	QPSK	3/4	19.5	21.7	40.5	45
3	1	16-QAM	1/2	26	28.9	54	60
4	1	16-QAM	3/4	39	43.3	81	90
5	1	64-QAM	2/3	52	57.8	108	120
6	1	64-QAM	3/4	58.5	65	121.5	135
7	1	64-QAM	5/6	65	72.2	135	150

Source: https://www.cablefree.net/wirelesstechnology/wireless-lan/data-rates-in-802-11n/

©2020 Mahbub Hassan

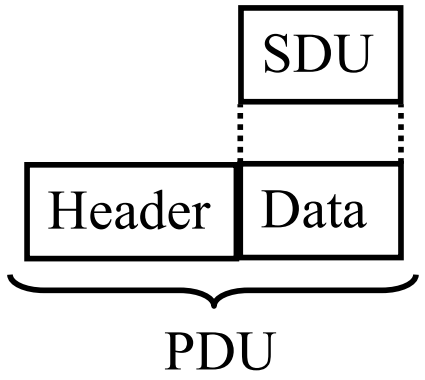
Data rates for 802.11n (Multiple Streams)

Source: https://www.cablefree.net/wirelesstechnology/wireless-lan/data-rates-in-802-11n/

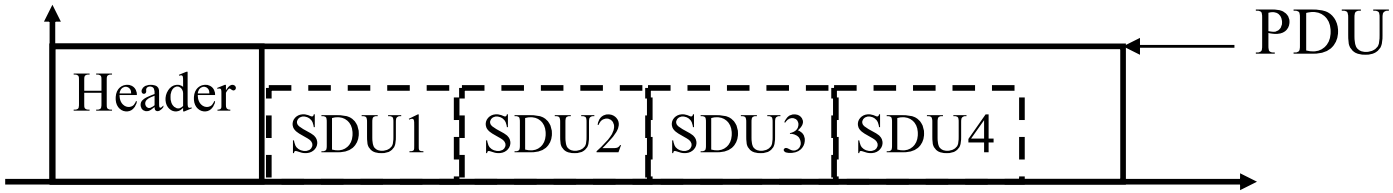
MCS index	Spatial streams	Modulation type	Coding rate	Data rate (Mbit/s)			
				20 MHz channel		40 MHz channel	
				800 ns GI	400 ns GI	800 ns GI	400 ns GI
0	1	BPSK	1/2	6.5	7.2	13.5	15
1	1	QPSK	1/2	13	14.4	27	30
2	1	QPSK	3/4	19.5	21.7	40.5	45
3	1	16-QAM	1/2	26	28.9	54	60
4	1	16-QAM	3/4	39	43.3	81	90
5	1	64-QAM	2/3	52	57.8	108	120
6	1	64-QAM	3/4	58.5	65	121.5	135
7	1	64-QAM	5/6	65	72.2	135	150
8	2	BPSK	1/2	13	14.4	27	30
9	2	QPSK	1/2	26	28.9	54	60
10	2	QPSK	3/4	39	43.3	81	90
11	2	16-QAM	1/2	52	57.8	108	120
12	2	16-QAM	3/4	78	86.7	162	180
13	2	64-QAM	2/3	104	115.6	216	240
14	2	64-QAM	3/4	117	130	243	270
15	2	64-QAM	5/6	130	144.4	270	300
16	3	BPSK	1/2	19.5	21.7	40.5	45
17	3	QPSK	1/2	39	43.3	81	90
18	3	QPSK	3/4	58.5	65	121.5	135
19	3	16-QAM	1/2	78	86.7	162	180
20	3	16-QAM	3/4	117	130	243	270
21	3	64-QAM	2/3	156	173.3	324	360
22	3	64-QAM	3/4	175.5	195	364.5	405
23	3	64-QAM	5/6	195	216.7	405	450
24	4	BPSK	1/2	26	28.8	54	60
25	4	QPSK	1/2	52	57.6	108	120
26	4	QPSK	3/4	78	86.8	162	180
27	4	16-QAM	1/2	104	115.6	216	240
28	4	16-QAM	3/4	156	173.2	324	360
29	4	64-QAM	2/3	208	231.2	432	480
30	4	64-QAM	3/4	234	260	486	540
31	4	64-QAM	5/6	260	288.8	540	600

©2020 Mahbub Hassan

Frame Aggregation

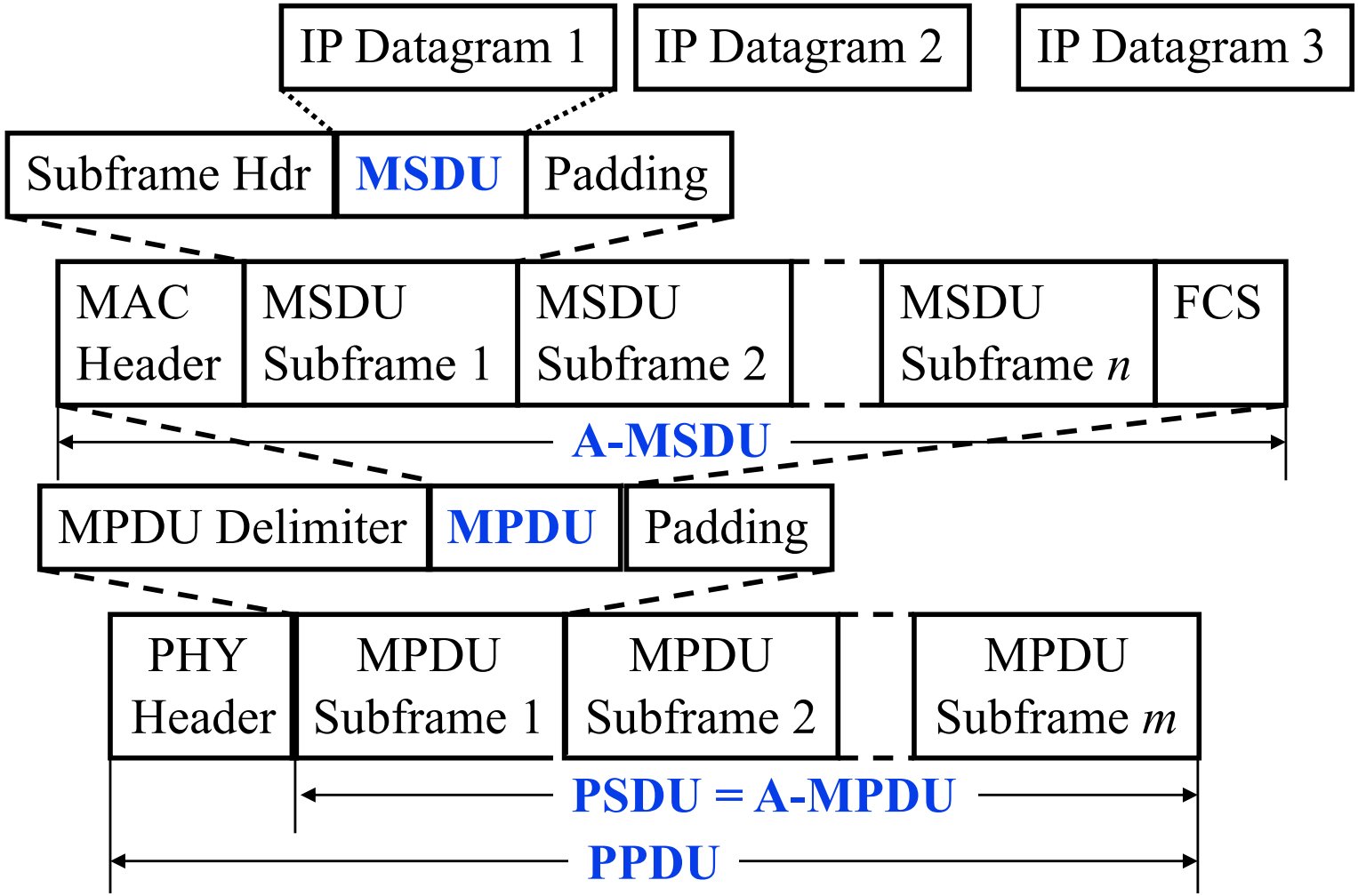


- Each layer has Service Data Units (**SDUs**) as input
- Each layer makes Protocol Data Units (**PDUs**) as output to communicate with the corresponding layer at the other end
  - PDUs have a header specific to the layer (*header means overhead*)
- **Frame Aggregation**: Multiple SDUs in one PDU
  - All SDUs must have the same transmitter and receiver address



©2020 Mahbub Hassan

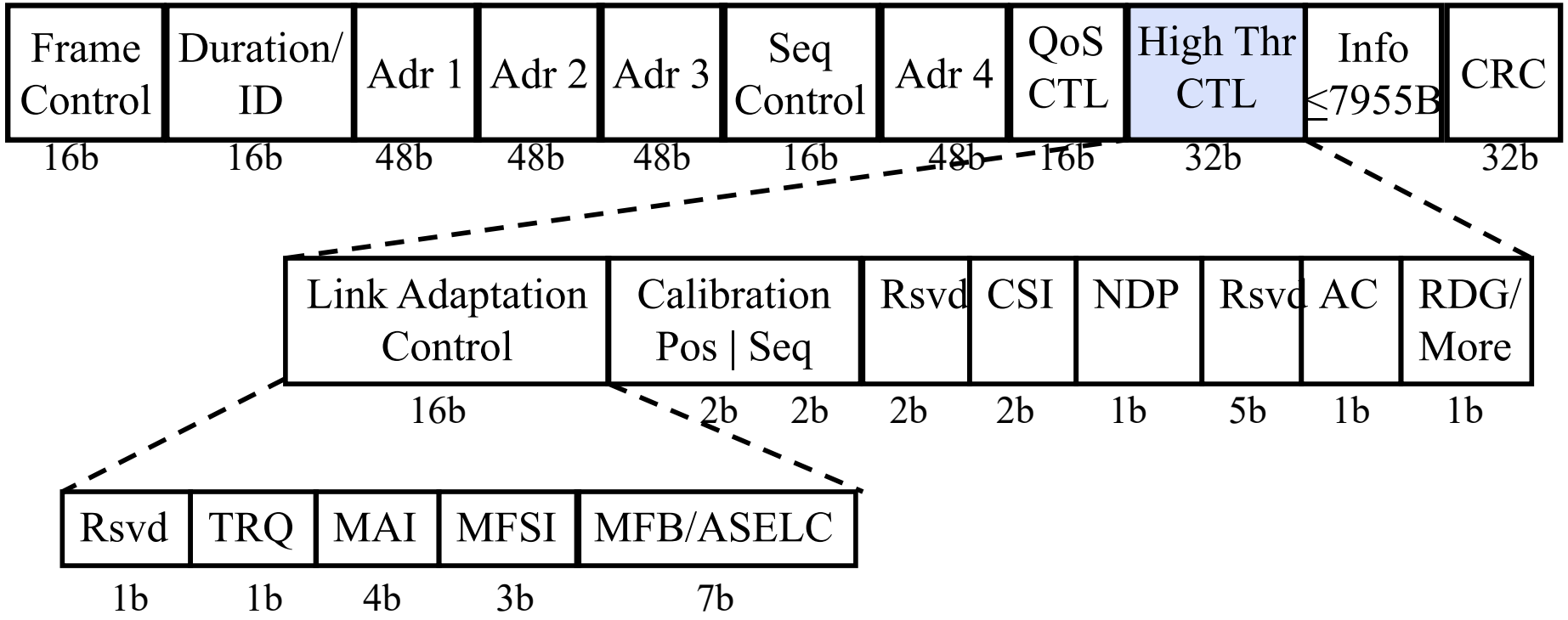
802.11n Frame Aggregation



Ref: D. Skordoulis, et al., "IEEE 802.11n MAC Frame Aggregation Mechanisms for Next-Generation High-Throughput WLANs," IEEE Wireless Magazine, February 2008, http://tinyurl.com/k2gvl2g

©2020 Mahbub Hassan

802.11n CSI Feedback



- 802.11n introduced a "High Throughput Control" field to exchange channel state information (CSI)
- Receivers can derive CSI from the pilots embedded in the transmissions (e.g., OFDM pilot subcarriers), but the transmitters cannot learn it unless receivers explicitly feedback this information. This new field in 802.11n provides this opportunity

©2020 Mahbub Hassan

IEEE 802.11ac-2013

©2020 Mahbub Hassan

IEEE 802.11ac

pilot subcarriers

- 5 GHz only (2.4 GHz not supported)
- Enhanced channel bonding: 20, 40, 80, 160 MHz channels
- More data subcarriers: 52+4 (20 MHz), 108+6 (40 MHz), 234+8 (80 MHz), 468+16 (160 MHz)
  - *More data subcarriers achieved due to wider channels*
  - *Subcarrier spacing remains 312.5 kHz (same as 11a/g/n)*
- Higher modulation: up to 256-QAM $\log_2 256 = 8$
- More MIMO streams: up to 8 streams allowed

needs 8 antennas
5GHz has smaller wavelength ->
can pack more antennas
because antennas are separated
by lambda/2

Ref: M. Gast, "802.11ac: A Survival Guide," O'Reilly, July 2013, ISBN:978-1449343149, Safari Book

©2020 Mahbub Hassan

Example: 802.11ac data rate (1)

Question: Calculate the maximum achievable data rate for an 802.11ac mobile client with a *single antenna*.

Answer:

Single antenna → only **1 stream** possible (even if the AP has many antennas)

Minimum guard interval: 400ns (data interval=3200ns) → 3.6μs symbol interval

Maximum modulation: 256 QAM

Maximum coding: 5/6

Maximum # of data carriers: 468 (for 160MHz bonded channels)

Coded bits per symbol = $\log_2 256$ ✘ #-of-data-subcarriers = 8x468 = 3744

Data bits per symbol = coding rate x 3744 = 5/6 x 3744 = 3120

Symbol rate = 1/symbol-interval = 1/3.6Msps

Data rate (single MIMO stream) = symbol rate x data bits per symbol = 1/3.6 x 3120 Mbps = **866.67 Mbps**

©2020 Mahbub Hassan

Example: 802.11ac data rate (2)

Question: An 802.11ac mobile client fitted with two antennas is connected to a wireless LAN via an 802.11ac access point equipped with four antennas. Calculate the maximum achievable data rate for the mobile client.

Answer:

Max. # of streams = min(2,4) = 2

Max. data rate with single stream(from previous example) = 866.67 Mbps

Therefore, max. data rate with 2 streams = 2x866.67 Mbps = 1.733 Gbps

©2020 Mahbub Hassan

802.11ac Data Rates in Mbps (Single Stream)

MCS index[b]	Modulation type	Coding rate	20 MHz channels		40 MHz channels		80 MHz channels		160 MHz channels	
			800 ns GI	400 ns GI	800 ns GI	400 ns GI	800 ns GI	400 ns GI	800 ns GI	400 ns GI
0	BPSK	1/2	6.5	7.2	13.5	15	29.3	32.5	58.5	65
1	QPSK	1/2	13	14.4	27	30	58.5	65	117	130
2	QPSK	3/4	19.5	21.7	40.5	45	87.8	97.5	175.5	195
3	16-QAM	1/2	26	28.9	54	60	117	130	234	260
4	16-QAM	3/4	39	43.3	81	90	175.5	195	351	390
5	64-QAM	2/3	52	57.8	108	120	234	260	468	520
6	64-QAM	3/4	58.5	65	121.5	135	263.3	292.5	526.5	585
7	64-QAM	5/6	65	72.2	135	150	292.5	325	585	650
8	256-QAM	3/4	78	86.7	162	180	351	390	702	780
9	256-QAM	5/6	N/A	N/A	180	200	390	433.3	780	866.7

Source: https://www.cablefree.net/wirelesstechnology/wireless-lan/data-rates-802-11ac/

©2020 Mahbub Hassan

Example: 802.11ac maximum data rate

Question: What is the maximum achievable data rate in 802.11ac?

Answer:

802.11ac allows a maximum of **8** MIMO streams

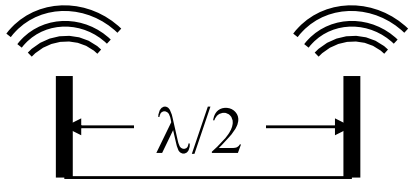
Maximum achievable with single stream = **866.67** Mbps

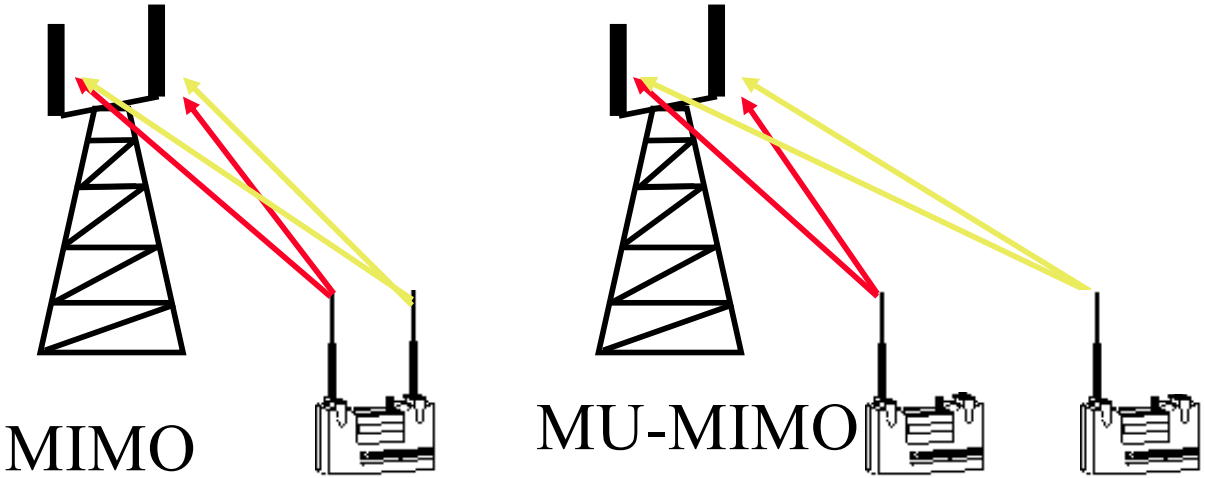
Maximum achievable data rate of 802.11ac = 8x866.67 = **6.9** Gbps

©2020 Mahbub Hassan

802.11ac supports Multi-User MIMO

- **MIMO**: Multiple uncorrelated spatial beams
  Multiple antenna's separated by λ/4 or λ/2 (*absolute minimum*)
  - Cannot put too many antennas on a small device; also cost increases with number of antennas
- **MU-MIMO**: Two single-antenna users can act as one multi-antenna device. The users do not really need to know each other. They do not even know that their antennas are used in a MU-MIMO system!

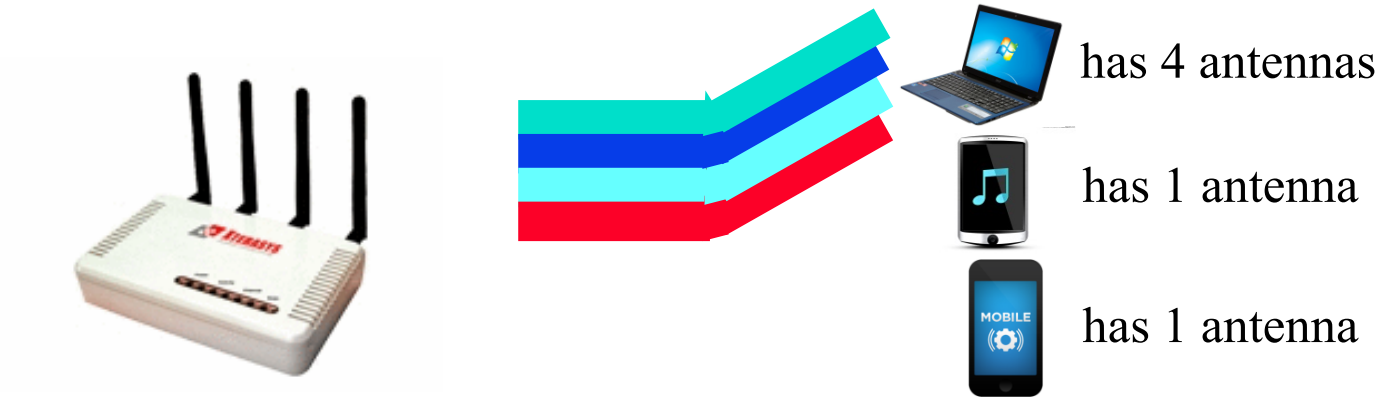




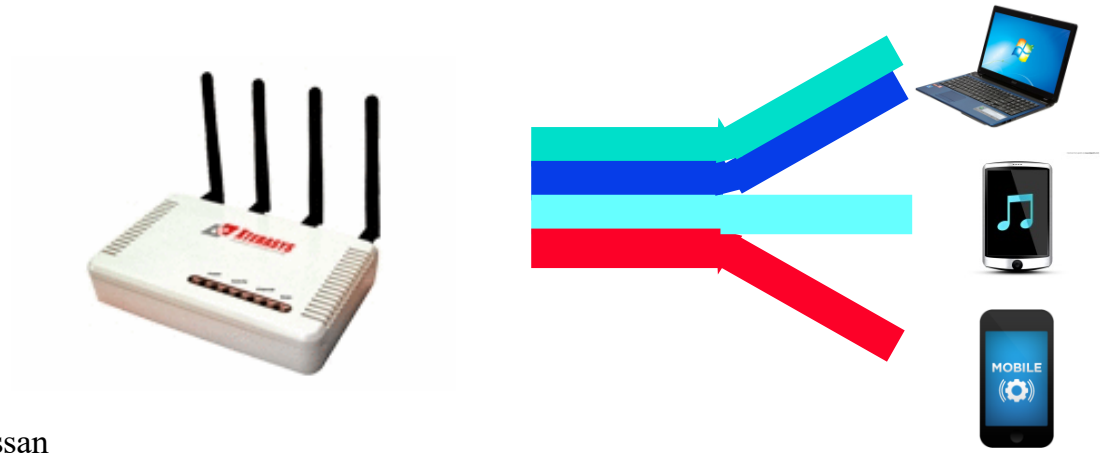
©2020 Mahbub Hassan

Directing streams with Beamforming in Multi-User MIMO

- **Single User MIMO**: Colors represent transmission signals (streams) not frequency.



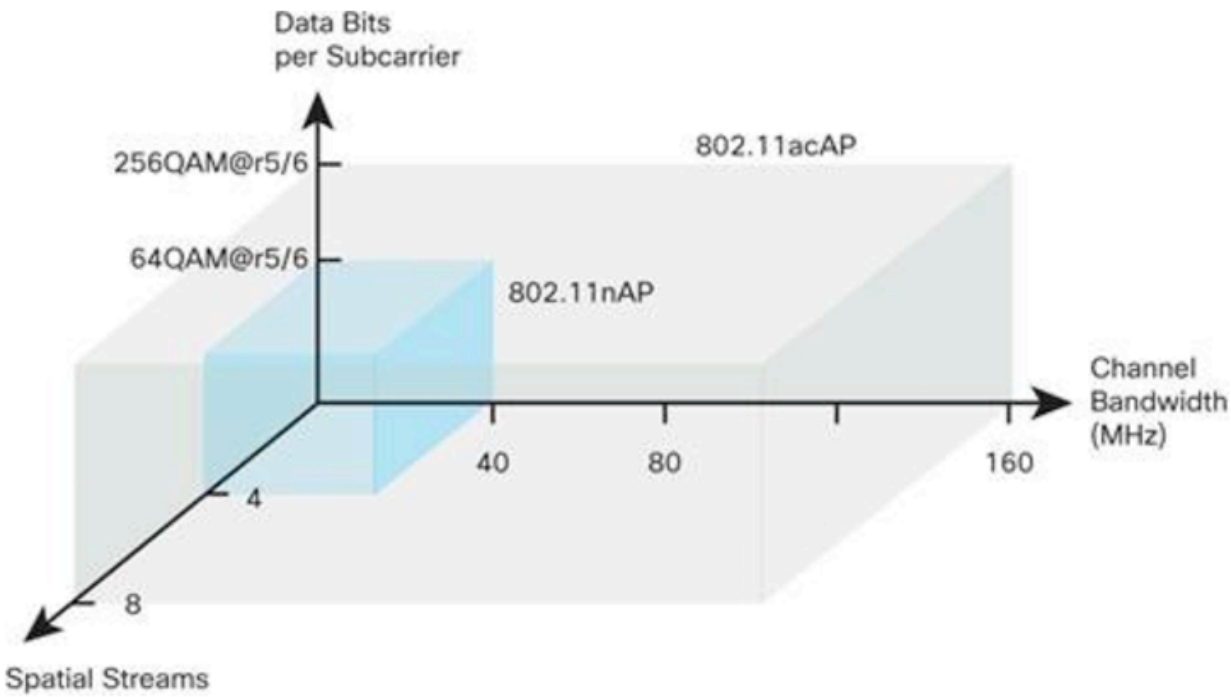
- **Multi User MIMO**:



©2020 Mahbub Hassan

802.11n vs. 802.11ac

Data Rate Enhancements in 3 Dimensions



[Affects # of data subcarriers]

https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-3600-series/white_paper_c11-713103.html

©2020 Mahbub Hassan

IEEE 802.11ax-2020 (expected)

©2020 Mahbub Hassan

802.11ax High Efficiency (HE): Motivation

- Up until now, 802.11 evolution was purely driven by pushing the data rates and throughput (we were crazy about speed!)
  - From humble 2Mbps in 1997 (802.11 legacy) to ~7Gbps in 2013 (11ac) an increase of 3500x in just 16 years!
- WiFi has become so popular and dense that we cannot really use all that speed due to congestion, collisions, and interference
- Need a new WiFi that can work **efficiently** in dense deployments, in outdoors, for short message communications between IoT machines etc.
- 802.11ax is more about efficiency for such new environments than pushing the data rates
- 802.11ax has only a modest data rate increase of 37% against its predecessor 802.11ac; whereas 11ac increased data rate by 10x compared to 11n

©2020 Mahbub Hassan

Parameters of 802.11ax

- Supports both 2.4 and 5GHz bands
- No change for coding rate: 5/6 max.
- No change for channel width: 160 MHz max for 5GHz
  - Upto 40MHz for 2.4GHz band
- No change with MIMO stream numbers: 8 streams max.
- Increased modulation rate: 1024 QAM max.
- Increased symbol interval to address longer delay spread in challenging **outdoor** environments
  - Symbol data interval increased to 12.8µs (vs. 3.2µs in 11a/g/n/ac)
  - Guard interval increased to 0.8µs, 1.6µs, or 3.2µs (3 options allowed)

overhead = 3.2/16 = 20%

two additional types

- OFDM subcarrier spacing reduced to 78.125 kHz (vs. 312.5kHz in 11a/g/n/ac)
  - Total subcarriers: 256 (20MHz), 512 (40MHz), 1024 (80MHz), 2048 (160MHz)
  - Total subcarriers = data+pilot+guard+DC+null (5 types of subcarriers)
  - Data subcarriers = 234 (20MHz), 468 (40MHz), 980 (80MHz), 1960 (160MHz)

©2020 Mahbub Hassan

802.11ax OFDM Parameters

PHY	Modulation		R	N_{SS}	N_{SD}				T_{DFT}	T_{GI}		
	Name	N_{BPSCS}			20MHz	40MHz	80MHz	160MHz		Short	Medium	Long
802.11ax (HE)	BPSK	1	1/2	1 to 8	234	468	980	1960	12.8 µs	0.8 µs	1.2 µs	3.2 µs
	QPSK	2	1/2 & 3/4									
	16-QAM	4	1/2 & 3/4									
	64-QAM	6	1/2 & 2/3 & 3/4									
	256-QAM	8	2/3 & 5/6									
	1024-QAM	10	3/4 & 5/6									

N_{BPSCS}: number of coded bits per data subcarrier
R: coding rate
Nss: number of spatial streams
Nsd: number of data subcarriers
T_{DFT}: symbol data interval
T_{GI}: guard interval

©2020 Mahbub Hassan

Example: 802.11ax OFDM maximum data rate

Question: Calculate the maximum achievable data rate for 802.11ax OFDM

Answer:

Minimum guard interval: ~~8~~ 0.8µs (data interval=12.8µs) → 13.6µs symbol interval

Maximum modulation: 1024 QAM

Maximum coding: 5/6

Maximum # of MIMO streams: 8

Maximum # of OFDM data subcarriers: 1960 (for 160MHz channels)

Coded bits per symbol = $\log_2 1024$ ✘ #data-subcarriers = 10x1960 = 19600

Data bits per symbol = coding rate x 19600 = 5/6 x 19600 = 16333.33

Symbol rate = 1/symbol-interval = 1/13.6Msps

Data rate (single MIMO stream) = symbol rate x data bits per symbol = 1/13.6 x 5/6 x 19600 Mbps = **1.2 Gbps**

Data rate with 8 streams = 8 x 1.2 = 9.6 Gbps

©2020 Mahbub Hassan

802.11ax OFDM Data Rates in Mbps (Single Stream)

MCS index	Modulation type	Coding rate	Data rate (in Mb/s)							
			20 MHz channels		40 MHz channels		80 MHz channels		160 MHz channels	
			1600 ns GI	800 ns GI	1600 ns GI	800 ns GI	1600 ns GI	800 ns GI	1600 ns GI	800 ns GI
0	BPSK	1/2	4	4	8	9	17	18	34	36
1	QPSK	1/2	16	17	33	34	68	72	136	144
2	QPSK	3/4	24	26	49	52	102	108	204	216
3	16-QAM	1/2	33	34	65	69	136	144	272	282
4	16-QAM	3/4	49	52	98	103	204	216	408	432
5	64-QAM	2/3	65	69	130	138	272	288	544	576
6	64-QAM	3/4	73	77	146	155	306	324	613	649
7	64-QAM	5/6	81	86	163	172	340	360	681	721
8	256-QAM	3/4	98	103	195	207	408	432	817	865
9	256-QAM	5/6	108	115	217	229	453	480	907	961
10	1024-QAM	3/4	122	129	244	258	510	540	1021	1081
11	1024-QAM	5/6	135	143	271	287	567	600	1134	1201

Source: https://www.cablefree.net/wirelesstechnology/wireless-lan/802-11ax/

©2020 Mahbub Hassan

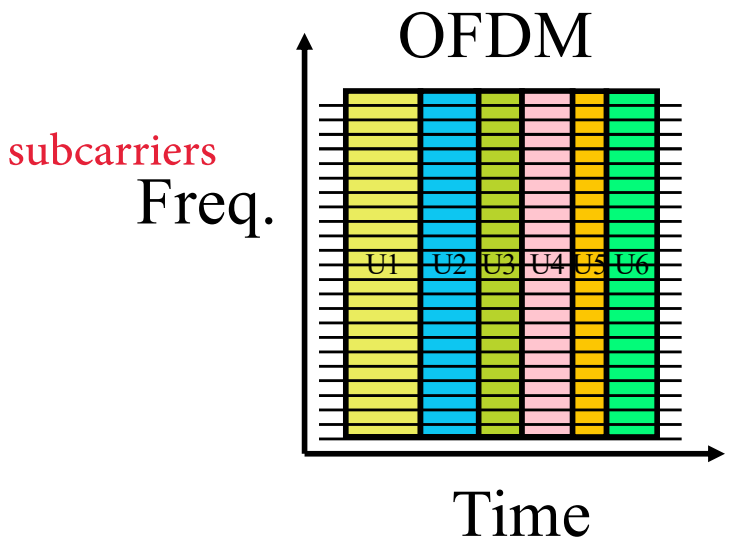
OFDMA: new access control for WiFi

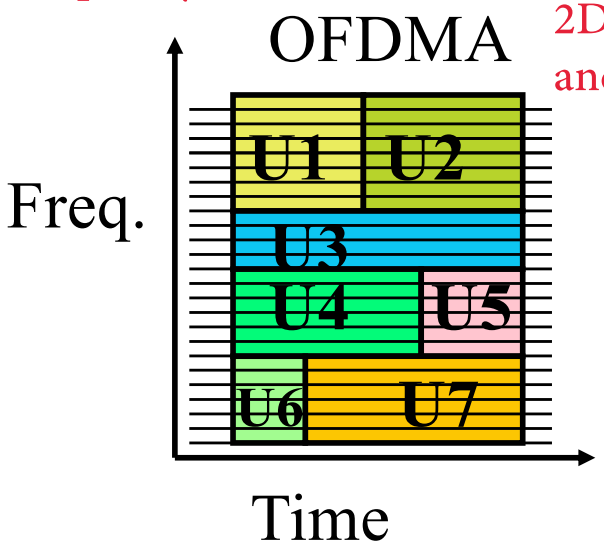
- OFDMA: **O**rthogonal **F**requency **D**ivision **M**ultiple **A**ccess
- 802.11ax introduces OFDMA as an option to centrally allocate channel resources to each competing station using fine-grained time and frequency resource units (RUs) like cellular networks
- Channel bandwidth is first divided into many narrow subcarriers
  - Subcarrier spacing = 78.125kHz (vs. 312.5kHz in previous WiFi)
- Subcarriers are grouped into RUs called tones
- 26, 52, 106, 242, 484, or 996 tones per station. Each tone consist of a single subcarrier of 78.125 kHz bandwidth.
- Smallest resource allocated to an OFDMA communication: 26x78.125kHz = 2031.25kHz (~2MHz)
- Largest tone has: 996x78.125kHz = 77812.5kHz (~80MHz)
- A station can have a maximum of TWO 996 tones allocated

©2020 Mahbub Hassan

OFDMA Illustrated

1D allocation (only time, not frequency)





2D allocation (both time and frequency/subcarrier)

©2020 Mahbub Hassan

802.11ax RUs

RU type	20 MHz	40 MHz	80 MHz	160 (80+80) MHz
26-tone	9	18	37	74
52-tone	4^{+1}	8^{+2}	16^{+5}	32^{+10}
106-tone	2^{+1}	4^{+2}	8^{+5}	16^{+10}
242-tone	1	2	4^{+1}	8^{+2}
484-tone	NA	1	2^{+1}	4^{+2}
996-tone	NA	NA	1	2

$*^{+n}$ means "plus n 26-tone RUs".

Source: A Tutorial on IEEE 802.11ax High Efficiency WLANs, Khorov et al., IEEE Communications Surveys and Tutorial, 2019.

©2020 Mahbub Hassan

802.11ax OFDMA Parameters

PHY	Modulation		R	N_{SS}	N_{SD}						T_{DFT}	T_{GI}		
	Name	N_{BPSCS}			26-tone	52-tone	106-tone	242-tone	484-tone	996-tone		Short	Medium	Long
802.11ax (HE)	BPSK	1	1/2	1 to 8	24	48	102	234	468	980	12.8 µs	0.8 µs	1.2 µs	3.2 µs
	QPSK	2	1/2 & 3/4											
	16-QAM	4	1/2 & 3/4											
	64-QAM	6	1/2 & 2/3 & 3/4											
	256-QAM	8	2/3 & 5/6											
	1024-QAM	10	3/4 & 5/6											

HE OFDMA Parameters

N_{BPSCS}: number of coded bits per data subcarrier
R: coding rate
Nss: number of spatial streams
Nsd: number of data subcarriers
T_{DFT}: symbol data interval
T_{GI}: guard interval

©2020 Mahbub Hassan

802.11ax OFDMA Data Rates in Mbps (Single Stream)

MCS Index	Spatial Stream	Modulation	Coding	MU-OFDMA (802.11ax)																	
				26-tone RU			52-tone RU			106-tone RU			242-tone RU			484-tone RU			996-tone RU		
				0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI
0	1	BPSQ	1/2	0.9	0.8	0.8	1.8	1.7	1.5	3.8	3.5	3.2	8.6	8.1	7.3	17.2	16.3	14.6	36.0	34.0	30.6
1	1	QPSK	1/2	1.8	1.7	1.5	3.5	3.3	3.0	7.5	7.1	6.4	17.2	16.3	14.6	34.4	32.5	29.3	72.1	68.1	61.3
2	1	QPSK	3/4	2.6	2.5	2.3	5.3	5.0	4.5	11.3	10.6	9.6	25.8	24.4	21.9	51.6	48.8	43.9	108.1	102.1	91.9
3	1	16-QAM	1/2	3.5	3.3	3.0	7.1	6.7	6.0	15.0	14.2	12.8	34.4	32.5	29.3	68.8	65.0	58.5	144.1	136.1	122.5
4	1	16-QAM	3/4	5.3	5.0	4.5	10.6	10.0	9.0	22.5	21.3	19.1	51.6	48.8	43.9	103.2	97.5	87.8	216.2	204.2	183.8
5	1	64-QAM	2/3	7.1	6.7	6.0	14.1	13.3	12.0	30.0	28.3	25.5	68.8	65.0	58.5	137.6	130.0	117.0	288.2	272.2	245.0
6	1	64-QAM	3/4	7.9	7.5	6.8	15.9	15.0	13.5	33.8	31.9	28.7	77.4	73.1	65.8	154.9	146.3	131.6	324.3	306.3	275.6
7	1	64-QAM	5/6	8.8	8.3	7.5	17.6	16.7	15.0	37.5	35.4	31.9	86.0	81.3	73.1	172.1	162.5	146.3	360.3	340.3	306.3
8	1	256-QAM	3/4	10.6	10.0	9.0	21.2	20.0	18.0	45.0	42.5	38.3	103.2	97.5	87.8	206.5	195.0	175.5	432.4	408.3	367.5
9	1	256-QAM	5/6	11.8	11.1	10.0	23.5	22.2	20.0	50.0	47.2	42.5	114.7	108.3	97.5	229.4	216.7	195.0	480.4	453.7	408.3
10	1	1024-QAM	3/4	13.2	12.5	11.3	26.5	25.0	22.5	56.3	53.1	47.8	129.0	121.9	109.7	258.1	243.8	219.4	540.4	510.4	459.4
11	1	1024-QAM	5/6	14.7	13.9	12.5	29.4	27.8	25.0	62.5	59.0	53.1	143.4	135.4	121.9	286.8	270.8	243.8	600.5	567.1	510.4

Source: https://www.semfionetworks.com/blog/mcs-table-updated-with-80211ax-data-rates

©2020 Mahbub Hassan

Example: 802.11ax OFDMA Communication

Question: A single antenna 802.11ax client receives a 26-tone RU allocation from the AP when trying to transmit a 147-byte data frame. What could be the minimum possible time required to transmit the frame?

Answer:

Single antenna means single stream

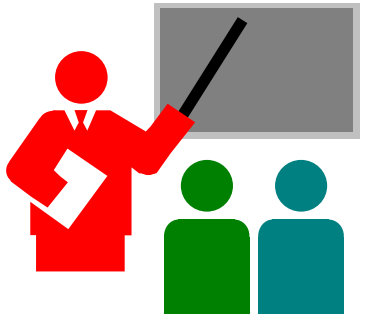
Maximum data rate for single-stream 26-tone (1024-QAM@5/6, 0.8µs GI) = 14.7Mbps

Data frame length in bits: 147x8 bits

Minimum frame transmission time: (147x8)/14.7µs = **80µs**

©2020 Mahbub Hassan

Summary



1. 802.11a/g use OFDM with 64 subcarriers in 20 MHz. 48 Data, 4 Pilot, 12 guard.
2. 802.11n adds MIMO and channel bonding.
3. IEEE 802.11ac supports multi-user MIMO with 80+80 MHz channels with 256-QAM and 8 streams to give 6.9 Gbps
4. Multi-User MIMO allows several users with smaller number of antennas to be combined in a large MIMO pool.
5. 802.11ax introduces OFDMA for finer control and allocation of channel resources achieving high efficiency in dense deployments

©2020 Mahbub Hassan

WiFi Part III

IEEE 802.11 for Niche Applications
802.11af/ah/ad/ay

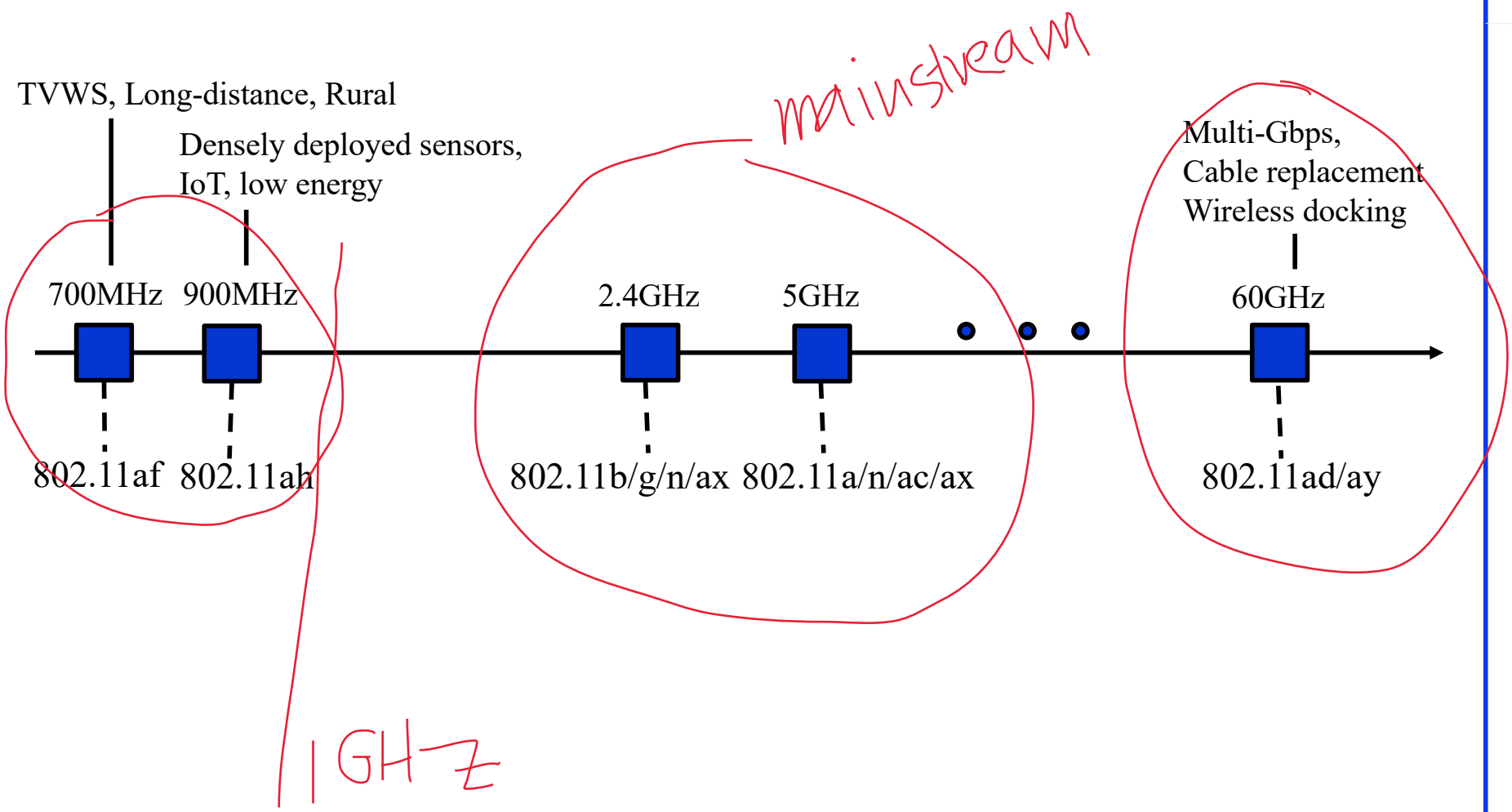
©2020 Mahbub Hassan

Overview

- IEEE 802.11af
- IEEE 802.11ah
- IEEE 802.11ad
- IEEE 802.11ay

©2020 Mahbub Hassan

802.11 Standards



©2020 Mahbub Hassan

IEEE 802.11af-2014 (a.k.a. White-Fi)

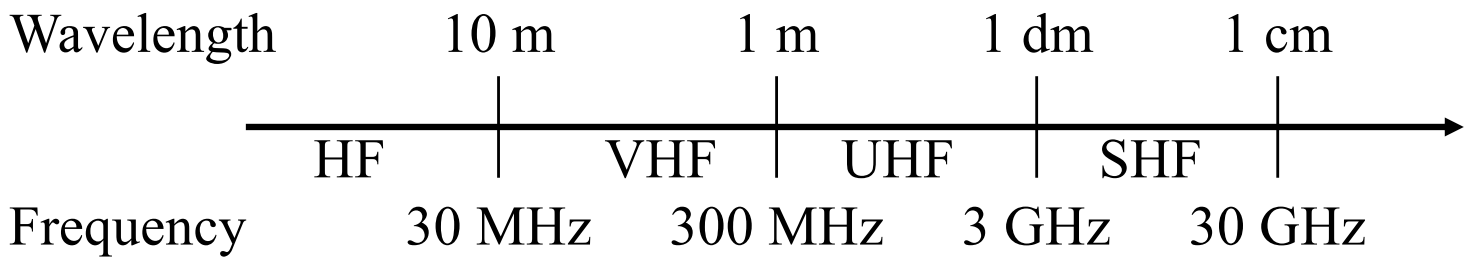
©2020 Mahbub Hassan

802.11af Overview

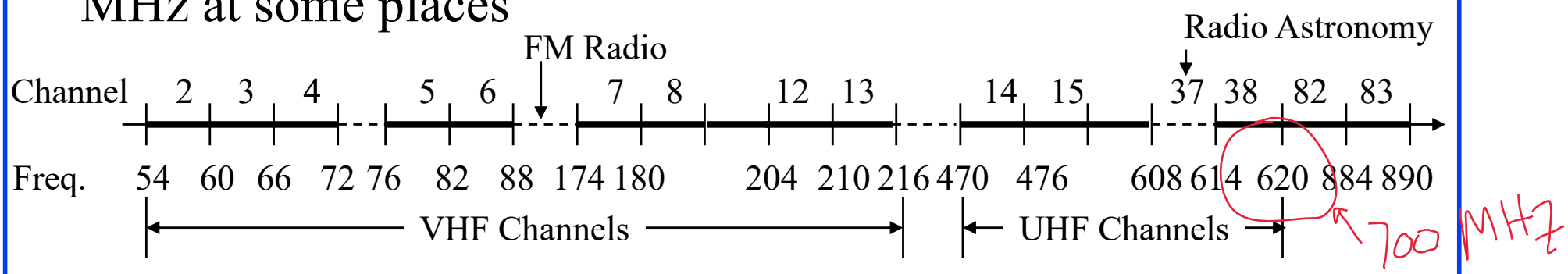
1. Television Channels
2. Software Defined Radios
3. Spectral White Spaces
4. FCC Rules for White Spaces
5. Data rates and MCS
6. Whitespace Database and Whitespace Access Protocol

©2020 Mahbub Hassan

Over-the-Air Television Channels

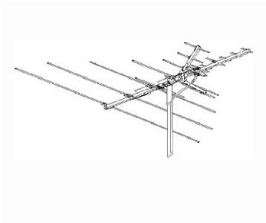


- Television channels use Very High Frequency (VHF) and Ultra High Frequency (UHF) bands
- Each channel uses 6 MHz in USA, 8 MHz in Europe, and 7 MHz at some places



- At least one channel is skipped between two analog stations in neighboring areas to avoid interference

©2020 Mahbub Hassan



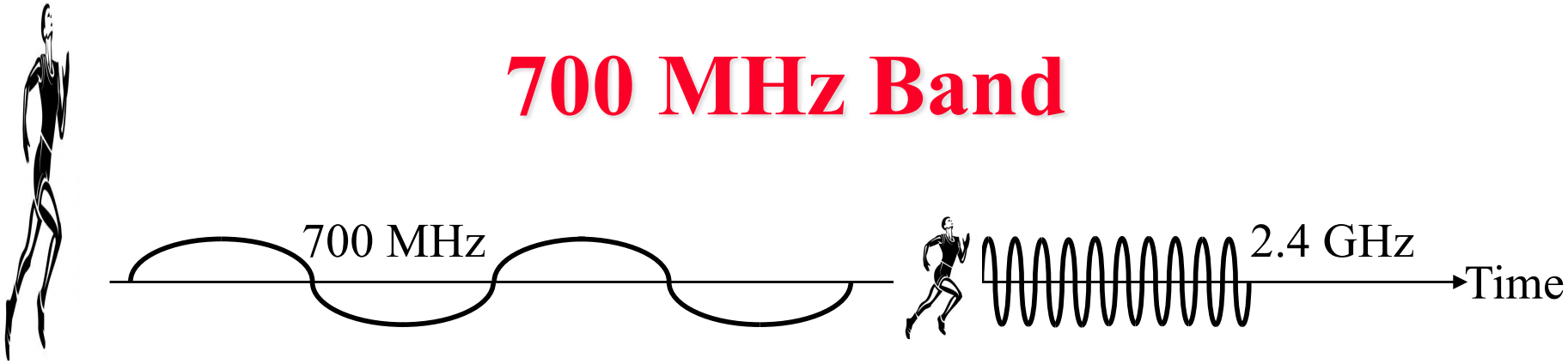
Digital Television

- Converting pixels to bits
  ⇒ Can easily encrypt, multiplex, mix with data
- Change Standard Definition (SD), High Definition (HD)
- Do not need empty channels between neighbors
- Need about 19 Mbps ⇒ Can transmit 6-8 channels in 6-8 MHz.
- US FCC stopped analog transmissions on June 12, 2009
- A lot of TV spectrum became available ⇒ **Digital Dividend**
- Big demand for this "new" spectrum in **700 MHz band**:
  - Cellular, Emergency Services, ISM, everyone wants it
  - Government raised $19.5 billion from auction to cellular companies and saved some for unlicensed use

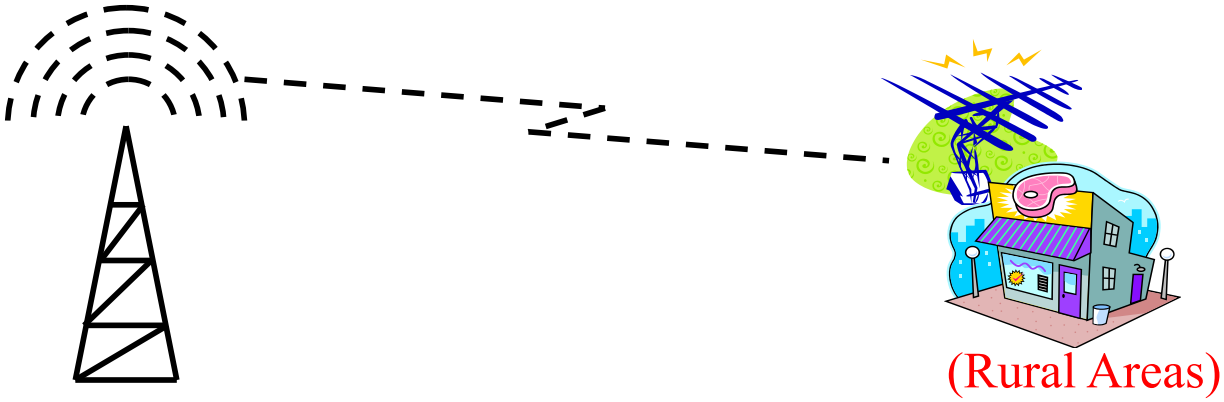
saves bandwidth

©2020 Mahbub Hassan

700 MHz Band



- Lower attenuation (1/7th to 1/9th of 1800/1900/2100 MHz)
  ⇒ Lower transmission power
  ⇒ Longer mobile battery life
- Larger Cell radius ⇒ Smaller number of towers
- Long distance propagation ⇒ Good for rural areas.

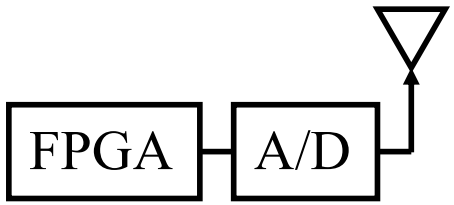


Ref: Adam LaMore, "The 700 MHz Band: Recent Developments and Future Plans,"
http://www.cse.wustl.edu/~jain/cse574-08/700mhz.htm

©2020 Mahbub Hassan

Software Defined Radio

- Analog radio circuits are specific to frequency, channel width, data rate, modulation (AM, FM), multiplexing (FDMA, TDMA, CDMA, OFDMA)
- Need multi-mode radios: Multiband, multi-channel, multi-carrier, multi-mode (AM, FM, CDMA), Multi-rate (samples per second) ⇒ Possible using digital computation
- Generally using Digital Signal Processing (DSP) or field programmable gate arrays (FPGAs)
- Signal is digitized as close to the antenna as possible. Logic reconfigured on demand.
- Software reconfigurable radio
- Flexibility, Upgradability, Lower cost (digital), Lower power consumption.
- **Software Defined Antenna**: Small pixel elements reconfigured by software for desired band.



©2020 Mahbub Hassan

GNU Radio

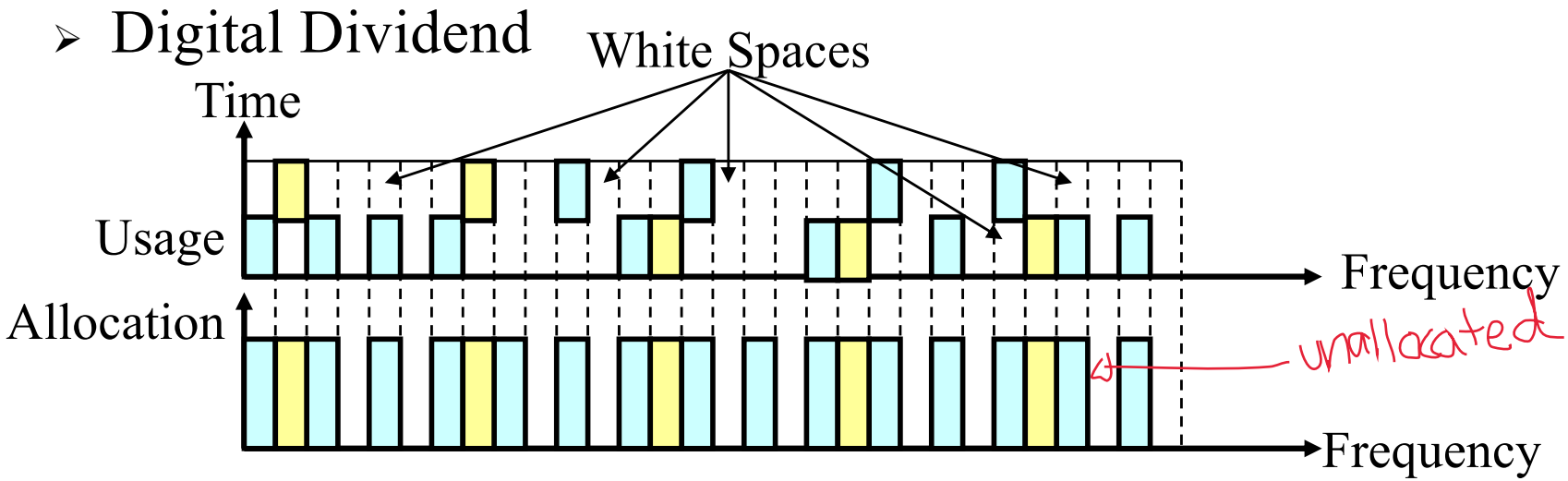
- Open-source software defined radio toolkit
- Uses Python and C++ on Linux
- Performance critical signal processing in C++
- Universal Software Radio Peripheral (USRP): General purpose computer for SDRs.
  - Host CPU for waveform specific processing, like modulation, demodulation
  - High-Speed operations in Field Programmable Gate Arrays (FPGAs)

Ref: GNU Radio, http://gnuradio.org/redmine/,
http://en.wikipedia.org/wiki/GNU_Radio
http://en.wikipedia.org/wiki/Universal_Software_Radio_Peripheral
Ettus Research, "USRP Bus Series Products," https://www.ettus.com/product/category/

©2020 Mahbub Hassan

Spectral White Spaces

- Any spectrum at a given area at a given time available for use on a non-interfering basis:
  - Unallocated spectrum
  - Allocated but under-utilized
  - Channels not used to avoid interferences in adjacent cells
  - Digital Dividend

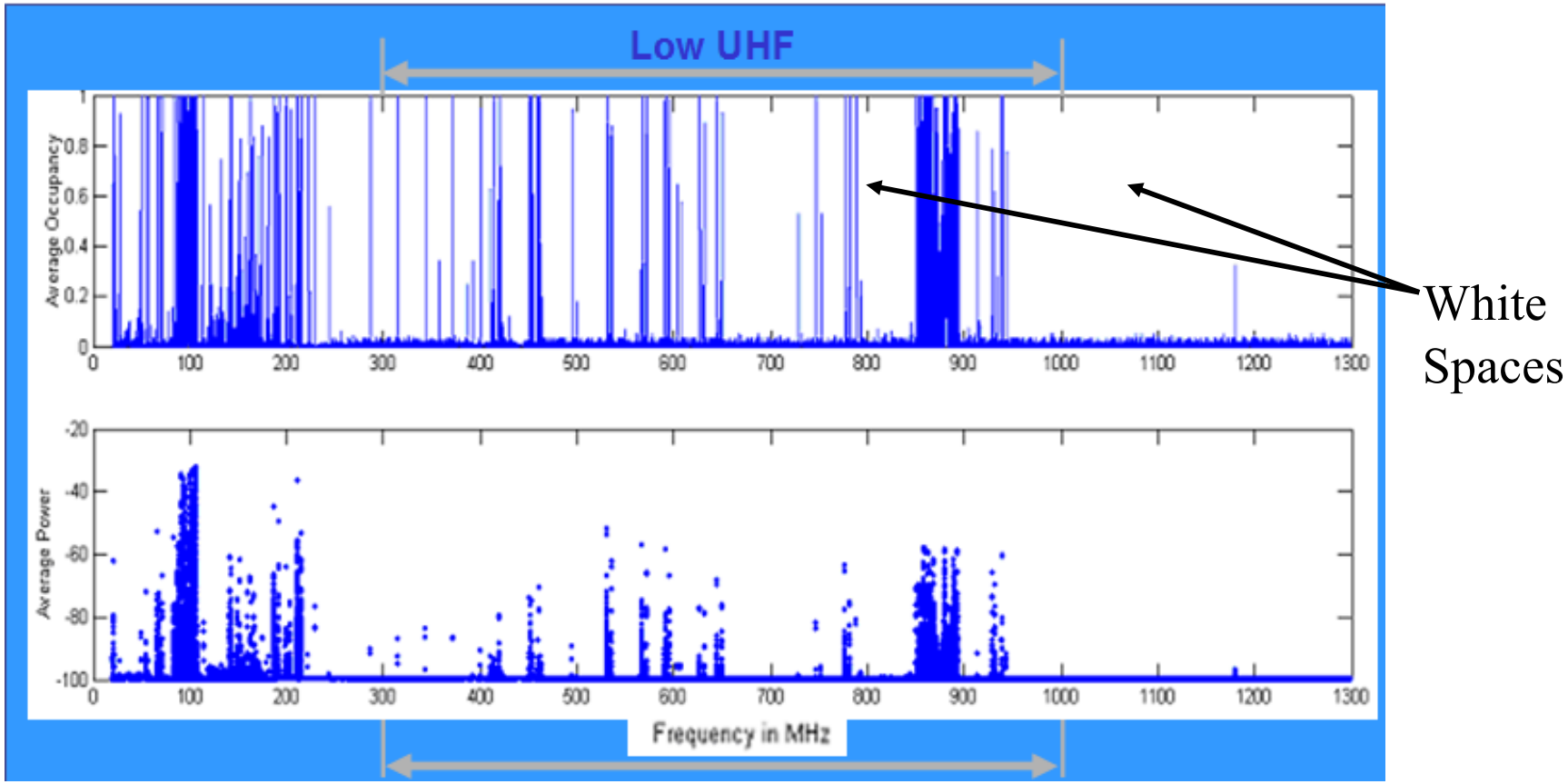


Ref: C. Gomez, "White Spaces for Rural Broadband," April 2013, http://www.itu.int/ITU-D/asp/CMS/Events/2013/PacificForum/ITU-APT-S3_Cristian_Gomez.pdf

©2020 Mahbub Hassan

Spectrum Usage Example

(Test conducted with antenna at a height of 22.1 metres above the ground in the rural sector west of Ottawa, Canada)



Ref: C. Stevenson, et al., "Tutorial on the P802.22.2 PAR for: *Recommended Practice for the Installation and Deployment of IEEE 802.22 Systems*" http://www.ieee802.org/802_tutorials/06-July/Rec-Practice_802.22_Tutorial.ppt

©2020 Mahbub Hassan

TVWS Databases

- FCC has authorized 10 companies to administer TVWS databases.
  - Get info from FCC database
  - Register fixed TVWS devices and wireless microphones
  - Synchronize databases with other companies
  - Provide channel availability lists to TVWS devices
- Europe requires devices to check every two hours

©2020 Mahbub Hassan

White Spaces Near WUSTL, St. Louis, USA

Channel Details

Channel Number	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
Power [dBm]	36			36	36	36	36	36	36	36	36	36					36	36	36		36																			36				36				36		
Channels 3 and 4		⊗	⊗																																															
KNLC:1173281													⊗	⊗																																				
KDTL-LD:1478335														⊗	⊗	⊗																																		
WPXS:1276019																				⊗																														
KMOV:1294216																						⊗	⊗	⊗																										
K25NG-D:1567407																							⊗	⊗	⊗																									
KPLR-TV:672275																								⊗	⊗	⊗																								
KEFN-CA:1090638																										⊗	⊗	⊗																						
KDNL-TV:619025																													⊗	⊗	⊗																			
K33GU:694719																															⊗	⊗	⊗																	
Wireless mic																																	⊗						⊗											
KSDK:428499																																	⊗	⊗	⊗															
KPTN-LD:1427975																																		⊗	⊗	⊗														
KPTN-LD:1446774																																		⊗	⊗	⊗														
Radio astronomy																																			⊗	⊗	⊗													
K38HD-D:1413449																																				⊗	⊗	⊗												
KETC:1325997																																					⊗	⊗	⊗											
KTVI:1010391																																									⊗	⊗	⊗							
WRBU:624511																																													⊗	⊗	⊗			
KUMO-LD:1431002																																																	⊗	⊗
Power [dBm]	36			36	36	36	36	36	36	36	36	36					36	36	36		36																			36				36				36		
Channel Number	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51

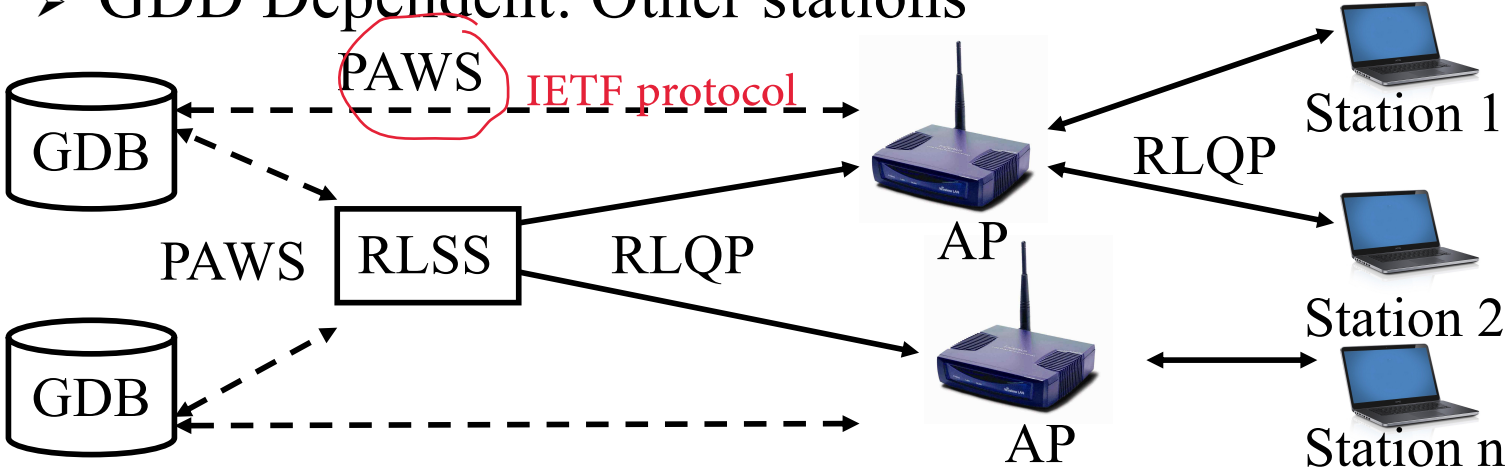
- 17 channels. Zipcode 63130.

Ref: Google Spectrum Database (not available anymore), https://www.google.com/get/spectrumdatabase/channel/

©2020 Mahbub Hassan

802.11af Database Operation

- Geolocation Database (GDB)
- Registered Location Secure Server (RLSS):
  - Provide faster response to access points (APs) locally in a campus.
  - May be Internet Service Provider (ISP) owned.
- Geolocation Database Dependent (GDD) entities:
  - GDD Enabling: Access Point
  - GDD Dependent: Other stations

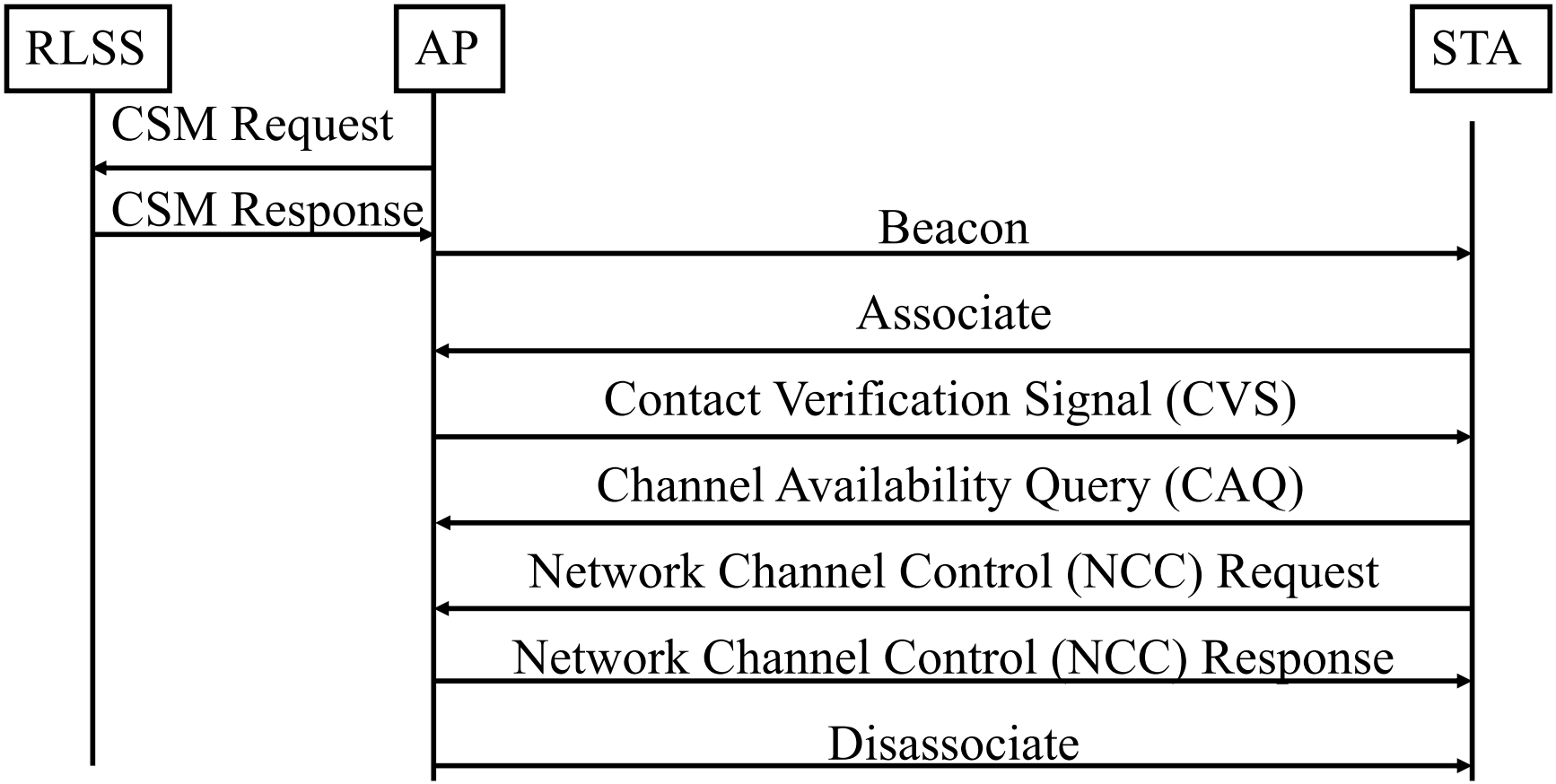


Ref: A. Flores, et al., "IEEE 802.11af: A Standard for TV White Space Spectrum Sharing," http://networks.rice.edu/papers/FINAL_article_80211af.pdf

©2020 Mahbub Hassan

Registered Location Query Protocol (RLQP)

- Protocol for exchange of white space map (WSM) among RLSS, APs, and stations, aka, Channel Schedule Management (CSM)



©2020 Mahbub Hassan

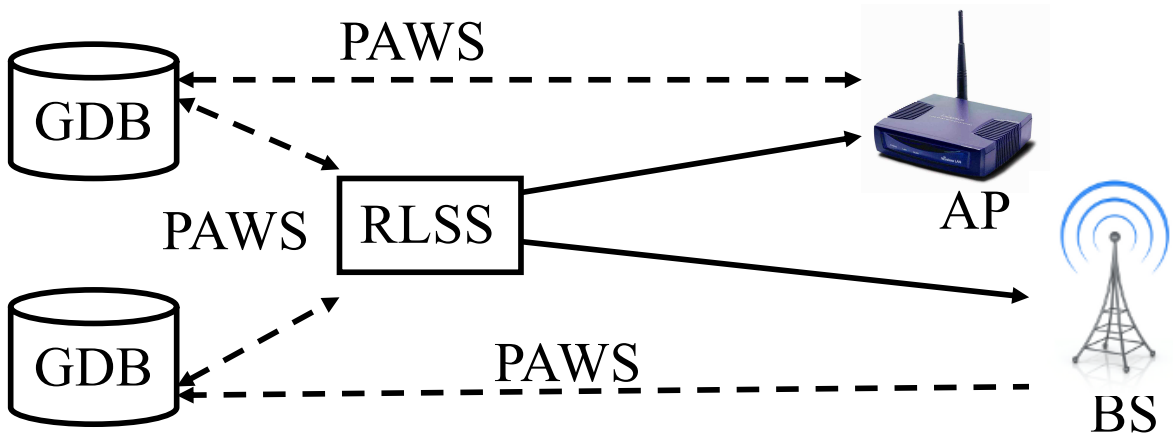
RLQP (Cont)

- CSM Request: APs ask other APs or RLSS about white space map
- APs broadcast beacons on all channels selected.
- Stations associate with the APs.
- Contact Verification Signal (CVS): APs tell their stations white space map and confirm that stations are still associated
- Contact Availability Query (CAQ): Stations ask AP, if they do not receive the map within a timeout interval
- CAQ Response
- Network Channel Control (NCC) Request: Sent by stations to APs requesting use of a channel. AP may forward to RLSS.
- NCC Response: Permission to transmit on requested channel
- Stations may be disassociated by APs if necessary

©2020 Mahbub Hassan

Protocol to Access White-Space (PAWS)

- IETF working group
- Mechanism to discover white space database
- Protocol to communicate with the database
- Interface Agnostic: 802.11af, 802.15.4m, 802.22, …
- Spectrum agnostic: 6 MHz, 7 MHz, 8 MHz, …
- Master Device: White-Space Device (WSD) connects to database
- Slave Device: WSD that get info from master devices



Ref: V. Chen, et al, ed. "Protocol to access White-Space (PAWS) Databases," Feb 2014, http://datatracker.ietf.org/doc/draft-ietf-paws-protocol/

©2020 Mahbub Hassan

PAWS (Cont)

- Stations should be able to discover WS Database, its regulatory domain. May be preconfigured similar to DNS or Certification Authorities.
- Listing Server: Web page listing all national database servers. Highly static ⇒ Can be cached by master
- Master may register with the database (model, serial, owner, …) of itself and its slaves
- Mutual authentication and authorization using certificates or passwords
- Master can then query the database
- The database should be able to push updates on channel availability changes
- Ensure security of discovery mechanism, access method, and query/response

Ref: A. Mancuso, Ed., at al, "Protocol to Access White-Space (PQWS) Databases: Use Cases and Requirements," IETF RFC 6953, May 2013, http://tools.ietf.org/pdf/rfc6953

©2020 Mahbub Hassan

PAWS (Cont)

- Allows WSD to specify geolocation, height, serial number, Certificates, device class, radio access technology (RAT), antenna gain, maximum EIRP, radiation pattern, spectrum mask, owner contact information
- Allows database to specify available spectrum, available area, allowed power levels
- Allows WSD to register its selected spectrum for use
- Allows privacy to WSD (encryption)

Ref: V. Chen, et al, ed. "Protocol to access White-Space (PAWS) Databases," Feb 2014, http://datatracker.ietf.org/doc/draft-ietf-paws-protocol/

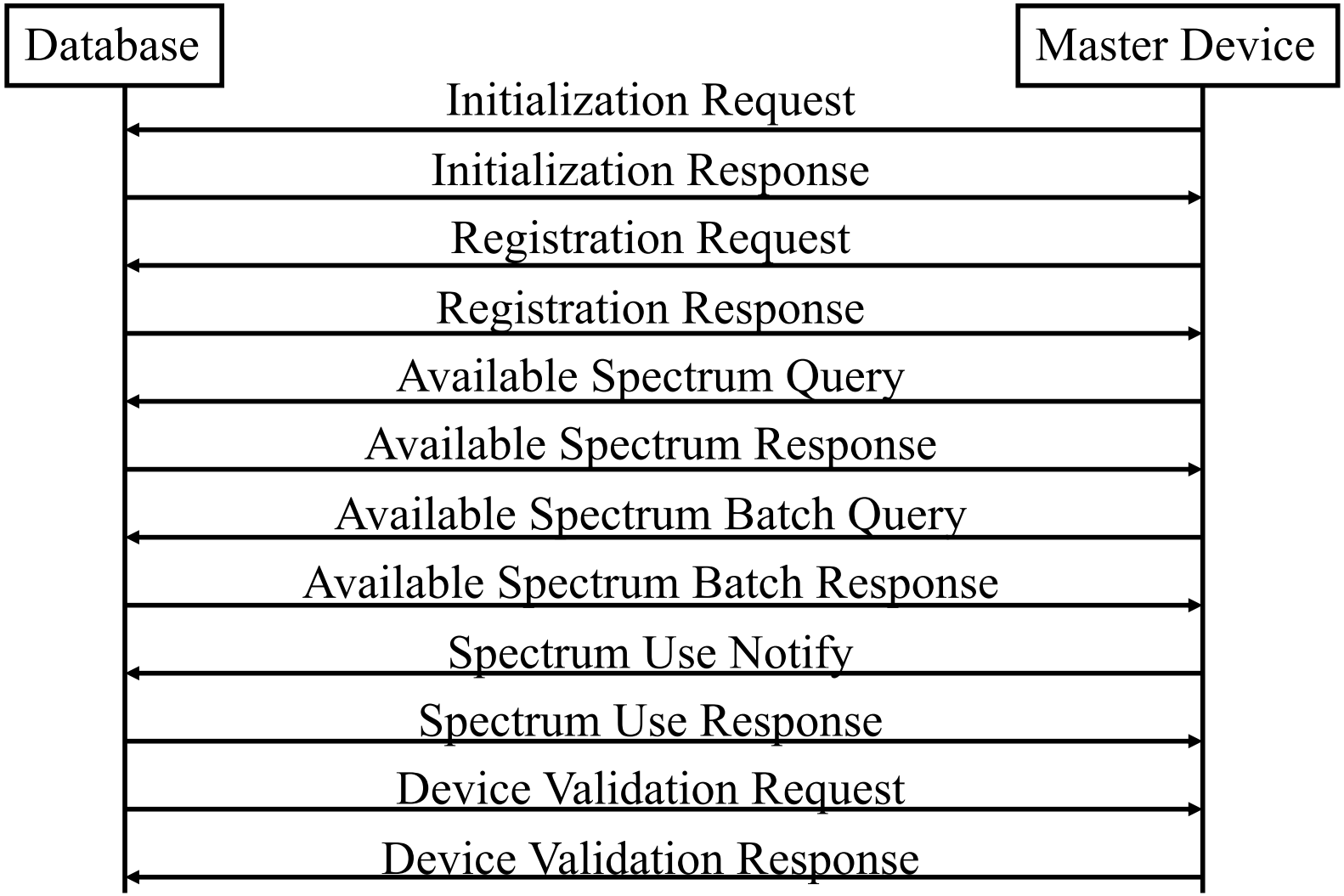
©2020 Mahbub Hassan

PAWS Messages (Cont)

- Listing Request/Response: To/from listing server (not shown)
- Initialization: Exchange capability, location, get rules
- Registration: Model, serial, antenna characteristics, owner, etc
- Available Spectrum: individual or batch request
- Spectrum Use: register used spectrum, location, antenna etc. Get time limits in response.
- Device Validation: Database may ask masters to authenticated slaves

©2020 Mahbub Hassan

PAWS Messages



©2020 Mahbub Hassan

802.11af-2014: White-Fi

- Basic Channel Unit (BCU): One TV Channel
  W = 6 MHz in USA
- Channel Bonding: Optional
  - Contiguous: 2W, 4W
  - Non-contiguous: W+W, 2W+2W

©2020 Mahbub Hassan

IEEE 802.11af OFDM Data Rates

- Modulation: 256-QAM highest
- Coding: 5/6 highest
- OFDM similar to 40 MHz in 802.11n down-clocked by 7.5x
- 6MHz channel: 144 total subcarriers, **108 Data**, 3 DC, 6 pilots, 36 Guard
- 7.5x down clocking
  - 0.4µs GI in 802.11n -→ 3µs in 802.11af (0.4x7.5=3)
  - 3.2µs data interval → 3.2x7.5 = 24µs
  - Total symbol interval = 24+3 = 27µs
- Data rate (single stream, single channel): 26.67 Mbps
- Max. Data rate (4 stream,4 channel): 26.67x16 = 426.7 Mbps

©2020 Mahbub Hassan

IEEE 802.11af Data Rates in Mbps (Single Stream)

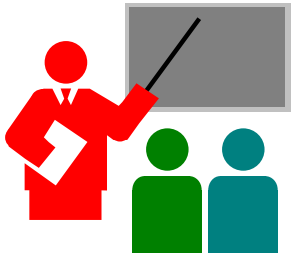
			6 and 7 MHz channels	
MCS Index	Modulation	Rate	6 μs GI	3 μs GI
0	BPSK	2-Jan	1.8	2
1	QPSK	2-Jan	3.6	4
2	QPSK	4-Mar	5.4	6
3	16-QAM	2-Jan	7.2	8
4	16-QAM	4-Mar	10.8	12
5	64-QAM	3-Feb	14.4	16
6	64-QAM	4-Mar	16.2	18
7	64-QAM	6-May	18	20
8	256-QAM	4-Mar	21.6	24
9	256-QAM	6-May	24	26.7

0.8x7.5 = 6

2-jan = ½
4-mar = ¾
3-feb = 2/3
6-may = 5/6

©2020 Mahbub Hassan

Summary



1. Analog to Digital conversion of TV channels has freed up spectrum in 700 MHz band ⇒ White Space.
2. 700MHz allows long-distance communication, useful for rural areas
3. FCC has allowed license-exempt use of some of the white space in TV bands. Requires software defined radio.
4. IEEE 802.11af White-Fi spec achieve up to 426.7 Mbps using OFDM, 4-stream MIMO, 256-QAM@5/6.
5. PAWS is the protocol for accessing white space databases.

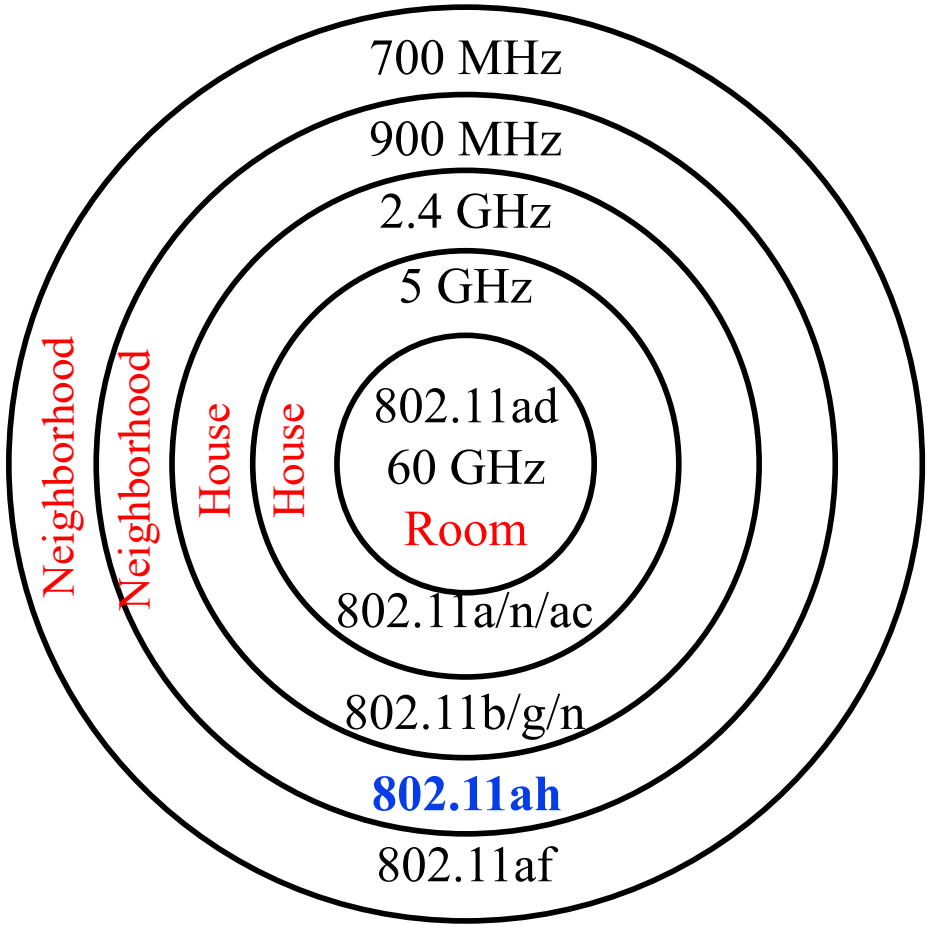
©2020 Mahbub Hassan

IEEE 802.11ah-2017 (a.k.a HaLow)

©2020 Mahbub Hassan

802.11 Standards: Ranges

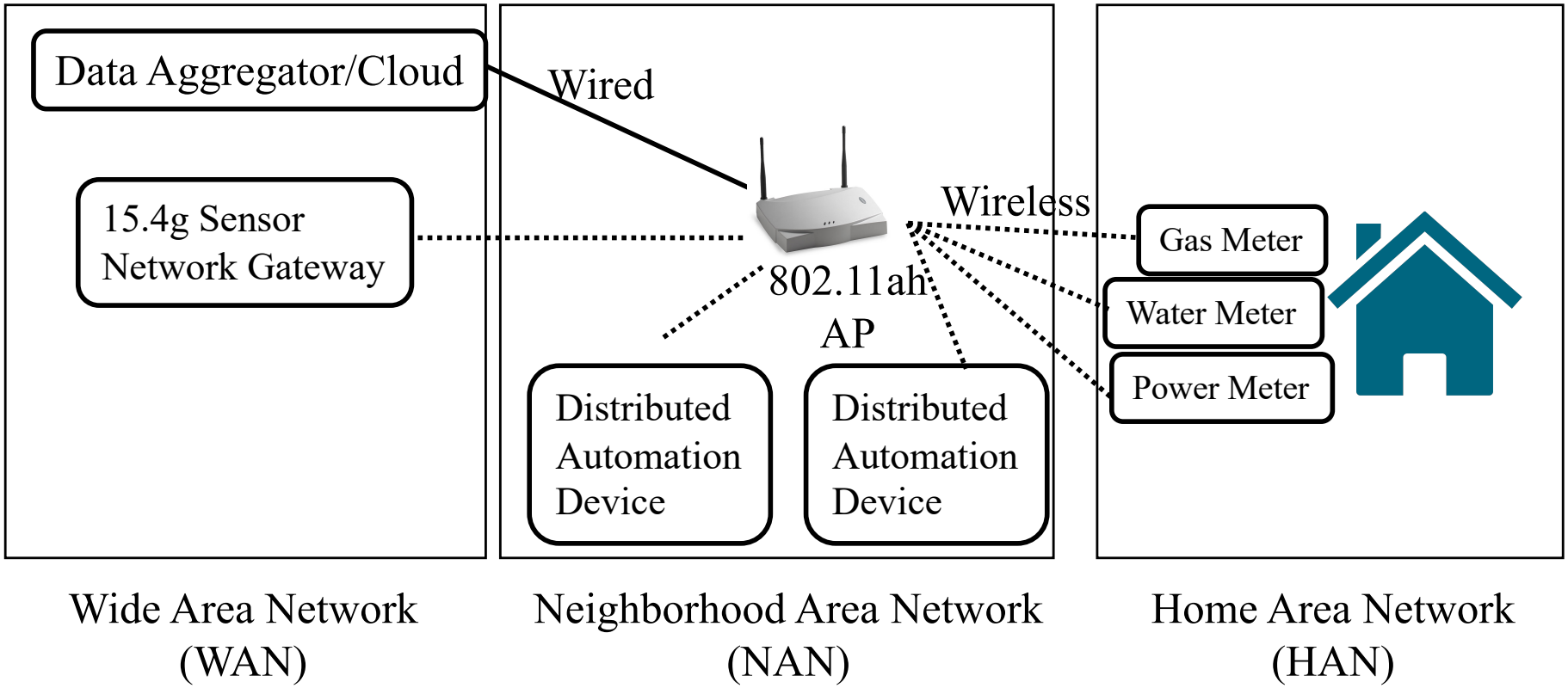
- 150 kbps to 78 Mbps per spatial stream (up to 4 streams)



Ref: J. DeLisle, "What's the difference between 802.11af and 802.11ah," Microwave and RF, Oct 2015, http://mwrf.com/active-components/what-s-difference-between-ieee-80211af-and-80211ah

©2020 Mahbub Hassan

Sample Application



Ref: H. Wei, "Self-Organizing Energy Efficient M2M Communications," http://cc.ee.ntu.edu.tw/~ykchen/1123-HWei.pdf

©2020 Mahbub Hassan

802.11ah PHY

1. 802.11ac PHY **down clocked** by 10X
   - 2/4/8/16 MHz channels in place of 20/40/80/160 MHz in ac
   - 20 MHz 11ac and 2 MHz 11ah both have 64 FFT size and 48 data subcarriers + 4 pilots $\Rightarrow$ 1/10th inter-carrier spacing
     $\Rightarrow$ 10X longer Symbols $\Rightarrow$ Allows 10X delay spread
     $\Rightarrow$ All times (SIFS, ACKs) are 10x longer
   - New 1 MHz PHY with 24 data subcarriers

many IoT devices require small bandwidth

2. **Adjacent channel bonding**: 1MHz+1MHz = 2 MHz
3. All stations have to support 1MHz and 2MHz
4. Up to **4 spatial streams** (compared to 8 in 11ac)
5. 1 MHz also allows a new MCS 10 which is MCS0 with 2x repetition $\Rightarrow$ Allows 9 times longer reach than 2.4GHz
6. **Beam forming** to create sectors

Ref: W. Sun, M. Choi, and S. Choi, "IEEE 802.11ah: A Long Range 802.11 WLAN at Sub 1 GHz," River Journal, 2013, pp. 1-26, http://riverpublishers.com/journal/journal_articles/RP_Journal_2245-800X_115.pdf

©2020 Mahbub Hassan

Example

- If we reduce the clock speed of 802.11ac by a factor of 10, what would be the new symbol rate (symbols/s)?

802.11ac has a symbol duration of 3.6 μs (for 400 ns GI).

New symbol duration with a 10x slower clock = 36 μs

New symbol rate = $1/(36 \times 10^{-6})$ = 27,777 sym/s

©2020 Mahbub Hassan

Example

- In USA, 902-928 MHz has been allocated for 802.11ah. How many different channels can be used if 16 MHz channel option is used?

902-928 MHz has a total bandwidth of 26 MHz. There is *only one (non-overlapping)* 16 MHz channel possible out of 26 MHz.

©2020 Mahbub Hassan

802.11 MAC

- **Large number of devices** per Access Point (AP)
  - Hierarchical Association Identifier (AID)
- **Relays** are used to allow connectivity outside the coverage area. Limited to 2-hops.
- **Power Savings Enhancements**:
  - Allows stations to sleep and save energy.
  - AP negotiates a Target Wake Time (TWT) for individual stations
- **Speed frame exchange** allows stations to exchange a sequence of frames for a TXOP.

Ref: E. Khorov, et al., "A survey on IEEE 802.11ah: An enabling networking technology for smart cities," Computer Communications, 2014, http://dx.doi.org/10.1016/j.comcom.2014.08.008

©2020 Mahbub Hassan

MAC Protocol Versions

- Protocol Version 0 (PV0) is same as that for b/a/g/n/ac
- Protocol version 1 (PV1) is optimized for IoT
  - Short headers
  - Null Data packets
  - Speed frame exchange
  - Improved channel access

©2020 Mahbub Hassan

Short MAC Header

- MAC Header shortened by 12-26 Bytes:
  - Removed: High throughput control, QoS, Duration field (No virtual carrier sensing)
  - Optional: 3rd address
  - 2-byte AID in place of some 6-byte addresses
  - Frame Control indicates what protocol version is being used
  - Sequence field indicates if 3rd /4th addresses are present

local addressing

is now gone

10byte at minimum

Legacy 802.11 36B	Frame Control 2B	Duration/ ID 2B	Addr 1 6B	Addr 2 6B	Addr 3 6B	Seq. Control 2B	Addr 4 6B	QoS Control 2B	HT Control 4B
802.11ah Downlink 10-24B	Frame Control 2B	AID 2B	BSS ID 6B	Seq. Control 0 or 2B	Addr 3 0 or 6B	Addr 4 0 or 6B			
802.11ah Uplink 10-24B	Frame Control 2B	BSS ID 6B	AID 2B	Seq. Control 0 or 2B	Addr 3 0 or 6B	Addr 4 0 or 6B			

©2020 Mahbub Hassan

Example

- A garbage bin sensor uses 802.11ah to upload 10 bytes of bin-fill-level data once every hour. Compared to legacy 802.11 (a/b/g/n/ac), the bin sensor has to upload how many less bytes per day?

Legacy 802.11 MAC header length = 36 byte

Total bytes uploaded with legacy 802.11 = 24x(10+36) = 1104 bytes/day

Total bytes uploaded with 802.11ah = 24x(10+10) = 480 bytes/day (min)

1104 - 480 = 624 less bytes per day

©2020 Mahbub Hassan

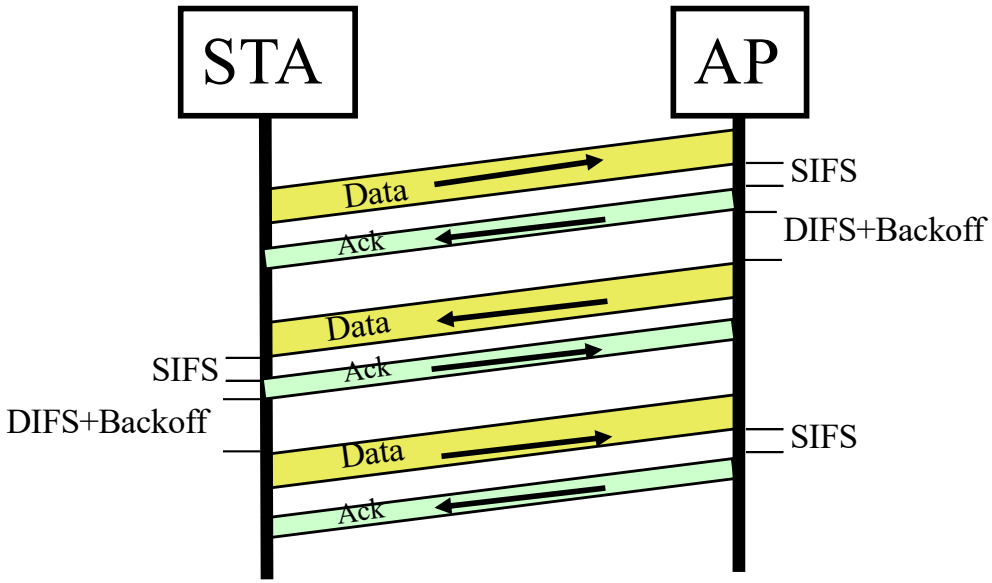
Null Data Packet (NDP)

- RTS/CTS/ACK has no data, but consumes too much MAC overhead
- 802.11ah removes the entire MAC header for these packets and identifies these packets via the *modulation and coding* (MCS) scheme at the PHY
- ACK, Block ACK, CTS, etc, all use different MCS

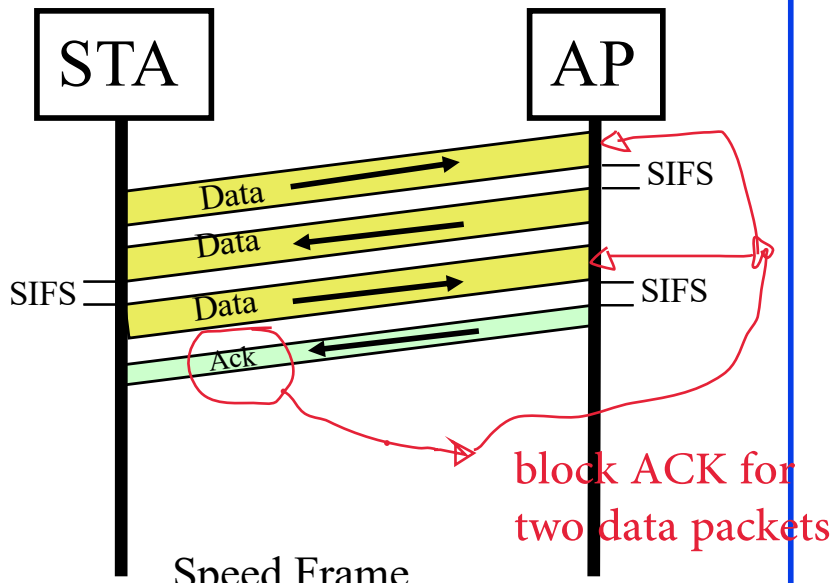
©2020 Mahbub Hassan

Speed Frame Exchange

- Also called "**Bi Directional Transmit** (BDT)"
- Initiator sends a frame with response indicator set to "long response"
  - Receiver can send data instead of ACK within a SIFS
  - Frames are sent until there are no more frames; block ACK at end



Legacy 802.11



Speed Frame Exchange in 802.11ah

©2020 Mahbub Hassan

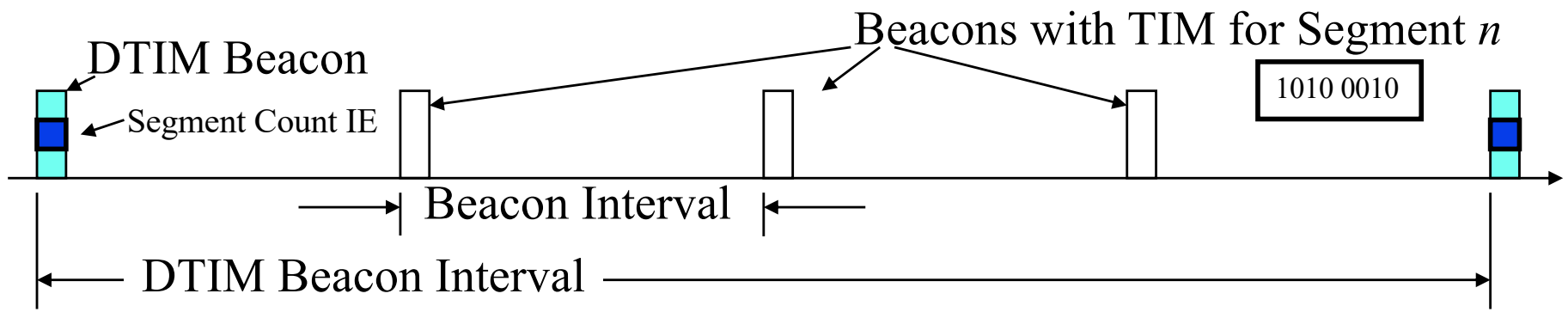
Types of Stations

- **High-Traffic**: Listens to Traffic Indication Map (TIM) in beacons and transmit accordingly within a restricted access window ⇒ *TIM Stations*
  - *Remain awake all the time to monitor all beacons*
- **Periodic Low-Traffic**: Negotiate a transmission time allocated in a periodic restricted access windows. Do not listen to beacons ⇒ *Non-TIM Stations*
- **Very Low-Traffic**: Send a poll to AP and get a transmission opportunity in response ⇒ *Unscheduled Stations*

©2020 Mahbub Hassan

Page Segmentation

- Announcing all buffered frames in each beacon
  $\Rightarrow$ 8096 bits would be wasted per beacon interval
- AP segments the TIM stations in segments and announces only one segment at a time.
- Every Delivery TIM (DTIM) interval, AP announces which segments have pending data and downlink, uplink periods.



©2020 Mahbub Hassan

Channel Access for TIM

- Each station knows what segments they belong to.
- Stations wake up every "*DTIM*" interval and find out which beacon they should listen to. The beacon has detailed map indicating which station has pending traffic and when stations can contend for access
- If the map indicates, AP has buffered packets for a station, the station uses DCF (distributed coordination function) to send a PS-poll to get the packet
- If a station has a packet to send, it listens to the map and uses DCF to send RTS in the allocated slot (two or more stations may be allocated to the same slot → collision is possible)
- Small number of stations per slot reduces chances of collisions
- Under low load, it becomes TDMA

©2020 Mahbub Hassan

Response Indication Deferral (RID)

- New virtual carrier sense mechanism replacing NAV (Network Allocation Vector)
- Can not use NAV since there is no duration field
- RID is also a time count down mechanism similar to NAV
  - NAV is MAC-based, RID is PHY-based
- RID is set after reception of PHY header
  NAV is set after reception of complete MAC frame
- RID is set based on the 2-bit response indication field in the PHY header (2 bits → 4 combinations)
  - Normal Response: RID ← SIFS + Ack or Block Ack time
  - NDP Response: RID ← SIFS + NDP Frame time
  - No Response (Broadcast frames): RID ← 0
  - Long Response: RID ← SIFS + Longest transmission time
    (Used with Speed Frame Exchange)

©2020 Mahbub Hassan

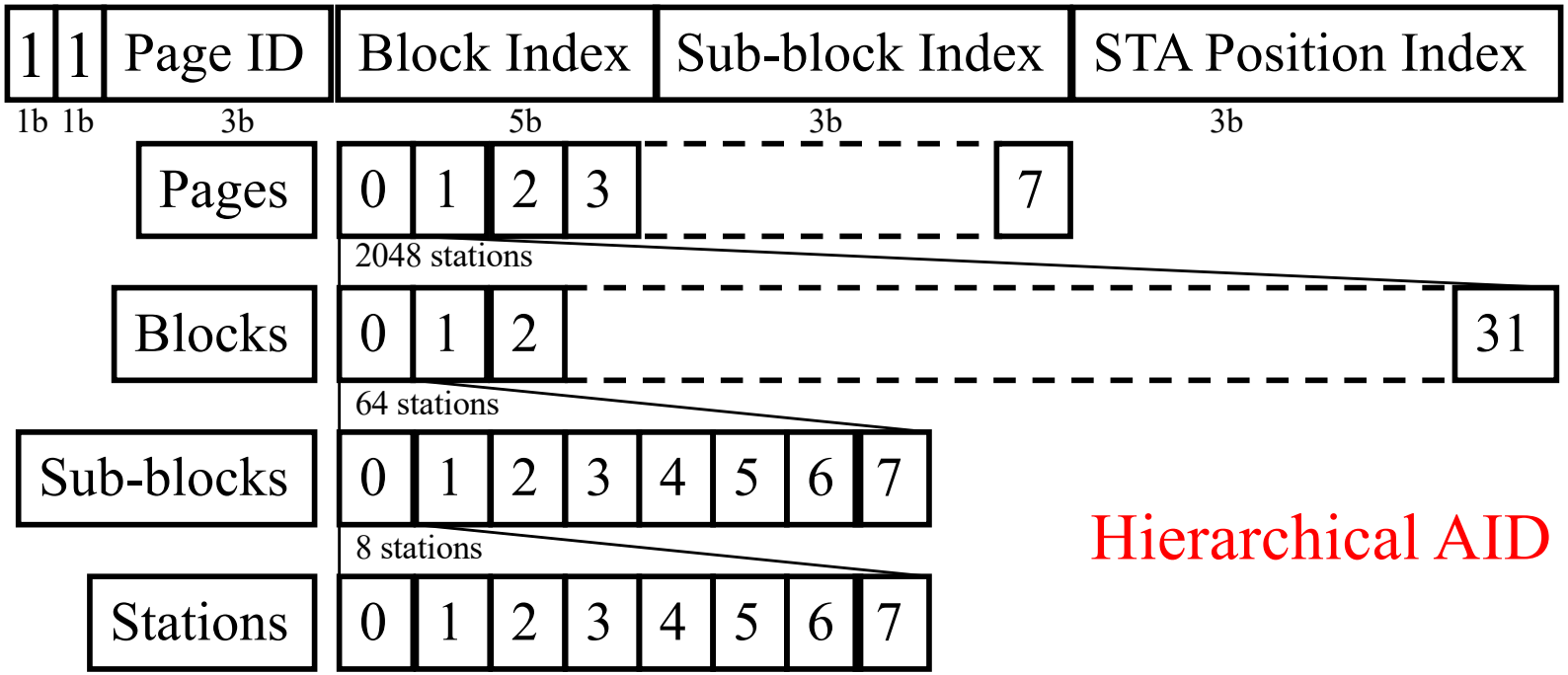
Power Enhancements

- Page Segmentation
- Restricted Access Window
- Target Wake Time

©2020 Mahbub Hassan

Association Identifier

- 802.11 b/g/n/ac use 11-bit identifier ⇒ 2007 stations
  - 2000+ bits required in "Traffic Indication Map (TIM)"
- 802.11ah uses 16-bit identifier ⇒ 8X stations
  - 8 pages of ~2^{11} stations each. Actually 2007 stations.
    Currently only page 0 is allowed. Page 1-7 are reserved.
    First 2 bits should be 11 to distinguish AID from duration and others.



Hierarchical AID

©2020 Mahbub Hassan

Restricted Access Window (RAW)

- Allows a set of slot to be restricted to a group of stations (pages/blocks/subblocks)
  ⇒ Reduces contention
- A TIM station can be allocated slots during restricted access window (RAW) to transmit/receive packets
- RAW is a part of "Contention Free Period"
- Access may granted for transmission, reception, polling, etc for one or a group of stations
- A RAW schedule is transmitted at the beginning of RAW interval
- A station can tell AP that it has a frame to transmit using a Uplink Data Indication (UDI) bit
  - Helps AP to workout which stations need access in the next round
- Dividing stations into groups and dividing time into slots for each group increases the efficiency under heavy load.
  - At 100% load: RAW gives close to 100%. Regular EDCF gives 0%.

because of high collision and backoff

©2020 Mahbub Hassan

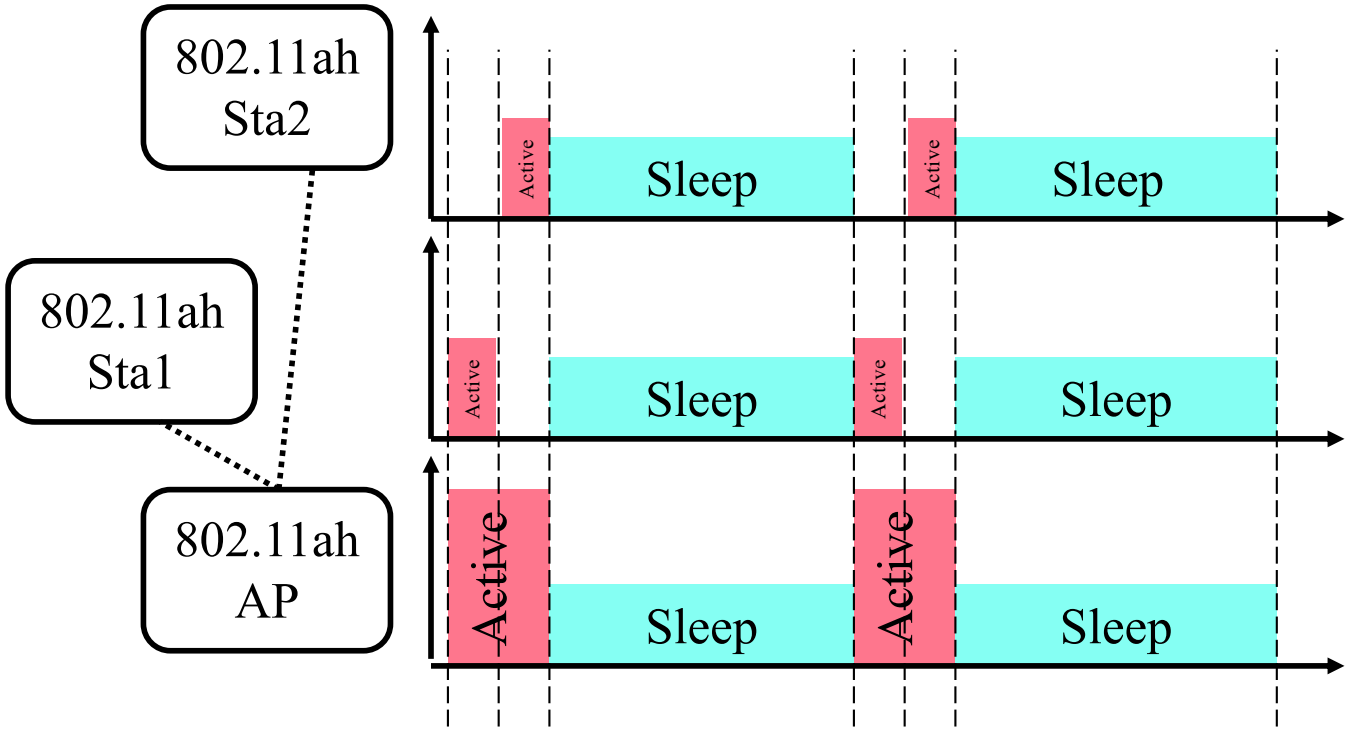
Other RAWs

- **Periodic RAW**: Period and duration of PRAW are announced by AP for *periodic* stations
- **Sounding RAW**: used for sector sounding
- **AP Power Management RAW**: used by AP to announce the time when it will be sleeping
- **Non-TIM RAW**: Protects transmission of non-TIM stations
  - Prevents TIM stations from hogging the channel
- **Triggering Frame RAW**: Used to allow stations to send PS-poll frames indicating their need to transmit

©2020 Mahbub Hassan

Target Wake Time (TWT)

- Non-TIM stations may sleep for a long time → waste for AP to include their buffer information in every beacon
- Non-TIM stations can provide a Target Wake Time (TWT), so the AP does not worry about these stations during their long sleeps
- Because sleeps can be very long, it is difficult to precisely provide waking tie in ms and sec. - → three parameters: Target-Wake-Time, Minimum-Wake-Duration, and Wake Interval mantissa.
- AP sends a "Null Data Packet (NDP)" to a station at its target wake up time containing buffering status. A station can then send a PS-poll and get its frames.
- AP can also sleep if all stations are sleeping



©2020 Mahbub Hassan

Sectorization

- AP can divide the space in sectors
  Each station is told which sector it belongs to.
- Beacon announces which sectors can transmit in this sector interval
- Some sector intervals may be for omni-directional transmissions
  Some may be for only some sectors
- Allows spatial reuse and increase throughput

©2020 Mahbub Hassan

802.11ah: Summary

1. 802.11ah runs at 900 MHz band ⇒ Longer distance
2. 802.11ah is 802.11ac down by 10x.
   It uses OFDM with 1/2/4/8/16 MHz channels.
   Longer symbols ⇒ Can handle longer multi-path
3. MAC is more efficient by reducing header, aggregating acks, null data packets, speed frame exchanges → good for short M2M communications
4. Saves energy by allowing stations and AP to sleep longer using Target Wakeup Time, Restricted Access Window

©2020 Mahbub Hassan

Wireless LAN III

IEEE 802.11ad-2012 (a.k.a WiGig)
60 GHz WLAN

©2020 Mahbub Hassan

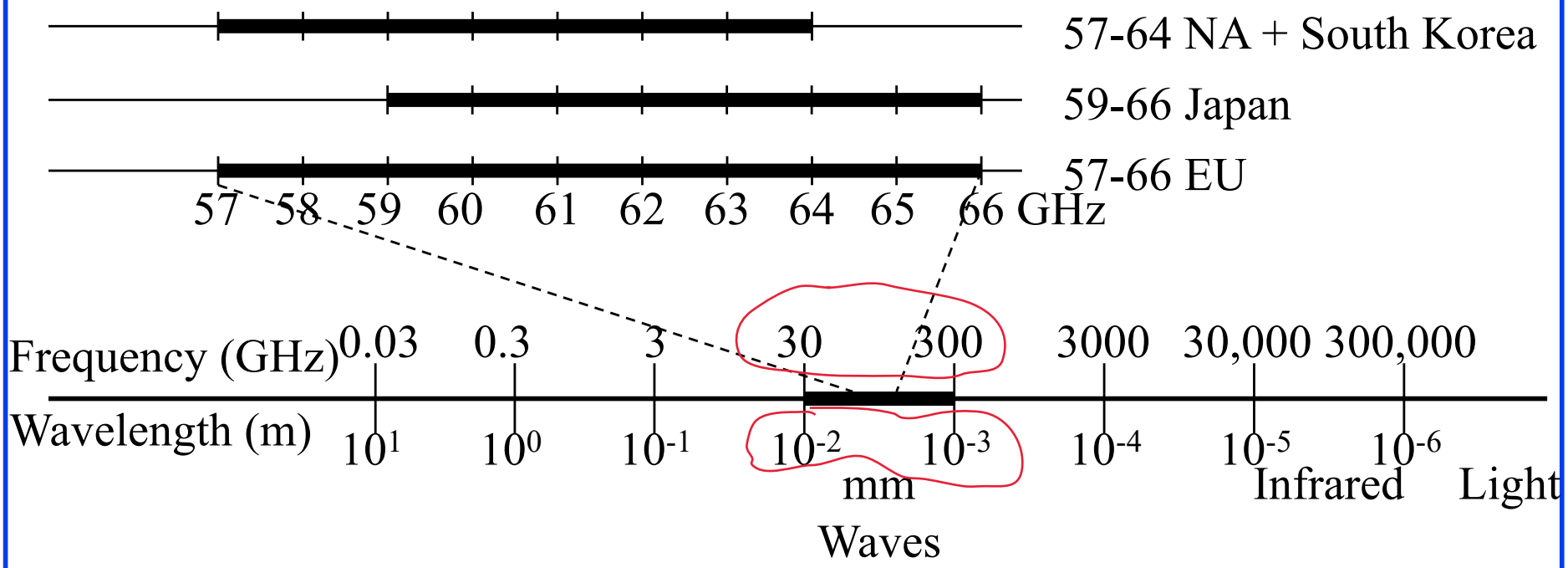
Overview

1. 60 GHz Frequency Allocations and characteristics
2. IEEE 802.11ad
   - PHY data rates
   - Network topology and MAC
   - Beamforming
   - Spatial Frequency Sharing

©2020 Mahbub Hassan

60 GHz Frequency Allocations

- 7-9 GHz in 57-66 GHz (**millimeter** waves 30GHz-300GHz)
- 4 Channels of ~ 2 GHz
- Significant activity after FCC made 57-64 GHz license-exempt



Ref: FCC, "Part 15 Rules for Unlicensed Operation in the 57-64 GHz Band," FCC13-112, August 2013, http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-13-112A1.pdf

©2020 Mahbub Hassan

Advantages of 60 GHz Band

1. **Large spectrum**: 7 GHz
   - 7 Gbps requires only 1 b/Hz (BPSK ok).
   - Complex 256-QAM not needed
2. **Small Antenna Separation**:
   5 mm wavelength. ¸/4=1.25 mm
3. **Easy Beamforming**: Antenna arrays on a chip.
4. **Low Interference**: Does not cross walls.
   Good for urban neighbors
5. **Directional transmissions**: Spatial reuse is easy
6. **Inherent security**: Difficult to intercept

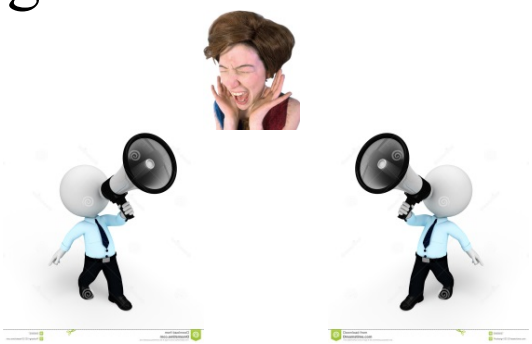
©2020 Mahbub Hassan

Disadvantages of 60 GHz Band

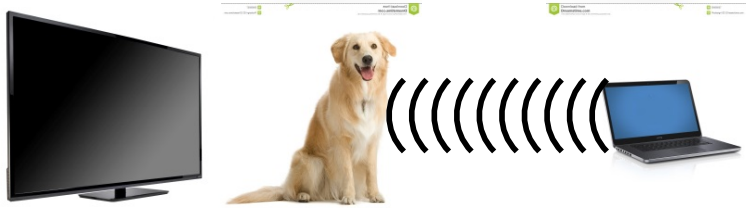
1. **Large Attenuation**: Attenuation / frequency^2
   - Strong absorption by Oxygen
   - Need larger transmit power
   - Need high antenna gain ⇒ directional antennas
   - Short Distance ~ 10m

focusing all energy to one direction

2. **Directional Deafness**: Can't hear unless aligned
   - Carrier sense not possible
   - RTS/CTS does not work
   - Multicast Difficult



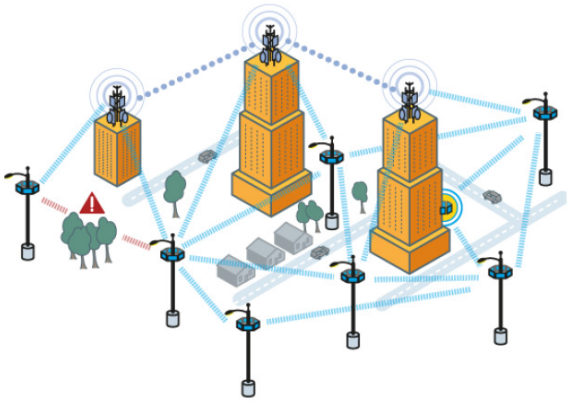
3. **Easily Blocked**: By a human/dog
   Need a relay



©2020 Mahbub Hassan

Multi-Gigabit Wireless Applications

- **Cable Replacement**: High-Definition Uncompressed streaming video
- Interactive **gaming**
- High-speed file transfer
- Wireless Mesh **Backhaul** (200-400m)



©2020 Mahbub Hassan

802.11ad OFDM PHY

- Total 355 subcarriers at inter-carrier spacing of 5.15626MHz ➔ 1830.47MHz channel bandwidth
- 336 data subcarriers (16 pilots, 3 DC)
- Guard interval = ¼ of the data symbol interval
  - GI = 1/5 of the total symbol interval = data interval+GI
- Symbol interval = ~242ns (=336/1386)
- Guard interval = ~48.4ns
- Modulation: QPSK, 16-QAM, 64-QAM
- Coding rates: ½, ¾, 5/8, 13/16
- Only single stream allowed

©2020 Mahbub Hassan

802.11ad OFDM Data Rates (Mbps)

MCS.	Modulation	Coding	Data Rate
13	SQPSK	1/2	693.00
14	SQPSK	5/8	866.25
15	QPSK	1/2	1386.00
16	QPSK	5/8	1732.50
17	QPSK	3/4	2079.00
18	16-QAM	1/2	2772.00
19	16-QAM	5/8	3465.00
20	16-QAM	3/4	4158.00
21	16-QAM	13/16	4504.50
22	64-QAM	5/8	5197.50
23	64-QAM	3/4	6237.00
24	64-QAM	13/16	6756.75

©2020 Mahbub Hassan

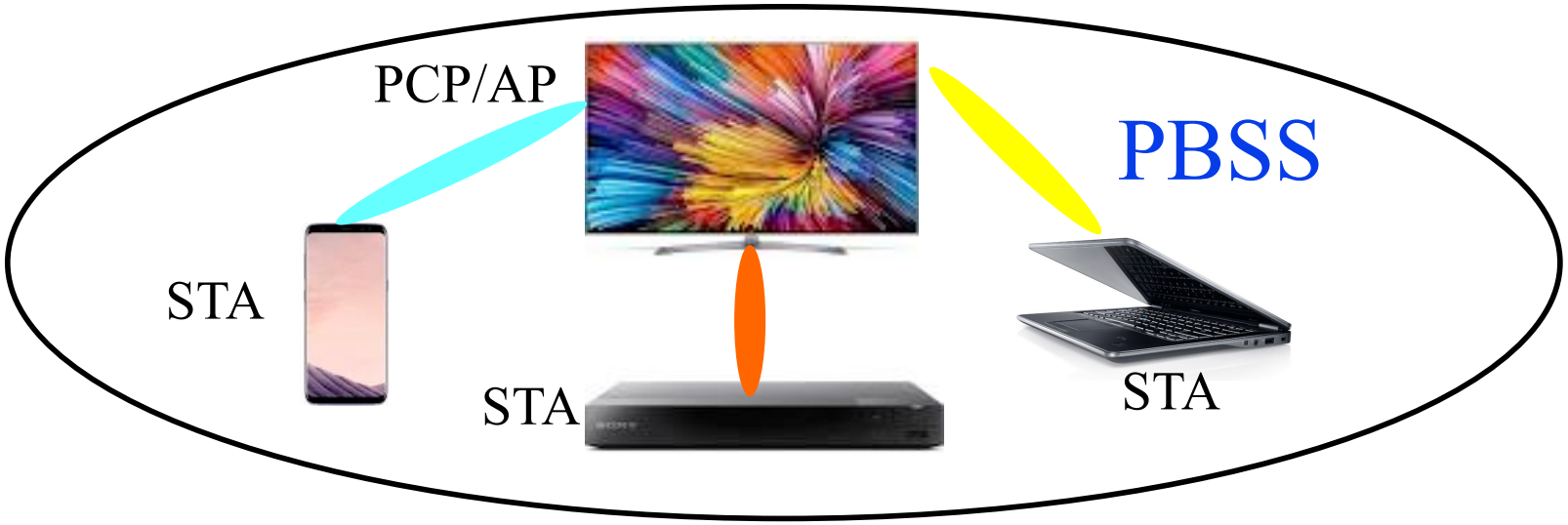
MAC Challenges for 60 GHz

- High path loss at 60 GHz
  - 28 dB higher than 2.4 GHz WLAN, 22 dB higher than 5 GHz WLAN
- Stations must have high antenna gain to overcome high path loss → directional antenna/beamforming
  - The narrower the beam, the higher the antenna gains
- Directional communication complicates MAC design
  - AP can talk to a STA only if their beams point to each other
  - Similarly, two STAs must point their beams to each other before they can exchange data
- MAC must always facilitate all stations to find the right beam directions
  - Different beam directions for different destinations
  - Beam directions change with mobility
  - Becomes challenging with many stations in a network

©2020 Mahbub Hassan

IEEE 802.11ad Network Topology

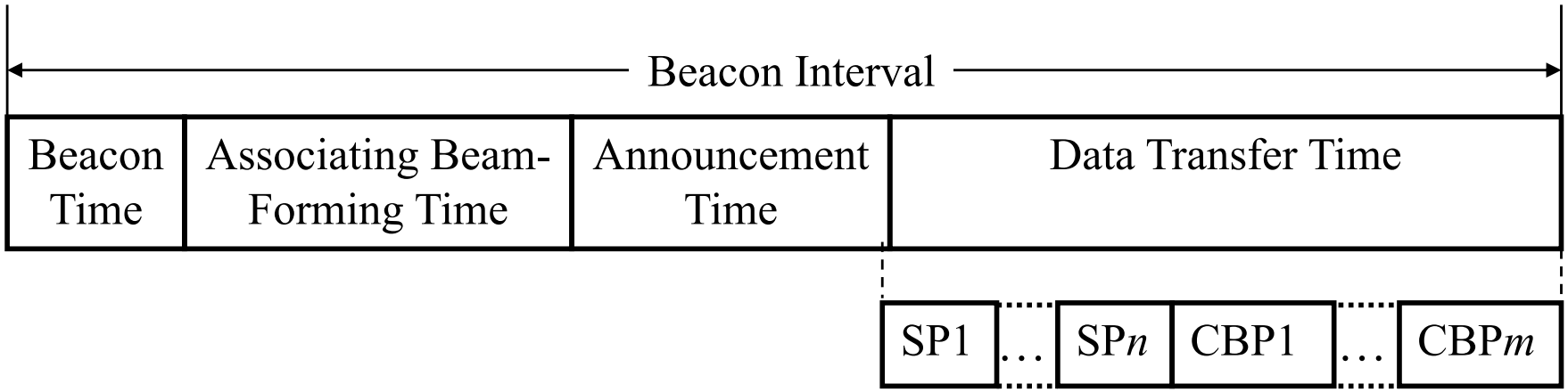
- **Personal Basic Service Set (PBSS):**
  Group of stations that communicate
- **PBSS Central Point (PCP)** provides scheduling and timing using beacons
  - Dedicated AP not needed, PCP function can be assumed by any 802.11ad device, such as a TV in the room can be PCP/AP
- **1 PCP/AP per PBSS, 1-254 non-PCP stations (STA)**



©2020 Mahbub Hassan

802.11ad MAC – Beacon Interval

- Each super-frame called "**Beacon Interval**" is divided into 4 *access periods*: Beacon Time (**BT**), Associating Beamforming Training (**A-BFT**), Announcement Time (**AT**), and Data Transfer Time (**DTT**)



©2020 Mahbub Hassan

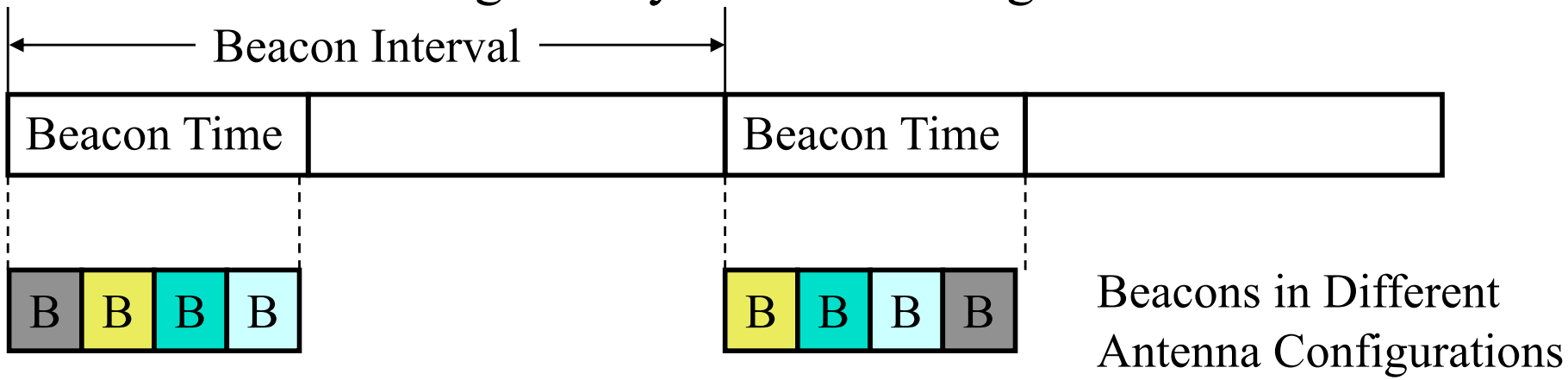
Access Periods in 802.11ad Beacon Interval

- BT: Only PCP can send a beacon during beacon time; PCP starts beamforming training in BT by sending training frames; STAs cannot transmit
- A-BFT: PCP performs antenna training with its members (STAs)
- AT: PCP polls members and receives non-data responses (STAs can request *service periods or SPs* to be scheduled during DTT)
- DTT: STA-to-STA exchange happens. All stations exchange data frames in a dedicated **service period (SP)** or by **contention in contention-based period (CBP)**
  - CBP uses Distributed Coordination Function (DCF); SP uses Hybrid Coordination Function (HCF)

©2020 Mahbub Hassan

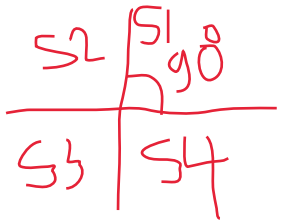
IEEE 802.11ad Beacon

- Beacon transmissions are omni-directional ⇒ One beacon is transmitted through every antenna configuration/sectors



©2020 Mahbub Hassan

Example 1



- A 802.11ad PCP/AP has a four-sector antenna with every sector covering 90 degrees. During a Beacon Time (BT), how many beacons the AP should transmit?

Beacons must be transmitted in omni-direction, so all STAs receive it. 360 degree coverage is achieved by four sectors (each sector covers 90 degrees). The AP therefore will send four beacons, one per sector.

©2020 Mahbub Hassan

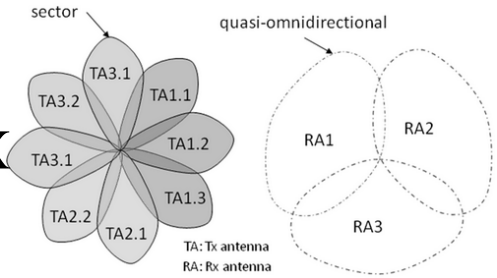
Beamforming Options

- The goal of beamforming is to choose the best beam direction pair that gives the highest gain
- Exhaustive search: exhaustively examine all beam pairs
  - E.g., 64 pairs for 8x8, 1024 pairs for 32x32 → O(B1xB2)
  - Time and energy consuming

# of sectors in device 1

#of sectors on device 2

TX



RX

- Searching with omni-directional antenna
  - Transmitter transmits on all beam directions (B1 transmissions)
  - Receiver uses omni-directional antenna to record RSS for all beam directions of the transmitter
  - Receiver selects the highest RSS as the best beam for the transmitter
  - The pair takes turn to find each others best beam direction (B2 transmissions) → O(B1+B2)

©2020 Mahbub Hassan

Example 2

- Two 802.11ad devices, STA1 and STA2, want to beamform. STA1 has 32 different antenna configurations (i.e., capable of steering the beam to 32 different directions). STA2 has only 4 beam directions. For Exhaustive Search, how many training frames are transmitted in total by these two devices before they discover the optimum beam pairs for communication?

Total combinations of antenna configurations between the two stations is 32x4 = 128. Therefore, 128 training frames are transmitted, one per specific pair of antenna configurations, before the best combination (pair) is finally selected.

©2020 Mahbub Hassan

Example 3

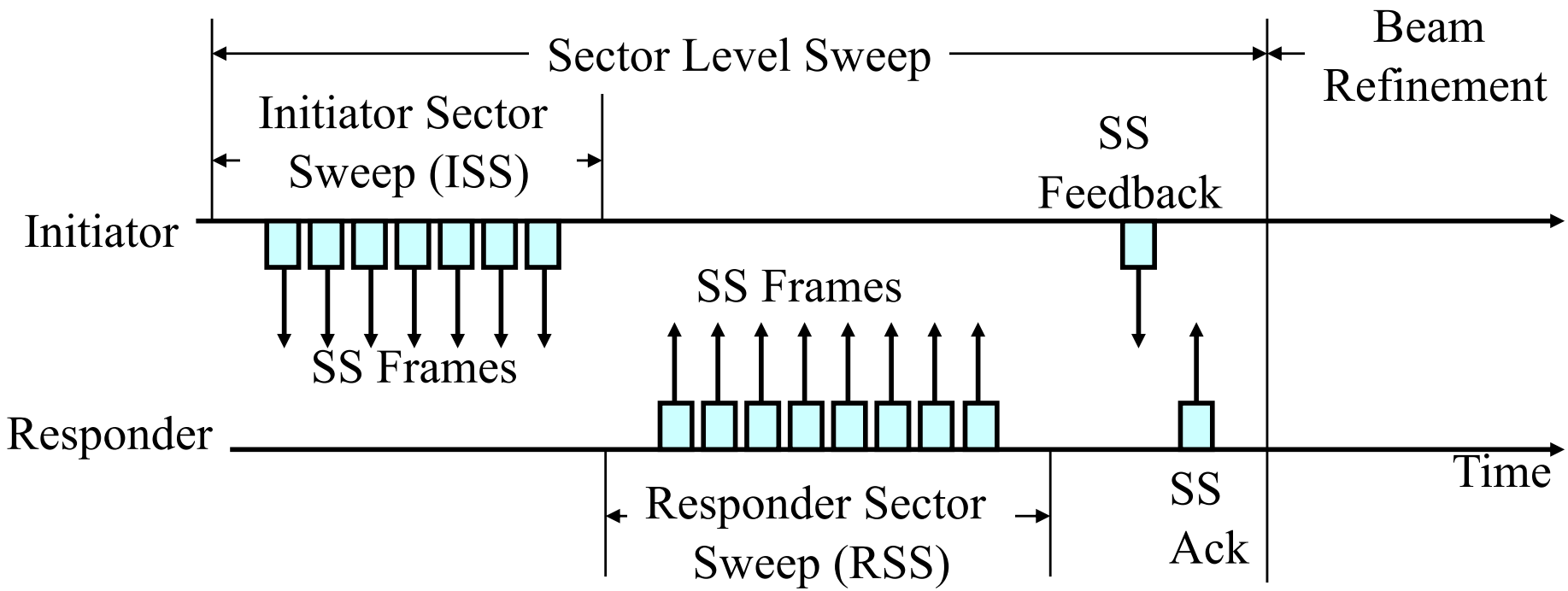
- Two 802.11ad devices, STA1 and STA2, want to beamform. STA1 has 16 different antenna configurations (i.e., capable of steering the beam to 16 different directions). STA2 has only 4 beam directions. For Omni-direction Antenna approach, how many training frames are transmitted in total by these two devices before they discover the optimum beam pairs for communication?

STA1 first transmits 16 training frames while STA2 is listening in omni-direction. Then STA2 transmits 4 frames while STA2 is listening. Total frames transmitted = 16+4 = 20.

©2020 Mahbub Hassan

IEEE 802.11ad Beamforming Training

- Each station finds the optimal antenna configuration with its recipient using a two-stage search --- SLS followed by BRP
- **Sector Level Sweep (SLS):** Sends in all sectors and finds the optimal *sector pair*
  - Sector → coarse direction (there can be several sharper beams within a sector)
  - Low data rate with sector-level beamforming
- **Beam Refinement Protocol (BRP):** Searches through the optimal sector to find the optimal parameters in that sector (identify a narrower beam)
  - Higher data rate (multi-gigabit) with beam refinement



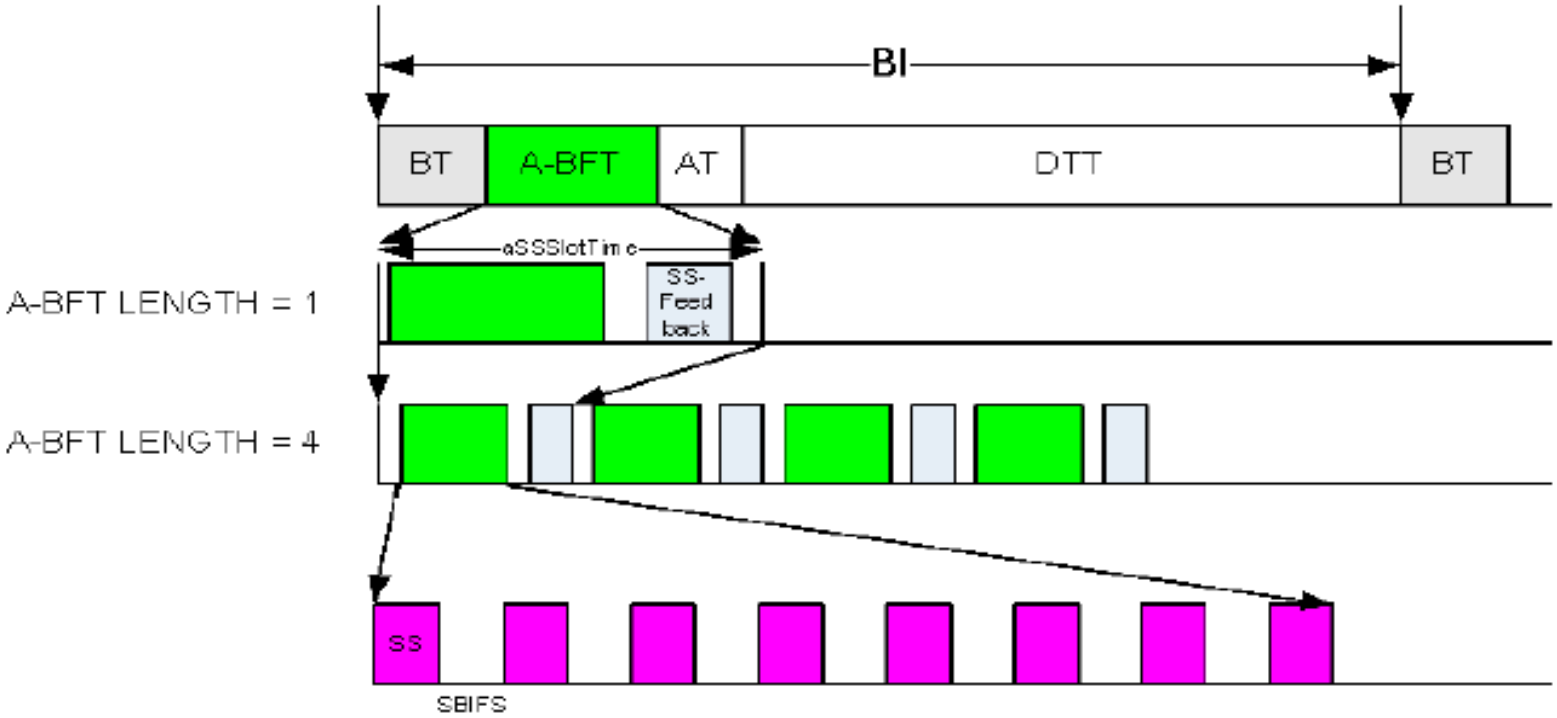
©2020 Mahbub Hassan

AP-STA Beamforming

- Takes place during BT and A-BFT durations
- During BT, AP transmits training frames on all its sectors; all STAs listen in omni-direction mode
- A-BFT duration is slotted; each STA selects a slot randomly and transmits training frames on all its sectors; AP listens in omni-direction mode
- Random slot selection may lead to collision. No feedback from AP to the STA if collision; STA tries in next beacon interval
- Only SLS is completed in BT and A-BFT; BFP is optional and may take place in DT duration

©2020 Mahbub Hassan

SLS in A-BFT



Example: consider that the A-BFT LENGTH = 8 and 3 mSTAs A, B and C are competing. All mSTAs choose a random value between [0,7]. mSTA A chooses value = 2, while mSTAs B and C choose a value = 5 which may result in a collision.

Akhtar and Ergen, "Efficient Network Level Beamforming Training for IEEE 802.11ad WLANs", SPECTS 2015

©2020 Mahbub Hassan

Example 4

- The table shows the received signal strength (RSS) at the responder for each transmitted training frame from the beam training initiator during SLS. There are four sectors for both initiator and responder, and the number after the station letter denotes the sector number. For example, row 1 shows the frame transmitted by station A on its sector 1. What is the optimum beam (sector) pair discovered after the SLS?

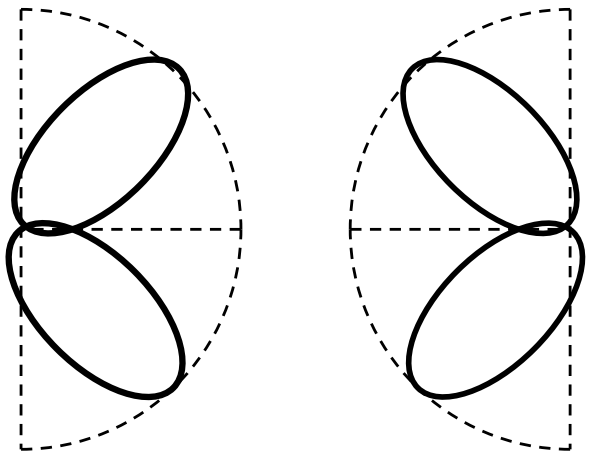
Transmitted Training Frame	RSS at Responder
A.1	-70 dBm
A.2	-62 dBm
A.3	-50 dBm
A.4	-64 dBm
B.1	-49 dBm
B.2	-71 dBm
B.3	-75 dBm
B.4	-80 dBm

The sector that produces the strongest signal is selected as the best sector. For A, the strongest sector is 3 (-50 dBm). For B, sector 1 produces the strongest signal at A (-49 dBm). The optimum beam pair for (A,B) therefore is (3,1).

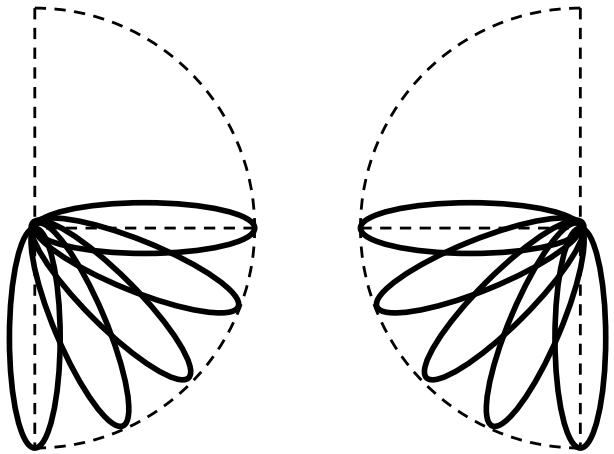
©2020 Mahbub Hassan

SLS vs. Beam Refinement

- SLS uses "coarse" (wider) beams
  - Quick, but low gain and hence low data rate
- Beam refinement finds narrower beams within the same sector
  - Increases gain and data rate, but takes additional time before communication can begin



Sector-Level Sweep



Beam Refinement

©2020 Mahbub Hassan

Spatial Frequency Sharing (SFS)

- Multiple transmissions may be scheduled on the same frequency at the same time if they don't interfere
- PCP asks stations to send results of any STA-STA beamforming training outcomes. PCP then has the complete knowledge of beam pairing among the stations within its PBSS. PCP then can work out which station pairs can share the same slot (will not interfere).

©2020 Mahbub Hassan

Example 6

a.k.a. sector pair

- In a given PBSS, all stations have 12 antenna sectors with 30 degree transmission angle. The table shows the beam pairs learned from beam training among 6 stations, A to F. For example, the first row of the table shows that A would use its beam #1 to communicate with B while B would use its beam #7 to communicate with A. If a communication, SP1, between A and B has already been scheduled, can SP2, a new communication between E and F, be spatially shared with SP1, i.e., be allocated during the same time slots without interference?

STA Pair	Beam Pair
(A,B)	(1,7)
(A,E)	(4,12)
(B,E)	(7,2)
(B,F)	(9,10)
(C,D)	(10,4)
(A,F)	(2,7)
(E,F)	(3,7)

No. During SP1, B will transmit on its beam #7, which is the same beam number found to be optimum to communicate with E (Row 3 in the table). Therefore B's transmissions to A during SP1 will affect E. SP2 therefore cannot be spatially shared with SP1 without interference.

©2020 Mahbub Hassan

Summary

1. 60 GHz, a.k.a. mm wave, has large bandwidth, small antenna separation allows easy beamforming and gigabit speeds but short distance due to large attenuation
2. Tri-band Wireless LAN devices with 2.4 GHz, 5.8GHz, and 60GHz are coming
3. 802.11ad LAN uses a PBSS central control point (PCP)
4. In all cases antenna alignment and tracking is required.
5. **Centralized** scheduling. Only **PCP** can send beacons. It sends beacons in all sectors.
6. Superframe (**Beacon Interval**) consists of Beacon Time, Associating Beamforming Training, Announcement Time, and Data Transfer Time
7. Announcement time is used for collecting requests from STAs
8. Data transfer can be pre-allocated or by contention
9. **Antenna training** is a 2-phase process. Sector selection and beam refinement.
10. Multiple transmission can take place on the same frequency at the same time (**Spatial Frequency Sharing**).

©2020 Mahbub Hassan

IEEE 802.11ay-2020 (expected)
Faster 60 GHz WLAN

©2020 Mahbub Hassan

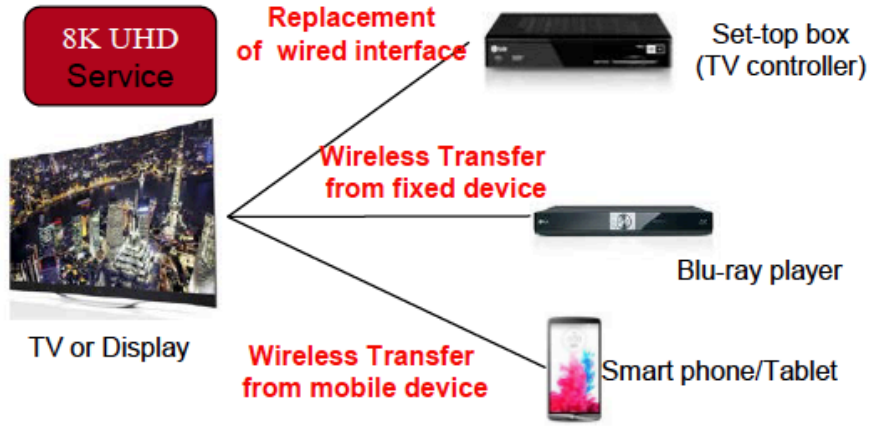
802.11ay

- 60GHz like 802.11ad, but faster than 802.11ad
  - 802.11ad is single stream and cannot bond channels (channel = 2.16GHz)
  - Single channel, single stream max speed: ~7Gbps
- 802.11ay expects to support 4 streams and bond multiple channels
  - 4 channels = 8.64GHz bandwidth
  - Max speed (4 channel, 4 stream) 170+ Gbps
- 802.11ay also offers longer range: up to 500m
- Expected in 2020

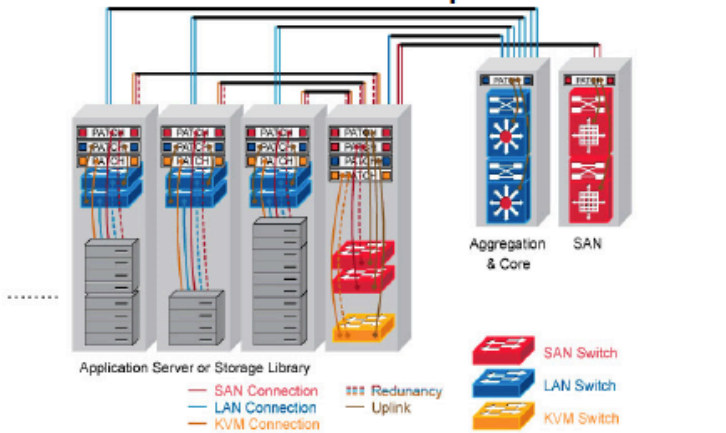
©2020 Mahbub Hassan

802.11ay projected use cases

Wireless Video

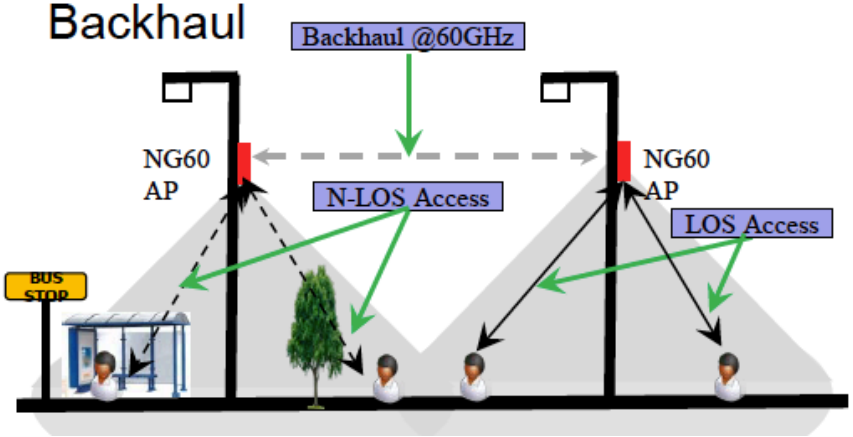


Data Center backup connection



VR/AR

Backhaul



Source: KEYSIGHT Technologies

©2020 Mahbub Hassan

Summary: Niche WiFi

- Mainstream WiFi operates in 2.4/5GHz band: hugely popular and used in many consumer products: mobile phone, tablets, laptops, …
  - IEEE 802.11a/b/g/n/ac/ax (11n=WiFi4, 11ac=WiFi5, 11ax=WiFi6)
- Niche WiFi: both sub-GHz and 60GHz
- Sub-GHz: 802.11af (700 MHz TV Whitespace: long-distance) and 802.11ah (900 MHz: IoT, sensors networks, home automation, large number of connections)
- 60GHz: 802.11ad (7Gbps; already penetrated some niche products) and 802.11ay (upcoming; 100+Gbps cable replacement, backhaul, …)

©2020 Mahbub Hassan

Bluetooth

Bluetooth Classic
Bluetooth Low Energy (BLE) - Bluetooth 4
BLE Advanced – Bluetooth 5

©2020 Mahbub Hassan

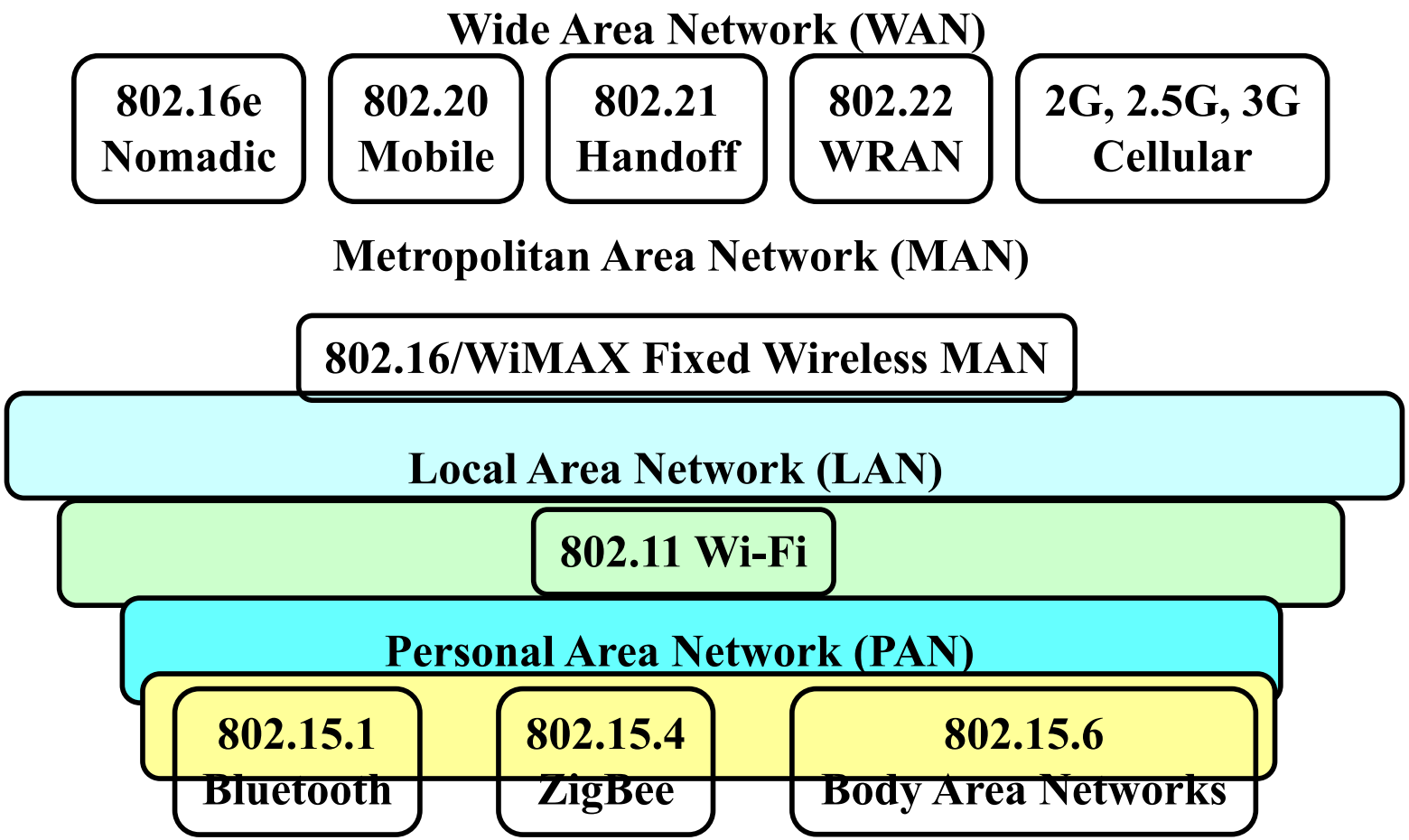
Overview

1. Bluetooth History: Wireless Personal Area Networks (WPANs) and IEEE 802.15 projects, Bluetooth Special Interest Group (SIG), Bluetooth Versions
2. Bluetooth Markets and Applications
3. Bluetooth Classic: Network Topology, Channel Structure, Modulation and Data Rates, Frequency Hopping, Packet Format, Operating States, Power Saving, Protocol Stack, Application Profiles
4. Bluetooth Low Energy (BLE): Channel Structure, Frequency Hopping, PHY, MAC
5. Bluetooth 5: PHY, Advertising, and Frequency Hopping Extensions

©2020 Mahbub Hassan

Wireless Personal Area Networks (WPANs)

- 10m or less



©2020 Mahbub Hassan

WPAN: Design Challenges

- **Battery powered**: Maximize battery life.
  A few hours to a few years on a coin cell.
- **Dynamic topologies**: Short duration connections and then device is turned off or goes to sleep
- **No infrastructure:** No access point or base station
- **Avoid Interference** due to larger powered LAN devices
- **Simple and Extreme Interoperability**: Billions of devices. More variety than LAN or MAN
- **Low-cost**: A few dollars

©2020 Mahbub Hassan

IEEE 802.15 Projects

we focus only on BT

- **IEEE 802.15.1-2005**: **Bluetooth** 1.2
- **IEEE 802.15.4-2011**: Low Rate (250kbps) WPAN – **ZigBee**
- **IEEE 802.15.4f-2012**: PHY for Active **RFID**
- **IEEE 802.15.6-2012**: Body Area Networking. Medical and entertainment. Low power
- **IEEE 802.15.7-2011**: Visible Light Communications

©2020 Mahbub Hassan

Bluetooth

Bluetooth SIG → IEEE 802.15.1 → Bluetooth SIG

- Started with Ericsson's Bluetooth Project in 1994 for radio-communication between cell phones over short distances
- Named after Danish king Herald Blåtand (=Bluetooth) (AD 940-981) who was fond of blueberries
- Intel, IBM, Nokia, Toshiba, and Ericsson formed Bluetooth SIG in May 1998
- Version 1.0A of the specification came out in late 1999.
- IEEE 802.15.1 approved in early 2002 is based on Bluetooth Later versions handled by Bluetooth SIG directly
- Key Features:
  - Lower Power: 10 mA in standby, 50 mA while transmitting
  - Cheap: $5 per device
  - Small: 9 mm^2 single chips

©2020 Mahbub Hassan

Example of a Bluetooth Chipset

MICROCHIP

RN4020

Bluetooth® Low Energy Module

Features

- Fully certified Bluetooth® version 4.1 module
- On-board Bluetooth Low Energy 4.1 stack
- ASCII command interface API over UART
- Device Firmware Upgrade (DFU) over UART or Over the Air (OTA)
- Microchip Low-energy Data Profile (MLDP) for serial data applications
- Remote commands over-the-air
- 64 KB internal flash
- Compact form factor: 11.5 x 19.5 x 2.5 mm
- Castellated SMT pads for easy and reliable PCB mounting
- Environmentally friendly, RoHS compliant
- Certifications: FCC, IC, CE, QDID, VCCI, KCC, and NCC

very thin!

Operational

- Single operating voltage: 1.8V to 3.6V (3.3V typical)
- Temperature range: -30°C to 85°C
- Low-power consumption
- Simple, UART interface
- Integrated Crystal, I^2C Interface, Internal Voltage Regulator, Matching Circuitry, and PCB Antenna
- Multiple IOs for control and status
- GPIO, ADC
- Three Pulse Width Modulation (PWM) outputs

RF/Analog Features

- ISM Band 2.402 to 2.480 GHz operation
- Channels 0-39
- RX Sensitivity: -92.5 dBm at 0.1% BER
- TX Power: -19.0 dBm to +7.5 dBm
- RSSI Monitor

12.5microwatt

Applications

- Health/Medical Devices
  - Glucose meters
  - Heart rate
  - Scale
- Sports Activity and Fitness
  - Pedometer
  - Cycling computer
  - Heart rate
- Retail
  - Point of Sale (POS)
  - Asset tagging and tracking
  - Proximity advertising
- Beacon Applications
- Internet of Things (IoT) Sensor tag
- Remote Control
  - Embedded Device Control
  - AV consoles and game controllers
- Wearable Smart Devices and Accessories
- Industrial Control
  - Private (custom) services
  - Low bandwidth cable replacement

©2020 Mahbub Hassan

Bluetooth Versions

IEEE

- **Bluetooth 1.1**: IEEE 802.15.1-2002
- **Bluetooth 1.2**: IEEE 802.15.1-2005. *Adaptive frequency hopping (avoid frequencies with interference)*.

SIG

- **Bluetooth 2.0** + Enhanced Data Rate (EDR) (Nov 2004): 3 Mbps using DPSK. For video applications. Reduced power due to reduced duty cycle

major milestone

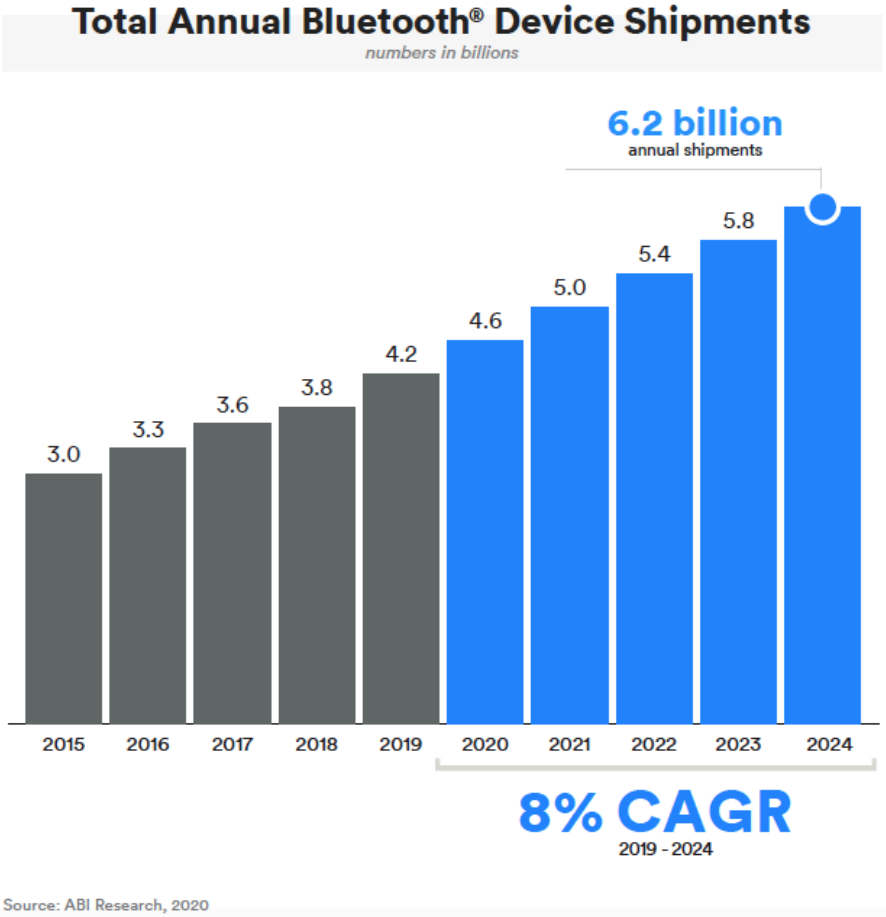
- **Bluetooth 4.0** (June 2010): Low energy. Smaller devices requiring longer battery life (several years). New incompatible PHY. Bluetooth Smart or BLE

another milestone

- **Bluetooth 5.0** (December 2016): Make BLE go faster and further.

©2020 Mahbub Hassan

The Rise of Bluetooth



48 BILLION

devices will be connected to the internet by the year 2021 — of those, **30%** are forecasted to include Bluetooth technology.

Source: Bluetooth SIG

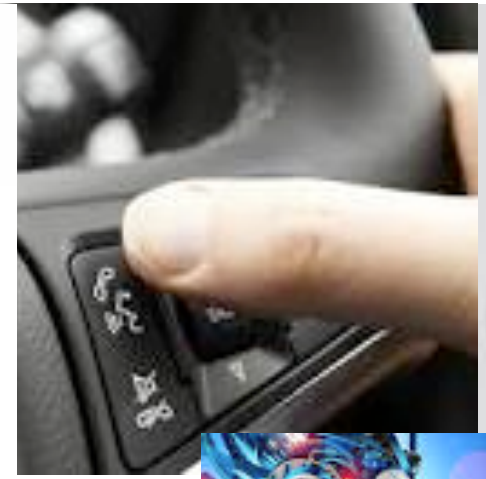
©2020 Mahbub Hassan

Bluetooth technology is factory installed in most new vehicles

87%

OF NEW CARS

come standard with Bluetooth® technology



The Bluetooth Impact

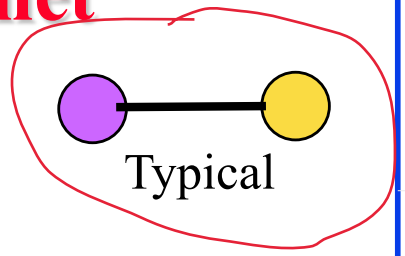
©2020 Mahbub Hassan

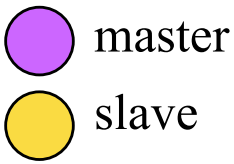
Bluetooth Classic

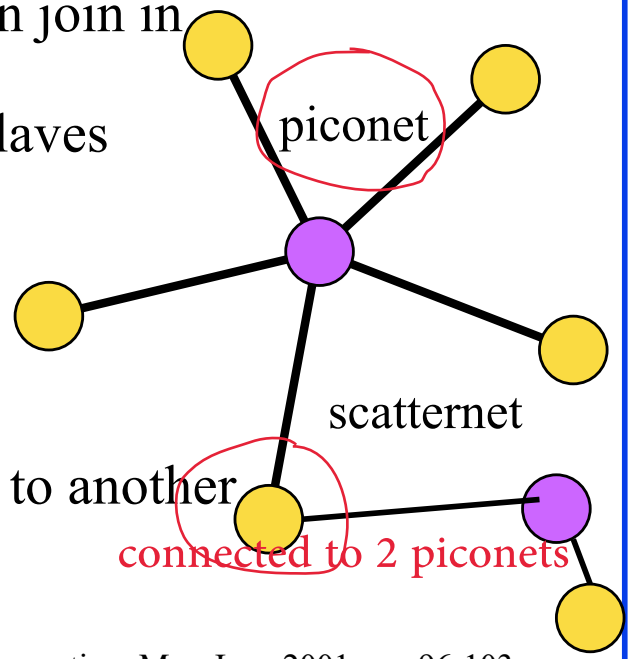
©2020 Mahbub Hassan

Bluetooth Network Topology: Piconet

- Piconet is formed by a master and many slaves (typically 1)
  - Up to 7 active slaves. Slaves can only transmit when requested by master
  - Up to 255 parked slaves
- Active slaves are polled by master for transmission
- Any device can become a master (initiator becomes master)
- Each station gets an 8-bit parked address
  $\Rightarrow$ 255 parked slaves/piconet
- A parked station can join in 2ms. Other stations can join in more time.
- Slaves can only transmit/receive to/from master. Slaves cannot talk to another slave in the piconet
- **Scatter net**: A device can participate in multiple Pico nets $\Rightarrow$ Timeshare and must synchronize to the master of the current piconet. *Active* in one piconet, *parked* in another.
- Routing protocol not defined (a node can only talk to another node if within Bluetooth range of 10m)



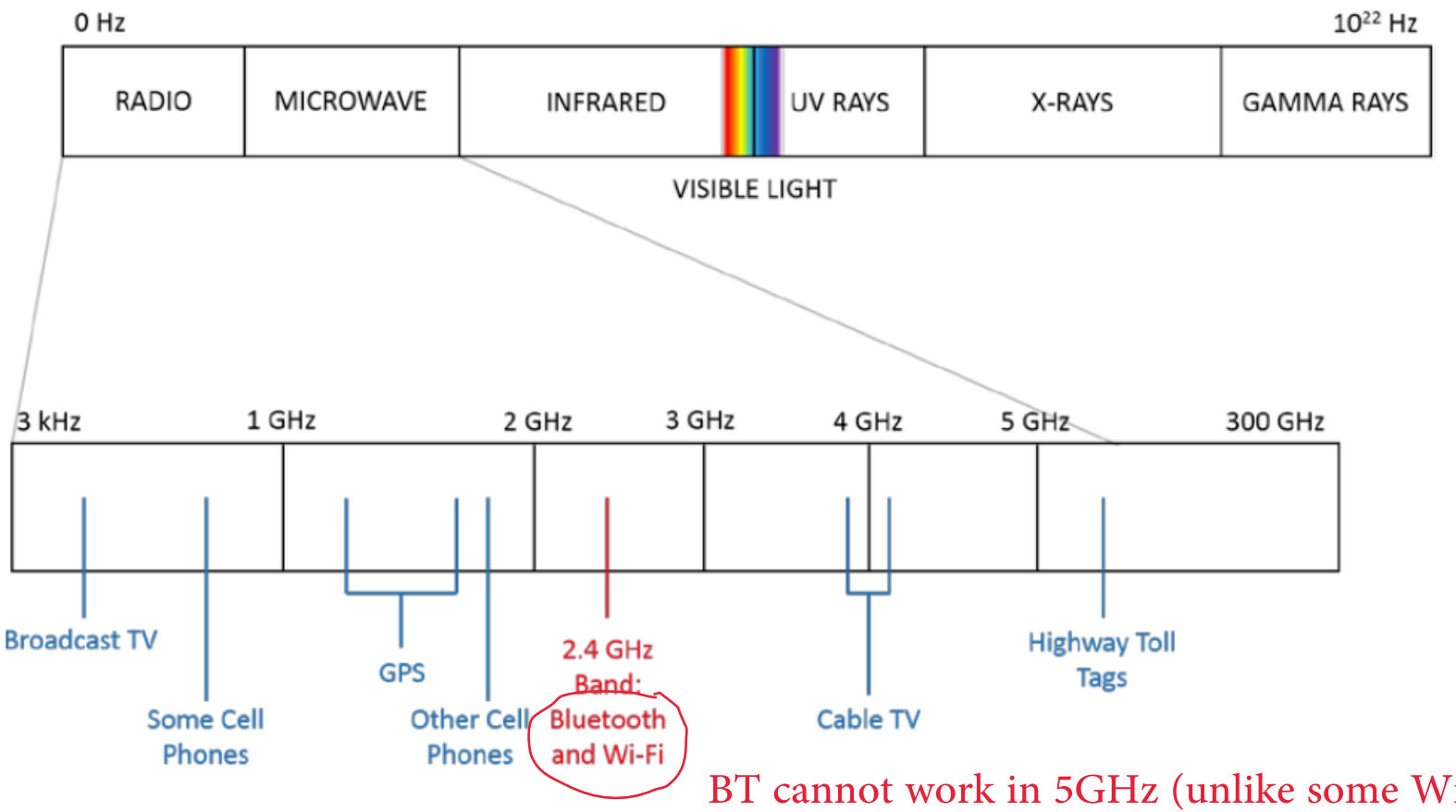




Ref: P. Bhagwat, "Bluetooth Technology for short range wireless Apps," IEEE Internet Computing, May-June 2001, pp. 96-103,

©2020 Mahbub Hassan

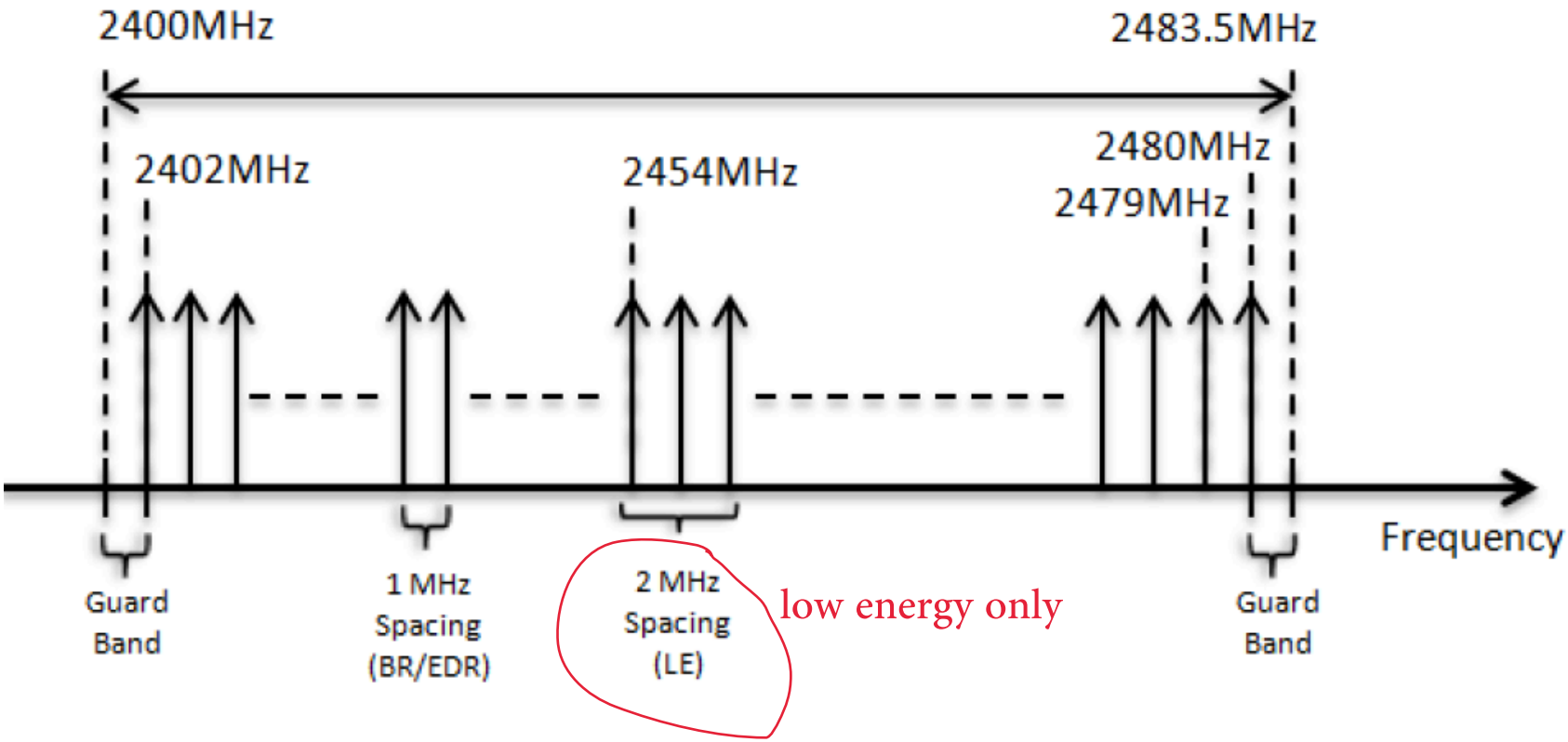
Bluetooth Operating Spectrum



BT cannot work in 5GHz (unlike some WiFi)

©2020 Mahbub Hassan

Bluetooth Channels



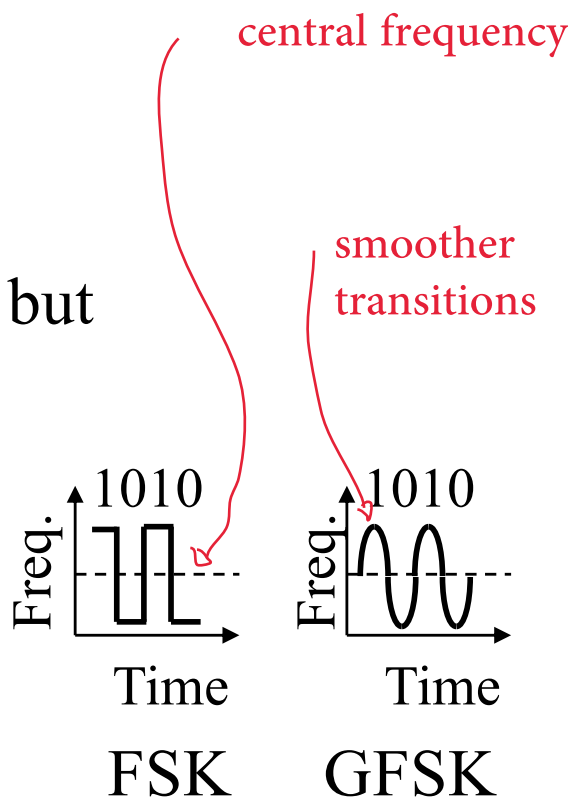
f_c = (2402+k) MHz; k = 0, 1, …, 78

k: channel index (79 1-MHz wide channels)

©2020 Mahbub Hassan

Modulation and Data Rate

- Basic rate (BR):
  - Binary Gaussian FSK (GFSK): 1 bit/symbol
  - Symbol duration = 1 μs: 1 Msps
  - Data rate: 1 Mbps
- Enhanced data rate (EDR):
  - Symbol duration is still 1 μs (1 Msps), but
  - μ/4-DQPSK; 2 bits/symbol; 2 Mbps
  - 8DPSK: 3 bits/symbol; 3 Mbps

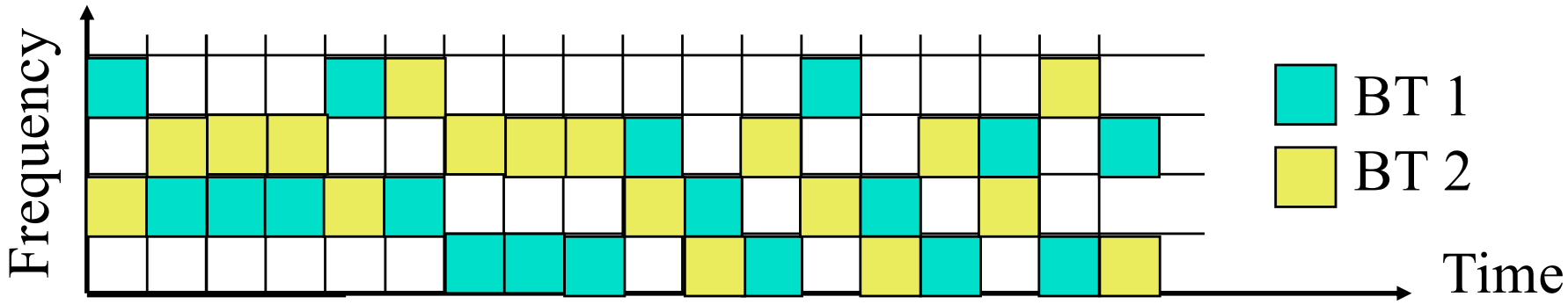


©2020 Mahbub Hassan

FHSS

Frequency Hopping (1)

- Unlike WiFi, Bluetooth constantly switches channel within the same connection to avoid collisions with other nearby Bluetooth communications
- No two packets are transmitted on the same channel/frequency, but frequency is never switched in the middle of a packet transmission
- Such frequency switching is known as frequency hopping



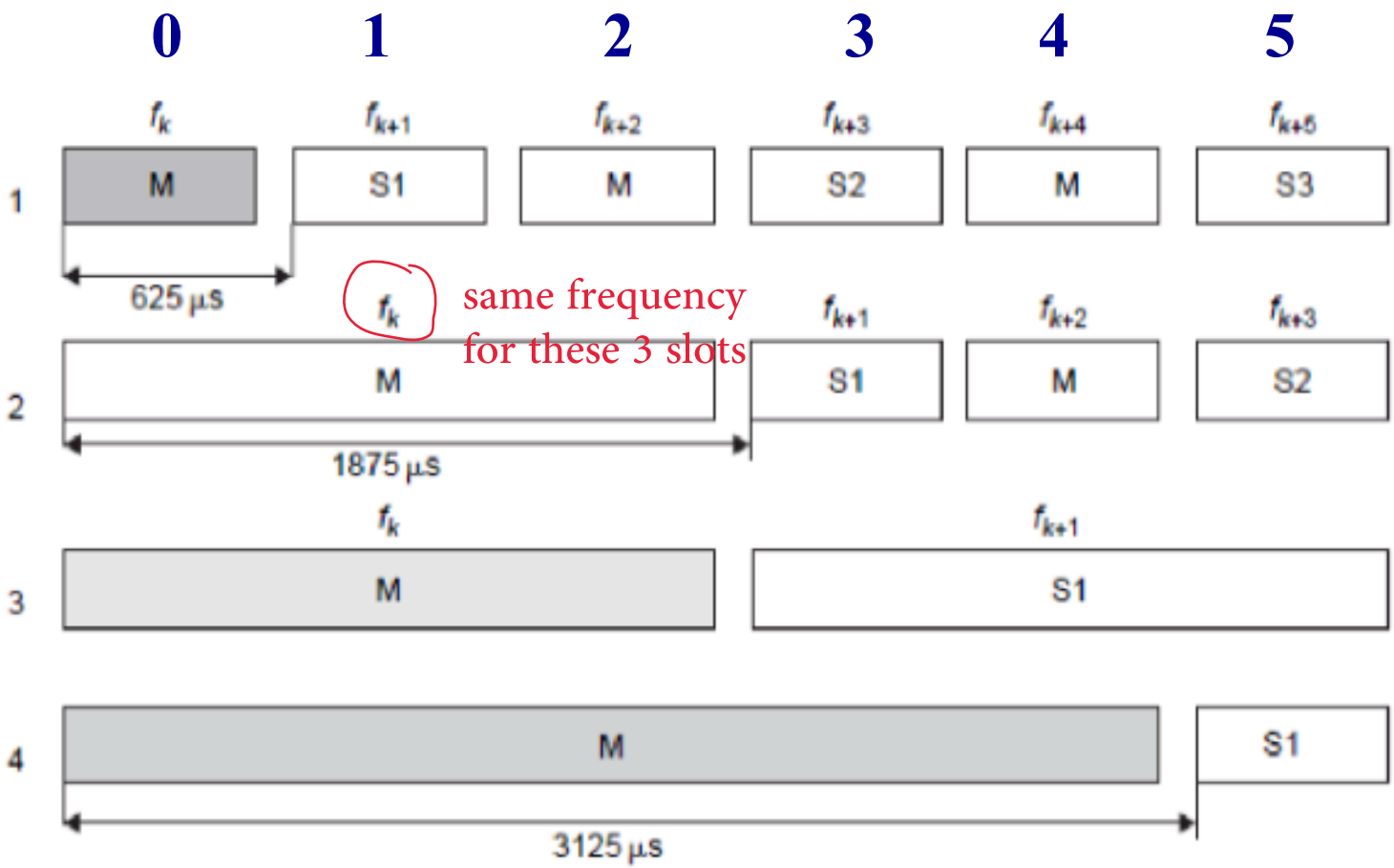
©2020 Mahbub Hassan

Frequency Hopping (2)

- Bluetooth connections are slotted: packet transmission can start only at the beginning of a time slot
- 625 μs slots using a 312.5 μs (3200Hz) clock (1 slot = 2 clock ticks)
- Time-division duplex (TDD)
  ⇒ Downstream (master-to-slave) and upstream (slave-to-master) alternate
- Master starts in even numbered slots only.
- Slaves start in odd numbered slots only
- Slaves can transmit right after receiving a packet from master
- Packets = 1 slot, 3 slot, or 5 slots long
  - Enables master to start in even and slave in odd slots
- The frequency hop is skipped during a packet; frequency is hopped only at slot boundaries; at the beginning of the next slot after packet transmission/reception is complete; packet lengths may not align with slot boundaries

©2020 Mahbub Hassan

Frequency Hopping Illustrated

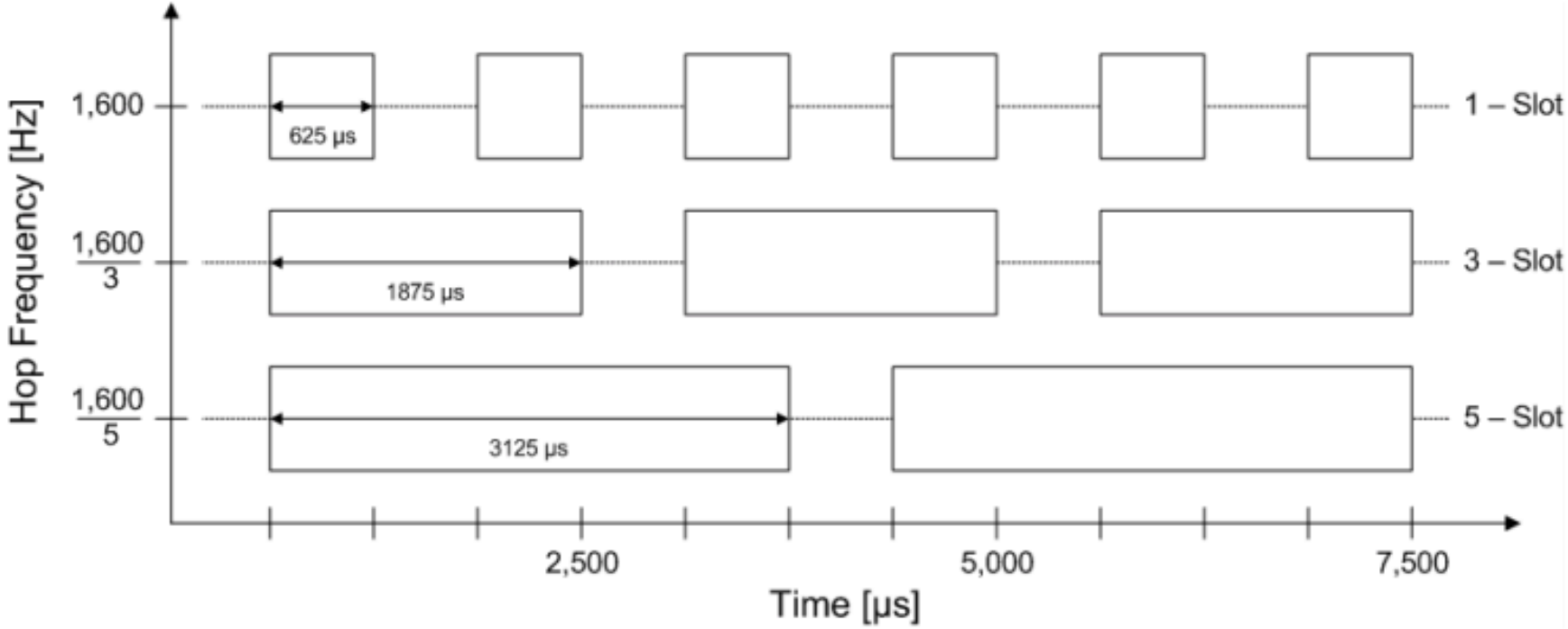


1. One-slot symmetrical; 2. Three-slot asymmetrical; 3. Three-slot symmetrical; 4. Five-slot asymmetrical

M=master, S = slave

©2020 Mahbub Hassan

Frequency Hopping Rate



1 frequency hop per packet: a packet can be 1,3, or 5 slot long (no hop in the middle of the packet); maximum FH rate = 1600Hz, minimum FH rate = 320Hz

©2020 Mahbub Hassan

Example

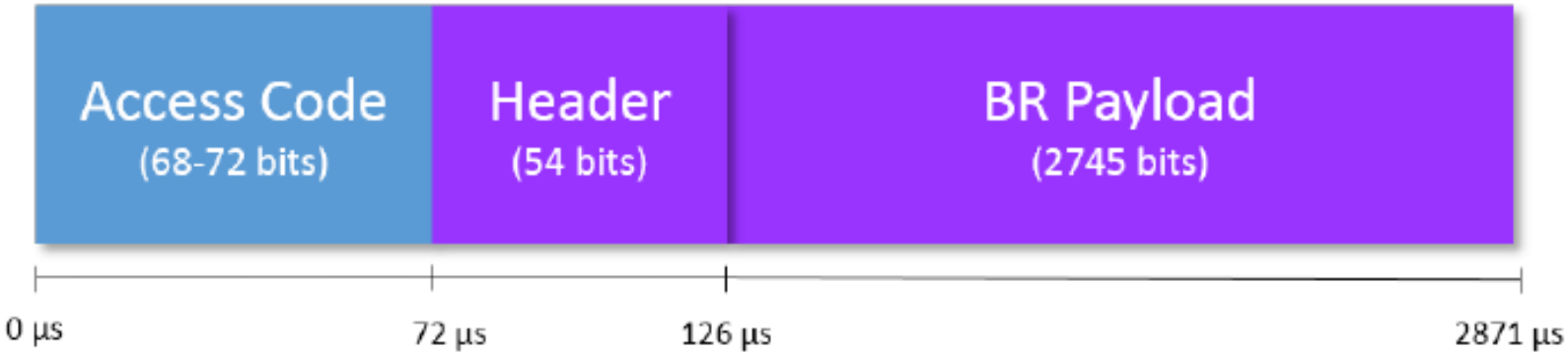
- Consider a Bluetooth link where the *master* always transmits 3-slot packets. The transmission from the master is always followed up by a single-slot transmission from a *slave*. Assuming 625 μs slots, what is the effective frequency hopping rate (# of hopping per second)?

Answer: Given that frequency hopping cannot occur in the middle of a packet transmission, we only have 2 hops per 4 slots, or 1 hop per 2 slots.

The effective hopping rate = $1/(2 \times 625 \times 10^{-6})$ = 800 hops/s = 800Hz

©2020 Mahbub Hassan

Bluetooth Packet Format: Basic Rate (BR)



- Packets can be up to five slots long. 5 slots =625x5=3125 µs.
  - Maximum packet size = 72+54+2745 = 2871 µs (@1Mbps)
  - Some *residual* slot-time cannot be used (2871 < 3125)
- Access codes:
  - Channel access code identifies the piconet
  - Device access code for paging requests and response
  - Inquiry access code to discover units
- Header: member address (3b)+type code (4b)+flow control (1b)+ack/nack (1b)+sequence number (1b)+header error check (8b)=18b, which is encoded using 1/3 rate FEC resulting in 54b =18x3

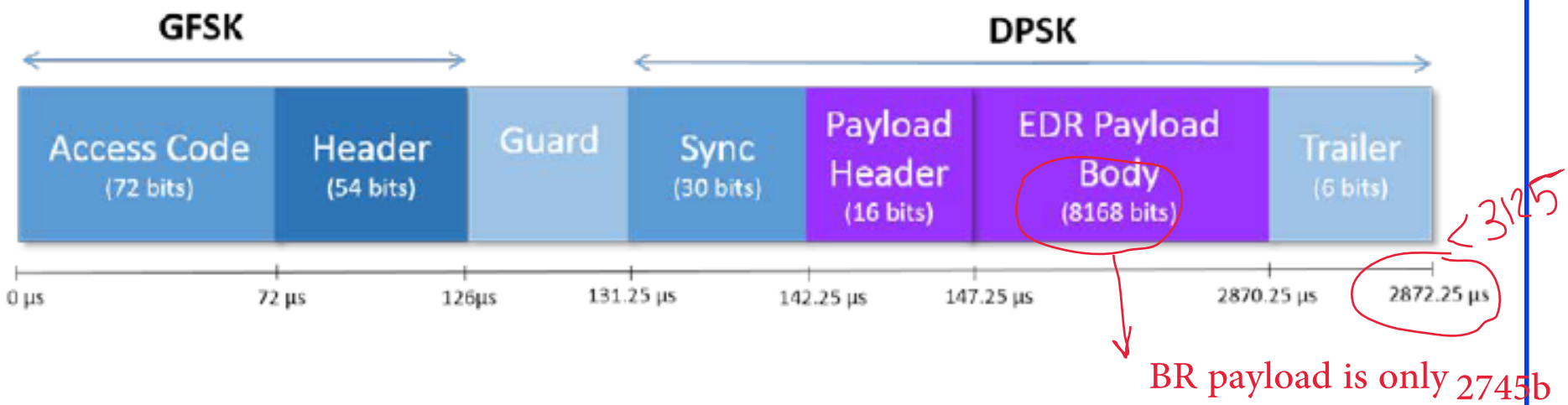
©2020 Mahbub Hassan

Example

- How many slots are needed to transmit a Bluetooth Basic Rate packet if the payload is (a) 400 bits, (b) 512 bits, and (c) 2400 bits. Assume that the non-payload portions do not change.
- Answer:
  - Bluetooth transmissions are 1, 3, or 5 slots (2, 4, 6, etc. not allowed)
  - Non-payload bits (max) = 54+72 = 126 bits
  - Each slot can carry 625 bits at most
  - (a) 400b payload → 400+126 = 526b packet → 1 slot
  - (b) 512b payload → 512+126 = 638b packet → 2 slots would be sufficient, but will have to be padded for a 3-slot transmission (2-slot packets not allowed)
  - (c) 2400b payload → 2400+126 = 2526b packet → 5 slots

©2020 Mahbub Hassan

Bluetooth Packet Format: Enhanced Data Rate (EDR)



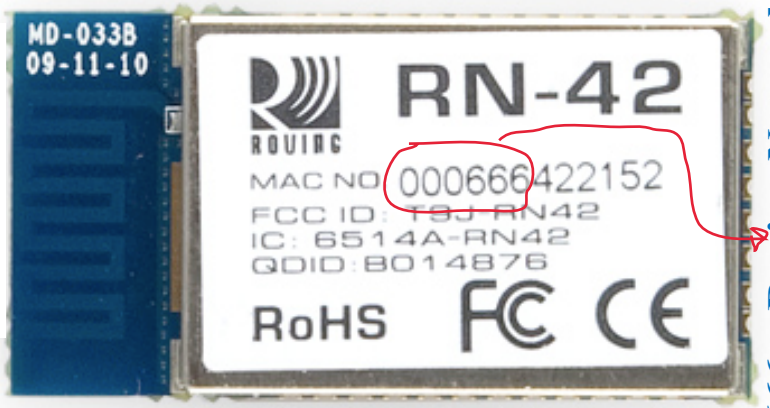
- Modulation changes within the packet; facilitated by a *guard interval lasting between 4.75 µs and 5.25 µs*
- GFSK for Access Code and Header
- µ/4-DQPSK (2Mbps) or 8DPSK (3Mbps) after guard interval
- EDR payload can accommodate more data than BR, but still fits within maximum 5-slot due to higher data rates

©2020 Mahbub Hassan

Bluetooth Address Format

company assigned		company id									
LAP						UAP		NAP			
0000	0001	0000	0000	0000	1100	0010	0111	1011	0011	0101	1001

LSB MSB



000666 = Roving Networks

- The Bluetooth device address is a unique 48-bit address sent in the *access code* field of the packet header.
- The first (most significant) 24 bits represent the OUI (Organization Unique Identifier) or the Company ID
- The main purpose of the Bluetooth address is for identification and authentication, but
- The address is also used to seed the frequency hopping pseudorandom generator, to synchronize master and slave clocks, and to pair devices.

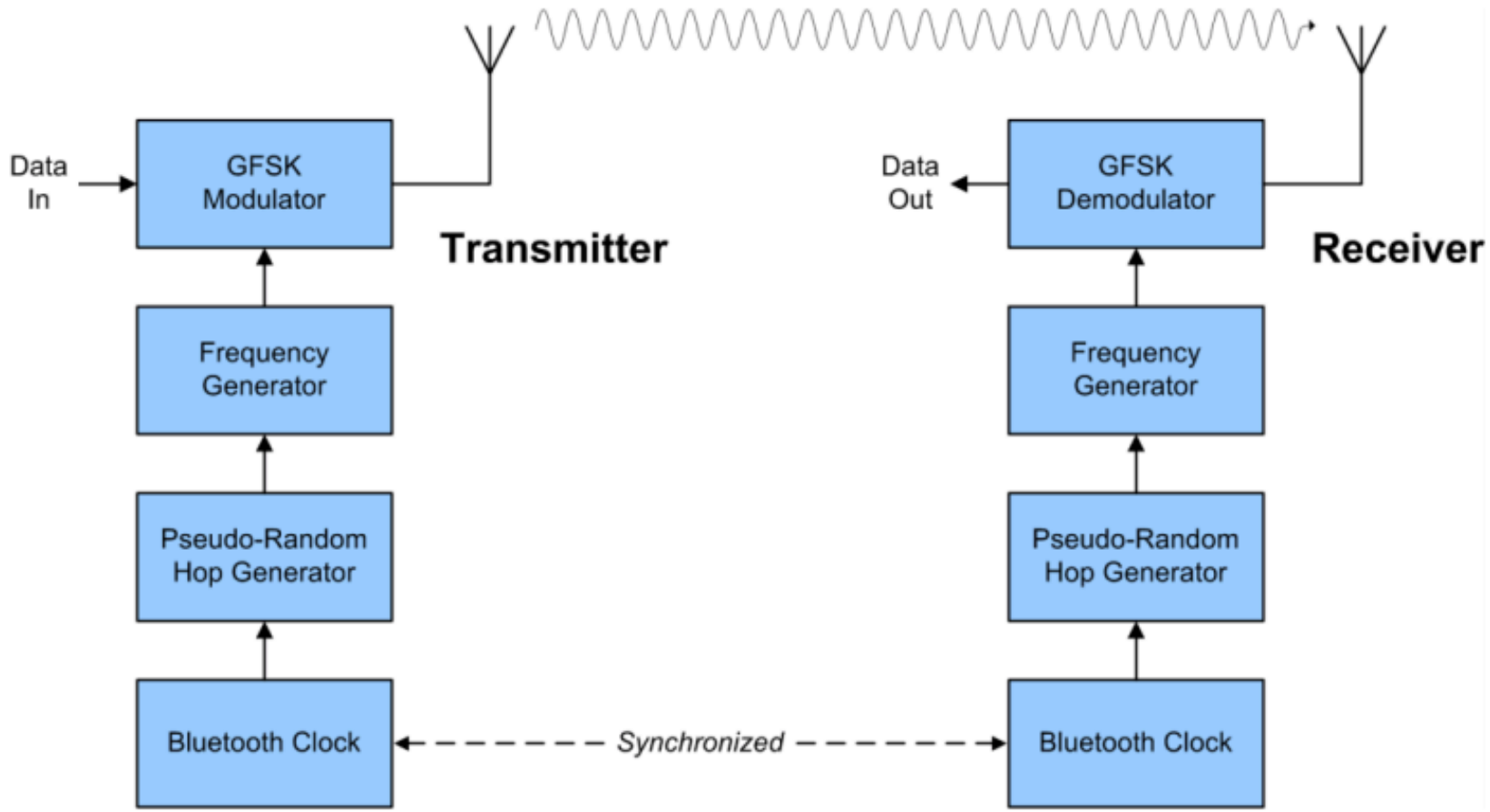
©2020 Mahbub Hassan

Frequency Hopping with Pseudorandom Number Generator

- In Bluetooth Classic, FH is defined by a pseudorandom generating algorithm seeded with the following values
  - UAP and LAP of the master device address, and
  - Bits 1-26 of the 28-bit Bluetooth clock
- The pseudorandom pattern would repeat itself after 2^{27} hops
  - Would take 23.3 hours@1600Hz to repeat!
  - In practice the pseudorandom sequence is never repeated

©2020 Mahbub Hassan

Bluetooth is both Time and Frequency Synchronised



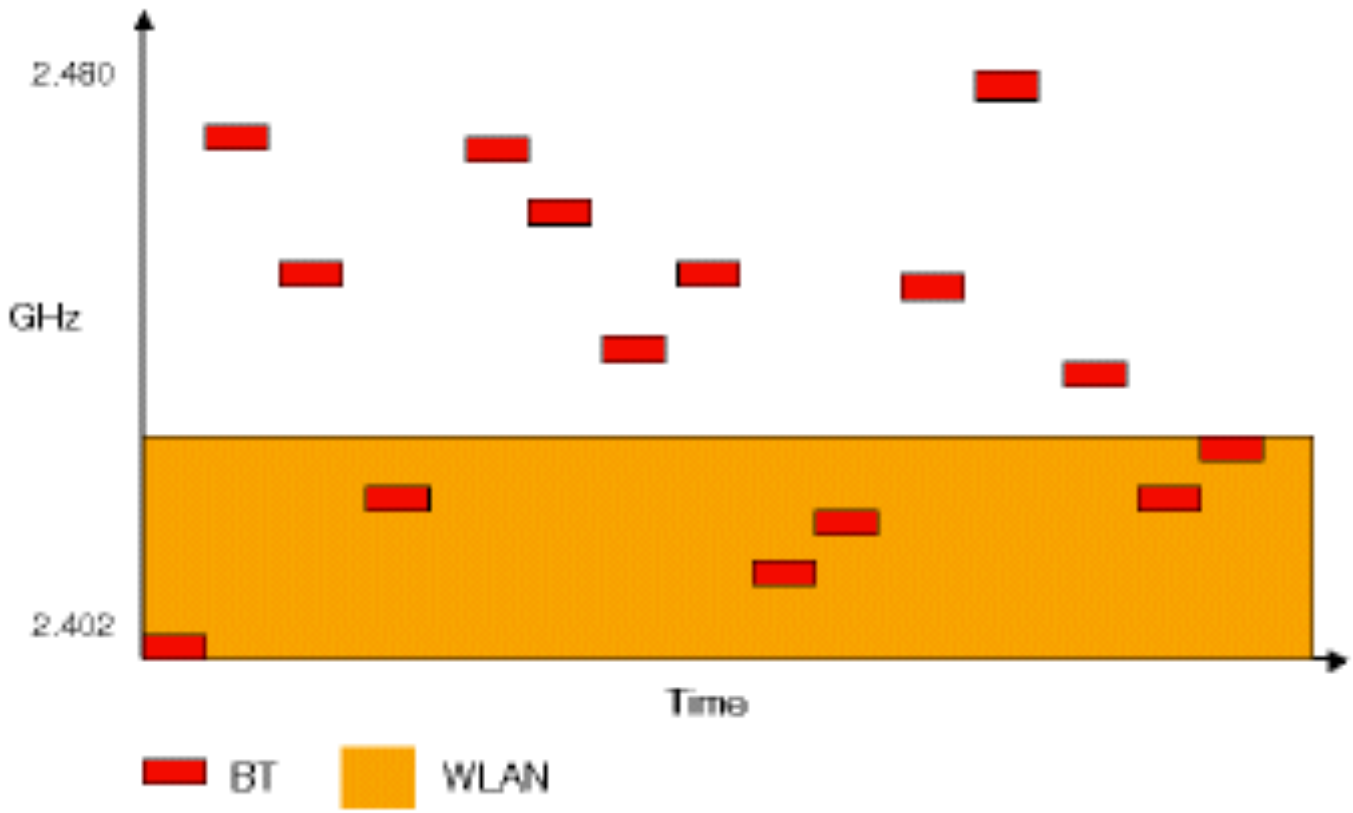
©2020 Mahbub Hassan

Illustration of Pseudorandom FH

Time	Slot/Hop	Hopset															
10.000 ms	17 (TX)		▲TX														
9.375 ms	16 (RX)															▼RX	
8.750 ms	15 (TX)				▲TX												
8.125 ms	14 (RX)						▼RX										
7.500 ms	13 (TX)										▲TX						
6.875 ms	12 (RX)															▼RX	
6.250 ms	11 (TX)										▲TX						
5.625 ms	10 (RX)									▼RX							
5.000 ms	9 (TX)																▲TX
4.375 ms	8 (RX)									▼RX							
3.750 ms	7 (TX)										▲TX						
3.125 ms	6 (RX)							▼RX									
2.500 ms	5 (TX)						▲TX										
1.875 ms	4 (RX)																▼RX
1.250 ms	3 (TX)											▲TX					
0.625 ms	2 (RX)				▼RX												
0.000 ms	1 (TX)			▲TX													
	Bluetooth Channel	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	Frequency	2402 MHz	2403 MHz	2404 MHz	2405 MHz	2406 MHz	2407 MHz	2408 MHz	2409 MHz	2410 MHz	2411 MHz	2412 MHz	2413 MHz	2414 MHz	2415 MHz	2416 MHz	2417 MHz

©2020 Mahbub Hassan

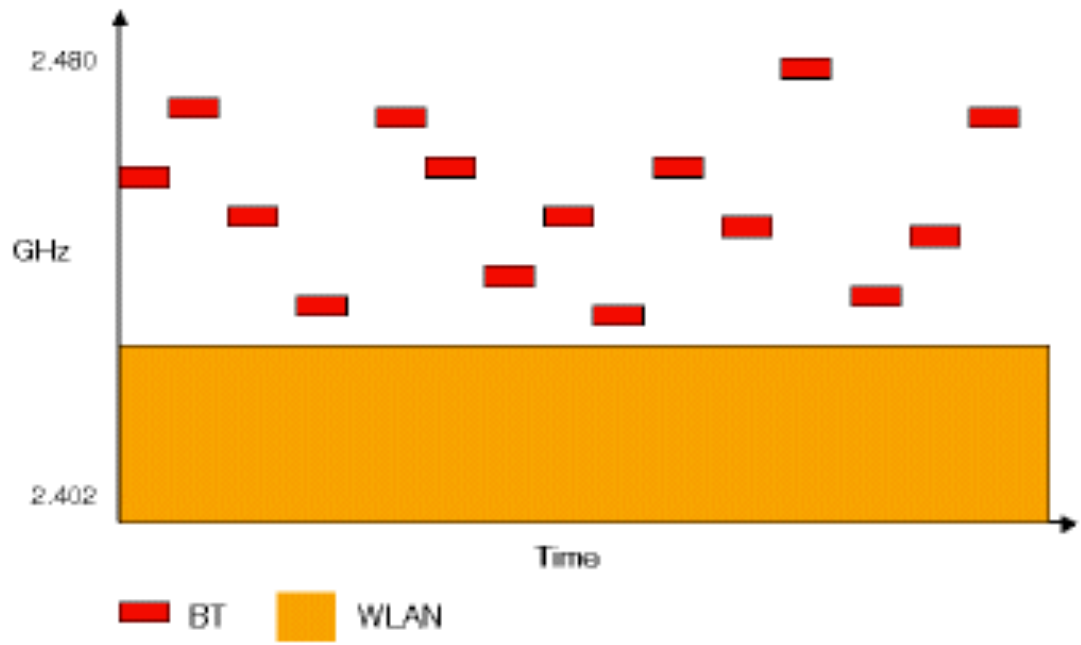
Collision with WiFi: fixed (non-adaptive) hopping



©2020 Mahbub Hassan

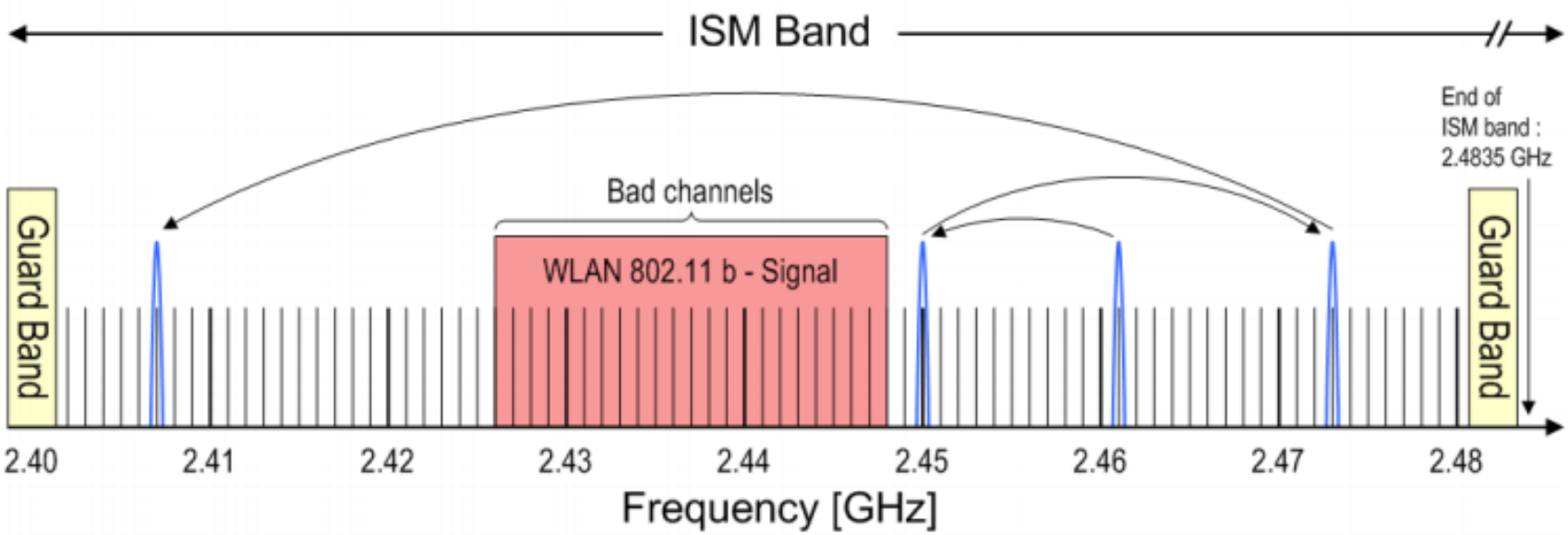
Collision Avoidance via Adaptive FH (AFH)

- Mark interfering channels as *bad channels*
- Avoid bad channels; hop between *good channels* only
- Minimum available (good) channels to hop = 20 (max. 79-20=59 channels can be marked as bad)
- AFH available only during Connected state (i.e., when two devices are exchanging data)



©2020 Mahbub Hassan

AFH Illustration: hopping only between good channels



packet error rate

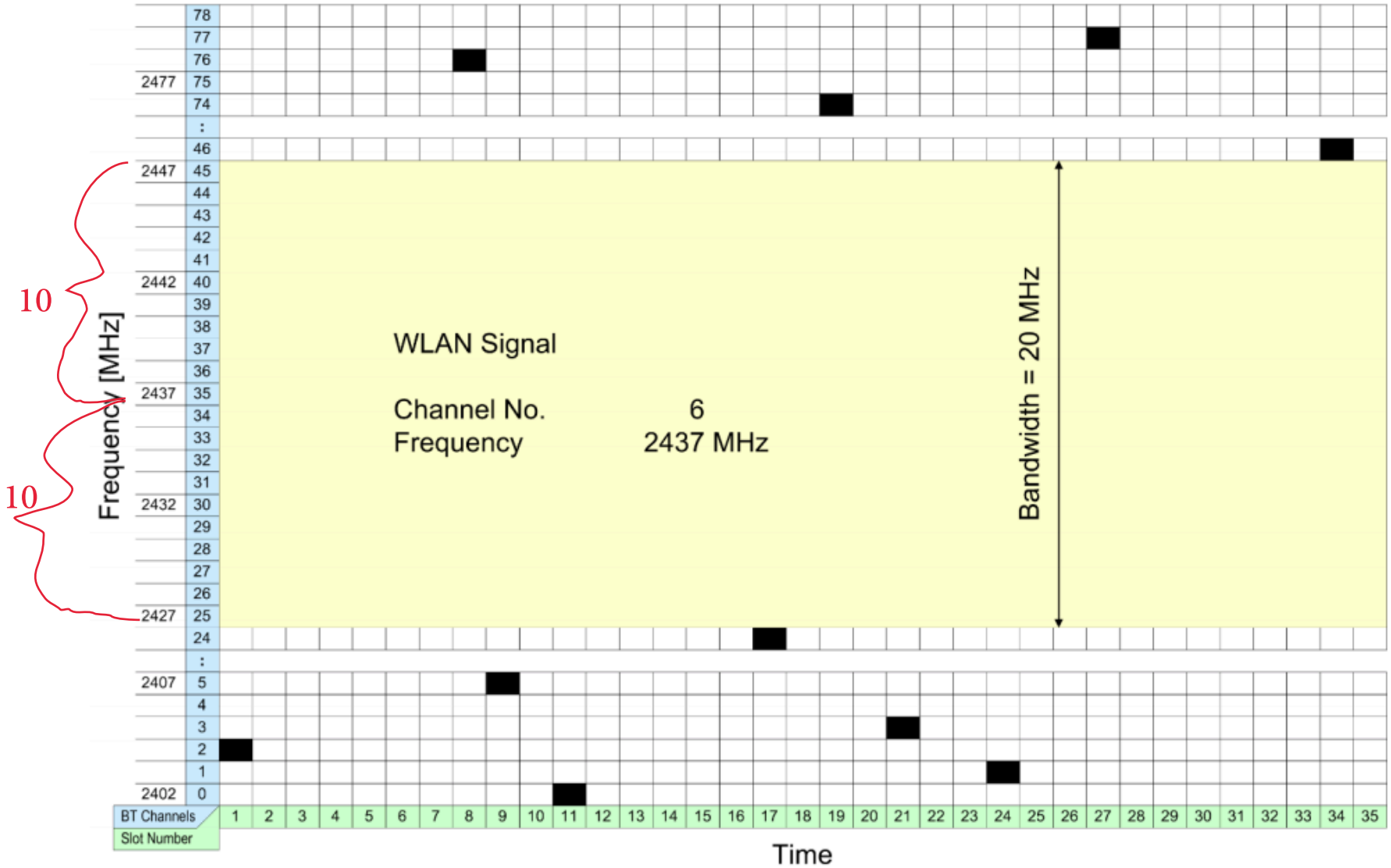
Channel assessment: RSSI/SNR, PER (left to chipset vendor; not specifid in standard)

©2020 Mahbub Hassan

Channel Map

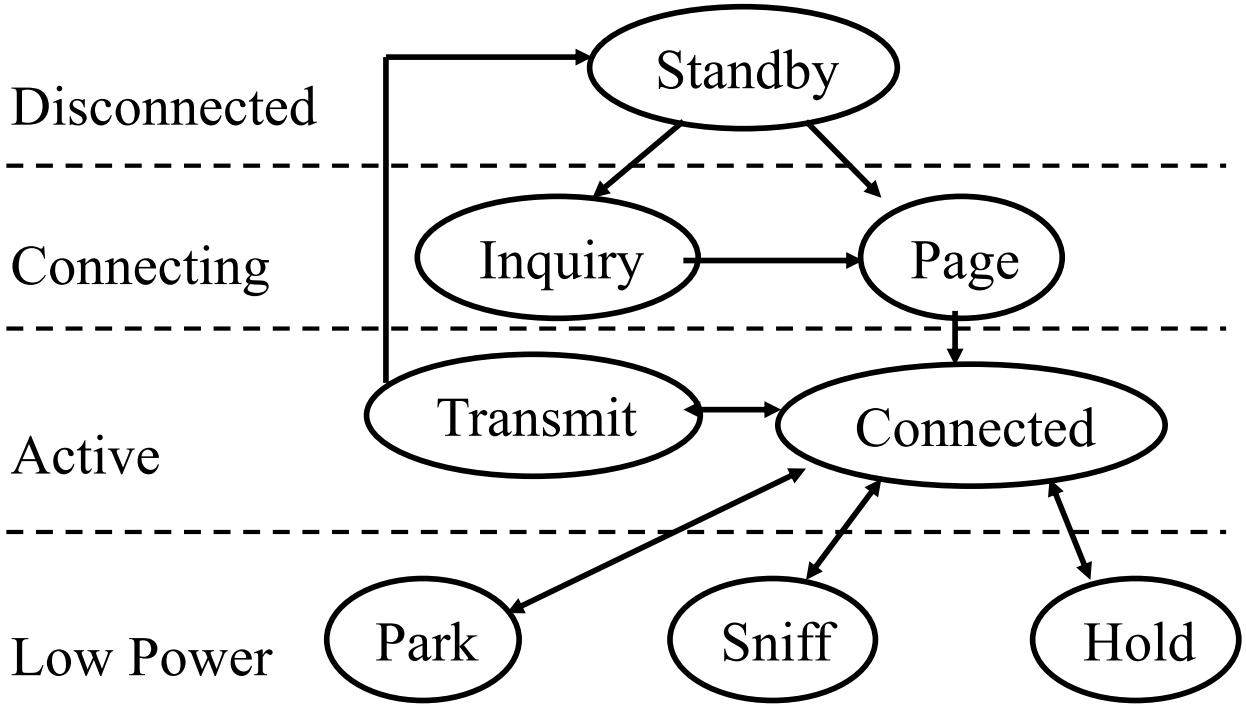
- Black: used (by another piconet)
- White: available (good to use)
- Yellow: Bad

Master updates the map dynamically and sends it to slaves



©2020 Mahbub Hassan

Bluetooth Operational States

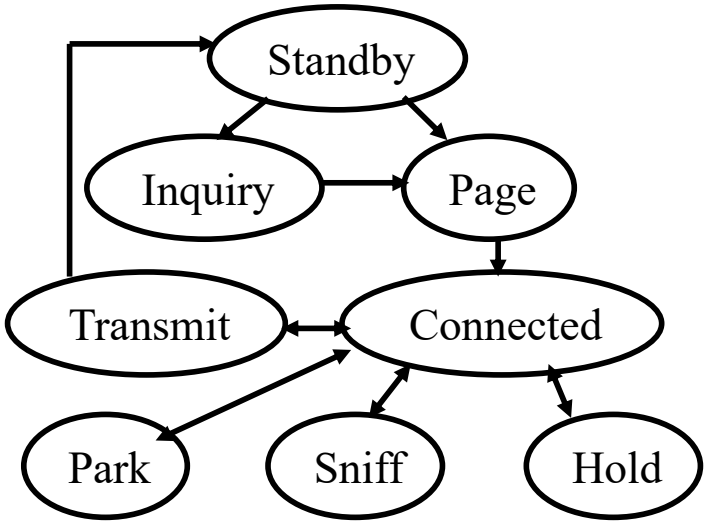


- 8 distinct states grouped under 4 high-level states
- **Standby**: Initial state
- **Inquiry**: Master broadcasts an inquiry packet. Slaves scan for inquiries and respond with their address and clock after a random delay (CSMA/CA)

©2020 Mahbub Hassan

Bluetooth Operational States (Cont)

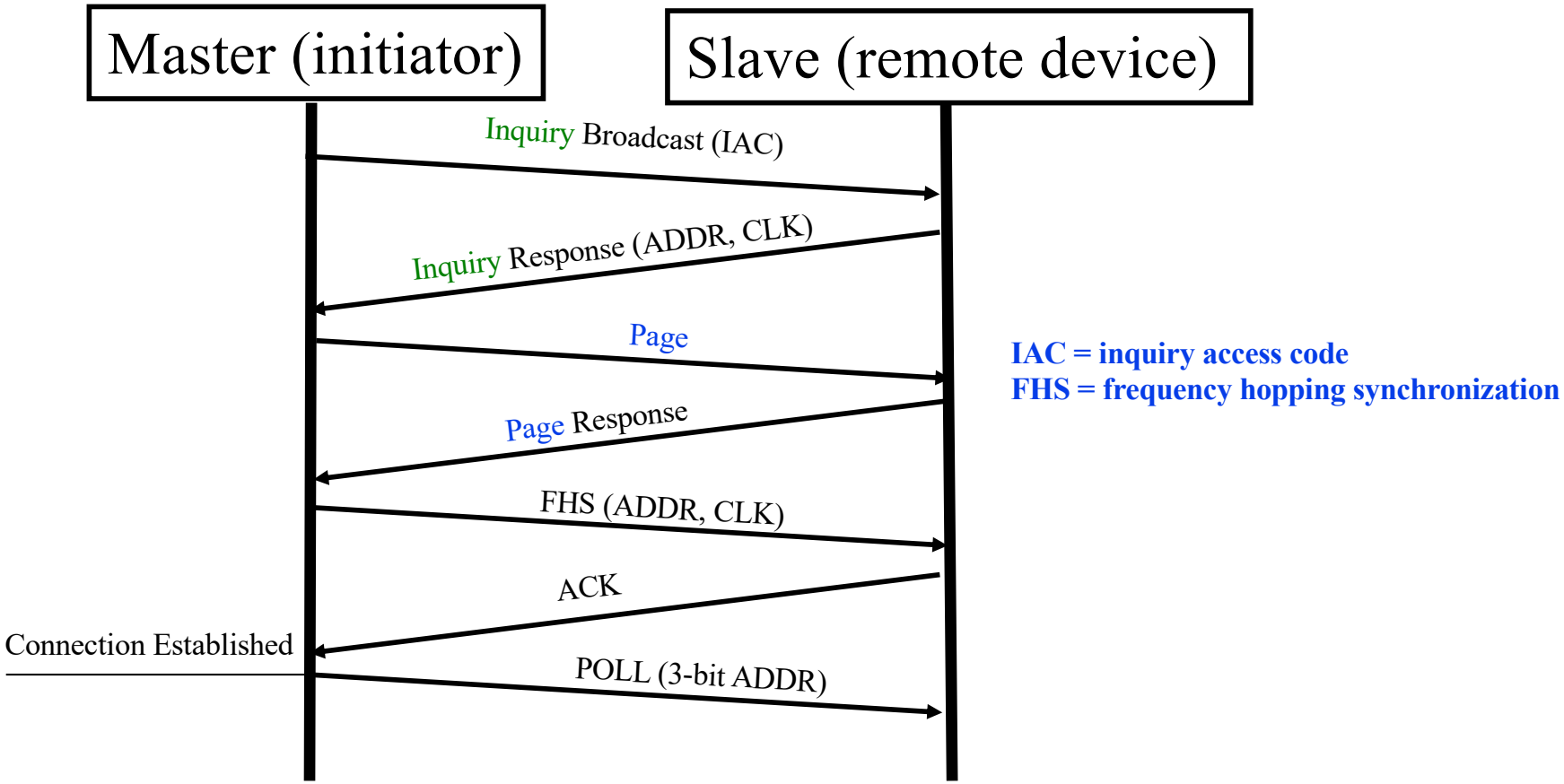
- **Page**: Master in page state invites a slave device to join the piconet. Slave enters page response state and sends page response to the master.
- Master informs slave about its *clock* and *address* so that slave can participate in piconet.
- **Connected**: A short 3-bit logical address (*member address* within *control header* field) is assigned for the slave
- **Transmit**: station is transmitting or receiving a packet



©2020 Mahbub Hassan

Bluetooth Connection Establishment Procedure

Inquiry and Paging Flow Diagram



©2020 Mahbub Hassan

Bluetooth Connection Establishment Procedure
Inquiry and Paging Frequency Hopping

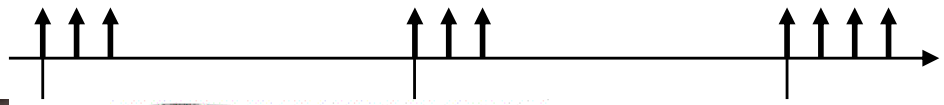
- Inquiry/page hopping sequence
  - Hop over 32 subset of 79 channels/frequencies (to speedup)
  - 32 is divided into two 16-channel *trains*
  - For inquiry, each train is repeated 256 times before *switching* to the other train; must have 3 train switches ($1^{st} \rightarrow 2^{nd} \rightarrow 1^{st} \rightarrow 2^{nd}$): each train effectively repeated 256 x 2 times
  - Master sends two inquiry/page packets using 2 different frequencies per slot (hops in the middle of the slot; hops frequency in 312.5µs!), and listens for responses (both frequencies) in the following slots (to speed up) → eventually 2 frequencies covered in 2 slots
- Connection establish time
  - 16 x 625 µs = 10 ms for completing a train once
  - Inquiry time (maximum) = 256 x 4 x 10 ms = 10.24 s
  - There is an additional paging time

©2020 Mahbub Hassan

Power Saving Modes in Bluetooth

Three inactive (power-saving) states:

1. **Hold**: Go inactive for a single short period and become active after that
2. **Sniff**: Low-power mode. Slave listens periodically after fixed sniff intervals.
3. **Park**: Very Low-power mode. Gives up its 3-bit active member address and gets an 8-bit parked member address. Wake up periodically and listen to beacons. Master broadcasts a train of beacons periodically

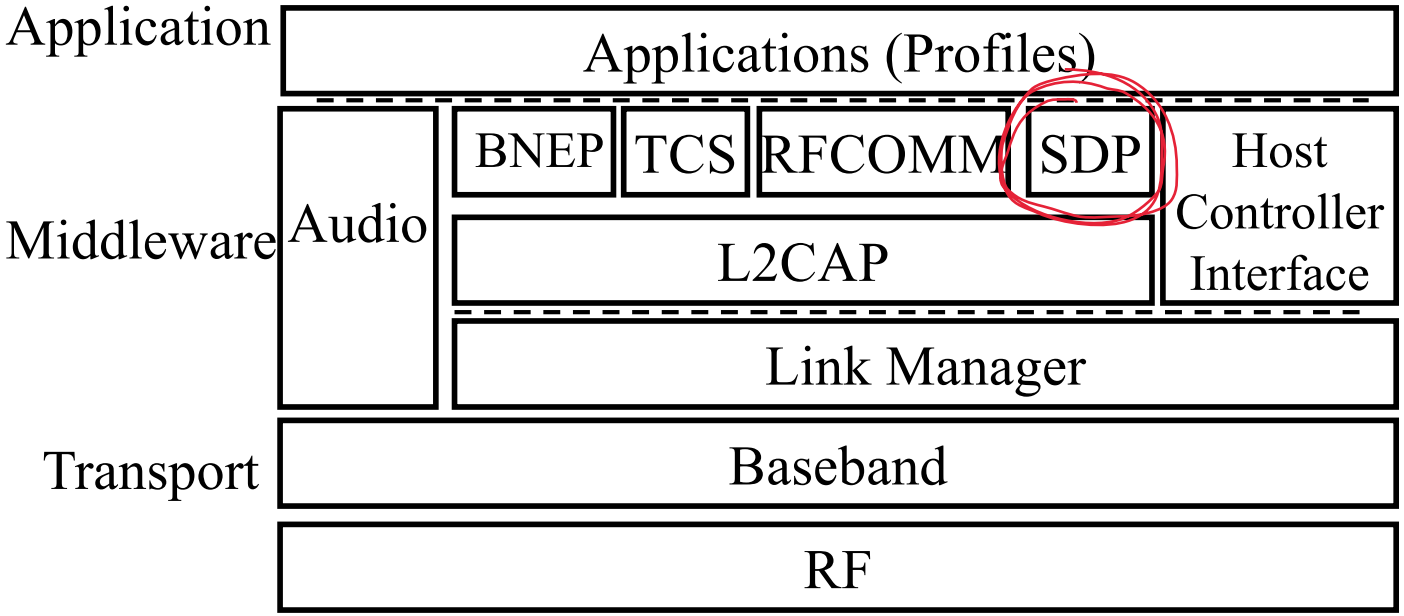


Sniff

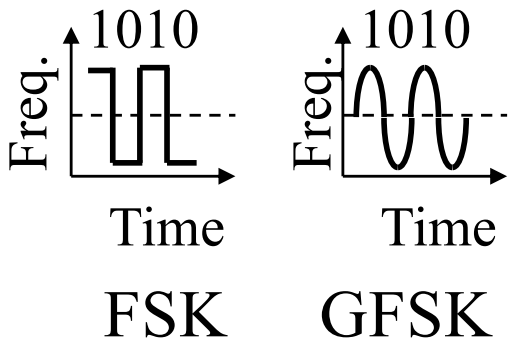
Park

©2020 Mahbub Hassan

Bluetooth Protocol Stack



- **RF**: Gaussian Frequency Shift Keying (GFSK) modulation
- **Baseband**: Frequency hop selection, connection, MAC



©2020 Mahbub Hassan

Baseband Layer

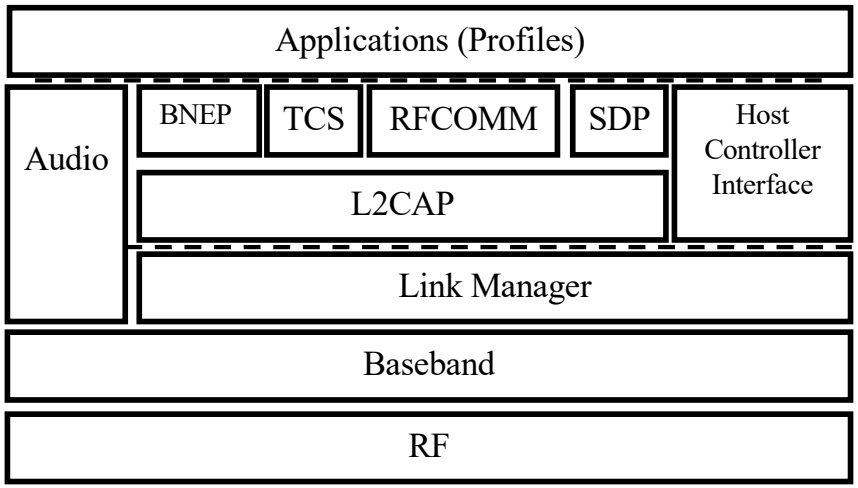
- Each device has a 48-bit IEEE MAC address
- 3 parts:
  - Lower address part (LAP) – 24 bits
  - Upper address part (UAP) – 8 bits
  - Non-significant address part (NAP) - 16 bits
- UAP+NAP = Organizationally Unique Identifier (OUI) from IEEE
- LAP is used in identifying the piconet and other operations
- Clock runs at 3200 cycles/sec or 312.5 μs (twice the hop rate)

Upper Address Part	Non-sig. Address Part	Lower Address Part
8b	16b	24b

©2020 Mahbub Hassan

Bluetooth Protocol Stack (Cont)

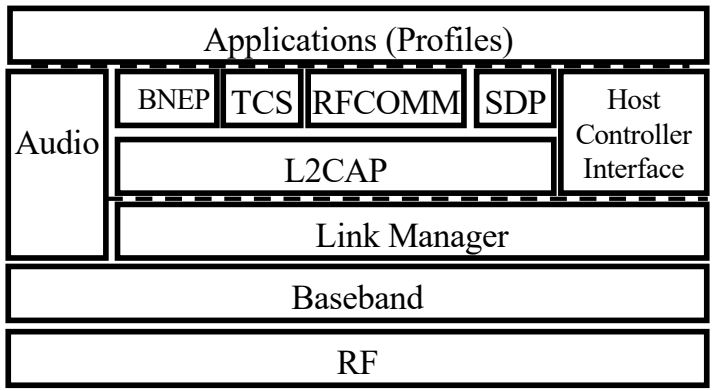
- **Link Manager:** Negotiate parameters, Set up connections
- **Logical Link Control and Adaptation Protocol (L2CAP)**:
  - Protocol multiplexing
  - Segmentation and reassembly
  - Controls peak bandwidth, latency, and delay variation
- Host **Controller Interface**: Chip independent interface to Bluetooth chip. Allows same software to run on all chips.
- **RFCOMM Layer**: Presents a virtual serial port
  - Sets up a connection to another RFCOMM
- **Service Discovery Protocol (SDP):** Devices can discover the services offered and their parameters
  - E.g., Bluetooth keyboard,
  - Bluetooth mouse
  - Bluetooth headset
  - …



©2020 Mahbub Hassan

Bluetooth Protocol Stack (Cont)

- **Bluetooth Network Encapsulation Protocol (BNEP):** To transport Ethernet/IP packets over Bluetooth
- **IrDA Interoperability protocols**: Allow existing IrDA applications to work w/o changes. IrDA object Exchange (IrOBEX) and Infrared Mobile Communication (IrMC) for synchronization
- **Audio** is carried over 64 kbps over SCO links over baseband
- **Telephony control specification binary (TCS-BIN)**: Call control including group management (multiple extensions, call forwarding, and group calls)
  - Telephony has both audio and control
  - Bluetooth telephone very popular in cars
- **Application Profiles**: Set of algorithms, options, and parameters
  - To support specific applications



©2020 Mahbub Hassan

Application Profile Examples

- Headset Profile
- Global Navigation Satellite System Profile
- Hands-Free Profile
- Phone Book Access Profile
- SIM Access Profile
- Synchronization Profile
- Video Distribution Profile
- Blood Pressure Profile
- Cycling Power Profile
- Find Me Profile
- Heart Rate Profile
- Basic Printing Profile
- Dial-Up Networking Profile
- File Transfer Profile

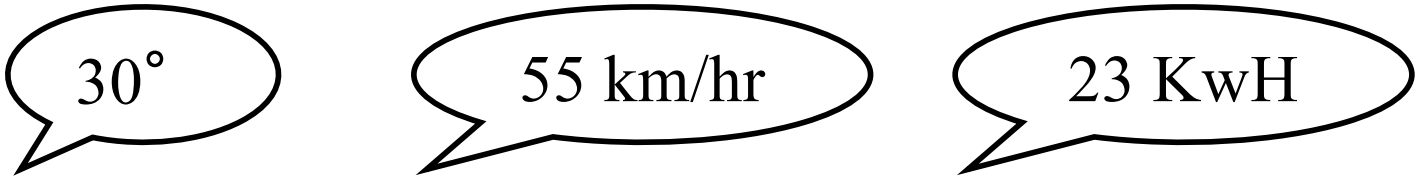
With IoT, the list is expected to grow rapidly over the coming years

Ref: Bluetooth SIGn, "Adopted Bluetooth Profiles, Services, Protocols and Transports," https://www.bluetooth.org/en-us/specification/adopted-specifications

©2020 Mahbub Hassan

IoT Communications Requirements

- IoT depends on large number of sensors that repetitively announce their *states* when enquired or polled



- Sensors need to transmit such small messages to a nearby gateway with minimal energy consumption
- Requires simpler protocols (more power saving and avoid complicated connecting procedures) than Bluetooth Classic → Bluetooth Smart or BLE

©2020 Mahbub Hassan

Bluetooth Low Energy (BLE)
a.k.a Bluetooth 4

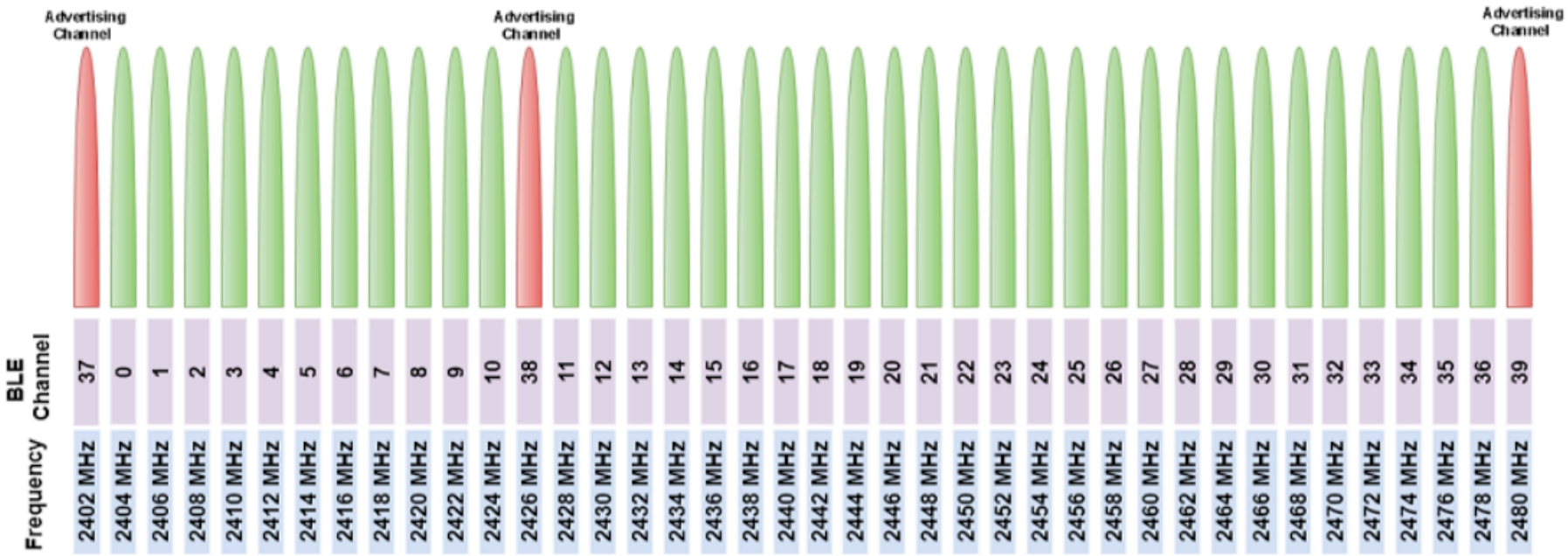
©2020 Mahbub Hassan

Bluetooth LE or BLE

- **Low Energy**: 1% to 50% of Bluetooth classic
- **For short broadcast**: Your body temperature, Heart rate, Wearables, **sensors**, automotive, industrial.
  Not for voice/video, file transfers, …
- **Small messages**: 1Mbps data rate but throughput not critical.
- **Battery life**: In years from coin cells
- **Simple**: Star topology. No scatter nets, mesh, …
- **Lower cost** than Bluetooth classic
- New protocol design based on Nokia's **WiBree** technology
  Shares the same 2.4GHz radio as Bluetooth
  ⇒ Dual mode chips
- Most smartphones (iPhone, Android, …) have dual-mode chips

©2020 Mahbub Hassan

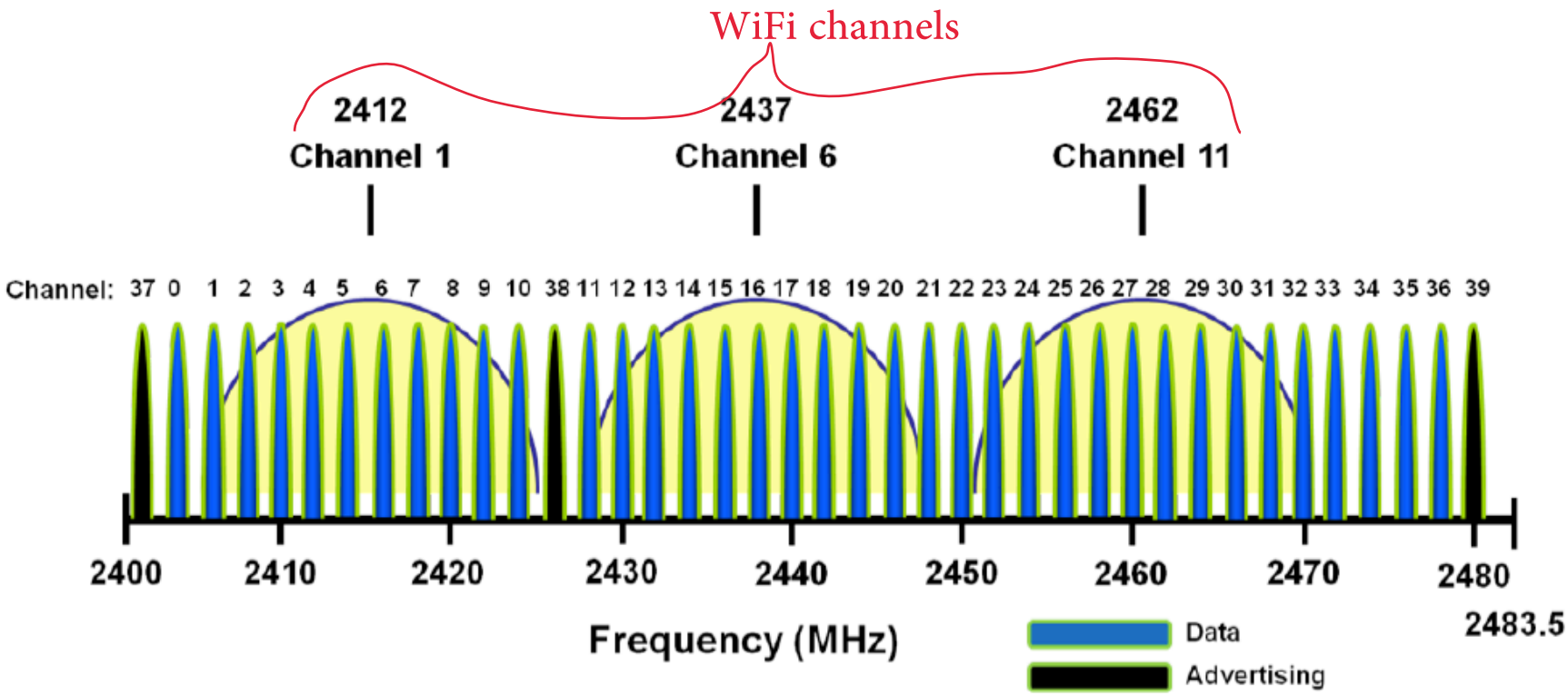
BLE Channels



- 40 2MHz-wide channels: 3 (37,38,39) for advertising and 37 (0-36) for data
- Advertising channels specially selected to avoid interference with popular default WiFi channels (1,6,11)

©2020 Mahbub Hassan

BLE Advertising Channels Avoiding Popular WiFi Channels



©2020 Mahbub Hassan

BLE Modulation and Data rate

- Binary GFSK over 2MHz channel: More significant frequency separations for ‘0’ and ‘1’ allows longer range with low power
  - Note that with Bluetooth Classic, channel bandwidth is only 1MHz, so frequency separations are smaller
- 1 million symbols per second → 1 Mbps data rate

©2020 Mahbub Hassan

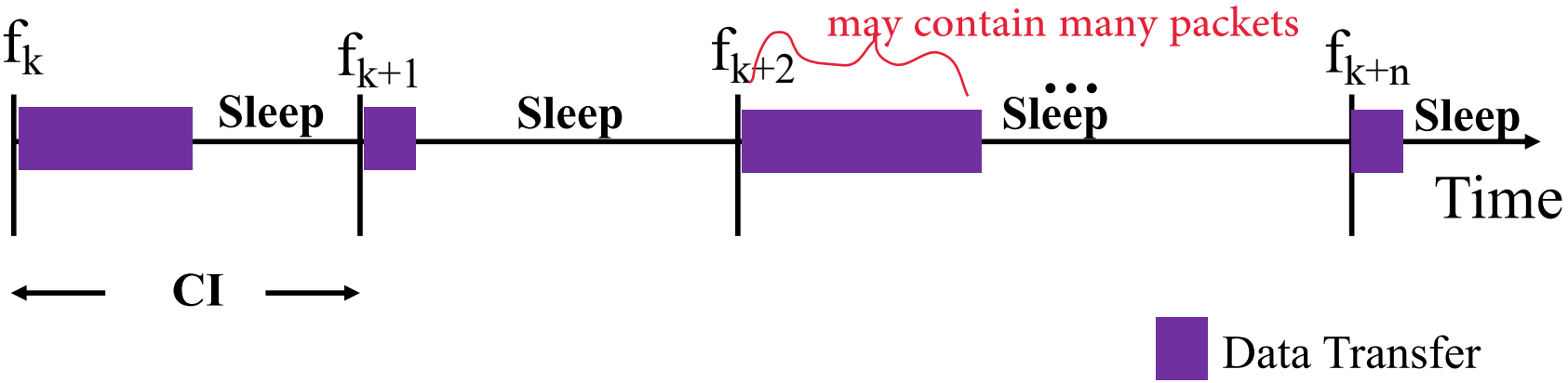
Benefit of Advertising Channels

- BLE simplifies discovery and broadcasting by using only three advertising channels (instead of 32 channels for inquiry/paging in BT Classic)
- A BLE device can broadcast advertising beacons on these 3 channels giving information about the device, so other devices can connect, but can also broadcast some sensor data
- Data channels are used to exchange data bidirectionally between two devices

©2020 Mahbub Hassan

Connection Events and Connection Intervals

- In BLE connections, devices wake up periodically after every connection interval (CI) time; transmit some data (connection event) and then go back to sleep until the next connection event
- Send a short blank packet if no data to send during a connection event
- More than one packet can be sent during a connection event
- Connection interval time can vary from 7.5ms to 4s and is negotiated during connection set up
- Hop frequency (switch to different data channel) at each event



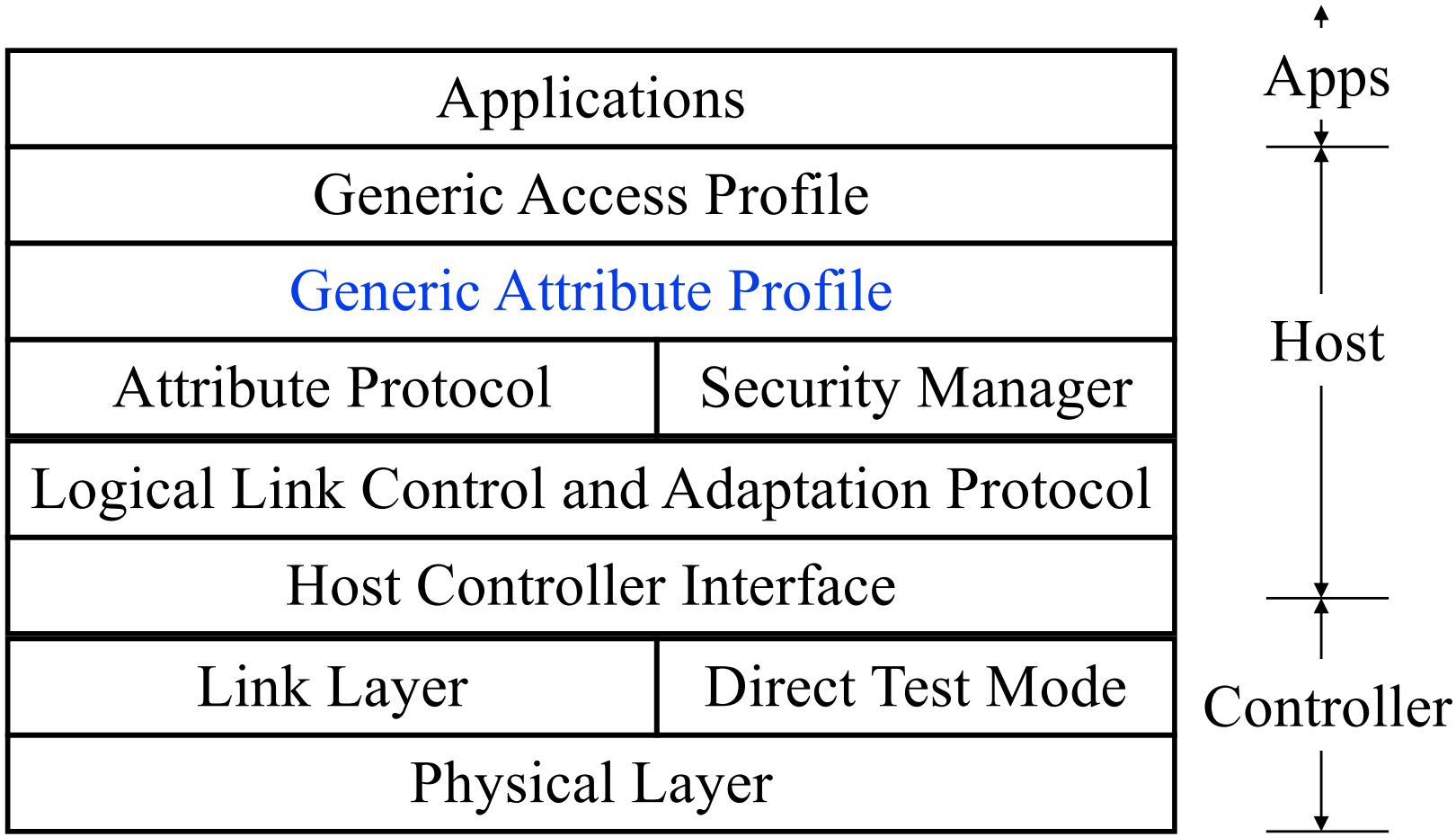
©2020 Mahbub Hassan

BLE Frequency Hopping Algorithm
a.k.a Algorithm #1

- *Fixed* hopping instead of *pseudorandom*
- $f_{k+1} = (f_k + h) \bmod 37$
  - Where h (hop increment) is a fixed value negotiated during connection setup
  - Note: Data channels range from 0-36
- Example hopping sequence for h=10: 0→10→20→30→~~4~~ 3→~~14~~ 13
- Adaptive FH: If the hopping lands on a *bad* channel, the channel is remapped to a *good* channel using a channel *remapping* algorithm

©2020 Mahbub Hassan

Bluetooth Smart Protocol Stack



©2020 Mahbub Hassan

Generic Attribute (GATT) Profile

- Defines data formats and interfaces with the Attribute Protocol
  - Define attributes instead of applications (a major difference from Bluetooth Classic); temperature, pressure, heart rates are examples of attributes
  - New applications can be supported by using appropriate attributes
- Type-Length-Value (TLV) encoding is used
- Each attribute has a 16-bit Universally Unique ID (UUID) standardized by Bluetooth SIG
  - 2^{16}=65 thousand unique attributes can be defined!
- 128-bit UUID if assigned by a manufacturer
  - Manufacturers can define their own attributes and still interoperate
- Allows any client to find a server, read/write data
  Allows servers to talk to generic gateways
- Allows security up to AES-128
- Each to encode in XML
- Makes profile (application) development easier

©2020 Mahbub Hassan

Bluetooth Gateway Devices

- A gateway device helps connect a Bluetooth device to the Internet. Smart phone, Tablets, PC, …
- A generic app can forward the data to the URL sent by the device

©2020 Mahbub Hassan

Bluetooth Smart Applications

- Proximity: In car, In room 303, In the mall
- Locator: Keys, watches, Animals
- Health devices: Heart rate monitor, physical activities monitors, thermometer
- Sensors: Temperature, Battery Status, tire pressure
- Remote control: Open/close locks, turn on lights

©2020 Mahbub Hassan

Beacons

- Advertizing based on proximity
- Peripherals (your phone) broadcasts its presence if Bluetooth is turned on
- Primary aim of these broadcasts is to allow device discovery
- Advertising packets consist of a header and max 27B of payload with multiple TLV-encoded data items
  - May include signal strength → Distance
- iPhones can send/received iBeacons
- Can be used for customized advertising, indoor location, geofencing
- PayPal uses this to identify you.
  You can pay using a PIN and your phone.

©2020 Mahbub Hassan

Bluetooth 5

“Go Faster. Go Further”

©2020 Mahbub Hassan

Bluetooth 5: Motivation

- BLE (Bluetooth 4) was great in terms of reducing energy consumption and extending battery life
- BLE, however, could not support high data rate applications, such as audio and file transfer (e.g., quick firmware updates), and the range was still limited for some new IoT applications
- Bluetooth 5 extends BLE to realise a faster (2x) and longer range (4x) Bluetooth without compromising the battery life; advertising is also improved
- Bluetooth 5 is seen as a significant new milestone in the evolution of Bluetooth; expected to support many new markets in home and industrial automation, health and fitness tracking, and so on.

©2020 Mahbub Hassan

Bluetooth 5: Major Improvements

- Two new PHYs: one for 2x higher speed and the other for 4x longer range than BLE 4
- New Advertising
- Improved frequency hopping

©2020 Mahbub Hassan

Benefits and use cases for 2x speed

- Quick firmware updates for millions of home and industrial automation devices
- Sports and fitness wearable multi-dimensional and buffered data uploads to edge/cloud
- Medical device data uploads, e.g., ECG, EEG, …
- Higher spectral efficiency for the congested 2.4GHz space

©2020 Mahbub Hassan

PHY: 2M

- Two mega symbols per sec: symbol duration = 500ns
  - Symbol duration reduced by half from BLE 4
- Binary GFSK, but with higher frequency deviation to combat inter-symbol interference arising from shorter symbols:
  - Frequency deviation (from central frequency) to denote ‘1’ or ‘0’ in FSK > 370kHz (180kHz in BLE 4)

©2020 Mahbub Hassan

PHY: Coded

- 1 Mega symbols per sec: the same as in BLE 4
- However, to increase the range, data is coded with FEC; two coding rates
  - ½: cuts data rate by half → 500Kbps; 2x range increase against BLE 4
  - ¼: → 250Kbps; 4x range increase
- BLE 4 and BT Classic do not employ any FEC (*not coded*)

©2020 Mahbub Hassan

Advertising Extensions

- Motivation: Bluetooth beacons is a major advertising use case
- BLE 4 typically allow just ID or URL to be advertised in the beacon due to limited advertising packet size (31 bytes payload) and heavy load on advertising channels
  - BLE 4 uses channels 37,38,39 for advertising; all beacon have to be transmitted on all three channels
- Bluetooth 5 allows advertising packets up to 255B payload
  - Devices and products can advertise many more things and status, such as a fridge can advertise its contents, temperature, expiry dates of sensitive items, etc.

©2020 Mahbub Hassan

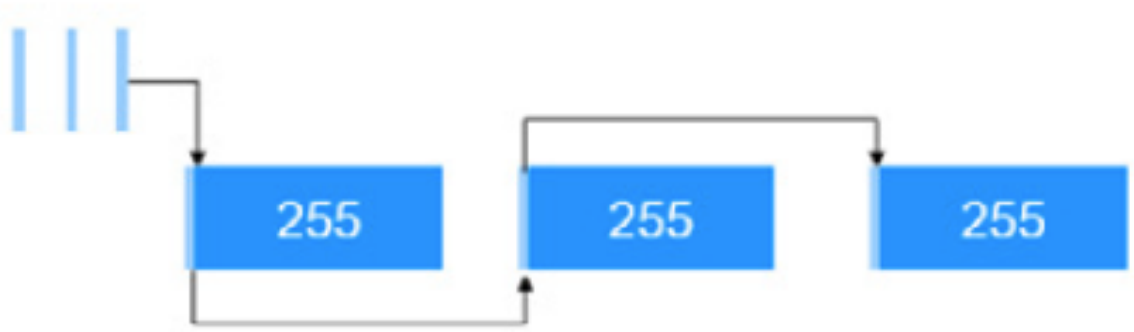
Advertising Extension: Channel Offload

- Only header is transmitted over advertising channels and the actual payload is offloaded to a data channel
- Note: BLE 4 reserves data channels only for data transfers during Connection Events when connections are established; Channel offload allows use of data channels in connectionless manner

©2020 Mahbub Hassan

Advertising Extension: Packet Chaining

- Chain multiple 255B packets together to carry a very large advertising message



©2020 Mahbub Hassan

Frequency Hopping Extension

- BLE 4 supports only a simple hopping algorithm
  - Algorithm #1: fixed hopping increment only
- Fixed hopping increment limits the number of possible sequences to choose from
- Bluetooth 5 supports pseudorandom hopping like the BT Classic
  - Algorithm #2: large number of sequences possible

©2020 Mahbub Hassan

Summary

1. Bluetooth basic rate uses frequency hoping over 79 1-MHz channels with 1, 3, 5 slot packets.
2. Bluetooth Smart (BLE) is designed for short broadcasts by sensors. 40 2-MHz channels with 3 channels reserved for advertising.
3. Bluetooth 5 extends BLE to support higher data rate and longer-range use cases

©2020 Mahbub Hassan

Cellular Networks

©2020 Mahbub Hassan

Overview

1. Cell Structure/Geometry
2. Cellular Frequency Reuse
3. Cellular Handoff
4. Cellular System Capacity
5. Overview of Cellular Generations: 1G→2G→3G→LTE/4G→5G

©2020 Mahbub Hassan

Wide Area Networking

- Bluetooth is good to exchange short messages between two devices located close to each other (~10m)
- WiFi is good mainly within a home/building (~20-50m)
- How about wide area networking (many kilometers)?
- Cellular networking addresses wide area; much more complex and expensive

Bluetooth

WiFi

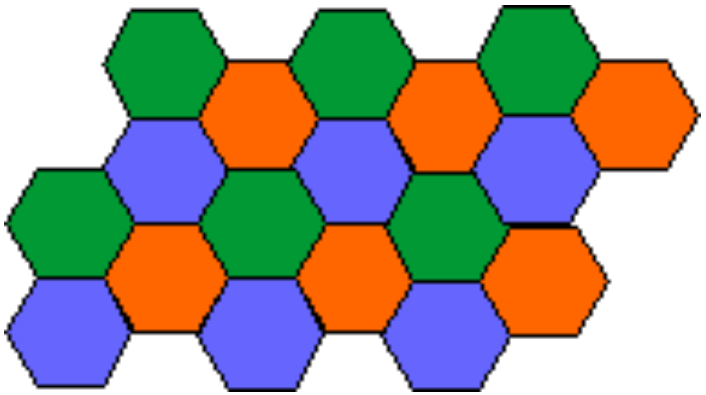
Cellular

©2020 Mahbub Hassan

Cellular Concept

- First proposed in ‘70s; commercial services offered early ‘80s
- A large geographic service area is divided into many smaller cells; no matter where you are located, you are always within a cell
- Each cell has a base station to connect users within the cell; all base stations are in turn connected to a central control system
- Adjacent cells must not use the same frequency to avoid interference
- The same frequency can be reused by a `distant’ base station increase reuse the spectral resources and increase system capacity

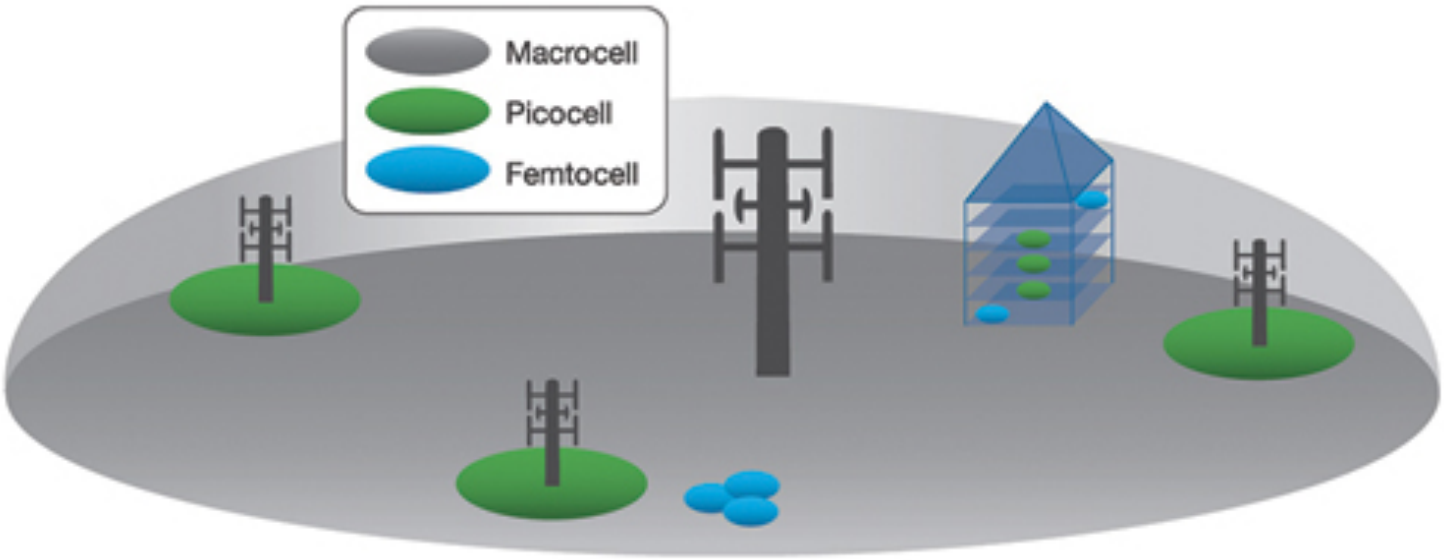
3 frequencies, red, green, and blue, reused by distant cells



©2020 Mahbub Hassan

How large are the cells?
Macro, Micro, Pico, Femto Cells

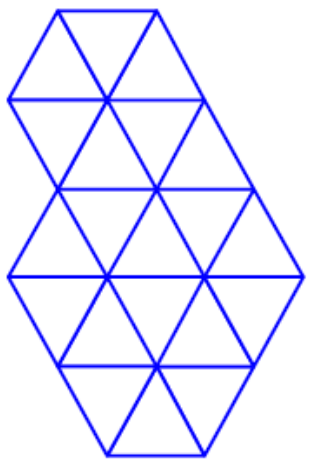
- Macro: Sections of a city, more than 1 km radius
- Micro: Neighborhoods, less than 1 km
- Pico: Busy public areas: Malls, airports, …, 200 m
- Femto: Inside a home, 10 m

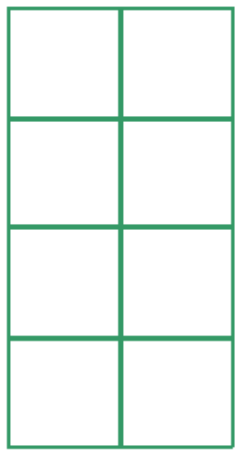


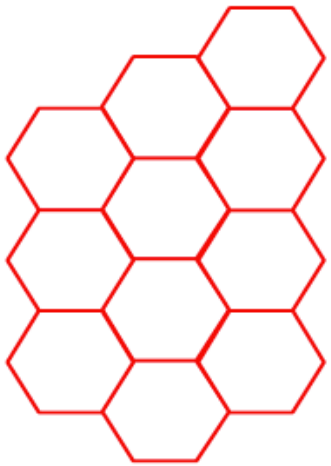
©2020 Mahbub Hassan

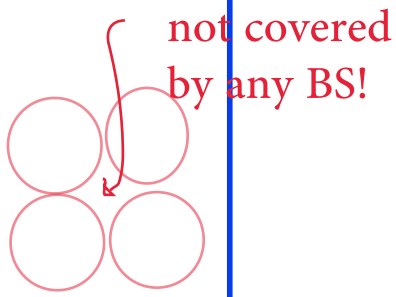
Cell Geometry

- Although there is no regular cell geometry in practice due to natural obstacles to radio propagations, a model is required for planning and evaluation purposes
- Simple model: All cells have identical geometry and should *tessellate* perfectly to avoid any coverage gaps in the service area
  - Radio propagation models lead to circular cells, but circles do not tessellate!
- Three options for tessellation: equilateral triangle, square, regular hexagon
- Hexagon has the largest area among the three; hence its typical use









©2020 Mahbub Hassan

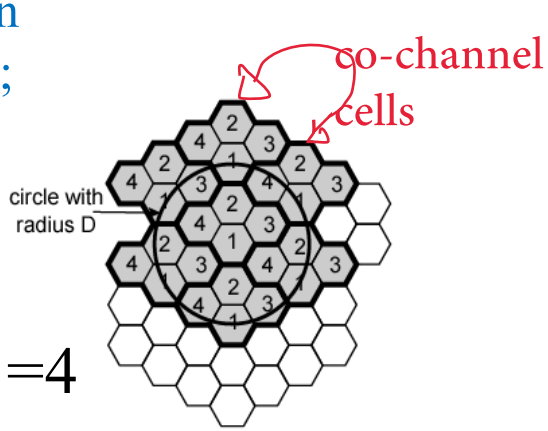
Frequency reuse and clustering

- Adjacent cells cannot use the same channel due to interference
- All cells in the service area are grouped into many clusters; the total spectrum is divided into sub-bands that are distributed among the cells within a cluster; the spatial distribution of sub-bands within the cluster should make sure that adjacent cells do not share the same sub-band
- A cluster of cells together use the entire spectrum
- By dividing the service area into many clusters, the operator can reuse the allocated spectrum spatially over the entire service area

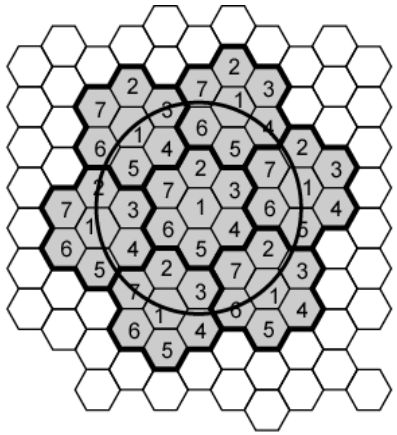
©2020 Mahbub Hassan

Cluster Size

Clusters are shown with solid borders; N represents cluster size

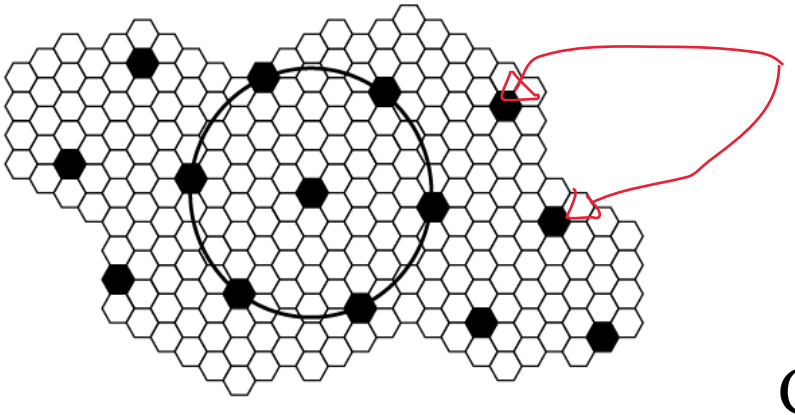


Cluster Size =4



Cluster Size =7

(a) Frequency reuse pattern for N = 4 (b) Frequency reuse pattern for N = 7



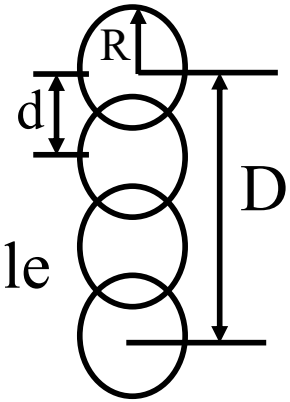
Cluster Size =19

(c) Black cells indicate a frequency reuse for N = 19

©2020 Mahbub Hassan

Characterizing Frequency Reuse

- D = minimum distance between centers of cells that use the same band of frequencies (called co-channels)
- R = radius of a cell
- d = distance between centers of adjacent cells ($d = R\sqrt{3}$)
  - $d < 2R$ due to *overlapping* cells
- N = number of cells in repetitious pattern (**Cluster**)
  - Frequency Reuse Factor = 1/N
  - Each cell in cluster uses unique band of frequencies
- For hexagonal cells, following values of N are possible
  - $N = I^2 + J^2 + (I \times J)$, $I, J = 0, 1, 2, 3, \ldots$
- Possible values of N are 1, 3, 4, 7, 9, 12, 13, 16, 19, 21, …
- Reuse Ratio = Distance/Radius = $D/R = \sqrt{3N}$
- $D/d = \sqrt{N}$



$i = 2$
$j = 0$

©2020 Mahbub Hassan

Example

distance between co-channel cells (D)

Q. What would be the minimum distance between the centers of two cells with the same band of frequencies if *cell radius* is 1 km and the *reuse factor* is 1/12?

Sol. R = 1 km, N = 12

$D/R = \sqrt{3N}$

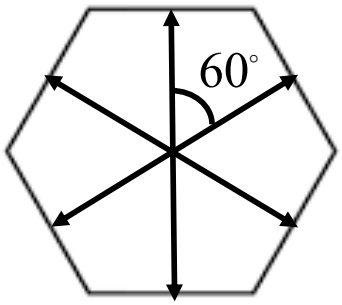
$D = (3\times12)^{1/2} \times 1$ km

$= 6$ km

you cannot reuse the spectrum before 6km

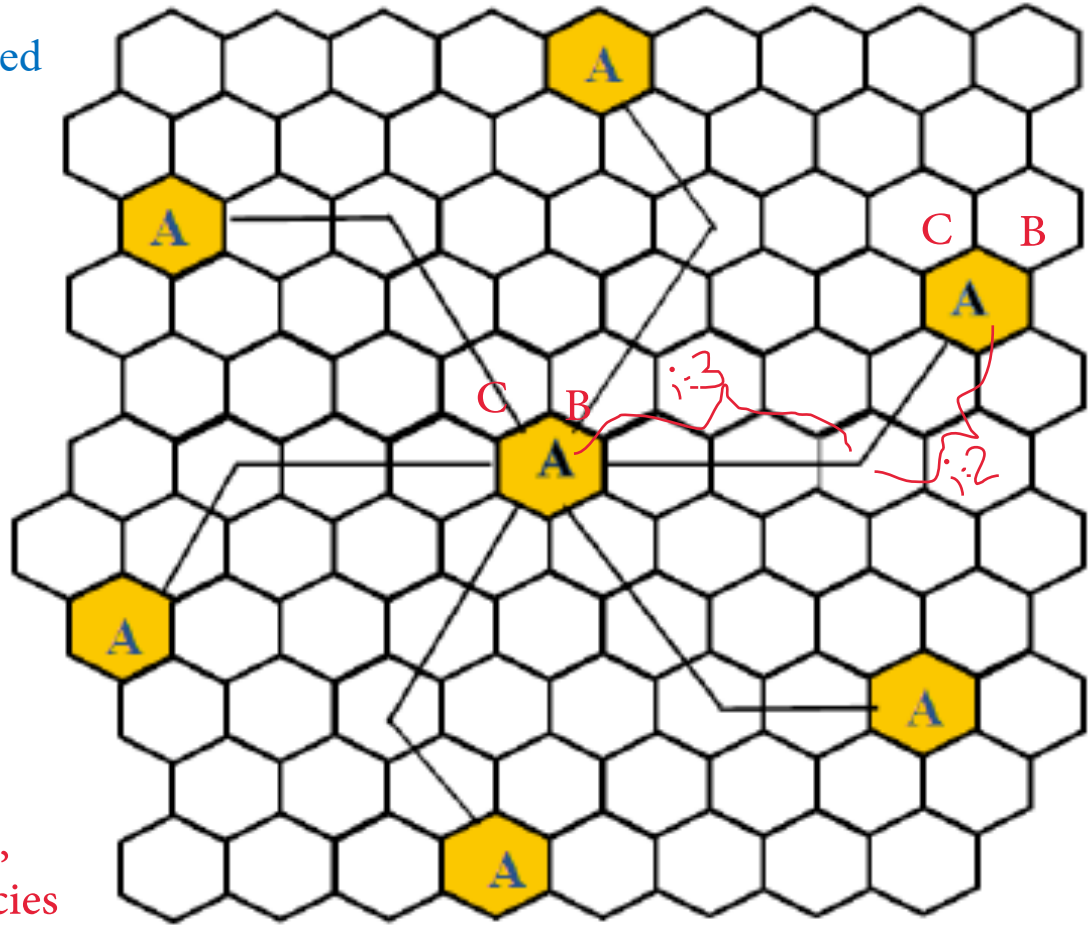
©2020 Mahbub Hassan

Locating Co-channel Cells



6x60 = 360 degrees

6 directions of a hexagon, separated by 60 degrees



- Move *i* cells in any direction
- Turn 60° counter-clock and move *j* cells

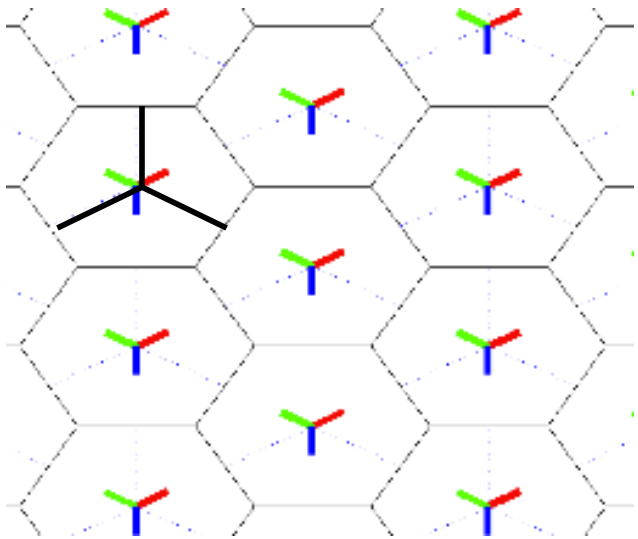
if you switch the values of i and j, the physical locations of frequencies will be slightly different, but you will still have the same frequency re-use factor in your system

i=3, j=2; N=19

©2020 Mahbub Hassan

How to distribute channels among cells within a cluster?

- For simplicity, it is assumed that the total spectrum is divided equally among all cells in the cluster
  - T (total channels), N (cluster size), K (number of channels per cell)
  - K = T/N
- Cells are usually divided into sectors; channels allocated to a cell is then further sub-allocated to different sectors according to the load/demand in each sector; spatial allocation of channels to sectors should try to minimize interference/overlap with the adjacent cell sectors



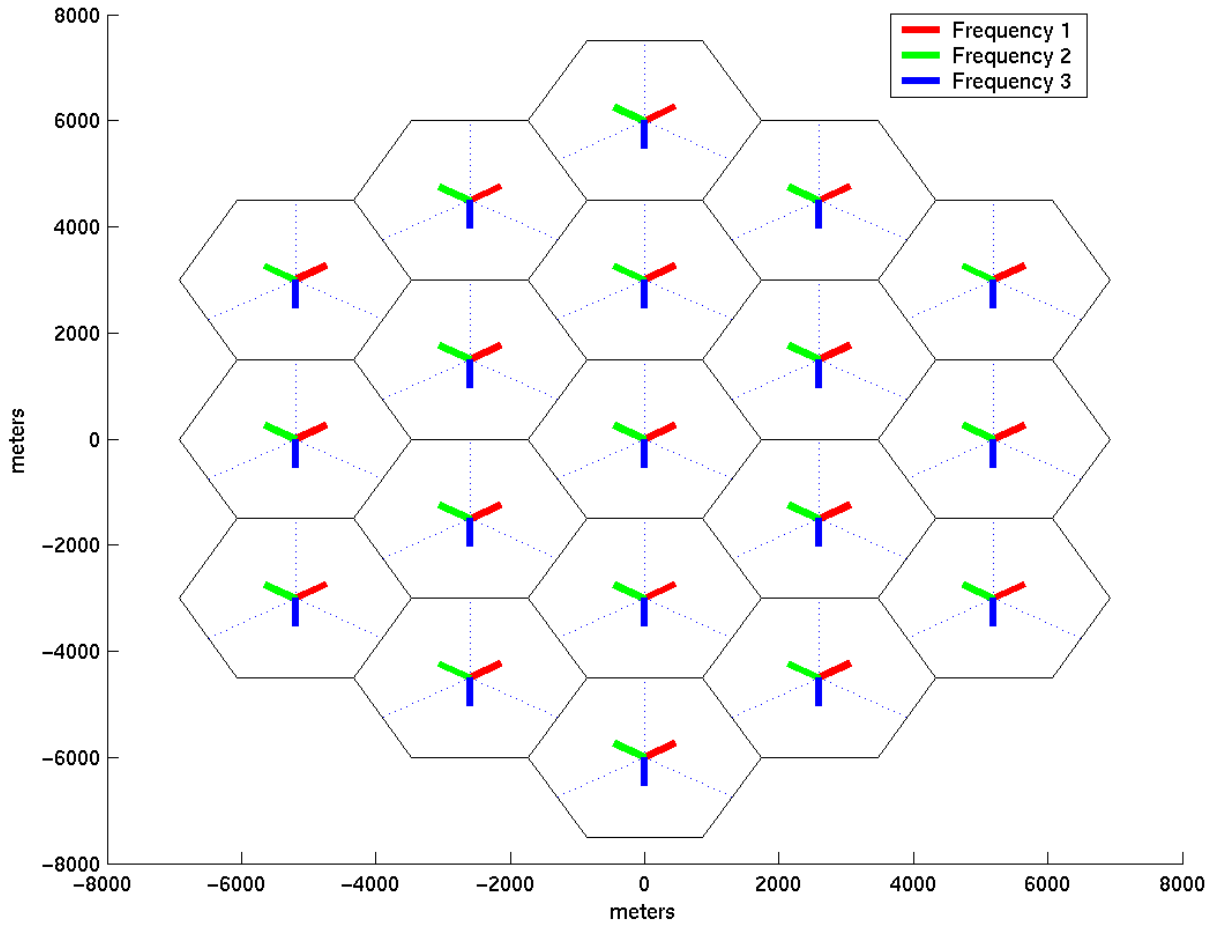
©2020 Mahbub Hassan

Frequency Reuse Notation

- N × S × K frequency reuse pattern
- N=Number of cells per cluster
- S= Number of sectors in a cell
- K = Number of frequency/channel allocations per cell

1X3X3

In this case, K is evenly distributed among all sectors. Uneven allocations can address uneven demands in different sectors. NxSxK notation does not capture the frequency distribution among sectors.



©2020 Mahbub Hassan

Frequency Reuse Notation (Cont)

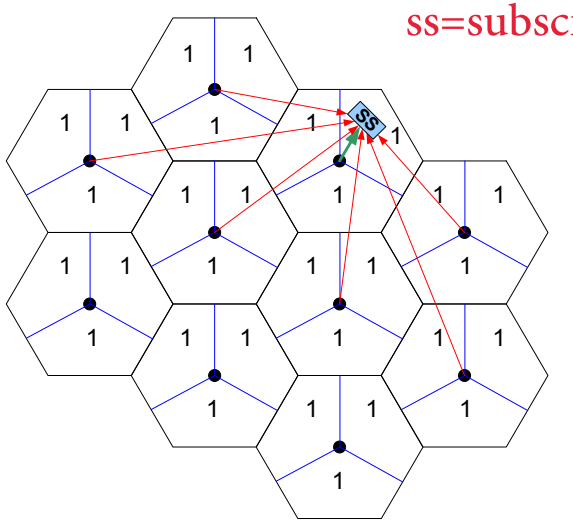
1x3x1

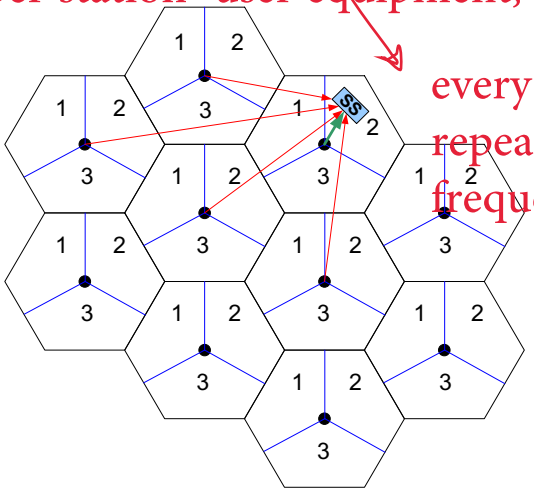
1x3x3

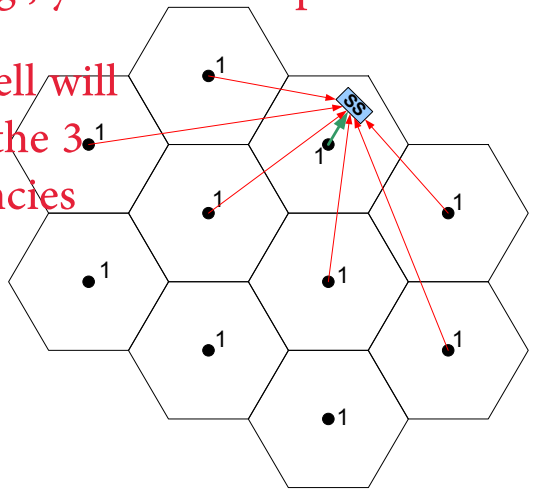
1x1x1

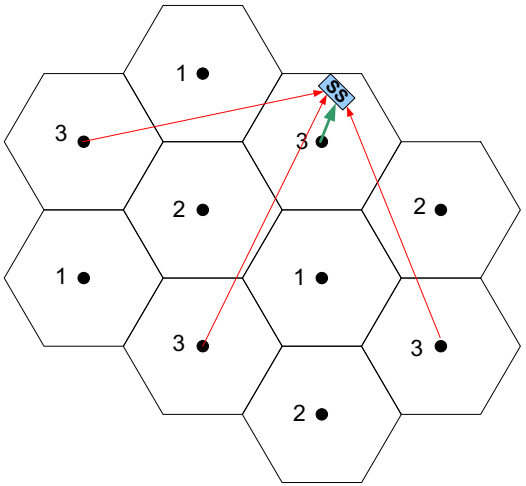
ss=subscriber station=user equipment, e.g., your mobile phone

every cell will repeat the 3 frequencies

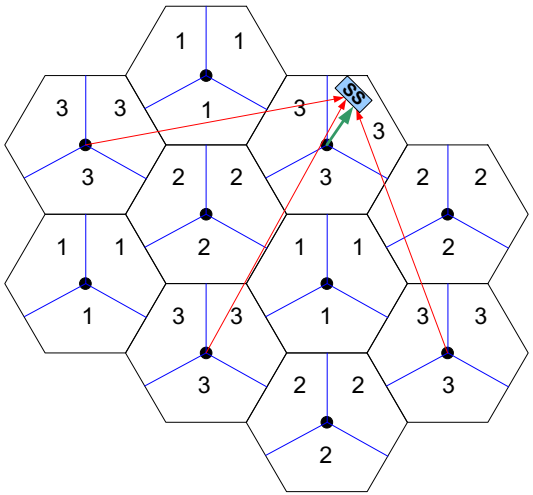




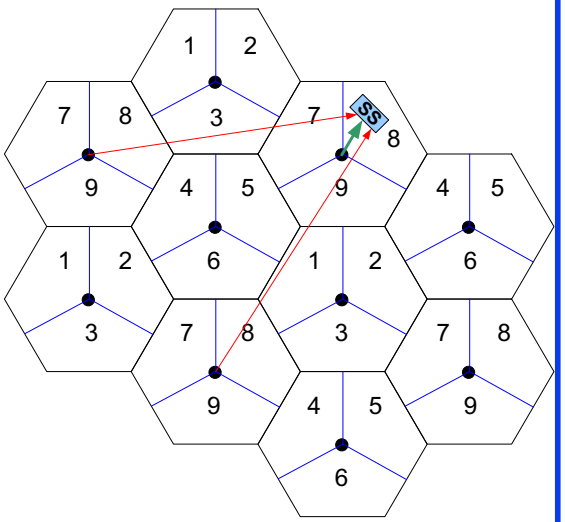




3x1x1



3x3x1

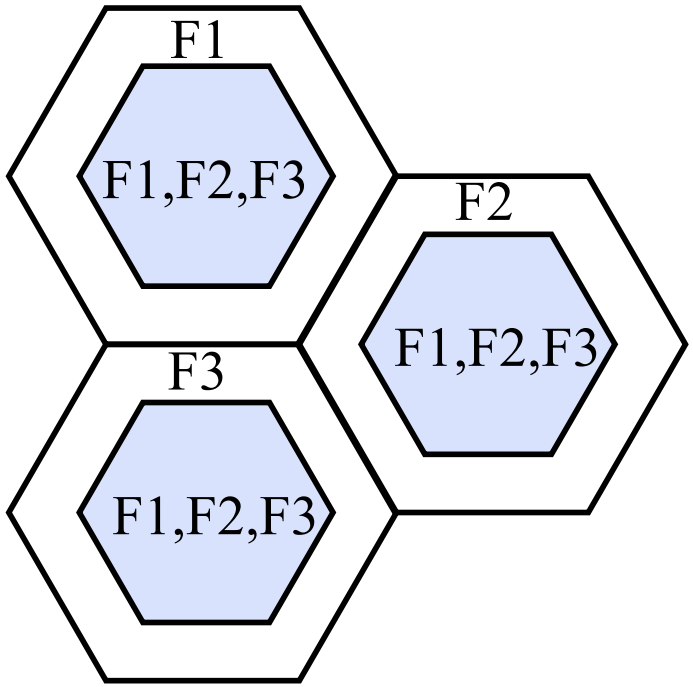


3x3x3

©2020 Mahbub Hassan

Fractional Frequency Reuse

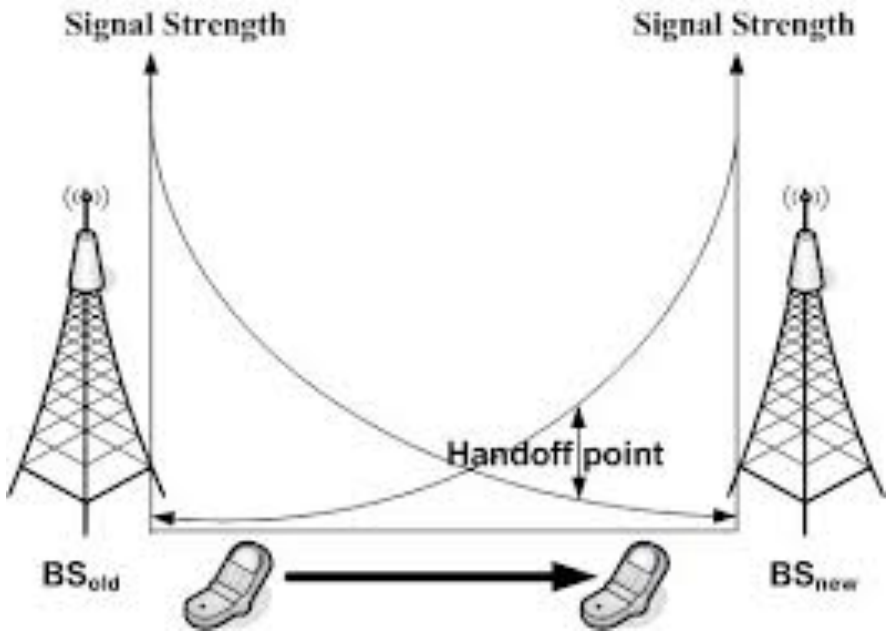
- Users close to the BS use all frequencies
- Users at the cell boundary use only a fraction of available frequencies
- Border frequencies are designed to avoid interference with adjacent cells;



©2020 Mahbub Hassan

Handoff

- User mobility poses challenges for cellular networks; cannot remain connected to the same BS; as the RSS becomes too weak, the mobile device must connect to a new BS with a stronger RSS
- Disconnecting from one and connecting to a new BS during an on-going session is called handoff



©2020 Mahbub Hassan

Frequency Allocation for Handoff

- To handoff successfully, the new BS must have available channels to support the on-going call; otherwise the call will be dropped
- Dropping an ongoing call is worse than rejecting a new call
- BSs therefore usually reserve some channels, called guard channels, exclusively for supporting handoff calls
- Unfortunately, guard channels increases blocking probability of new calls
- The number of guard channels is left to the operators to optimize (not part of the standard)

©2020 Mahbub Hassan

Cellular System Capacity Example

- A particular cellular system has the following characteristics: cluster size =7, uniform cell size, user density=100 users/sq km, allocated frequency spectrum = 900-949 MHz, bit rate required per user = 10 kbps uplink and 10 kbps downlink, and modulation code rate = 1 bps/Hz.

DL=BS-->mobile
UL=mobile--> BS

A. Using FDMA/FDD:
   1. How much bandwidth is available per cell using FDD?
   2. How many users per cell can be supported using FDMA?
   3. What is the cell area?
   4. What is the cell radius assuming circular cells?

B. If the available spectrum is divided in to 35 channels and TDMA is employed within each channel:
   1. What is the bandwidth and data rate per channel?
   2. How many time slots are needed in a TDMA frame to support the required number of users?
   3. If the TDMA frame is 10ms, how long is each user slot in the frame?
   4. How many bits are transmitted in each time slot?

©2020 Mahbub Hassan

Cellular System Capacity (Cont)

- A particular cellular system has the following characteristics: cluster size =7, uniform cell size, user density=100 users/sq km, allocated frequency spectrum = 900-949 MHz, bit rate required per user = 10 kbps uplink and 10 kbps downlink, and modulation code rate = 1 bps/Hz.
- A. Using FDMA/FDD:
  1. How much bandwidth is available per cell using FDD?

     49 MHz/7 = 7 MHz/cell

     FDD ⇒ 3.5 MHz/uplink or downlink
  2. How many users per cell can be supported using FDMA?

     10 kbps/user = 10 kHz ⇒ 350 users per cell

     3.5 MHz / 10 kHz
  3. What is the cell area?

     100 users/sq km ⇒ 3.5 Sq km/cell
  4. What is the cell radius assuming circular cells?

     $\pi r^2 = 3.5 \Rightarrow r = 1.056$ km

©2020 Mahbub Hassan

Cellular System Capacity (Cont)

B. If the available spectrum is divided in to 35 channels and TDMA is employed within each channel:

1. What is the bandwidth and data rate per channel?

   3.5 MHz/35 = 100 kHz/Channel = 100 kbps

2. How many time slots are needed in a TDMA frame to support the required number of users?

   10 kbps/user ⇒ 10 users/channel

3. If the TDMA frame is 10ms, how long is each user slot in the frame?

   10 ms/10 = 1ms

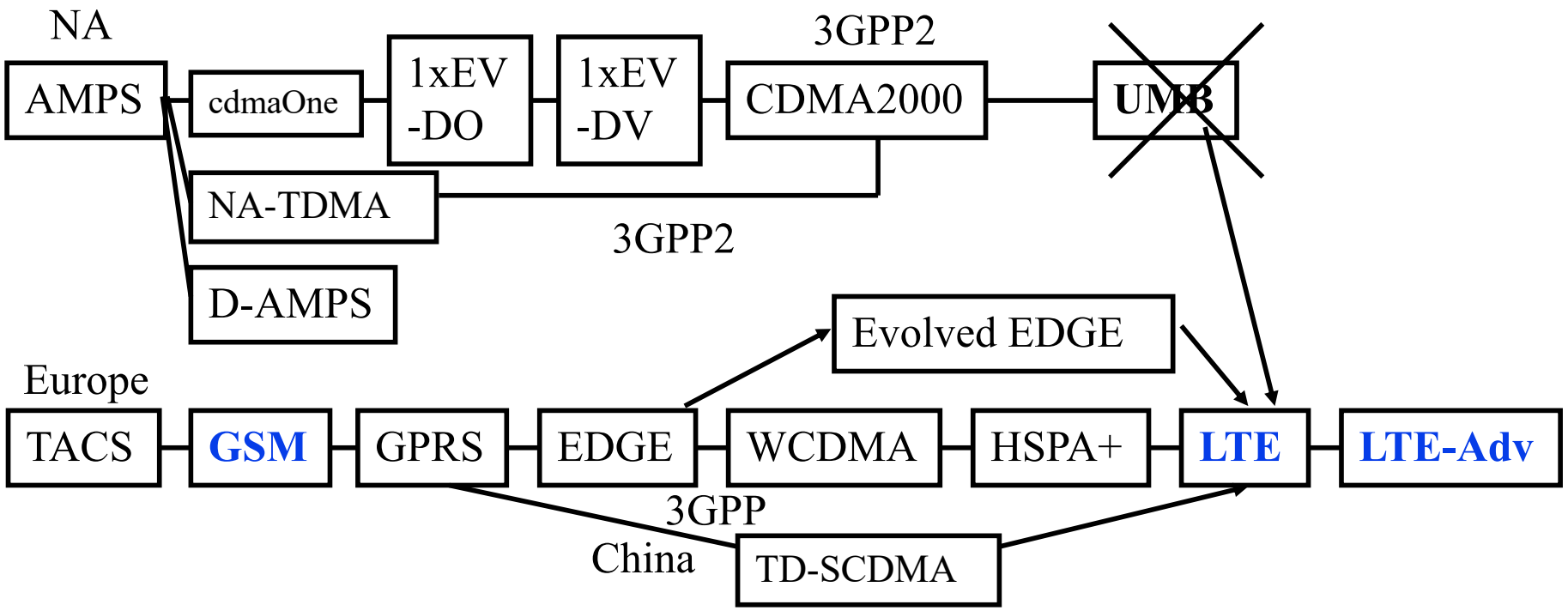
4. How many bits are transmitted in each time slot?

   1 ms x 100 kbps = 100 b/slot = 100 b/ms = ?

   = 100 b/10 ms = 10 kbps

©2020 Mahbub Hassan

Cellular Telephony Generations



Analog FDMA	Digital TDMA CDMA		CDMA	OFDMA+ MIMO	
Voice	Voice	Voice+Data	Voice+Data	Voice+HS Data	All-IP
1G 1983	2G 1990	2.5G	3G 2000	3.5G	4G 2013

©2020 Mahbub Hassan

Cellular Generations (Cont)

- **1G: Analog Voice. FDMA. 1980s**
  - AMPS: Advanced Mobile Phone System
  - TACS: Total Access Communications System
- **2G: Digital Voice. TDMA. 1990**
  - cdmaOne: Qualcomm. International Standard IS-95.
  - NA-TDMA
  - Digital AMPS (D-AMPS)
  - **GSM**: Global System for Mobile Communications
- **2.5G: Voice + Data. 1995.**
  - 1xEV-DO: Evolution Data Optimized
  - 1xEV-DV: Evolution Data and Voice
  - General Packet Radio Service (GPRS)
  - Enhanced Data Rate for GSM Evolution (EDGE)

©2020 Mahbub Hassan

Cellular Generations (Cont)

- **3G: Voice + High-speed data. All CDMA. 2000.**
  - CDMA2000: Qualcomm. International Standard IS-2000.
  - W-CDMA: Wideband CDMA
  - TD-SCDMA: Time Division Synchronous Code Division Multiple Access (Chinese 3G)
  - 384 kbps to 2 Mbps
- **3.5G: Voice + Higher-speed data**
  - EDGE Evolution
  - High-Speed Packet Access (HSPA)
  - Evolved HSPA (HSPA+)
  - Ultra Mobile Broadband (UMB)

©2020 Mahbub Hassan

Cellular Generations (Cont)

- Two Tracks for 1G/2G/3G:
  - Europe 3GPP (3rd Generation Partnership Project)
  - North America 3GPP2
- **3.9G: High-Speed Data. VOIP. OFDMA.**
  - Long Term Evolution (LTE)
- **4G: Very High-Speed Data. 2013.**
  - LTE-Advanced
  - 100 Mbps – 1 Gbps
- **5G: Ultra High-Speed Data. 2020.**
  - IP based

©2020 Mahbub Hassan

LTE: Key Features

Long Term Evolution. 3GPP Release 8, 2009.

1. **Many different bands**: 700/1500/1700/**2100**/2600 MHz
2. **Flexible Bandwidth**: 1.4/3/5/10/15/20 MHz
3. Frequency Division Duplexing (FDD) and
   Time Division Duplexing (TDD)
   $\Rightarrow$ Both *paired* and *unpaired* spectrum
4. 4x4 MIMO, Multi-user collaborative MIMO
5. Beamforming in the downlink

Ref: A. Ghosh, J. Zhang, J. G. Andrews, R. Muhamed, "Fundamentals of LTE," Prentice Hall, 2010, ISBN: 0137033117, 464 pp. Safari book.

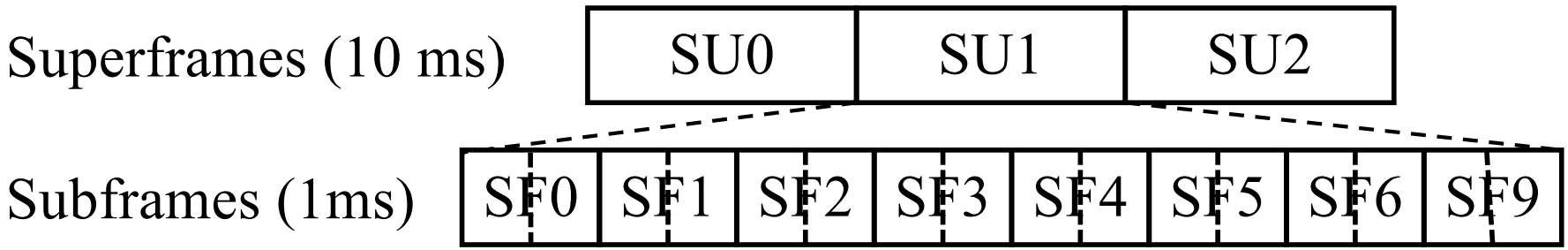
©2020 Mahbub Hassan

LTE: Key Features (Cont)

8. Data Rate: 326 Mbps/down 86 Mbps up (4x4 MIMO 20 MHz)
9. Modulation: OFDM with QPSK, 16 QAM, 64 QAM
10. **OFDMA** downlink,
    Single Carrier Frequency Division Multiple Access (**SC-FDMA**) uplink
11. **Hybrid ARQ** Transmission
12. Short **Frame Sizes** of 10ms and 1ms ⇒ faster feedback and better efficiency at high speed
13. **Persistent scheduling** to reduce control channel overhead for low bit rate voice transmission.
14. **IP based** flat network architecture

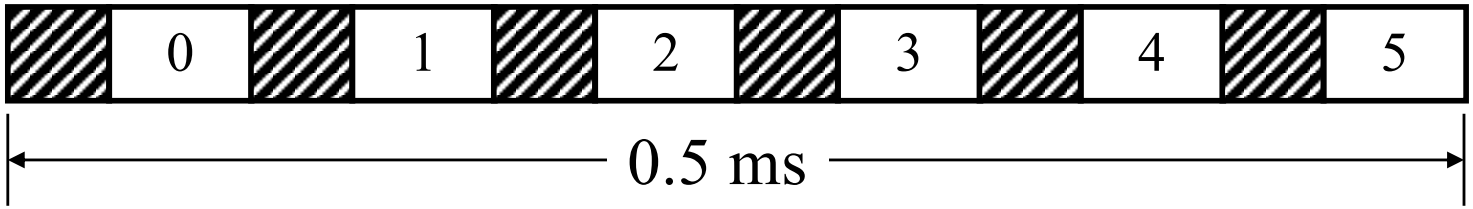
©2020 Mahbub Hassan

LTE Frame Structure



- Subframe = 2 slots of 0.5 ms each
- Slot = 6 or 7 symbols of 66.7 μs (1/15 kHz) each
- Normal Cyclic Prefix: 5.2 μs for 1st symbol, 4.7 μs for others

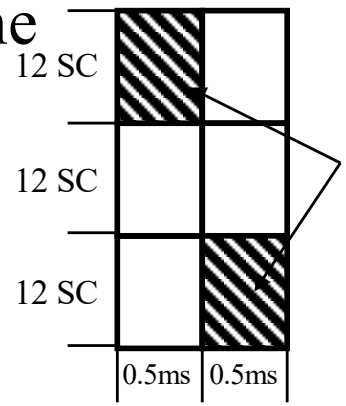
- Extended Cyclic Prefix: for larger networks. 16.7 μs each



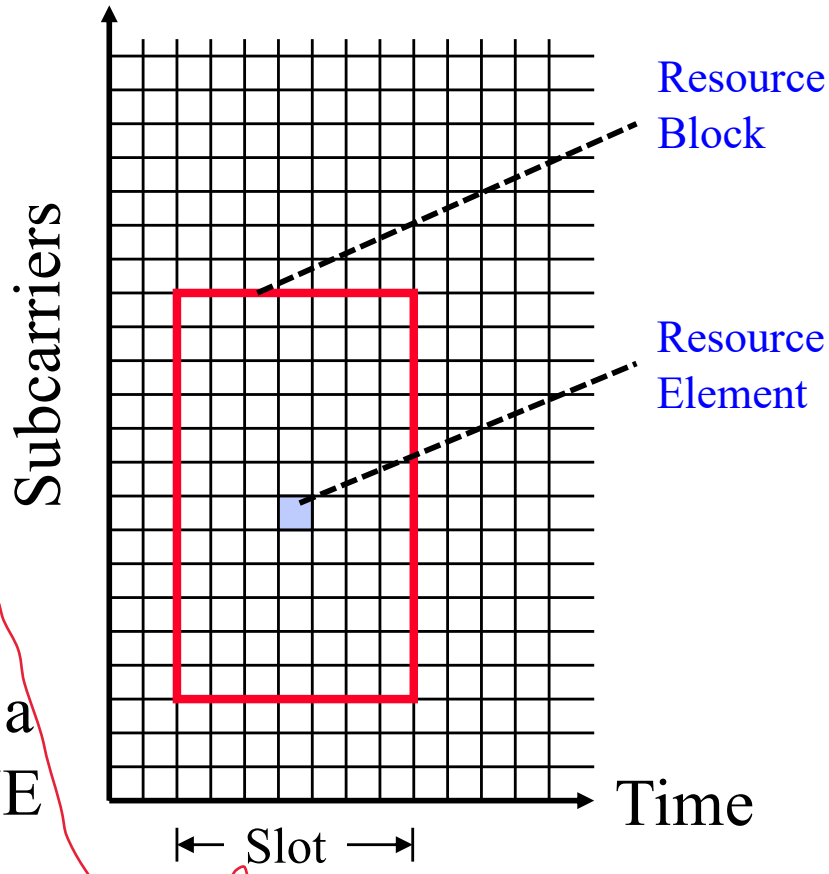
©2020 Mahbub Hassan

Resource Allocation

- **Time slot:** 0.5 ms
  6 or 7 OFDM symbols
- **Subcarriers:** 15 kHz
- **Physical Resource Block (RB):**
  12 subcarriers (180 kHz)
  over 1 time slot
- **Minimum Allocation**: 2 RBs
  per subframe



RBs for a single UE



a slot here has 7 symbols

Ref: A. Ghosh, J. Zhang, J. G. Andrews, R. Muhamed, "Fundamentals of LTE," Prentice Hall, 2010, ISBN: 0137033117, 464 pp.

©2020 Mahbub Hassan

Example

- For *normal* cyclic prefix (CP), how many resource elements (REs) are there in 2 RBs?
- Solution
  - With normal CP, we have 7 symbols per slot
  - Number of REs per RB = 12 x 7 = 84
  - Number of REs in 2 RB = 2 x 84 = 168

©2020 Mahbub Hassan

LTE Transmission Bandwidth

- For downlink, LTE does not use all subcarriers
- Transmission bandwidth < Channel bandwidth

Channel bandwidth [MHz]	1.4	3	5	10	15	20
Transmission bandwidth [MHz]	1.08	2.7	4.5	9	13.5	18
Transmission bandwidth [RB]	6	15	25	50	75	100

http://www.viavisolutions.com/sites/default/files/technical-library-files/LTE_PHY_Layer_Measurement_Guide_0.pdf

©2020 Mahbub Hassan

Example

- What is the *transmission bandwidth* for a resource allocation of 10 RBs?
- Solution
  - Each RB = 180 kHz
  - Transmission Bandwidth = 10 x 180 = 1.8 MHz

©2020 Mahbub Hassan

Example

- What is the *peak data rate* of DL LTE?
- Solution
  - For peak data rate, we assume best conditions, i.e., 64 QAM (6 bits per symbol), short CP (7 symbols per 0.5 ms slot), and 20 MHz channel
  - Each symbol duration = 0.5 ms / 7 = 71.4 μs
  - Number of RB for 20 MHz = 100
  - Number of subcarriers per RB = 12
  - Number of subcarriers for 20 MHz channel = 100 x 12 = 1200
  - Number of bits transmitted per symbol time = 6 x 1200 bits
  - Data rate = (6 x 1200 bits) / (71.4 μs) = 100.8 Mbps (without MIMO)

©2020 Mahbub Hassan

What is 4G?

- International Mobile Telecommunication (IMT) Advanced
- Requirements in ITU M.2134-2008
- IP based packet switch network
- 1.0 Gbps peak rate for fixed services with 100 MHz
- 100 Mbps for mobile services. High mobility to 500 km/hr

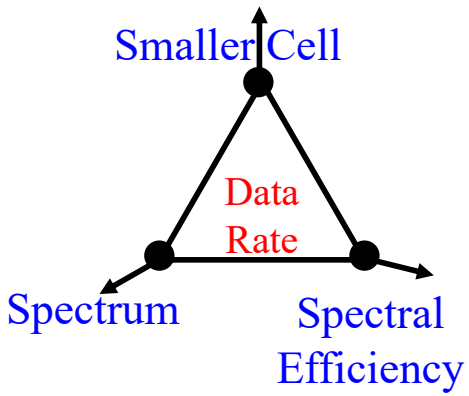
Feature	Cell	Cell Edge	Peak
DL Spectral Efficiency (bps/Hz)	2.2	0.06	15
UL Spectral Efficiency (bps/Hz)	1.4	0.03	6.75

- Seamless connectivity and global roaming with smooth handovers
- High-Quality Multimedia

©2020 Mahbub Hassan

LTE Advanced Techniques

- **Three dimensions of data rates**: Spectrum (Band, Bandwidth), Spectral Efficiency (coding/modulation, MIMO), and Cell sizes (spatial re-use of spectrum)



- **Bandwidth**: 100 MHz using carrier aggregation
  5 carriers allowed now. 32 in future.

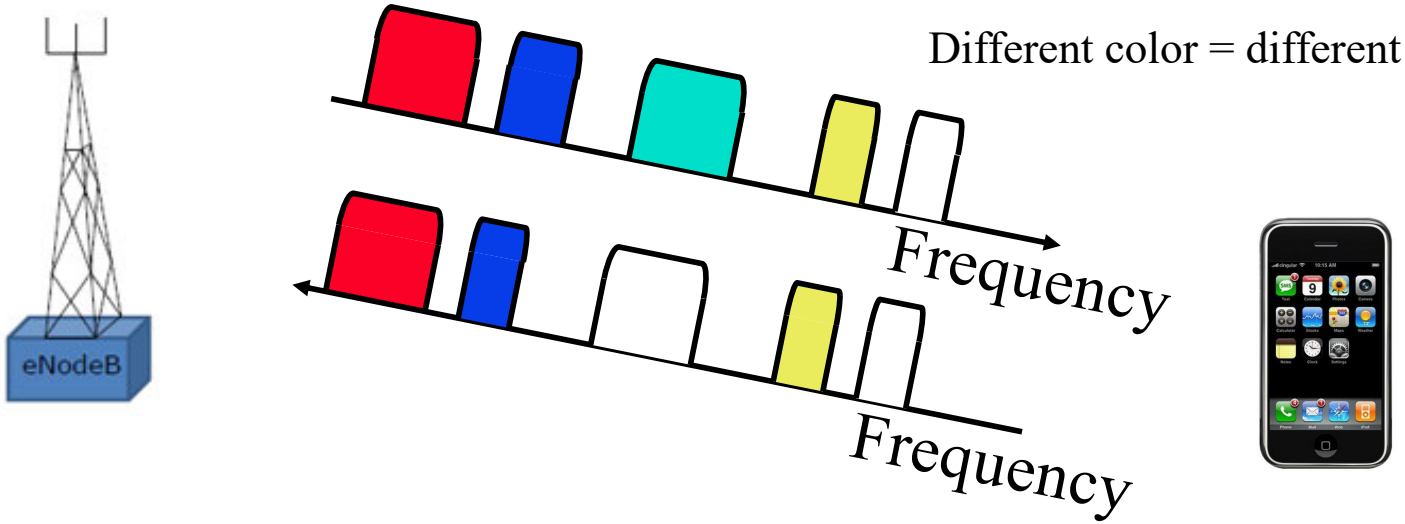
- **Cell Sizes and Spectrum Re-use**:
  - Smaller cells
  - Frequency Reuse Factor of 1

- **Spectral Efficiency**:
  - Higher order MIMO (8x8 DL, 4x4 UL)
  - New MIMO Techniques: Single-user uplink MIMO
  - Inter-Cell Interference Co-ordination and cancellation

©2020 Mahbub Hassan

Carrier Aggregation

- Aggregation = Combine multiple bands (Component Carriers)

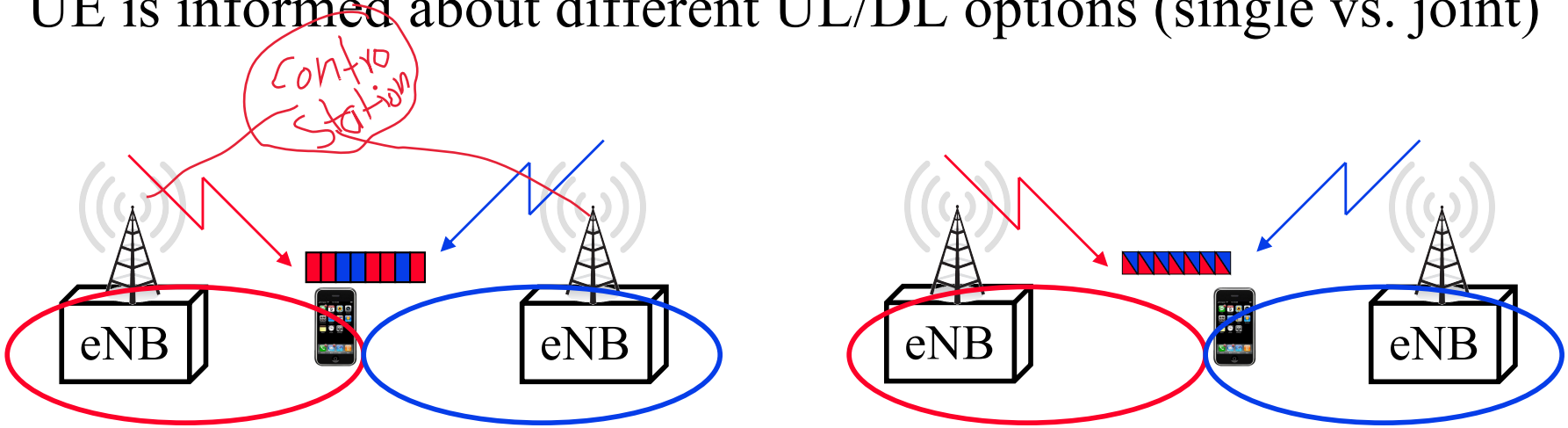


- Backward compatible with LTE (Single carrier)
  ⇒ Each band can be 1.4, 3, 5, 10, or 20 MHz
- Maximum 5 component carriers ⇒ 100 MHz max
- Each component can be different width
- Number of components in DL and UL can be different, but
  Number of components in DL ≥ Number of components in UL

©2020 Mahbub Hassan

Coordinated Multipoint Operation (CoMP)

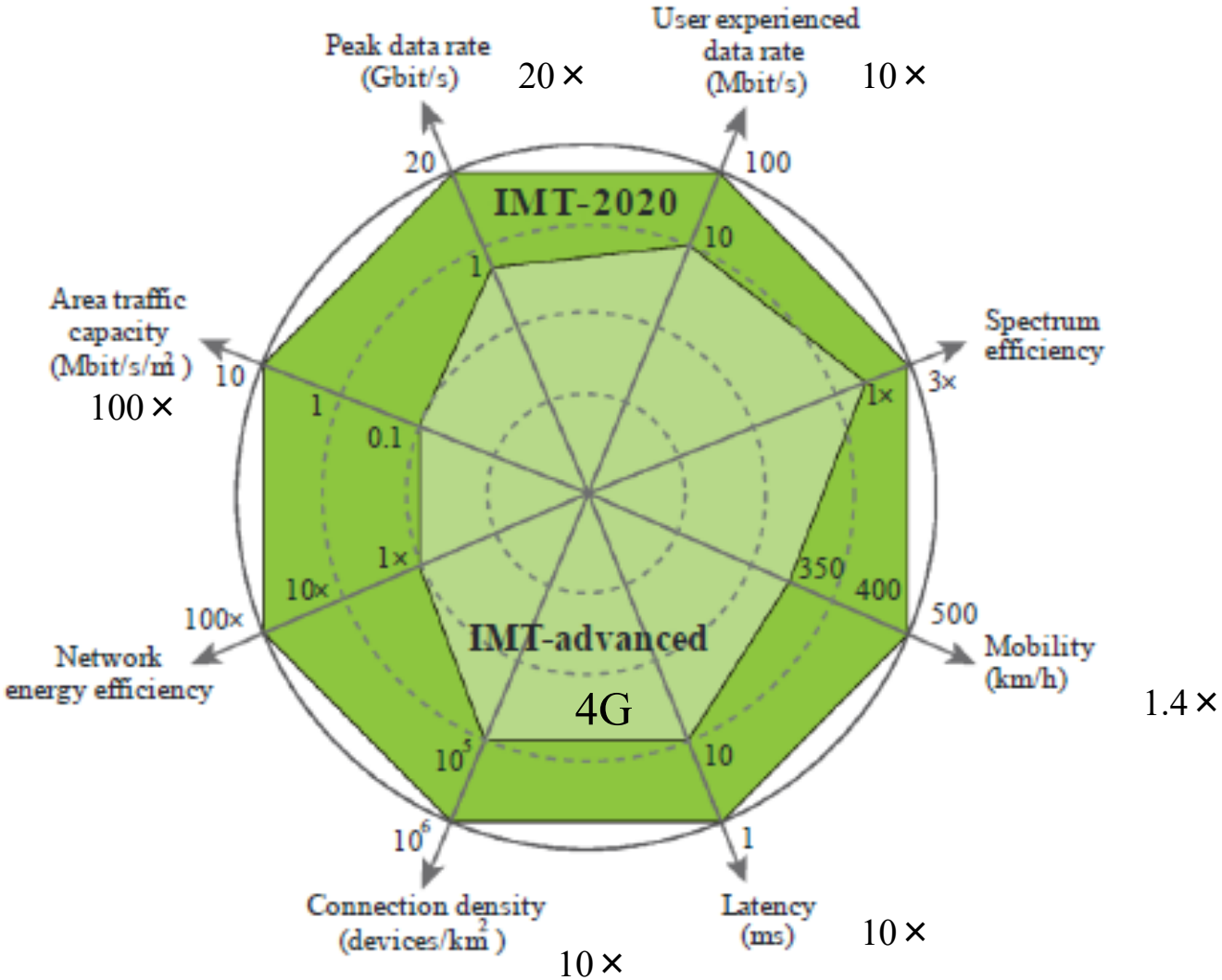
- To improve performance at cell edge
- Base stations coordinate transmissions and reception
- Single Tx (DL): Only one BS transmits in each subframe
- Joint Tx (DL): Multiple transmitters in the same subframe
- Joint Reception (UL): Multiple BSs receive the signal from one UE and combine
- UE is informed about different UL/DL options (single vs. joint)



(a) Single transmission (b) Joint Transmission

©2020 Mahbub Hassan

5G Definition

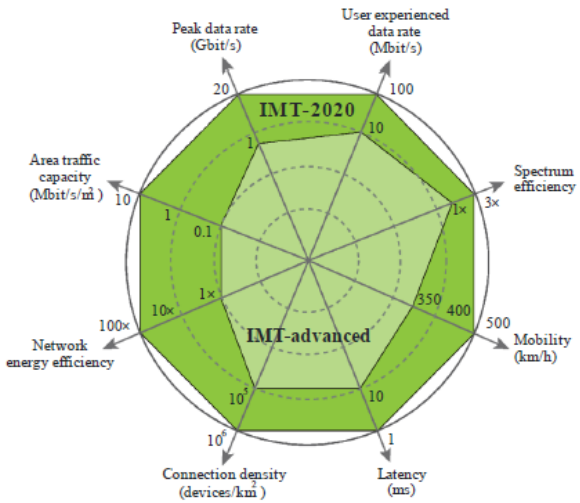


Ref: ITU-R Recommendation M.2083-0, "IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond," Sep. 2015, 21 pp., https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf

©2020 Mahbub Hassan

5G Definition (Cont)

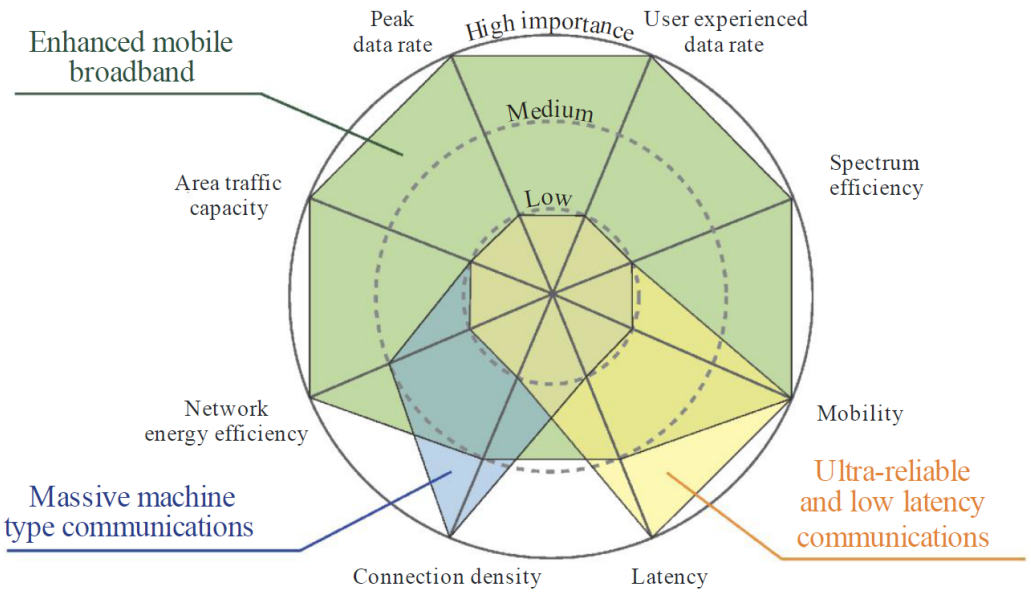
1. Peak Data Rate: max rate per user under ideal conditions. 10 Gbps for mobiles, 20 Gbps under certain conditions.
2. User experienced Data Rate: Rate across the coverage area per user. 100 Mbps in urban/suburban areas. 1 Gbps hotspot.
3. Latency: Radio contribution to latency between send and receive
4. Mobility: Max speed at which seamless handover and QoS is guaranteed
5. Connection Density: Devices per km^2
6. Energy Efficiency: Network bits/Joule, User bits/Joule
7. Spectrum Efficiency: Throughput per Hz per cell
8. Area Traffic Capacity: Throughput per m^2



©2020 Mahbub Hassan

Importance

- Three Key Application Areas:
  - Enhanced Mobile Broadband
  - Ultra-Reliable and Low Latency: Real-time, safety
  - Massive Machine Type Communications (IoT)

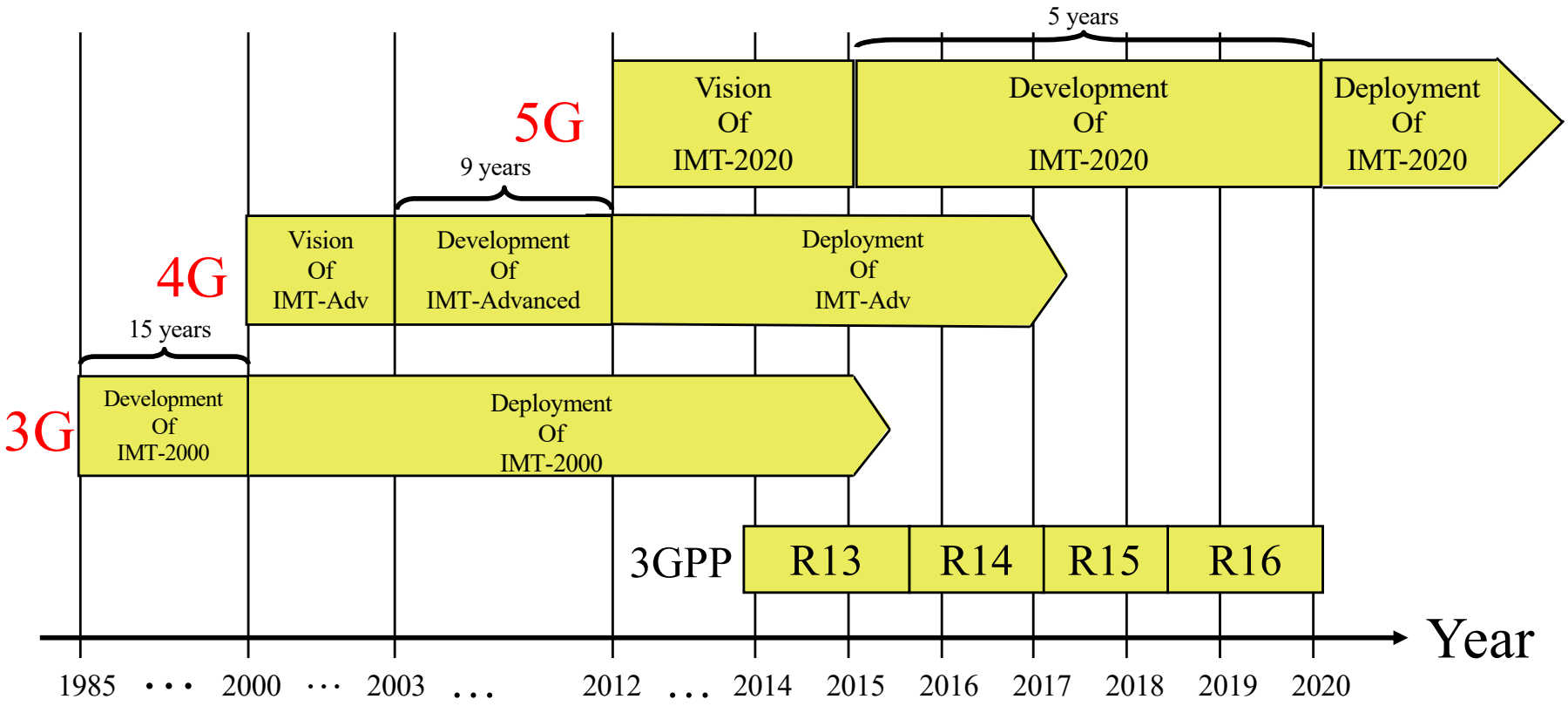


Ref: ITU-R Recommendation M.2083-0, "IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond," Sep. 2015, 21 pp., https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf

©2020 Mahbub Hassan

Timeline

- 3G: IMT-2000 started in 1985, first release in 2000
- 4G: IMT-Advanced, vision in 2003, first release in 2012
- 5G: IMT-2020, vision in 2015, first release in 2020



Ref: ITU-R, "Workplan, timeline, process and deliverables for the future development of IMT," 4pp.,

©2020 Mahbub Hassan

How?

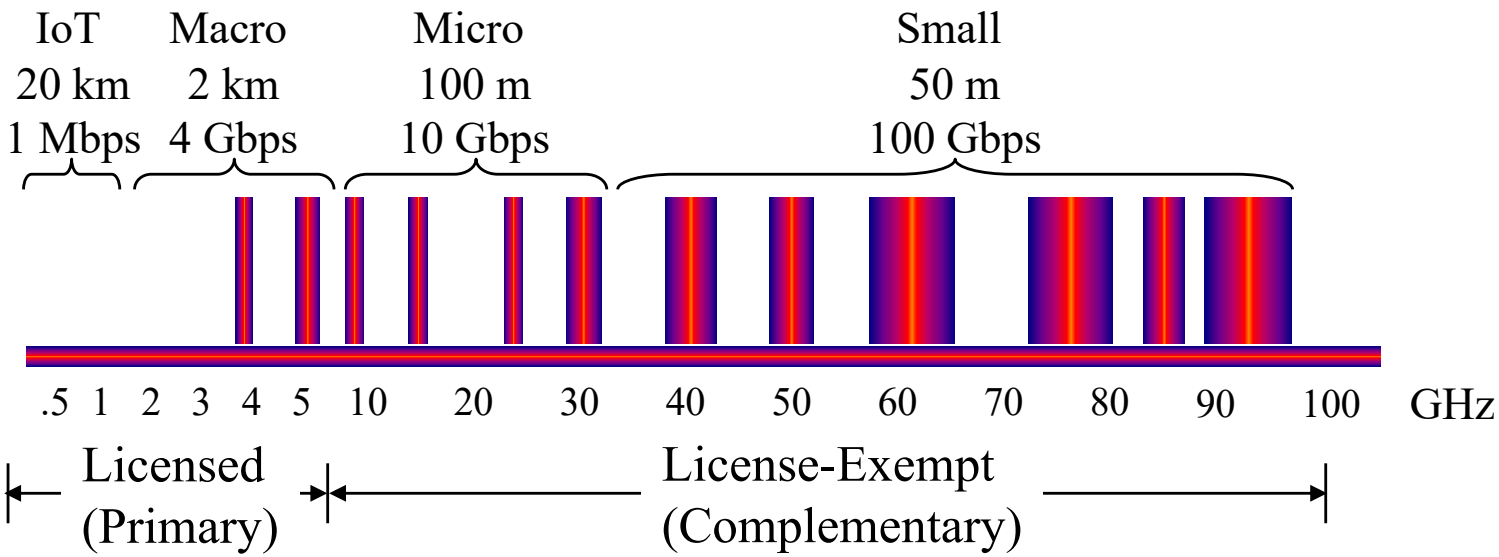
5G

- **New Radio Multiplexing Techniques** [Spectrum Filtered OFDM (f-OFDM), Filtered Bank Multicarrier (FBMC), Non-Orthogonal Multiple Access (NOMA), Pattern Division Multiple Access (PDMA), Low Density Spreading, (LDS), Sparse Code Multiple Access (SCMA), Interleave-Division Multiple Access (IDMA)]
- **New Efficient Spectrum Usage** [3D Beamforming and Massive MIMO, FDD-TDD Carrier Integration, Distributed Antenna Systems (DAS), Simultaneous Transmission and Reception, Dynamic TDD, License Assisted Access (LAA), Multimode Base Stations, Intelligent Multi-Mode RAT Selection, Higher order modulations in small cells]
- **New Spectrum**
- **New Energy Saving** [Discontinuous Transmission (DTX), Antenna Muting, Cell on/off switching, Power Save Mode for IoT]
- **CapEx/OpEx Reduction** [Software Defined Networking (SDN), Network Function Virtualization (NFV), Mobile Edge Computing (MEC), Cloud Radio Access Network (C-RAN)]
- **Application Specific Improvements** [HTTP-based Video, Narrow-band IoT]

©2020 Mahbub Hassan

New Spectrum

- ITU estimates 900-1420 MHz required for 4G/5G by 2020 and 440-540 MHz required for 2G/3G and their enhancements



Ref: P. Zhu, "5G Enabling Technologies," PIMRC, Sep 2014, 20 slides, http://www.ieee-pimrc.org/2014/2014-09-03%205G%20Enabling%20Technologies%20PMIRC%20Huawei_Final.pdf

Ref: ITU-R M.2290-0, "Future Spectrum Requirements estimate for Terrestrial IMT," Dec 2013, http://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2290-2014-PDF-E.pdf

Huawei, "White Paper on Spectrum," February 2013, http://www.huawei.com/us/others/index-cdf_en_group_white_book.htm

©2020 Mahbub Hassan

Above 6 GHz

- Free-space loss increases in proportion to square of frequency and square of distance. 88 dB loss with 30 GHz at 20 m $\Rightarrow$ 10-100 m cell radius
- Outdoor-to-Indoor: Glass windows add 20-40 dB
- Mobility: Doppler shift is proportional to frequency and velocity. Multipath results in varying Doppler shifts $\Rightarrow$ Lower mobility
- Wide Channels: Duplex filters cover only 3-4% of center frequency $\Rightarrow$ Need carrier aggregation.
- Antenna: 8x8 array at 60 GHz is only 2cm x 2cm. A/D and D/A converters per antenna element may be expensive
- 2 Gbps up to 1 km may be feasible using mm waves

©2020 Mahbub Hassan

Summary

- In a cellular cluster of size N, the minimum distance between cells with same frequencies is D =R$\sqrt{3N}$. Here R is the cell radius.
- 1G was analog voice with FDMA
- 2G was digital voice with TDMA. Most widely implemented 2G is GSM. Data rate was improved by GPRS and EDGE.
- 3G was voice+data with CDMA. Most widely implemented 3G is W-CDMA using two 5 MHz FDD channels. Data rate was improved later using HSPA and HSPA+.
- LTE uses a **super-frame** of 10 subframes of 1 ms each. Each **subframe** has one 0.5 ms **slot** for uplink and downlink each.
- LTE Advanced truly meets 4G requirements; supports up to 100 MHz channels by aggregating bandwidth from the same or different carriers
- 5G is being launched in 2020 promising to offer ultra-high data rates, ultra-low latency, and massive connectivity for Internet of Things; it will use new spectrum in the millimeter wave band and deploy new techniques for improving spectrum efficiency and energy savings.

©2020 Mahbub Hassan

Mobile IP

©2020 Mahbub Hassan

Lecture Overview

- IP Mobility
  - Significance of mobility in IP networks
  - Peculiarities of IP addressing
  - Quasi-mobility vs. Full IP mobility
- Mobile IP
  - conceptual framework
  - basic operation
  - latency problem and route optimisation
  - ingress filtering and reverse tunneling
  - handoff delay
  - improvements in IP Version 6
- Network Mobility
- Proxy Mobile IP

©2020 Mahbub Hassan

Prerequisite knowledge

- IP Addressing
- DHCP
- ICMP
- PPP
- Reference textbooks
  - any introductory text on networking

©2020 Mahbub Hassan

Significance of TCP/IP Mobility

why move in TCP/IP networks?

©2020 Mahbub Hassan

Data means IP

- Internet is based on IP
- IP is ubiquitous
- IP is the *de facto* standard for data
- You want data, you must connect to IP network

©2020 Mahbub Hassan

Mobile data ➔ IP mobility

- Mobile data requires mobile connectivity to IP networks (or the Internet)
- Mobile data (wireless Internet access) increasingly desired
- Phone calls can be made over IP (VOIP)
  - (next to) free phone calls!

©2020 Mahbub Hassan

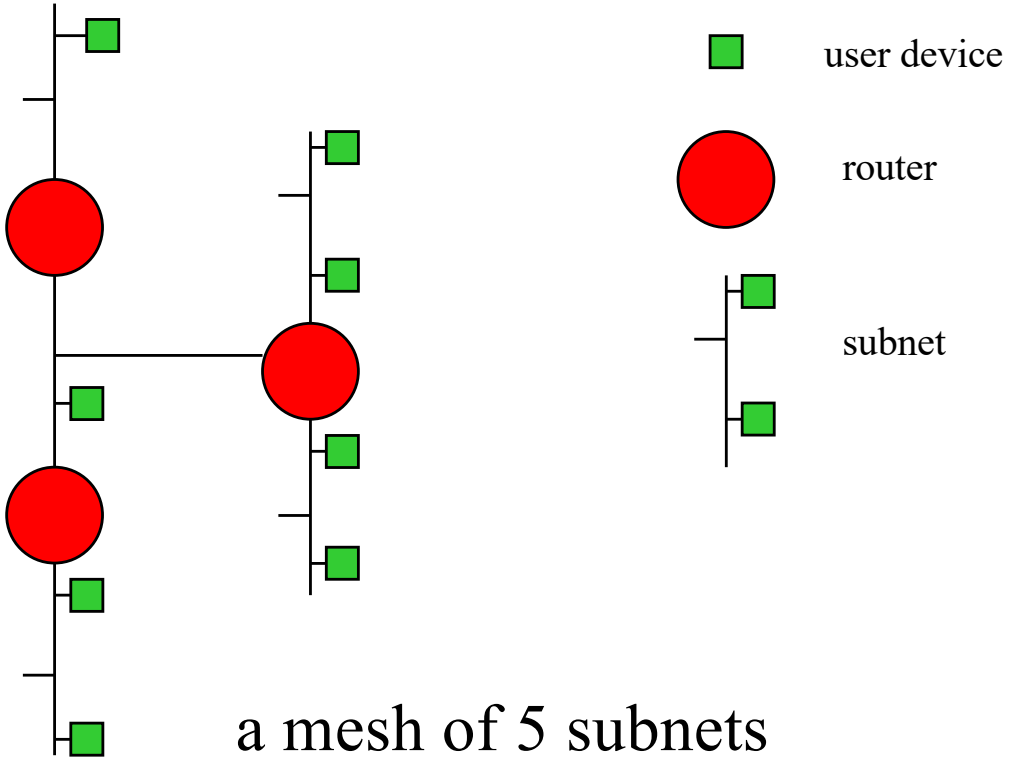
Peculiarities of IP addressing

what IP addressing has got to do with mobility

©2020 Mahbub Hassan

The world of IP

- A mesh of subnets interconnected by routers
- User device must be connected to one of the subnets

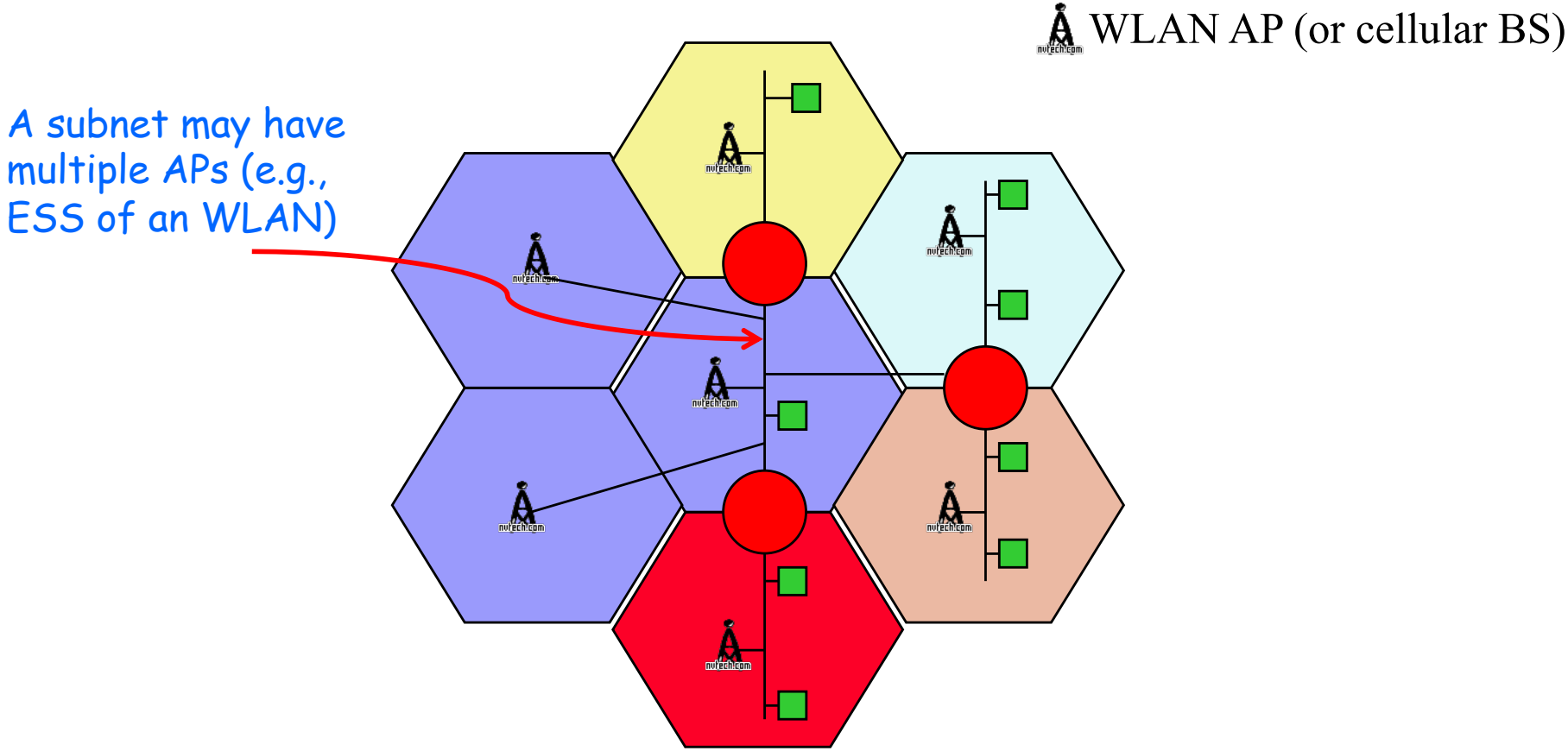


a mesh of 5 subnets

©2020 Mahbub Hassan

The world of IP
going wireless

- Wireless makes it easy to connect to a subnet



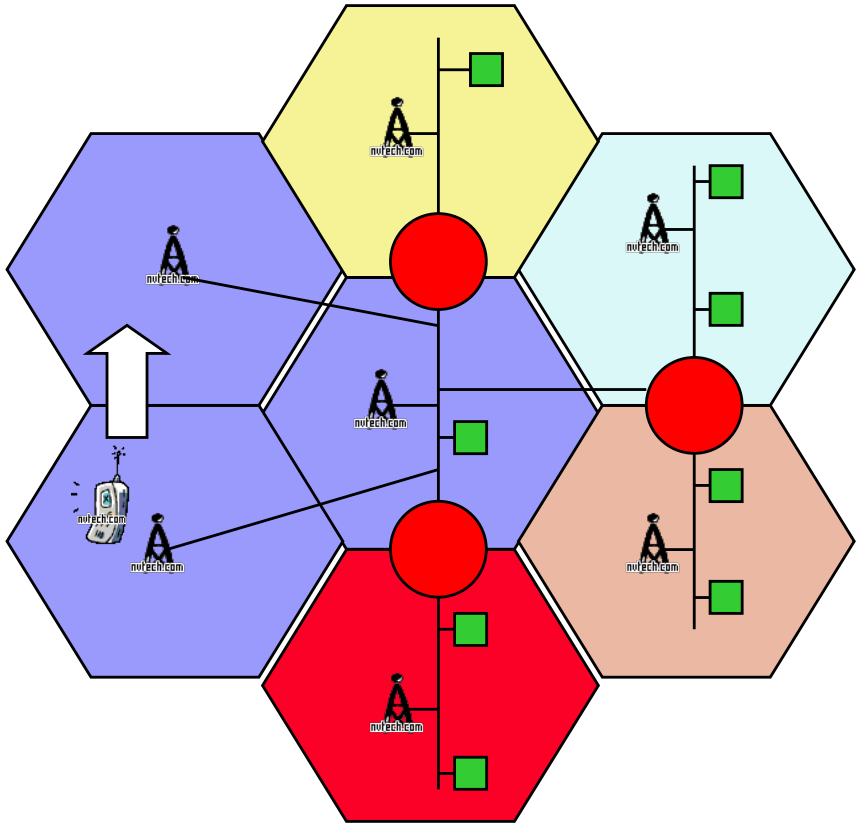
©2020 Mahbub Hassan

Peculiarities of IP addressing

- A device must use a unique IP address to connect
- An IP address must carry the subnet prefix
  - eg 10.3.4.24/8 defines a host attached to subnet 10.0.0.0/8, and
  - 10.3.4.24/8 cannot be used to connect to subnet 12.0.0.0/8
- Subnet prefix is unique (makes IP address unique)
  - Used for routing
- Result ➔ inter-subnet movement requires change of IP address for the mobile device (intra-subnet movement does not)

©2020 Mahbub Hassan

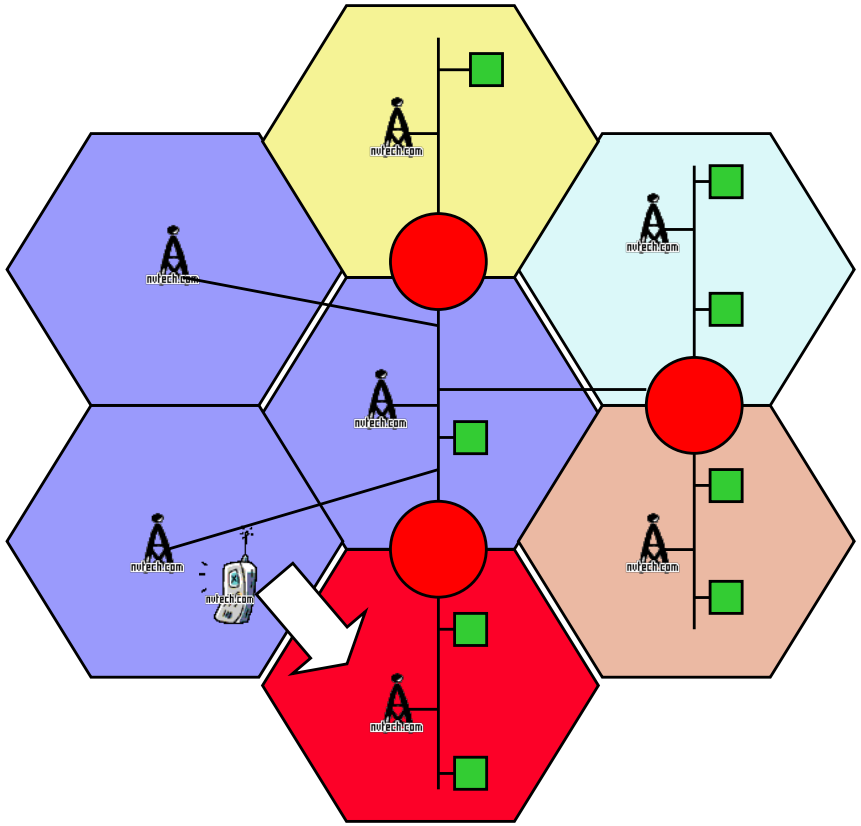
Intra-subnet movement



this movement *does not* require change of IP address

©2020 Mahbub Hassan

Inter-subnet movement



this movement *does* require change of IP address

©2020 Mahbub Hassan

Quasi-mobility vs Full Mobility

©2020 Mahbub Hassan

Grades of mobility

- Quasi-mobility
  - YES: connect to Internet from any subnet
  - NO: move across subnet boundary within session
- Full mobility
  - YES: connect to Internet from any subnet
  - YES: move across subnet boundary within session

©2020 Mahbub Hassan

Quasi-mobility using DHCP-WLAN

- DHCP enables automatic IP address acquisition
  - get a new IP address valid for the new subnet
- WLAN makes connectivity even more effortless
  - Laptops and smartphones have built-in 802.11 capability (no WLAN cards required)
- Enables wireless/mobile Internet access
  - web browsing, e-mails, on-line chat, VPN, download, …
  - from cafes, airports, hotels, train stations, …
  - proved very useful and popular

©2020 Mahbub Hassan

Challenges of Full IP Mobility

©2020 Mahbub Hassan

Difficult to avoid address change (at subnet border crossing)

- Change of IP address at subnet border crossing is a key mobility problem
- No address change ➔ host-based routing
- Host-based routing does not scale
  - billions of hosts ➔ routing table explosion
  - routing table update required for every move
- Must find solutions that work with change of IP address

©2020 Mahbub Hassan

Mobile IP
enabling full mobility in IP networks

©2020 Mahbub Hassan

Conceptual framework

- Location = subnet
  - change of subnet = change of location
- Update location at subnet border crossing
- Location server always knows the current location of the mobile

©2020 Mahbub Hassan

Mobile IP Solution

- An IETF standard
  - (originally RFC 3344, now obsoleted by RFC5944)
- Most vendors support Mobile IP in their products, such as CISCO Routers

©2020 Mahbub Hassan

Dual IP Address

- With MIP, A mobile host has TWO IP addresses
  - a permanent address (or home address)
  - a temporary care of address (CoA)

©2020 Mahbub Hassan

Home Address

- Home address = permanent IP address of the mobile host assigned during subscription
  - prefix of home address defines mobile's home subnet
- Mobile is always known by its home address
  - like the cellular phone number
- Anyone can reach the mobile anytime using home address
  - Home address does not change due to mobility
- DNS tables store home address
  - not updated during mobility
  - *mobility remains transparent to the rest of the world*

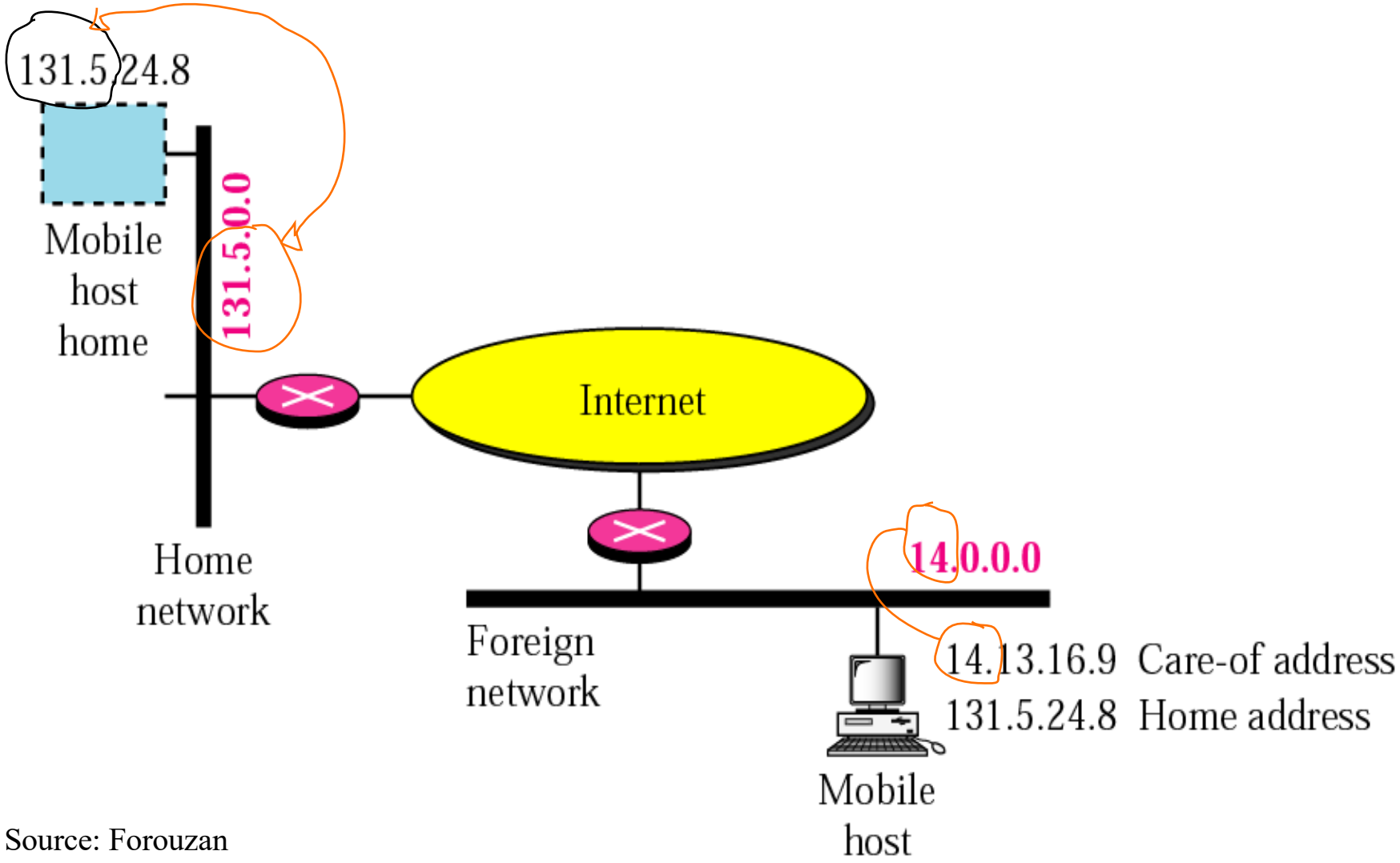
©2020 Mahbub Hassan

Care of Address

- A mobile host attached to a foreign network can be reached using a CoA
- CoA of a mobile host changes as it attaches to different subnets over time
  - mobile would require to update its CoA as it moves through different subnets

©2020 Mahbub Hassan

Illustration of Home Address and CoA address



Source: Forouzan

©2020 Mahbub Hassan

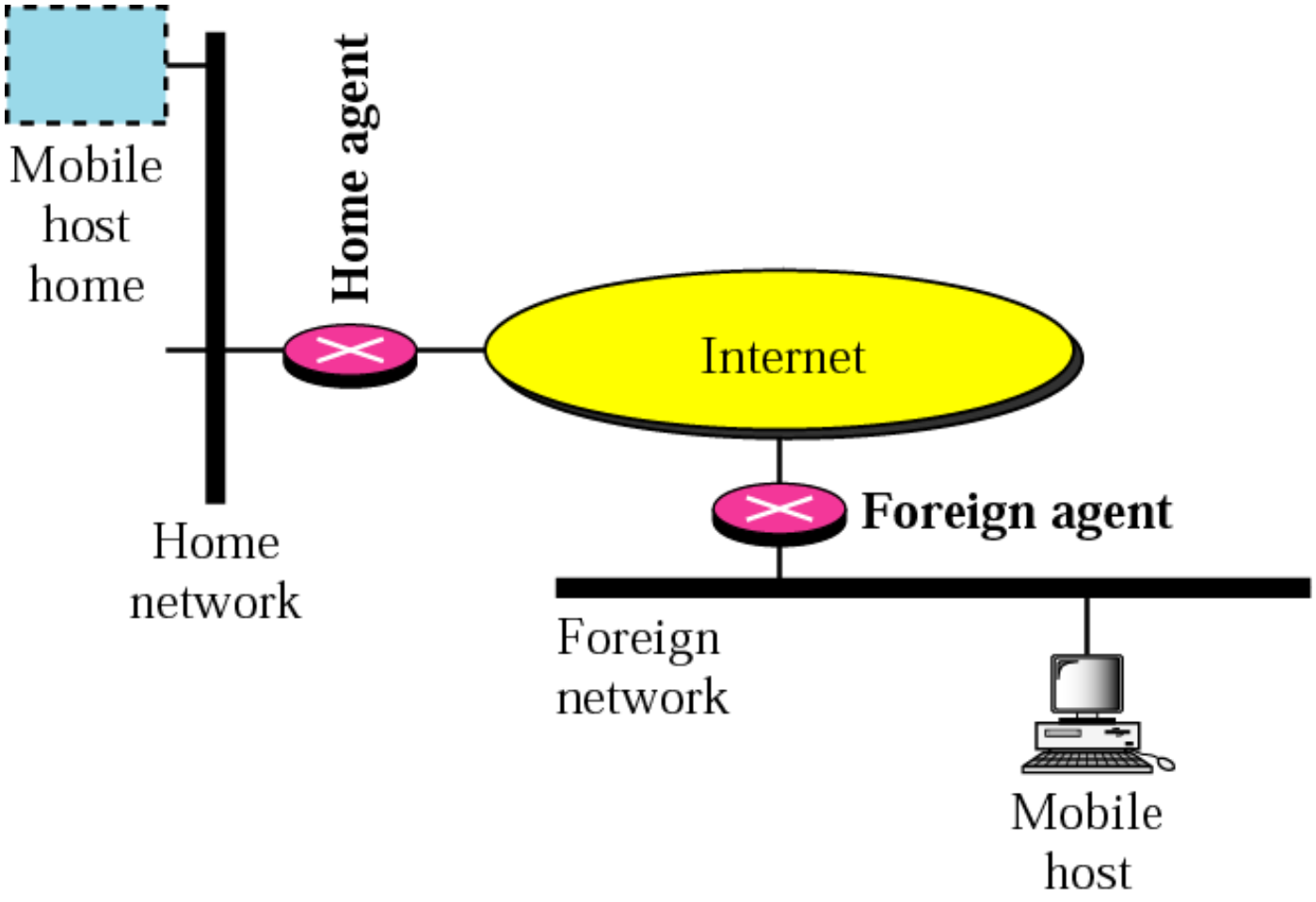
Mobile IP agents

- Mobile IP requires two agents for its operation
- Home agent (HA) resides at home network
- Foreign agent (FA) resides at foreign network
- A network has both home agent & foreign agent
  - A network is home to some and foreign to others

©2020 Mahbub Hassan

Illustration of HA and FA

Agents are usually implemented in the routers



©2020 Mahbub Hassan

Home agent functions

- Typically implemented in a router
- Maintains up-to-date whereabouts (CoA) of mobile (home) hosts
  - acts as a location server for home hosts
- Receives packets on behalf of "out of town" mobile hosts and sends them to foreign agents

©2020 Mahbub Hassan

Foreign agent functions

- Accepts packets from home agents and delivers them to visiting mobile hosts
- Typically implemented in a router attached to the foreign subnet (or domain)
- Alternatively, FA can be located at mobile
  - called co-located CoA
  - mobile host does not need services of FA from the foreign network, but needs a new IP address to connect to foreign subnet

©2020 Mahbub Hassan

A Note on CoA

this CoA address is an IP address exclusively for the mobile device

- Co-located CoA
  - mobile needs unique IP address (consumes IP address)
  - unique address is obtained using DHCP etc.
- Foreign agent CoA
  - typically FA is a router known by several IP addresses
  - mobile uses one of FA IP addresses as CoA
  - several mobiles can use the same CoA
  - no new IP address is consumed (*DHCP not used!*)
  - Mobile connects using its permanent address

©2020 Mahbub Hassan

Phases of Mobile IP
FA located in router

Agent discovery is replaced by DHCP for colocated CoA

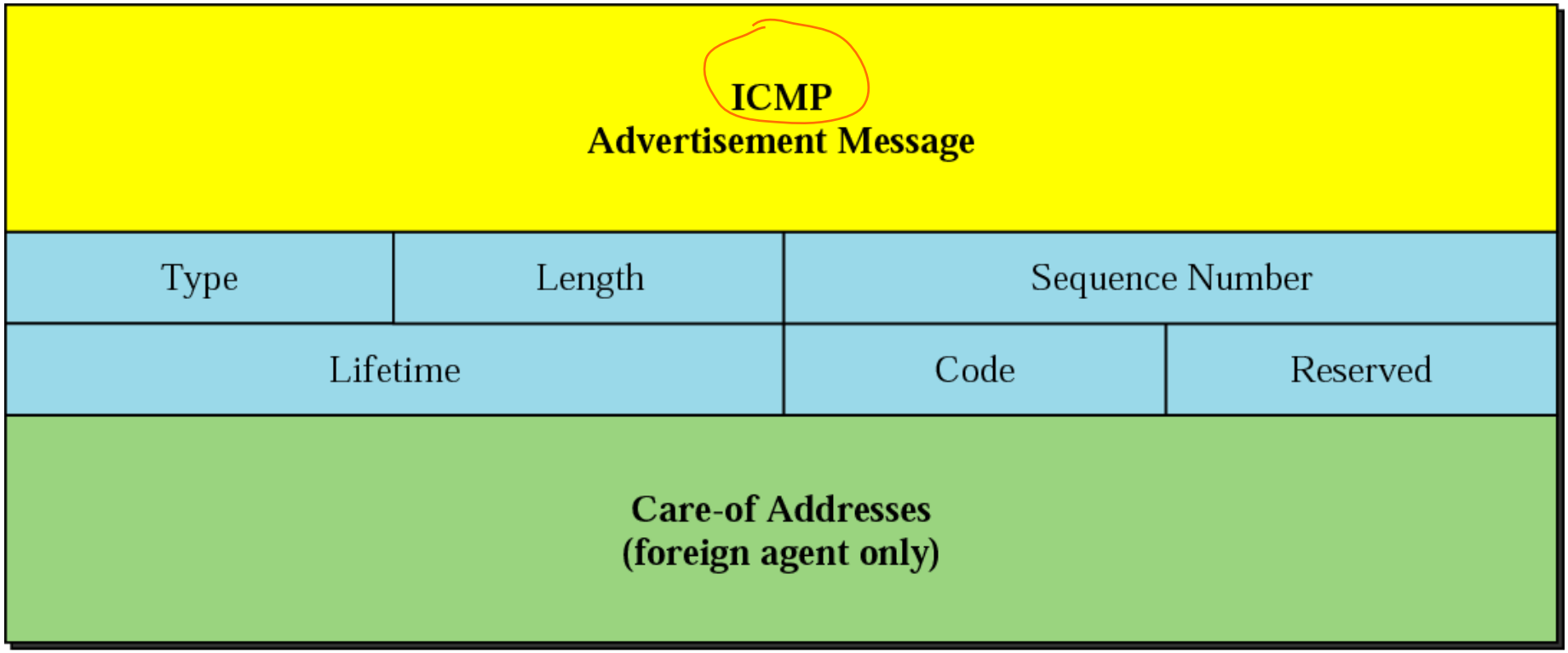
©2020 Mahbub Hassan

Agent discovery

- *This phase is needed if FA is located in router*
  - *Skip this phase if FA is colocated in the mobile*
- Mobile waits for periodic advertisement from FA
  - advertisement contains CoAs
- Mobile could solicit for CoA
  - If it didn't want to wait for periodic advertisement

©2020 Mahbub Hassan

Agent advertisement
FA located in router



FA advertises router addresses as CoAs

©2020 Mahbub Hassan

Agent advertisement
Reuse of ICMP

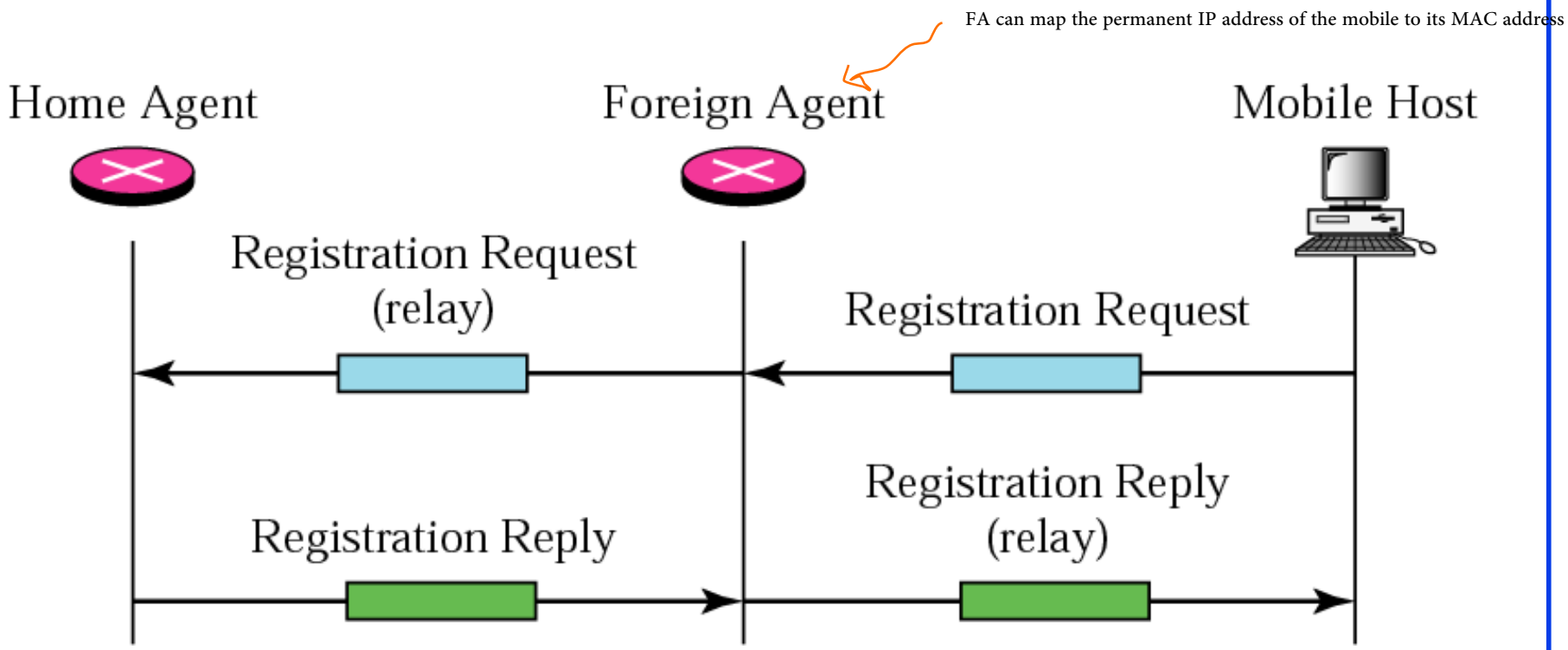
Mobile IP does not use a new packet type for agent advertisement; it uses the router advertisement packet of ICMP, and appends an agent advertisement message.

Mobile IP does not use a new packet type for agent solicitation; it uses the router solicitation packet of ICMP.

©2020 Mahbub Hassan

Registration request and reply

FA is located in a router



mobile talks directly to HA for colocated CoA

©2020 Mahbub Hassan

Registration request format

Type	Flag	Lifetime
Home Address		
Home Agent Address		
Care-of Address		
Identification		
Extensions ...		

©2020 Mahbub Hassan

Registration reply format

Type	Code	Lifetime
Home Address		
Home Agent Address		
Identification		
Extensions ...		

©2020 Mahbub Hassan

Transport protocol for registration

A registration request or reply is sent by UDP using the well-known port 434.

©2020 Mahbub Hassan

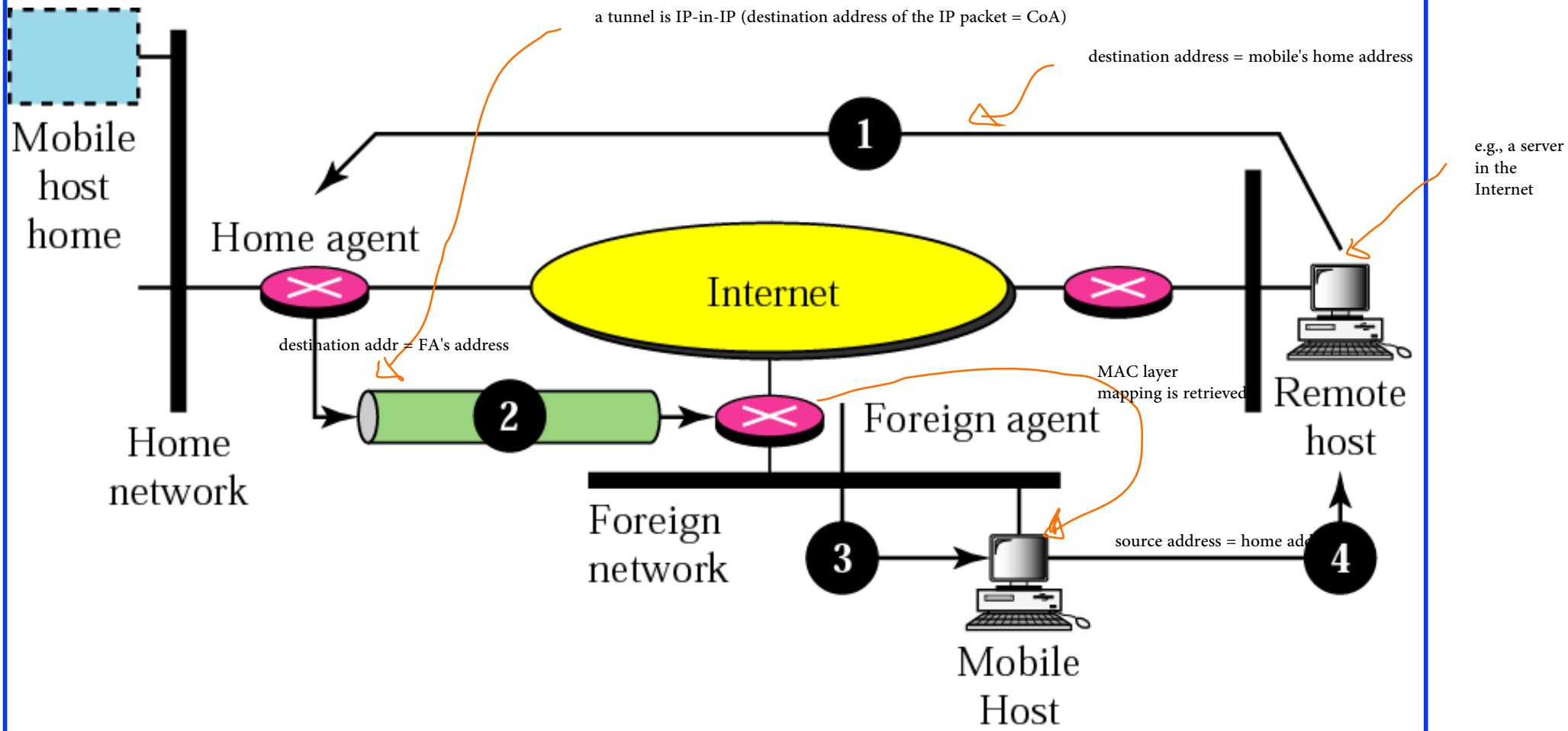
CN-MN Data Exchange

CoA is not co-located

- Step1: CN sends a packet to MN using home address
  - mobility remains transparent to CN
- Step2: HA intercepts it, encapsulates it in another packet with destination address as CoA and retransmits it (tunneling to FA)
- Step3: FA decapsulates, looks up MAC address of MN in registry, and sends the packet in LAN frame to MN
- Step4: MN sends packets directly to CN with source address as home address
  - mobility remains transparent to CH

©2020 Mahbub Hassan

CH-MH Data transfer (Remote host = CH)



©2020 Mahbub Hassan

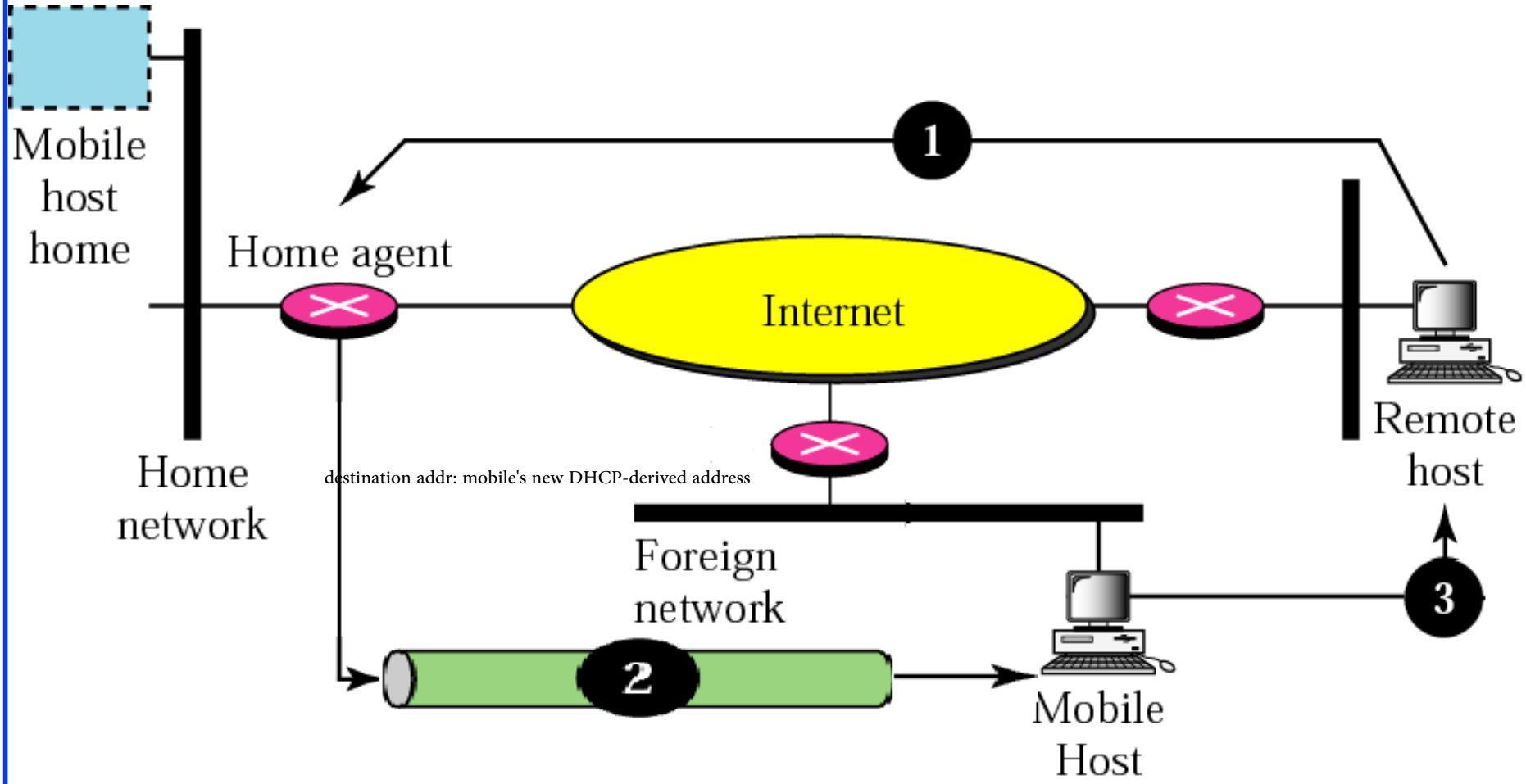
CH-MH Data Exchange

CoA is co-located

- Step1: CH sends packet to MH using home address
  - mobility remains transparent to CH
- Step2: HA intercepts it, encapsulates it in another packet with destination address as CoA and retransmits it (tunneling to MH), MH decapsulates and delivers to upper layers
- Step3: MH sends packets directly to CH with source address as home address
  - mobility remains transparent to CH

©2020 Mahbub Hassan

Data transfer Co-located CoA (Remote host = CH)



©2020 Mahbub Hassan

Headers of a Tunneled Packet

Using IP-in-IP Encapsulation

Inner Header: From CN to MN
Outer Header: From HA → FA/CoA

Outer IP Header	Inner IP Header	Transport Layer Header	User Data (if any)
Src Addr = HA Dest Addr =CoA Proto = IP	Src Addr = CN Dest Addr = MN Proto = TCP/UDP		

©2020 Mahbub Hassan

IP handoff

- Registration may take 'long' time
- Registration delay can cause problems
  - packets may got lost during IP handoff
- Solution A: previous FA buffer data and forward to new FA
  - works for data services, but not for voice
- Solution B: predict mobility and complete registration before moving to new subnet
  - Requires overlapping wireless coverage
  - Handoff delay reduced (good for voice)

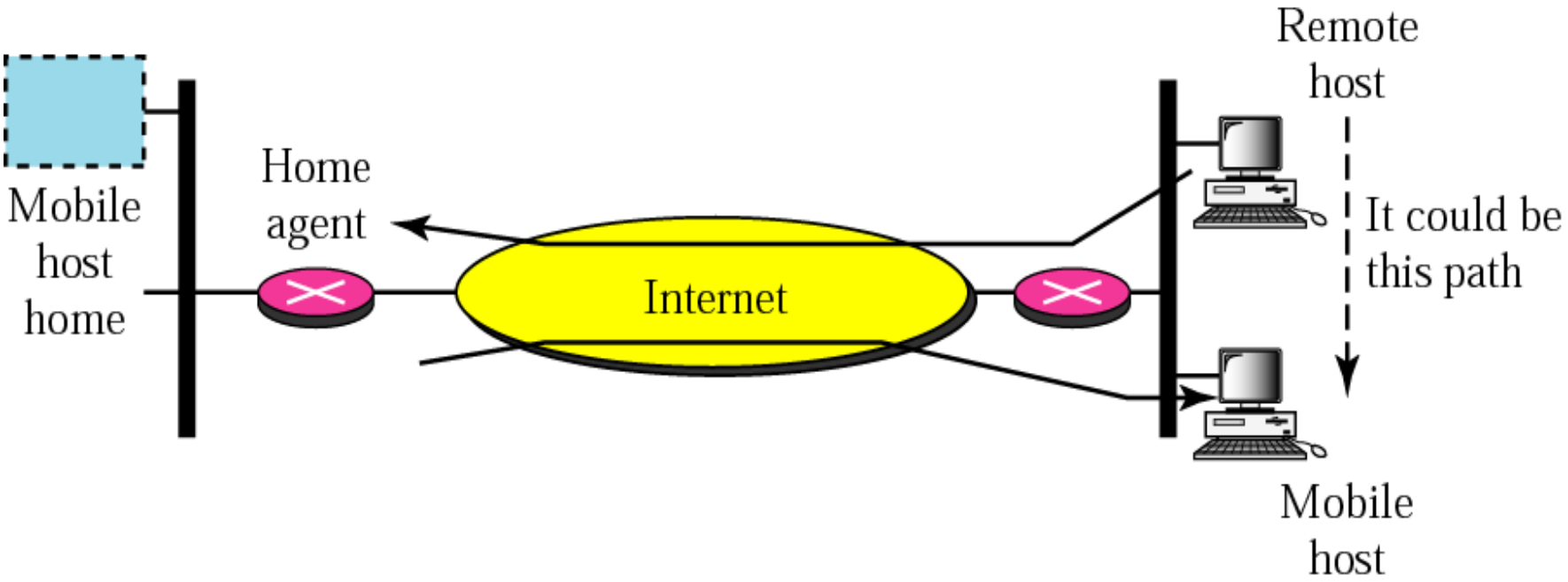
©2020 Mahbub Hassan

Latency problem

- Mobile IP stretches communication routes
  - more hops increases packet transit time
  - Not good for voice over IP
- Route stretch
  - Double crossing
  - Triangular routing

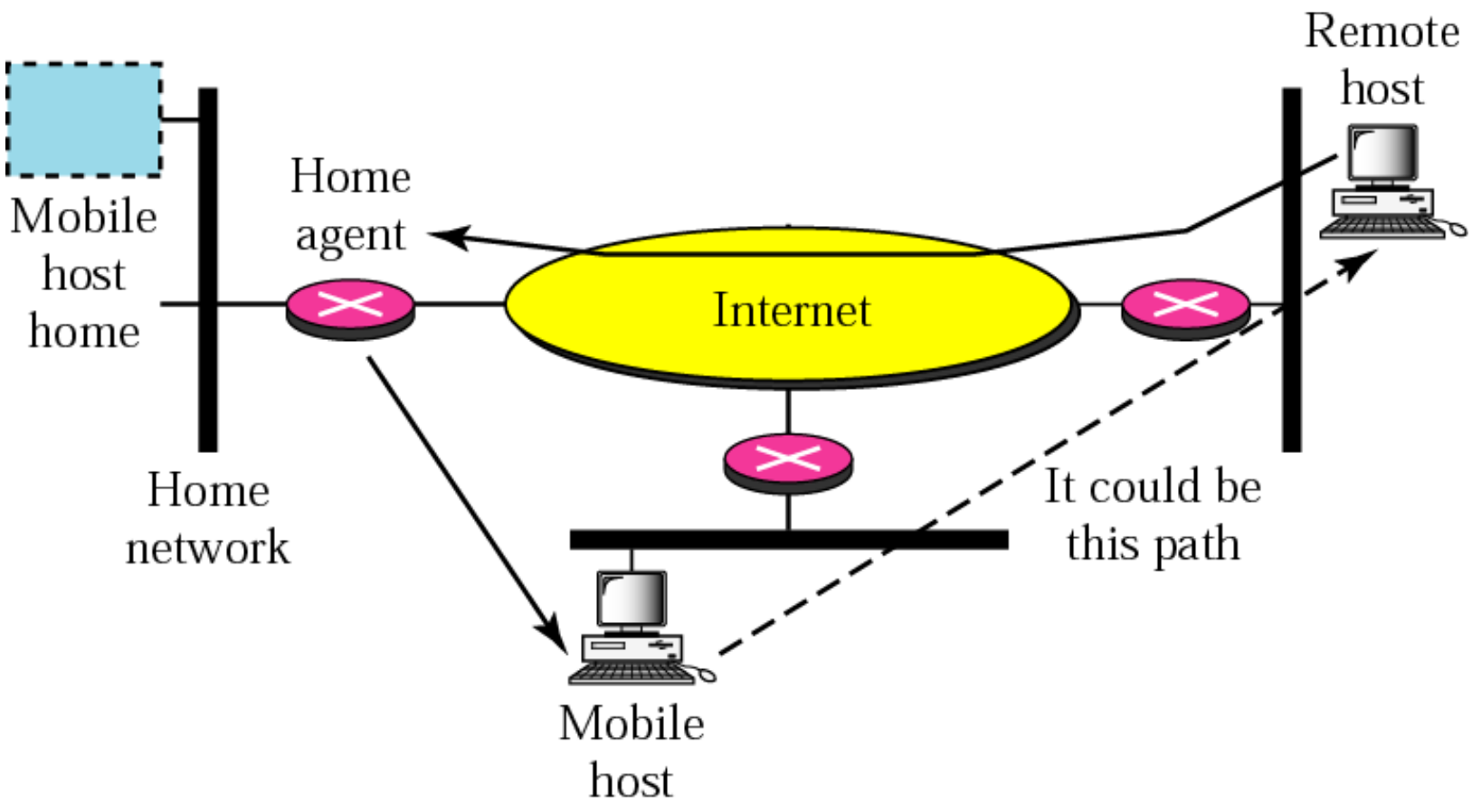
©2020 Mahbub Hassan

Double crossing



©2020 Mahbub Hassan

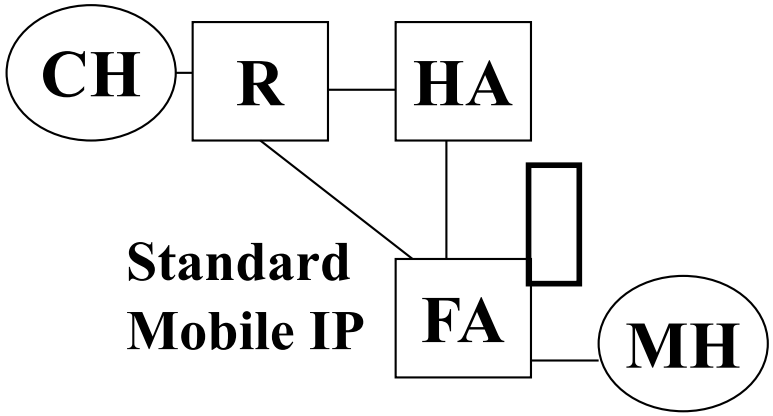
Triangular routing

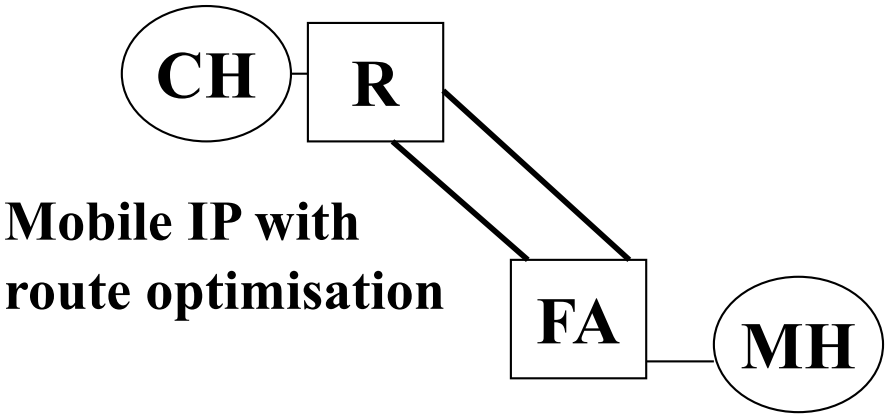


©2020 Mahbub Hassan

Route optimisation
Principle

- CH directly tunnels to CoA
  - bypassing HA
- Triangular routing avoided





©2020 Mahbub Hassan

Route Optimisation

How does CH know CoA?

- Initially it does not know
- It sends packets to HA
- HA tunnels to FA, *but also sends CoA to CH*
- CH sends all subsequent packets directly to CoA (route optimisation)

©2020 Mahbub Hassan

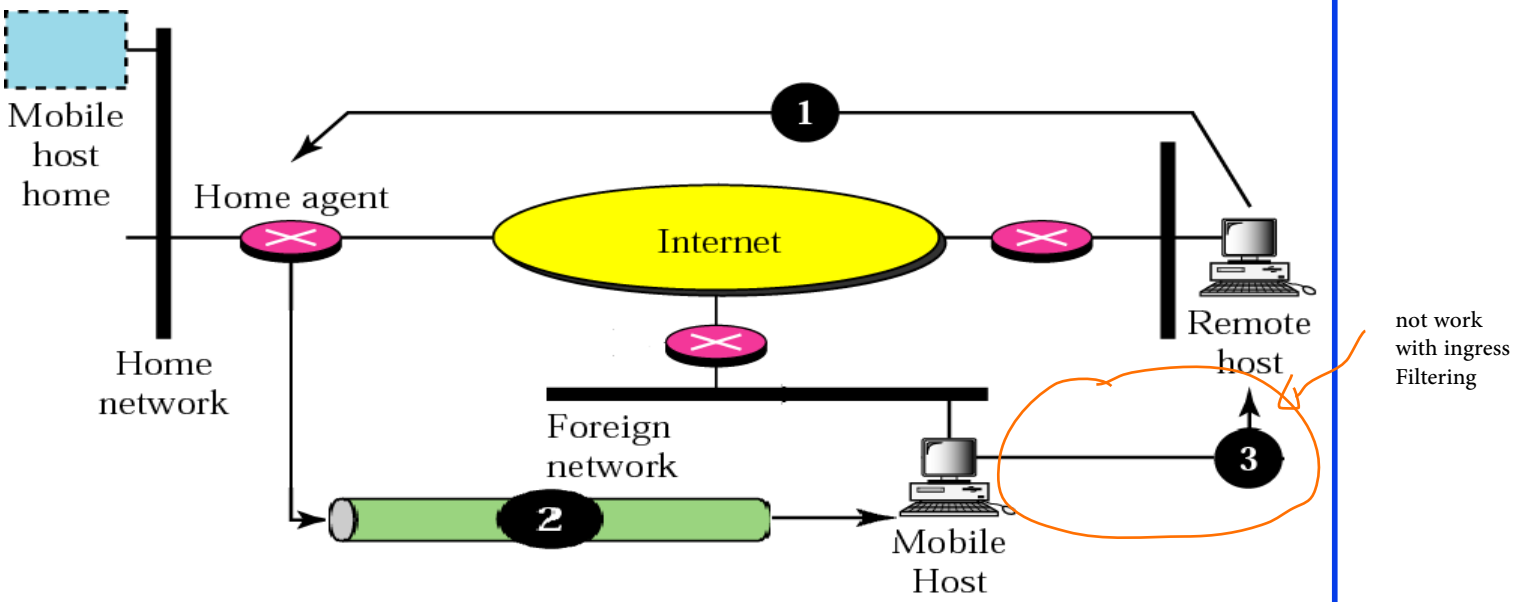
Route Optimisation
problems

- CH learns the CoA
  - mobility is *not* transparent (privacy issue)
- Existing IP software at CH will not work
  - needs to be mobile IP capable
- Stored CoA may be invalid

©2020 Mahbub Hassan

Reverse tunneling (1)

- Original version of MIPv4 allows MH to send replies directly to CH
  - MH always uses Home Address as the source address



©2020 Mahbub Hassan

Reverse tunneling (2)

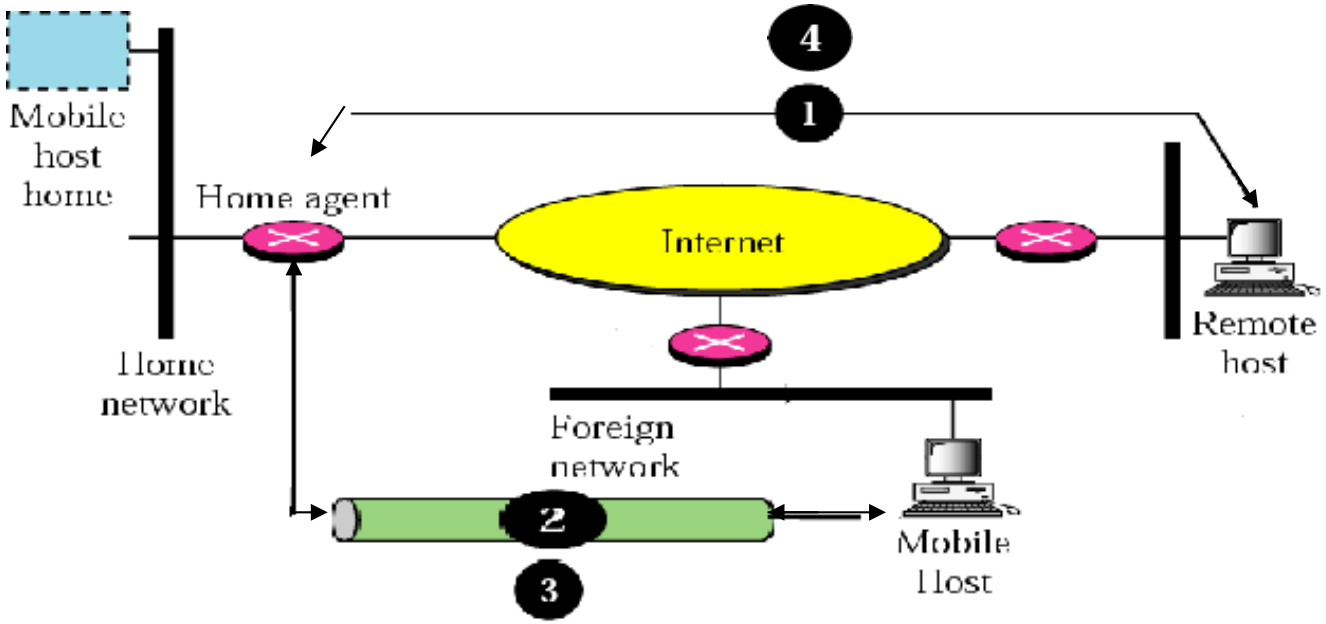
- To overcome Denial of Service(DoS) attacks, Internet routers began filtering packets passing through them.
  - Routers would allow a packet to pass through it only if the source address matched the origin of the packet
  - Called Ingress filtering
- Reverse tunneling was introduced to enable MIP to work with ingress filtering mechanism.

©2020 Mahbub Hassan

Reverse tunneling (3)

(Remote host = CH)

- MH-CH data exchange also takes place through a reverse tunnel between the MH/FA and HA
- Double Triangular routing ?

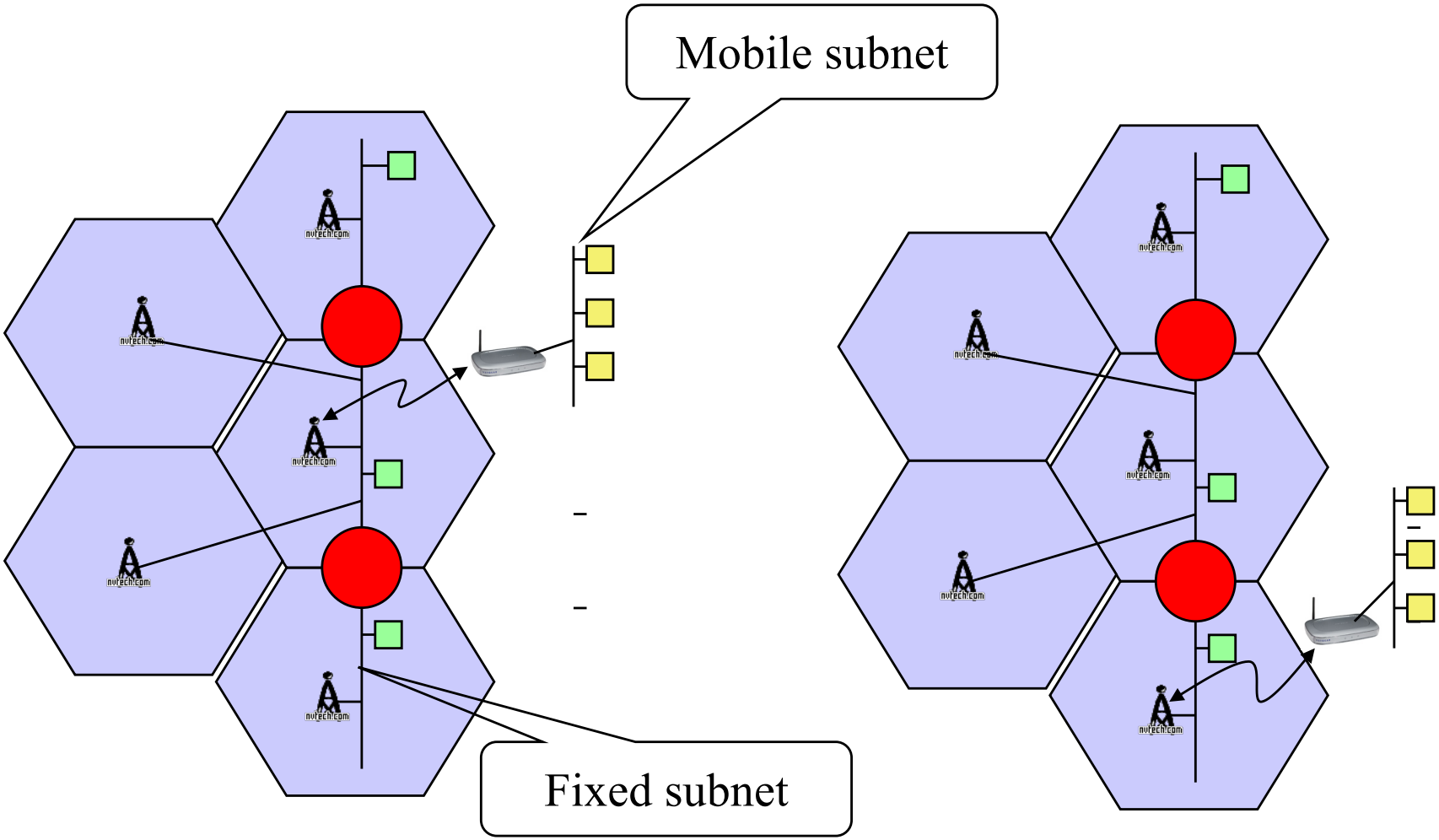


©2020 Mahbub Hassan

Network Mobility

©2020 Mahbub Hassan

What is network mobility?



Consider a *stub* subnet

Mobile subnet has moved

©2020 Mahbub Hassan

Motivation for supporting network mobility

- Commuters in trains and buses may wish to connect their devices to an onboard LAN
  - similar to connecting to the LAN at work
- If the onboard LAN could remain connected to the Internet, mobility could be hidden from the commuters
  - no *individual* mobility management
  - battery power saving by not connecting to a distant outdoor radio tower (low power)

©2020 Mahbub Hassan

Implications

- The onboard IP subnet will change its point of attachment to the Internet
- Reachability and session continuity must be preserved despite these changes
- IETF has set up a working group to standardise protocols that can support *subnet mobility* in the TCP/IP infrastructure

©2020 Mahbub Hassan

Solutions

- Let us study a standard from IETF called NEMO
- NEMO is based on MIP
- IN NEMO, there is an *onboard central entity* that manages the mobility of the onboard IP subnet
  - onboard user devices require no action when the subnet changes point of attachment
  - movement of the subnet remains transparent to the onboard devices

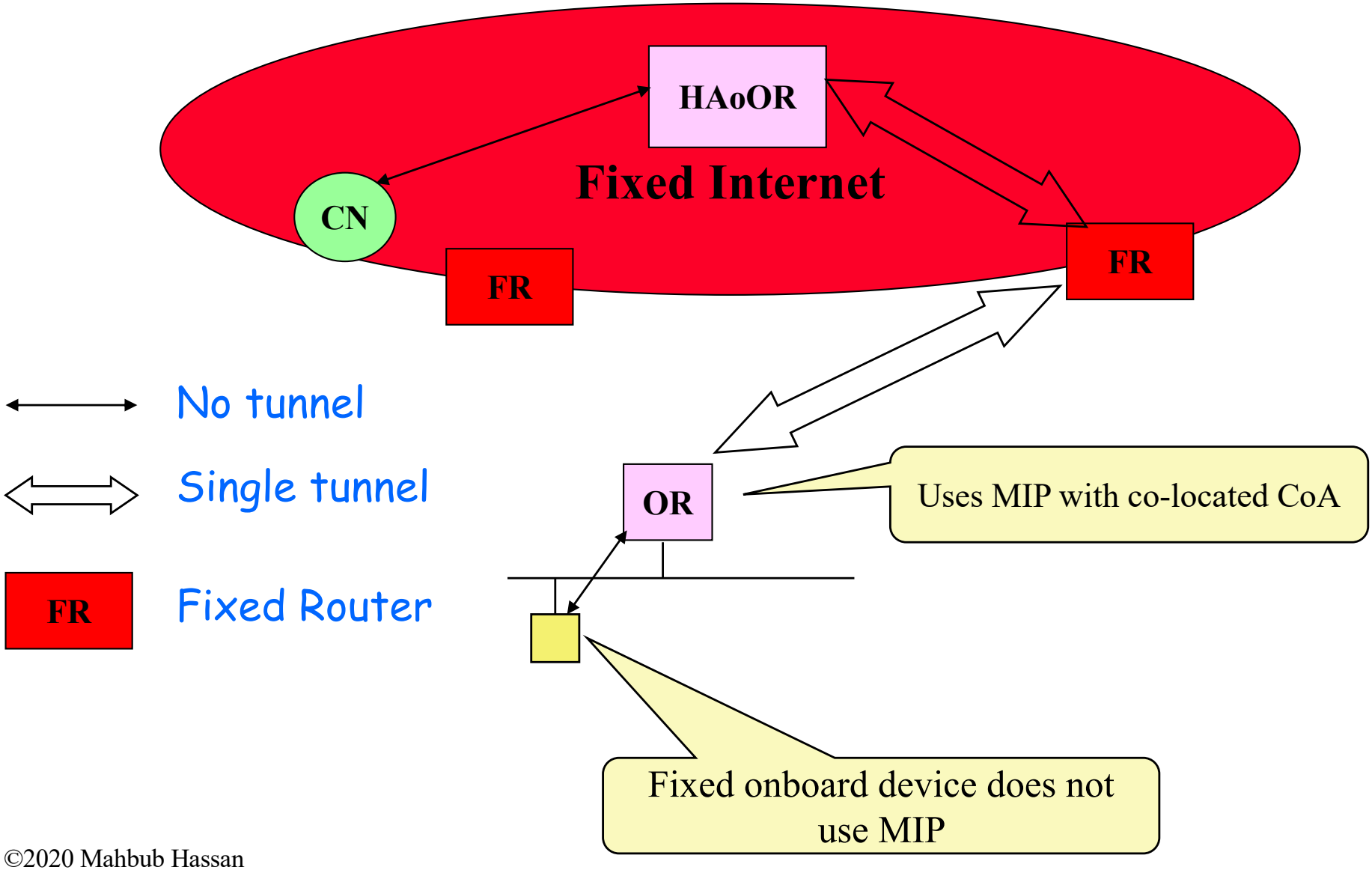
©2020 Mahbub Hassan

NEMO overview

- RFC3963 released in 2005
- Onboard router (OR) uses MIP to manage the mobility of the moving subnet
- Bidirectional tunnel between OR and router home agent (RHA)
- If onboard mobile device uses MIP as well, we have a *recursive* MIP
  - fixed onboard devices may not need to use MIP
  - onboard user devices may need to use MIP

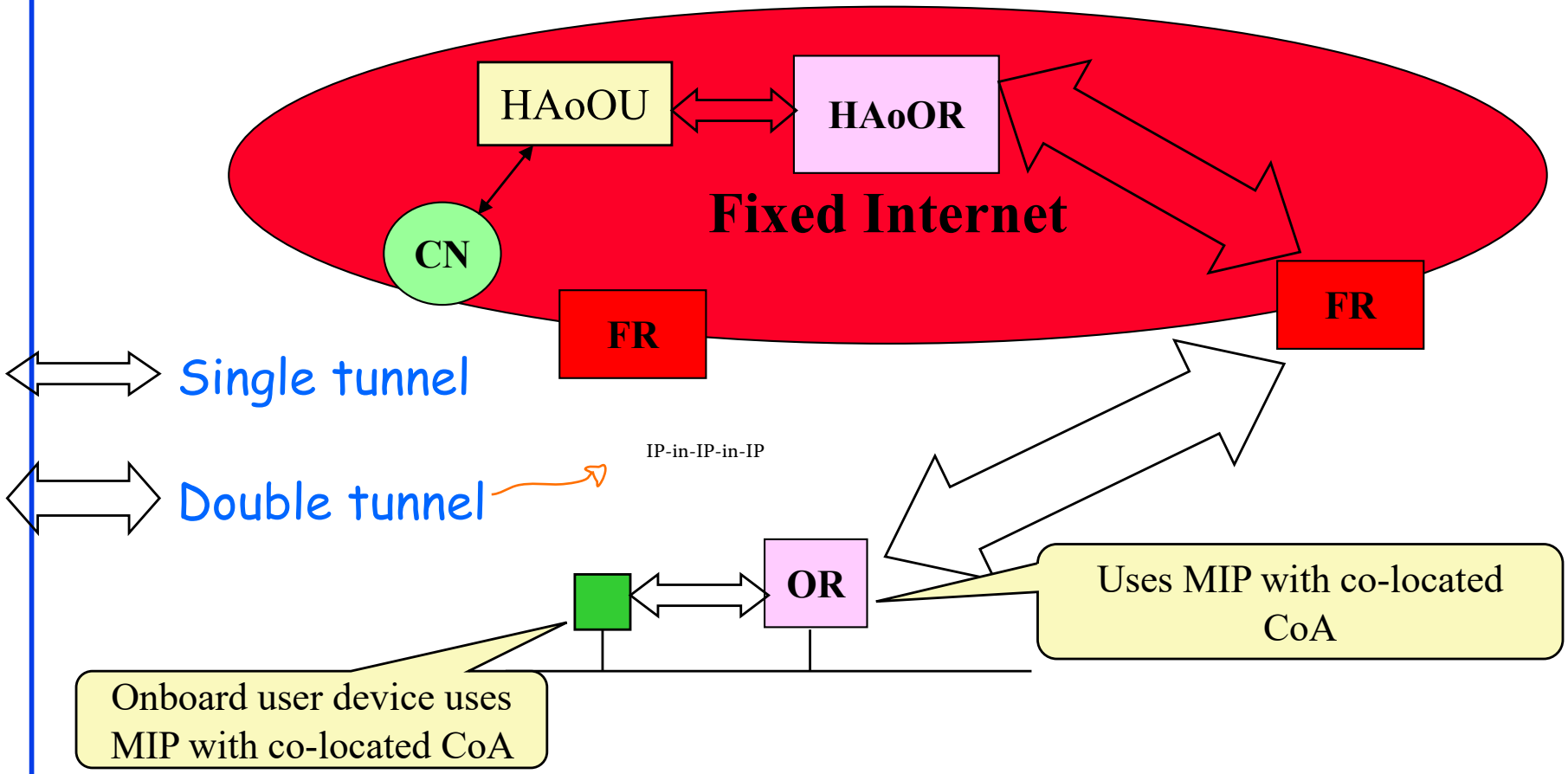
©2020 Mahbub Hassan

NEMO
Communication with fixed onboard device



©2020 Mahbub Hassan

NEMO
Communication with onboard user device



HAoOU: HA of onboard user device

©2020 Mahbub Hassan

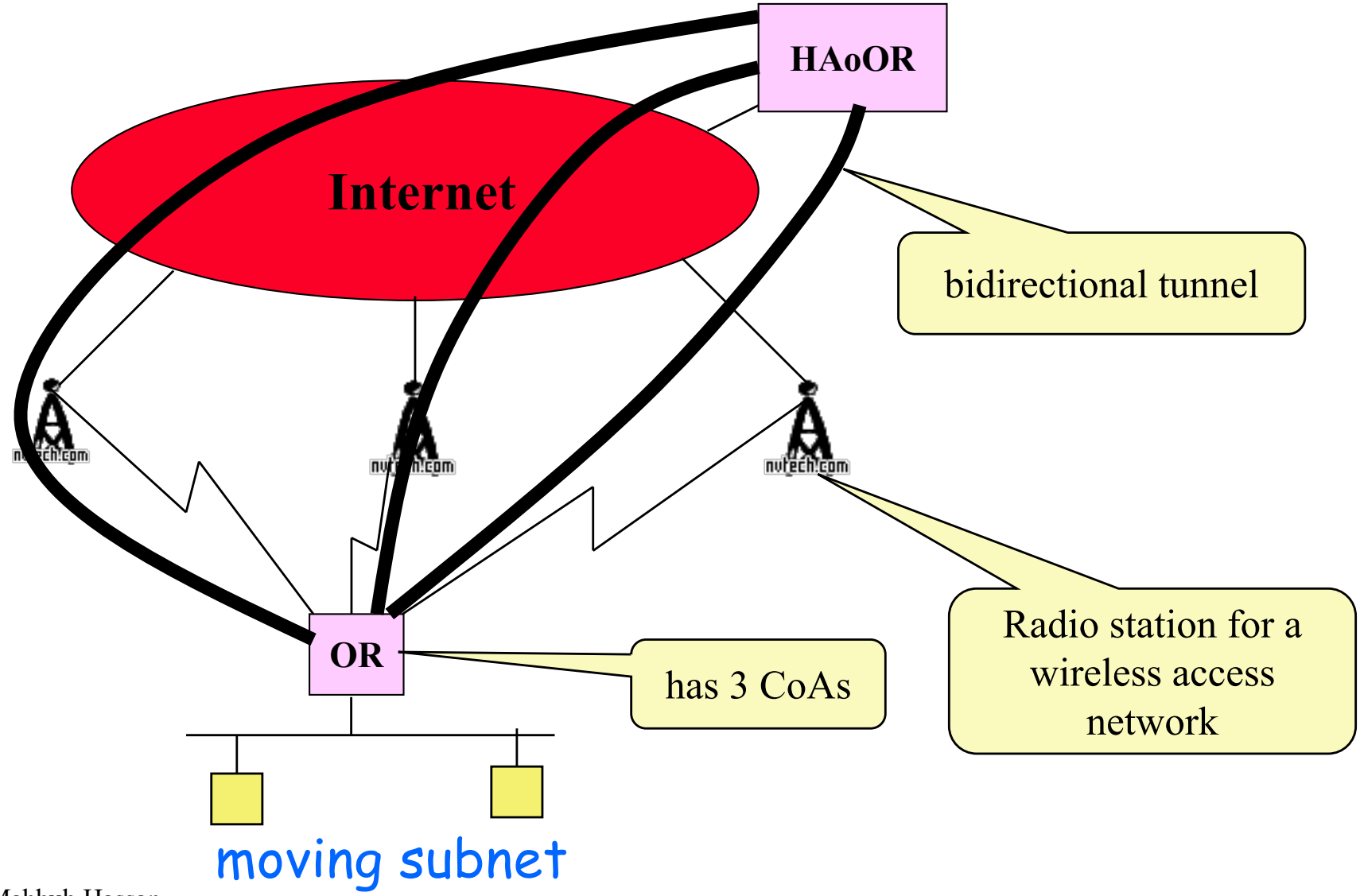
Multihoming with NEMO

- (RFC4980, Oct 2007)
- Connect the mobile subnet to the Internet via multiple wireless access networks
  - Example of wireless access networks: cellular networks, WiFi, etc.
- All wireless interfaces can be used simultaneously
  - Registering multiple CoA with the HA is allowed
- Improves reliability and robustness of the Internet connectivity

©2020 Mahbub Hassan

Multihoming with MIP-NEMO

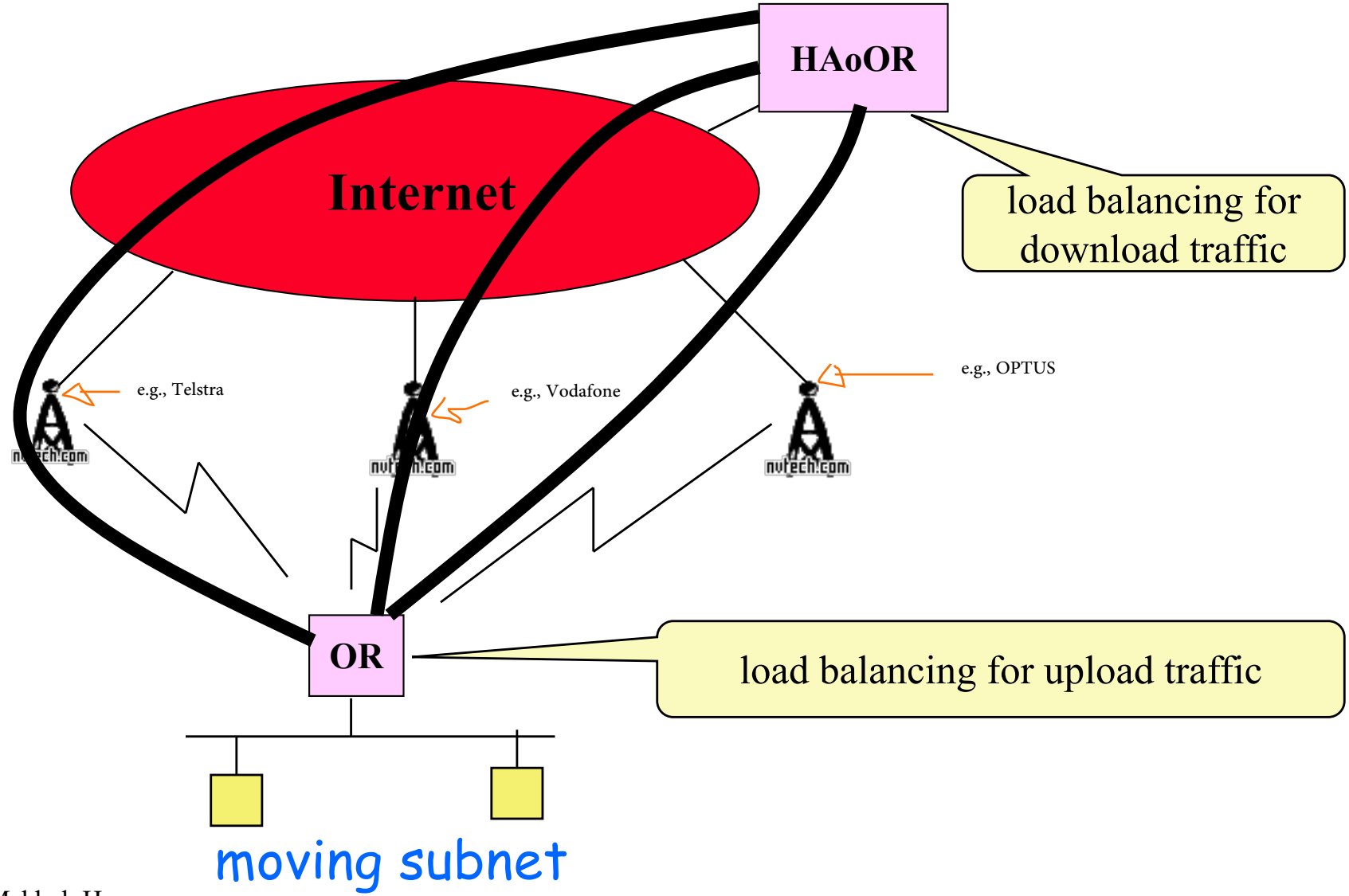
graphical illustration



©2020 Mahbub Hassan

Multihoming with MIP-NEMO

load balancing



©2020 Mahbub Hassan

Mobile IPv6 (RFC 3775)

- IPv6 simplifies MIP
- CoA can be achieved through address auto-configuration mechanism of IPv6
  - No need for DHCP
  - There is no need for FA, mobile hosts can operate without any special support
- MIPv6 tries to avoid tunneling as much as possible

©2020 Mahbub Hassan

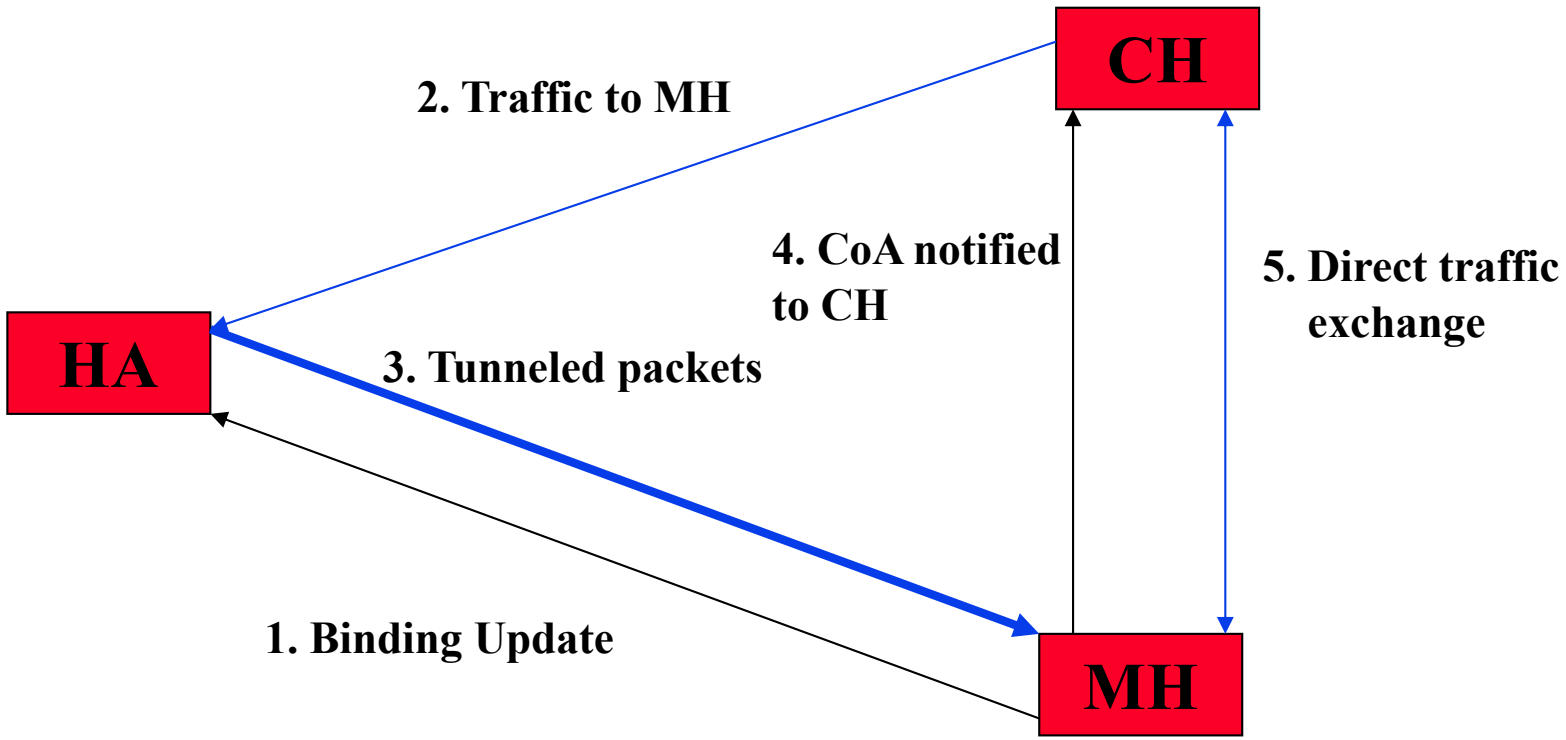
implementing Mobile IP in the IPv6 platform is more efficient than it is on the existing IPv4 platforms

Mobile IPv6

- Supports two different modes of operation
- Bidirectional tunneling mode
  - Same as IPv4 with reverse tunneling
  - No support from CH
- Route optimisation mode
  - Binding updates are sent to CHs from MHs
  - From CH→MH, new type of IPv6 routing header(Type 2) is used instead of IP-in-IP encapsulation
  - From MH→CH, new Home address option carries the Home address of MH
  - Each packet now contain both CoA and Home address, ingress filtering routers are now satisfied

©2020 Mahbub Hassan

Mobile IPv6
illustration



©2020 Mahbub Hassan

Proxy Mobile IP

©2020 Mahbub Hassan

Disadvantages of Mobile IP

- User device requires software upgrade
  - Cost
  - Admin overhead (MIP requires kernel support)
  - Population of mobile device may be dynamic (for a large organisation, it may be difficult to keep track which devices need MIP)
  - Security hole: MIP is in the kernel, opening new threats for security for the organisation

©2020 Mahbub Hassan

Key features of PMIP

- Seamless mobility across IP subnets within a *local area (campus)*
- No client software needed (totally transparent to the mobile devices)
- Network edge (access point) installs MIP client-proxy to relieve the client
- Support from both Internet and 3GPP:
  - IETF RFC5213 2008 "Proxy Mobile IPv6"
  - Adopted in 3GPP (3G/4G/5G) architectures, such as LTE (mobility management in IP-based mobile core)

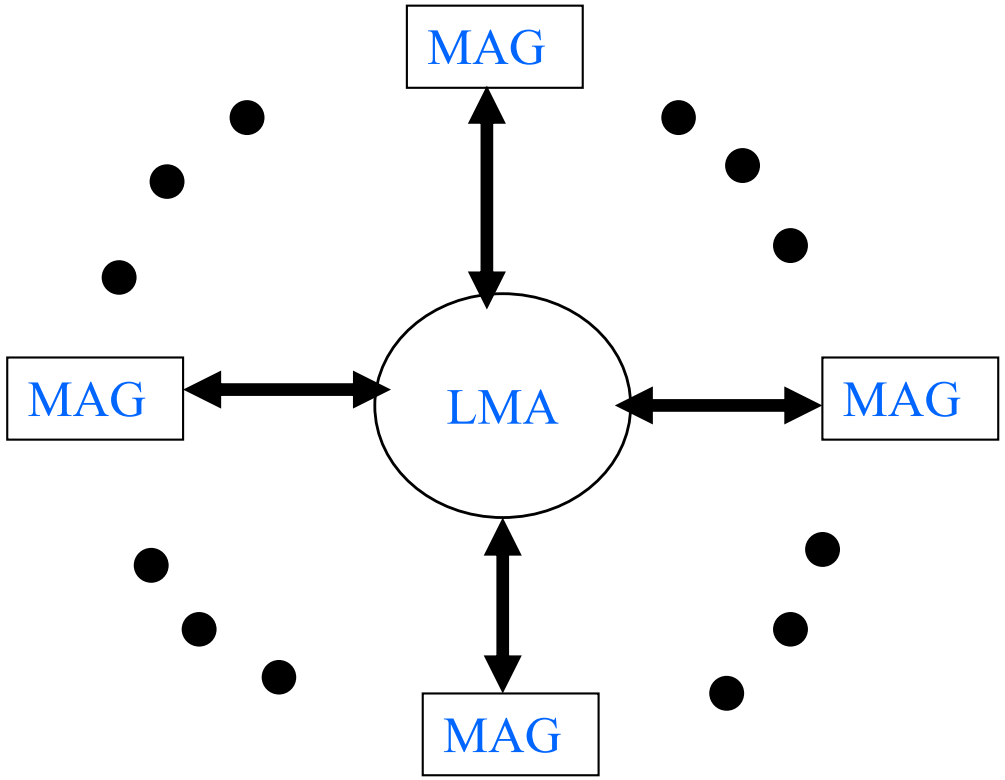
©2020 Mahbub Hassan

PMIP Entities

- LMA (local mobility anchor)
  - Only one LMA per local mobility domain (LMD)
  - LMA usually hosted in a router
  - all traffic to and from CN go via LMA
  - Traffic between two MNs in different MAGs go via LMA
  - Two MNs in the *same* MAG *do not* have to via LMA
- MAG (mobile access gateway)
  - Works as a *MIP client proxy* and does the registration with LMA etc.
  - Many MAGs per LMD
  - APs (wireless routers) must be configured to act as MAGs

©2020 Mahbub Hassan

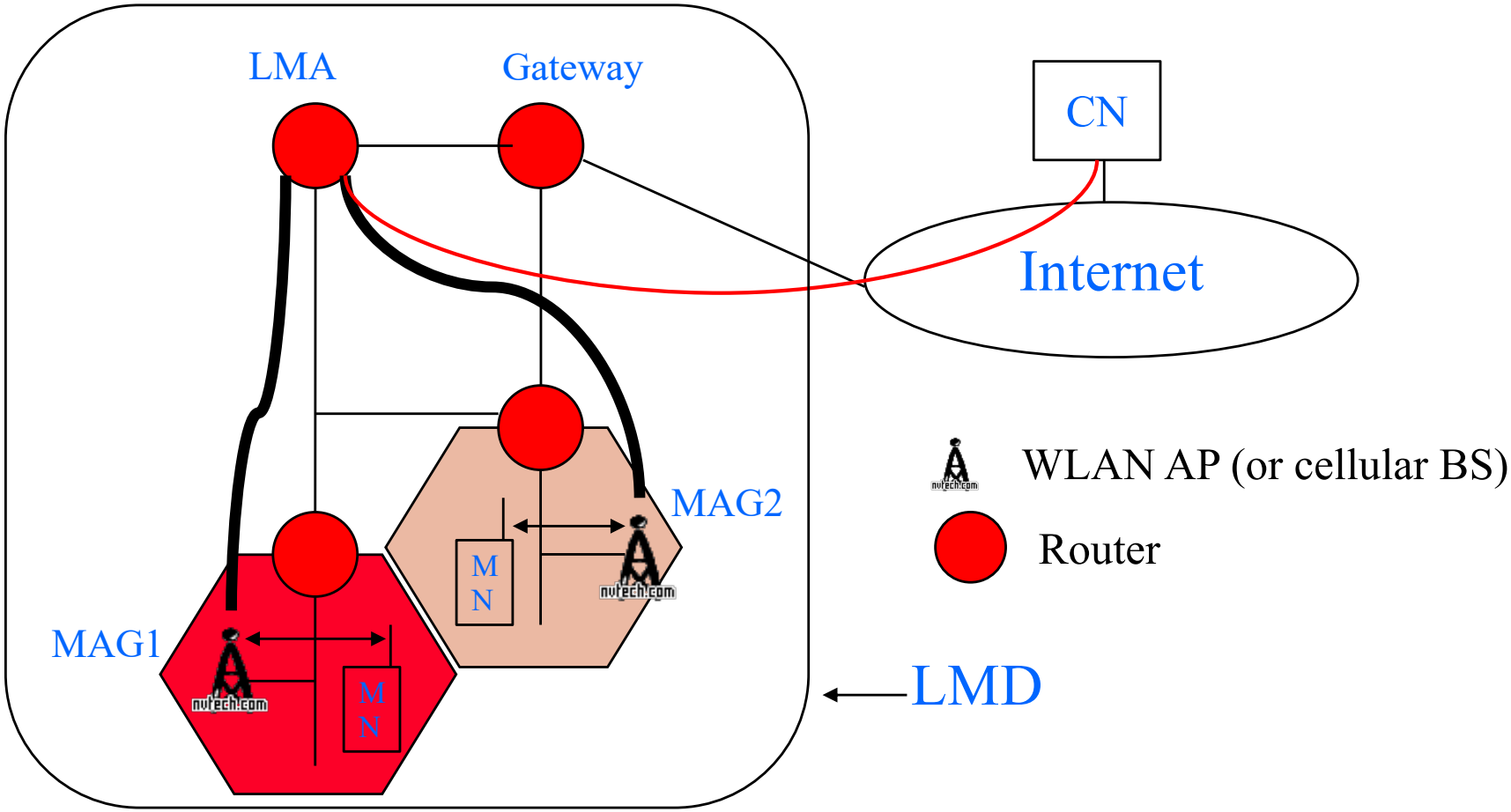
LMA and MAGs



One LMA opens bi-directional tunnels with many MAGs

©2020 Mahbub Hassan

PMIP Topology



©2020 Mahbub Hassan

An example of PMIP operation

1. AP1, connected to subnet1, is configured as MAG1. AP2, connected to subnet2, is configured as MAG2.
2. MN associates with AP1 and obtains an IP address valid for subnet1. MAG1 registers MN's MAC address, IP address, and MAG number with LMA and establishes a bidirectional tunnel between LMA and MAG1. All traffic to and from CN now go via this tunnel.
3. MN moves closer to AP2 and based on signal strength, associates to AP2.
4. After associating with AP2, it starts to send traffic to AP2 with the IP address obtained earlier from subnet1. MAG2 detects that the IP address is from another subnet. MAG2 registers the new MAG (MAG2) for this MN with LMA and establishes a bidirectional tunnel between LMA and MAG2.
5. All traffic to and from CN now follow the new tunnel between LMA and MAG2. The MN is oblivious of the fact that it has moved to a new subnet. Any TCP connections between CN and MN remain intact. The mobility was handled completely by the network without any special actions from the MN.

©2020 Mahbub Hassan

Summary

1. In the beginning, the Internet was designed for fixed devices. This means that existing TCP sessions will break if the devices moves across subnet boundaries.
2. MIP was designed to support device mobility.
3. MIP is a network layer function, which hides mobility from transport and application layer protocols.
4. MIP requires software upgrades for mobile devices.
5. PMIP was designed later to manage mobility without requiring any software for the mobile devices. With PMIP, all existing mobile devices can enjoy the benefits of MIP without requiring any update.

©2020 Mahbub Hassan

Wireless Power Transfer

Wireless Sensing

©2020 Mahbub Hassan

Overview

1. Simultaneous Wireless Information and Power Transfer (SWIPT)
2. Radio Frequency (RF) Sensing

©2020 Mahbub Hassan

The 3 Capabilities of Radio Frequency

- Wireless communication: data/information transfer from a Tx to a Rx
- Wireless power transfer: transfer of power/energy from a Tx to a Rx
- Wireless sensing: remote sensing of humans and other phenomena

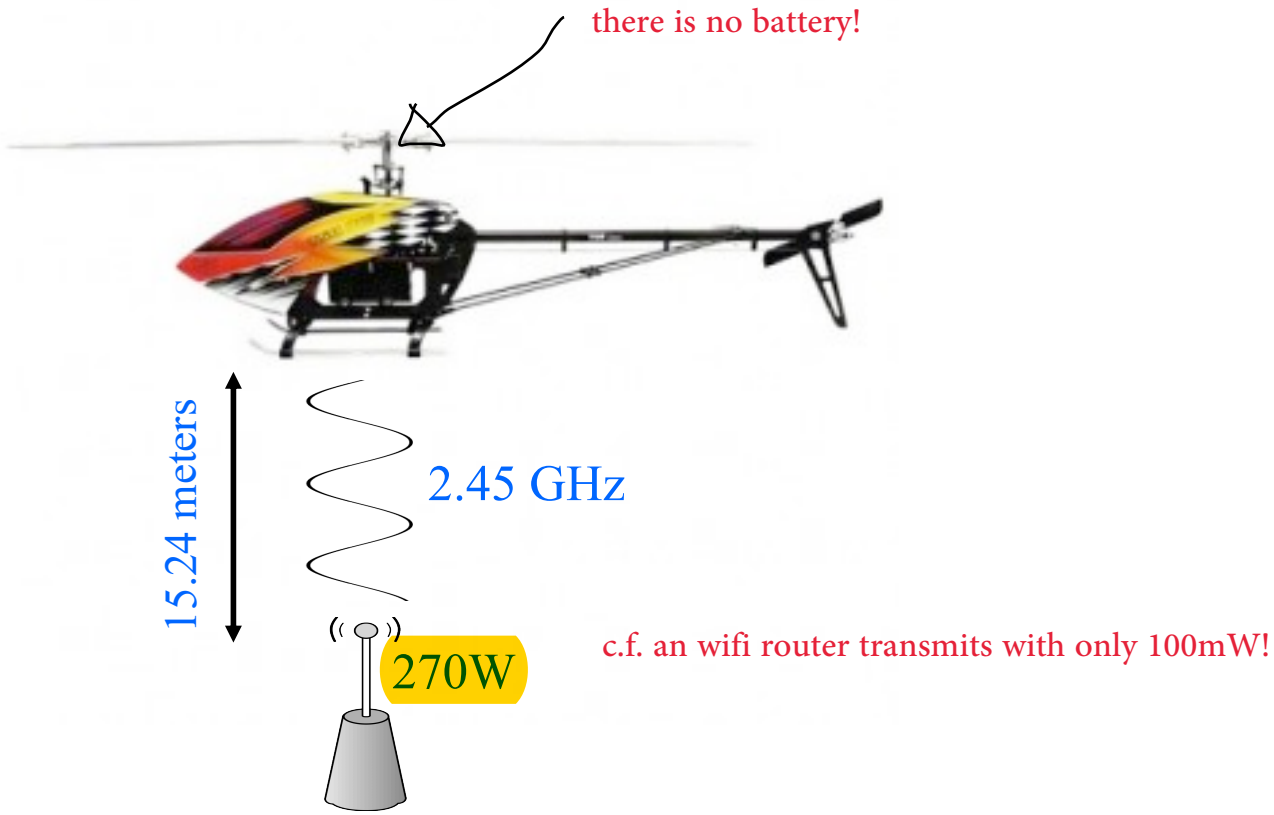
©2020 Mahbub Hassan

Simultaneous Wireless Information and Power Transfer (SWIPT)

©2020 Mahbub Hassan

Flying a Helicopter without a Battery!

A 1960 Experiment!



©2020 Mahbub Hassan

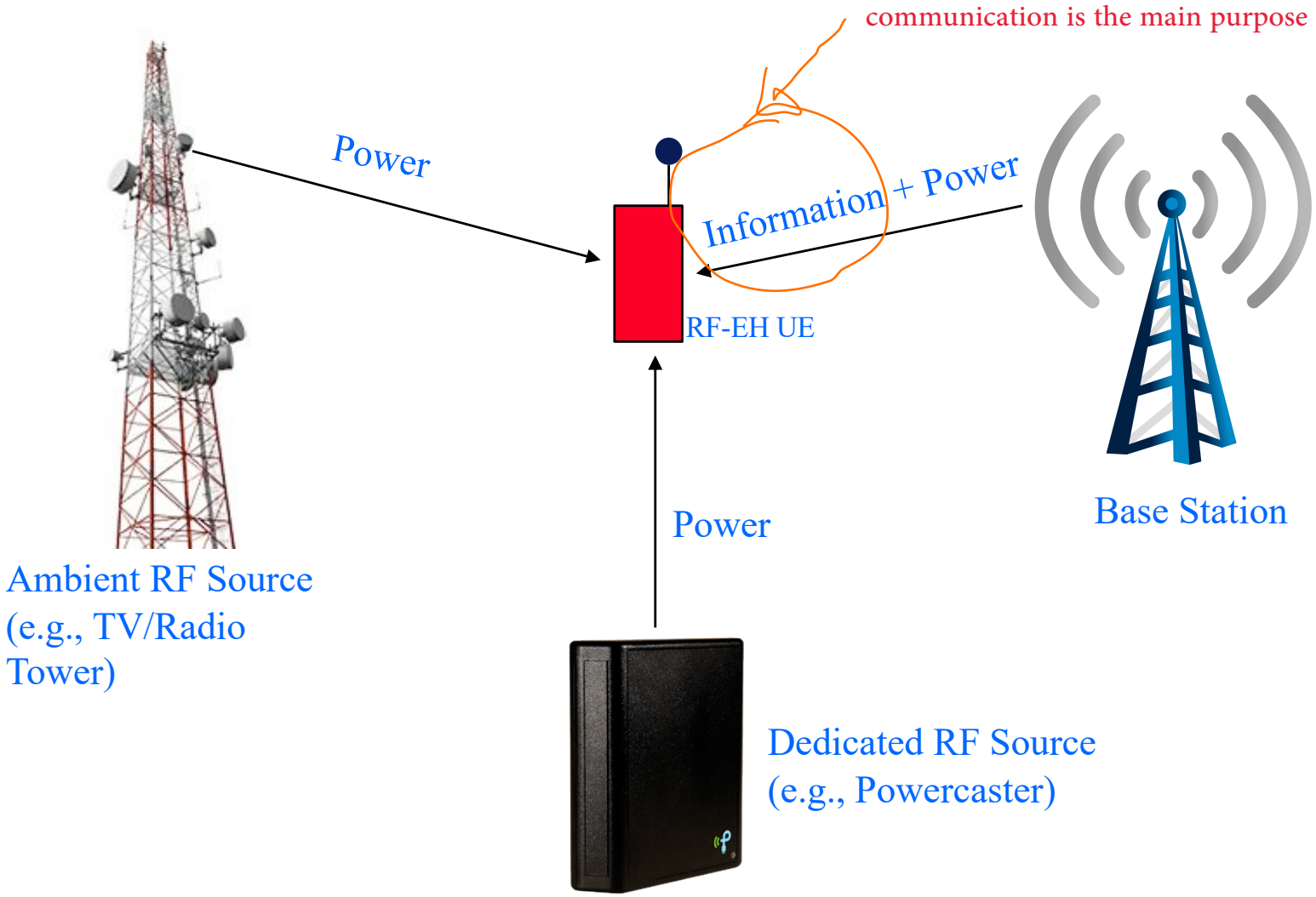
Applications of Wireless Power Transfer and RF Energy Harvesting

- Sensor and IoT networks: recharge/power difficult to reach sensors through RF energy harvesting
- Medical implants: recharge/power electronic circuits in modern implanted medical devices
- Wearable and body area networks: recharge/power body-worn sensors
- Cellular relays: power relays through RF energy harvesting
- UAV/drone: extend flying time of UAVs/drones through remote charging (UAVs can be used as flying relays in cellular networks)

©2020 Mahbub Hassan

RF Energy Sources

RF-EH UE: RF energy harvesting user equipment



©2020 Mahbub Hassan

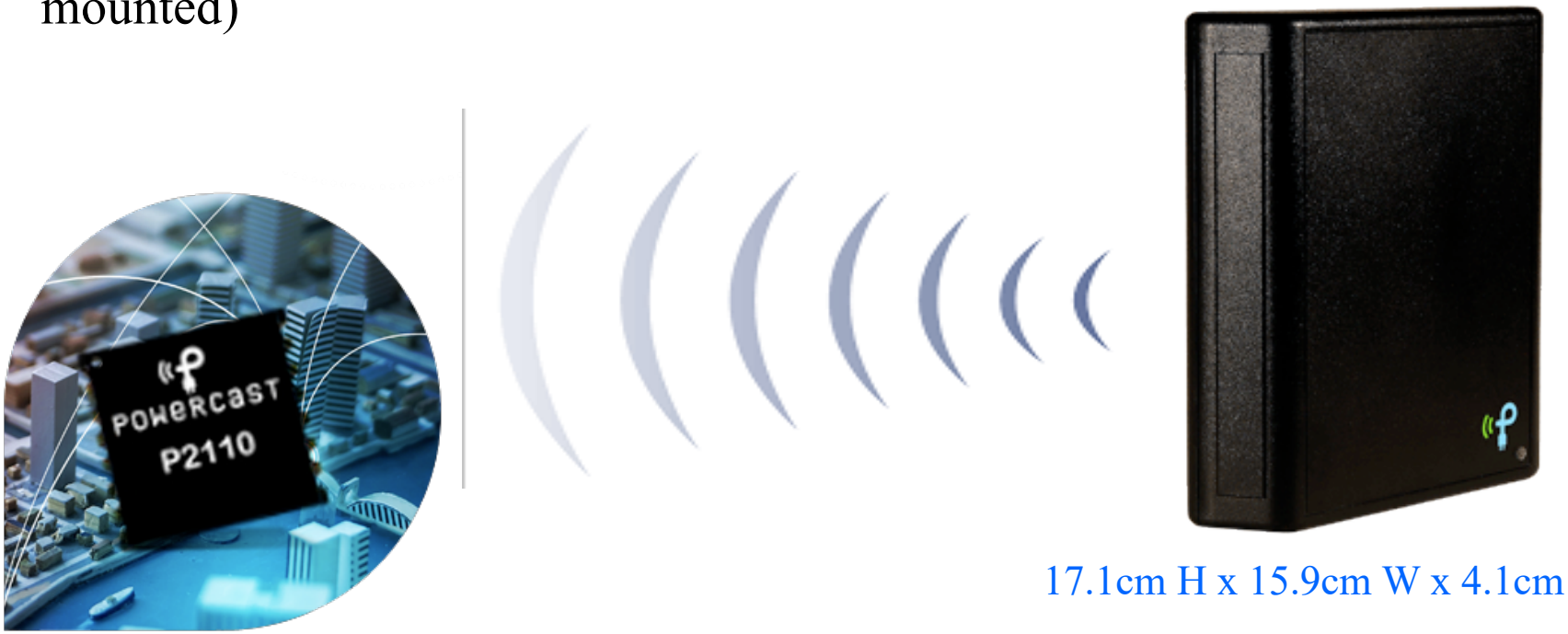
RF energy sources

- Ambient sources
  - e.g. TV/radio/cellular towers
- Dedicated sources
  - Deploy static RF sources (high cost)
  - Mobile RF sources (can move around and provide power where needed; e.g., mobile robot to charge IoT sensors in a factory, flying drone to charge sensors in a large agriculture field, etc.)
  - Hybrid (some static and some mobile)

©2020 Mahbub Hassan

Dedicated sources

- Deploy dedicated infrastructure
- Density and coverage must be planned for the deployment
- Example of commercial products (indoor): *powercaster* (can be wall-mounted)



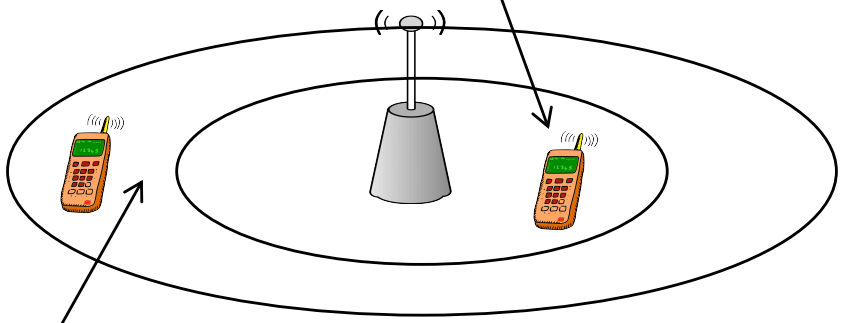
17.1cm H x 15.9cm W x 4.1cm

915 MHz TX91501 powercaster transmitter (3W/1W)
www.powercastco.com

©2020 Mahbub Hassan

Base station as an RF energy source

EH possible in this zone



EH circuits usually have higher sensitivity (e.g., -10 dBm) than conventional information decoders (e.g., -60 dBm)

Information decoding possible in this zone, but not EH

©2020 Mahbub Hassan

In-band vs. Out-of-band RF Energy Harvesting

e.g., 900MHz for power transfer and 2.4GHz for communication

- Out-of-band: energy harvesting uses different frequencies than those used for communication; must use separate antennas for energy harvesting and communications (the antenna is tuned to the frequencies used for either energy harvesting or communication)

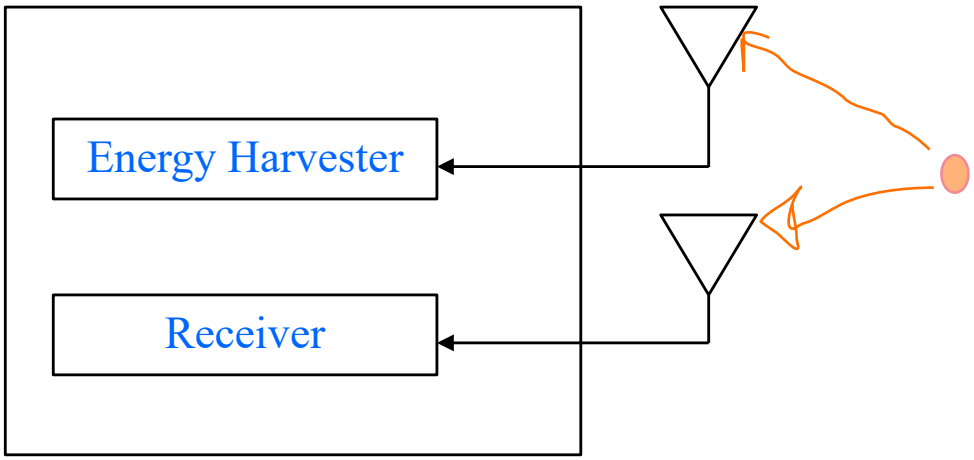
e.g., use 2.4GHz for both power transfer and comms

- In-band: the same RF signals used for both communication and energy harvesting; unfortunately, if signal is processed for communication (decoding), it *cannot* be used for energy harvesting
- Three choices for in-band energy harvesting
  - Separate antennas (similar to out-of-band; independent antennas for communication and energy harvesting)
  - Single antenna with time switching (use the signal for either communication or EH, one at a time)
  - Single antenna with power splitting (use the same signal for both communication and energy harvesting in parallel, but by splitting the signal power)

©2020 Mahbub Hassan

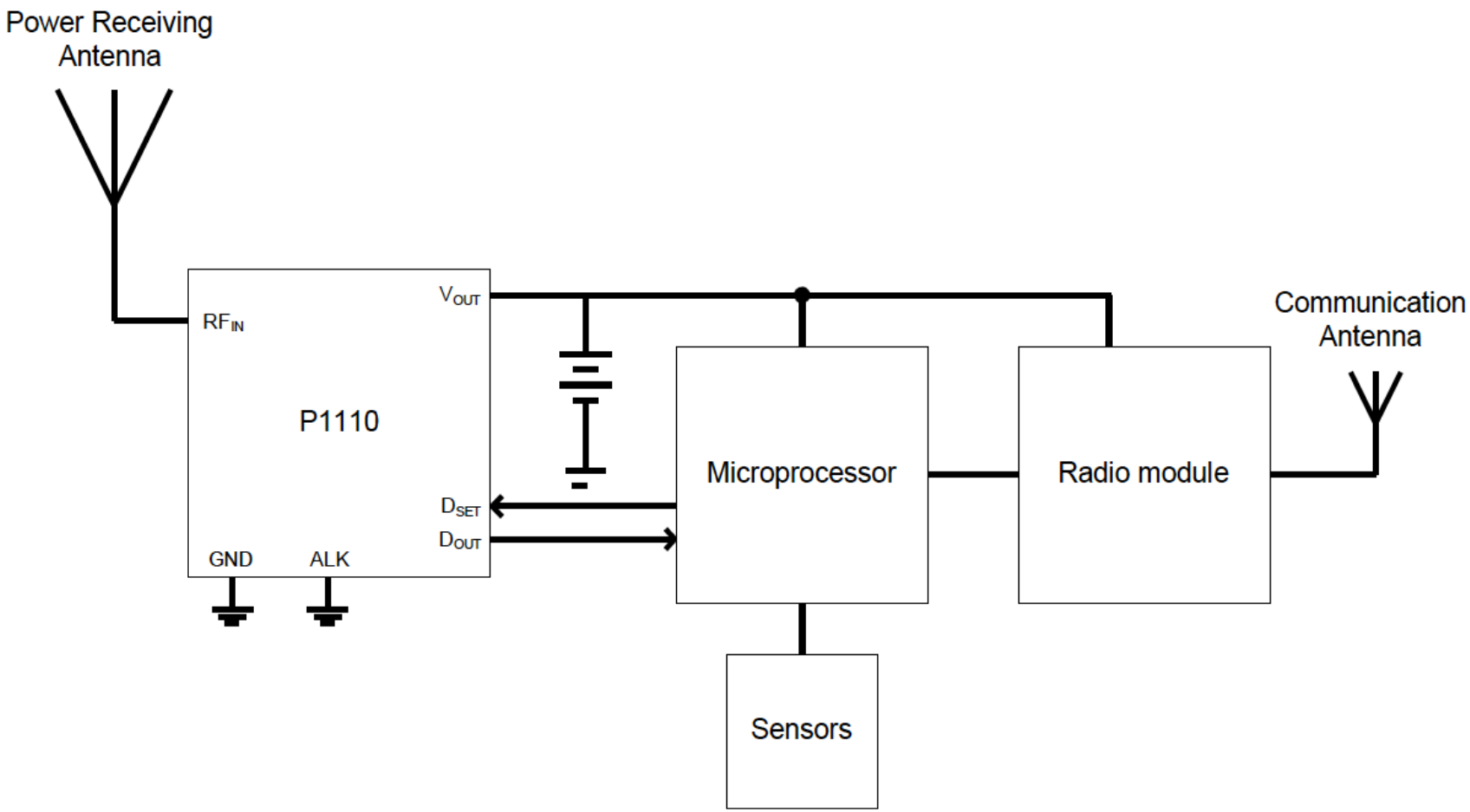
Energy harvesting with separate antennas

- Larger form factor and higher cost, but
- Cleaner separation of signals
  - Entire signal power available for energy harvesting ($P_H = P_R \times \eta$; η is RF-DC conversion efficiency)
  - No additional noise for information processing ($C=W\log(1+P_R/P_N)$; P_N is thermal/antenna noise)



©2020 Mahbub Hassan

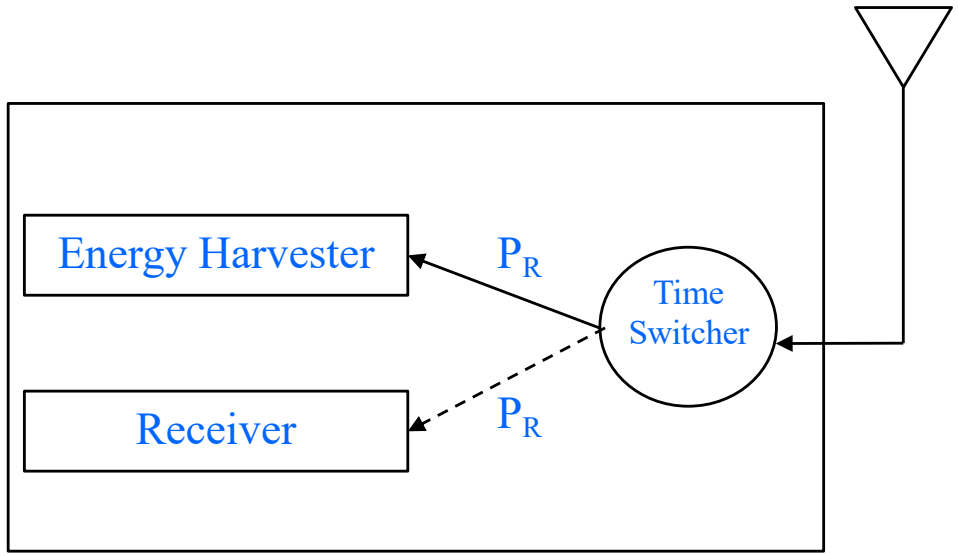
Commercial example of in-band RF energy harvesting with separate antennas [from powercastco.com]



©2020 Mahbub Hassan

Energy harvesting with a single antenna: *time switching*

- Loss of opportunity (time slots) for both energy harvesting and communication, but
- Cleaner separation (in time) of signals
  - Entire signal power available for energy harvesting [$P_H = P_R \times \eta$]
  - No additional noise for information processing [$C=W\log(1+P_R/P_N)$]



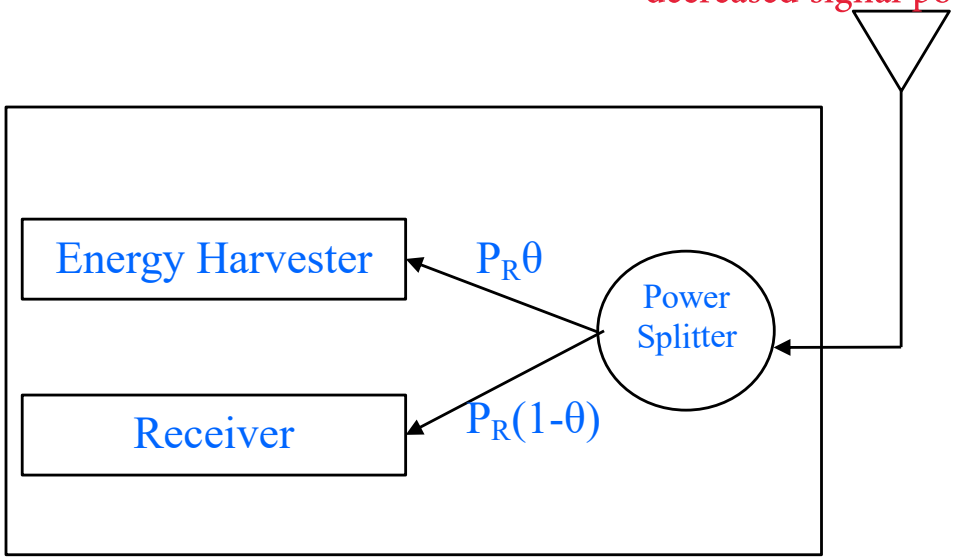
©2020 Mahbub Hassan

Energy harvesting with a single antenna: *power splitting*

- No opportunity (time slot) loss, but
- Power is split, which reduces harvested energy [$P_H = P_R \times \theta \times \eta$; θ is fraction of received signal used for energy harvesting]
- Signal sharing introduces signal processing noise, which further reduces communication capacity [$C=W\log(1+P_R(1-\theta)/(P_N+P_{SP})$; P_{SP} is the power of signal processing noise]

increased noise

decreased signal power



©2020 Mahbub Hassan

From power to energy

- Harvested RF energy (E_H) is a product of two variables
  - Harvested RF power at the receiver (P_H)
  - Time duration, T, for which the P_H is being harvested
  - $E_H = P_H \times T$
- P_H may vary over time (e.g., the mobile device is at different distances from the power transmitter at different times)
  - $E_H = P_{H1} \times T_1 + P_{H2} \times T_2 + \ldots$

©2020 Mahbub Hassan

RF harvested power at the receiver

- Harvestable power at receiver (P_H) = received power (P_R) x RF-DC conversion efficiency (η)
- $P_H = P_R \times \eta = RSS \times \eta$ (RSS is reported by most devices)
- Example: we can harvest only 500pW for a RSS of -60dBm for a 50% RF-DC conversion efficiency
- Received power (P_R) depends on RF propagation model

1 nW

©2020 Mahbub Hassan

Can WiFi AP become an ambient source?

- AP transmit power = 1 mW
- AP transmission frequency = 2.4 GHz
- AP to receiver distance = 2 m
- Conversion efficiency $\eta = 0.5$
- Assume free-space unit antenna gain
- Q: How much power harvested during packet reception?
- A:
  - P_R = 244 nW (-36 dBm)
  - P_H = 244 nW x 0.5 = 122 nW (122nJ/s)
- Q: How long will it take to harvest 122mJ?
- A: 1 million seconds = 277 hours!!

Lesson learned: WiFi frequency is too high and the transmit power is too low to be an effective RF energy source

©2020 Mahbub Hassan

Experimental RF energy harvesting rates

Source	Source Power	Frequency	Distance	EH rate
Isotropic RF Transmitter	4 W	902-928 MHz	15 m	5.5 μW
Isotropic RF Transmitter	1.78 W	868 MHz	25 m	2.3 μW
Powercaster	3 W	915 MHz	5 m	189 μW
TV Tower	960 kW	674-680 MHz	4.1 km	60 μW

can power many small sensors

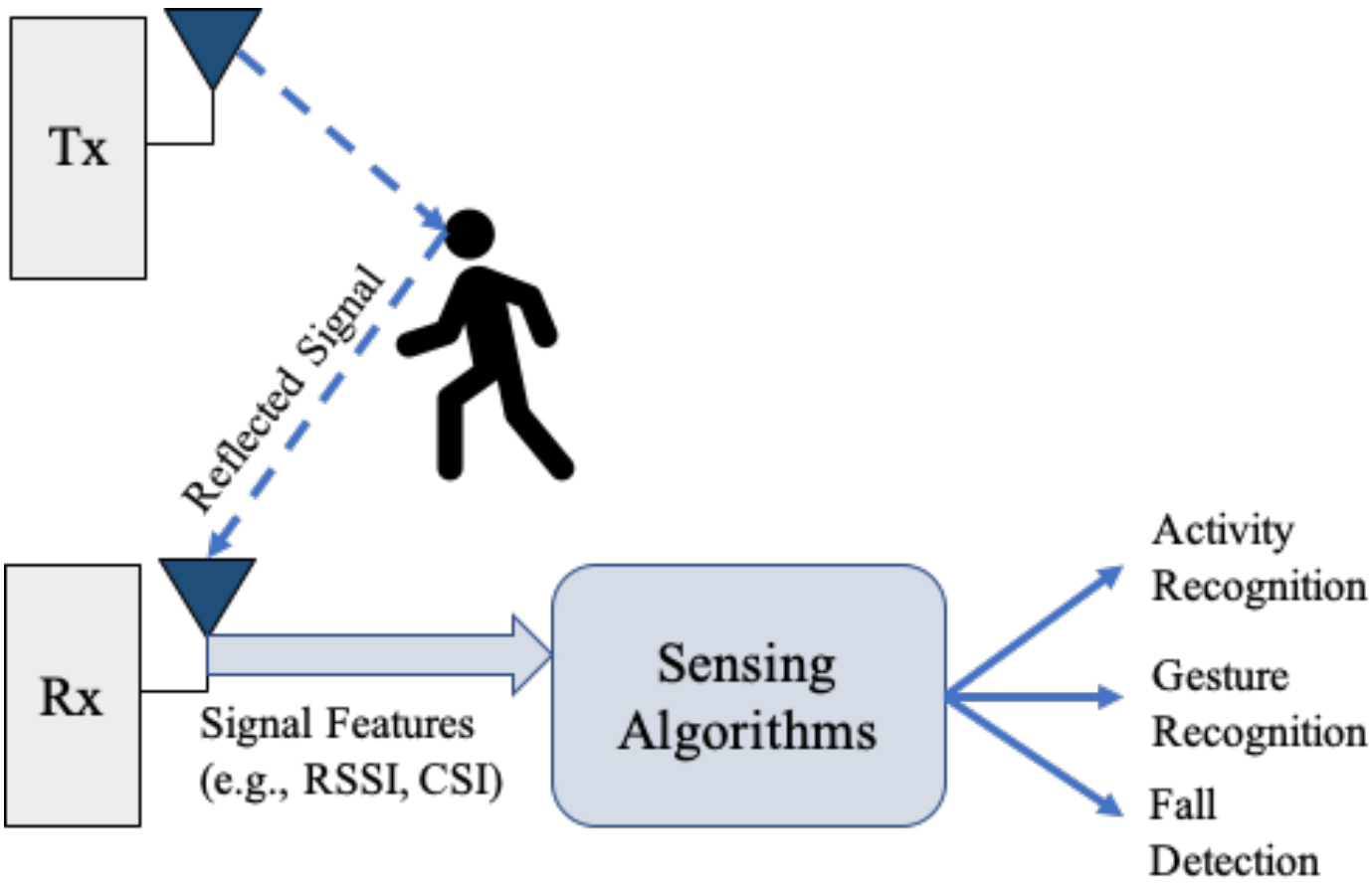
Source: Wireless Networks With RF Energy Harvesting: A Contemporary Survey, by Xiao Lu, Ping Wang, Dusit Niyato, Dong In Kim, and Zhu Han, IEEE Communications Surveys and Tutorials, VOL. 17, NO. 2, SECOND QUARTER 2015

©2020 Mahbub Hassan

RF Sensing

©2020 Mahbub Hassan

Human Sensing



©2020 Mahbub Hassan

Commercial Success of RF Sensing

- Several start-ups now offer commercial RF Sensing solutions: sleep monitoring, vital sign monitoring, fall detection, localization and tracking, activity monitoring, people counting, and so on.
  - https://www.celeno.com/wifi-doppler-imaging
  - https://www.emeraldinno.com/
  - https://walabot.com/walabot-home
  - https://www.originwirelessai.com/wirelessai
  - https://xkcorp.com/

©2020 Mahbub Hassan

Signal Features

- Received Signal Strength (RSS): *average* signal amplitude
- Channel State Information (CSI): *detailed* amplitude/phase
- Time of Flight (ToF): estimates range
- Doppler shift: estimates velocity

©2020 Mahbub Hassan

Human Sensing with RSS

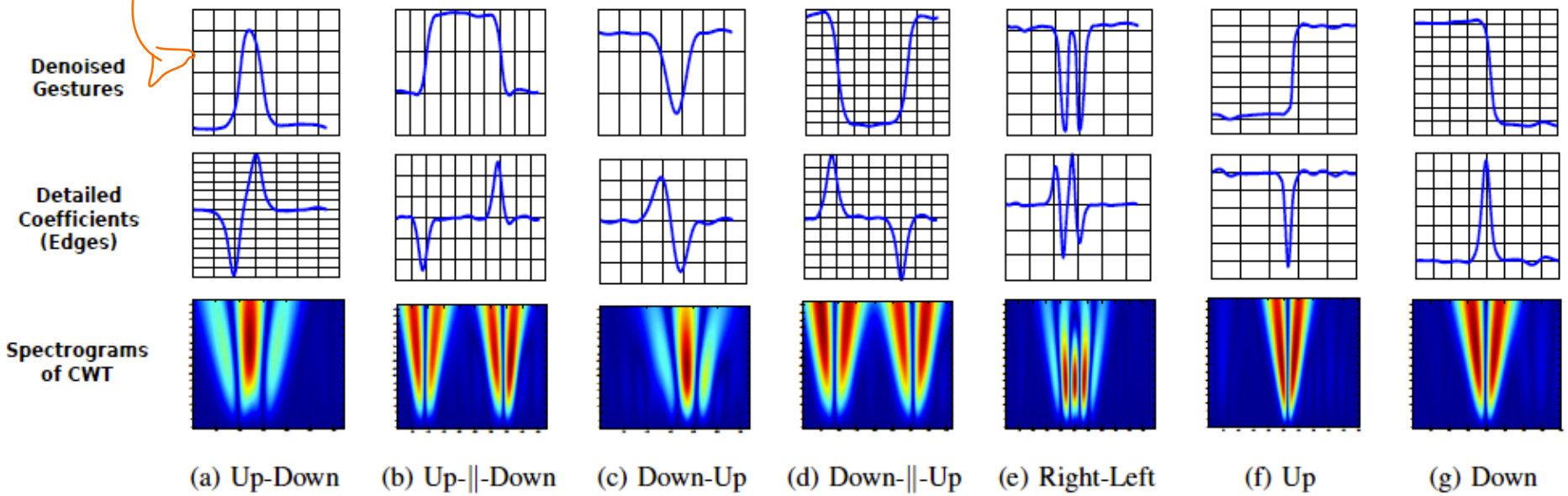
- Single scaler power value (dBm) reported for the whole channel
- Built-in support: all mobile devices measure and report RSS; no special hardware/software needed
- As RSS is affected by human presence in the wireless environment, human activities can be detected from the RSS patterns

Controlling a smartphone through hand gesture; hand gestures affect the WiFi RSS at the phone

©2020 Mahbub Hassan

Example of RSS-based hand Gesture Detection

the first row is simply filtered RSS time series



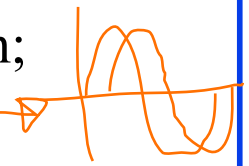
available in Moodle for you to read

Source: Abdelnasser, Youssef, and Harras: WIGEST, INFOCOM 2015

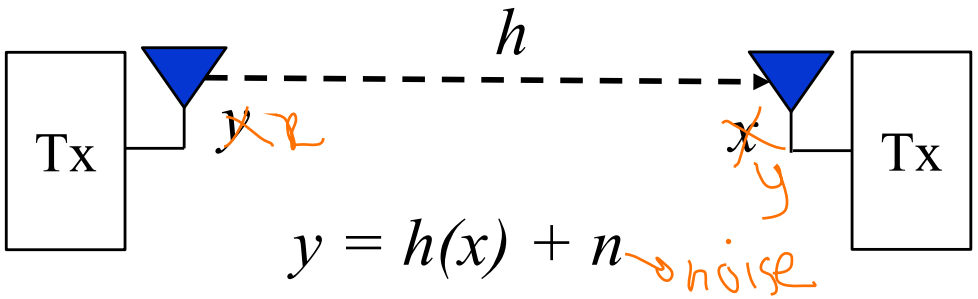
©2020 Mahbub Hassan

CSI

- RSS averages signal amplitude over the entire channel bandwidth; cannot reveal the channel response, i.e., how the amplitude and phase changes for different frequencies within the channel; RSS therefore is good only for **coarse** sensing and unsuitable for **detailed** sensing tasks
- Signal **phase** changes when the reflector moves or changes location; changes in path length will cause phase change (why?)



- CSI refers to known channel properties, i.e., how the channel affect the amplitude and phase of the transmitted signal, between a Tx and Rx

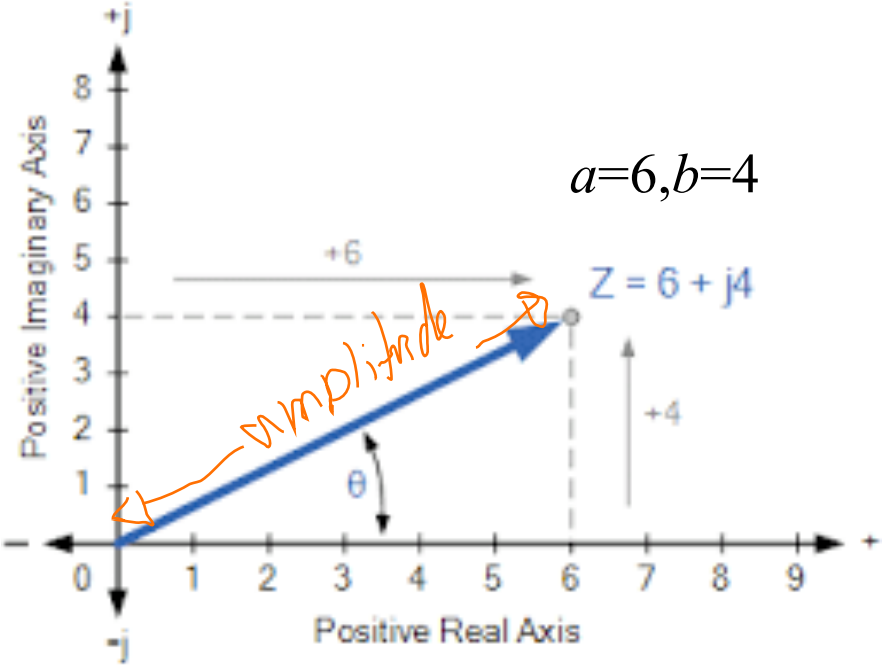


CSI estimation involves estimating *h*

©2020 Mahbub Hassan

Mathematical Representation of CSI

- CSI tells us how much the channel will **attenuate the amplitude** and how much it will **shift the phase** of the transmitted signal
- CSI is a **complex number**, which can be represented as either
  - $Ae^{j\theta}$ (A=amplitude, θ=phase, j=$\sqrt{-1}$), or
  - a+jb (Amplitude = $\sqrt{a^2+b^2}$, $Phase = \tan^{-1}\frac{b}{a}$)



a=6,b=4

©2020 Mahbub Hassan

Use of CSI in Wireless Communication

- CSI is used at the PHY layer
- CSI is used in the PHY layer of WiFi and cellular networks to estimate the channel (quality) and improve communication reliability and data rates
- In WiFi, the packet preamble contains known signals, which is compared with the received signals to estimate CSI at the receiver; the receiver then uses the CSI to decode the data symbols in the packet payload; the Rx may also provide CSI feedback to the Tx, e.g., in 802.11n, so the Tx can adjust the data rates (modulation and coding) or configure MIMO transmission parameters

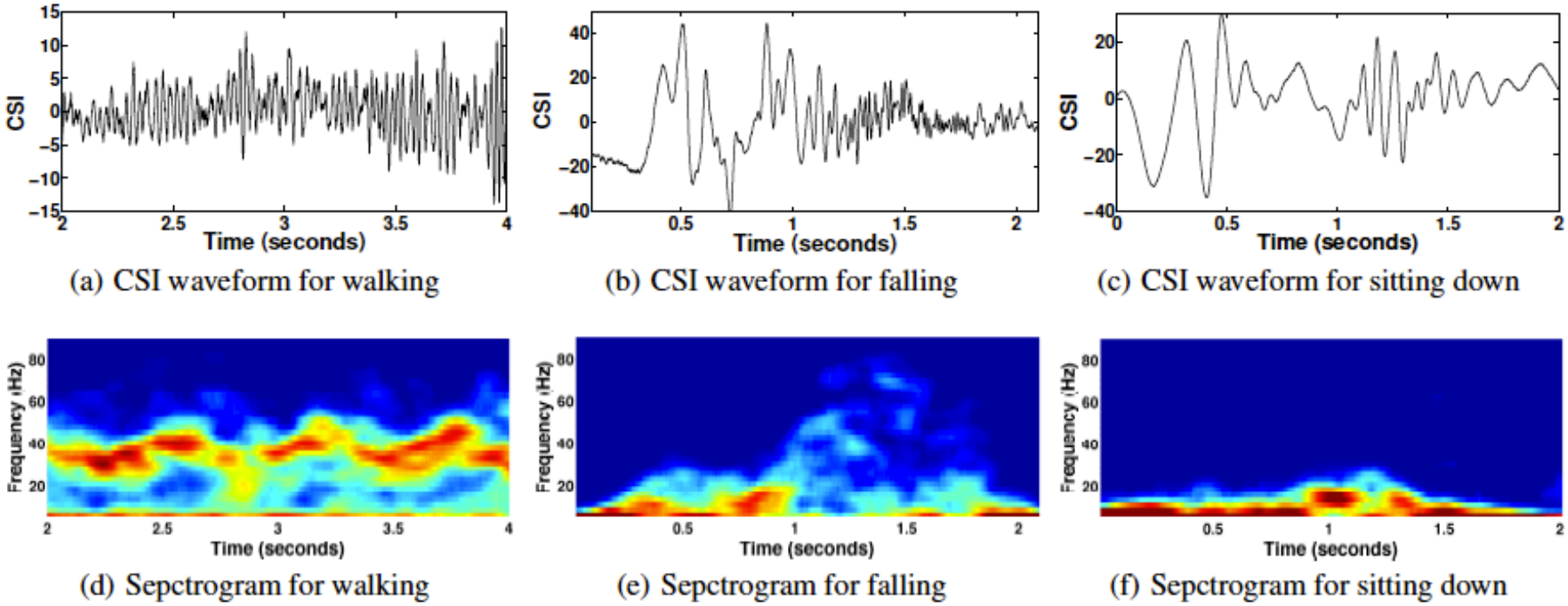
©2020 Mahbub Hassan

Human Sensing with CSI

- RSS averages signal amplitude over the entire channel bandwidth; cannot reveal the channel response, i.e., how the amplitude and signal changes for different frequencies within the channel; RSS therefore is good only for **coarse** sensing; unsuitable for **detailed** sensing tasks
- Signal phase changes when the reflector moves or changes location; changes in path length will cause phase change (why?)
- CSI returns both amplitude and phase for each subcarrier of WiFi OFDM; e.g., up to 52 amplitude-phase values for 20MHz channel for each packet received
- **CSI time series:** by configuring a Tx to transmit packets at a fixed rate, a receiver can obtain a time series of CSI at a target rate, e.g., 100 packets/s leads to CSI sampling at 100Hz
- Patterns for different human activities, such as a fall, can be learnt from the CSI time series

©2020 Mahbub Hassan

Example of CSI-based Sensing



(a) CSI waveform for walking (b) CSI waveform for falling (c) CSI waveform for sitting down

(d) Sepctrogram for walking (e) Sepctrogram for falling (f) Sepctrogram for sitting down

Source: Wang, Liu, Shahzad, Ling, and Lu: *Understanding and Modeling of WiFi Signal Based Human Activity Recognition* MOBICOM 2015

©2020 Mahbub Hassan

CSI Extraction Tools

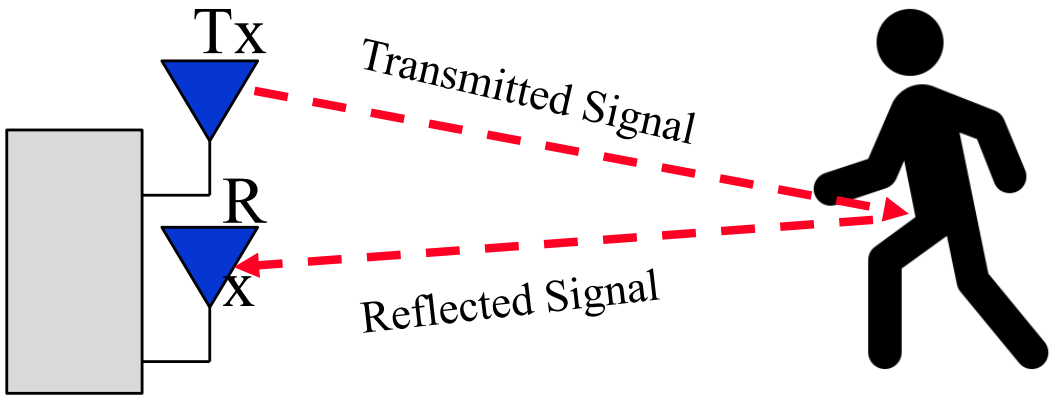
in hardware

- CSI is generated and consumed at the **PHY layer**, but human sensing algorithms execute at the **application layer**
- How to access CSI from application layer?
- Firmware of most WiFi chipsets can be modified to extract CSI
- Example of a freely available CSI extraction tool: **nexmon** (https://github.com/seemoo-lab/nexmon_csi)

©2020 Mahbub Hassan

ToF and Range Estimation

- Range, i.e., distance can be obtained if we can measure ToF
  - Range = ToF x speed of light
- Distance can help localizing and differentiate multiple objects located at different distances
- **Radar:** a fundamental concept to estimate ToF and range by generating a wireless signal and then measuring the reflected signal



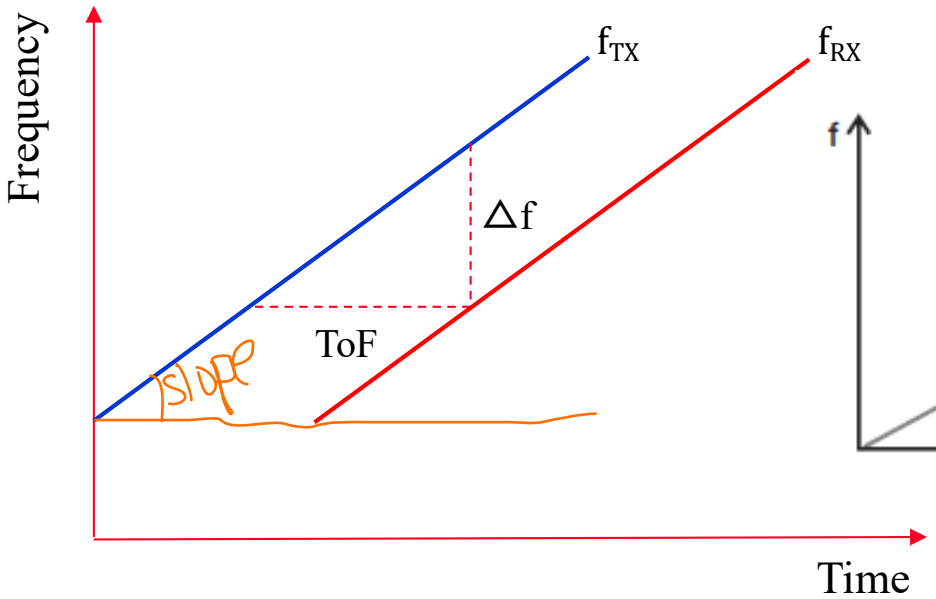
Time of Flight = time for the signal to reach the object and come back

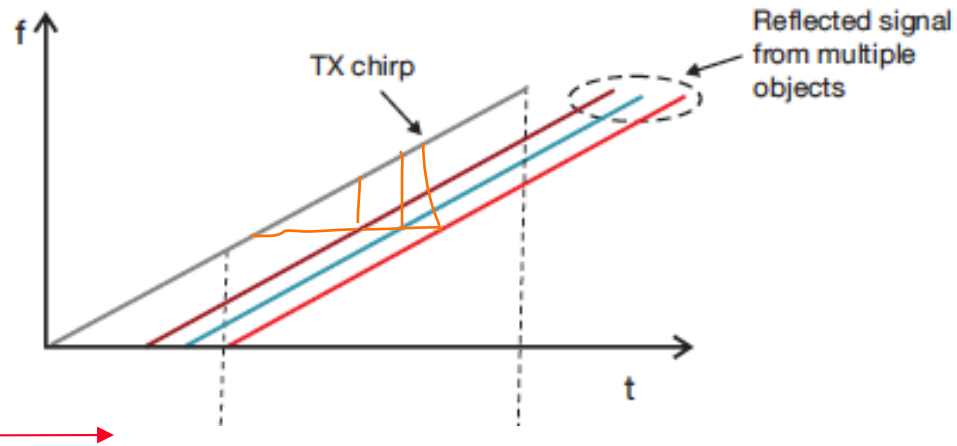
©2020 Mahbub Hassan

Range Estimation with FMCW

- FMCW: Frequency Modulated Continuous Wave
- Linear chirp: frequency is increased a known constant rate → slope
- Received signal is compared to transmitted signal to work out the frequency difference (Δf)
- $\text{ToF} = \frac{\Delta f}{slope}$; Range = ToF x c (c = speed of light)

TI IWR6843 mmWave FMCW RADAR sensor





©2020 Mahbub Hassan

Human Sensing with Doppler Effect

- Human movement can be captured through Doppler shift at the receiver
- **Radial velocity** of different human body parts can be obtained from Doppler Shift (difference between transmitted and received frequency)
  - $v = \frac{\Delta f \times c}{f}$; c = speed of light

transmitted frequency

- Using FFT, it is possible to estimate Doppler and velocity from
  - FMCW range data (more accurate)
  - CSI (less accurate)

©2020 Mahbub Hassan

Summary

- Wireless signals are good for communication, power transfer, as well as sensing
- Time switching and power splitting are two fundamental techniques to simultaneously harvest energy from the wireless signal while using it for communications
- Using RSS and CSI, WiFi can be used for many human sensing and monitoring applications; WiFi Doppler can be used for imaging.
- FMCW, a low-cost radar technology, enables more advanced sensing with RF signals, but it cannot be achieved with existing WiFi; it requires dedicated infrastructure
- New start-ups are offering commercial RF Sensing solutions

©2020 Mahbub Hassan