Technische Universität Darmstadt

Telecooperation

Ubiquitous & Mobile Computing

Connectivity: Mobile Networks 2

Dr. Erwin Aitenbichler

Wireless Classification: Architecture

Note: acronym / classification Babylon reigns!

1. *Pico* Network
2. *Sensor* Network
3. *Trunked* Mobile Radio System
4. *Paging* Network
5. *Cellular* / PLMN (PLMTS)
6. *Packet data* (wWAN)
7. *Satellite* (→cellular)
8. *Cordless* Telephony (CT) → wPABX
9. *WLAN*
10. *Broadcast networks (DAB, DVB)*
11. *Ad-hoc* net (packet radio PRN)

→ subchapters

2-5 years:

UMTS (3G) → LTE (4G)?
(long term evolution)

+

mobile broadband (MBS)
integration?

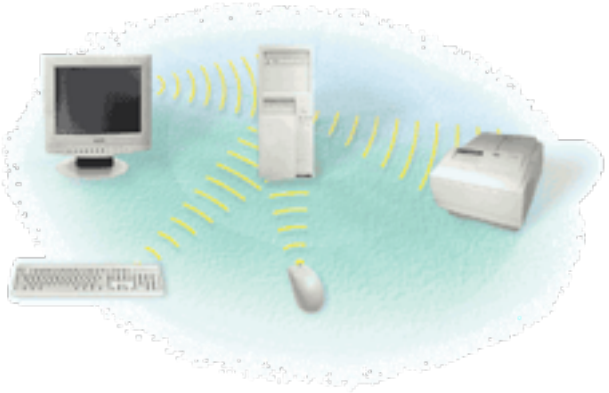
+

5-10+ years: ?

Bluetooth: Goals

- Provide small, inexpensive, power-conscious radio system
- Personal short-range ad-hoc networks
- Not really intended as WLAN technology
- „Cable replacement“

1. *The cordless desktop*
   (headset, loudspeaker... → audio!)
2. *Object Exchange (OBEX) Push*
   (send images from phone to PC)
3. *Tethering*
   (Internet access from PC via GSM phone)



Profiles: define functionality for connection of “logically matching” devices (e.g., headset profile, handsfree profile, …)

- origin of technology:
  - five founders: Nokia, Ericsson, Intel, IBM, Toshiba) → 1000+ !!
  - idea: advance „wireless car key“ chip („1$-world“) to appliances
- origin of name:
  - Danish king Bluetooth (940-981), unified (!) Danemark & Norway

Bluetooth: Basics

Bluetooth Version upgrades:

- 1.1, 1.2: speed, HW functionality → better communication, audio, …
- 2.0: Enhanced Data Rate (EDR): up to 2.1 Mbps. Security
  - Eventually, over 30 profiles
- 3.0: Ultra WideBand (UWB)

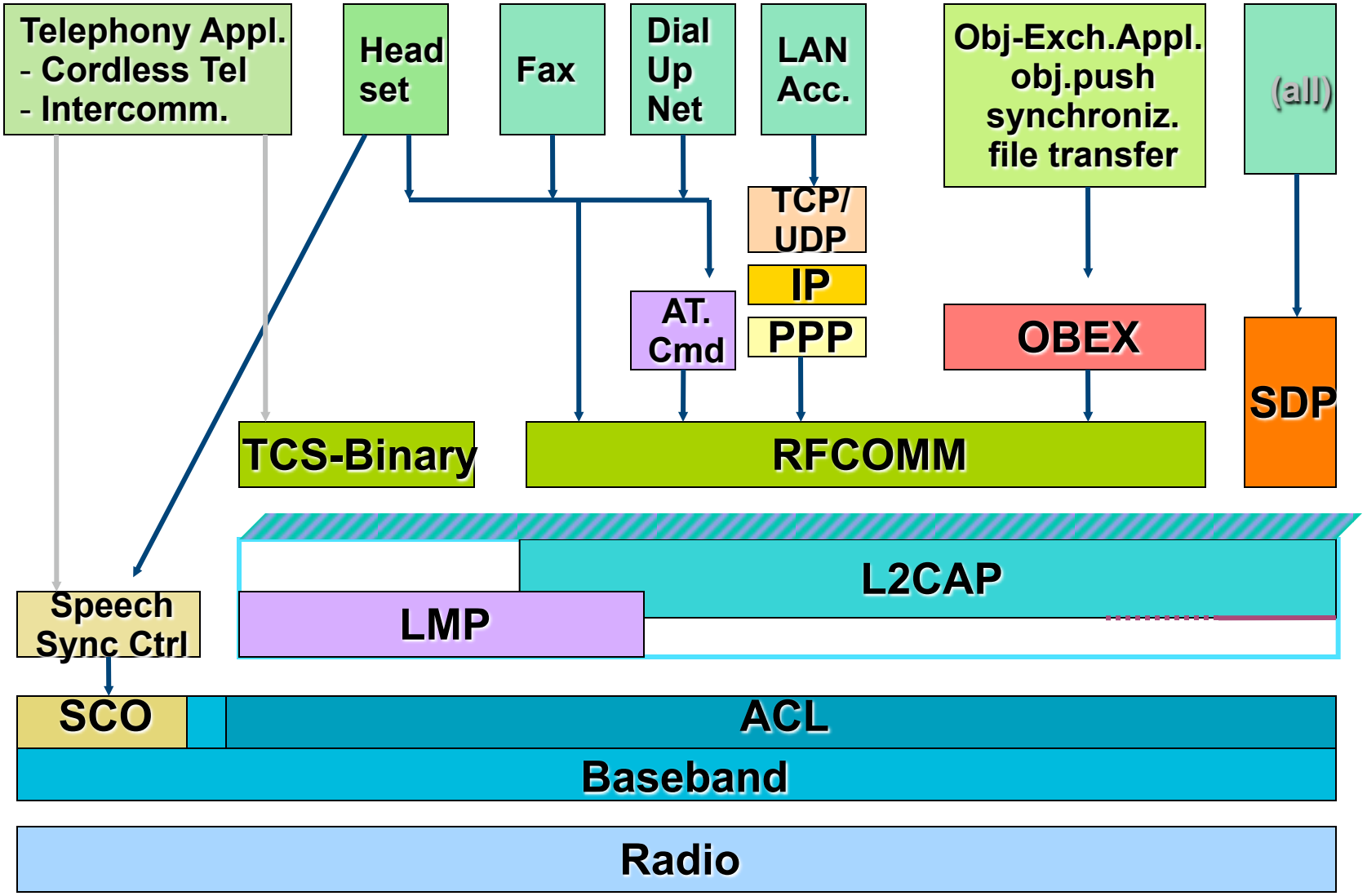
PicoNets, Scatternets:

- Each piconet has one master and ≤ 7 slaves
- Master determines hopping sequence, slaves have to synchronize
  - Look for access code (72 bit) = f (master-ID) in wake-up carrier
  - then: follow master's hopping scheme
- Participation in a piconet = synchronization to hopping sequence
- Scatternet - communication between piconets:
  - devices jumping back and forth between the piconets
  - different MAC addr in different piconets
  - Device can be master in one piconet only

"Radio" Layer: TDD, FH-CDMA (1600 hops/s: slot 625µs)

- 79 (.fr, .jp, .es: 23) frequencies ("hop carriers"); 32 (…: 16) of them: "wake-up carriers"
- Radio layer spec: details of GFSK, power, signal strength/tolerance etc.
- Bands used (USA, most of Europe: 2.4 – 2.4835 GHz) etc.

Bluetooth Protocol Stack



Bluetooth Protocol Stack

- HCI: Host Controller Interface: device ⇔ driver in PC
  - may shield differences of USB, PCcard BT device etc.
  - position may vary dependent on HW/SW tradeoff
- radio, baseband: see below, voice (SCO) / data (ACL) links
- Link Manager Protocol LMP responsible for SCO/ACL link mgmt.
- L2CAP: logical link control & adaptation protocol: general API
- TCS-bin (telephony control protocol specification binary) common management for telephony applications
- RFCOMM emulates serial link „cable“ (up to 60 logical links)
- AT command emulation for modem compatibility
- SDP (service discovery protocol) in later chapter
- Mgmt. Entity ME provides overall configuration management
- OBEX (object exchange) is compatible w/ IrDA
  - Object push, e.g., for biz card exchange
  - Synchronization: e.g., organizer and PC

Bluetooth: selection of profiles

This selection is provided for better understanding of the “profile” concept:

A2DP *Advanced Audio Distribution Profile*
Protocols and procedures that define the distribution of high quality audio content.

AVRCP *Audio Video Remote Control Profile*
Features and procedures that ensure interoperability between BR devices with audio/video control functions.

CIP *Common ISDN Access Profile:* Provision of ISDN services over Bluetooth

CTP *Cordless Telephony Profile:* Forwarding telephone calls to Bluetooth devices.

DUN *Dial Up Networking Profile:* A Bluetooth link to a modem.

ESDP *Extended Service Discovery Profile*
Using the Bluetooth Service Discovery Protocol (SDP) to discover devices that support UPnP services

FTP *File Transfer Profile Specification :* Transferring files between Bluetooth devices.

GAP *Generic Access Profile:* Rules for using protocol stack, foundation for all other profiles.

GAVDP *Generic Audio Video Distrib. Profile:* Distribution of audio/video content using an ACL channel.

GOEP *Generic Object Exchange Profile* Using OBEX (for file transfer, object push and synchronization)

HCRP *Hard Cable Replacement Profile* Includes printing and scanning of documents.

HFP *Hands Free Profile* Interactions for using hands free devices with an in-car kit.

HID *Human Interface Device Profile*
protocols, procedures, features used by BT Human Interface Devices (keyboards, pointing/ gaming devices, …)

HP *Headset Profile* Duplex link to headset, controlled by audio gateway (e.g., mob. phone)

LPP *Local Positioning Profile*
Mechanism / formats for transfer of position related data (position determination and location awareness).

OPP *Object Push Profile* Pushing objects from a Bluetooth enabled server to a client.

PAN *Personal Area Network Profile*
Makes two or more devices form an ad-hoc network and access a remote net via access anpoint

SIM *SIM Access Profile* Protocols and procedures used to access a SIM card via a Bluetooth link.

SPP *Serial Port Profile* RFCOMM's serial port emulation

Bluetooth Baseband

CDMA: FHSS, 1Mbps (per channel i.e. piconet), remember slot size 625 µs;

- Hop frequency changes per-packet if packet < slot
- „multi-slot packets“: 3 or 5 slots (hop frequency unchanged)
- TDD: all even-numbered slots reserved for master (except multi-slot)

- SCO (synch. connection-oriented) link, telephony: „reserve each *n*-th slot“
- ACL (asynch. connectionless) links for everything else

BT device has 48bit address; first 24 (LAP lower addr. part) used to compute „Access Codes“ CAC and DAC (cf. address field in BT packets)

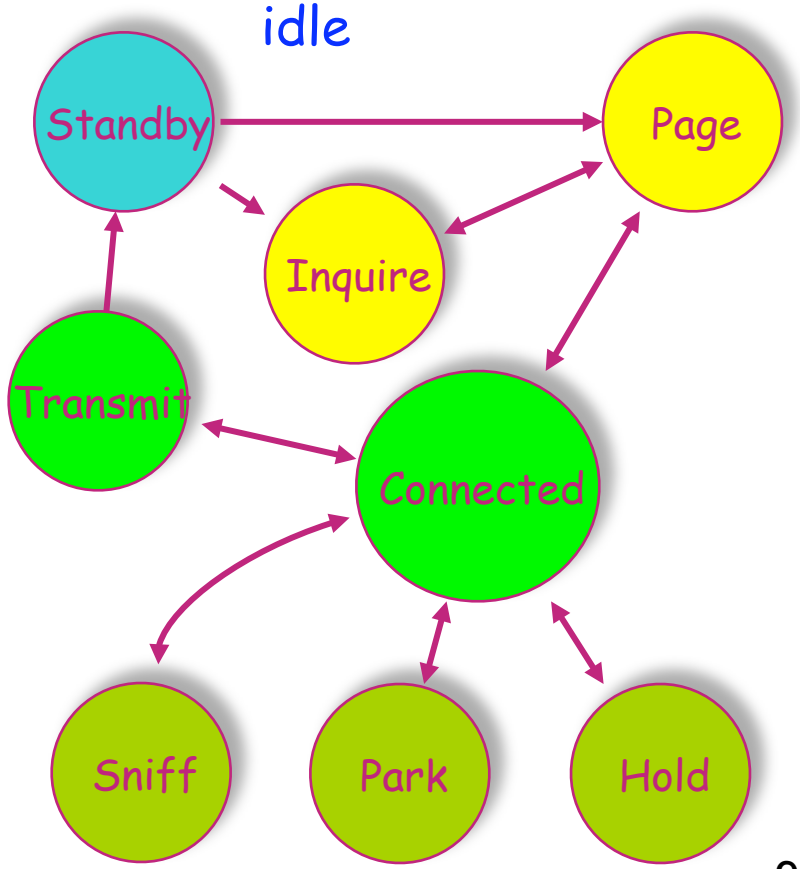
Use of ACs in three important phases of building a piconet:

1. InquiryAC: General (GIAC) or Dedicated (DIAC, for device classes)
   (initial broadcast addr. for „inquiry“ by future master in wake-up carriers)
2. DeviceAC: DAC → reply-msg of reachable devices (or those of DIAC class)
3. ChannelAC: CAC characterizes channel of piconet, forms preamble of all packets

(CAC derived from master‘s LAP, DAC from slave‘s LAP)

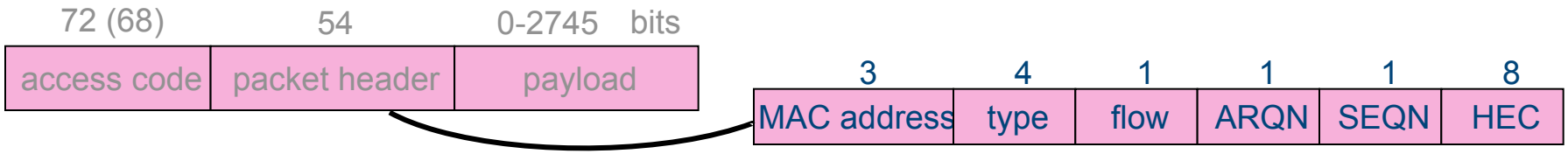
BT Device Connection States

- Standby – waiting to join a piconet (look for paging msg every 1.28s)
- Inquire – master looking for Bluetooth devices
- Page – master wants to connect specific device
- Connected – actively involved in a piconet
- Hold – power conservation state
  - Internal timer runs, connection maintained
- Park – power conservation state
  - Connection "broken„: forgets member address, but can be reactivated
- Sniff – listen at reduced rate



Dr. Erwin Aitenbichler
Prof. Dr. M. Mühlhäuser
Telekooperation

Bluetooth MAC layer



- 68/72b access codes AC – for DAC and CAC:
  - *f*(24bit-LAP) → 64bit (*f* such that robust, easy correlation)
  - +4bit-preamble (synchronization) [+4bit-trailer IF header follows]
- Error correction schemes: none, „1/3“ or „2/3“
  - 1/3: each bit individually repeated 3 times
  - 2/3: groups of ten bits always expanded to 15 bits (5bit-FEC)
- Header contains „link type“ i.e. packet class with or w/o payload, such as
  - ID (68 bit): IAC, DAC
  - POLL (126b, master polls slave), NULL (126b, ack only, nothing to send)
  - HV1/2/3 (HiFi voice, all 1-slot, SCO, reserves every 2nd/ 4th /6th slot),
  - DM 1/3/5 (data medium), DH 1/3/5 (3 and 5 are multislot), all ACL

  HV1/2/3 payload uses FEC1/3, 2/3, and none; all have 240B payload); DM uses FEC1/3, DH uses none)
- Header further contains (note stop-and-wait ARQ → ping-pong behavior):
  - Active member address - also MAC: 000 … 111
  - Flow bit: tells other end to (temporarily) stop sending (overflow!)
  - ARQN: acknowledges last packet (pos./neg)
  - SEQN: alternates, needed to distinguish „resent copy“ from „new“
  - HEC: 8b header specific error check (cyclic redundancy check CRC)
  - ∑ 18bit → FEC1/3 → 54 bit

ZigBee

ZigBee Alliance

- Bluetooth - Desktop / Personal Area Net: few, „valued“ devices
- ZigBee – scales up to sensor networks („smart dust“)
  in terms of power, #of nodes, management …

Market Name Standard	GPRS/UMTS (TDMA/CDMA)	Wi-Fi™ 802.11b	Bluetooth™ 802.15.1	ZigBee™ 802.15.4
Application Focus	LongDist. Voice/ Data	Web, Email, Video	Cable Replacement	Monitoring & Cntrl
System Resources	16MB+	1MB+	250KB+	4KB - 32KB
Battery Life (days)	1-7	.5 - 5	1 - 7	100 - 1,000+
Network Size	(1)	(32)	7	255 / 65,000
Bandwidth (kb/s)	14 - 2000	11,000+	720	20 - 250
Transmission Range (m)	1,000+	1 - 100	1 - 10+	1 - 100+
Success Metrics	Reach, Quality	Speed, Flexibility	Cost, Convenience	Reliab., Power, Cost

Dr. Erwin Aitenbichler
Prof. Dr. M. Mühlhäuser
Telekooperation

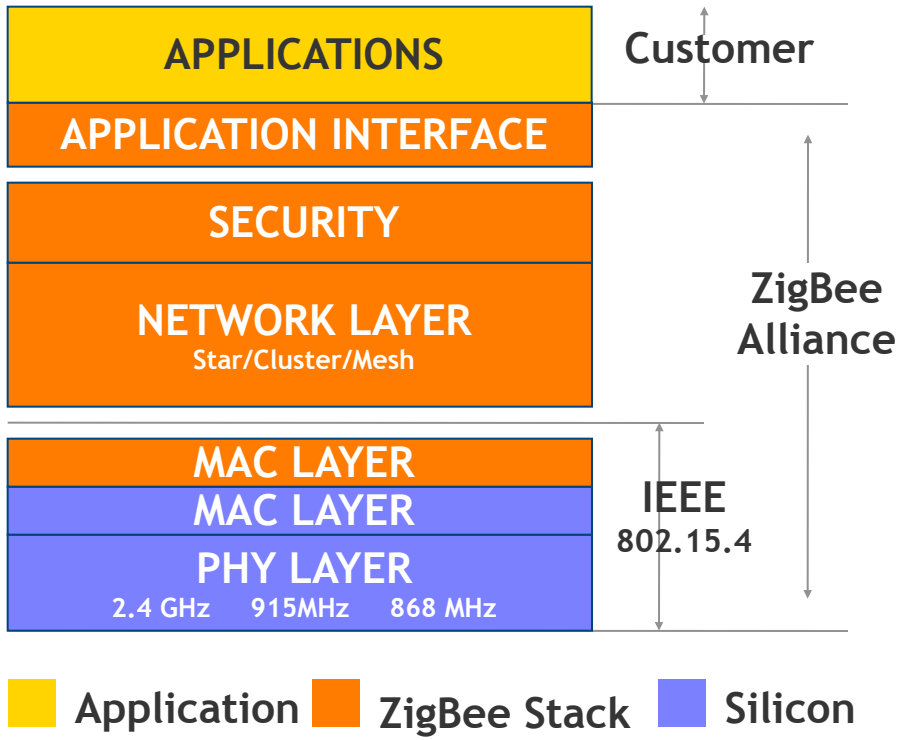
ZigBee Node Types, Protocol Stack

a) FFN vs. RFN: Full Function Nodes- Reduced Function Nodes

b) Coordinator vs. Router vs. EndNode

Only EndNode may (!) be RFN

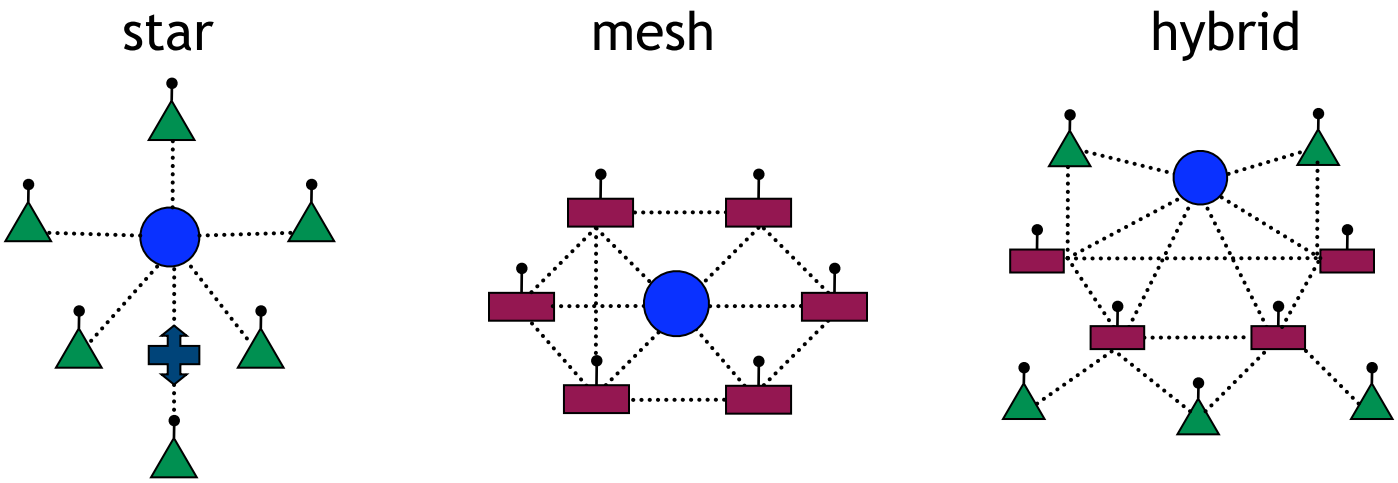
- Microcontroller utilized
- FFN protocol stack <32 k
- RFN protocol stack ~4k
- Coordinators: extra RAM
  (DBs f. nodes/transactions/pairing)
- PHY: OQPSK (2.4GHz); CDMA
- MAC: CSMA/CA



ZigBee Net can be replaced w/ IEEE802 MAC + IP

ZigBee: More Characteristics

- 3 Bands: ISM-Europe (868 MHz) / ISM US (915) / 2.4 GHz → different no. of available channels (1/10/16), speeds (20/40/250 kbps) no. of chips/symbol in CDMA (15/15/32 – note: WLAN has 11)
- 3 network types, made of:



- *star:* low battery ↔ low reliability; *mesh:* opposite (+routg complex!)
- *hybrid:* tradeoff possible

ZigBee: MAC Options

2 Channel Access Mechanisms

- Non-beacon network: unslotted CSMA/CA
  - acknowledgement for successfully received packets
- Beacon-enabled network
  - ZigBee router transmits periodic beacons
    - 15ms to 252sec ($15.38ms*2^n$ where $0 \leq n \leq 14$)
    - 16 equal-width time slots between beacons
    - Channel access in each time slot is contention free
  - Nodes can sync with beacons and may sleep between beacons

3 security levels

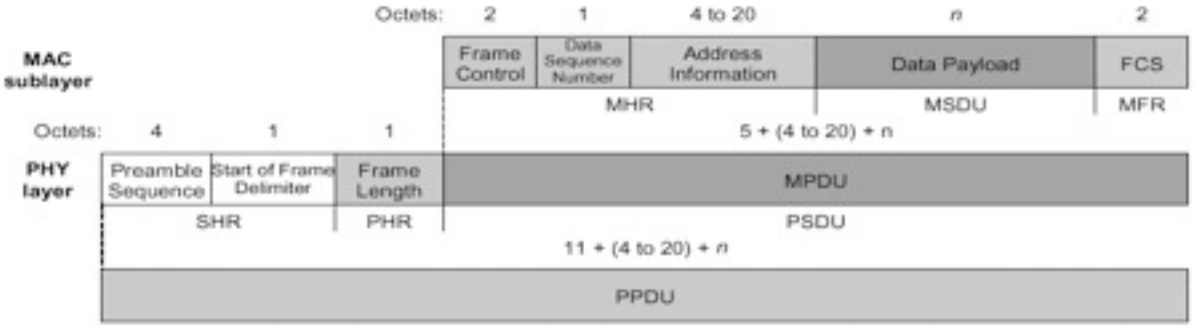
- None
- Access control lists
- Symmetric key (AES-128)

Dr. Erwin Aitenbichler
Prof. Dr. M. Mühlhäuser
Telekooperation

ZigBee: Frame formats

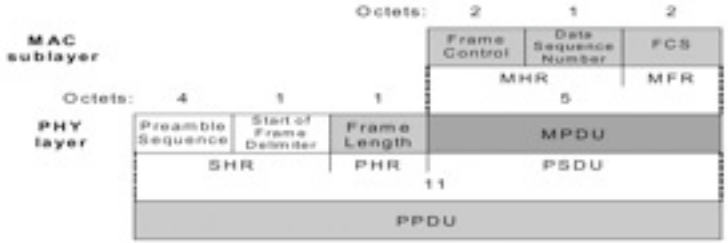
DATA:

- max. payload: 104 Byte
- seq. no. for ACK
- error control (FCS)
- robust structure



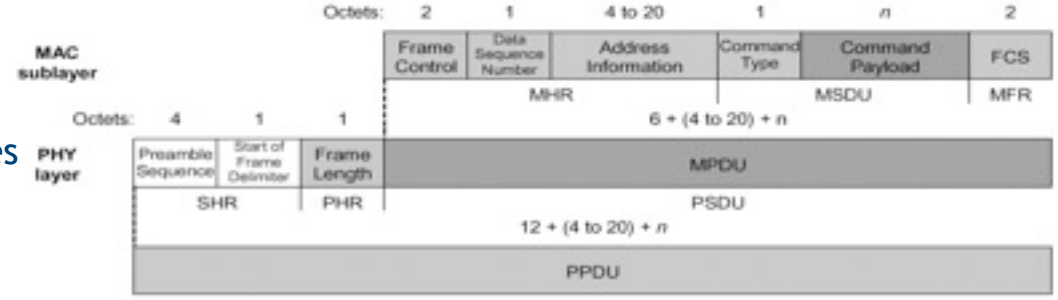
ACK:

- fast response about successful delivery:
- uses “quiet time” immediately after data packet transmission



Command:

- remote control/config. of client nodes
- → centralized net mgr. can configure clients no matter how large the net



GSM Overview

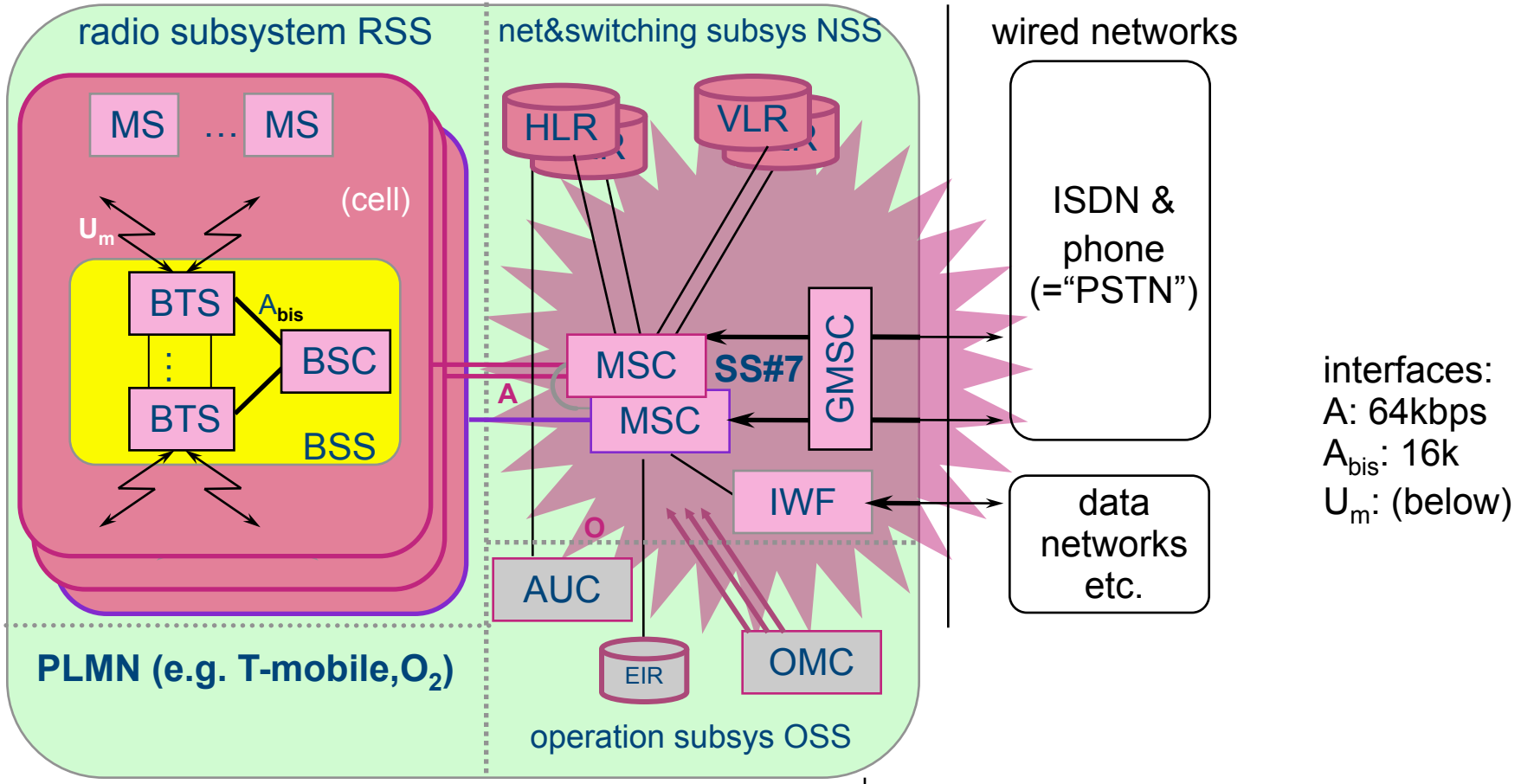
Origin: Intl. Telecom. Union ITU → Eur. branch CEPT → groupe spéciale mobile

today: a) European standards rather by ETSI (telecoms + vendors +...)
b) name change: Global System for Mobile communication

- frequencies: ⇧890-915MHz; ⇩935-960 (1710-85/1805-80; US: 19xx)
- per frequency channel: 200kHz, 256kbps raw symbols + slot guard time
  - 8 slots → phys. channel: pair (freq. channel no. C_n; timeslot no. t_m), t_m=0..7
  - 32kbps raw symbols per channel; 24,7 kbps raw bits per channel
  - multiframes within (C_n, t_m): 26 (or 51) slots; x-in26/51: logical channels
  - Full rate channel: 24 of 26 slots → 22,8 kbps
  - Half rate channel: 12 of 26 slots → 11,4 kbps
  - Full rate speech: 13kbps voice + 9,8 kbps FEC (forward error correction)
  - Full rate data: 2,4 / 4,6 / 9,6 kbps plus CRC plus FEC
    (CRC: cyclic redundancy check: checksum)

Dr. Erwin Aitenbichler
Prof. Dr. M. Mühlhäuser
Telekooperation

GSM Architecture



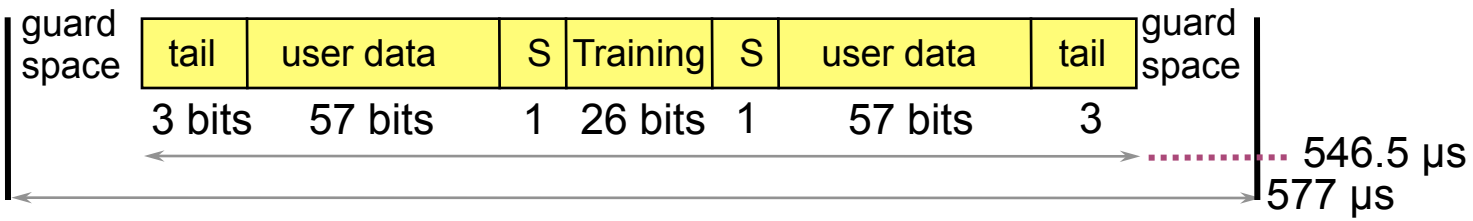
interfaces:
A: 64kbps
A_{bis}: 16k
U_m: (below)

BSC/BSS: base station controller / subsystem
MSC: mobile switching center (G: gateway)
EIR: equipment identity register
AUC: authentication ctr.

OMC: operation & mgmt. center
IWF: interworking function
SS#7: signaling system no. 7
(intl. standard for dialing, mgmt., ...)

GSM Air Interface U_m: Data Rate

- remember: TDMA: 8 slots, FDMA: 2* 124 (DCS1800: 374) *200kHz
- Layer 1: data rate? look at time slot (length: 577 µs)
  - carries „bursts“; for „normal bursts“ (channel in operation):



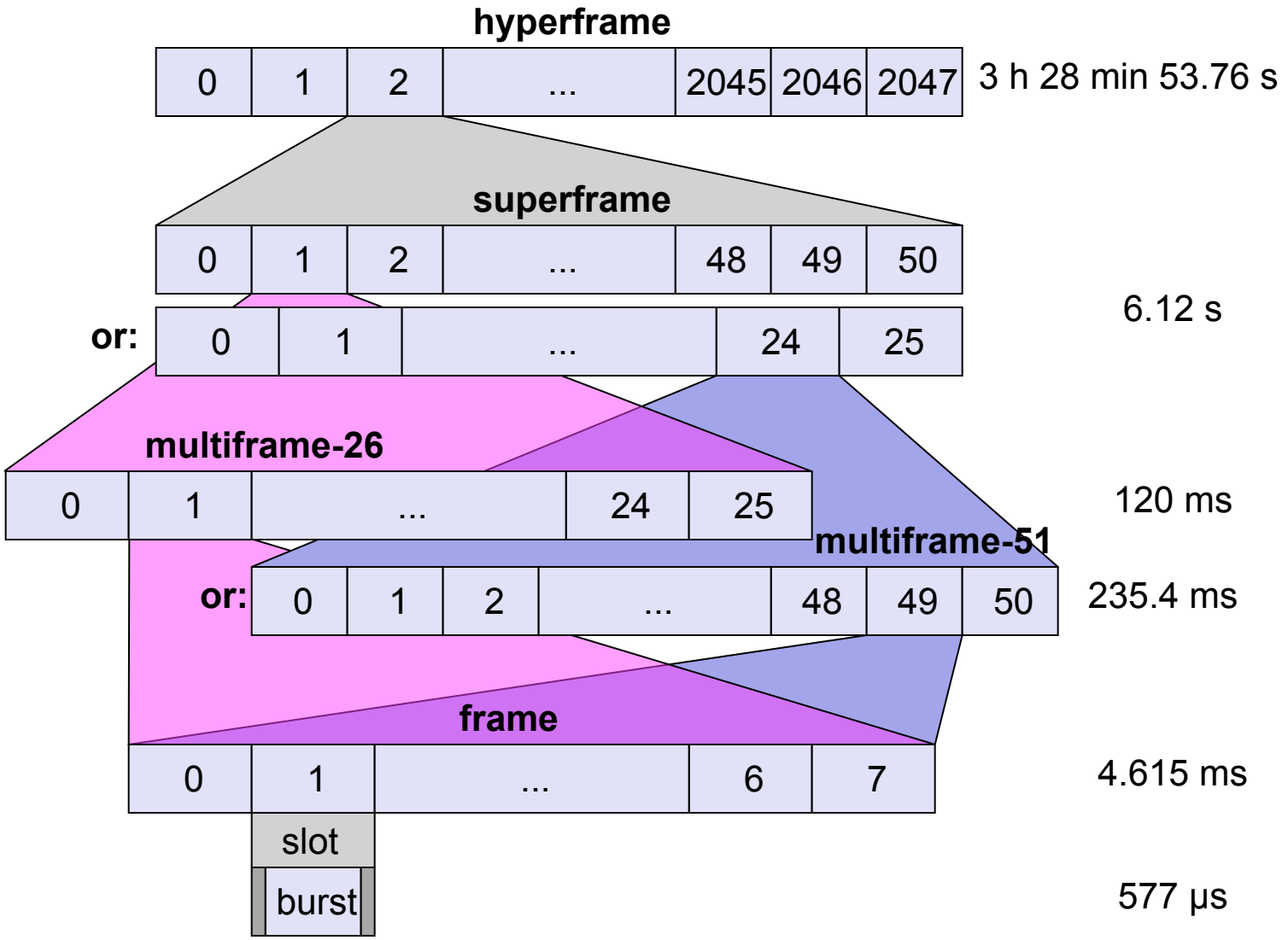
- 2*12 frames w/ 8 traffic slots, 13th/26th frame w/ 8 „associated“ slots

  → raw rate $^{24}/_{26}$ of (114b per (8*577µs)) = (114*12) / (8*577*13*10^{-6}) ≈ 22.8 kbps
- typical packet size: 456 bits (= 8 blocks of 57 bits ^= 20ms, see next slide)
- interleaving of blocks & bits (e.g.: bit 1-8 of 456 → bit 1 of blocks 1-8 etc.)

Note: GSM channel always frequency ch. number C_n plus timeslot no. t_n (C_n, t_n)

Dr. Erwin Aitenbichler
Prof. Dr. M. Mühlhäuser
Telekooperation

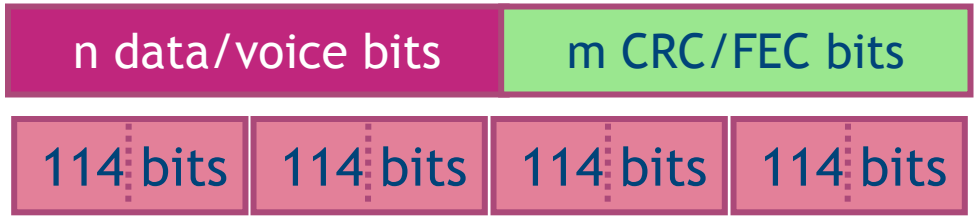
GSM Frame Hierarchy



GSM logical channel data rates

Data rate for logical channel LC?

- how many bursts out of 26 (51) in given (C_n, t_n) are used for LC?
  may be 24in26 (full rate traffic), 1in26, xin51
- „data“ bit percentage („raw“ msg. usually 8 blocks, 4 bursts, 456 bits)?
  note: for 24in26-types, 4 bursts take 1/6 in multiframe26, i.e. 20ms



- e.g., voice data rate: 13 kbps (samples of 20ms → 260 bits)

  Note:
  - GSM-„vocoder“: LPC : linear prediction codec
    with long-term prediction LTP (of waveform)
  - plus „error correction“ called RPE (regular pulse excitation)
- e.g., data channel: 9.6 kbps → 192 bit in 20 ms
  in RLP (radio link protocol) frame: 240 bit (12 kbps)
- e.g., fast signaling channel: 9.2 kbps → 184 bit in 20 ms

Data services in GSM

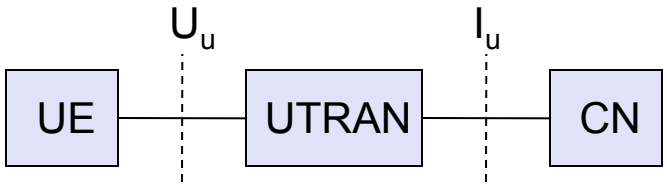
- CSD (Circuit Switched Data)
  - Data transmission standardized with only 9.6 kbit/s
  - advanced coding allows 14,4 kbit/s
  - not enough for Internet and multimedia applications
- HSCSD (High-Speed Circuit Switched Data)
  - bundling of several time-slots to get higher AIUR
    (Air Interface User Rate), e.g., 57.6 kbit/s using 4 slots, 14.4 each
  - advantage: ready to use, constant quality, simple
  - disadvantage: channels blocked (no voice transmission; cost!)
  - disadv.: equipment not ready for simultaneous xmit/rcv → ≤4 (2?) slots
- GPRS (General Packet Radio Service)
  - packet switching
  - using free slots only if data packets ready to send
    (e.g., 115 kbps using 8 slots temporarily: 8*14.4)
  - standardization 1998, introduction 2000

UMTS, architecture

UMTS: learning from enhancements of GSM

- EDGE (Enhanced Data rates for GSM Evolution): GSM up to 384 kbps
- CAMEL (Customized Application for Mobile Enhanced Logic)
- VHE (virtual Home Environment)

- fits into GMM (Global Multimedia Mobility) initiative from ETSI
- requirements
  - min. 144 kbit/s rural (goal: 384 kbit/s) at up to 500 km/h
  - min. 384 kbit/s suburban (goal: 512 kbit/s) at up to 120 km/h
  - up to 2 Mbit/s city at up to 10 km/h
- main standard today: UTRA (UMTS Terrestrial Radio Access)



UTRAN: UTRA Net, i.e.

- cell level mobility;
- Radio Net Subsystem (RNS)

UE: (User Equipment)

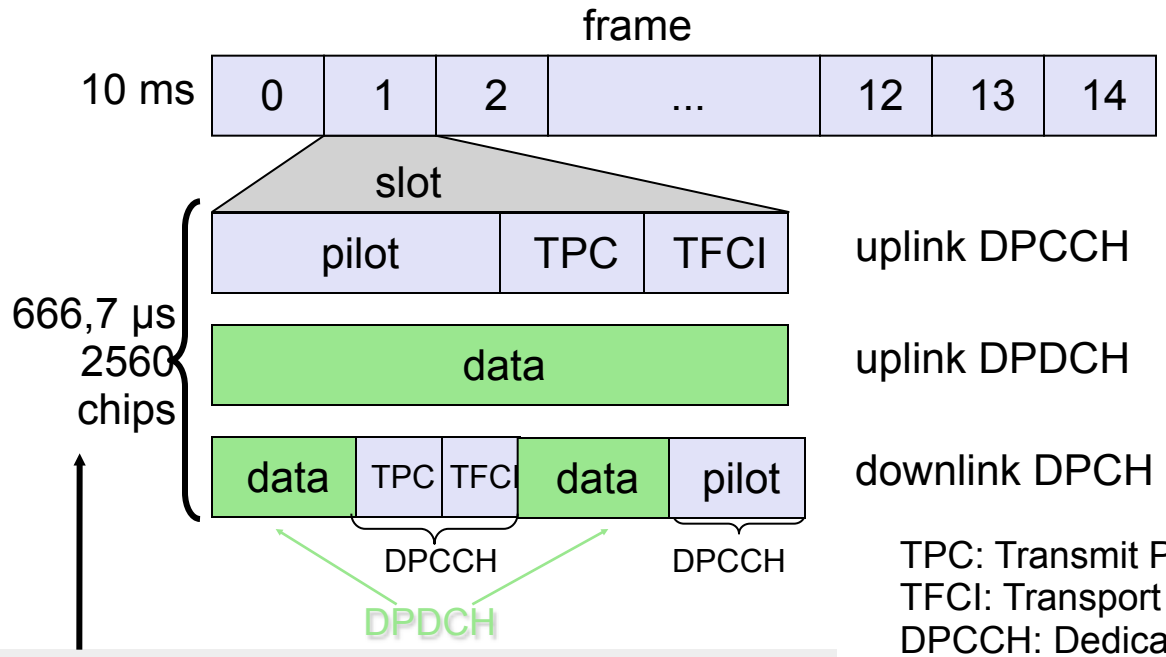
CN: Core Network: inter sys handover

Dr. Erwin Aitenbichler
Prof. Dr. M. Mühlhäuser
Telekooperation

UMTS Frame Structure

W-CDMA (Europe)

- 1920-1980 MHz uplink, 2110-2170 MHz downlink
- chipping rate: 3,84 Mchip/s; data rate determined by ratio chips/bit
- OVSF: orthogonal variable spreading factor may be 3 * ¼ + 1/8 + 2* 1/16 bandwidth
- max. data rate p. user (1/4 spread): 960 kbps, in principle max. 6 channels (reality: 2)
- soft handover, localization of MS with ca. 20 m precision (?)
- complex power control (1500 power control cycles/s)



DPDCH	60	240	960
→ spread factor	64	16	4
DPCCH	15	15	15

user data rate < ½ DPDCH rate: convolution or turbo codes used for FEC; plus: only 2^k spread allowed
→ 384 kbps user ↔ 960 kbps raw

spread factor 4 means here: 640 bits
(times 15, times 100 frames per sec) → 960 kbps

TPC: Transmit Power Control
TFCI: Transport Format Control Identifier
DPCCH: Dedicated Physical Control Channel
DPDCH: Dedicated Physical Data Channel
DPCH: Dedicated Physical Channel

8. WLAN – here: 802.11 Standard

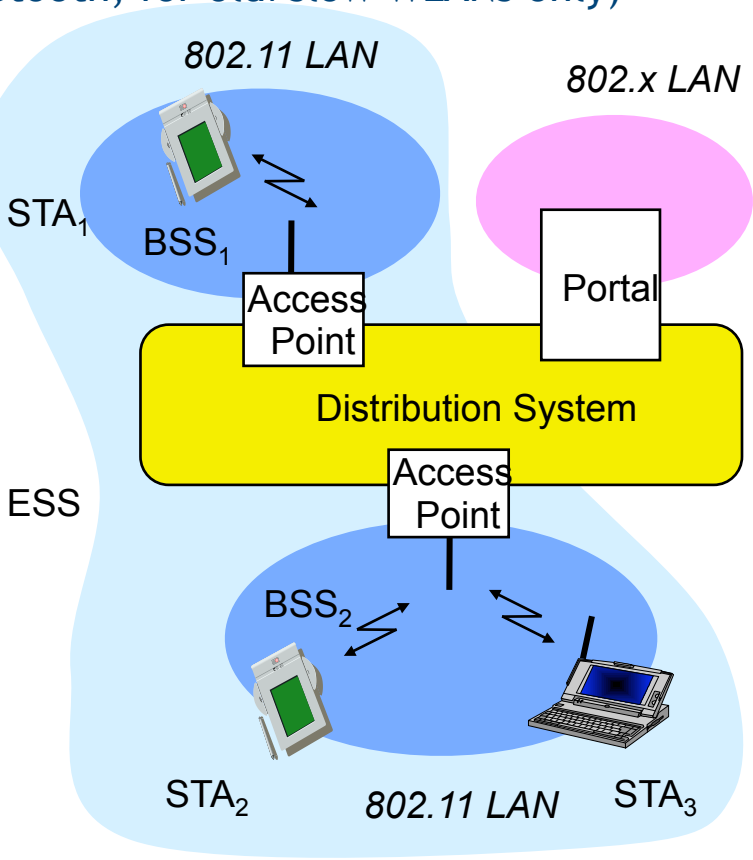
Supports “AdHoc Networks” and “Infrastructure Networks”

Supports “WLAN cells” → roaming

FH: same pseudo random hopping per domain (cf. Bluetooth; for old/slow WLANs only)

DS: standard chipping sequence; different time shift, stations „know“ domain

unlicensed ISM band (industry, science, med.)
[PCS: licensed extension]
ISM: 0.9 (not Europe!) / 2.4 / 5.8 / ~60? GHz



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 same radio freq.

Access Point

- station integrated into WLAN *and* distr. system

Portal: bridge to other (wired) networks

Distribution System: interconnection net →
one logical net (ESS: Extended Service Set) based on several BSS

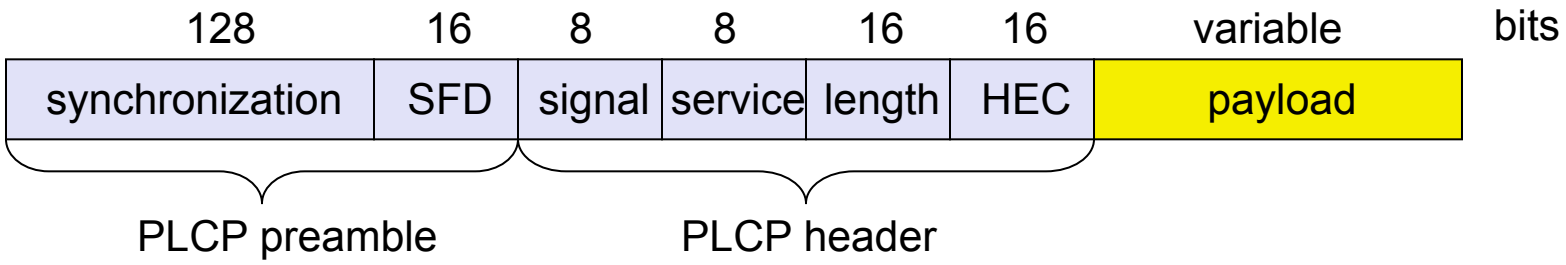
802.11 - Physical layer

- 3 versions: 2 radio (typical 2.4 GHz), 1 IR
  - data rates 1 or 2 Mbps → 3 (FHSS) & 11 (DSSS) Mbps
- FHSS (Frequency Hopping Spread Spectrum)
  - spreading, despreading, signal strength, typ. 1 Mbps
  - min. 2.5 frequency hops/s (USA), two-level GFSK modulation
- DSSS (Direct Sequence Spread Spectrum)
  - DBPSK modulation for 1 Mbps (Differential Binary Phase Shift Keying), DQPSK for higher rates (Differential Quadrature PSK)
  - preamble and header of a frame is always transmitted with 1 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, synchronization

Dr. Erwin Aitenbichler
Prof. Dr. M. Mühlhäuser
Telekooperation

DSSS PHY packet format

- Note: DSSS PHY packet different from FHSS PHY packet!
- 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 / length of the payload
- HEC (Header Error Check)
  - protection of signal, service and length, $x^{16}+x^{12}+x^5+1$

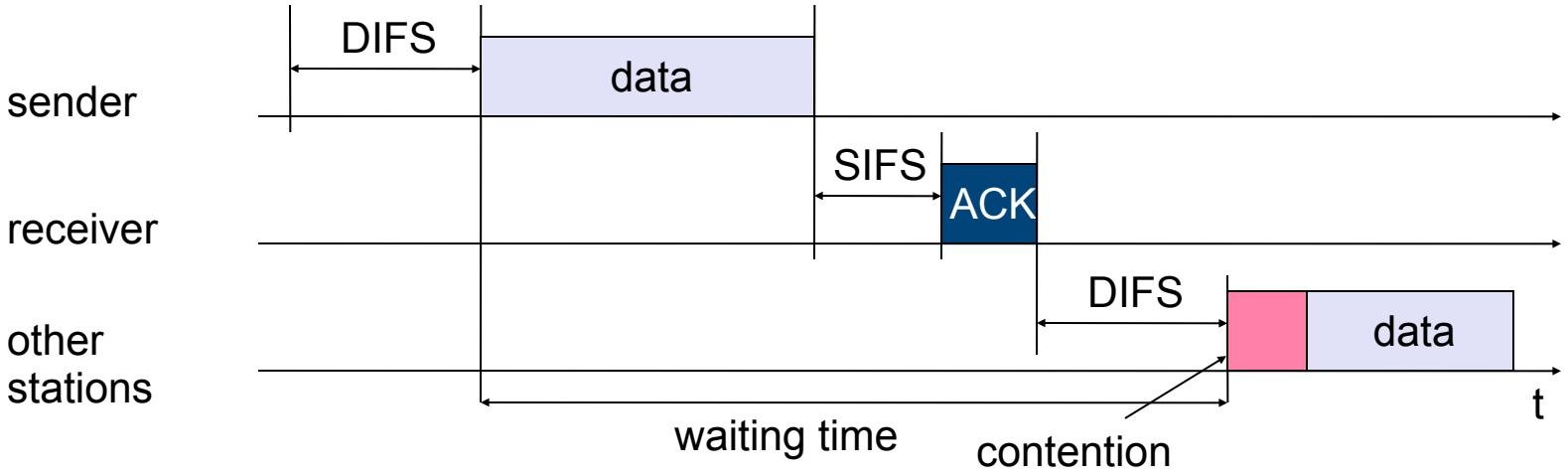


802.11 - MAC layer I - DFWMAC

- 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 = Distributed Foundation Wireless MAC (distributed „D“ or polling based „P“ access ctrl. functions DCF/PCF)
  - 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)
    - avoids hidden terminal problem
  - DFWMAC- PCF (optional)
    - access point polls terminals according to a list

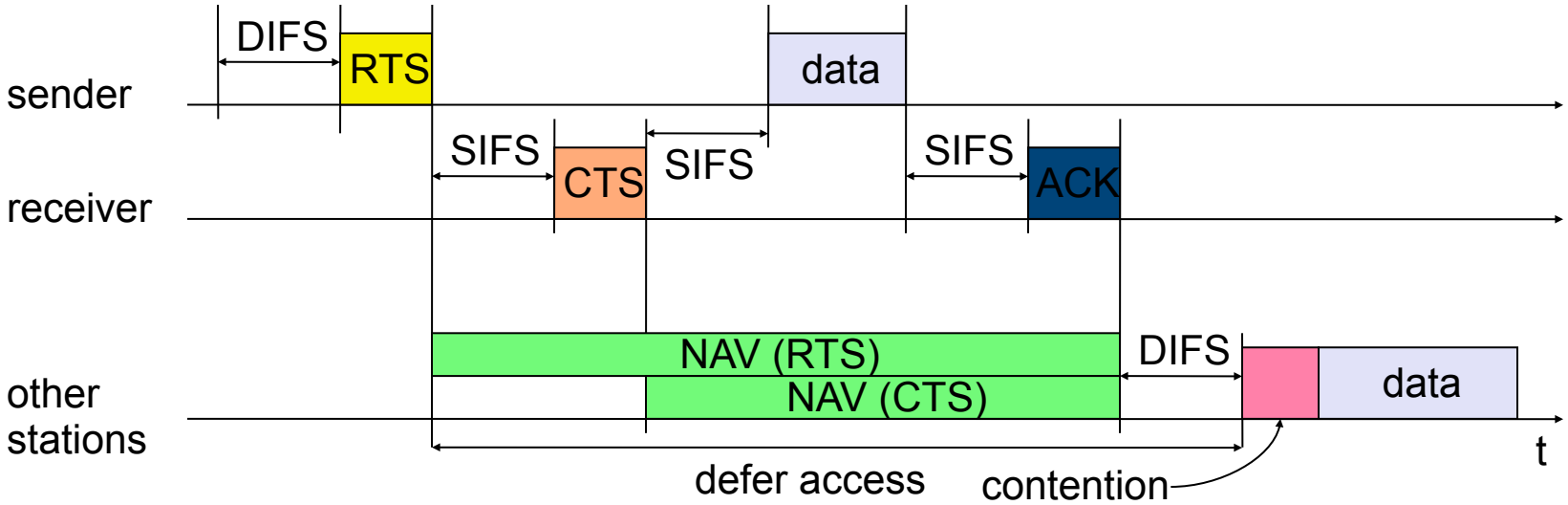
802.11 - CSMA/CA detail

- remember: CSMA/CA
  - DIFS = Data Inter-Frame Spacing, SIFS = Signal Inter-Frame Spacing
- here: acknowledging 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



802.11 – DFWMAC w/ RTS/CTS

- Sending unicast packets
  - station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs 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
  - optional fragmentation (data fragmented → reduced error probability

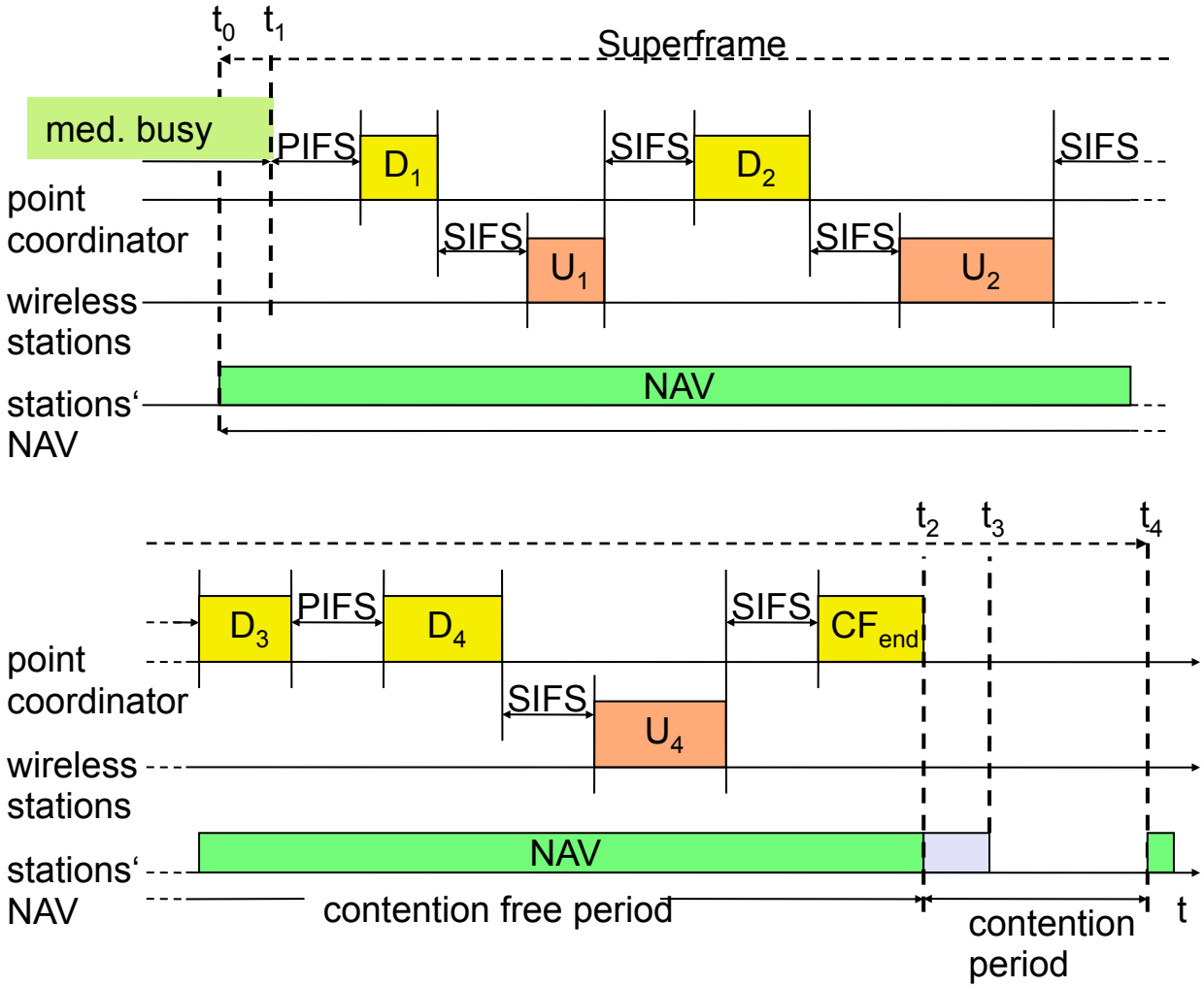


NAV: Net allocation vector (min. forbidden time for other stations)

Dr. Erwin Aitenbichler
Prof. Dr. M. Mühlhäuser
Telekooperation

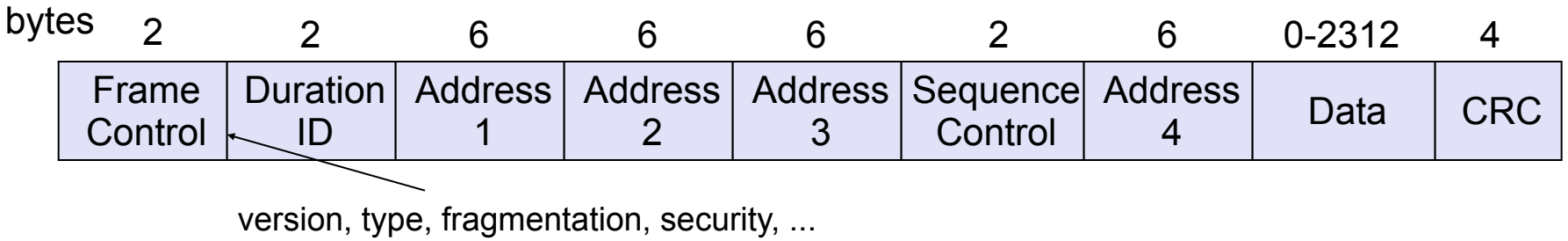
802.11: DFWMAC w/ PCF

point coordinator determines access (down/up link); polling & contention phases may alter



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



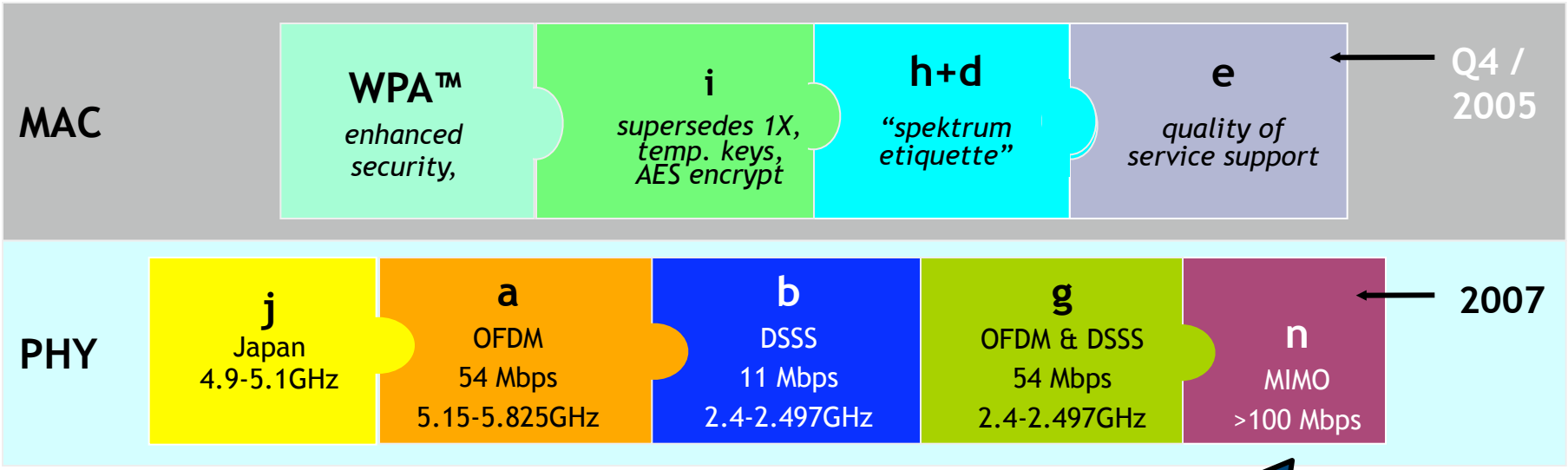
scenario	to DS	from DS	addr. 1	addr. 2	addr. 3	addr. 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
infrastructure network, within DS	1	1	RA	TA	DA	SA

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

Dr. Erwin Aitenbichler
Prof. Dr. M. Mühlhäuser
Telekooperation

IEEE 802.11 sub-standards

802.11: 2.4 GHz, 2 Mbps, FHSS and DSSS (5Mbps not standard)
802.11b: 2.4 GHz, 11 Mbps, DSSS
802.11a: 5 GHz, 54 Mbps, OFDM
802.11g: 2.4 GHz, 54 Mbps, OFDM & DSSS



802.11i: security (considered safe)
802.11e: quality of service (QoS)
802.11n: high throughput via MIMO

and more every couple of months

Summary: Mobile Networks

- Physics
  - Electromagnetic Spectrum
  - Effects caused by obstacles: shadowing, reflection, scattering, diffraction
- Intersymbol Interference
  - Hidden-Terminal Problem, Exposed-Terminal Problem
- Effects of Path Loss
- Cellular Networks
- Multiplex: SDMA, FDMA, TDMA, CDMA
- Concurrent Access: ALOHA, CSMA
- Modulation
- Case Studies
  - Bluetooth
  - ZigBee
  - GSM, UMTS
  - 802.11