INTRODUCTION TO WIRELESS LAN, MAC PROTOCOLS and INTERFERENCE

cshong@khu.ac.kr, Choong Seon Hong, KHU

Outline

- Introduction
  - Wireless LAN Architecture
  - Wireless LAN standards
  - Media Access Problem
- The IEEE 802.11 MAC standard
  - MAC Sublayer
  - Access Procedures
  - DCF and PCF in detail
  - DCF Performance
  - Frame Aggregation
- Radio Propagation and Interference
  - Receiver Sensitivity, Capture Threshold
  - Interference Models

Wireless vs. Wired (1)

- Scarce resources, i.e., bandwidth
  - < 100 Mbps WLAN vs. > 1 Gbps LAN
- Less-reliable communication
  - Fading, shadowing, background noise
  - Interferences – ISI, inter-cell interference, interference from other systems
- Use mobility
  - Handoff, location management
  - Mobility makes channel less reliable

Wireless vs. Wired (2)

- Time-varying environment
  - Time-varying channel and user mobility
  - Time-varying interferers
  - Location-dependent errors
- Broadcast nature of channel
  - Multiple access for sharing the medium
- Less-secure environment
  - Mainly due to the broadcast nature of the wireless

Wireless vs. Mobile

- Wireless ≠ mobile !
- Wireless node may be static and fixed
  - E.g., Fixed wireless local loop (WLL) or IEEE 802.16 Broadband wireless access (BWA)
- Mobile node may be using a wireline networking
  - E.g., laptop with Ethernet link
- Different techniques used to tackle either of them!

Wireless & Mobile Networks

- Nomadic systems
  - Communications is typically done while the node is stationary
  - WLAN, WPAN
- Mobile systems
  - Communications can be done while the node is moving fast
  - 1G/2G/2.5G/3G cellular systems
- Nomadic system can provide faster link !

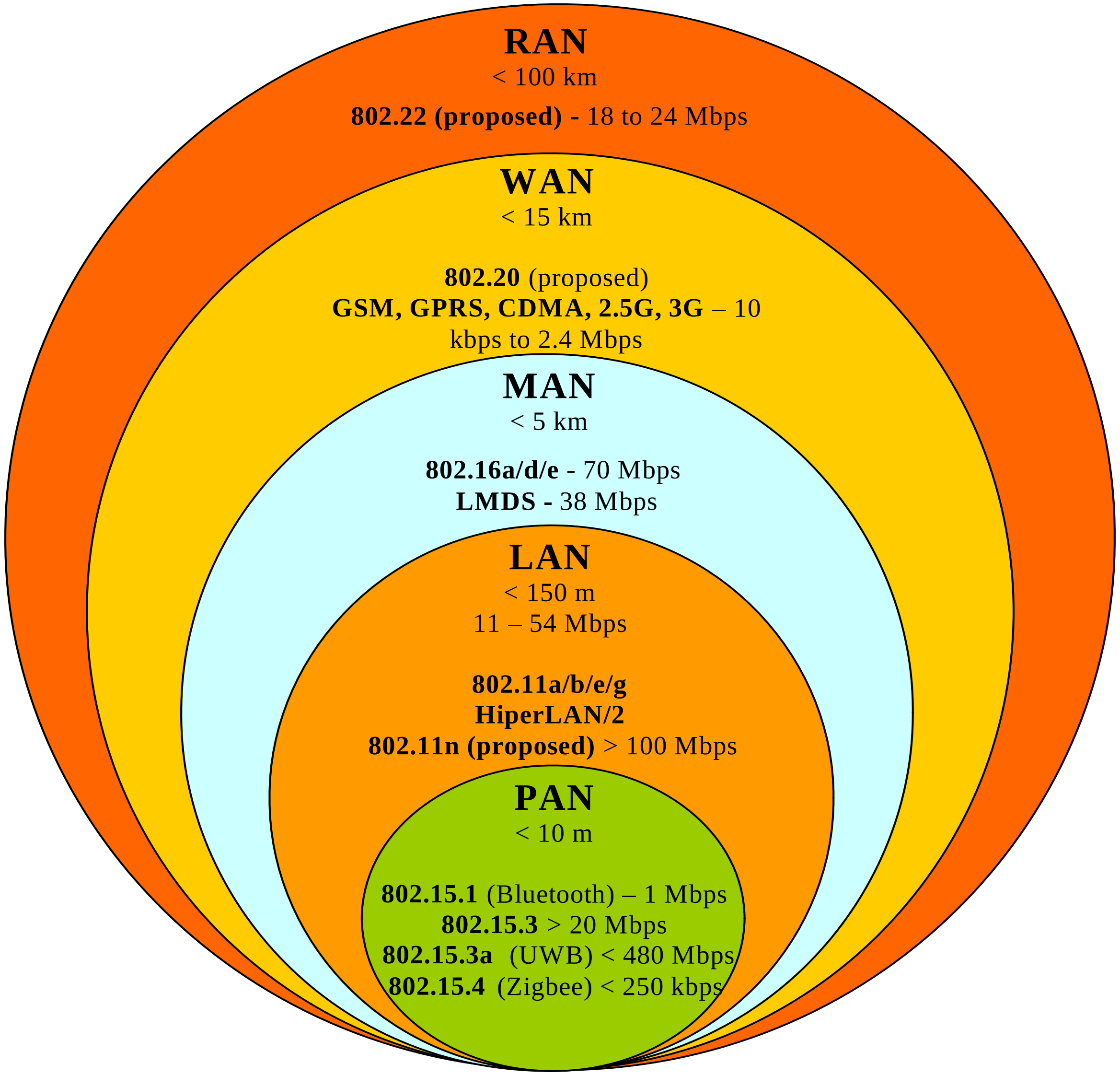
Infrastructure vs. ad hoc

- Infrastructure-based wireless networks
  - An access point (AP) or base station (BS) as an interface between wireless and (wireline) backbone
  - Star topology, hand-off support
  - Requires cell planning with frequency reuse
  - Cellular systems, typical 802.11 WLANs, …
- Ad hoc networks
  - Wireless multi-hop transmission
  - Peer-to-peer topology
  - 802.11 ad hoc mode, Bluetooth, …

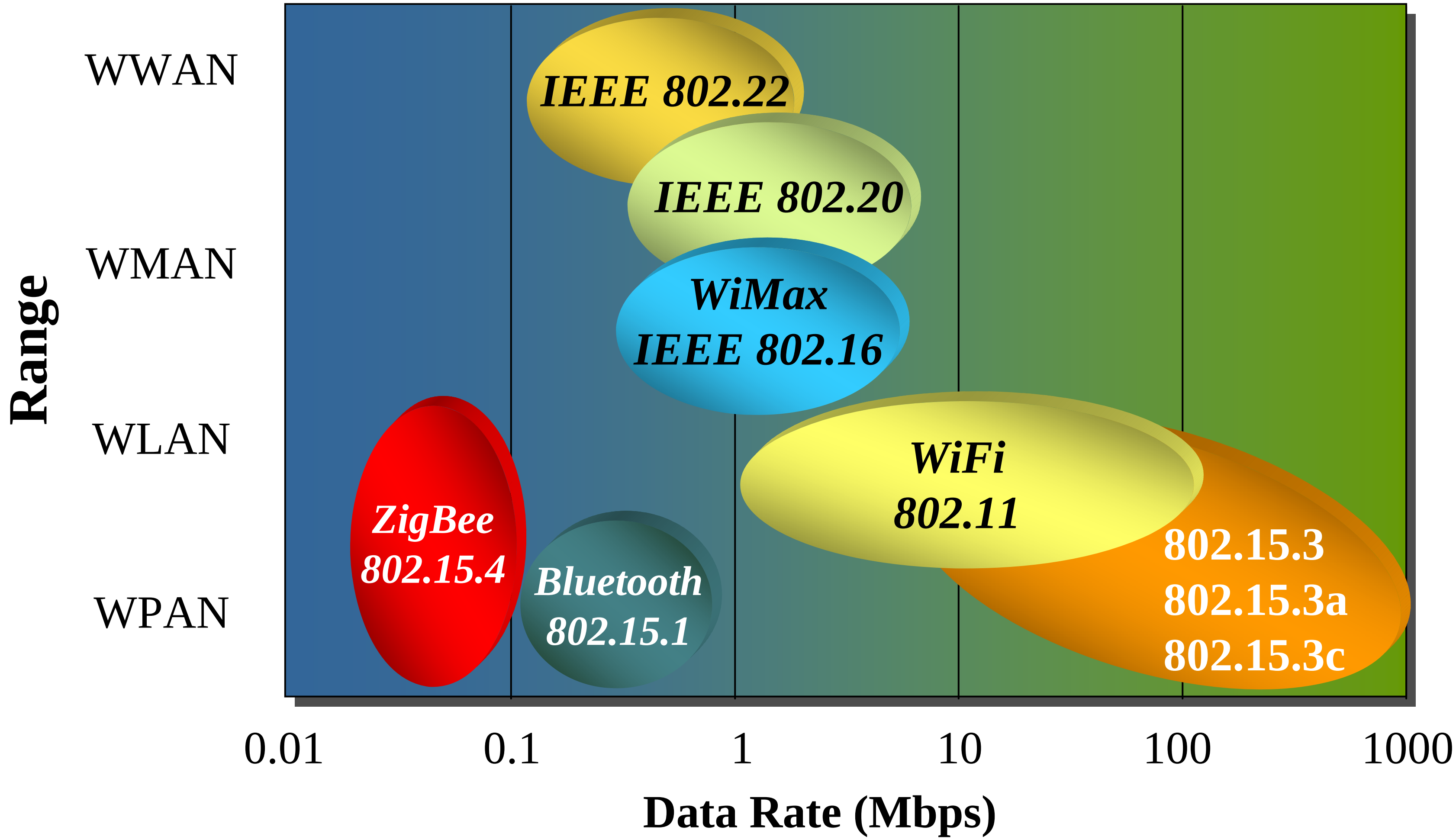
WPAN, WLAN, WMAN, WWAN

- Wireless Personal Area Network
  - IEEE 802.15.x, Bluetooth, …
- Wireless Local Area Network
  - IEEE 802.11, ETSI BRAN HIPERLAN/2
- Wireless Metropolitan Area Network
  - IEEE 802.16
- Wireless Wide Area Network
  - Cellular systems, satellite, …

Various 802 Wireless Solutions



The 802 Wireless Space



Licensed vs. Unlicensed Bands

- Licensed bands
  - Operators get the license by paying money, …
  - 800 MHz cellular, 1.9 GHz PCS, 2GHz IMT-2000 (2.1GHz)
- Unlicensed bands
  - Used without license as long as the regulatory requirements are met such as maximum transmit power level, specific modulation schemes, spectral mask, …
  - 900 MHz, 2.4GHz, 5GHz ISM bands
- Different for different countries

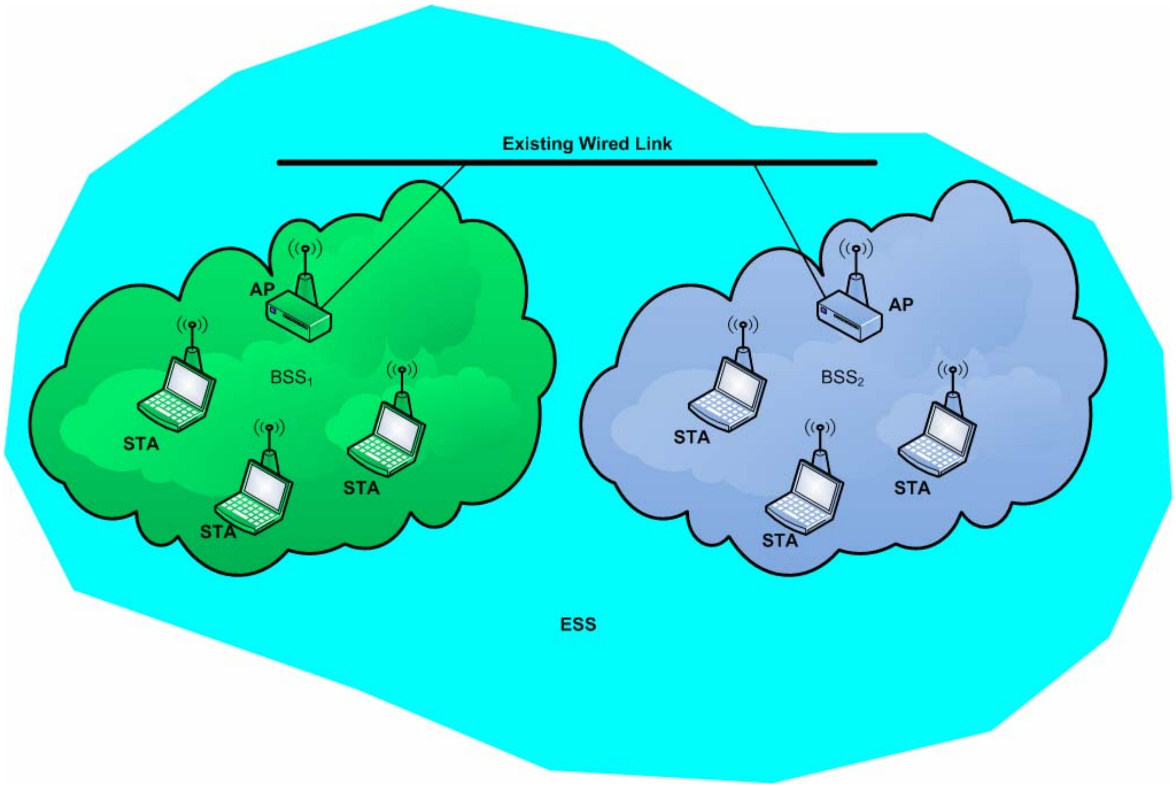
Wireless LAN Pros and Cons

- **Pros**
  - **Flexibility –** Place your device anywhere in you house
  - **Easy Setup –** No cable, connectors.
  - **Cost –** Initially higher, afterwards no cost for new wiring.
- **Cons**
  - **Speed –** Lower compared to wired. 100Mbps can be achieved using 802.11n hardware.
  - **Radio Interference –** Cordless phones, microwaves, and ham radios interfere the communication
  - **Distance –** Signal strength degrades exponentially over distance
  - **Security –** Radio signal broadcasts in all directions, anyone within range can tune in.

WLAN Architecture

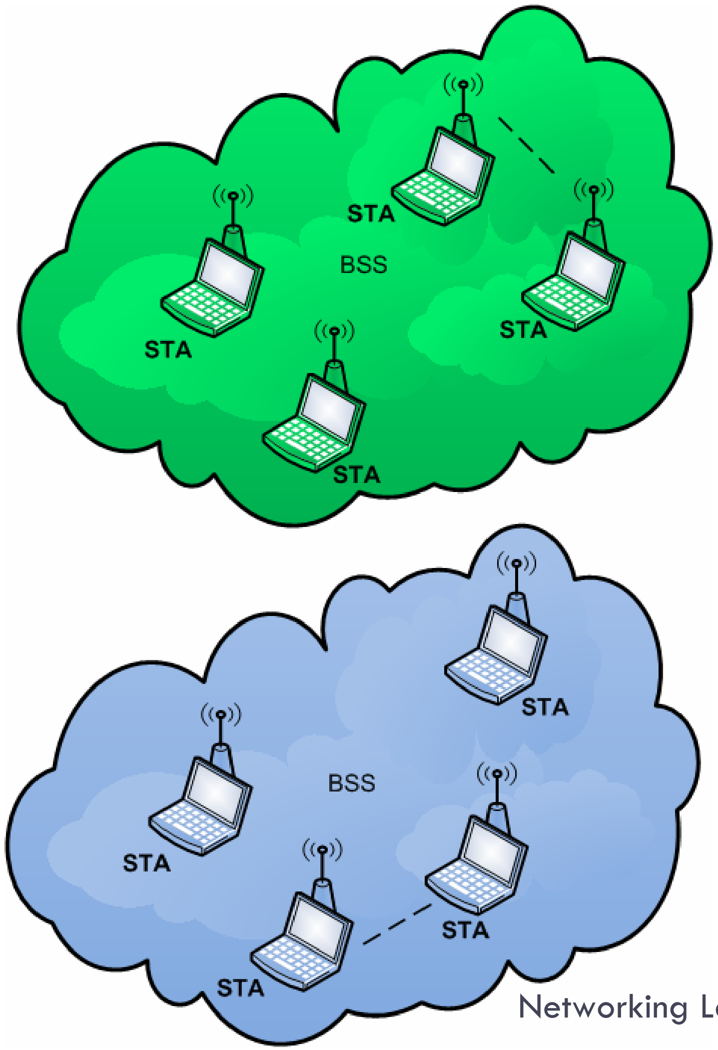
- Infrastructure
  - Wireless stations communicate with a Central Coordinator named as Access Point (AP)
  - The coverage area of an AP is referred to as Basic Service Set (BSS)
  - Coverage area of other Access Points is called Extended Service Set (ESS)
- Ad-hoc
  - Distributed Coordination (Local)
- Mesh Network
  - A combination of Infrastructure and Ad-hoc
  - Communication between BSS and ESS

Infrastructure Architecture



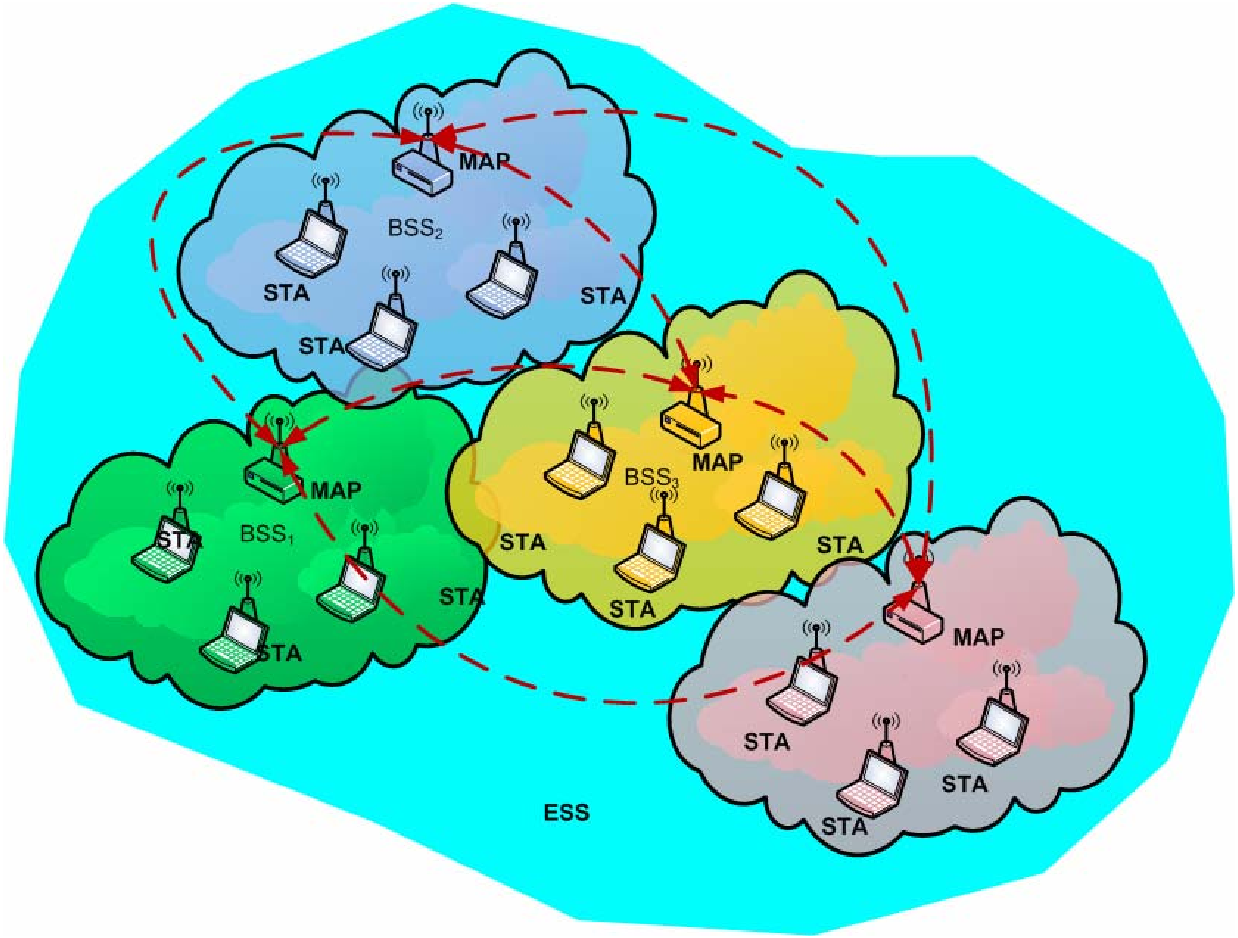
- APs are used to coordinate BSS
- STAs communicate with AP within BSS
- AP to AP communication through Wired Network

Ad-hoc Architecture



- Distributed Coordination by each STA within their vicinities
- No AP present, Hop-by-Hop communication

Mesh Architecture



- Infrastructure like Architecture
- Access Points are called Mesh Access Point (MAP)
- MAPs communicate with each other by wireless links
- MAPs are capable to route through available wireless links

Wireless LAN Standards

- 802.11a
  - Speed 54Mbs
  - Frequency used is 5 gigahertz (GHz)
- 802.11b
  - Speed 11Mbs
  - Frequency used is 2.4 gigahertz (GHz)
- 802.11g
  - Speed 54Mbs
  - Frequency used is 2.4 gigahertz (GHz)

Wireless LAN Standards (Contd.)

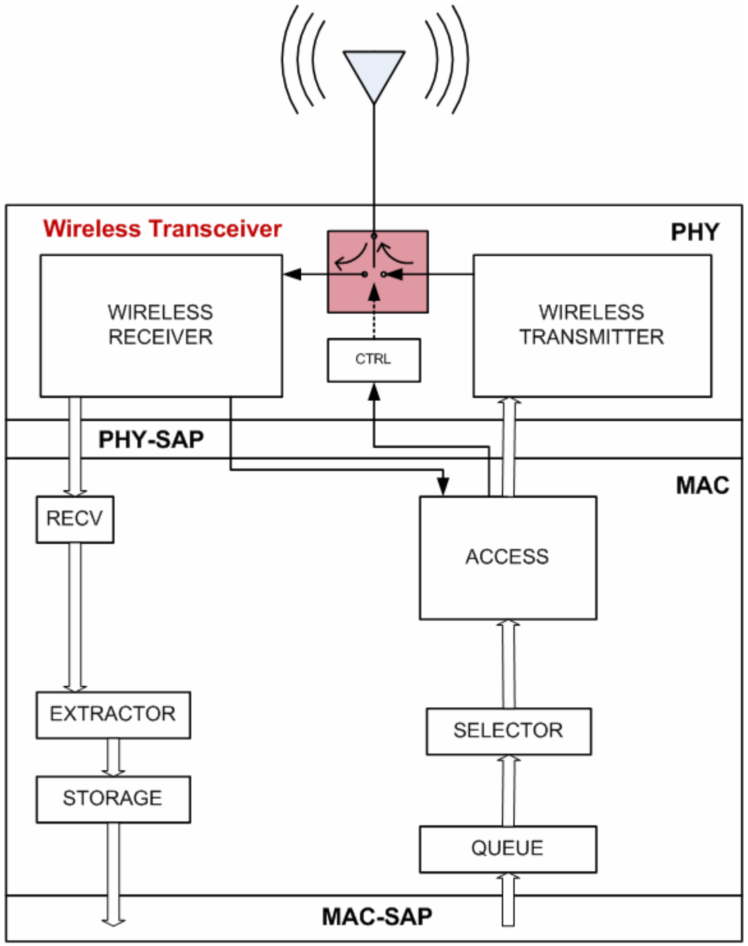
New and Future Technology

- Multiple-Input Multiple-Output (MIMO)
  - Allows present technology to achieve greater throughput with the present standards
    - Occurring Fading (distortion, delay spread)

- **802.11n** going to be the new standard for LAN:
  - Throughput may reach 540 Mbps (PHY)
  - 10 times faster than 802.11a or 802.11g
  - 100 Mbps at MAC Service Access Point (SAP)
  - A better operating distance
  - Shall include the MIMO technology

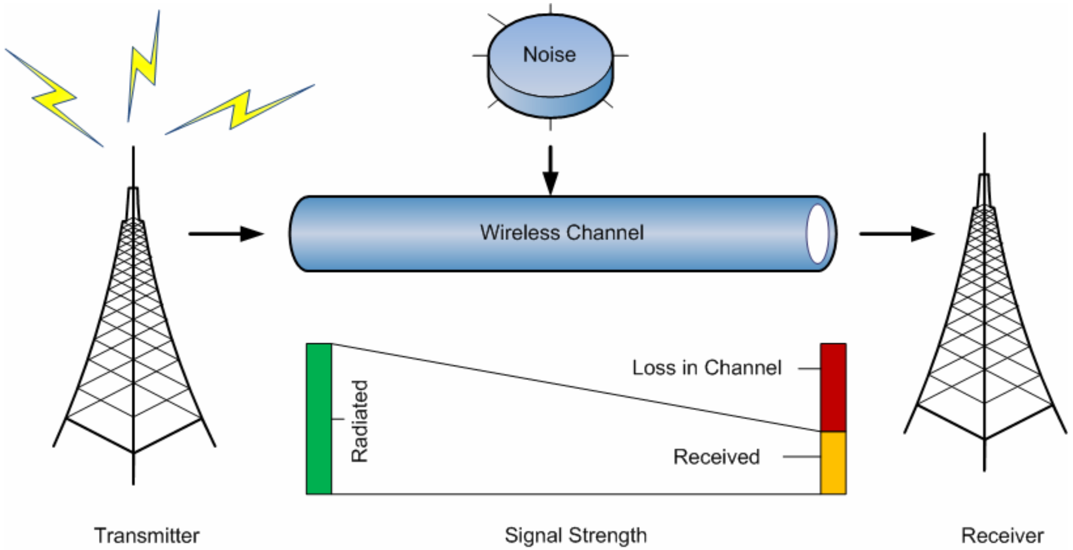
- **802.11s** going to be the new standard for Mesh Networks:
  - All features up to the 802.11n
  - With Layer–2 Routing (Router to Router)
  - With Mesh Deterministic Access to the channel (MDA)
    - Combination of DCF and PCF

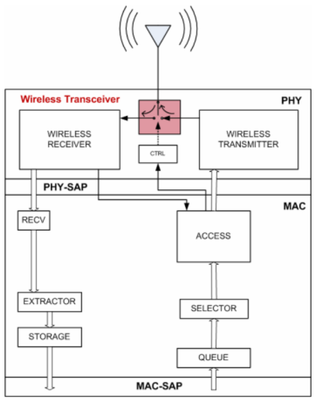
Wireless Nodes/Stations

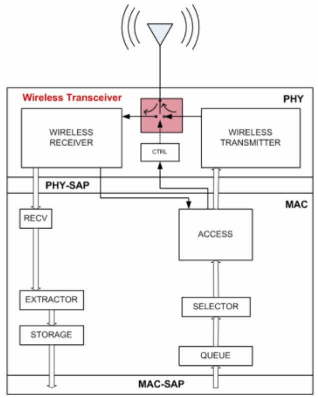


- STAs either can transmit or receive at any instant
- As the receiving circuit is inactive when transmit, STA cannot detect collisions at the transmitting end (CSMA/CD is not possible)
- **Basic Access idea** is: Transmit packets if and only if there is **no signal in the channel**.

Wireless Tx-Rx



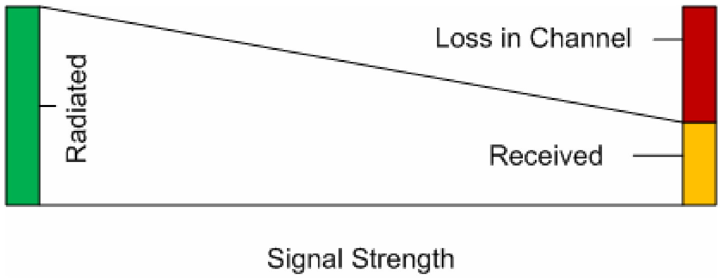




- One STA acts as Transmitter, one or more STAs receives
- Transmitter injects the electro-magnetic signal into the wireless channel
- The signal follows radio propagation rules and attenuates over distance
- If the signal strength at a receiver is high enough to receive and decode, the packet is received by the receiver.

Wireless Tx-Rx (Contd.)

- **Signal Level at Receiver**
  - Radiated (Transmitted) Signal Strength
  - Channel Quality (Attenuation Factor)
  - Distance between the Transmitting and Receiving STAs



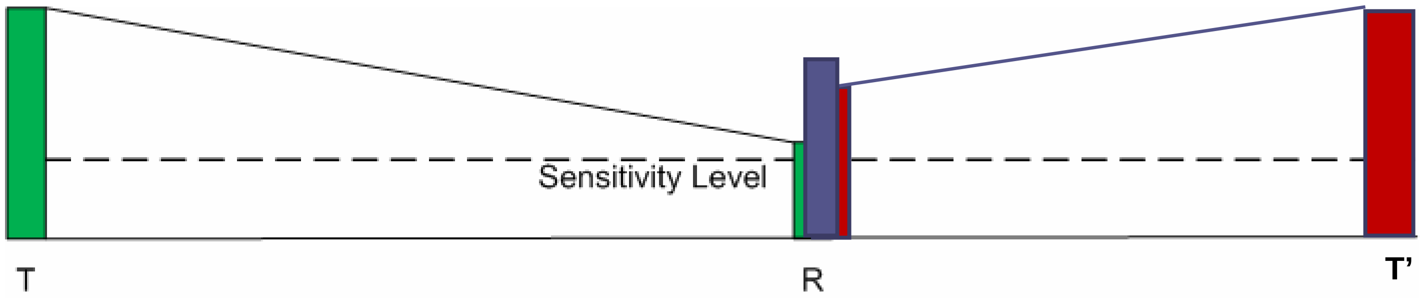
- **Receiver Sensitivity**
  - The minimum level of the signal strength for receiving a packet
  - Receiver cannot receive and extract a packet if the received signal is below this level

Wireless Tx-Rx (Contd.)

- Question:
  - Is there any Transmission Range?

- Answer:
  - **NO**
  - It is better to use the term as **Communication Range**
  - The Receiver Sensitivity and Transmission Power jointly define the Communication Range

Collision (Simple Illustration)

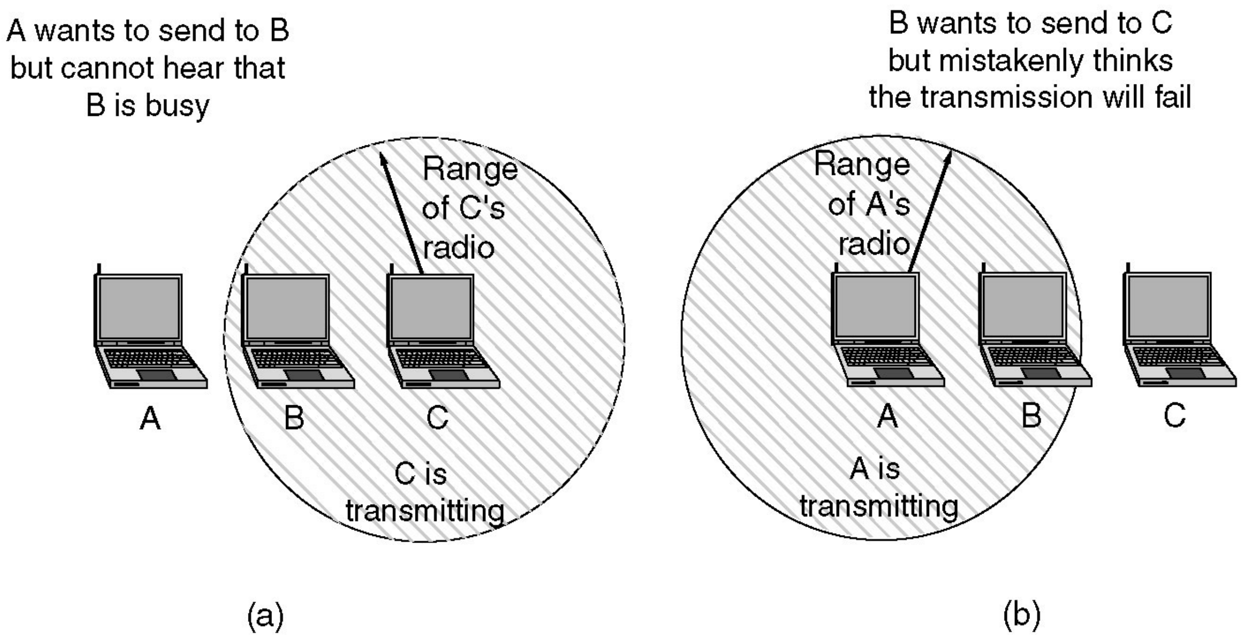


- Receiver R is supposed to receive signal from T as the received signal is above the threshold
- Receiver R can/cannot receive from T' depending on signal strength
- When they arrive simultaneously at R, the combined level is also above the sensitivity, however, R cannot receive either

Media Access Problems in WLAN

- Signal strength decreases proportional to the square of the distance
- Sender would apply carrier sense (CS) and collision detection (CD), but the collisions happen at the receiver
- Sender may not “hear” the collision, i.e., CD does not work
- CS might not work, e.g. if a terminal is “hidden”

Media Access Problems in WLAN (cont'd)



(a) The hidden station problem (b) The exposed station problem

Popular Wireless MAC Protocols

- **Carrier Sense Multiple Access (CSMA)**
  - Transmit when the channel is found free (Don't create problem to others)
  - Collides when n (n>1)STAs access simultaneously

- **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**
  - If the channel is free, wait for some random time (Referred to as **Random Backoff Period**), and if the channel is still free, start transmission
  - Don't create problem to others who already accessed the channel **PLUS** wait for some time if any other starts
  - Collides when n (n > 1) STAs wait for same random time after channel becomes free

IEEE-802.11 Protocol

- MAC is based on CSMA/CA
- 802.11 Comprises of MAC and PHY layer management for Wireless LAN Environment
- The PHY Layer has two sub-layers:
  - **PLCP:** PHY Layer Convergence Procedure : Medium Independent
  - **PMD:** PHY Layer, Medium Dependent

Protocol Architecture

<table>
<tr><td rowspan="2">MAC sublayer</td><td rowspan="2">MAC layer management</td></tr>
<tr></tr>
<tr><td>PLCP sublayer</td><td rowspan="2">Physical layer management</td></tr>
<tr><td>PMD sublayer</td></tr>
</table>

IEEE 802.11 MAC Sub-layer

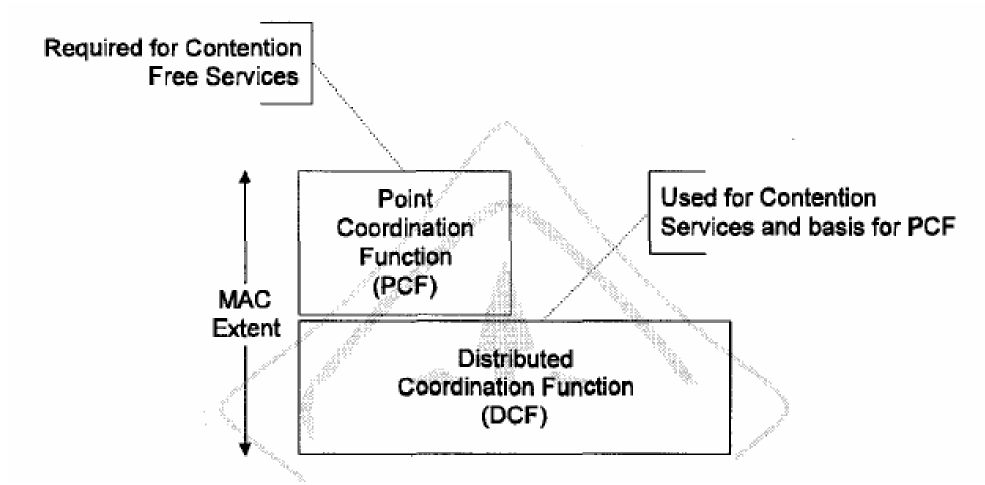
- Coordinates the Channel Access at every STA
- Channel Access Types
  - **(Access after) Contention**

    Known as **DCF**

    STAs contend for channel access and the winning STA gets access
  - **Contention Free**

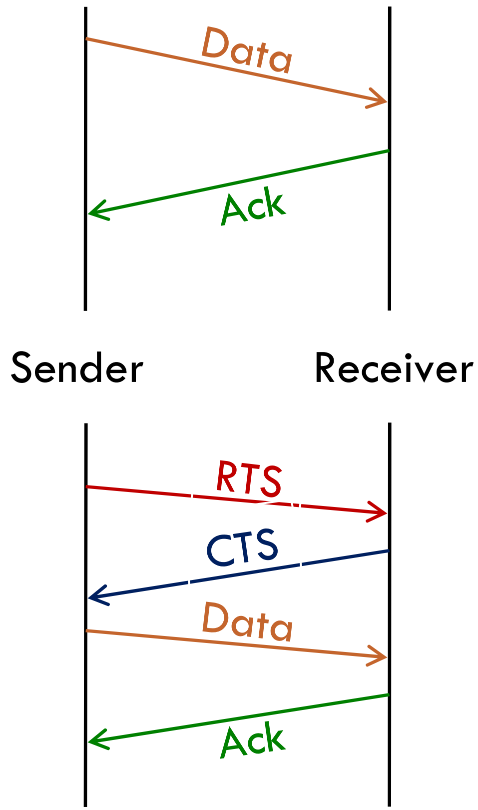
    Known as **PCF**

    Time bound, uses beacons to synchronize transmissions



MAC Sub-layer (Contd.)

- Data Transfer
  - 2-way handshaking
    - Data Packet is Acknowledged by Receiver
    - Acks are used to maintain reliability
  - 4-way handshaking
    - 2+2 way
    - First, reserve the channel by Request-to-Send (RTS) and Clear-to-Send (CTS)
    - Then Follow 2-way data transfer



RTS/CTS

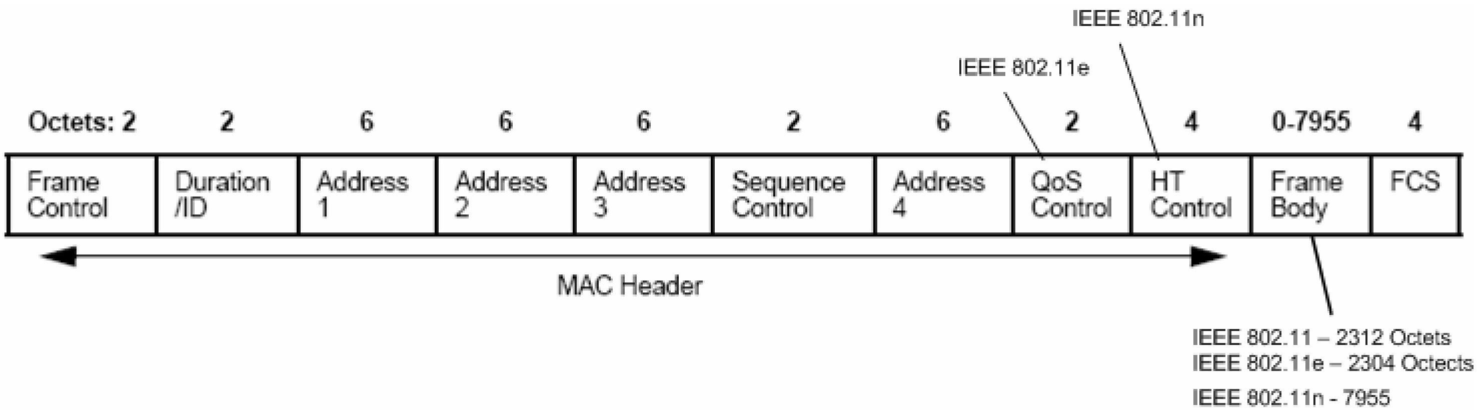
- If packet size > RTSThreshold (typically 500 bytes) 4-way handshaking is used

- Two-fold benefit
  - Channel Reservation for long data packets, and thus, reducing collision probability by hidden and exposed terminals
  - Long data transmission defers until receiving STA clears; determining collisions before transmitting large packets

MAC Sub-layer (Contd.)

- MAC Layer Packets are named as Frames
- Frames are categorized into several classes, like:

    Data, Control, Action, Management.
- General Form of a MAC frame is:



MAC Frames (Data and ACK)

Data Frame:

Receiver (Address 1) — Sender (Address 2)

Octets: 2	2	6	6	6	2	6	2	4	0-7955	4
Frame Control	Duration / ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	QoS Control	HT Control	Frame Body	FCS

MAC Header (Frame Control through HT Control)

Here is the Data (Frame Body)

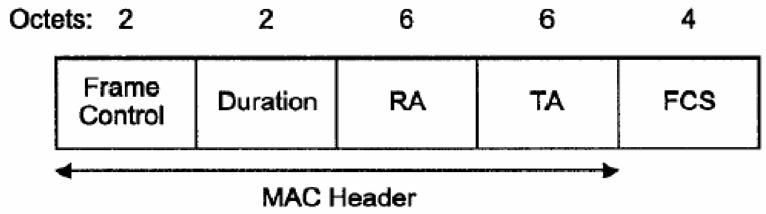
ACK Frame: (Control)

Octets: 2	2	6	4
Frame Control	Duration	RA	FCS

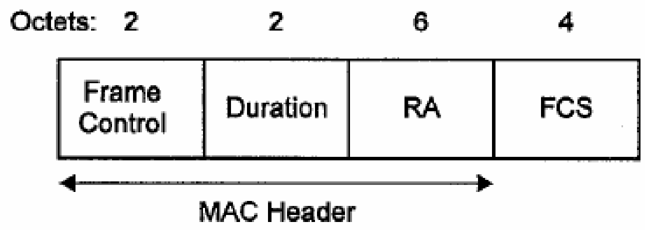
MAC Header (Frame Control through RA)

Frame Formats (RTS and CTS)

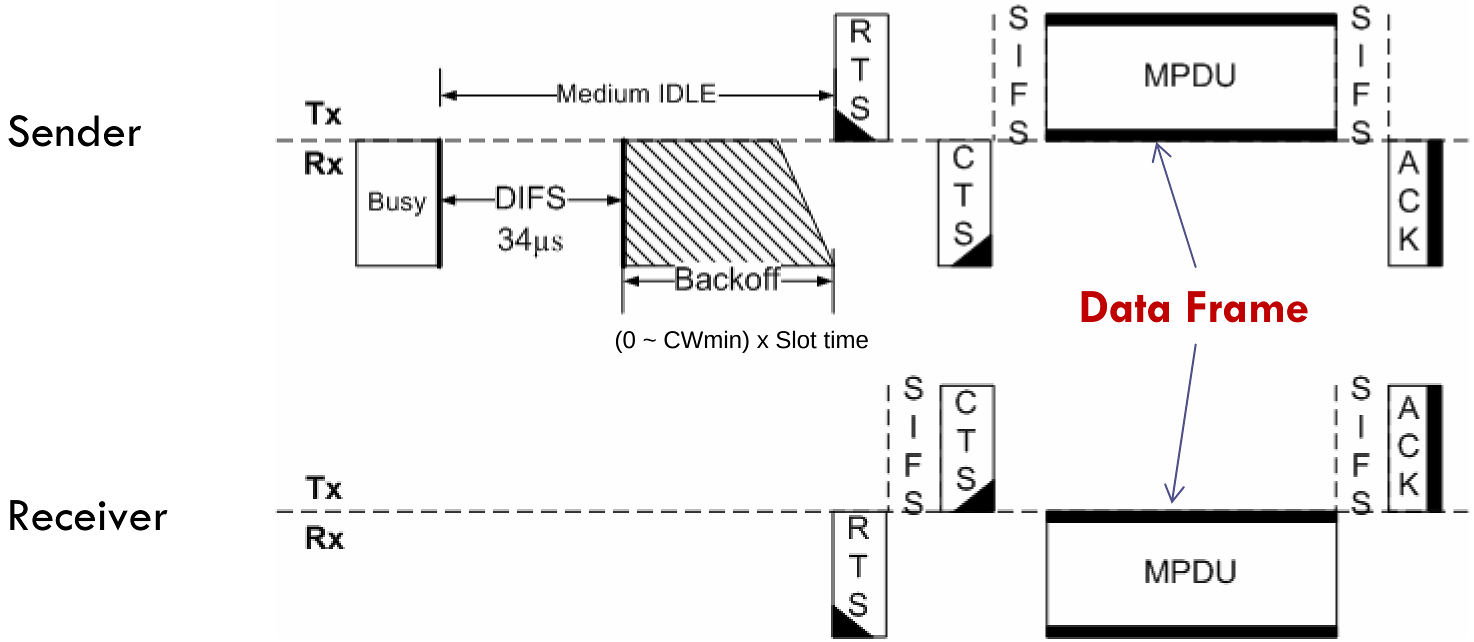
RTS Frame:
(Control)



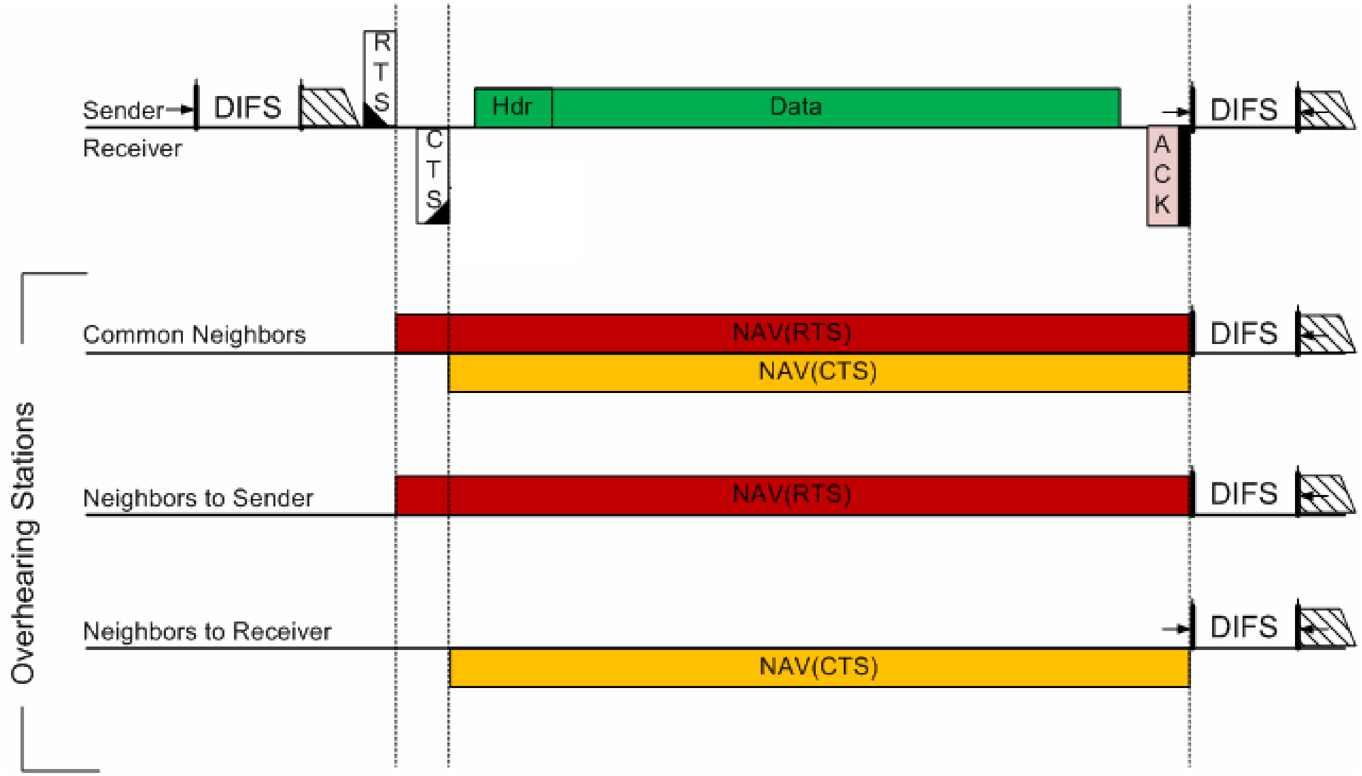
CTS Frame:
(Control)

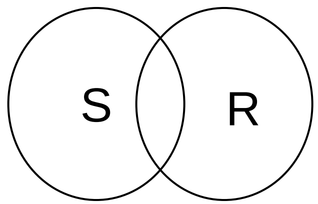


DCF Channel Access (Tx-Rx)



DCF Channel Access (Regional)





Distributed Coordination Function (DCF)

- Local Coordination using..
  - Carrier Sensing (CS)
  - Inter-frame Space (IFS)
  - Adaptive Random Backoff
  - Retransmission Scheme (Retry)

DCF - Carrier Sensing

- Two Types of Carrier Sense mechanism
  - **Physical Carrier Sensing**
    - Receives 0/1 from PHY layer indicating absence or presence of carrier in the medium
  - **Virtual Carrier Sensing**
    - From overheard frames, STAs can find duration of current transmission
    - Physical Carrier Sensing is worthless during this period
    - Maintains a Counter named as Network Allocation Vector (NAV) that indicates how long the medium would be occupied by other station
    - If NAV > 0, the channel is busy
    - The NAV is decremented at each time slot and when it reaches to zero, the physical carrier sensing is applied

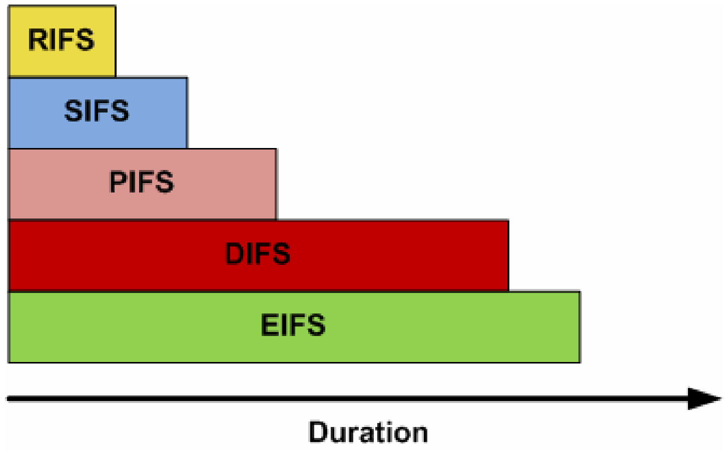
Inter-Frame Space (IFS)

- Inter-Frame Spaces are used to control the frame sequences during 2-way or 4-way handshaking

- Five IFS are available:
  - DIFS – DCF IFS; used for accessing channel for Data Frames
  - SIFS – Shortest IFS; used to continue with obtained access
  - PIFS – PCF IFS; entry point for PCF mode from DCF
  - EIFS – Extended IFS; for receivers received erroneous /incomplete packet
  - RIFS – Reduced (S)IFS (802.11n); for High Throughput (HT)

IFS (Contd.)

- Specific IFS is selected for specific channel access
- Duration of IFS implements the priority
- RIFS (802.11n)/SIFS is used to complete ongoing handshaking/transmission (before sending ACK/CTS or another fragment)
- DIFS is used to access for new Data Frame
- PIFS is used to switch from Contention based access to Contention-free access
- EIFS is used instead of DIFS if a receiver receives incomplete packet



Random Backoff

- CSMA/CA uses Random Backoff in order to prevent simultaneous access by two transmitters in order to avoid collision

- The random backoff period is determined by a chosen random number from a pool of numbers named as Contention Window (CW)

- STAs uniformly pick a number ***r*** from range **[0,CW)** and determines the Backoff period using:

$$\textit{Backoff Period} = \mathbf{r} \times \textit{Slot time}$$

- DCF uses Residual Backoff; that means, if a backoff value is chosen, it is continued for consecutive busy/free medium until it reaches to zero and the STA gets access to the channel

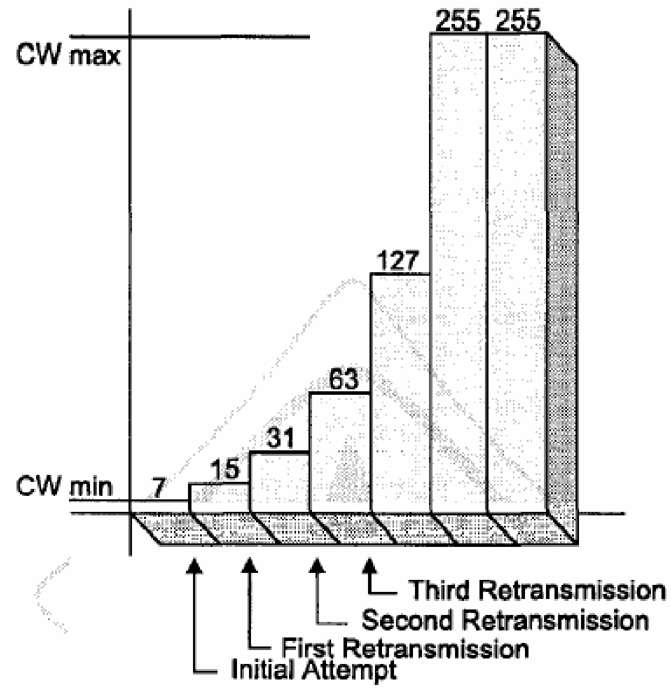
Adaptive Random Backoff

- Adaptive CW value

  [floor **CW_{min}** , ceiling **CW_{max}**]
- CW is chosen adaptively according to channel condition and congestion
- Larger CW, possibility of picking larger random number
- If the previous frame sent successfully, **$CW=CW_{min}$**

  Otherwise,

  $CW = \min(2*CW, CW_{max})$



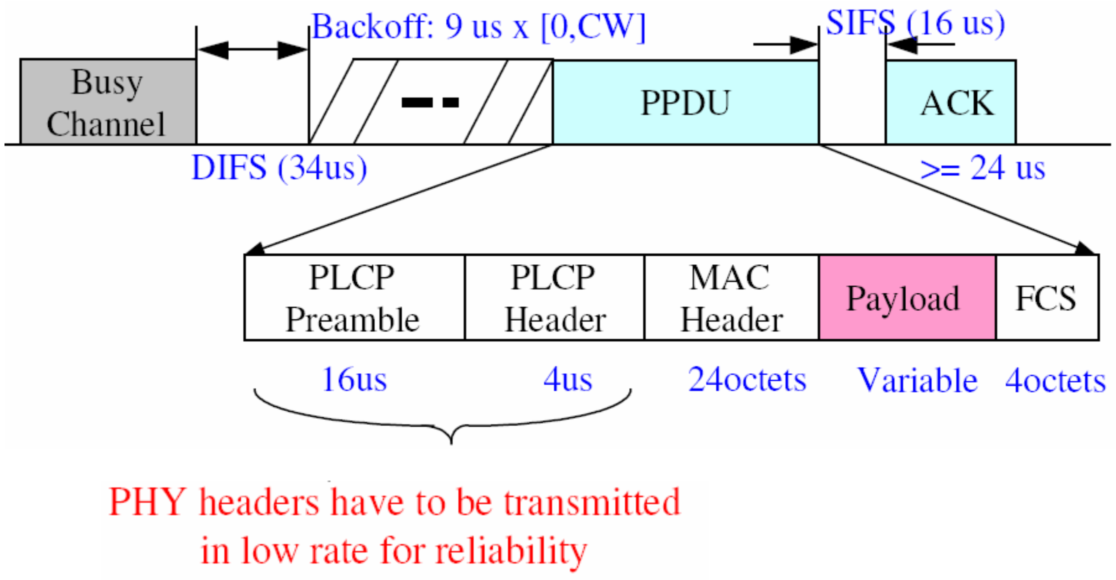
Retransmission

- Wireless links are not stable and error prone
- DCF retransmits up to certain limit(s) for unsuccessful transmissions
- How DCF detects unsuccessful transmission?
  - If the sender is unable to receive ACK frame
- Why the Sender may not receive ACK?
  - The receiver didn't send it (the data frame is not successfully received at the receiver)
  - The receiver sent the ACK frame, but it collided at sender or channel condition distorted the ACK frame

Retransmission (Contd.)

- DCF retransmits a data frame up to
  - 4 times (short retry limit) when no RTS/CTS is required
  - 7 times (long retry limit) when RTS/CTS is required
- Each retransmission follows same DCF cycle
- Entire data frame is resent (large overhead for long data frames)

DCF performance



- Overheads are: several IFS, low rate PHY header transmission, MAC header and FCS
- IF RTS/CTS is used, then transmission and IFS time would be added as overheads

DCF performance (Contd.)

- PHY/MAC Parameters to measure overheads

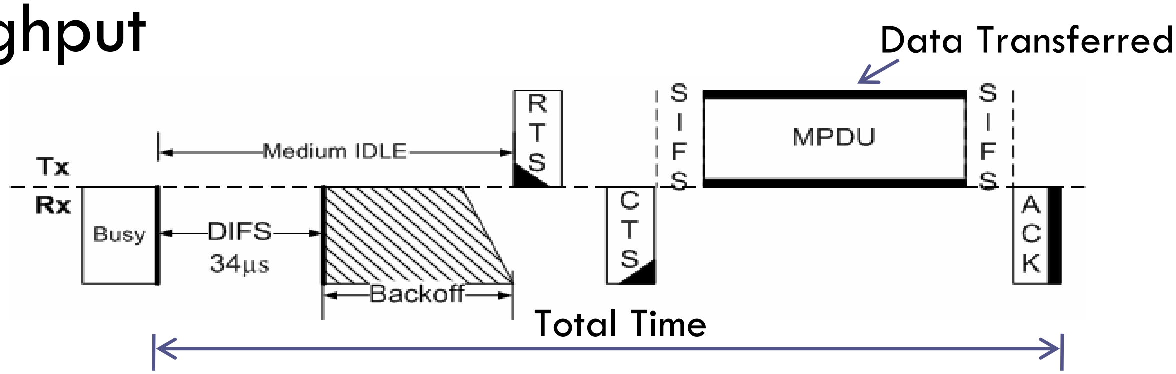
	802.11b	802.11a	802.11n
T_{SIFS} (μs)	10	16	16
Slot time - σ (μs)	20	9	9
T_{DIFS} (μs)	50	34	34
T_{PHYhdr} (μs)	192	20	20
CW_{min}	31	15	15
MAChdr (bits)	224	224	224
CRC (bits)	32	32	32
Propagation delay - δ (μs)	1	1	1
OFDM symbol delay (μs)	-	4	4
NBpS (No. of bits per symbol)	-	216	216·k
PHY layer peak rate (Mbps)	11	54	54·k

k : diversity factor

DCF performance (Contd.)

- Ideal Max Throughput

$$S_{ideal} = \frac{Data\ Transferred}{Total\ Time}$$



$$S_{ideal} = \frac{8 \times Payload}{T_{DIFS} + T_{\overline{CW}} + T_{RTS} + T_{SIFS} + T_{CTS} + T_{SIFS} + T_{PHYHdr} + T_{Payload} + T_{SIFS} + T_{ACK} + 48}$$

- Throughput Upper Limit (TUL): when data rate infinite

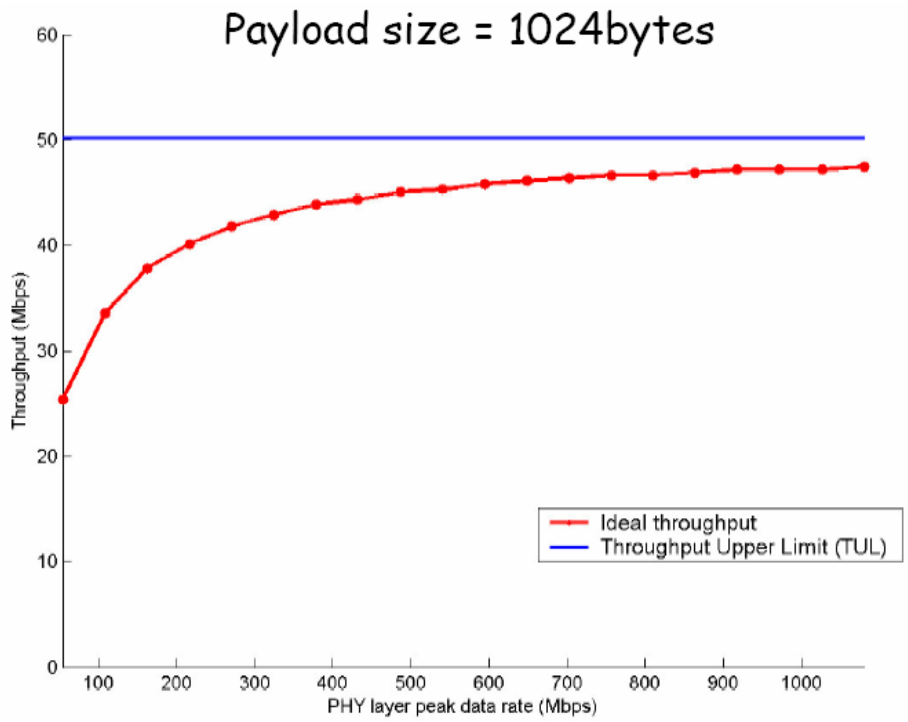
$$S_{ideal} = \frac{8 \times Payload}{T_{DIFS} + T_{\overline{CW}} + T_{RTS} + T_{SIFS} + T_{CTS} + T_{SIFS} + T_{PHYHdr} + T_{SIFS} + T_{ACK} + 48}$$

DCF performance (Contd.)

Ideal Maximum MAC Throughput

(when no collision occurs and there is no noise)

We Cannot get throughput higher than 50Mbps with 1KB frame by increasing PHY layer DATA RATE



How to improve DCF performance?

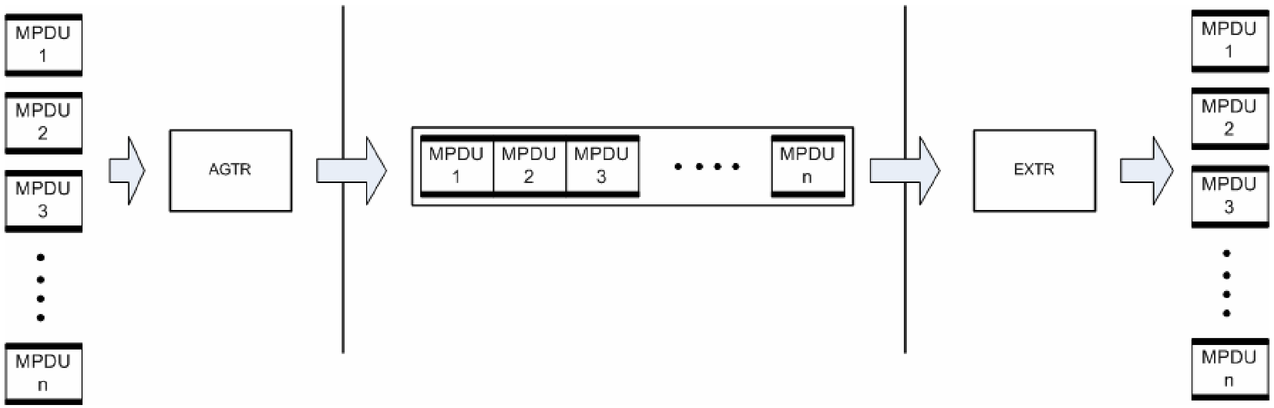
- Send MAX data packets once a STA gets access
- Use a Reduced IFS when multiple data packets are sent

- **Why we cannot change DIFS and other timing?**
  - To cooperate with Legacy 802.11 devices

- **What is the consequence of sending multiple frames in single access?**
  - Neighbors of transmitter and receiver would experience large NAV
  - For each unsuccessful transmissions, if same aggregated frame is retransmitted, it would create a large overhead

Frame Aggregation (802.11n)

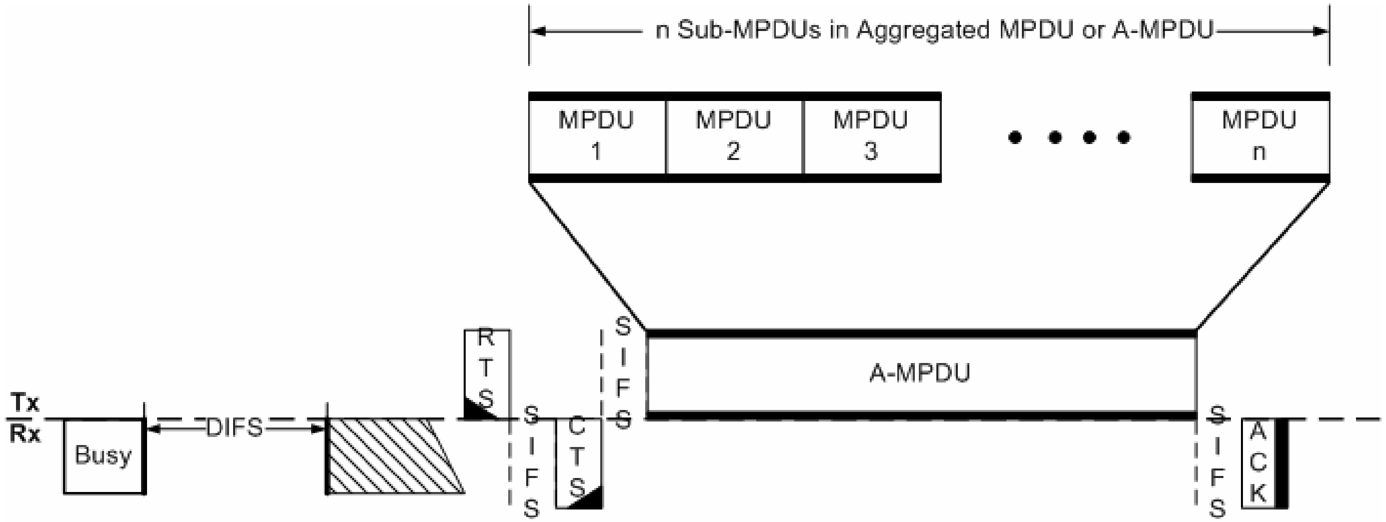
- Sender aggregates/merges n-frames and form a super fame called Aggregated frame (A-MPDU)



- At the receiving end, the receiver extracts n-subframes from the A-MPDU

Frame Aggregation (FA) (Contd.)

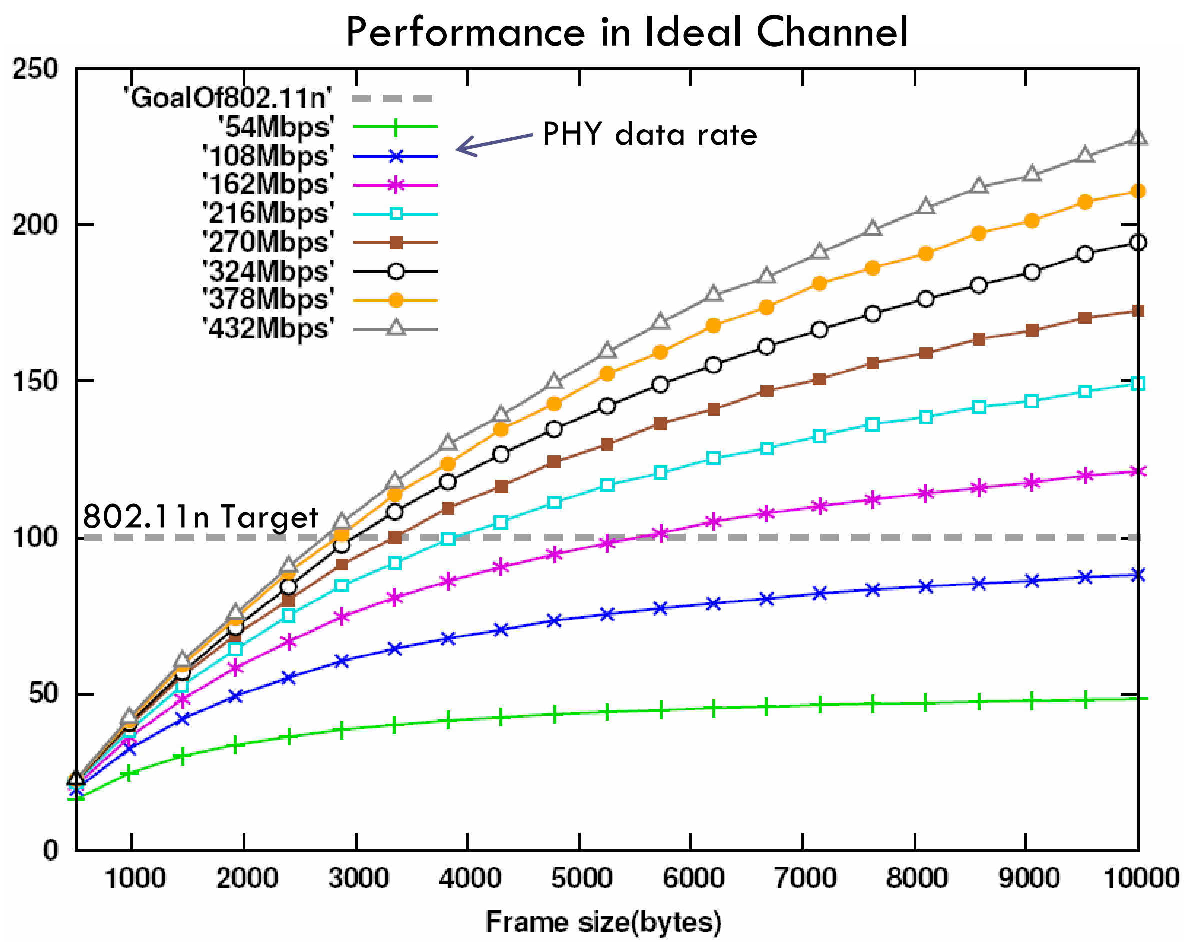
- The Sender contends for channel access according to DCF procedure



- It transmits the aggregated frame as a single frame when it gets access to the channel

Performance with FA

- Link Throughput increases as the aggregated frame size increases
- 802.11n protocol defines the maximum size as 7955 bytes

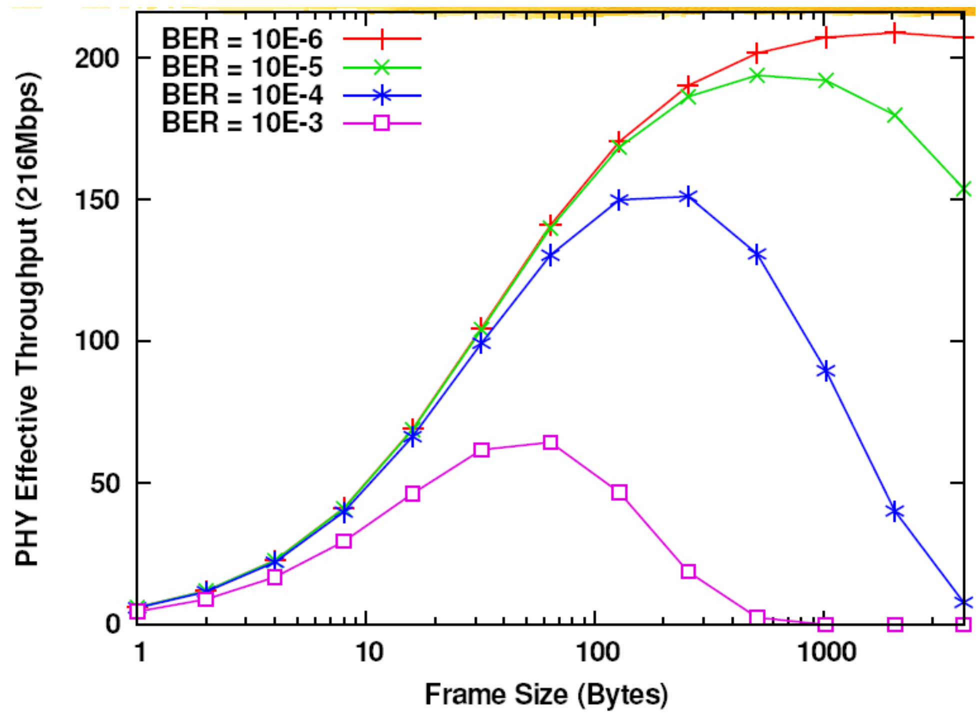


Performance with FA (Contd.)

- Performance drops with large frame size due to frame retransmissions

- Retransmission scheme should be improved..

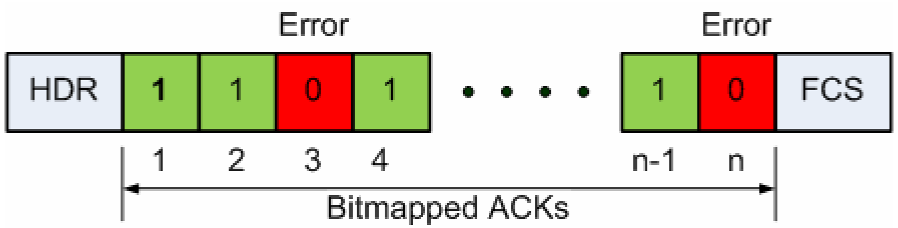
Performance in Noisy Channel



PHY layer peack rate = 216Mbps

Block ACK

- In case of unsuccessful transmission, the sender asks for a Block ACK from the receiver
- The Block ACK is a bitmapped ACK, with 1 bit for each sub-frame in the A-MPDU

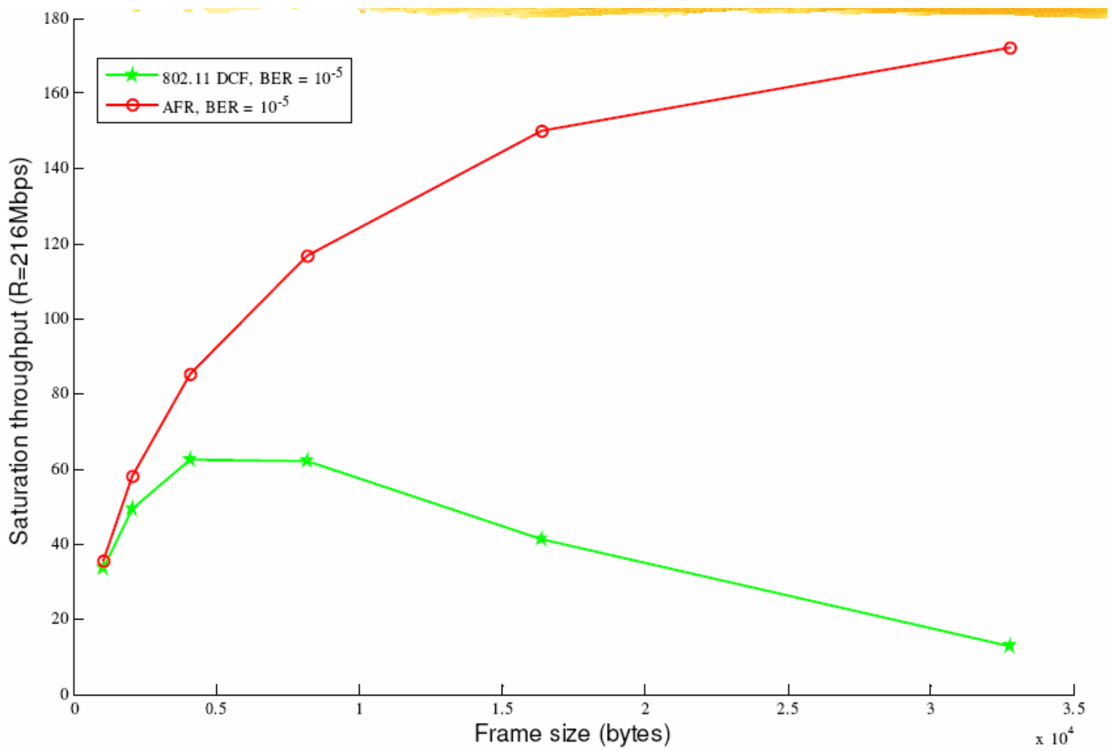


- 0 indicates unsuccessful reception
- Sender retransmits unsuccessful frames only

Performance with FA and BlockACK

- AFR = Aggregation with Fragment Retransmission

- Throughput stabilizes with AFR scheme

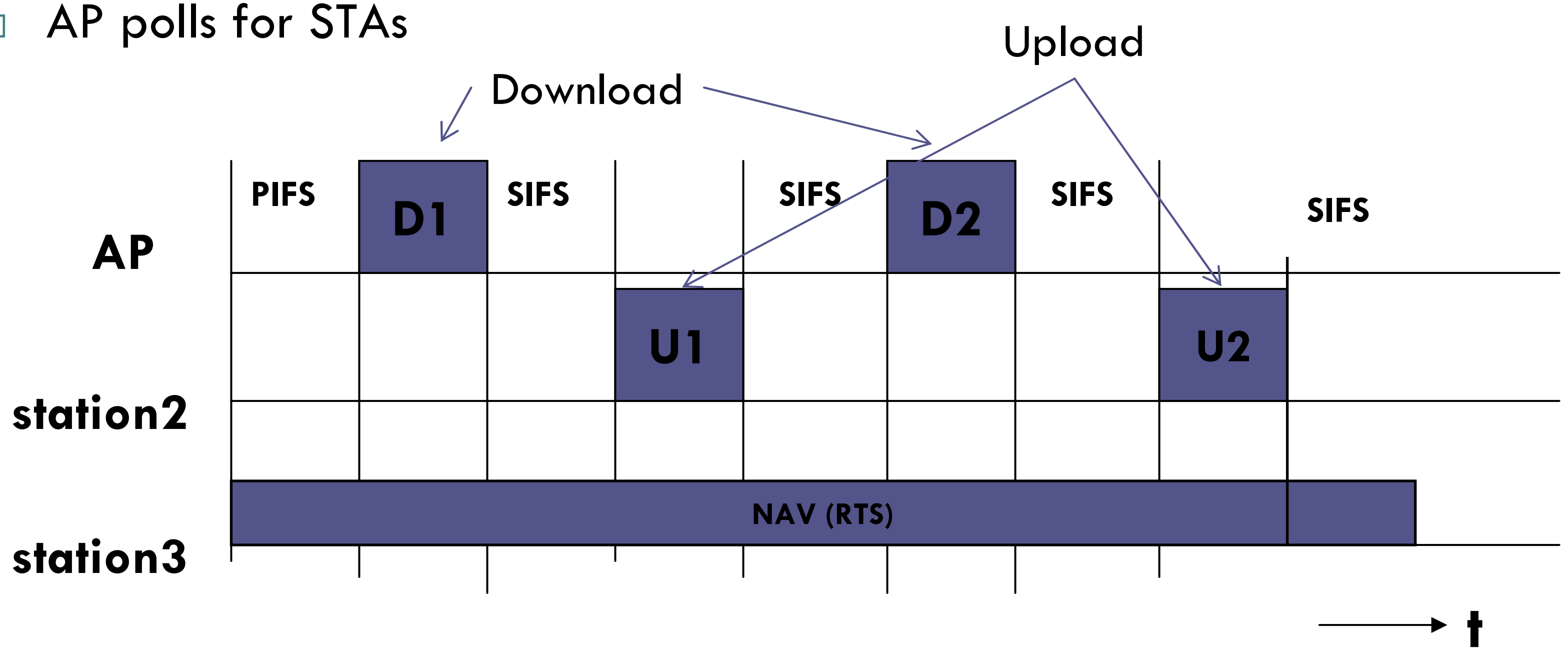


Point Coordination Function (PCF)

- To provide time bounded service.
- Requires an access point.
- Access point polls each station during contention free period (CFP : started by beacon)
- Becomes an overhead during light load

PCF (Contd.)

- AP captures the access right after PIFS period when the medium is free
- PIFS means all RIFS/SIFS is complete, and Contention based DIFS is still counting
- AP polls for STAs



A closer look to the Physical Layer Properties and Interference

Radio Propagation

- Received Signal at distance d from Transmitter is given by:

$$r_i(d) = r(\bar{d}) - \gamma \log_{10}\left(\frac{d}{\bar{d}}\right)$$

$\gamma \cong$ Pathloss exponent (2~6)

$$Outdoor = 2 \sim 4, indoor = 3 \sim 6$$

$\bar{d}$ = reference distance (usually 1m)

r_i = received signal from transmitter i

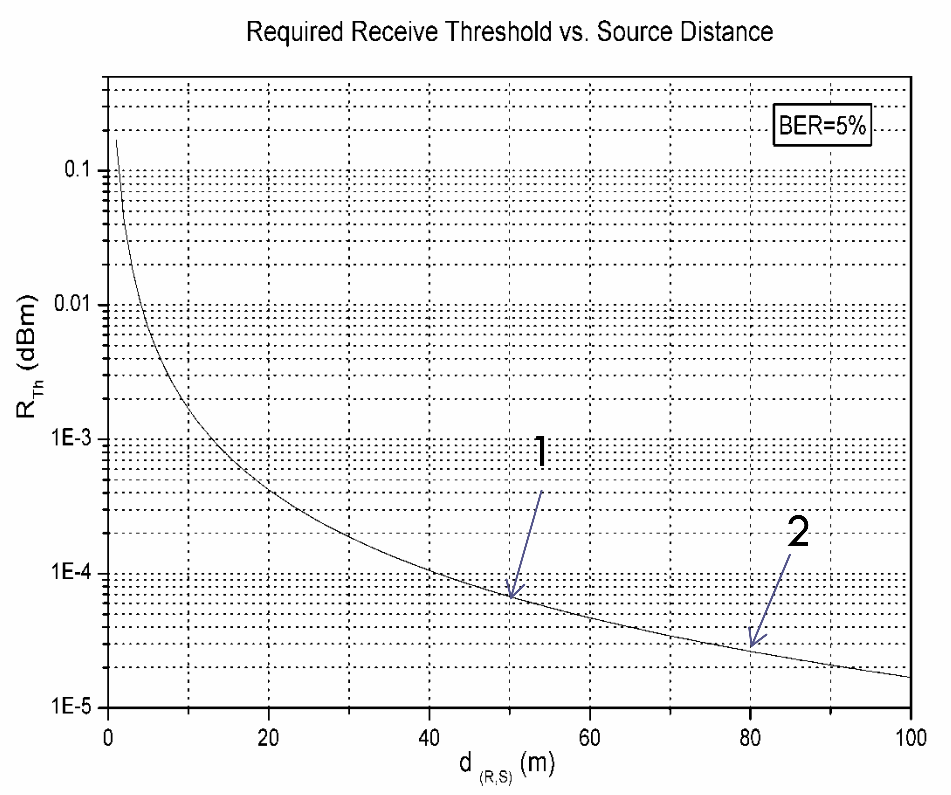
N.B.: The model takes reference distance received signal instead of transmitted signal power

Receiver Sensitivity and Distance

- Signal Strength Decays exponentially as distance increases

- Receiver Sensitivity or Required Receive Threshold determines the Communication Range

- However, this theory is very much simple where there is no additive noise in the channel, or there is no interference at the receiver



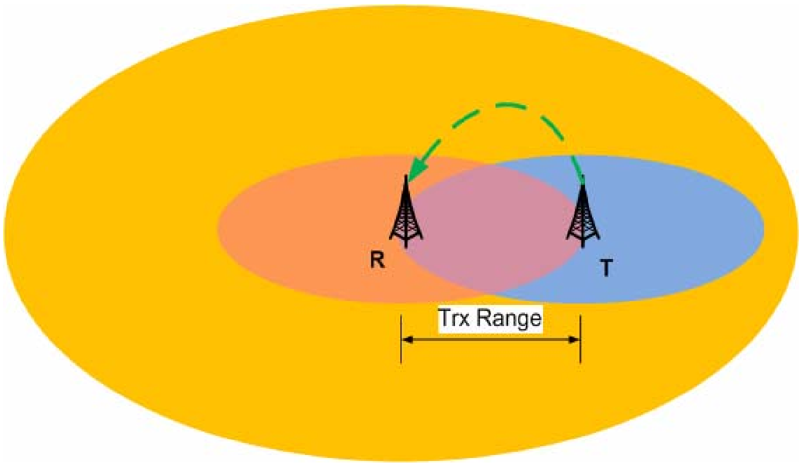
Misconceptions (1)

Misconception: Transmission Range depends on Transmit Power

- High transmit power gives high receive signal strength at far distance

But actually depends on…

- Receiver Sensitivity: Signal Strength at Receiver
- Capture Threshold: If Noise and Interfering Signals are present at Receiver



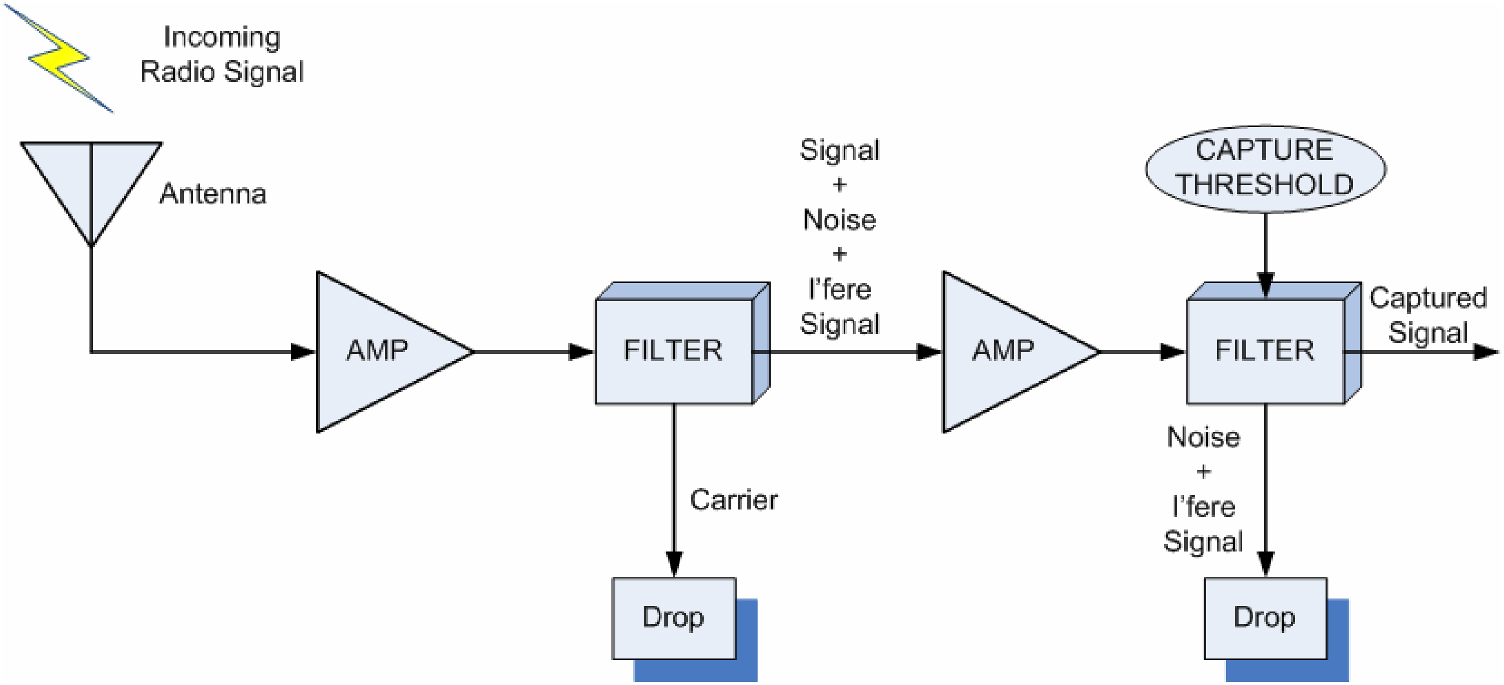
Can be determined for homogeneous stations only, and when no interfering signal is present

Received Signal Capturing

- In practice, wireless channel state varies over time, and it consists of a number of noise sources that add noise
- Transmitted signals from other STAs are also added with intended signal
- **Capture** means Extracting information from received signal from superposed received signal having noise and signals from other STAs (completely depends on receiver circuitry)
- **Capture Threshold** (Receiving Circuitry Property): The minimum **required ratio** of intended signal to noise and interference at which the receiver can capture intended signal

Received Signal Capturing (Contd.)

- Receiver Circuitry and Capture Threshold



Received Signal Capturing (Contd.)

- In general, Signal Capturing is expressed as

$$\frac{r_i}{\sum_{i \neq j} r_j + N} \geq \beta_0$$

$r_i \equiv$ intended signal from STA i

$r_j \equiv$ signal from other STAs

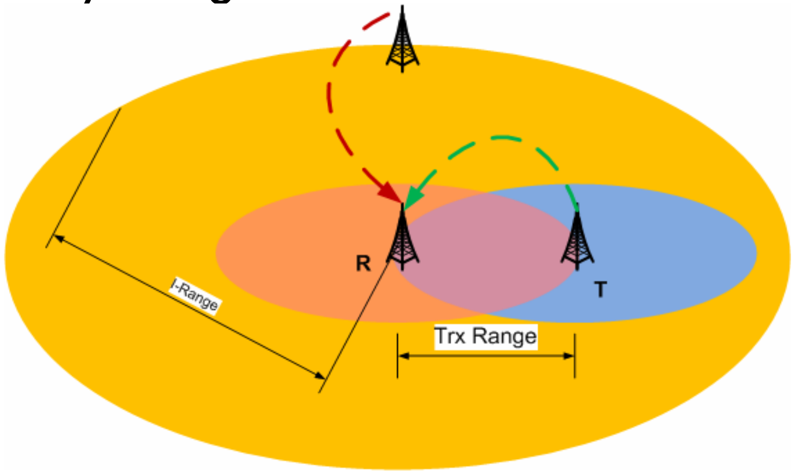
$N \equiv$ Ambient White Noise

$\beta_0 \equiv$ Capture Threshold

- If the SNIR of the received signal is less than Capture Threshold, then the receiver experience **INTERFERENCE** (or **COLLISION** from MAC point of view)

Misconceptions (2):

Misconception: Only Neighbors can Interfere



- Outside the Transmission Range, a node can cause SINR to fall below Capture Threshold
- **Interference Range (I-Range):**
  - When the distance between Sender and Receiver is equal to the Communication (Transmission) Range
  - Maximum distance from where an Interferer can degrade the SINR at Receiver below Capture Threshold

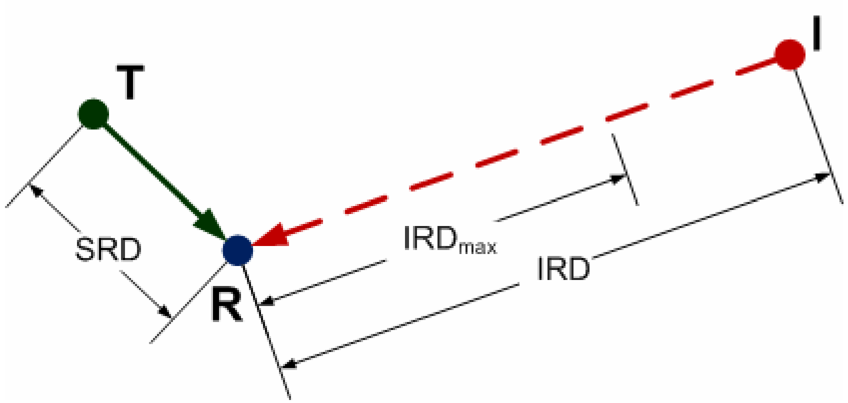
Simple Interference Model

- Interferer 'I' would interfere at 'R' and disrupt the reception of signals transmitted from 'T' if..

$$IRD \leq SRD\left(\frac{r(SRD)}{r(IRD)+N}\right)^{\frac{1}{\gamma}}$$

or,

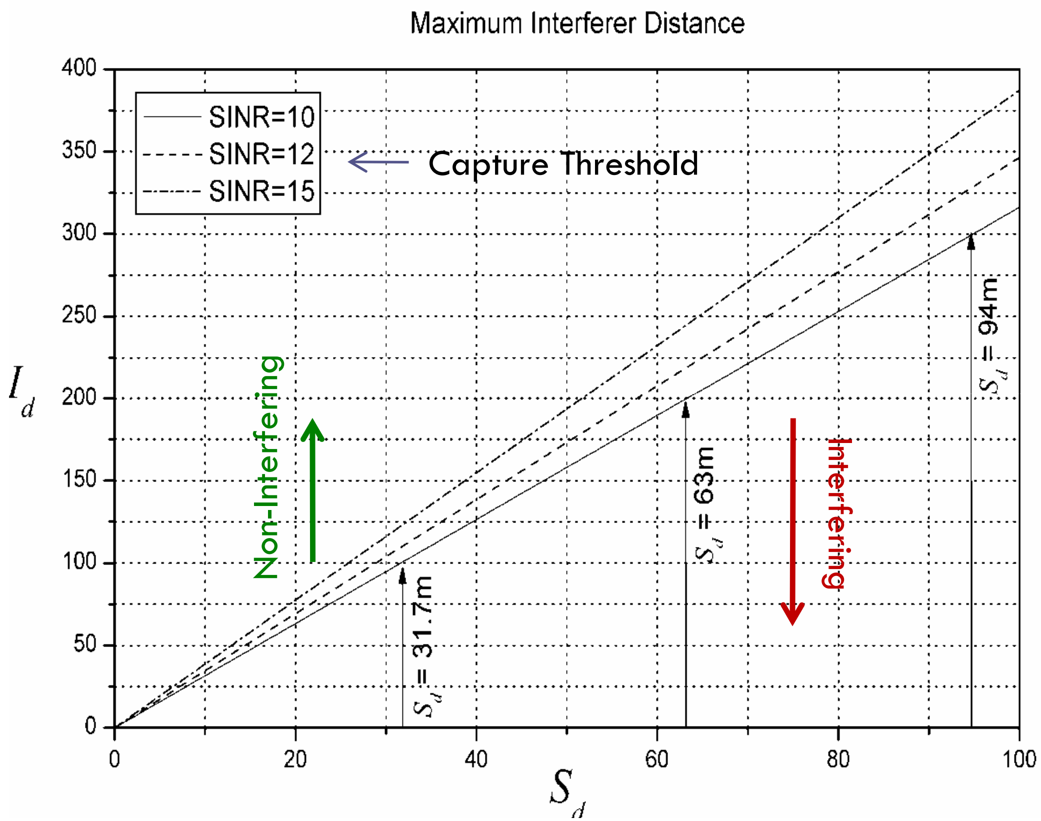
$$IRD \leq SRD \times \beta_0^{\frac{1}{\gamma}}$$



- Angle of arrival is not important excepting the mobility condition

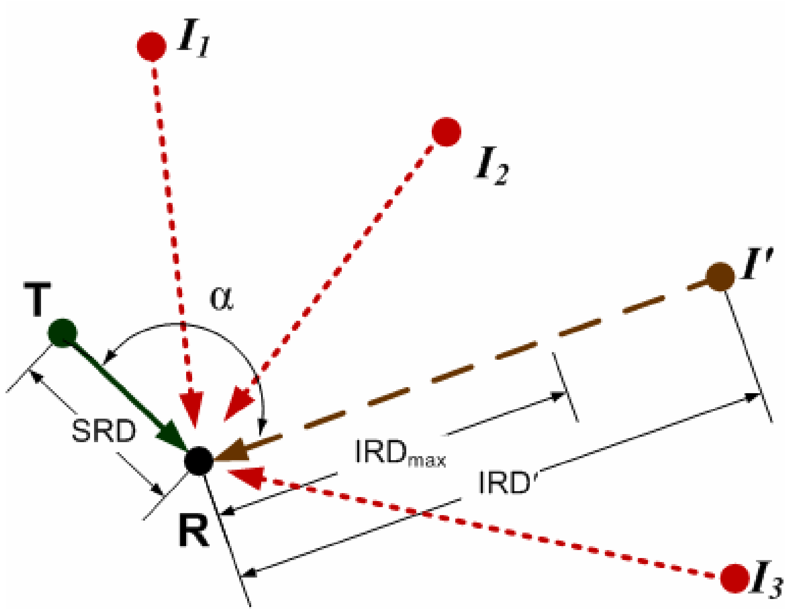
Which STAs can Interfere?

- IRDmax depends on SRD for a given Communication Pair
- Realistic compared to Trx/I'ference Range Concept
- Hard to implement in MAC Protocols, if other stations don't have any knowledge about SRD



General Interference Model

- Multiple Interferers can interferer a reception
- Multiple Interferers can be replaced by a single virtual interferer
- The model becomes simple when virtual interferer is used



IEEE 802.11 Interference Handling

- IEEE 802.11 protocol avoids interference/collisions by means of Carrier Sensing
- A Carrier Sense Threshold (CS Threshold) is used that defines the Interference Range (I-Range), where

  CS Threshold < Receiver Sensitivity

- **Strength:**
  - Before transmitting, each STA can check whether it shall I'fere other communication or not
- **Weakness:**
  - Fixed Interference Range: Unnecessary blocking of a large number of nodes when SRD is smaller than Trans. Range
  - Lower Aggregated Throughput

Challenge

- Enhancement of the DCF protocol for Spatial Reuse of the Channel by..
  - using appropriate (or as close as possible) Interference Ranges, and,
  - reducing number of blocking STAs during an ongoing transmission