18-452/18-750
Wireless Networks and Applications
Lecture 14: Wireless LANs
802.11*

Peter Steenkiste

Spring Semester 2017

http://www.cs.cmu.edu/~prs/wirelessS17/

Outline

- Brief history
- 802 protocol overview
- Wireless LANs – 802.11 – overview
- 802.11 MAC, frame format, operations
- 802.11 management
- 802.11 security
- 802.11 power management
- 802.11*: b/g/a, h, e, n

Some IEEE 802.11 Standards

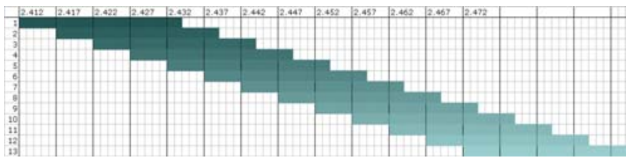
» IEEE 802.11a
  – PHY Standard : 8 channels : up to 54 Mbps : some deployment
» IEEE 802.11b
  – PHY Standard : 3 channels : up to 11 Mbps : widely deployed.
» IEEE 802.11d
  – MAC Standard : support for multiple regulatory domains (countries)
» IEEE 802.11e
  – MAC Standard : QoS support : supported by many vendors
» IEEE 802.11f
  – Inter-Access Point Protocol : deployed
» IEEE 802.11g
  – PHY Standard: 3 channels : OFDM and PBCC : widely deployed (as b/g)
» IEEE 802.11h
  – Suppl. MAC Standard: spectrum managed 802.11a (TPC, DFS): standard
» IEEE 802.11i
  – Suppl. MAC Standard: Alternative WEP : standard
» IEEE 802.11n
  – MAC Standard: MIMO : standardization expected late 2008

IEEE 802.11 Family

Protocol	Release Data	Freq.	Rate (typical)	Rate (max)	Range (indoor)
Legacy	1997	2.4 GHz	1 Mbps	2Mbps	?
802.11a	1999	5 GHz	25 Mbps	54 Mbps	~30 m
802.11b	1999	2.4 GHz	6.5 Mbps	11 Mbps	~30 m
802.11g	2003	2.4 GHz	25 Mbps	54 Mbps	~30 m
802.11n	2008	2.4/5 GHz	200 Mbps	600 Mbps	~50 m

802.11b Channels

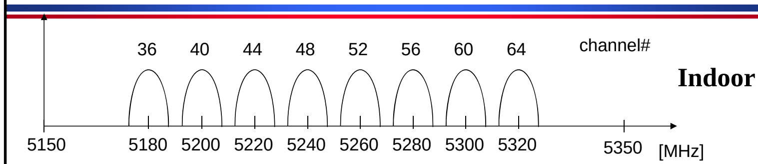
- In the UK and most of EU: 13 channels, 5MHz apart, 2.412 – 2.472 GHz
- In the US: only 11 channels
- Each channel is 22MHz
- Significant overlap
- Non-overlapping channels are 1, 6 and 11



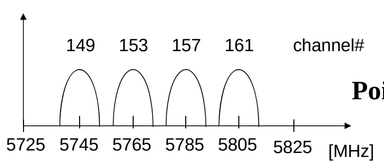
802.11b Physical Layer

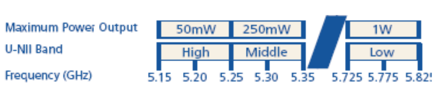
- FHSS (legacy)
  - » 2 & 4 GFSK
  - » Using one of 78 hop sequences, hop to a new 1MHz channel (out of the total of 79 channels) at least every 400milliseconds
- DSSS (802.11b)
  - » DBPSK & DQPSK
  - » Uses one of 11 overlapping channels (22 MHz)
  - » 1 and 2 Mbps: multiply the data by an 11-chip spreading code (Barker sequence)
  - » 5.5 and 11 Mbps: uses Complementary Code Keying (CKK) to generate spreading sequences that support the higher data rates
    - – Spreading code is calculated based on the data bits

802.11a Physical Channels



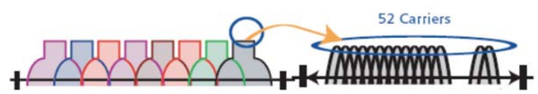
center frequency =
5000 + 5*channel number [MHz]





802.11a Modulation

- Use OFDM to divide each physical channel (20 MHz) into 52 subcarriers (20M/64=312.5 KHz each)
  - » 48 data, 4 pilot



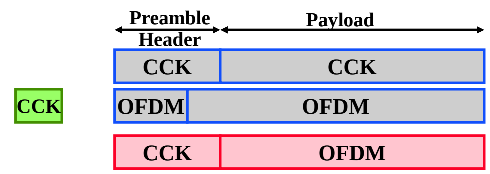
- Adaptive modulation
  - » BPSK: 6, 9 Mbps
  - » QPSK: 12, 18 Mbps
  - » 16-QAM: 24, 36 Mbps
  - » 64-QAM: 48, 54 Mbps

802.11a Discussion

- Uses OFDM in the 5.2 and 5.7 GHz bands
- What are the benefits of 802.11a compared with 802.11b?
  - » Greater bandwidth (up to 54Mb)
    - – 54, 48, 36, 24, 18, 12, 9 and 6 Mbs
  - » Less potential interference (5GHz)
  - » More non-overlapping channels
- But does not provide interoperability with 802.11b, as 802.11g does

Going Faster: 802.11g

- 802.11g basically extends of 802.11b for higher rates – effectively 802.11a at 2.4 GHz
  - » Use the same technology DSSS/CCK for old rates (1,2, 5.5, 11)
  - » Uses 802.11a OFDM technology for new rates (6 Mbs and up)
  - » Using OFDM makes it easier to build 802.11a/g cards
- But it creates an interoperability problem since 802.11b cards cannot interpret OFDM signals
  - » Solutions: send CTS using CCK before OFDM packets in hybrid environments, or use (optional) hybrid packet format



Outline

- Brief history
- 802 protocol overview
- Wireless LANs – 802.11 – overview
- 802.11 MAC, frame format, operations
- 802.11 management
- 802.11 security
- 802.11 power management
- 802.11*: b/g/a, h, e, n

Spectrum and Transmit Power Management (802.11h)

- Support 802.11 operation in 5 GHz band in Europe: coexistence with primary users
  - » Radar: cannot use the band
  - » Satellite: limit power to 3dB below regulatory limit
- Dynamic Frequency Selection (DFS)
  - » Detect primary users and adapt
- Transmit Power Control (TPC)
  - » Goal is to limit interference
- Has broader uses such as range/interference control, reduced energy consumption, automatic frequency planning, load balancing, ..

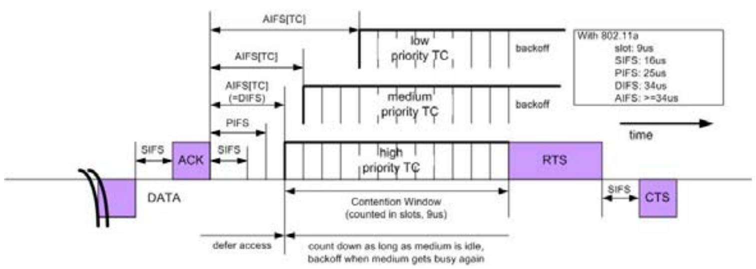
IEEE 802.11e

- Original intent was that 802.11 PCF could be used to provide QoS guarantees
  - » Scheduler in the PCF priorities urgent traffic
  - » But: overhead, “guarantees” are very soft
- 802.11e Enhanced Distributed Coordination Function (EDCF) is supposed to fix this.
  - » Provides Hybrid Coordination Function (HCF) that combines aspects of PCF and DCF
- EDCF supports 4 Access Categories
  - » *AC_BK (or AC0)* for Back-ground traffic
  - » *AC_BE (or AC1)* for Best-Effort traffic
  - » *AC_VI (or AC2)* for Video traffic
  - » *AC_VO (or AC3)* for Voice traffic

Service Differentiation Mechanisms in EDCF

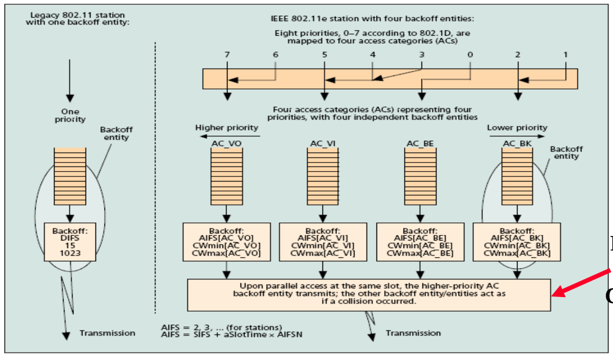
- The two types of service differentiation mechanisms proposed in EDCF are:
- ***Arbitrate Inter-frame Space (AIFS) Differentiation***
  - Different AIFSs instead of the constant distributed IFS (DIFS) used in DCF.
  - Back-off counter is selected from [1, CW[AC]+1] instead of [0,CW] as in DCF.
- Contention Window (CWmin) Differentiation
  - Different values for the minimum/maximum CWs to be used for the back-off time extraction.

IEEE 802.11e: Priorities



Mapping different priority frames to different AC

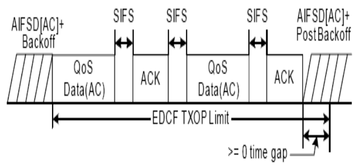
- Each frame arriving at the MAC with a priority is mapped into an AC as shown in figure below.



Resolves Virtual Collisions

Other 802.11 MAC Improvements

- *TXOP- **Transmission opportunity*** **(TXOP) is an interval of time during which a back-off entity has the right to deliver multiple MSDUs.**
  - » A TXOP is defined by its starting time and duration
  - » Announced using a traffic specification (length, period)
  - » Can give more transmission opportunities to a station
  - » Can also limit transmission time (e.g. for low rate stations)
- *CFB-* **In a single TXOP, multiple MSDUs can be transmitted.**
  - » ***"Contention Free Burst" (CFB)***
  - » ***Can use a block acknowledgement***



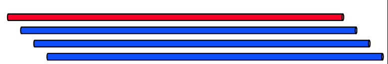
Increasing Capacity: MIMO

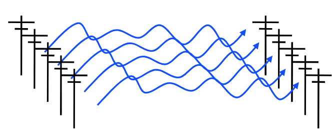
- **Refresher: spatial diversity**
- **Multiple-In Multiple-Out basics**
- **MIMO in 802.11:**
  - » Single user MIMO: 802.11n
  - » Multi user MIMO: 802.11ac

How Do We Increase Throughput in Wireless?

- **Wired world:**

Pull more wires!

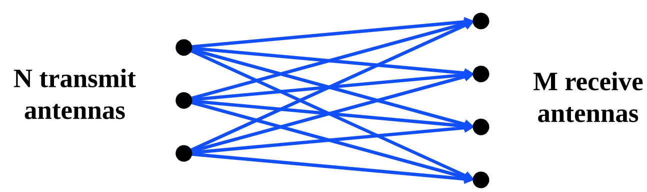




- **Wireless world:**

How about if we could do the same thing and simply use more antennas?

MIMO Multiple In Multiple Out



- **N x M subchannels that can be used to send multiple data streams simultaneously**
- **Fading on channels is largely independent**
  - » Assuming antennas are separate ½ wavelength or more
- **Combines ideas from spatial and time diversity, e.g. 1 x N and N x 1**
- **Very effective if there is no direct line of sight**
  - » Subchannels become more independent

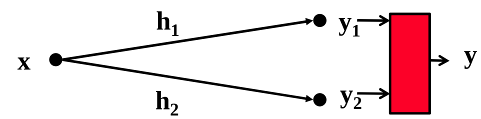
Why So Exciting?

Method	Capacity
SISO	$B \log_2(1 + \rho)$
Diversity (1xN or Nx1)	$B \log_2(1 + \rho N)$
Diversity (NxN)	$B \log_2(1 + \rho N^2)$
Multiplexing	$NB \log_2(1 + \rho)$

Peter A. Steenkiste, CMU

Spatial Diversity

- Use multiple antennas that pick up the signal in slightly different locations
  - Channels uncorrelated with sufficient antenna separation
- Receiver diversity: i x H x P_R = o



$\vec{y} = \vec{h} * x + \vec{n}$

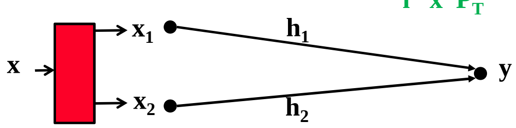
$y = \vec{h}^* * (h * \vec{x} + \vec{n})$

- Receiver can pick strongest signal: y_1 or y_2
- Or combines the signals: multiply $\vec{y}$ with the complex conjugate h^* of the channel vector h
  - Can learn h based on training data

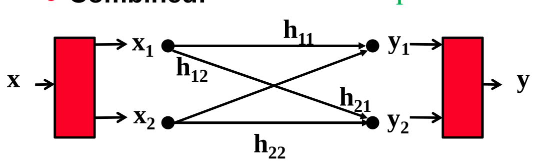
Peter A. Steenkiste, CMU

Other Diversity Options

- Transmit diversity: i x P_T x H = o



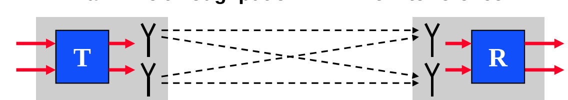
- Combined: i x P_T x H x P_R = o



Peter A. Steenkiste, CMU

MIMO
How Does it Work?

- Transmit and receive <u>multiple data streams</u>
- Coordinate the processing at the transmitter and receiver to overcome channel impairments
  - Maximize throughput or minimize interference



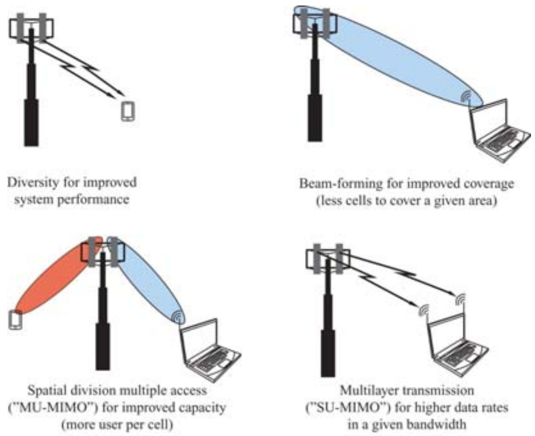
I x P_T x H x P_R = O

Precoding — Channel Matrix — Combining

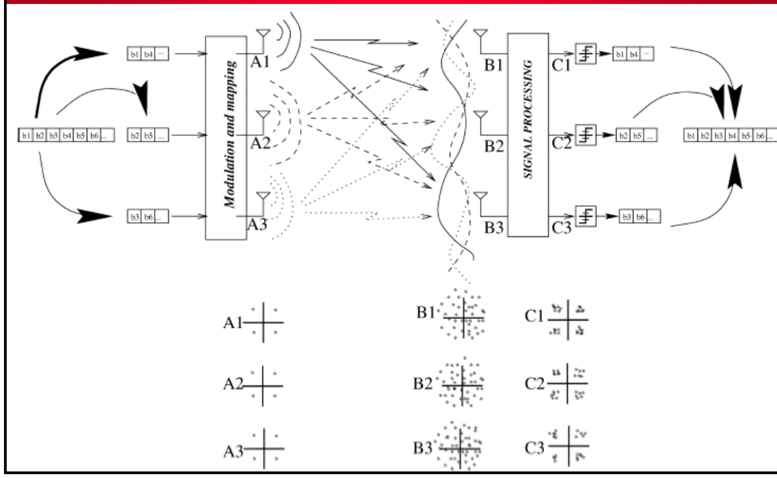
- Combines previous techniques

Peter A. Steenkiste, CMU

Mechanisms Supported by MIMO



An Example of Space Coding



Direct-Mapped NxM MIMO

Effect of transmission $\underset{M}{\vec{R}} = \underset{MxN}{H} * \underset{N}{\vec{C}} + \underset{M}{\vec{N}}$

Decoding $\underset{D}{\vec{O}} = \underset{DxM}{P_R} * \underset{M}{\vec{R}}$ $\underset{N}{\vec{C}} = \underset{N}{\vec{I}}$

Results $\vec{O} = P_R * H * \vec{I} + P_R * \vec{N}$

- How do we pick P_R ? "Inverse" of H: H^{-1}
  - » Equivalent of nulling the interfering possible (zero forcing)
  - » Only possible if the paths are completely independent
- Noise amplification is a concern if H is non-invertible – its determinant will be small
  - » Minimum Mean Square Error detector balances two effects

Precoded NxM MIMO

Effect of transmission $\underset{M}{\vec{R}} = \underset{MxN}{H} * \underset{N}{\vec{C}} + \underset{M}{\vec{N}}$

Coding/decoding $\underset{D}{\vec{O}} = \underset{DxM}{P_R} * \underset{M}{\vec{R}}$ $\underset{N}{\vec{C}} = \underset{NxD}{P_T} * \underset{D}{\vec{I}}$

Results $\vec{O} = P_R * H * P_T * \vec{I} + P_R * \vec{N}$

- How do we pick P_R and P_T ?
- Singular value decomposition of H = U * S * V
  - » U and V are unitary matrices – $U^{H} * U = V^{H} * V = I$
  - » S is diagonal matrix

MIMO Discussion

- Need channel matrix H: use training with known signal
- So far we have ignored multi-path
  - » Each channel is multiple paths with different properties
  - » Becomes even messier!
- MIMO is used in 802.11n
  - » Can use two adjacent non-overlapping “WiFi channels”
  - » Raises lots of compatibility issues
  - » Potential throughputs of 100s of Mbps
- Focus is on maximizing throughput between two nodes
  - » Is this always the right goal?

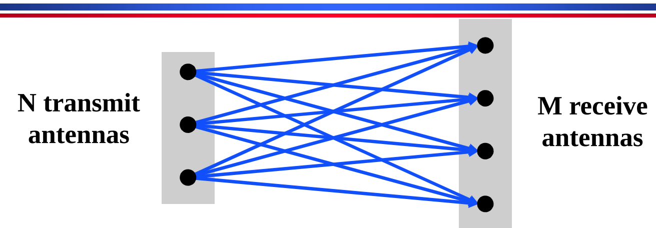
802.11n Overview

- 802.11n extends 802.11 for MIMO
  - » Supports up to 4x4 MIMO
  - » Preamble that includes high throughput training field
- Standardization was completed in Oct 2009, but, early products have long been available
  - » WiFi alliance started certification based on the draft standard in mid-2007
- Supported in both the 2.4 and 5 GHz bands
  - » Goal: typical indoor rates of 100-200 Mbps; max 600 Mbps
- Use either 1 or 2 non-overlapping channels
  - » Uses either 20 or 40 MHz
  - » 40 MHz can create interoperability problems
- Supports frame aggregation to amortize overheads over multiple frames
  - » Optimized version of 802.11e

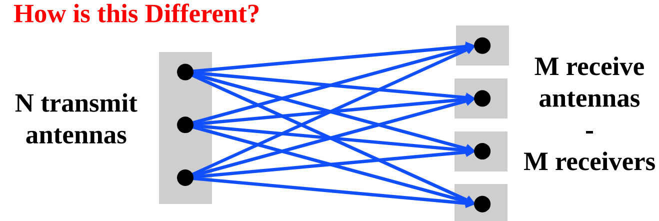
802.11n Backwards Compatibility

- 802.11n can create interoperability problems for existing 802.11 devices (abg)
  - » 802.11n does not sense their presence
  - » Legacy devices end up deferring and dropping in rate
- Mixes Mode Format protection embeds an n frame in a g or a frame
  - » Preamble is structured so legacy systems can decode header, but MIMO can achieve higher speed (training, cod/mod info)
  - » Works only for 20 MHz 802.11n use
  - » Only deals with interoperability with a and g – still need CTS protection for b
- For 40 MHz 802.11n, we need CTS protection on both the 20 MHz channels – similar to g vs. b
  - » Can also use RTS/CTS (at legacy rates)
  - » Amortize over multiple transmissions

MIMO in a Network Context

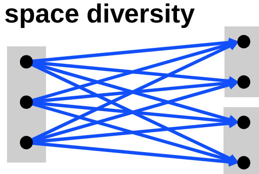


How is this Different?



Multi-User MIMO Discussion

- Math is similar to MIMO, except for the receiver processing (P_R)
  - » Receivers do not have access to the signals received by antennas on other nodes
  - » Limits their ability to cancel interference and extract a useful data stream
  - » Closer to transmit MRC
- MU-MIMO versus MIMO is really a tradeoff between TDMA and use of space diversity
  - » Sequential short packets versus parallel long packets
- Why not used in 802.11?



Multi-User MIMO Up versus Down Link

- Uplink: Multiple Access Channel (MAC)
  - » Multiple clients transmit simultaneously to a single base station
  - » Requires coordination among clients on packet transmission – hard problem because very fine-grained
- Downlink: Broadcast Channel (BC)
  - » Base station transmit separate data streams to multiple independent users
  - » Easier to do: closer to traditional models of having each client receive a packet from the base station independently

802.11ac Multi-user MIMO

- Extends beyond 802.11n
  - » MIMO: up to 8 x 8 channels (vs. 4 x 4)
  - » More bandwidth: up to 160 MHz by bonding up to 8 channels (vs. 40 MHz)
  - » More aggressive signal coding: up to 256 QAM (vs. 64 QAM); both use 5/6 coding rate (data vs. total bits)
  - » Uses RTS-CTS for clear channel assessment
  - » Multi-gigabit rates (depends on configuration)
- Support for multi-user MIMO on the downlink
  - » Can support different frames to multiple clients at the same time
  - » Especially useful for smaller devices, e.g., smartphones
  - » Besides beam forming to target signal to device, requires also nulling to limit interference

802.11ad 60 GHz WiFi

- Uses a new physical layer definition specifically for 60 GHz band
  - » Very different signal propagation properties
  - » Does not penetrate walls, but does work with reflections
  - » Shorter distances
  - » Small antennas and good beamforming properties
- Defined up to 7 Gbps
- Has been used for point-point links for a while
  - » APs now available
  - » Combined with other 802.11 versions
  - » 802.11ad only available for short distances