Mobile Computing
Lecture 17
Wireless LAN 2

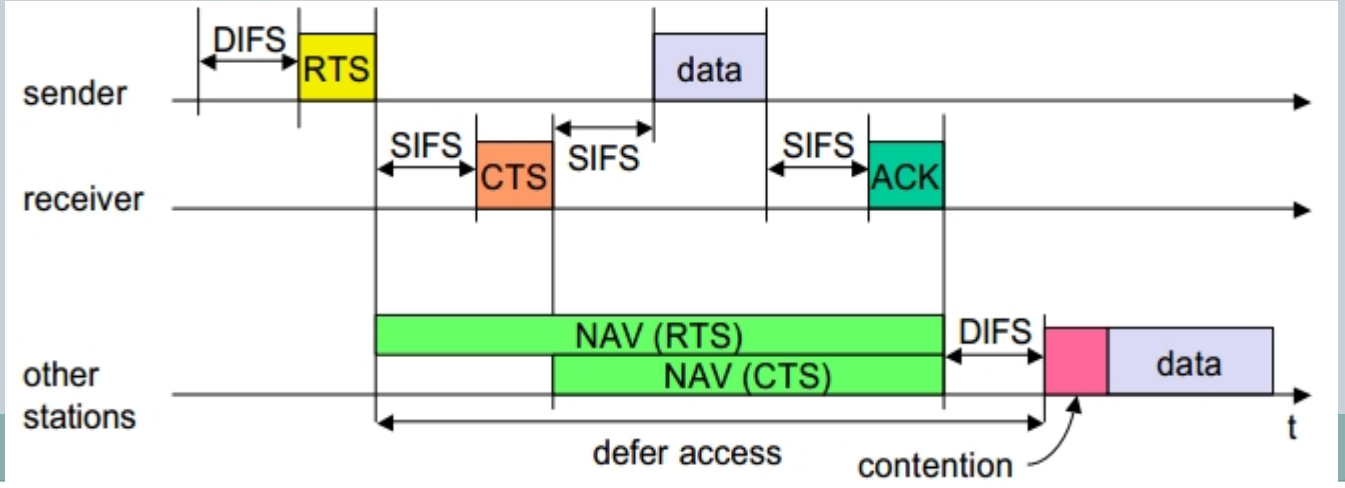
Contents

- 802.11 - DFWMAC
- Fragmentation
- 802.11 - Frame format
- WLAN: IEEE 802.11b
- Channel selection (non-overlapping)
- WLAN: IEEE 802.11a
- HIPERLAN
- Characteristics

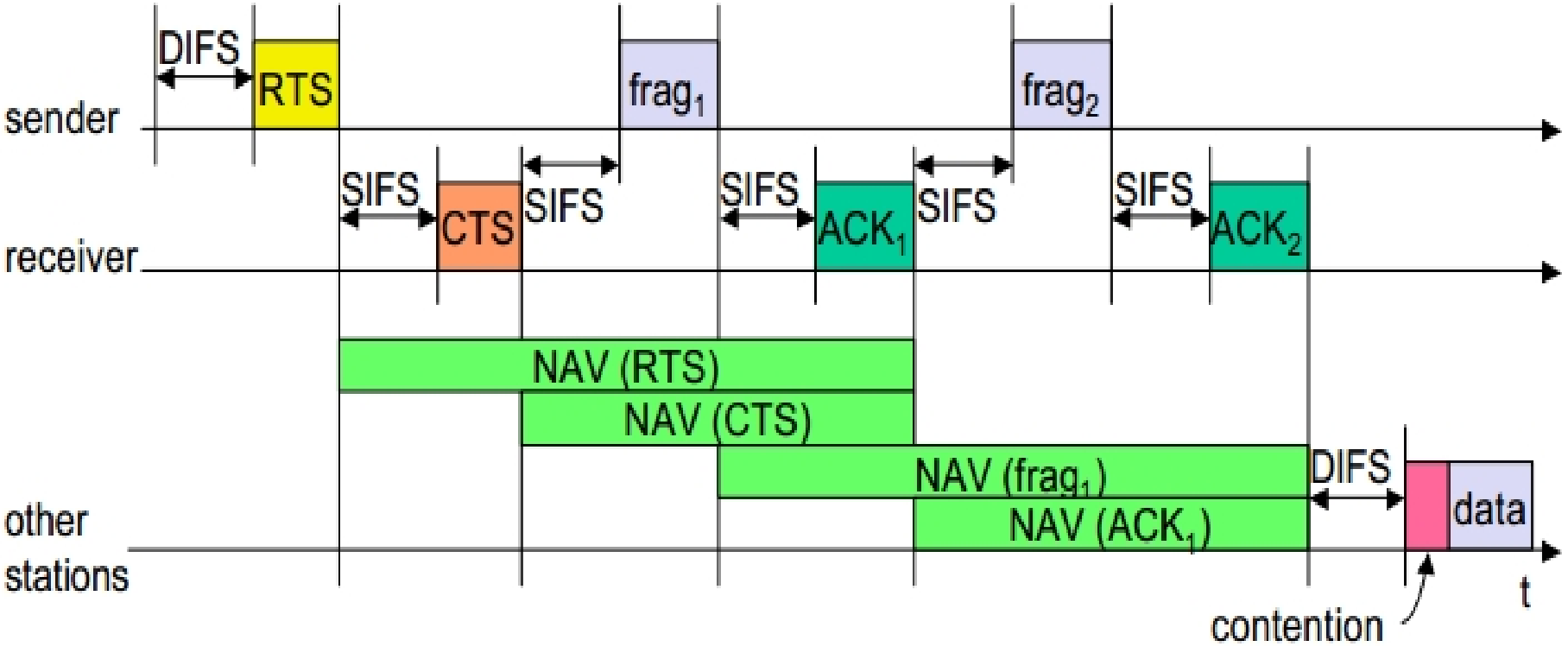
802.11 - DFWMAC

Sending unicast packets

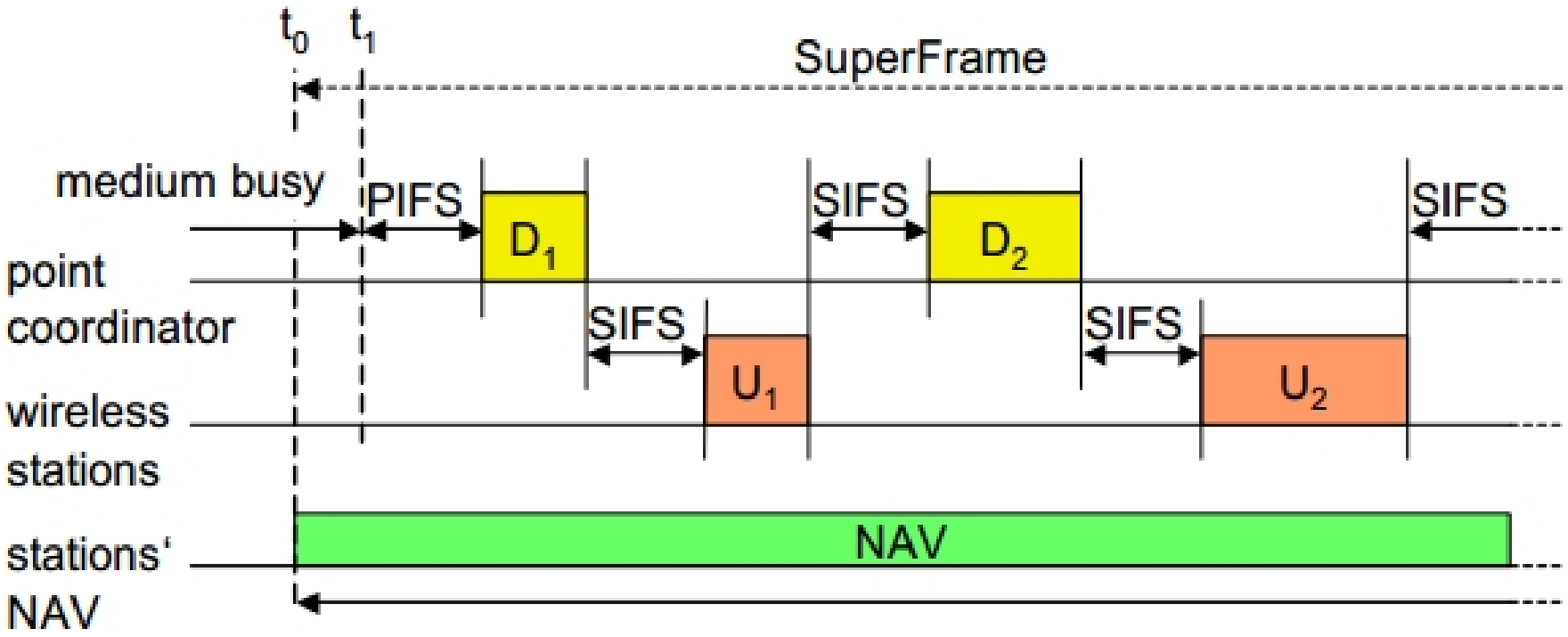
- station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
- acknowledgement via CTS after SIFS by receiver (if ready to receive)
- sender can now send data at once, acknowledgement via ACK
- other stations store medium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



Fragmentation



DFWMAC-PCF I


t0
t1
SuperFrame
medium busy
PIFS
D1
SIFS
D2
SIFS
point coordinator
SIFS
U1
SIFS
U2
wireless stations
stations' NAV
NAV

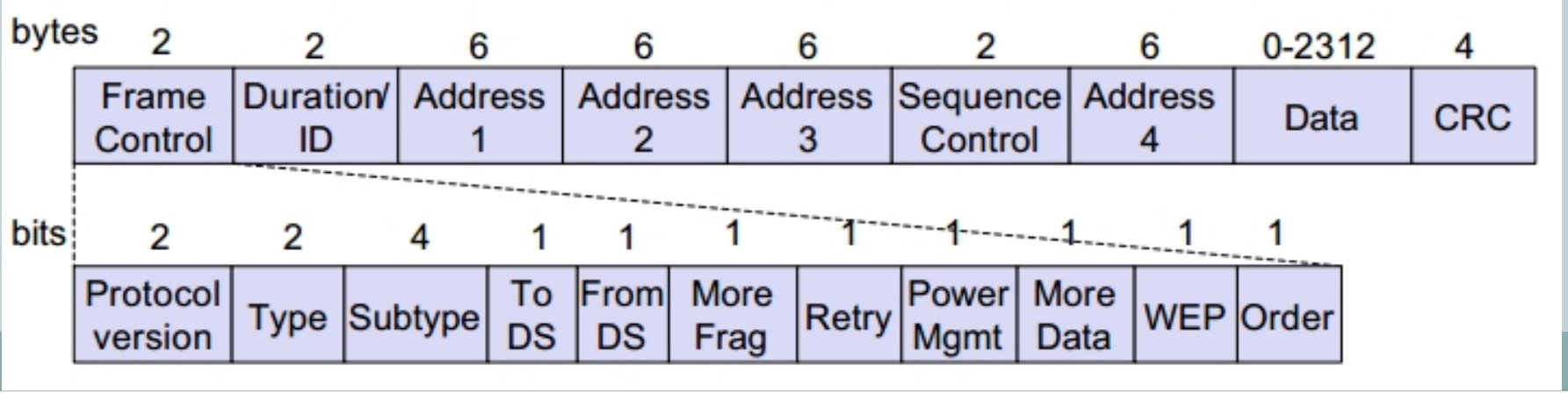
802.11 - Frame format

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



802.11 - MAC management

- Synchronization
  - Clock skew may happen
  - Infrastructure: AP broadcasts beacons, other nodes correct skew
  - Ad hoc: All nodes broadcast beacons
- Power management
  - Save battery, nodes can go to sleep, wake up periodically to receive
  - Infrastructure: AP buffers packets for sleeping nodes
  - Ad hoc: sender buffers packets for sleeping destinations
- Association/Reassociation
  - Roaming: Move from access point to access point as user moves
  - scanning, i.e. active search for a network
  - Node sends message to new AP, says goodbye to old AP
- MIB - Management Information Base
  - All information for managing network, node stored in SNMP MIB
  - MIB can be read (access) or written to (update)

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
- 300m outdoor, 30m indoor
- Max. data rate ~10m indoor

Frequency
- Free 2.4 GHz ISM-band

Security
- Limited, WEP insecure, SSID

Availability
- Many products, many vendors

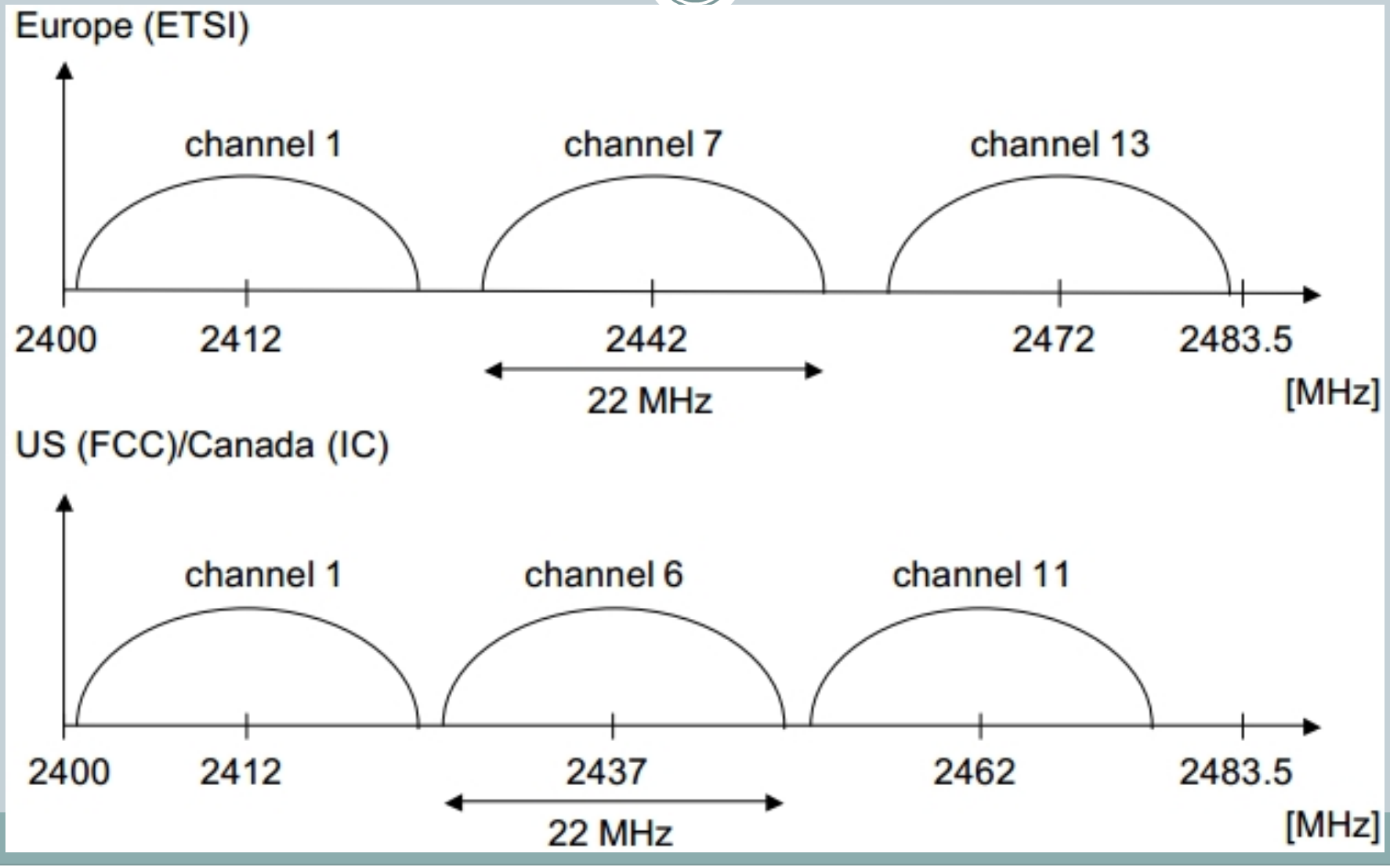
Connection set-up time
- Connectionless/always on

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

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

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

WLAN: IEEE 802.11 – future developments (03/2005)

802.11c: Bridge Support

- Definition of MAC procedures to support bridges as extension to 802.1D

802.11d: Regulatory Domain Update

- Support of additional regulations related to channel selection, hopping sequences

802.11e: MAC Enhancements – QoS

- 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
- Definition of a data flow ("connection") with parameters like rate, burst, period…
- Additional energy saving mechanisms and more efficient retransmission

802.11f: Inter-Access Point Protocol

- Establish an Inter-Access Point Protocol for data exchange via the distribution system
- Currently unclear to which extend manufacturers will follow this suggestion

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

- Successful successor of 802.11b, performance loss during mixed operation with 11b

802.11h: Spectrum Managed 802.11a

- Extension for operation of 802.11a in Europe by mechanisms like channel measurement for dynamic channel selection (DFS, Dynamic Frequency Selection) and power control (TPC, Transmit Power Control)

Cont..

802.11i: Enhanced Security Mechanisms

- Enhance the current 802.11 MAC to provide improvements in security.
- TKIP enhances the insecure WEP, but remains compatible to older WEP systems
- AES provides a secure encryption method and is based on new hardware

802.11j: Extensions for operations in Japan

- Changes of 802.11a for operation at 5GHz in Japan using only half the channel width at larger range

802.11k: Methods for channel measurements

- Devices and access points should be able to estimate channel quality in order to be able to choose a better access point of channel

802.11m: Updates of the 802.11 standards

802.11n: Higher data rates above 100Mbit/s

- Changes of PHY and MAC with the goal of 100Mbit/s at MAC SAP
- MIMO antennas (Multiple Input Multiple Output), up to 600Mbit/s are currently feasible
- However, still a large overhead due to protocol headers and inefficient mechanisms

802.11p: Inter car communications

- Communication between cars/road side and cars/cars
- Planned for relative speeds of min. 200km/h and ranges over 1000m
- Usage of 5.850-5.925GHz band in North America

Cont..

802.11r: Faster Handover between BSS

- Secure, fast handover of a station from one AP to another within an ESS
- Current mechanisms (even newer standards like 802.11i) plus incompatible devices from different vendors are massive problems for the use of, e.g., VoIP in WLANs
- Handover should be feasible within 50ms in order to support multimedia applications efficiently

802.11s: Mesh Networking

- Design of a self-configuring Wireless Distribution System (WDS) based on 802.11
- Support of point-to-point and broadcast communication across several hops

802.11t: Performance evaluation of 802.11 networks

- Standardization of performance measurement schemes

802.11u: Interworking with additional external networks

802.11v: Network management

- Extensions of current management functions, channel measurements
- Definition of a unified interface

802.11w: Securing of network control

- Classical standards like 802.11, but also 802.11i protect only data frames, not the control frames. Thus, this standard should extend 802.11i in a way that, e.g., no control frames can be forged.

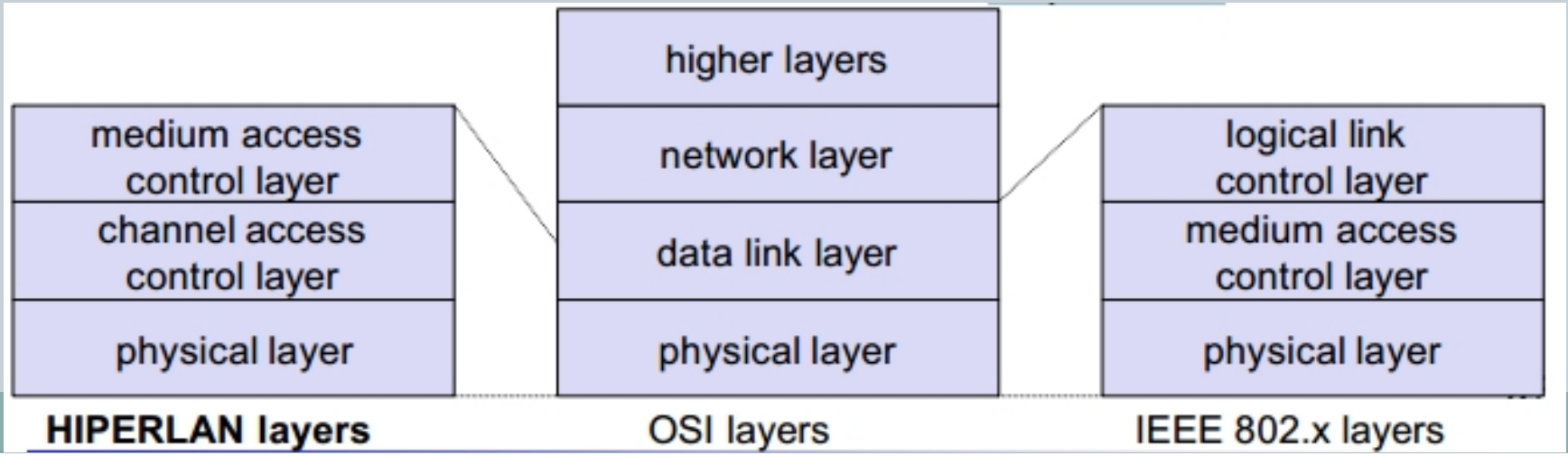
ETSI – HIPERLAN (historical)

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 fixed networks	wireless local loop	point-to-point wireless ATM connections
Frequency	5.1-5.3GHz			17.2-17.3GHz
Topology	decentralized ad-hoc/infrastructure	cellular, centralized	point-to-multipoint	point-to-point
Antenna	omni-directional		directional	
Range	50 m	50-100 m	5000 m	150 m
QoS	statistical	ATM traffic classes (VBR, CBR, ABR, UBR)		
Mobility	<10m/s		stationary	
Interface	conventional LAN	ATM networks		
Data rate	23.5 Mbit/s	>20 Mbit/s		155 Mbit/s
Power conservation	yes		not necessary	

HIPERLAN 1 - Characteristics

Data transmission

- point-to-point, point-to-multipoint, connectionless
- 23.5 Mbit/s, 1 W power, 2383 byte max. packet size

Services

- asynchronous and time-bounded services with hierarchical priorities
- compatible with ISO MAC

Topology

- infrastructure or ad-hoc networks
- transmission range can be larger then coverage of a single node („forwarding“ integrated in mobile terminals)

Further mechanisms

- power saving, encryption, checksums

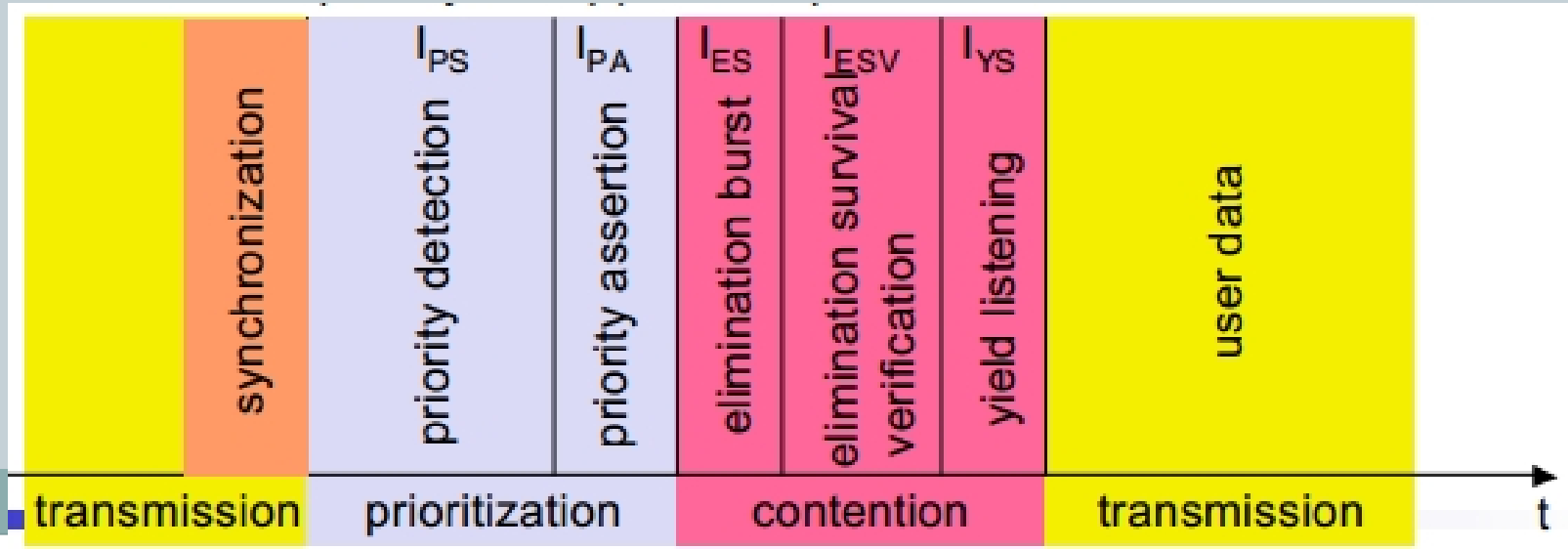
HIPERLAN 1 - CAC sublayer

Channel Access Control (CAC)

- assure that terminal does not access forbidden channels
- priority scheme, access with EY-NPMA
- 3 EY-NPMA phases: priority resolution, contention resolution, transmission

Priorities

- 5 priority levels for QoS support
- QoS is mapped onto a priority level with the help of the packet lifetime (set by an application)



HIPERLAN 1 - EY-NPMA II

Several terminals can now have the same priority and wish to send

- contention phase
  - Elimination Burst: all remaining terminals send a burst to eliminate contenders (11111010100010011100000110010110, high bit- rate)
  - Elimination Survival Verification: contenders now sense the channel, if the channel is free they can continue, otherwise they have been eliminated
  - Yield Listening: contenders again listen in slots with a nonzero probability, if the terminal senses its slot idle it is free to transmit at the end of the contention phase
  - the important part is now to set the parameters for burst duration and channel sensing (slot-based, exponentially distributed)
- data transmission
  - the winner can now send its data (however, a small chance of collision remains)
  - if the channel was idle for a longer time (min. for a duration of 1700 bit) a terminal can send at once without using EY-NPMA
- synchronization using the last data transmission

HIPERLAN 1 - MAC layer

Compatible to ISO MAC

Supports time-bounded services via a priority scheme

Packet forwarding

- support of directed (point-to-point) forwarding and broadcast forwarding (if no path information is available)
- support of QoS while forwarding

Encryption mechanisms

- mechanisms integrated, but without key management

Power conservation mechanisms

- mobile terminals can agree upon awake patterns (e.g., periodic wake-ups to receive data)
- additionally, some nodes in the networks must be able to buffer data for sleeping terminals and to forward them at the right time (so called stores)