Introduction to Wireless Networks

Chapter 2: Introduction to IEEE 802.11

Prof. Yuh-Shyan Chen Department of CSIE National Taipei University





Chapter 2: Introduction to IEEE 802.11

□IEEE 802.11 □ PHY □ MAC □ Roaming □ .11a, b, g, h, i ...

□ HIPERLAN

□ Standards overview

□ HiperLAN2

□ QoS





Comparison: infrastructure vs. ad-hoc networks







802.11 - Architecture of an infrastructure network



Station (STA)

 terminal with access mechanisms to the wireless medium and radio contact to the access point

Basic Service Set (BSS)

group of stations using the same radio frequency

Access Point

station integrated into the wireless
LAN and the distribution system

Portal

□ bridge to other (wired) networks

Distribution System

 interconnection network to form one logical network (ESS: Extended Service Set) based on several BSS





802.11 - Architecture of an ad-hoc network



Direct communication within a limited range

- Station (STA): terminal with access mechanisms to the wireless medium
- Independent Basic Service Set (IBSS): group of stations using the same radio frequency







IEEE standard 802.11







802.11 - Layers and functions

MAC

 access mechanisms, fragmentation, encryption

MAC Management

 synchronization, roaming, MIB, power management

- PLCP Physical Layer Convergence Protocol
 - clear channel assessment signal (carrier sense)
- PMD Physical Medium Dependent
 - modulation, coding
- PHY Management
 - □ channel selection, MIB
- **Station Management**
 - coordination of all management functions







802.11 - Physical layer

3 versions: 2 radio (typ. 2.4 GHz), 1 IR

□ data rates 1 or 2 Mbit/s

FHSS (Frequency Hopping Spread Spectrum)

- □ spreading, despreading, signal strength, typ. 1 Mbit/s
- □ min. 2.5 frequency hops/s (USA), two-level GFSK modulation

DSSS (Direct Sequence Spread Spectrum)

- DBPSK modulation for 1 Mbit/s (Differential Binary Phase Shift Keying), DQPSK for 2 Mbit/s (Differential Quadrature PSK)
- preamble and header of a frame is always transmitted with 1 Mbit/s, rest of transmission 1 or 2 Mbit/s
- □ chipping sequence: +1, -1, +1, +1, -1, +1, +1, -1, -1, -1, -1 (Barker code)

□ max. radiated power 1 W (USA), 100 mW (EU), min. 1mW

Infrared

- □ 850-950 nm, diffuse light, typ. 10 m range
- carrier detection, energy detection, synchonization





FHSS PHY packet format

Synchronization

□ synch with 010101... pattern

SFD (Start Frame Delimiter)

□ 0000110010111101 start pattern

PLW (PLCP_PDU Length Word)

□ length of payload incl. 32 bit CRC of payload, PLW < 4096

PSF (PLCP Signaling Field)

□ data of payload (1 or 2 Mbit/s)

HEC (Header Error Check)

CRC with $x^{16}+x^{12}+x^5+1$







DSSS PHY packet format

Synchronization

synch., gain setting, energy detection, frequency offset compensation
SFD (Start Frame Delimiter)

1111001110100000

Signal

□ data rate of the payload (0A: 1 Mbit/s DBPSK; 14: 2 Mbit/s DQPSK)

Service

Length

□ future use, 00: 802.11 compliant

Iength of the payload

HEC (Header Error Check)

□ protection of signal, service and length, $x^{16}+x^{12}+x^5+1$







802.11 - MAC layer I – DFWMAC (distributed foundation wireless medium access control)

Traffic services

- □ Asynchronous Data Service (mandatory)
 - exchange of data packets based on "best-effort"
 - support of broadcast and multicast
- □ Time-Bounded Service (optional)
 - implemented using PCF (Point Coordination Function)

Access methods

- □ DFWMAC-DCF CSMA/CA (mandatory)
 - collision avoidance via randomized "back-off" mechanism
 - minimum distance between consecutive packets
 - ACK packet for acknowledgements (not for broadcasts)
- □ DFWMAC-DCF w/ RTS/CTS (optional)
 - Distributed Foundation Wireless MAC
 - avoids hidden terminal problem
- DFWMAC- PCF (optional)
 - access point polls terminals according to a list





802.11 - MAC layer II

Priorities

- defined through different inter frame spaces
- □ no guaranteed, hard priorities
- □ SIFS (Short Inter Frame Spacing)
 - highest priority, for ACK, CTS, polling response
- □ PIFS (PCF IFS)
 - medium priority, for time-bounded service using PCF
- DIFS (DCF, Distributed Coordination Function IFS)
 - lowest priority, for asynchronous data service



802.11 - CSMA/CA access method I



- station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)





802.11 - competing stations - simple version







802.11 - CSMA/CA access method II

Sending unicast packets

- □ station has to wait for DIFS before sending data
- receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (CRC)
- □ automatic retransmission of data packets in case of transmission errors







Hidden-Terminal and Exposed-Terminal Problems



Fig. 1: (a) the hidden terminal problem, (b) the exposed terminal problem





802.11 - DFWMAC

Sending unicast packets

- station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
- □ acknowledgement via CTS after SIFS by receiver (if ready to receive)
- □ sender can now send data at once, acknowledgement via ACK
- other stations store medium reservations distributed via RTS and CTS







Fragmentation







DFWMAC-PCF I







DFWMAC-PCF II







802.11 - Frame format

Types

control frames, management frames, data frames
Sequence numbers

□ important against duplicated frames due to lost ACKs

Addresses

receiver, transmitter (physical), BSS identifier, sender (logical)
Miscellaneous

□ sending time, checksum, frame control, data

byte	es 2	2	6		6		6	2		6	0-2312	2	4
	Frame	Duratio	on/ Addr	ess	Addres	ss Ado	dress	Sequen	ce Ad	dress	Data		
	Control	ID	1		2		3	Contro		4	Dala		
bits	2	2	4	1	1	1	1		1	1	1		
	Protocol	Tupo	Subtype	То	From	More	Dotry	Power	More		Ordor		
	version Type		DS	DS	Frag	Reliy	Mgmt	Data		Order			





MAC address format

scenario	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure	0	1	DA	BSSID	SA	-
network, from AP						
infrastructure	1	0	BSSID	SA	DA	-
network, to AP						
infrastructure	1	1	RA	TA	DA	SA
network, within DS						

- DS: Distribution System AP: Access Point DA: Destination Address SA: Source Address BSSID: Basic Service Set Identifier RA: Receiver Address
- TA: Transmitter Address





Special Frames: ACK, RTS, CTS







802.11 - MAC management

Synchronization

- □ try to find a LAN, try to stay within a LAN
- □ timer etc.

Power management

- □ sleep-mode without missing a message
- □ periodic sleep, frame buffering, traffic measurements

Association/Reassociation

- □ integration into a LAN
- □ roaming, i.e. change networks by changing access points
- □ scanning, i.e. active search for a network
- MIB Management Information Base
 - □ managing, read, write





Synchronization using a Beacon (infrastructure)







Synchronization using a Beacon (ad-hoc)







Power management

Idea: switch the transceiver off if not needed

States of a station: sleep and awake

Timing Synchronization Function (TSF)

□ stations wake up at the same time

Infrastructure

- □ Traffic Indication Map (TIM)
 - list of unicast receivers transmitted by AP
- Delivery Traffic Indication Map (DTIM)
 - list of broadcast/multicast receivers transmitted by AP

Ad-hoc

- □ Ad-hoc Traffic Indication Map (ATIM)
 - announcement of receivers by stations buffering frames
 - more complicated no central AP
 - collision of ATIMs possible (scalability?)





Power saving with wake-up patterns (infrastructure)







Power saving with wake-up patterns (ad-hoc)





802.11 - Roaming

No or bad connection? Then perform:

Scanning

scan the environment, i.e., listen into the medium for beacon signals or send probes into the medium and wait for an answer

Reassociation Request

 \Box station sends a request to one or several AP(s)

Reassociation Response

- □ success: AP has answered, station can now participate
- □ failure: continue scanning

AP accepts Reassociation Request

- □ signal the new station to the distribution system
- □ the distribution system updates its data base (i.e., location information)
- typically, the distribution system now informs the old AP so it can release resources

infrastructure network

Layer-2 handoff procedure in WLAN

NTPU, Department of Computer Science and Information Engineering

Paper studying

Yuh-Shyan Chen, Ming-Chin Chuang, and Chung-Kai Chen, "DeuceScan: Deuce-Based Fast Handoff Scheme in IEEE 802.11 Wireless Networks," *IEEE Trans. on Vehicular Technology*, March 2008. (2006 SCI=1.071, ranking=17/59=28.81%)

WLAN: IEEE 802.11b

Data rate

- □ 1, 2, 5.5, 11 Mbit/s, depending on SNR
- User data rate max. approx. 6 Mbit/s
- Transmission range
 - **G** 300m outdoor, 30m indoor
 - □ Max. data rate ~10m indoor
- Frequency
 - □ Free 2.4 GHz ISM-band
- Security
 - □ Limited, WEP insecure, SSID

Cost

□ 100€ adapter, 250€ base station, dropping

Availability

□ Many products, many vendors

Connection set-up time

□ Connectionless/always on

Quality of Service

- Typ. Best effort, no guarantees (unless polling is used, limited support in products)
- Manageability
 - Limited (no automated key distribution, sym. Encryption)

Special Advantages/Disadvantages

- Advantage: many installed systems, lot of experience, available worldwide, free ISM-band, many vendors, integrated in laptops, simple system
- Disadvantage: heavy interference on ISM-band, no service guarantees, slow relative speed only

IEEE 802.11b – PHY frame formats

Channel selection (non-overlapping)

WLAN: IEEE 802.11a

Data rate

- □ 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s, depending on SNR
- User throughput (1500 byte packets): 5.3 (6), 18 (24), 24 (36), 32 (54)
- □ 6, 12, 24 Mbit/s mandatory

Transmission range

- □ 100m outdoor, 10m indoor
 - E.g., 54 Mbit/s up to 5 m, 48 up to 12 m, 36 up to 25 m, 24 up to 30m, 18 up to 40 m, 12 up to 60 m

Frequency

□ Free 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz ISM-band

Security

Limited, WEP insecure, SSID

Cost

□ 280€ adapter, 500€ base station Availability

□ Some products, some vendors

Connection set-up time

□ Connectionless/always on

Quality of Service

Typ. best effort, no guarantees (same as all 802.11 products)

Manageability

 Limited (no automated key distribution, sym. Encryption)

Special Advantages/Disadvantages

- Advantage: fits into 802.x standards, free ISM-band, available, simple system, uses less crowded 5 GHz band
- Disadvantage: stronger shading due to higher frequency, no QoS

IEEE 802.11a – PHY frame format

Operating channels for 802.11a / US U-NII

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

OFDM in IEEE 802.11a (and HiperLAN2)

802.11d: Regulatory Domain Update – completed

802.11e: MAC Enhancements – QoS – ongoing

- Enhance the current 802.11 MAC to expand support for applications with Quality of Service requirements, and in the capabilities and efficiency of the protocol.
- 802.11f: Inter-Access Point Protocol ongoing
 - Establish an Inter-Access Point Protocol for data exchange via the distribution system.

802.11g: Data Rates > 20 Mbit/s at 2.4 GHz; 54 Mbit/s, OFDM – ongoing

802.11h: Spectrum Managed 802.11a (DCS, TPC) – ongoing

802.11i: Enhanced Security Mechanisms – ongoing

□ Enhance the current 802.11 MAC to provide improvements in security.

Study Groups

- □ 5 GHz (harmonization ETSI/IEEE) closed
- □ Radio Resource Measurements started
- □ High Throughput started

ETSI - HIPERLAN

ETSI standard

- □ European standard, cf. GSM, DECT, ...
- □ Enhancement of local Networks and interworking with fixed networks
- □ integration of time-sensitive services from the early beginning

HIPERLAN family

- one standard cannot satisfy all requirements
 - range, bandwidth, QoS support
 - commercial constraints
- □ HIPERLAN 1 standardized since 1996 no products!

Overview: original HIPERLAN protocol family

	HIPERLAN 1	HIPERLAN 2	HIPERLAN 3	HIPERLAN 4		
Application	wireless LAN	access to ATM	wireless local	point-to-point		
		fixed networks	loop	wireless ATM		
				connections		
Frequency	Jency 5.1-5.3GHz					
Topology	decentralized ad-	cellular,	point-to-	point-to-point		
	hoc/infrastructure	centralized	multipoint			
Antenna	omni-dire	omni-directional directional directional directional directional directional directional direction directi				
Range	50 m	50-100 m	5000 m	150 m		
QoS	statistical	ATM traffic cla	asses (VBR, CBF	R, ABR, UBR)		
Mobility	<10n	n/s	stationary			
Interface	conventional LAN		ATM networks			
Data rate	23.5 Mbit/s	>20 N	/lbit/s	155 Mbit/s		
Power	yes	S	not necessary			
conservation						

HIPERLAN 1 never reached product status, the other standards have been renamed/modfied !

Homework #2

- 1. What's the hidden-terminal and exposed-terminal problems occurred in DFWMAC-DCF CSMA/CA ?
- 2. How to use RTS/CTS messages (DFWMAC-DCF w/ RTS/CTS) to **reduce** the hidden-terminal problem ?
- 3. How the PCF (Point Coordination Function) works?
- 4. What's the main operations of IEEE 802.11 roaming (layer-2 handoff procedure) ?
- 5. What's the power management in infrastructure and ad hoc modes?

