Episode 3: WLAN

Hannes Frey and Peter Sturm
University of Trier

Outline

802.11

- Most rapid growth of all wireless technologies
- Expected market growth
  - $ 1.79 billion (2001)
  - $ 3.85 billion (2004)
- More than 70% of all notebooks with 802.11 already embedded (2004)
- Wireless hotspots begin to pervade

Hotspots in Germany (January 2004)

www.regtp.de

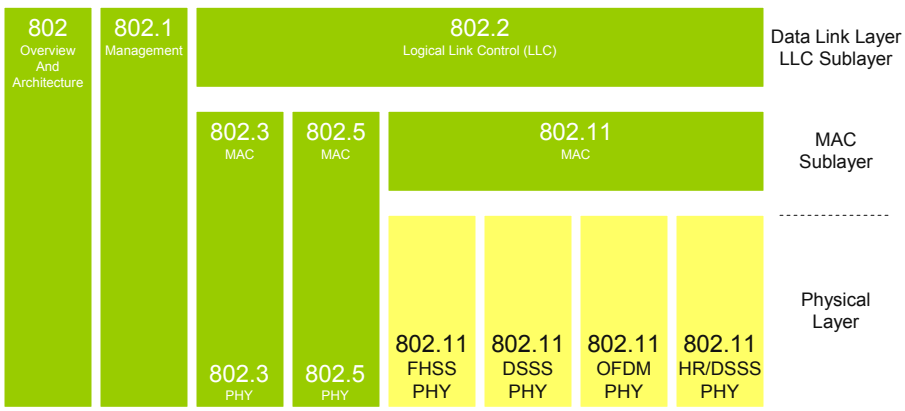
Applications

- Primary domain is traditional networking at home and in the office
- Wireless video connections between set-top boxes and TV sets
- Video streaming from camcorder/camera to TV set and/or PC
- Exchange & transmission of audio (network radio)
- Wide-area mobile networks (not intended)
- Others?

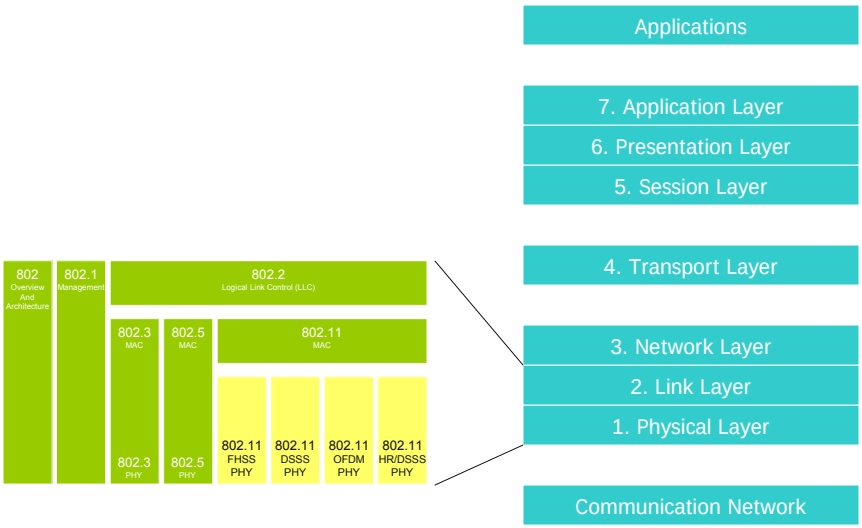
802.11 extensions

- 802.11
  - original standard provided for 1- and 2-Mbps PHY layer, CSMA/CA (1997)
- 802.11a
  - Enhancement to provide 54 Mbps in the 5 GHz band (1999)
- 802.11b
  - Enhancement to provide 11 Mbps in the 2.4 GHz band (1999)
- 802.11d
  - Changes for international regulatory compliance (2001)
- 802.11e
  - Enhancements to the MAC layer to provide QoS through prioritized CSMA and advanced polling techniques
- 802.11f
  - Recommended practices for inter-access point communication
- 802.11g
  - PHY layer enhancement to provide 54 Mbps in the 2.4 GHz band
- 802.11h
  - Enhancement to 802.11a to achieve regulatory compliance with Europe
- 802.11i
  - Security enhancement
- 802.11j
  - Changes to meet Japanese regulatory requirements
- 802.11k
  - Improved WLAN system management
- 802.11m
  - A generalized cleanup and editing of the existing standard
- 802.11?
  - More than 100 Mbps throughput

IEEE 802 family

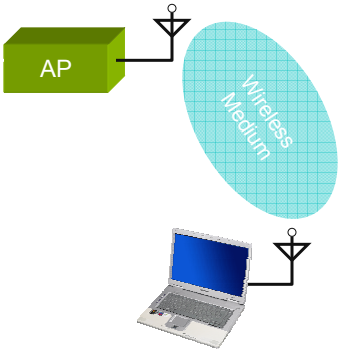


Relation to the OSI model



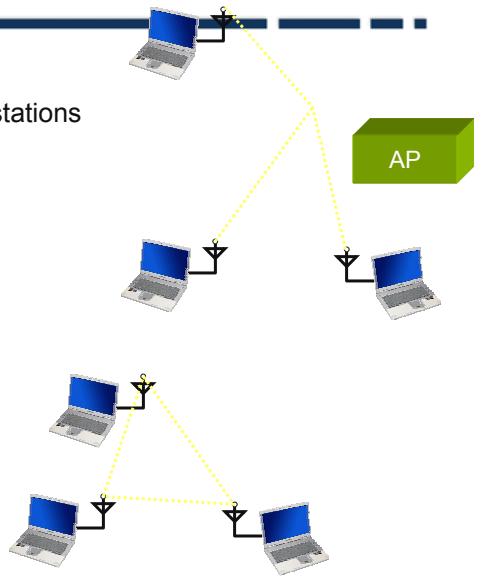
Major components

- Station
  - Computing device with wireless network interface
- Wireless medium
  - Radio frequency (RF) physical layer for communication
- Access point (AP)
  - Frame conversion
  - Wireless-to-wireless bridging
  - Wireless-to-wired bridging
- Distribution system
  - Forwarding frames from access point to access point



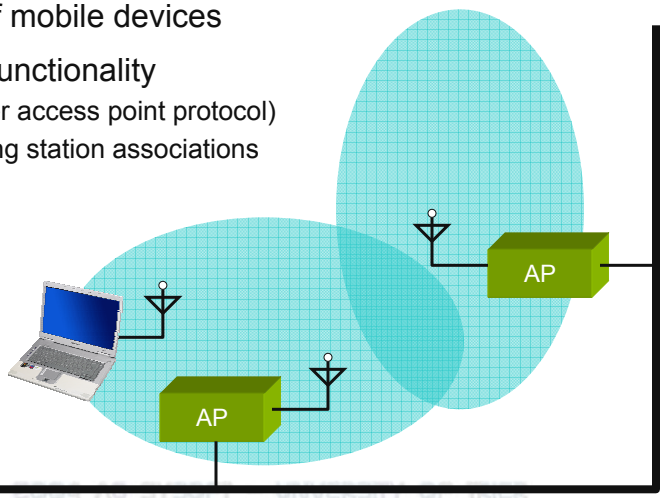
Network types

- Basic service set (BSS)
  - A group of communicating stations
- With access point
  - Infrastructure network
  - Infrastructure BSS
- Without access point
  - Independent network
  - Independent BSS (IBSS)
  - Ad hoc networks



Extended service sets

- Bridging between APs
- Roaming of mobile devices
- Additional functionality
  - IAPP (Inter access point protocol)
  - Exchanging station associations with AP



UBICOMP

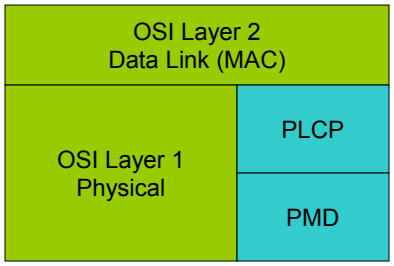
3.1 PHY Layer

Problems in wireless communication

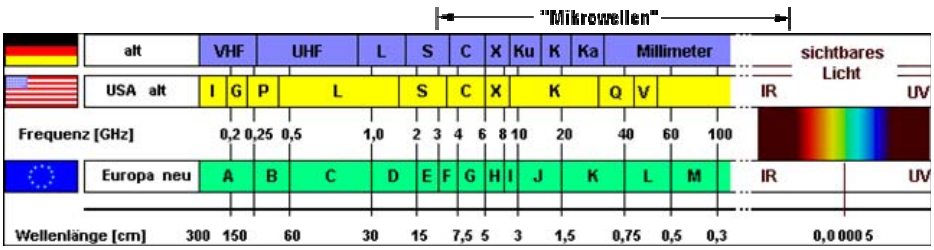
- Available unlicensed spectrum allocation (government regulation)
- Only low transmission power levels allowed (No brute force possible: strong signal in narrow band)
- Multi-path echoes
- Interference
- Noise

Physical layer architecture

- MAC Preamble (like in Ethernet)
  - Synchronize clocks
- Two sublayer
  - PLCP – Physical layer convergence procedure
  - PMD – Physical medium dependet
- Modulation-dependent preamble by PLCP
- Clear channel assessment (CCA)
  - Indication to MAC whether channel is free or not

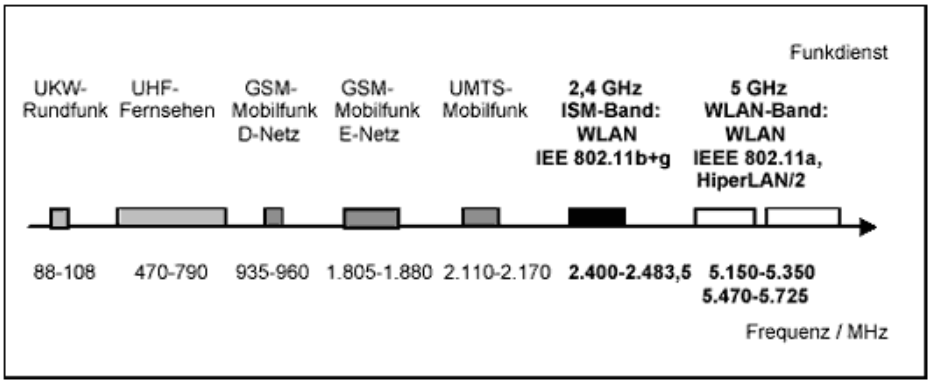


Radio frequencies



- Regulated by governments
  - FCC in the US
  - RegTP in Germany (Frequenznutzungsplan, > 600 pages)
- Unlicensed ISM bands
  - Industry Scientific Medicine

Frequencies for mobile communication

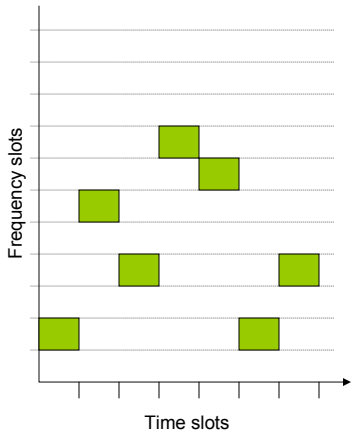


802.11 Modulation techniques

- Spreading spectrum
  - No narrow band transmission
  - Smearing of transmission into broad frequency band
    - Defined by mathematical functions
    - Required for unlicensed frequencies
- Expansion of input data stream (redundancy)
  - Error correction
- Complex transformation from data to transmission signal
  - FHSS (Frequency hopping spread spectrum)
  - DSSS (Direct sequence spread spectrum)
  - OFDM (Orthogonal frequency division multiplexing)

Frequency hopping

- Simple to implement, cheap
- Frequency changes in predetermined pseudorandom pattern
- No FDMA
  - FDMA = Assignment device depedent (for multiple access)
  - FH = Time dependet
- Time slot = Dwell time
- Non-overlapping sequences (orthogonal)
- 2 Mbps possible (802.11b)



Joining FH networks

- Functions to derive the hopping sequence are part of the specification
- Subdivision into non-overlapping sets
- Sets contain only orthogonal hopping sequences
- Sets contain between 23 and 35 sequences (depends on the country)
- Beacons carry required information for the devices

Modulation

- Gaussian frequency shift keying (GFSK)
  - Data encoded as series of frequency changes in a carrier
  - Relatively immune to noise
  - Gaussian refers to the shape of radio pulses
- 2-Level GFSK
  - Two frequencies for 0 and 1
  - Symbol rate about 1-2 million on a 2.4 Ghz carrier
- 4-Level GFSK
  - 4 discrete frequencies

Discrete sequence

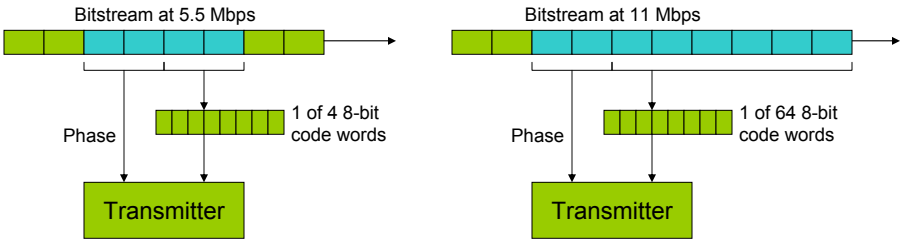
- Higher data rates possible than in FH
- Smear RF energy over a wider frequency band
  - More radio spectrum needed
- Chips = additional code to transmit data
  - typically, 1 data bit requires more than 1 chip
  - Coding appears as pseudorandom noise code
- DS uses Barker code
  - 0 is encoded into 10110111000
  - 1 is encoded into 01001000111
- Signal spread among 14 channels (each 5 MHz wide)

Modulation

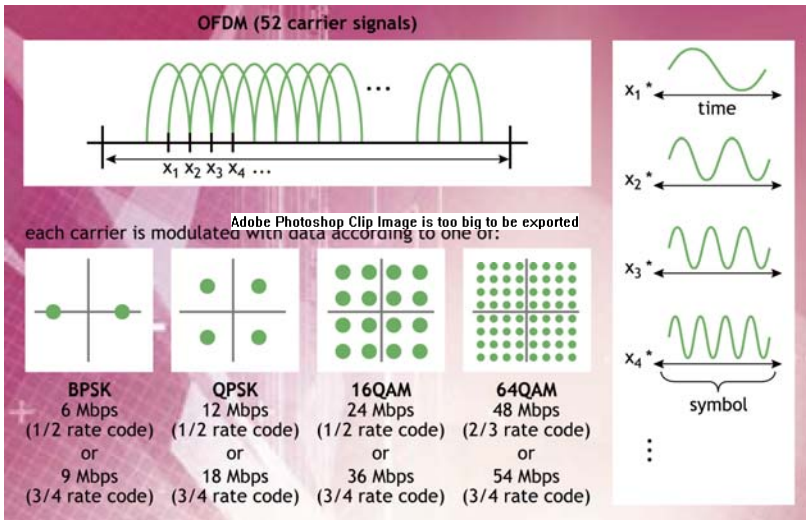
- Differential phase shift keying (DPSK)
- Variants
  - DBPSK (Differential binary PSK)
    - 0 uses phase shift 0
    - 1 uses phase shift π
  - DQPSK (Differential quadrature binary PSK)
    - 00 uses phase shift 0
    - 01 uses phase shift π/2
    - 10 uses phase shift π
    - 11 uses phase shift 1.5 π

HR/DSSS PHY (High data rates)

- Used in 802.11b
- Increasing number of smaller phase shifts hard to implement and even harder to recognize
- Alternative: CCK (Complementary code keying)



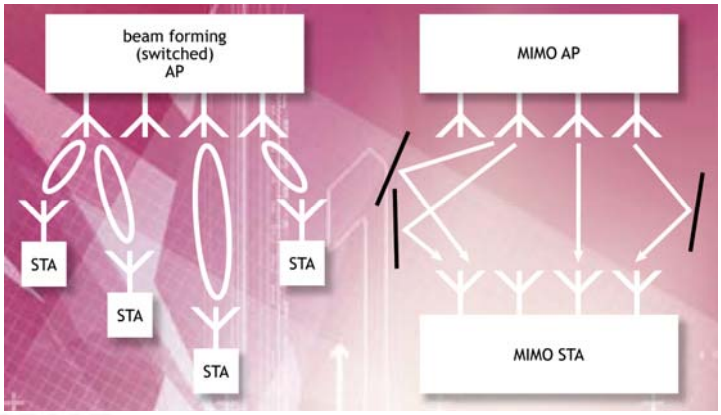
OFDM (802.11a and 802.11g)



McFarland and Wong

Trends

- Beam foaming
- MIMO (multiple input / multiple output)



McFarland and Wong

Power consumption

Chipset Vendor	WLAN Mode	Idle (Sleep)	TCP Uplink (Tx)	TCP Downlink (Rx)	Metric
Atheros	802.11a	0.75 W	2.48 J/MB	2.56 J/MB	3.16 J/MB
Cisco	802.11a	1.04 W	2.48 J/MB	2.88 J/MB	3.69 J/MB
Intersil	802.11a	2.06 W	2.40 J/MB	2.48 J/MB	4.09 J/MB
Atheros	802.11g	0.92 W	3.20 J/MB	3.20 J/MB	4.02 J/MB
Broadcom	802.11g	1.78 W	2.64 J/MB	3.28 J/MB	4.79 J/MB
Intersil	802.11g	1.31 W	2.48 J/MB	3.04 J/MB	4.12 J/MB
Agere	802.11b	0.14 W	15.28 J/MB	17.28 J/MB	17.14 J/MB
Atheros	802.11b	0.87 W	8.40 J/MB	8.08 J/MB	10.94 J/MB
Intersil	802.11b	0.46 W	16.40 J/MB	14.88 J/MB	17.28 J/MB

Not intended to be an exhaustive survey of WLAN cards.

McFarland and Wong

- Metric = 70% idle, 20% receiving, 10% transmitting

Basics

- CSMA/CA
  - Listen before talk
  - Collision avoidance
  - Slotted random backoff
- It's difficult to send and receive in parallel
  - Collision avoidance instead of collision detection
- Packet-by-packet acknowledge
  - Automatic repeat request (ARQ)

MAC access modes

- Distributed coordination function (DCF)
  - Contention-based services
  - Basic functionality
- Point coordination function (PCF)
  - Contention-free services possible
  - Requires infrastructure mode
  - Functionality provided by access point

Carrier sensing

- Physical carrier sensing
  - Depends on the modulation technique
  - Listen before talk
- Virtual carrier sensing
  - NAV (Network allocation vector)
  - 802.11 frame carry a duration field
  - Upon receipt of NAV station counts to zero before accessing the medium again

Interframe spacing

- Assign priorities to frames
- Short interframe space (SIFS)
  - Used to define atomar transactions such as RTS/CTS frames
- PCF interframe space (PIFS)
  - Provision of contention-free services
- DCF interframe space (DIFS)
  - Minium idle time for contention-based services
- Extended interframe space (EIFS)
  - Recover from transmission errors

Power saving mode

- Mobile station may enter power saving mode
  - Indicated by a set power management bit in the frame control field
  - Sending Null frame of no data to transmit
- Access point will buffer frame for sleeping device
- Upon wakeup: AP will send buffered frames
  - Immediate response
  - Deferred response

Beacons

- Typical period is 100ms

Security

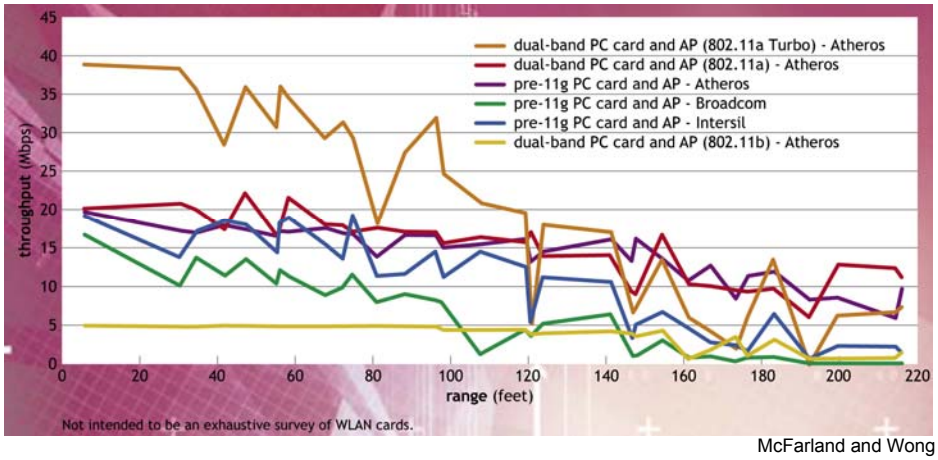
- WEP (Wired equivalent privacy)
  - Based on RC4 symmetric stream cypher
  - Pseudorandom number generator creates key stream from a fixed-length passphrase
  - 64 Bit = 40 bit secret and 24 bit
- WPA
- AES

Throughput and capacity

WLAN Mode	Maximum Link Rate	Maximum UDP Rate	Maximum TCP Rate	System Capacity	
				# of Channels	Maximum UDP Capacity
802.11a Turbo	108 Mbps	55.1 Mbps	42.7 Mbps	6	330.6 Mbps
802.11a	54 Mbps	30.7 Mbps	24.0 Mbps	13	399.1 Mbps
802.11g (11g-only)	54 Mbps	30.7 Mbps	24.0 Mbps	3	92.1 Mbps
802.11g (with 11b present and idle)	54 Mbps	19.6 Mbps	14.5 Mbps	3	58.8 Mbps
802.11g (with 11b present and active)	54 Mbps	11.2 Mbps	9.2 Mbps	3	33.6 Mbps
802.11b	11 Mbps	7.1 Mbps	6.1 Mbps	3	21.3 Mbps

McFarland and Wong

TCP downlink throughput



McFarland and Wong

References

- B. McFarland, M. Wong
  The Family Dynamics of 802.11
  ACM Queue, May 2003, pp. 18-38
- M.S. Gast
  802.11 Wireless Networks – The definitive guide
  O'Reilly, 2002