Kiel University
Christian-Albrechts-Universität zu Kiel

Research Group
Distributed Systems

# Internet of Things & Wireless Networks

## Wireless LANs - Lectures 6 to 8

(Matches Chapter 7 in the Course Book)

Olaf Landsiedel
Lecture today via Video from Jochen Schiller, FU Berlin

Summer Term 2020

Prof. Dr.-Ing Jochen H. Schiller
Inst. of Computer Science
Freie Universität Berlin
Germany

Freie Universität Berlin

# Mobile Communications
# Chapter 7: Wireless LANs

Characteristics
IEEE 802.11 (PHY, MAC, Roaming, .11a, b, g, h, i, n … z, ac, ad, …, ay, az, ba, bb, …)
Bluetooth / IEEE 802.15.x
IEEE 802.16/.18/.19/.21/.22
RFID
Comparison

# Mobile Communication Technology according to IEEE (examples)

**WiFi**

Local wireless networks
**WLAN** 802.11

- 802.11a → 802.11h
- 802.11i/e/…/n/…/z/az/ba/bb…
- 802.11b → 802.11g

**ZigBee**

Personal wireless nw
**WPAN** 802.15

- 802.15.4 → 802.15.4a/b/c/d/e/f/g…q/r/s
- 802.15.5, .6 (WBAN), …
- 802.15.3 → 802.15.3b/c…e
- 802.15.2
- 802.15.1

**Bluetooth**

Wireless distribution networks
**WMAN** 802.16 (Broadband Wireless Access) **WiMAX**

**+ Mobility**

[hist.: 802.20 (Mobile Broadband Wireless Access)]
802.16e (addition to .16 for mobile devices)

# Characteristics of wireless LANs

Advantages

- very flexible within the reception area
- ad-hoc networks without previous planning possible
- (almost) no wiring difficulties (e.g. historic buildings, firewalls)
- more robust against disasters like, e.g., earthquakes, fires - or users pulling a plug...

Disadvantages

- typically low bandwidth compared to wired networks (1-10 Mbit/s) due to shared medium, lots of interference
- different/proprietary solutions, especially for higher bit-rates or low-power, standards take their time (e.g. IEEE 802.11n, ac), devices have to fall back to older/standard solutions
- products have to follow many national restrictions if working wireless, it takes a very long time to establish global solutions like, e.g., IMT-2000

# Design goals for wireless LANs

- global, seamless operation
- low power for battery use
- no special permissions or licenses needed to use the LAN
- robust transmission technology
- simplified spontaneous cooperation at meetings
- easy to use for everyone, simple management
- protection of investment in wired networks
- security (no one should be able to read my data), privacy (no one should be able to collect user profiles), safety (low radiation)
- transparency concerning applications and higher layer protocols, but also location awareness if necessary
- …

# Comparison: infrastructure vs. ad-hoc vs. mesh networks

# 802.11 – Classical 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 (EES: 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

# 802.11 - Architecture of a mesh network

Mesh BSS forming a meshed network with possibly redundant paths using the Hybrid Wireless Mesh Protocol (HWMP)

Mesh Gate, AP and DS can be co-located in one device

# 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 (historical)

3 versions: 2 radio (typ. 2.4 GHz), 1 IR
- data rates 1 or 2 Mbit/s

FHSS (Frequency Hopping Spread Spectrum) - obsolete
- 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 - obsolete
- 850-950 nm, diffuse light, typ. 10 m range
- carrier detection, energy detection, synchronization

# DSSS PHY packet format (legacy)

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
- future use, 00: 802.11 compliant

Length
- length of the payload

HEC (Header Error Check)
- protection of signal, service and length, $x^{16}+x^{12}+x^{5}+1$

# IEEE 802.11 HR/DSSS – PHY frame formats (was 802.11b)

High Rate Direct Sequence Spread Spectrum @ 2.4GHz

Data rate

- 1, 2, 5.5, 11 Mbit/s, depending on SNR
- User data rate max. approx. 6 Mbit/s

Long PLCP PPDU format

Short PLCP PPDU format (optional)

# Channel selection (non-overlapping)

# IEEE 802.11 OFDM – PHY frame format (was 802.11a)

Orthogonal Frequency Division Multiplexing @ 5GHz

## Data rates

- E.g. 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s, depending on SNR and channel width
- 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

# Operating channels of 802.11a in Europe

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

# Operating channels for 802.11a / US U-NII

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

# OFDM in IEEE 802.11

OFDM with 52 used subcarriers (64 in total)

- 48 data + 4 pilot
  - (plus 12 virtual subcarriers)
- 312.5 kHz spacing

# IEEE 802.11 ERP – PHY frame formats (was 802.11g)

Extended Rate PHY @ 2.4GHz

Data rates

- Builds on classical 1, 2 Mbit/s (DSSS) and 1, 2, 5.5, 11 Mbit/s (HR DSSS)
- Uses additionally OFDM for 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/s (thus check 802.11 OFDM for frame formats)

Many more options and modulation modes standardized but obsolete or deprecated.

Basically, it applies the old 802.11a @ 2.4 GHz.

# IEEE 802.11 HT – PHY frame formats (was 802.11n)

High Throughput (HT) Orthogonal Frequency Division Multiplexing (OFDM) system @ 2.4 and 5 GHz

Based on the OFDM system, but now using up to 4 spatial stream operating in 20 MHz bandwidth (additionally, 40 MHz bandwidth specified offering up to 600 Mbit/s)

| Element | Description |
|---|---|
| L-STF | Non-HT Short Training field |
| L-LTF | Non-HT Long Training field |
| L-SIG | Non-HT SIGNAL field |
| HT-SIG | HT SIGNAL field |
| HT-STF | HT Short Training field |
| HT-GF-STF | HT-Greenfield Short Training field |
| HT-LTF1 | First HT Long Training field (Data) |
| HT-LTFs | Additional HT Long Training fields (Data and Extension) |
| Data | The Data field includes the PSDU |

IEEE
Std 802.11-2012

# IEEE 802.11 HT – PHY frame formats (was 802.11n)

# 802.11 - MAC layer architecture

# How to access the medium in 802.11

Distributed Coordination Function (DCF)

- Fundamental access method in 802.11, mandatory
- Also known as CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)
- Random backoff, certain fairness, refinement with RTS/CTS possible

Point Coordination Function (not really used)

- Contention free access, reservation of the medium

Hybrid Coordination Function (HCF)

- QoS support by combining DCF and PCF
- Contention-based channel access (Enhanced Distributed Channel Access, EDCA) and controlled channel access (HCF Controlled Channel Access, HCCA)
- Support of different priorities for, e.g., background, best effort, video, voice traffic

Mesh Coordination Function (MCF)

- Only in a MBSS, EDCA for contention-based access, MCCA (MCS Controlled Channel Access) for contention-free access

# 802.11 - MAC Inter Frame Space

Priorities of packets defined through different inter frame spaces (not always guaranteed)

- RIFS (Reduced IFS)
  - shortest IFS, reduced overhead, only if no SIFS expected, for higher throughput
- SIFS (Short IFS)
  - for ACK, CTS, polling response
- PIFS (PCF IFS)
  - for time-bounded service using PCF
- DIFS (DCF IFS)
  - for “normal” asynchronous data service
- AIFS (Arbitration IFS)
  - Variable depending on QoS
- EIFS (Extended IFS)
  - IFS e.g. after an incorrect FCS

# 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 (FCS)
- automatic retransmission of data packets in case of transmission errors, but exponential increase of contention window

# 802.11 – DCF with 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 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

# 802.11 – MAC 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

- Only the first three and the last field are present in all frames!
- 802.11ac allows for a variable frame body

| bytes | 2 | 2 | 6 | 6 | 6 | 2 | 6 | 2 | 4 | 0-7951 | 4 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Frame Control | Duration/ ID | Address 1 | Address 2 | Address 3 | Sequence Control | Address 4 | QoS Control | HT Control | Frame Body | FCS |

| bits | 2 | 2 | 4 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Protocol version | Type | Subtype | To DS | From DS | More Frag | Retry | Power Mgmt | More Data | Protec-ted Frame | Order |

# MAC address format (examples)

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

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

Acknowledgement

ACK

| bytes | 2 | 2 | 6 | 4 |
|---|---|---|---|---|
| | Frame Control | Duration | Receiver Address | FCS |

Request To Send

RTS

| bytes | 2 | 2 | 6 | 6 | 4 |
|---|---|---|---|---|---|
| | Frame Control | Duration | Receiver Address | Transmitter Address | FCS |

Clear To Send

CTS

| bytes | 2 | 2 | 6 | 4 |
|---|---|---|---|---|
| | Frame Control | Duration | Receiver Address | FCS |

# 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?)

APSD (Automatic Power Save Delivery)

- new method in 802.11e replacing above schemes

# 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

- 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

Fast roaming – 802.11r

- e.g. for vehicle-to-roadside networks

# WLAN: IEEE 802.11 – current developments (06/2015)

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… supported by HCCA (HCF (Hybrid Coordinator Function) Controlled Channel Access, optional)
- Additional energy saving mechanisms and more efficient retransmission
- EDCA (Enhanced Distributed Channel Access): high priority traffic waits less for channel access

802.11F: Inter-Access Point Protocol (withdrawn)
- 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
- 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)

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

# WLAN: IEEE 802.11 – current developments (06/2015)

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 802.11-2007 standard

**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

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

**802.11-2012: Current “complete” standard – 2793 pages!**
- Comprises many amendments

# WLAN: IEEE 802.11 – current developments (06/2013)

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.

802.11y: Extensions for the 3650-3700 MHz band in the USA

802.11z: Extension to direct link setup

802.11aa: Robust audio/video stream transport

**802.11ac**: Very High Throughput <6Ghz – up to almost 7 Gbit/s @ 5GHz using 8x8 MIMO

802.11ad: Very High Throughput in 60 GHz

802.11af: TV white space, ah: sub 1GHz, ai: fast initial link set-up; … aq: pre-association discovery, ax: High Efficiency Wireless LAN (HEW), ay: Next Generation 60 GHz (NG60), az: Next Generation Positioning (NGP)

Note: Not all “standards” will end in products, many ideas get stuck at working group level

Info: www.ieee802.org/11/, standards.ieee.org/getieee802/; dig into Task Group Meetings, e.g., http://www.ieee802.org/11/Reports/tgax_update.htm

# IEEE 802.11ac – The (current) high-speed standard for WLANs

Single link throughput > 500Mbit/s, multi-station > 1 Gbit/s

Bandwidth up to 160 MHz (80 MHz mandatory), up to 8x MIMO, up to 256 QAM, beamforming, SDMA via MIMO

Example home configuration:

- 8-antenna access point, 160 MHz bandwidth, 6.77 Gbit/s
- 4-antenna digital TV, 3.39 Gbit/s
- 2-antenna tablet, 1.69 Gbit/s
- Two 1-antenna smartphones, 867 Mbit/s each

Redefinition of many protocol fields and procedures!

# Bluetooth

Basic idea

- Universal radio interface for ad-hoc wireless connectivity
- Interconnecting computer and peripherals, handheld devices, PDAs, cell phones – replacement of IrDA
- Embedded in other devices, goal: 5€/device (already < 1€)
- Short range (10 m), low power consumption, license-free 2.45 GHz ISM
- Voice and data transmission, approx. 1 Mbit/s gross data rate

One of the first modules (Ericsson).

# Bluetooth

(was: Bluetooth )

History

- 1994: Ericsson (Mattison/Haartsen), “MC-link” project
- Renaming of the project: Bluetooth according to Harald “Blåtand” Gormsen [son of Gorm], King of Denmark in the 10th century
- 1998: foundation of Bluetooth SIG, www.bluetooth.org
- 1999: erection of a rune stone at Ercisson/Lund ;-)
- 2001: first consumer products for mass market, spec. version 1.1 released
- 2005: 5 million chips/week

Bluetooth™

Special Interest Group

- Original founding members: Ericsson, Intel, IBM, Nokia, Toshiba
- Added promoters: 3Com, Agere (was: Lucent), Microsoft, Motorola
- > 10000 members
- Common specification and certification of products

# History and hi-tech…

1999:
Ericsson mobile communications AB reste denna sten till minne av Harald Blåtand, som fick ge sitt namn åt en ny teknologi för trådlös, mobil kommunikation.

# …and the real rune stone

Located in Jelling, Denmark,
erected by King Harald “Blåtand”
in memory of his parents.
The stone has three sides – one side
showing a picture of Christ.

Inscription:
"Harald king executes these sepulchral monuments after Gorm, his father and Thyra, his mother. The Harald who won the whole of Denmark and Norway and turned the Danes to Christianity."

Btw: Blåtand has nothing to do
with a blue tooth…

This could be the “original” colors
of the stone.
Inscription:
“auk tani karthi kristna” (and
made the Danes Christians)

# Characteristics of the classical system

2.4 GHz ISM band, 79 (23) RF channels, 1 MHz carrier spacing

- Channel 0: 2402 MHz … channel 78: 2480 MHz
- G-FSK modulation, 1-100 mW transmit power

FHSS and TDD

- Frequency hopping with 1600 hops/s
- Hopping sequence in a pseudo random fashion, determined by a master
- Time division duplex for send/receive separation

Voice link – SCO (Synchronous Connection Oriented)

- FEC (forward error correction), no retransmission, 64 kbit/s duplex, point-to-point, circuit switched

Data link – ACL (Asynchronous ConnectionLess)

- Asynchronous, fast acknowledge, point-to-multipoint, up to 433.9 kbit/s symmetric or 723.2/57.6 kbit/s asymmetric, packet switched

Topology

- Overlapping piconets (stars) forming a scatternet

# Piconet

Collection of devices connected in an ad hoc fashion

One unit acts as master and the others as slaves for the lifetime of the piconet

Master determines hopping pattern, slaves have to synchronize

Each piconet has a unique hopping pattern

Participation in a piconet = synchronization to hopping sequence

Each piconet has one master and up to 7 simultaneous slaves (> 200 could be parked)

M=Master
S=Slave

P=Parked
SB=Standby

# Forming a piconet

All devices in a piconet hop together

- Master gives slaves its clock and device ID
  - Hopping pattern: determined by device ID (48 bit, unique worldwide)
  - Phase in hopping pattern determined by clock

Addressing

- Active Member Address (AMA, 3 bit)
- Parked Member Address (PMA, 8 bit)

# Scatternet

Linking of multiple co-located piconets through the sharing of common master or slave devices

- Devices can be slave in one piconet and master of another

Communication between piconets

- Devices jumping back and forth between the piconets

# Bluetooth protocol stack

AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol

SDP: service discovery protocol
RFCOMM: radio frequency comm.

# Frequency selection during data transmission

# Baseband

Piconet/channel definition

Low-level packet definition

- Access code
  - Channel, device access, e.g., derived from master
- Packet header
  - 1/3-FEC, active member address (broadcast + 7 slaves), link type, alternating bit ARQ/SEQ, checksum

# SCO payload types

# ACL Payload types

# Baseband data rates

| | Type | Payload Header [byte] | User Payload [byte] | FEC | CRC | Symmetric max. Rate [kbit/s] | Asymmetric max. Rate [kbit/s] Forward | Reverse |
|---|---|---|---|---|---|---|---|---|
| ACL, 1 slot | DM1 | 1 | 0-17 | 2/3 | yes | 108.8 | 108.8 | 108.8 |
| | DH1 | 1 | 0-27 | no | yes | 172.8 | 172.8 | 172.8 |
| ACL, 3 slot | DM3 | 2 | 0-121 | 2/3 | yes | 258.1 | 387.2 | 54.4 |
| | DH3 | 2 | 0-183 | no | yes | 390.4 | 585.6 | 86.4 |
| ACL, 5 slot | DM5 | 2 | 0-224 | 2/3 | yes | 286.7 | 477.8 | 36.3 |
| | DH5 | 2 | 0-339 | no | yes | **433.9** | **723.2** | 57.6 |
| ACL | AUX1 | 1 | 0-29 | no | no | 185.6 | 185.6 | 185.6 |
| SCO | HV1 | na | 10 | 1/3 | no | 64.0 | | |
| | HV2 | na | 20 | 2/3 | no | 64.0 | | |
| | HV3 | na | 30 | no | no | 64.0 | | |
| | DV | 1 D | 10+(0-9) D | 2/3 D | yes D | 64.0+57.6 D | | |

*D*ata *M*edium/*H*igh rate, *H*igh-quality *V*oice, *D*ata and *V*oice

# Baseband link types

Polling-based TDD packet transmission

- 625µs slots, master polls slaves

SCO (Synchronous Connection Oriented) – Voice

- Periodic single slot packet assignment, 64 kbit/s full-duplex, point-to-point

ACL (Asynchronous ConnectionLess) – Data

- Variable packet size (1, 3, 5 slots), asymmetric bandwidth, point-to-multipoint

# Robustness

Slow frequency hopping with hopping patterns determined by a master
- Protection from interference on certain frequencies
- Separation from other piconets (FH-CDMA)

Retransmission
- ACL only, very fast

Forward Error Correction
- SCO and ACL

# Baseband states of a Bluetooth device

Standby: do nothing
Inquire: search for other devices
Page: connect to a specific device
Connected: participate in a piconet

Park: release AMA, get PMA
Sniff: listen periodically, not each slot
Hold: stop ACL, SCO still possible, possibly participate in another piconet

# Example: Power consumption/CSR BlueCore2

**Typical Average Current Consumption[1]**

- VDD=1.8V  Temperature = 20°C
- **Mode**

| | |
|---|---|
| - SCO connection HV3 (1s interval Sniff Mode) (Slave) | 26.0 mA |
| - SCO connection HV3 (1s interval Sniff Mode) (Master) | 26.0 mA |
| - SCO connection HV1 (Slave) | 53.0 mA |
| - SCO connection HV1 (Master) | 53.0 mA |
| - ACL data transfer 115.2kbps UART (Master) | 15.5 mA |
| - ACL data transfer 720kbps USB (Slave) | 53.0 mA |
| - ACL data transfer 720kbps USB (Master) | 53.0 mA |
| - ACL connection, Sniff Mode 40ms interval, 38.4kbps UART | 4.0 mA |
| - ACL connection, Sniff Mode 1.28s interval, 38.4kbps UART | 0.5 mA |
| - Parked Slave, 1.28s beacon interval, 38.4kbps UART | 0.6 mA |
| - Standby Mode (Connected to host, no RF activity) | 47.0 µA |
| - Deep Sleep Mode[2] | 20.0 µA |

**Notes:**

- [1] Current consumption is the sum of both BC212015A and the flash.
- [2] Current consumption is for the BC212015A device only.

# Example: Bluetooth/USB adapter (2002: 50€, today: some cents if integrated)

# L2CAP - Logical Link Control and Adaptation Protocol

Simple data link protocol on top of baseband

Connection oriented, connectionless, and signaling channels

Protocol multiplexing
- RFCOMM, SDP, telephony control

Segmentation & reassembly
- Up to 64kbyte user data, 16 bit CRC used from baseband

QoS flow specification per channel
- Follows RFC 1363, specifies delay, jitter, bursts, bandwidth

Group abstraction
- Create/close group, add/remove member

# L2CAP logical channels

# L2CAP packet formats

Connectionless PDU

| 2 | 2 | ≥2 | 0-65533 | bytes |
|---|---|---|---|---|
| length | CID=2 | PSM | payload | |

Connection-oriented PDU

| 2 | 2 | 0-65535 | bytes |
|---|---|---|---|
| length | CID | payload | |

Signalling command PDU

| 2 | 2 | | bytes |
|---|---|---|---|
| length | CID=1 | One or more commands | |

| 1 | 1 | 2 | ≥0 |
|---|---|---|---|
| code | ID | length | data |

# Security

User input (initialization)
PIN (1-16 byte)
Pairing
PIN (1-16 byte)
E2
Authentication key generation
(possibly permanent storage)
E2
link key (128 bit)
Authentication
link key (128 bit)
E3
Encryption key generation
(temporary storage)
E3
encryption key (128 bit)
Encryption
encryption key (128 bit)
Keystream generator
Keystream generator
payload key
Ciphering
payload key
Cipher data
Data
Data

# SDP – Service Discovery Protocol

Inquiry/response protocol for discovering services

- Searching for and browsing services in radio proximity
- Adapted to the highly dynamic environment
- Can be complemented by others like SLP, Jini, Salutation, …
- Defines discovery only, not the usage of services
- Caching of discovered services
- Gradual discovery

Service record format

- Information about services provided by attributes
- Attributes are composed of an 16 bit ID (name) and a value
- values may be derived from 128 bit Universally Unique Identifiers (UUID)

# Additional protocols to support legacy protocols/apps.

RFCOMM

- Emulation of a serial port (supports a large base of legacy applications)
- Allows multiple ports over a single physical channel

Telephony Control Protocol Specification (TCS)

- Call control (setup, release)
- Group management

OBEX

- Exchange of objects, IrDA replacement

WAP

- Interacting with applications on cellular phones

# Profiles

Represent default solutions for a certain usage model
- Vertical slice through the protocol stack
- Basis for interoperability

Generic Access Profile
Service Discovery Application Profile
Cordless Telephony Profile
Intercom Profile
Serial Port Profile
Headset Profile
Dial-up Networking Profile
Fax Profile
LAN Access Profile
Generic Object Exchange Profile
Object Push Profile
File Transfer Profile
Synchronization Profile

**Additional Profiles**
Advanced Audio Distribution
PAN
Audio Video Remote Control
Basic Printing
Basic Imaging
Extended Service Discovery
Generic Audio Video Distribution
Hands Free
Hardcopy Cable Replacement

# Bluetooth versions

Bluetooth 1.1
- also IEEE Standard 802.15.1-2002
- initial stable commercial standard

Bluetooth 1.2
- also IEEE Standard 802.15.1-2005
- eSCO (extended SCO): higher, variable bitrates, retransmission for SCO
- AFH (adaptive frequency hopping) to avoid interference

Bluetooth 2.0 + EDR (2004, no more IEEE)
- EDR (enhanced date rate) of 3.0 Mbit/s for ACL and eSCO
- lower power consumption due to shorter duty cycle

Bluetooth 2.1 + EDR (2007)
- better pairing support, e.g. using NFC
- improved security

Bluetooth 3.0 + HS (2009)
- Bluetooth 2.1 + EDR + IEEE 802.11a/g = 54 Mbit/s

Bluetooth 4.0 (2010), 4.1 (2013), 4.2 (2014)
- Low Energy, much faster connection setup

Bluetooth 5 (2016)
- Longer range (100m) or higher data rate (2 Mbit/s without EDR), localization, no more park state

# WPAN: IEEE 802.15.1 – Bluetooth

Data rate
- Synchronous, connection-oriented: 64 kbit/s
- Asynchronous, connectionless
  - 433.9 kbit/s symmetric
  - 723.2 / 57.6 kbit/s asymmetric

Transmission range
- POS (Personal Operating Space) up to 10 m
- with special transceivers up to 100 m

Frequency
- Free 2.4 GHz ISM-band

Security
- Challenge/response (SAFER+), hopping sequence

Availability
- Integrated into many products, several vendors

Connection set-up time
- Depends on power-mode
- Max. 2.56s, avg. 0.64s

Quality of Service
- Guarantees, ARQ/FEC

Manageability
- Public/private keys needed, key management not specified, simple system integration

Special Advantages/Disadvantages
- Advantage: already integrated into several products, available worldwide, free ISM-band, several vendors, simple system, simple ad-hoc networking, peer to peer, scatternets
- Disadvantage: interference on ISM-band, limited range, max. 8 active devices/network, high set-up latency

# WPAN: IEEE 802.15 – additional developments 1

802.15.2: Coexistance

- Coexistence of Wireless Personal Area Networks (802.15) and Wireless Local Area Networks (802.11), quantify the mutual interference

802.15.3: High-Rate

- Standard for high-rate (20Mbit/s or greater) WPANs, while still low-power/low-cost
- Data Rates: 11, 22, 33, 44, 55 Mbit/s
- Quality of Service isochronous protocol
- Ad hoc peer-to-peer networking
- Security
- Low power consumption
- Low cost
- Designed to meet the demanding requirements of portable consumer imaging and multimedia applications

# WPAN: IEEE 802.15 – additional developments 2

Several working groups extend the 802.15.3 standard

802.15.3a: - withdrawn -
- Alternative PHY with higher data rate as extension to 802.15.3
- Applications: multimedia, picture transmission

802.15.3b:
- Enhanced interoperability of MAC
- Correction of errors and ambiguities in the standard

802.15.3c:
- Alternative PHY at 57-64 GHz
- Goal: data rates above 2 Gbit/s

Not all these working groups really create a standard, not all standards will be found in products later …

# WPAN: IEEE 802.15 – additional developments 3

802.15.4: Low-Rate, Very Low-Power

- Low data rate solution with multi-month to multi-year battery life and very low complexity
- Potential applications are sensors, interactive toys, smart badges, remote controls, and home automation
- Data rates of 20-250 kbit/s, latency down to 15 ms
- Master-Slave or Peer-to-Peer operation
- Up to 254 devices or 64516 simpler nodes
- Support for critical latency devices, such as joysticks
- CSMA/CA channel access (data centric), slotted (beacon) or unslotted
- Automatic network establishment by the PAN coordinator
- Dynamic device addressing, flexible addressing format
- Fully handshaked protocol for transfer reliability
- Power management to ensure low power consumption
- 16 channels in the 2.4 GHz ISM band, 10 channels in the 915 MHz US ISM band and one channel in the European 868 MHz band

Base of the ZigBee technology – www.zigbee.org

# ZigBee

Relation to 802.15.4 similar to Bluetooth / 802.15.1

Pushed by Chipcon (now TI), ember, freescale (Motorola), Honeywell, Mitsubishi, Motorola, Philips, Samsung…

More than 260 members – see www.zigbee.org
- about 11 promoters, 160 participants, 240 adopters
- must be member to commercially use ZigBee spec

ZigBee platforms comprise
- IEEE 802.15.4 for layers 1 and 2
- ZigBee protocol stack up to the applications

# WPAN: IEEE 802.15 – additional developments 4

802.15.4a:
- Alternative PHY with lower data rate as extension to 802.15.4
- Properties: precise localization (< 1m precision), extremely low power consumption, longer range
- Two PHY alternatives
  - UWB (Ultra Wideband): ultra short pulses, communication and localization
  - CSS (Chirp Spread Spectrum): communication only

802.15.4b, c, d, e, f, g, … r, s:
- Extensions, corrections, and clarifications regarding 802.15.4
- Usage of new bands, more flexible security mechanisms
- RFID, smart utility neighborhood (high scalability)

802.15.5: Mesh Networking
- Partial meshes, full meshes
- Range extension, more robustness, longer battery live

802.15.6: Body Area Networks
- Low power networks e.g. for medical or entertainment use

802.15.7: Visible Light Communication ……. and many, many more!

Not all these working groups really create a standard, not all standards will be found in products later … see http://www.ieee802.org/15/

# Some more IEEE standards for mobile communications

IEEE 802.16: Broadband Wireless Access / WirelessMAN / WiMax – dead due to LTE…

- Wireless distribution system, e.g., for the last mile, alternative to DSL
- 75 Mbit/s up to 50 km LOS, up to 10 km NLOS; 2-66 GHz band
- Initial standards without roaming or mobility support
- 802.16e adds mobility support, allows for roaming at 150 km/h

IEEE 802.21: Media Independent Handover Interoperability

- Standardize handover between different 802.x and/or non 802 networks

IEEE 802.22: Wireless Regional Area Networks (WRAN)

- Radio-based PHY/MAC for use by license-exempt devices on a non-interfering basis in spectrum that is allocated to the TV Broadcast Service

# RF Controllers – ISM bands

Data rate
- Typ. up to 115 kbit/s (serial interface)

Transmission range
- 5-100 m, depending on power (typ. 10-500 mW)

Frequency
- Typ. 27 (EU, US), 315 (US), 418 (EU), 426 (Japan), 433 (EU), 868 (EU), 915 (US) MHz (depending on regulations)

Security
- Some products with added processors

Cost
- Cheap: 10€-50€

Availability
- Many products, many vendors

Connection set-up time
- N/A

Quality of Service
- none

Manageability
- Very simple, same as serial interface

Special Advantages/Disadvantages
- Advantage: very low cost, large experience, high volume available
- Disadvantage: no QoS, crowded ISM bands (particularly 27 and 433 MHz), typ. no Medium Access Control, 418 MHz experiences interference with TETRA

# RFID – Radio Frequency Identification (1)

Data rate
- Transmission of ID only (e.g., 48 bit, 64kbit, 1 Mbit)
- 9.6 – 115 kbit/s

Transmission range
- Passive: up to 3 m
- Active: up to 30-100 m
- Simultaneous detection of up to, e.g., 256 tags, scanning of, e.g., 40 tags/s

Frequency
- 125 kHz, 13.56 MHz, 433 MHz, 2.4 GHz, 5.8 GHz and many others

Security
- Application dependent, typ. no crypt. on RFID device

Cost
- Very cheap tags, down to 1€ (passive)

Availability
- Many products, many vendors

Connection set-up time
- Depends on product/medium access scheme (typ. 2 ms per device)

Quality of Service
- none

Manageability
- Very simple, same as serial interface

Special Advantages/Disadvantages
- Advantage: extremely low cost, large experience, high volume available, no power for passive RFIDs needed, large variety of products, relative speeds up to 300 km/h, broad temp. range
- Disadvantage: no QoS, simple denial of service, crowded ISM bands, typ. one-way (activation/ transmission of ID)

# RFID – Radio Frequency Identification (2)

Function

- Standard: In response to a radio interrogation signal from a reader (base station) the RFID tags transmit their ID
- Enhanced: additionally data can be sent to the tags, different media access schemes (collision avoidance)

Features

- No line-of sight required (compared to, e.g., laser scanners)
- RFID tags withstand difficult environmental conditions (sunlight, cold, frost, dirt etc.)
- Products available with read/write memory, smart-card capabilities

Categories

- Passive RFID: operating power comes from the reader over the air which is feasible up to distances of 3 m, low price (1€)
- Active RFID: battery powered, distances up to 100 m

# RFID – Radio Frequency Identification (3)

Applications

- Total asset visibility: tracking of goods during manufacturing, localization of pallets, goods etc.
- Loyalty cards: customers use RFID tags for payment at, e.g., gas stations, collection of buying patterns
- Automated toll collection: RFIDs mounted in windshields allow commuters to drive through toll plazas without stopping
- Others: access control, animal identification, tracking of hazardous material, inventory control, warehouse management, ...

Local Positioning Systems

- GPS useless indoors or underground, problematic in cities with high buildings
- RFID tags transmit signals, receivers estimate the tag location by measuring the signal‘s time of flight

# RFID – Radio Frequency Identification (4)

Security

- Denial-of-Service attacks are always possible
  - Interference of the wireless transmission, shielding of transceivers
- IDs via manufacturing or one time programming
- Key exchange via, e.g., RSA possible, encryption via, e.g., AES

Future Trends

- RTLS: Real-Time Locating System – big efforts to make total asset visibility come true
- Integration of RFID technology into the manufacturing, distribution and logistics chain
- Creation of „electronic manifests“ at item or package level (embedded inexpensive passive RFID tags)
- 3D tracking of children, patients

# RFID – Radio Frequency Identification (5)

Relevant Standards

- American National Standards Institute
  - ANSI, www.ansi.org, www.aimglobal.org/standards/rfidstds/ANSIT6.html
- Automatic Identification and Data Capture Techniques
  - JTC 1/SC 31, www.uc-council.com/sc31/home.htm, www.aimglobal.org/standards/rfidstds/sc31.htm
- European Radiocommunications Office
  - ERO, www.ero.dk, www.aimglobal.org/standards/rfidstds/ERO.htm
- European Telecommunications Standards Institute
  - ETSI, www.etsi.org, www.aimglobal.org/standards/rfidstds/ETSI.htm
- Identification Cards and related devices
  - JTC 1/SC 17, www.sc17.com, www.aimglobal.org/standards/rfidstds/sc17.htm,
- Identification and communication
  - ISO TC 104 / SC 4, www.autoid.org/tc104_sc4_wg2.htm, www.aimglobal.org/standards/rfidstds/TC104.htm
- Road Transport and Traffic Telematics
  - CEN TC 278, www.nni.nl, www.aimglobal.org/standards/rfidstds/CENTC278.htm
- Transport Information and Control Systems
  - ISO/TC204, www.sae.org/technicalcommittees/gits.htm, www.aimglobal.org/standards/rfidstds/ISOTC204.htm

# RFID – Radio Frequency Identification (6)

ISO Standards

- ISO 15418
  - MH10.8.2 Data Identifiers
  - EAN.UCC Application Identifiers
- ISO 15434 - Syntax for High Capacity ADC Media
- ISO 15962 - Transfer Syntax
- ISO 18000
  - Part 2, 125-135 kHz
  - Part 3, 13.56 MHz
  - Part 4, 2.45 GHz
  - Part 5, 5.8 GHz
  - Part 6, UHF (860-930 MHz, 433 MHz)
- ISO 18047 - RFID Device Conformance Test Methods
- ISO 18046 - RF Tag and Interrogator Performance Test Methods

# ISM band interference

Many sources of interference
- Microwave ovens, microwave lighting
- 802.11, 802.11b, 802.11g, 802.15, …
- Even analog TV transmission, surveillance
- Unlicensed metropolitan area networks
- …

Levels of interference
- Physical layer: interference acts like noise
  - Spread spectrum tries to minimize this
  - FEC/interleaving tries to correct
- MAC layer: algorithms not harmonized
  - E.g., Bluetooth might confuse 802.11

© Fusion Lighting, Inc., now used by LG as Plasma Lighting System

# 802.11 vs.(?) 802.15/Bluetooth

Bluetooth may act like a rogue member of the 802.11 network

- Does not know anything about gaps, inter frame spacing etc.

IEEE 802.15-2 discusses these problems

- Proposal: Adaptive Frequency Hopping
  - a non-collaborative Coexistence Mechanism

Real effects? Many different opinions, publications, tests, formulae, …

- Results from complete breakdown to almost no effect
- Bluetooth (FHSS) seems more robust than 802.11b (DSSS)