

15-496 : A Hand-on Introduction to Wireless Networks

Lecture 7: 802.11 abg

Peter Steenkiste
 Departments of Computer Science and
 Electrical and Computer Engineering
 Spring Semester 2008
<http://www.cs.cmu.edu/~prs/wireless08/>

Peter A. Steenkiste, CMU

1

Announcements

- Quiz on Thursday
 - » Lectures 1-5
 - » 30 minutes at the end of the lecture slot
- Assignment 2 is out
 - » Send e-mail if you have questions
- Project proposals

Peter A. Steenkiste, CMU

2

Outline

- Brief history
- 802 protocol overview
- Wireless LANs – 802.11
 - » Overview of 802.11
 - » 802.11 MAC, frame format, operations
 - » 802.11 management
 - » 802.11*
- Wireless Access – 802.16
- Personal Area Networks – 802.15
- Special topics

Peter A. Steenkiste, CMU

3

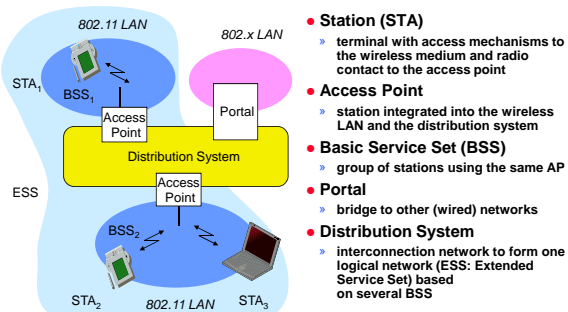
Management and Control Services

- Association management
- Handoff
- Power management
- Security: authentication and privacy
- QoS

Peter A. Steenkiste, CMU

4

802.11: Infrastructure Reminder



Peter A. Steenkiste, CMU

5

Service Set Identifier - SSID

- Mechanism used to segment wireless networks
 - » Multiple independent wireless networks can coexist in the same location
 - » Effectively the name of the wireless network
- Each AP is programmed with a SSID that corresponds to its network
- Client computer presents correct SSID to access AP
- Security Compromises
 - » AP can be configured to "broadcast" its SSID
 - » Broadcasting can be disabled to improve security
 - » SSID may be shared among users of the wireless segment

Peter A. Steenkiste, CMU

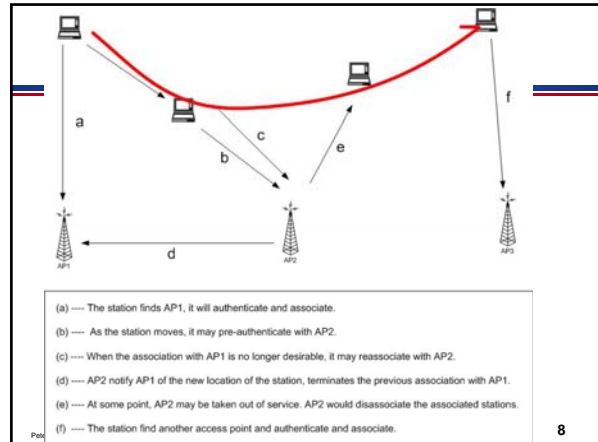
6

Association Management: Scanning, and Joining

- **Station must associate with an AP before they can use the network**
 - › AP must know about them so it can forward packets
- **Reassociation: association is transferred**
 - › Supports mobility in the same ESS
- **Disassociation: station or AP can terminate association**
- **Stations can detect AP based by scanning**
 - › **Passive Scanning:** station simply listens for Beacon and gets info of the BSS. Power is saved.
 - › **Active Scanning:** station transmits Probe Request; elicits Probe Response from AP. Saves time.
- **Joining a BSS**
 - › Synchronization in Timestamp Field and frequency
 - › Adopt PHY parameters
 - › Other parameters: BSSID, WEP, Beacon Period, etc.

Peter A. Steenkiste, CMU

7



Peter A. Steenkiste, CMU

8

Power Management

- **Goal is to enhance battery life of the stations**
- **Idle receive state dominates LAN adapter power consumption over time**
- **Allow stations to power off their NIC while still maintaining an active session**
- **Different protocols are used for infrastructure and independent BSS**
 - › Our focus is on infrastructure mode

Peter A. Steenkiste, CMU

9

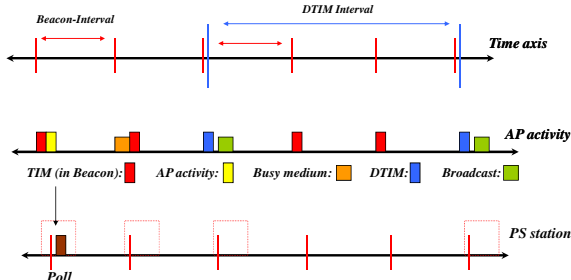
Power Management Approach

- **Idle station to go to sleep**
- **AP keeps track of stations in Power Savings mode and buffers their packets**
 - › Traffic Indication Map (TIM) is included in beacons to inform which power-save stations have packets waiting at the AP
- **Power Saving stations wake up periodically and listen for beacons**
 - › If they have data waiting, they can send a PS-Poll to request that the AP sends their packets
- **TSF assures AP and stations are synchronized**
 - › Synchronizes clocks of the nodes in the BSS
- **Broadcast/multicast frames are also buffered at AP**
 - › Sent after beacons that includes Delivery Traffic Indication Map (DTIM)
 - › AP controls DTIM interval

Peter A. Steenkiste, CMU

10

Infrastructure Power Management Operation



Peter A. Steenkiste, CMU

11

WLAN Security Requirements

- **Authentication: only allow authorized stations to associate with and use the AP**
- **Confidentiality: hide the contents of traffic from unauthorized parties**
- **Integrity: make sure traffic contents is not modified while in transit**

Peter A. Steenkiste, CMU

12

Security in 802.11b

- **WEP: Wired Equivalent Privacy**
 - › Achieve privacy similar to that on LAN through encryption
 - › Intended to provide both privacy and integrity
 - › RC4 and CRC32
 - › Has known vulnerabilities
- **WPA: Wi-Fi Protected Access**
 - › Larger, dynamically changed keys
- **802.1x: port-based authentication for LANs**
 - › Port-based authentication for LANs
- **802.11i (WPA2)**
 - › Builds on WPA
 - › Uses AES for encryption

Peter A. Steenkiste, CMU

13

WLAN Security Exploits

- **Insertion attacks**
 - › Unauthorized Clients or AP
- **Client-to-Client Attacks**
 - › DOS - duplicate MAC or IP addresses
 - › Can also be used to get free service on "secured" APs
- **Interception and unauthorized monitoring**
 - › Packet Analysis by "sniffing" – listening to all traffic
- **Jamming – denial of service**
 - › Cordless phones, baby monitors, leaky microwave oven, etc.

Peter A. Steenkiste, CMU

14

WLAN Security Exploits

- **Brute Force Attacks Against AP Passwords**
 - › Dictionary Attacks Against SSID
- **Encryption Attacks**
 - › Exploit known weaknesses of WEP
- **Misconfigurations**
 - › APs ship in an unsecured configuration
 - › Many people use APs with default configuration

Peter A. Steenkiste, CMU

15

MAC Filtering

- Each client identified by its 802.11 NIC Mac Address
- Each AP can be programmed with the set of MAC addresses it accepts
- Combine this filtering with the AP's SSID
- Overhead of maintaining list of MAC addresses
- But it is possible to forge MAC addresses ...

Peter A. Steenkiste, CMU

16

Wired Equivalent Privacy WEP

- **Employs RC4 to Encrypt/Decrypt data**
 - › RC4 is a stream cypher based on a symmetric algorithm
 - › 40 bit encryption key is supplied by the user
 - › 24 bit initialization vector (IV) is supplied in the header
 - › 64 bit string is seed for PRNG to generate a "key sequence"
 - › 40 and 64 bit WEP are the same thing
- **ICV (integrity check value) is computed for plaintext (CRC-32)**
- **ICV is appended to plaintext to create data string**
- **Key Sequence is XORed to data string to create ciphertext**
- **Ciphertext and IV are sent to receiver**
- **128-bit encryption uses a 104+24 bit key**

Peter A. Steenkiste, CMU

17

WEP-Based Security Discussion

- **WEP has known vulnerabilities**
- **Key can be cracked with a couple of hours of computing**
 - › IV transmitted in the clear
 - › No protocol for encryption key distribution
 - › Clever optimizations can reduce time to minutes
- **All data then becomes vulnerable to interception**
 - › WEP typically uses a single shared key for all stations
- **The CRC32 check is also vulnerable so that the data could be altered as well**
 - › Can make changes without even decrypting!
- **128-bit WEP encryption is recommended**

Peter A. Steenkiste, CMU

18

WEP Authentication

- Access request by client
- Challenge text sent to client by AP
- Challenge text encoded by client using shared secret then sent to AP
- If challenge text encoded properly, AP allows access; else access is denied

Peter A. Steenkiste, CMU

19

Wi-Fi Protected Access WPA

- Introduced by Wi-Fi Alliance as an interim solution after WEP flaws were published
 - › Uses a different Message Integrity Check
 - › Encryption still based on RC4, but uses 176 bit key (48bit IV) and keys are changed periodically
 - › Also frame counter in MIC to prevent replay attacks.
- Can be used with 802.1x authentication (optional)
 - › It generates a long WPA key that is randomly generated, uniquely assigned and frequently changed.
 - › Attacks are still possible since people sometimes use short, poorly random WPA keys that can be cracked
- 802.11i is a “permanent” security fix
 - › Builds on the interim WPA standard (i.e. WPA2)
 - › Replaces RC4 by the more secure Advanced Encryption Standard (AES) block encryption
 - › Better key management and data integrity
 - › Uses 802.1x for authentication.

Peter A. Steenkiste, CMU

20

Port-based Authentication

- 802.1x is the IEEE standard for port-based authentication
- Users get a username/password to access the access point
- Was originally defined for switches but extended to APs
- Can be used to bootstrap other security mechanisms
 - › Effectively creating a session

Peter A. Steenkiste, CMU

21

Best Practices for WiFi Security

- Use WEP
 - › But change default key and change WEP key frequently
 - › Better than no security plus some possible legal benefits
- Change the default configuration of your AP:
 - › Change default passwords on APs
 - › Don't name your AP by brand name
 - › Don't name your AP by model #
 - › Change default SSID
- Use MAC filtering if available
- Use a VPN
 - › Must assume that wireless segment is untrusted
 - › Provides end-to-end encryption

Peter A. Steenkiste, CMU

22

Wardriving

- The act of locating and possibly exploiting to a wireless network while driving around a city
- You need a vehicle, a laptop, a wireless PC card and some kind of antenna
- People can intercept your wireless signal when the signal exceeds your building
- <http://www.wardriving.com>
- Is this legal??

Peter A. Steenkiste, CMU

23

Outline

- Brief history
- 802 protocol overview
- Wireless LANs – 802.11
 - › Overview of 802.11
 - › 802.11 MAC, frame format, operations
 - › 802.11 management
 - › 802.11*
- Wireless Access – 802.16
- Personal Area Networks – 802.15
- Cellular technologies

Peter A. Steenkiste, CMU

24

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

Peter A. Steenkiste, CMU

25

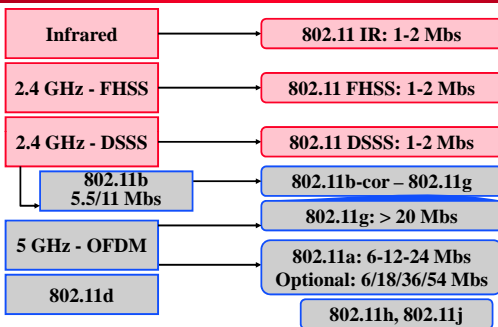
IEEE 802.11 Family

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

Peter A. Steenkiste, CMU

26

Physical Layer

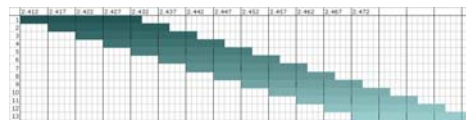


Peter A. Steenkiste, CMU

27

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



Peter A. Steenkiste, CMU

28

802.11b Physical Layer

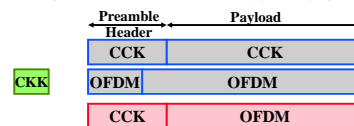
- FHSS (legacy)
 - » 2 & 4GFSK
 - » Using one of 78 hop sequences, hop to a new 1MHz channel (out of the total of 79 channels) at least every 400milliseconds
- DSSS (802.11b)
 - » DBPSK & DQPSK
 - » Uses one of 11 overlapping channels (22 MHz)
 - » 1 and 2 Mbps: multiply the data by an 11-chip spreading 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

Peter A. Steenkiste, CMU

29

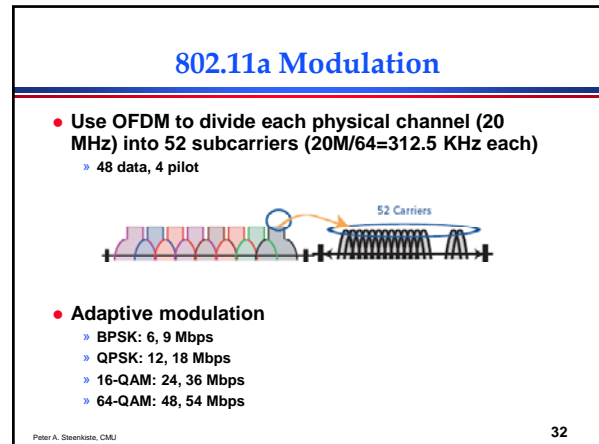
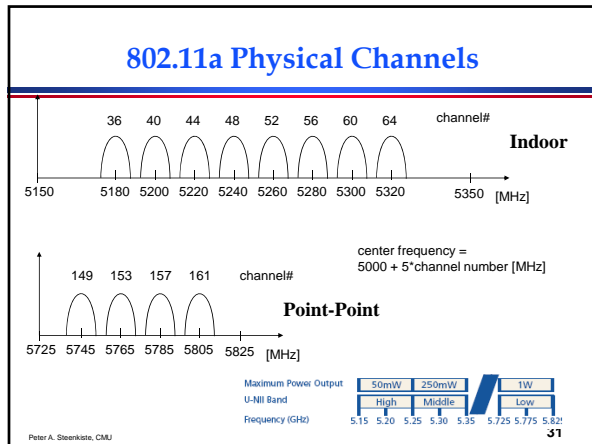
Going Faster: 802.11g

- 802.11g basically extends of 802.11b
 - » Use the same technology DSSS/CCK for lower rates
 - » Uses OFDM technology for rates > 20 Mbps
- Using OFDM makes it easier to build 802.11a/g cards
 - » Since 802.11a uses OFDM
- 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



Peter A. Steenkiste, CMU

30



- ### 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
- 33

- ### 802.11 Physical Layer Discussion
- Antenna diversity is very common
 - » Can significantly reduce the effect of multipath
 - RTS/CTS is almost never used
 - » Overhead is too high compared with benefit
 - Two key parameters are the transmit power and the Clear Channel Assessment (CCA) threshold
 - » The two parameters have impact on the hidden and exposed terminal problem
 - » With default settings, in most deployments, exposed terminals are a more common than hidden terminals
 - Transmit power is pretty high while CCA is pretty sensitive
 - Receive threshold controls what packets you will hear or ignore
- 34

- ### 802.11n
- 802.11n extends 802.11 for MIMO
 - Standardization is still ongoing, but early products are on the market
 - » Supported in both the 2.4 and 5 GHz bands
 - » Goal: typical indoor rates of 100-200 Mbps; max 600 Mbps
 - Early products typically use either 1 or 2 non-overlapping channels
 - » Maximum rate with 2 overlapping channels is ~300 Mbs
 - » Not clear what you get in practice
 - Tests have created interoperability problems for existing 802.11 devices
 - » 802.11n does not sense their presence
 - » Legacy devices end up deferring and dropping in rate
- 35

- ### 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
- 36

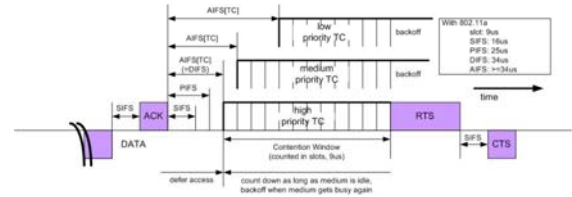
Service Differentiation Mechanisms in EDCF

- 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.

Peter A. Steenkiste, CMU

37

IEEE 802.11e: Priorities

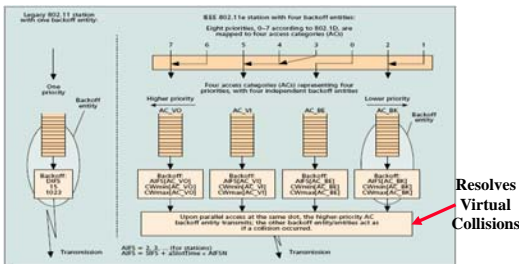


Peter A. Steenkiste, CMU

38

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.

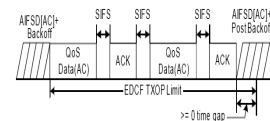


Peter A. Steenkiste, CMU

39

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 MSDUs.
 - » A TXOP is defined by its starting time and duration
- **CFB- In a single TXOP, multiple MSDUs can be transmitted.**
 - » "Contention Free Burst" (CFB)



Peter A. Steenkiste, CMU

40