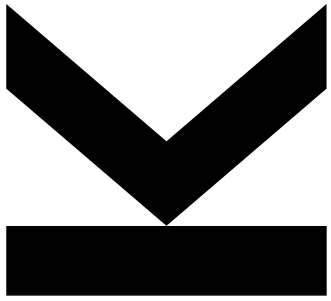
MOBILE COMPUTING (2H, KV)
WS 2019/20

WIRELESS TECHNOLOGIES & SYSTEMS



Mobile Communications and Positioning

Karin Anna Hummel (karin_anna.hummel@jku.at)

OUR CONNECTED WORLD

Major step in digitization: connecting physical world and virtual world through

- **Sensor** technology: **location**, luminance, humidity, accelerometers (motion) …
- **Smartness**: recognizing, adapting, reacting

- **Communication technologies**

karin_anna.hummel@jku.at

***How to connect* mobile devices?**

***How to enable* location/context-based services?**

karin_anna.hummel@jku.at

WIRELESS TECHNOLOGIES

Ultrasound

Iridium

GPS

WiMax

3G/LTE (Long Term Evolution)/4G/5G

NFC (Near Field Communication)

WLAN 802.11n/ac

RFID (Radio Frequency Identification)

ZigBee

Infrared

Bluetooth / Bluetooth LE (Low Energy)

Visible light

LoRa / LoRaWAN (for the Internet of Things)

LECTURE ORGANIZATION

Part I – Wireless Networking

- Principles of wireless communication
- Principles of cellular networks, 3G/4G/5G
- WLAN, Bluetooth

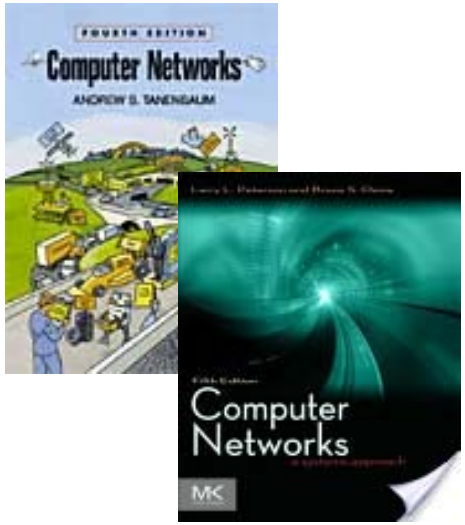
Part II – BREAK-OUT Session

- **Measuring & discussing network performance** (group work)

Part III – Identifying and Locating

- Positioning technologies: GPS, Indoor positioning

LITERATURE



[Tan10] A.S. Tanenbaum. *Computer Networks*, 5th ed., 2010

[Pet11] Peterson, Davie, *Computer Networks*, 5th ed., 2011

WLAN: IEEE 802.11-2012 (March 29, 2012)
http://standards.ieee.org/findstds/standard/802.11-2012.html

Bluetooth: Bluetooth White Paper
http://educypedia.karadimov.info/library/DOC1991.PDF
Bluetooth LE: Core Specification
https://www.bluetooth.org/en-us/specification/adopted-specifications

LoRaWAN Technical description (from LoRa Alliance)
https://lora-alliance.org/resource-hub/what-lorawantm

PRINCIPLES OF WIRELESS COMMUNICATION

- Classification of networks
- Electromagnetic spectrum, frequencies, wireless transmission
- Shared medium and medium access

CLASSIFICATION OF COMPUTER NETWORKS – RANGE (1)

Body Area Network (BAN); mostly wireless

- *A network allowing communication between (human)* ***implanted or near-body components and a station outside the body***
  - Examples: Medical devices
  - Standard: IEEE 802.15.6 (wireless BAN)

[Fraunhofer Institute]

Near Field Communication (NFC) – based networks; wireless

- *Communication between* ***appliances in proximity (close to "touching")***
  - Examples: Key systems, wireless payment
  - Sample technology: RFID

Personal Area Network (PAN); wireless

- *A network of* ***devices used by one person***
  - Examples: Connecting headphone/car media system and smartphone
  - Sample technology/standard: Bluetooth IEEE 802.15.1

CLASSIFICATION OF COMPUTER NETWORKS – RANGE (2)

Local Area Network (LAN); wireless and wired

- *A **private network connecting multiple computers** (and users) which is limited to an area*
  - Examples: High-throughput networking on a campus
  - Sample technology/standard: WLAN IEEE 802.11

Metropolitan Area Network (MAN) ; wireless and wired

- *A **city-scale network** connecting multiple computers (and users)*
  - Examples: High-throughput networking on a city scale
  - Sample technology/standard: WiMax IEEE 802.16

Wide Area Network (WAN)

- *A **global network** connecting multiple computers (and users)*
  - Examples: Internet, network covering a country or continent
  - Sample technology/standard: LTE, LoRaWAN

WIRELESS LINK PERFORMANCE

	Bluetooth (802.15.1)	Wi-Fi (802.11)	3G Cellular
Typical link length	10 m	100 m	Tens of kilometers
Typical data rate	Bluetooth: few Mbit/s with HS: 24 Mbit/s	11n: 600 Mbit/s 11ac: 7 Gbit/s	Hundreds of kbps (per connection)
Typical use	Link a peripheral to a computer	Link a computer to a wired base	Link a mobile phone to a wired tower
Wired technology analogy	USB	Ethernet	DSL

LTE

Downlink

4G LTE: 100Mbit/s

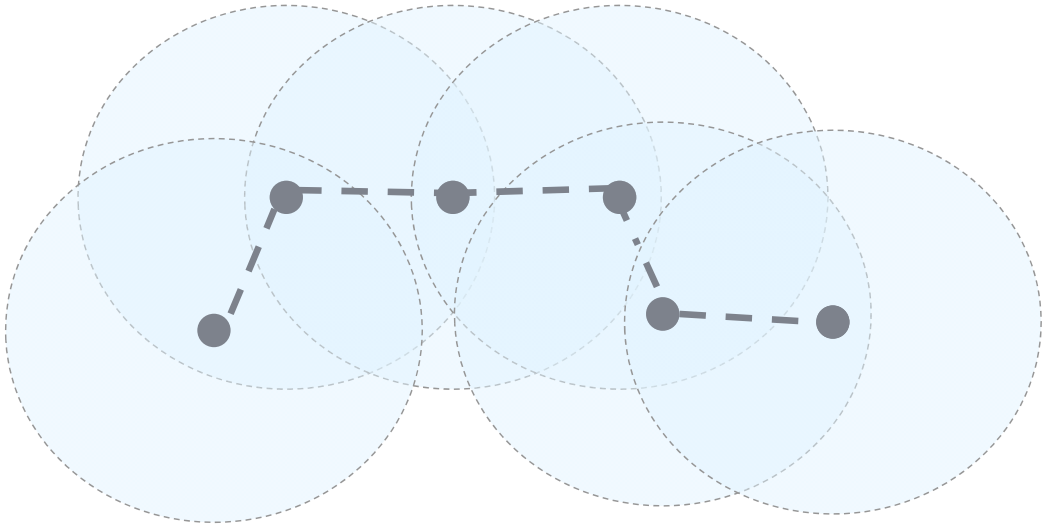
4G LTE Advanced: 1 Gbit/s (low mobility)

After: Peterson, Davie. 'Computer Networks' [Pet11]

Nominal performance numbers; experiments will show lower rates due to:

- Sharing of the network
- Disturbances on the wireless medium (not always optimal conditions)

MODELING WIRELESS TRANSMISSION: 2D DISK MODEL



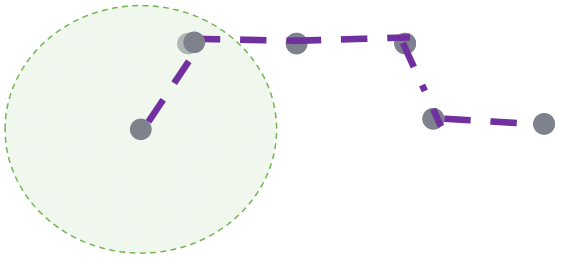
- Signal propagation assumed circular around transmitter
- Disk radius defines communication range
- Outside communication range: no connectivity
- From the disk model → network topology as a graph (nodes and links)

WIRELESS ACCESS NETWORK

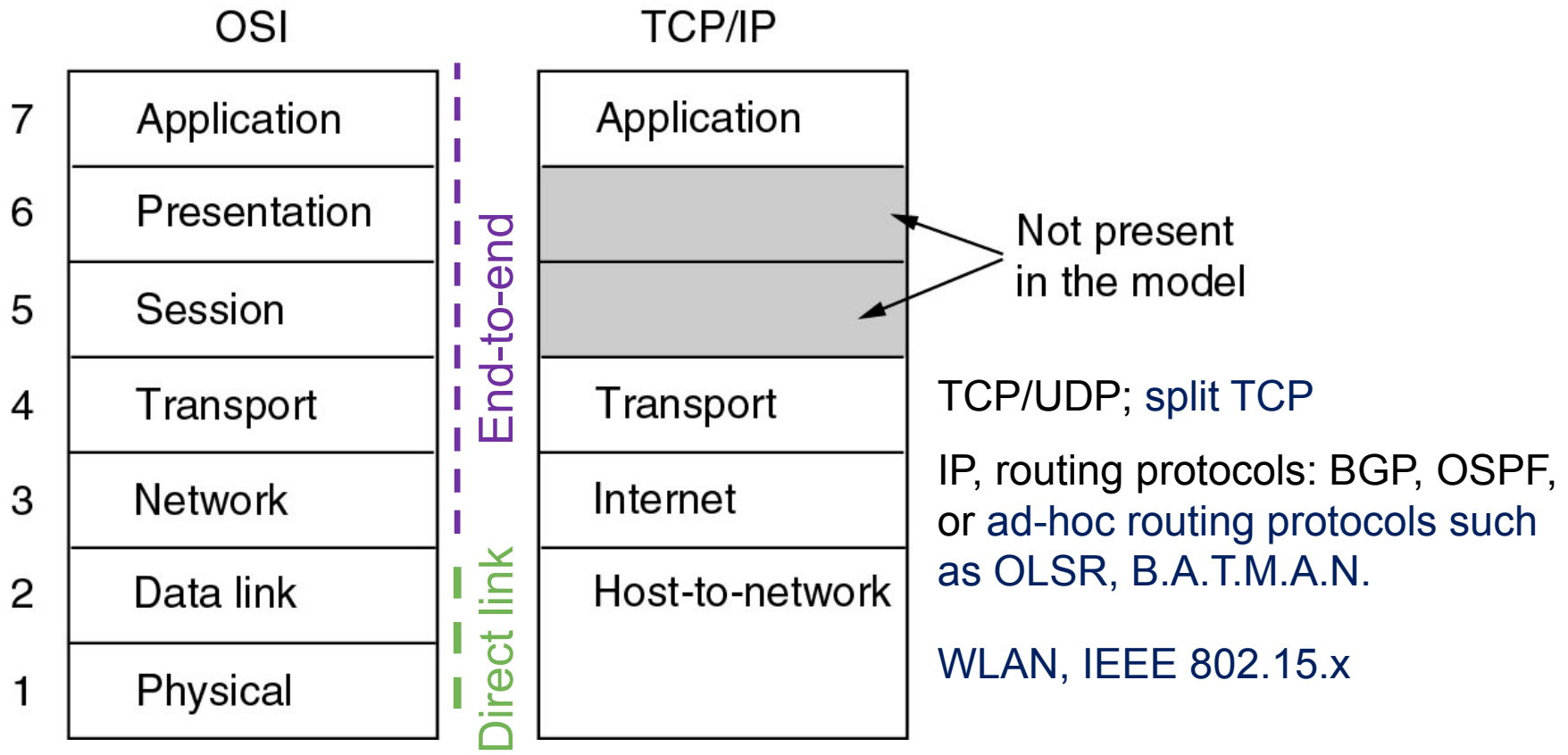
wireless

wired

NETWORK LAYERS



OSI (Open Systems Interconnection) Reference Model
by the International Standardization Organization (ISO); 1983, 1995 revised



TCP/UDP; split TCP

IP, routing protocols: BGP, OSPF, or ad-hoc routing protocols such as OLSR, B.A.T.M.A.N.

WLAN, IEEE 802.15.x

OSI LAYERS (1)

Implemented on all network nodes

Physical Layer (German: “Bitübertragungsschicht”)
- Transmission of raw bits over medium (e.g., wireless LAN), encoding

Data Link Layer (German: “Sicherungsschicht”)
- Transmission of frames (aggregated bits) between hosts
- Error control, flow control, medium access control

Network Layer (German: “Vermittlungsschicht”)
- End-to-end transmission of packets (variable length, datagram service)
- Routing

OSI LAYERS (2)

Implemented typically on end-hosts

Transport Layer (German: “Transportschicht”)

- Transmission of messages between processes
- Quality of service provisioning
- Reliable transfer (retransmission, ordering)
- Segmentation/reassembly, flow control, congestion control

Session Layer (German: “Sitzungsschicht”)

- Synchronization and checkpointing between processes, session management (e.g., restart a service)

Presentation Layer (German: “Darstellungsschicht”)

- Data representation during transmission (e.g., flattening of structures)

Application Layer (German: “Anwendungsschicht”)

- Patterns of communication used by the application (e.g., identifying remote hosts and resource availability, get/set values)

Starting at the physical layer (PHY) …

ELECTROMAGNETIC WAVES

$$f = \frac{c}{\lambda}$$

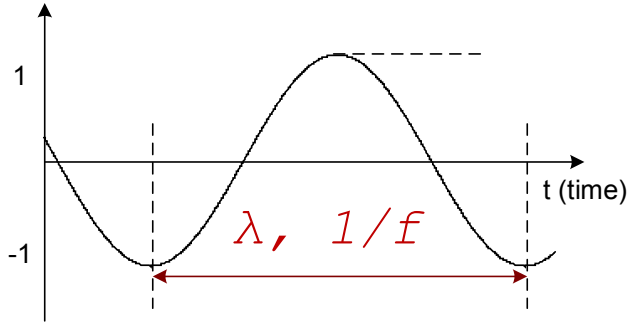
$$f = 100\,MHz \rightarrow \lambda = 3\,m$$
$$f = 1\,GHz \rightarrow \lambda = 0.3\,m$$

Frequency f

- Frequency (general) = Number of events per unit of time
- Frequency of electromagnetic waves
- Units: Hertz (Hz) … Number of wave oscillations per second

Wave length λ

- Distance between two repeating shapes of a propagation wave



Speed of light c

- $c \sim 300\,000\,000 = 3\,x\,10^8\ [\mathrm{m/s}]$

karin_anna.hummel@jku.at

WHY SHOULD WE CARE? – ELECTROM. WAVE CHARACTERISTICS

Electromagnetic waves used for wireless communication

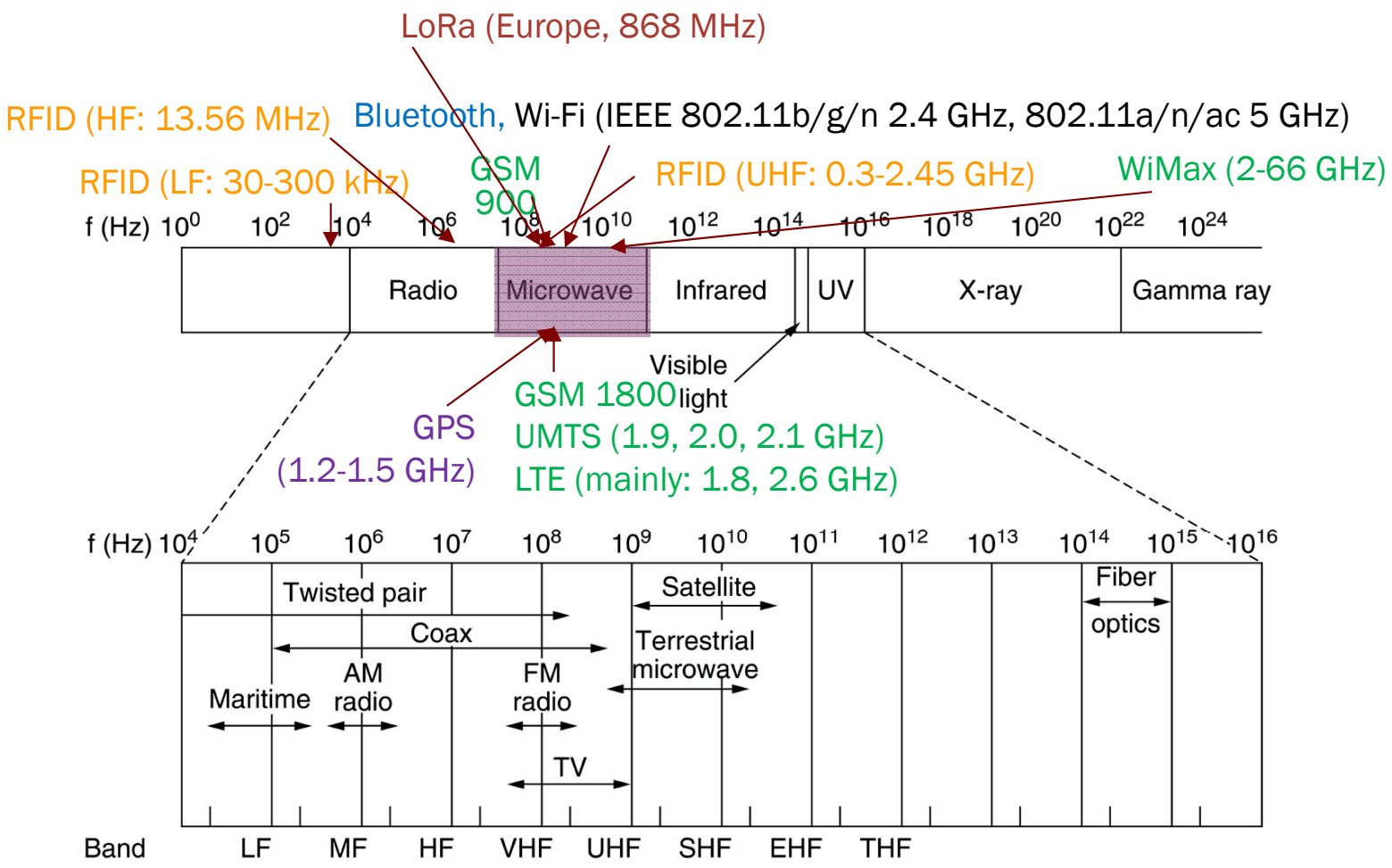
- Radio and microwave (kHz – GHz), Infrared (THz), Visible Light (300 THz)

Wave properties define and limit the characteristics of wireless transmission

- **Lower frequencies** (longer wavelengths) → pervade solid objects better, travel over long distances – Example: Radio pervades walls
- **Higher frequencies** (shorter wavelengths) → higher data rates, but easily disturbed – Example: Infrared cannot pervade walls

*The **bandwidth** is the difference between highest and lowest transmitted frequency (sometimes used synonymous to "throughput").*

ELECTROMAGNETIC SPECTRUM



10^3 … kHz
10^6 … MHz
10^9 … GHz

Source: Tanenbaum: Computer Networks [Tan10]

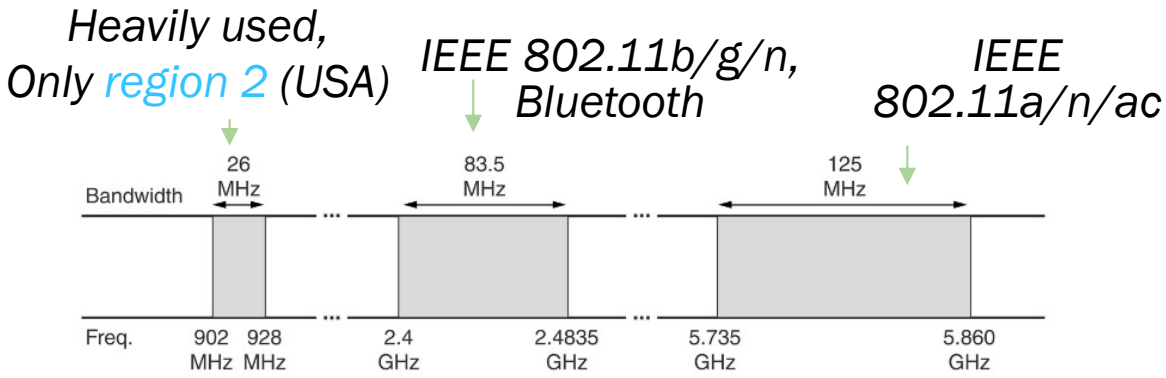
karin_anna.hummel@jku.at

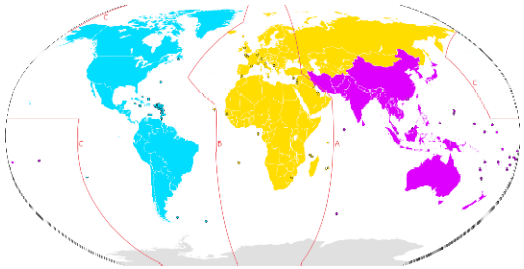
LICENSING OF FREQUENCY BANDS

AT: Rundfunk und Telekom Regulierungs GmbH (RTR, http://www.rtr.at/)

Regulations
- Via licensing of some frequencies; national laws apply
- Examples: Police radio, mobile telephony, TV, military, and …

ISM Band (Industrial, Scientific, Medical)
- Free frequency band





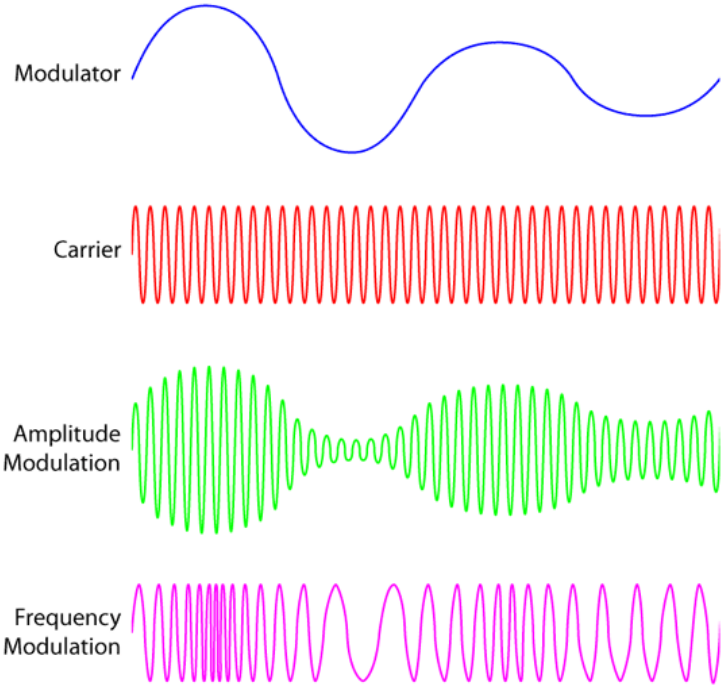
Europe (region 1): 433 MHz

karin_anna.hummel@jku.at

TRANSMISSION OF INFORMATION

Variation of physical characteristics of waves

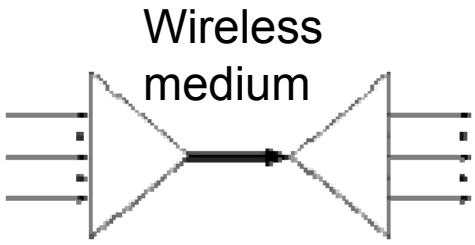
- Frequency Modulation (FM)
- Amplitude Modulation (AM)
- Phase Shift Modulation (PSM)



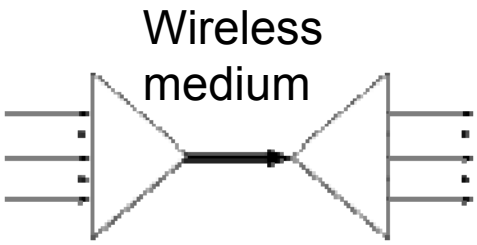
Principle techniques to share the wireless medium

…

between different stations or upper layer channels



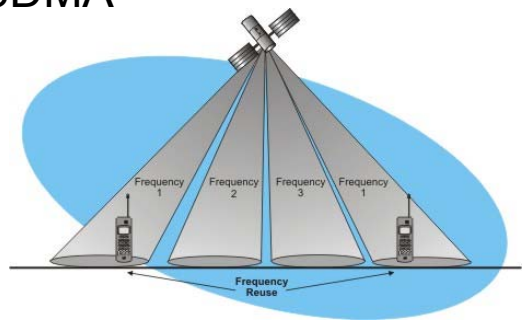
MULTIPLEXING



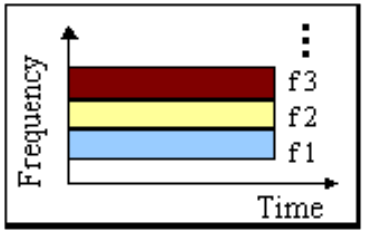
Multiple access to the medium

- Space-division multiple access, SDMA
- Time-division multiple access, TDMA
- Frequency-division multiple access, FDMA
- Code-division multiple access, CDMA

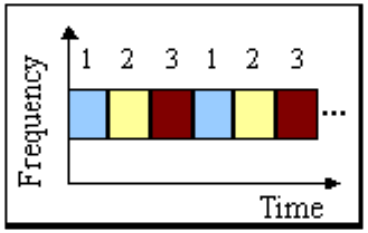
SDMA



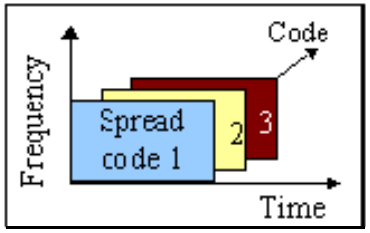
FDMA



TDMA



CDMA



karin_anna.hummel@jku.at

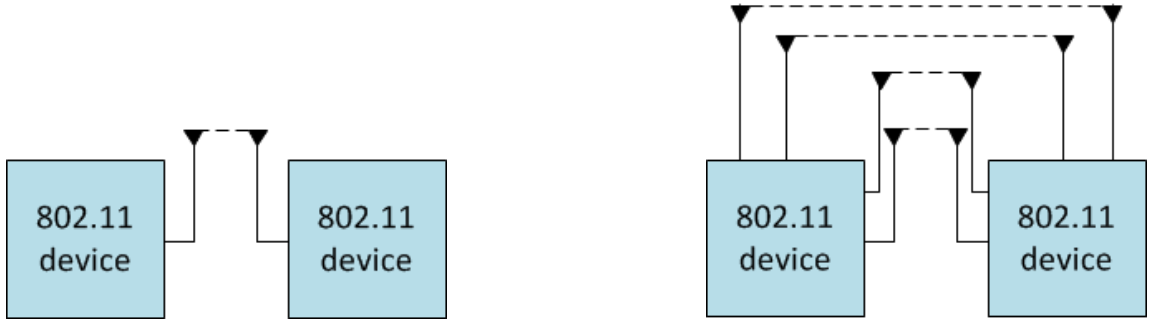
SDMA EXAMPLE: MIMO

– IN A NUTSHELL

Ex.: Planex base station
[http://www. heise.de/mobil/artikel/59219]

Multiple Input Multiple Output

- **THE major step** forward to higher data rates
- Use of multiple antennas (sender and receiver)
  - Sender sends **different signals in parallel**
  - Receiver reconstructs original signals
- Example: WLAN IEEE 802.11n,ac
- Time / frequency / space multiplexing – can be done at the same time



Single in/single out

Multiple in/multiple out

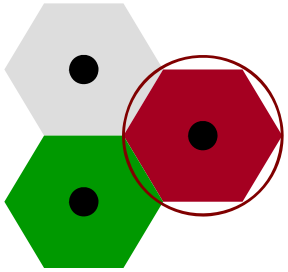
Source: Gast. IEEE 802.11n: A Survival Guide

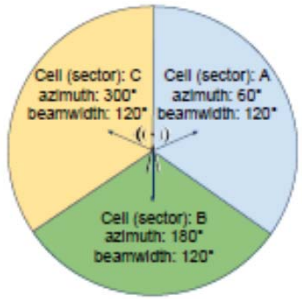
CELLULAR NETWORKS

- Principles of cellular communication
- Evolution: 2G (1992) / 3G (2001) / LTE (2009) and 4G (2012) / 5G (2020)

karin_anna.hummel@jku.at

PRINCIPLE OF CELLULAR NETWORKS





Model

- Mosaic (tesselation) of hexagons
- Cell (hexagon) supported by one “base station”
- (reality: often sectoral antennas)

Base station – manage a cell (in principle)

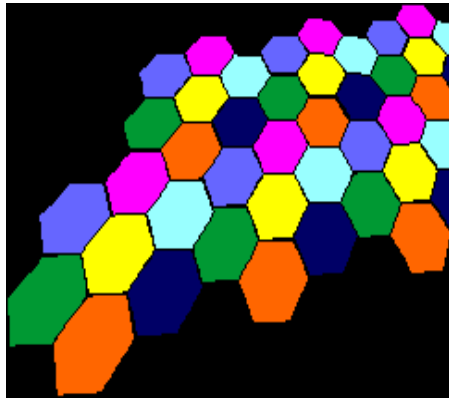
- Connecting to mobile device via air interface, pre-defined frequencies
- Coverage of area (rule of thumb: signal power decreases with $d^2, d \ldots distance$)

Advantages ?

- Time slot reuse, frequency band reuse (cluster of cells)
- Little disturbances due to smaller distance to the base station

Disadvantages ?

- Many base stations have to be installed and interconnected

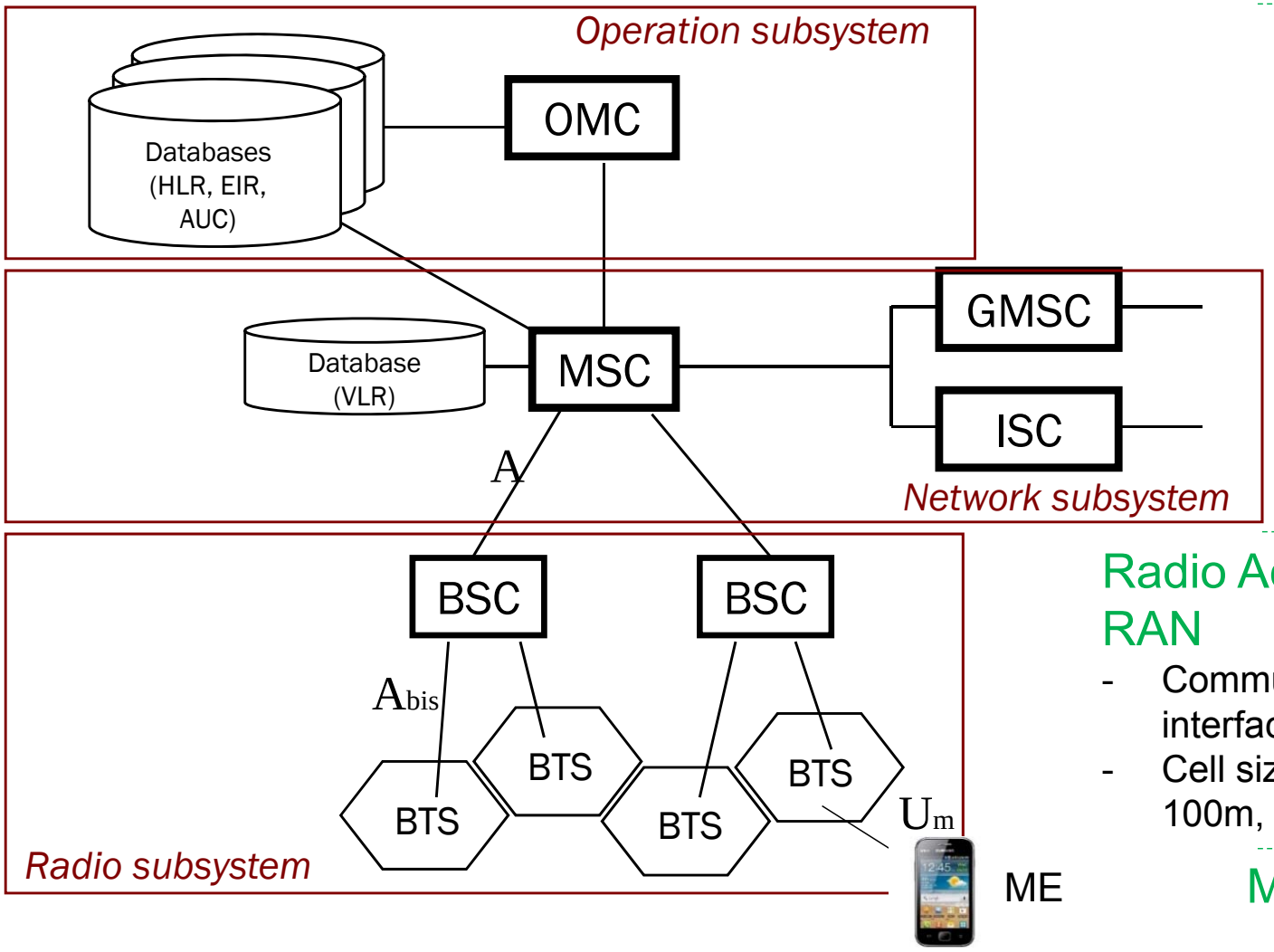


GSM, 2G

Global system for mobile communications

- **Digital** cellular wireless network
- FDD (Frequency Division Duplexing), TDD (Time DD)
- **Major aim:** support of **digital voice transmission**
  - Plus: value added services such as SMS, prepaid card service
- 1989: ETSI (European Telecommunication Standardization Institute) includes “Group Special Mobile” as technical committee
- **Roaming as major concept for mobile users**
  - Intra-country: Handover between network infrastructure elements
  - Inter-country: Roaming-agreement of foreign providers

GSM ARCHITECTURE – OVERVIEW



Core Network
CN

- Switching of calls
- Billing
- Mobility management
- Roaming
- Maintenance
- Monitoring logging

Radio Access Network
RAN

- Communication on air interface
- Cell size (radius).: city ~ 100m, outside cities ~ 35 km

Mobile Equipment

karin_anna.hummel@jku.at

GSM ABBREVIATIONS

HLR/VLR … Home/Visitor Location Register (primary databases for subscribers)
EIR … Equipment Identification Register (hardware database of MEs)
AUC … Authentication Center (authentication handling)
OMC … Operation and Maintenance Center (accounting)
MSC … Mobile Switching Center (switching/routing of calls – localization of MEs)
GMSC … Gateway MSC (gateway to other networks)
ISC … International Switching Center (interface to international networks)
BSC … Base Station Controller
BTS … Base Transceiver Station (radio antenna)

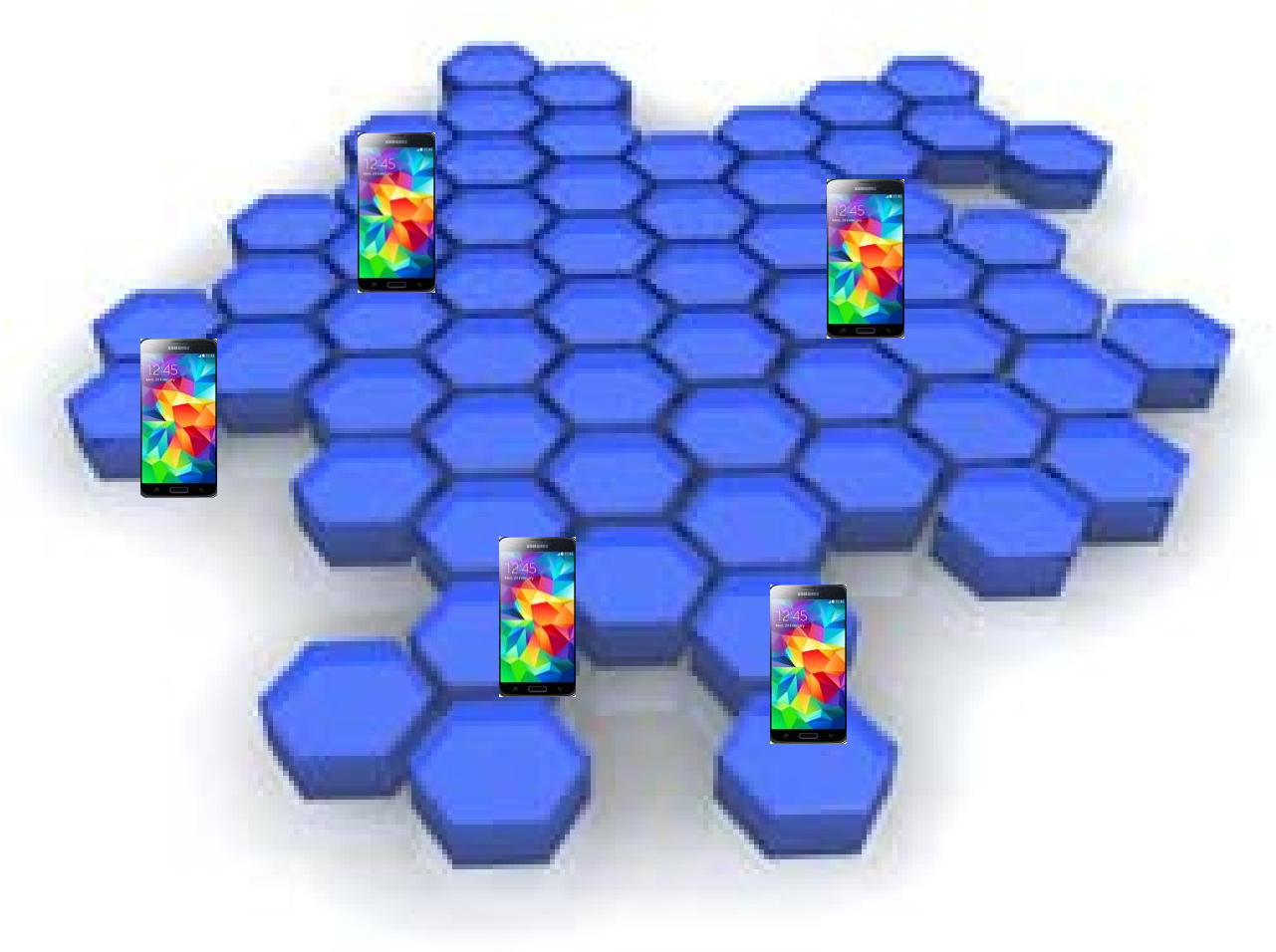
SIM CARD

Subscriber Identity Module: Assigned to a person (legal entity)

- **IMSI (International Mobile Subscriber Identity)**
- Temporary Mobile Subscriber Identity (TMSI)
  - Randomly assigned by the network (every time anew)
  - Valid for location area (of a VLR)
- Personal configuration and data (address book)
- Received SMS messages

When a phone attaches to the network, it sends IMSI to that cell → **IMSI catcher** (“man-in-the-middle-attack”, manhunt, emergencies)

DEVICE MOBILITY



karin_anna.hummel@jku.at

MOBILITY MANAGEMENT

Cell updates

- Performed for active devices
- Not performed for passive devices, only wider areas: location area

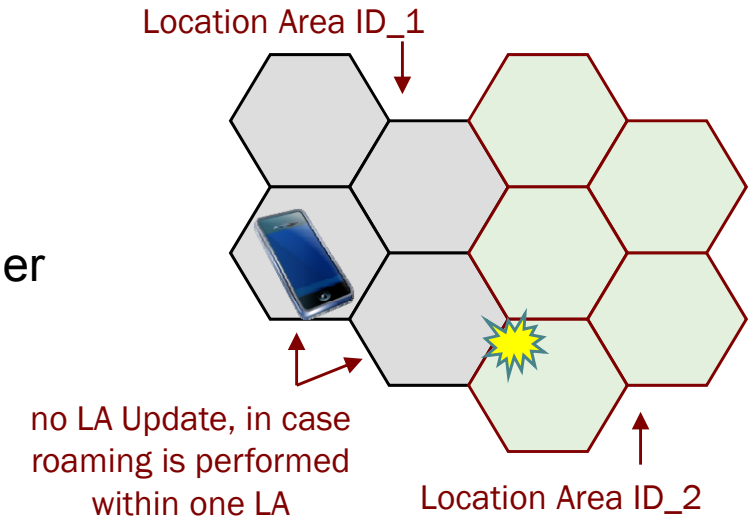
Location Area (LA) / Routing Area (RA)

- Area of connected cells
- BSS broadcasts LA ID periodically
- Moving out of LA: Location Area Update
- LTE: Tracking Area

→ LA always known

Paging

- To find Mobile Station (MS) in LA: every cell performs paging, MS answers to the cell



EVOLUTION OF CELLULAR NETWORKS

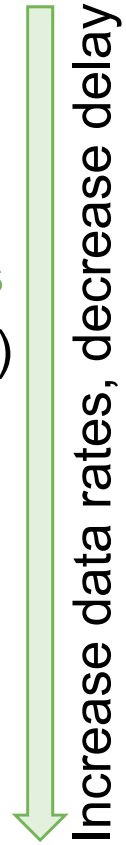
Today: Standardization and development by **3GPP (3rd Generation Partnership Project),** http://www.3gpp.org/

3G, UMTS (Universal Mobile Telecommunication System) – started 2001

- Major aim: to support video-telephony; services and applications became attractive: finance, e-books, location-based services, etc.
- UMTS – HSDPA (High Speed Downlink Packet Access): up to **7-14 Mbit/s**
- Limitations: too many nodes, spectral in-efficiency, QoS (quality of service) not sufficient for MM services

4G-LTE (Long Term Evolution) and 4G-advanced – started 2009/2012

- Freeze: release 8 (in 2008) to start with development of first products, more releases followed
- Technological enhancements: MIMO, better modulation (to transmit more symbols at a time), smaller cells, IPv6 support
- Support for high mobility (up to 500 km/h)



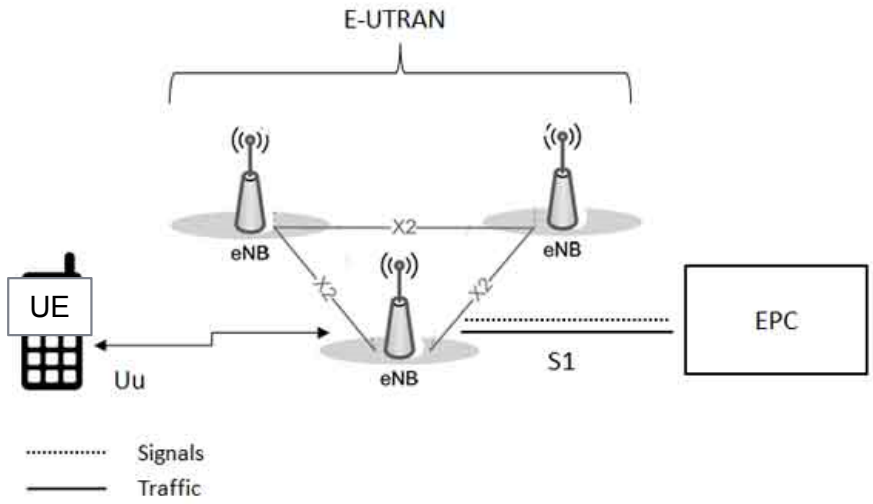
E-UTRAN … evolved UMTS radio access network
EPC … evolved packet core

LTE: EVOLVED UMTS RADIO ACCESS NETWORK (E-UTRAN)

- Handles radio communication
- **Evolved node B** (evolved base station): eNB (or eNodeB)
  - Provides connectivity to user equipment
  - Dynamic resource allocation (scheduling)
  - Implements the LTE air interface
- Home eNodeB
  - **Femtocell coverage** in the home
  - Closed subscriber group

Verizon

AT&T



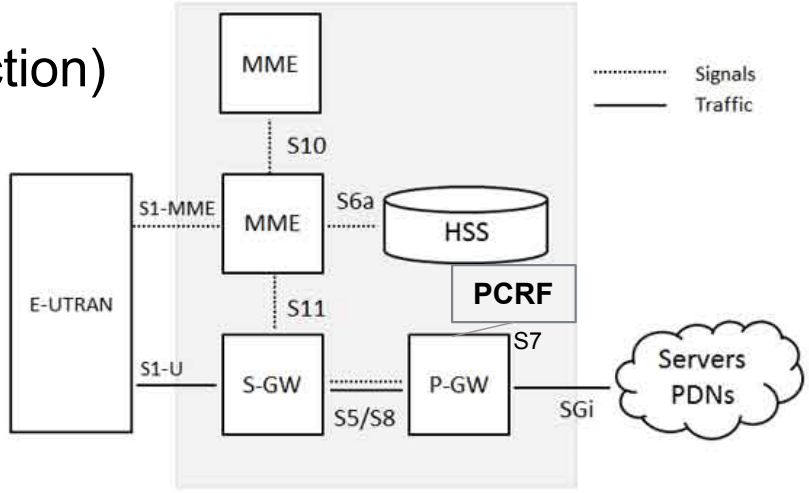
www.tutorialspoint.com/lte/lte_network_architecture.htm

karin_anna.hummel@jku.at

LTE: EVOLVED PACKET CORE (EPC)

- HSS (home subscriber server)
  - Central database of subscribers
- MME (mobility management entity)
  - Signalling for mobility handling
  - Uses HSS
- PCRF (policy control and charging rules function)
  - Charging control
- S-GW (serving gateway)
  - Router functions, mobility anchoring
- P-GW (packet data network gateway)
  - UE IP address allocation
  - Packet filtering

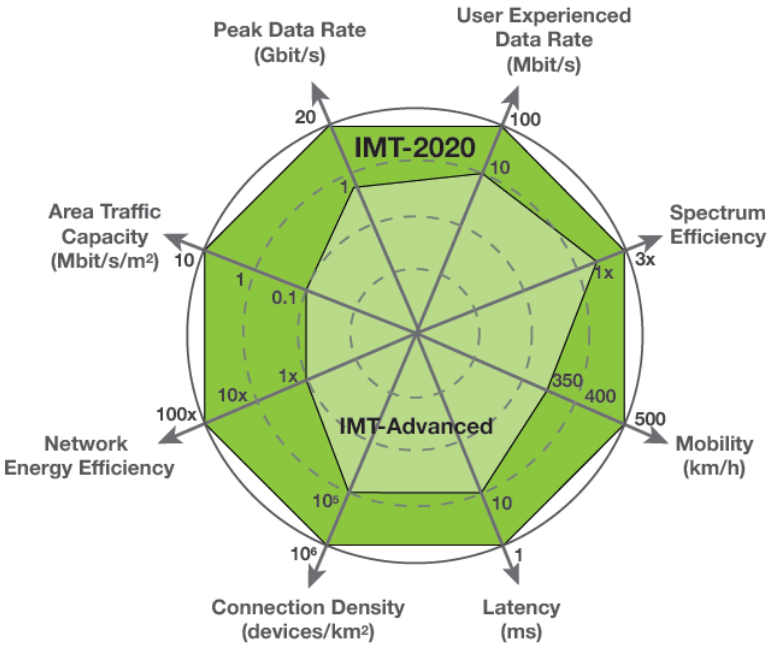
PDN … Packet Data Network



www.tutorialspoint.com/lte/lte_network_architecture.htm

karin_anna.hummel@jku.at

IMT-2020 – 5G



Samsung 5G requirements

To be expected in 2020

Problem: limited available radio spectrum

Important improvements:

- "Higher rates" "More devices" "Smaller latencies" "Higher spectral efficiency" "Lower battery consumption"

Requirements

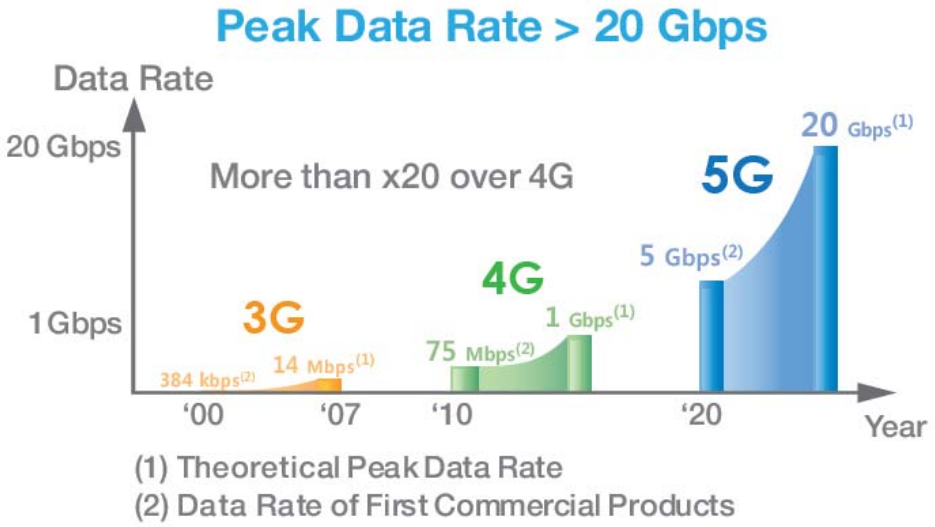
- Low deployment costs
- **Faster** (**latency < 5 ms**) and **wider coverage** (100 devices/m^2)

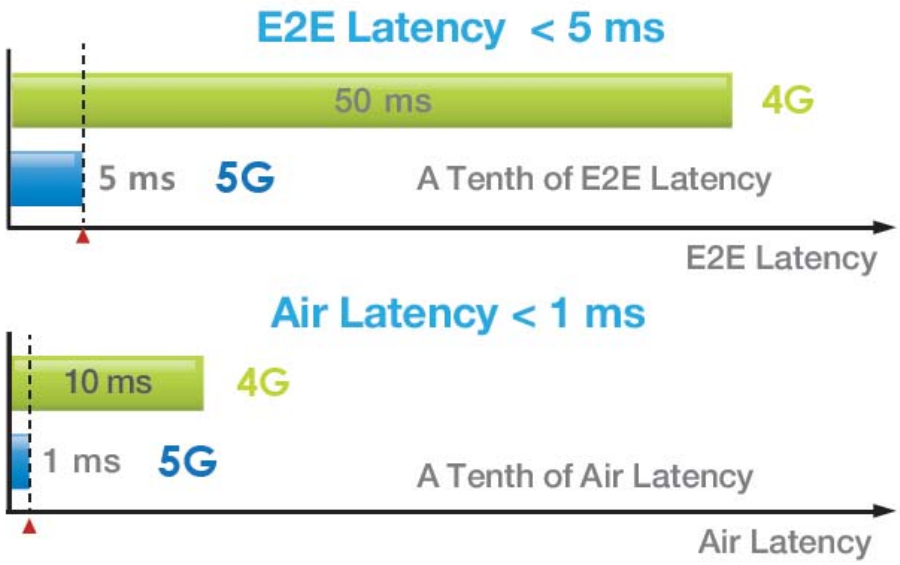
Technology changes

- Small cells, densely grouped
- Mm wave transmission (mmWave) in 20-60 GHz ranges

PERFORMANCE COMPARISON

Samsung summary on 3G/4G/5G





https://developer.samsung.com/tech-insights/5G/5g-requirements

karin_anna.hummel@jku.at

WIRELESS LOCAL AREA NETWORKING

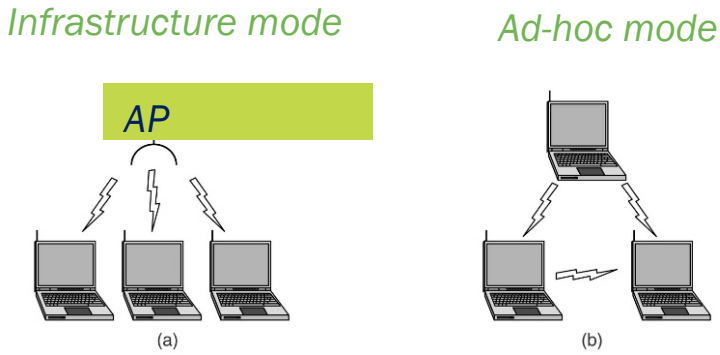
WLAN – STANDARD IEEE 802.11

Technology trademark: Wi-Fi (Wireless Fidelity)

Infrastructure mode:

- Dedicated coordination point: Access Point (AP) – clock synchronization, MAC (Medium Access Control), power management
- Used to connect stations to the Internet

Ad-hoc mode: direct communication of equal stations



WLAN Architectures - [Tan10]

karin_anna.hummel@jku.at


And lands automatically

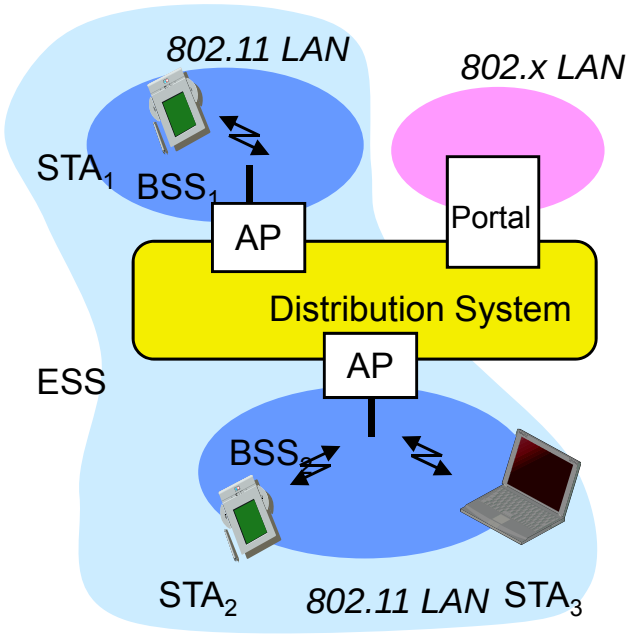
802.11 ARCHITECTURE INFRASTRUCTURE MODE

Station (STA), **Access Point** (AP)

Basic Service Set (BSS)
- Connection between multiple nodes
- Infrastructure: One node can act as AP

Distribution System (DS)
- Connection of APs

Extended Service Set (ESS)
- Connection of multiple BSSs via DS
- Roaming between APs is assured



IEEE 802.11 Infrastructure mode

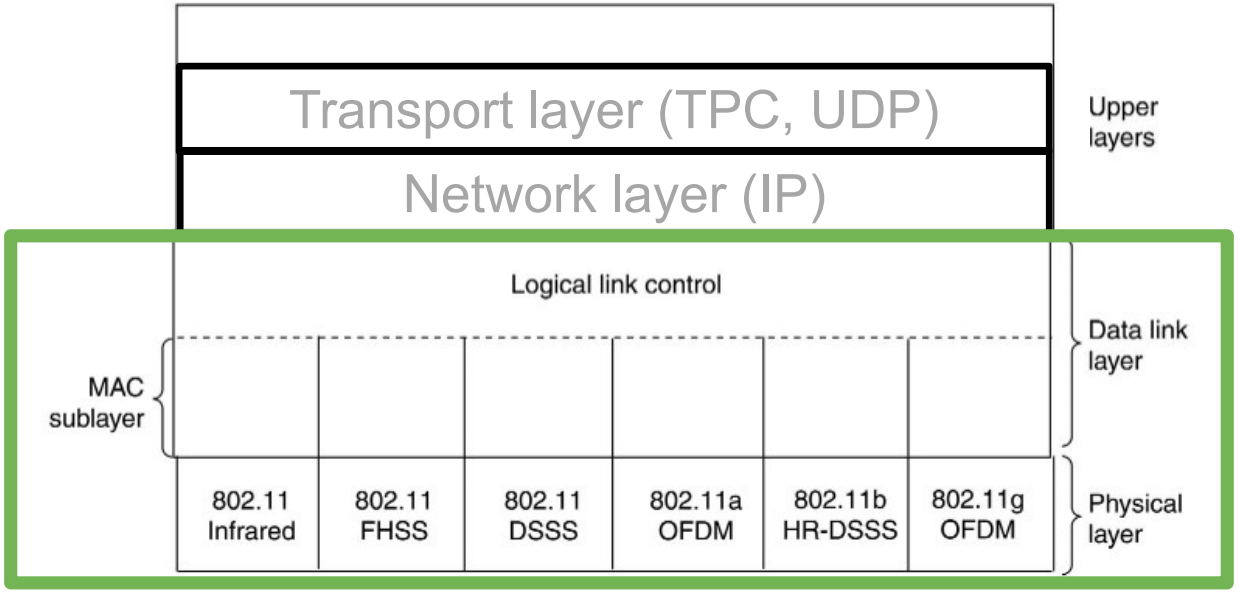
Portal: connection between DS and others

SSID: Service Set Identifier
Name of WLAN

If just BSS in ad-hoc mode → IBSS (Independent BSS)

karin_anna.hummel@jku.at

802.11 PROTOCOL STACK



802.11 specifies:

- Logical link control
- Medium access
- Use of spectrum
- Radio protocol

FHSS: Frequency Hopping Spread Spectrum
DSSS: Distributed Sequence Spread Spectrum
HR-DSSS: High Rate – DSSS
OFDM: Orthogonal Frequency Division Multiplexing
… (extended by 801.11n/ac/ad amendments)

802.11 STANDARD (802.11-2012) – OVERVIEW OF AMENDMENTS

802.11	WLAN 1-2 Mbit/s, 2.4 GHz Band
802.11a	WLAN 54 Mbit/s, 5 GHz Band
802.11b	Extension of 802.11 – 11 Mbit/s, 2.4 GHz Band
802.11d	Adaptation to national regulations
802.11e	Quality of Service (QoS)
802.11f	Inter-communication between APs
802.11g	Higher DTR (54 Mbit/s), 2.4 GHz Band
802.11h	Higher DTR, 5 GHz Band
802.11i	Improved security and authentication mechanisms (four-way handshake with cryptographic keys)
802.11n	MAC und PHY enhancements for DTR 108-600 Mbit/s
802.11p	Standard for car-to-car communication (closely related to 802.11a)
802.11ac	80/160 MHz channels DTR up to ~ 1 Gbit/s (netto 700 Mbit/s, 2014)
802.11ad	triple band (plus 60 GHz band), DTR up to 7 Gbit/s (published 2012)

802.11 PERFORMANCE-FOCUSED AMENDMENTS

Standard	Frequency band	Bandwidth	Modulation, spectrum use	Max. data rate	
802.11	2.4 GHz	20 MHz	DSSS, FHSS	2 Mbit/s	
802.11b	2.4 GHz	20 MHz	DSSS	11 Mbit/s	
802.11a	5 GHz	20 MHz	OFDM	54 Mbit/s	
802.11g	2.4 GHz	20 MHz	DSSS, OFDM	54 Mbit/s	
802.11n	2.4, 5 GHz	20, 40 MHz	OFDM	600 Mbit/s	MIMO
802.11ac	5 GHz	20, 40, 80, 160 MHz	(many, e.g. 256-QAM)	0.5-6.77 Gbit/s	MIMO
802.11ad	60 GHz	2.16 GHz	SC, OFDM	6.76 Gbit/s	MIMO WiGiG

DSSS (Direct Sequence Spread Spectrum), FHSS (Frequency Hopping Spread Spectrum), OFDM (Orthogonal Frequency-Division Multiplexing), SC (Single Carrier), QAM (Quadrature Amplitude Modulation)

How can multiple stations access the medium ?

karin_anna.hummel@jku.at

CSMA/CA

CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance)

Contention-based **Medium Access Control**

Carrier sense

- If the channel is idle → sender sends whole frame
- If the channel is busy → sender waits for waiting time W and does not transmit

Collision avoidance by **smart waiting** – aim is to achieve a low probability of collisions

CSMA/CA – SMART WAITING

- **Waiting time *W***

$$W = IFS + CW$$

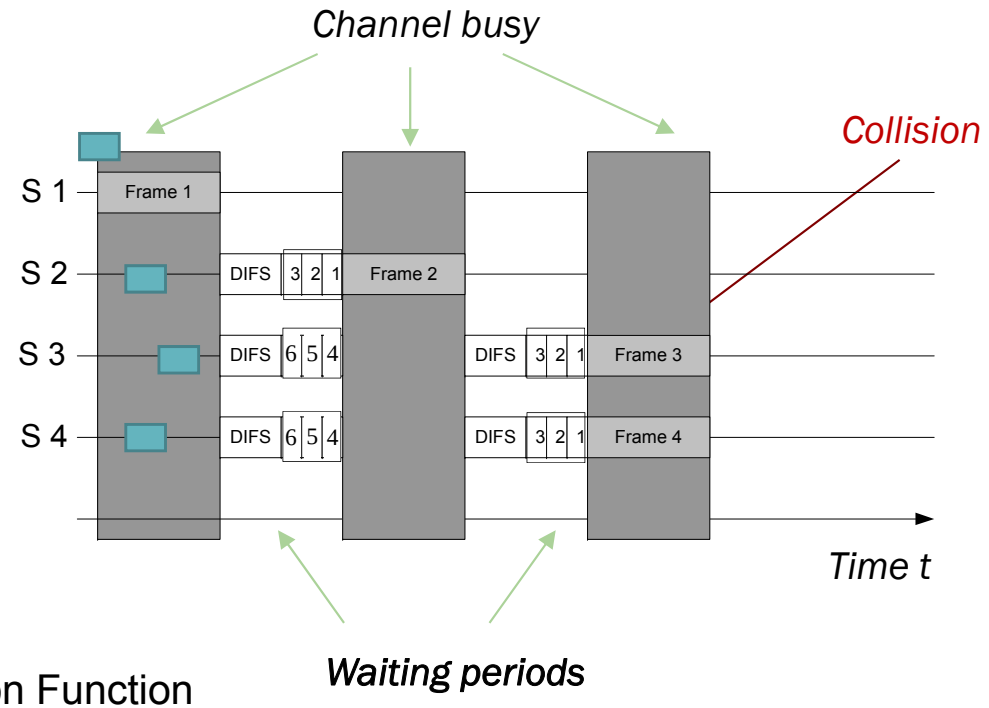
is calculated, where IFS is the **inter frame space** (“time between to frames on the medium”) and CW is a **random contention window**

- After IFS elapsed, decrement the initial contention window CW continuously (as long as the medium is free)
- If contention window is zero AND the medium is free, the station sends
- If medium becomes busy while waiting: freeze value of contention window CW to CW'; once channel is free again calculate new waiting time as

$$W = IFS + CW'$$

Why CW' ?

802.11 CSMA/CA - EXAMPLE



DIFS =
Distributed Coordination Function
Inter Frame Space
(e.g., DIFS=34 µs for OFDM)

after [Roth05] Abb. 4-7.

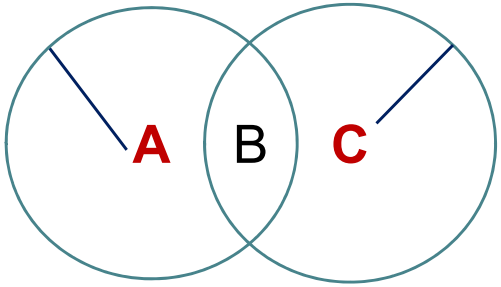
3 2 1 ... *Contention window*

karin_anna.hummel@jku.at

802.11 – STRUCTURAL PROBLEMS

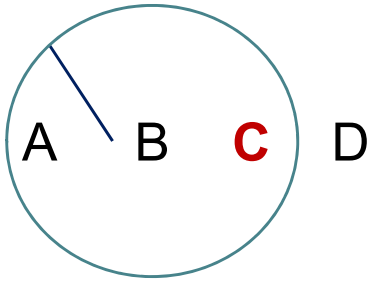
Hidden Terminal Problem

- A does not know that C is transmitting (and vice versa)
- Collision of transmissions at B



Exposed Terminal Problem

- C wants to send to D
- C detects that channel is busy and gives up although not necessary



karin_anna.hummel@jku.at

802.11 MAC (MEDIUM ACCESS CONTROL) IN DETAIL

DFWMAC (Distributed Foundation Wireless MAC)

DFWMAC-**DCF (Distributed Coordination Function)**

- Basic, mandatory, contention-based access
- **CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance**) – **listen** to the medium and **back-off** in case medium is busy

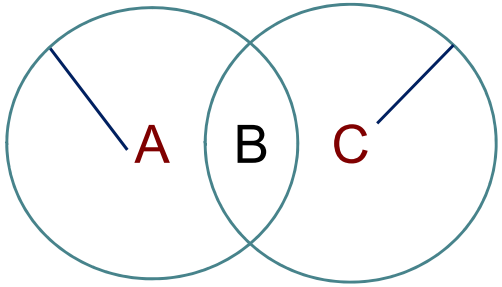
DFWMAC-**DCF with RTS/CTS (Request to Send / Clear to Send)**

- Optional, CSMA/CA with additional control messages before sending data
- Information about channel occupancy added in RTS/CTS messages (network allocation vector) → virtual channel sensing possible

DFWMAC-**PCF (Point Coordination Function)**

- Optional, non-contention access (polling based)

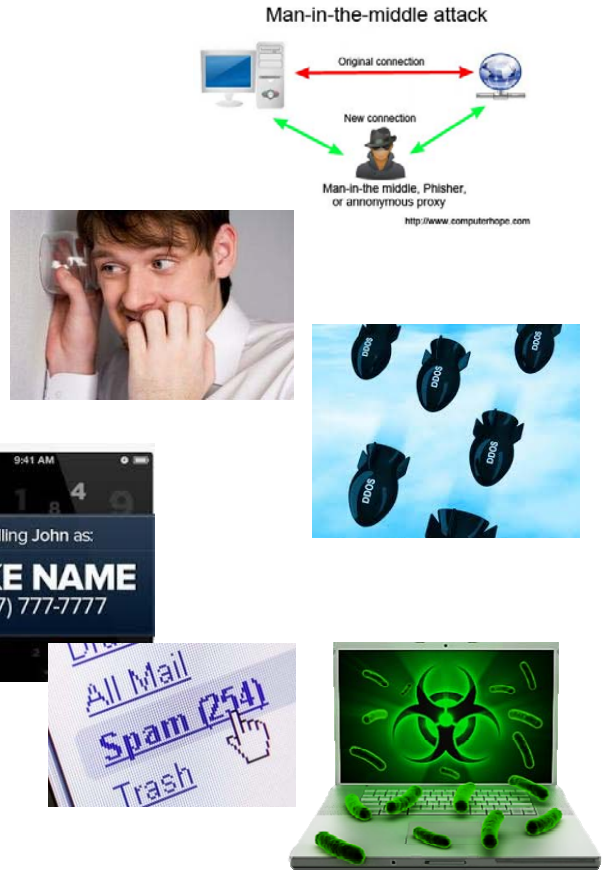
How can the Hidden Terminal Problem be solved with RTS/CTS?



karin_anna.hummel@jku.at

SECURITY THREATS

- Man in the middle attack (e.g., IMSI catcher, phishing)
- Eavesdropping / altering messages / deleting message
- Distributed denial of service attacks (DDoS)
- Identity theft (e.g., MAC spoofing, password cracking)
- Email spam
- Computer viruses, worms
- Using resources not authorized to use

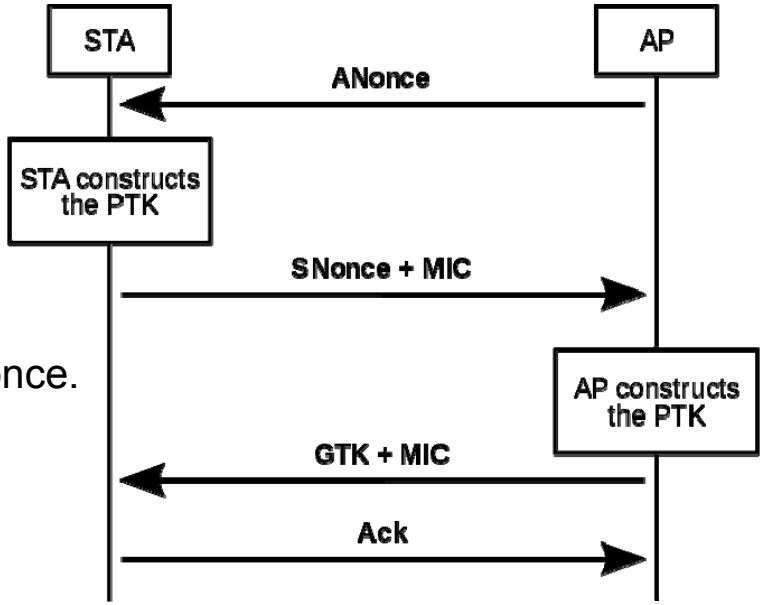


karin_anna.hummel@jku.at

802.11 SECURITY

PTK … Pairwise Transient Key
From Pairwise Master Key, ANonce.

GTK … Group Temporal Key
From SNonce
MIC … Message Integrity Code



- Access restrictions using lists: a list of all allowed MAC-addresses
- Disable SSID broadcasting
- **Passphrase and encryption** (WEP, WPA, WPA2)
  - **WPA2:** Cipher block Chaining Message authentication code Protocol (CCMP) based on **Advanced Encryption Standard (AES): block cipher requiring 128-bit key**, fresh temporal key, and nonce; **4-way handshake** between STA and AP; **IEEE 802.11i**
  - Additionally: Extensible Authentication Protocol (EAP, RFC 3748) – framework for authentication
- Connect to VPN

WPA2 … Wi-Fi Protected Access II

WIRELESS PERSONAL AREA NETWORKING

BLUETOOTH – TYPICAL USE CASES

Range: 10s – 100s m (approx.), depending on device class & version

Connecting personal devices

- Headset to phone
- Car entertainment system to phone
- Mouse/keyboard wirelessly to PC
- Medical device to PC/smartphone
- Internet of Things (IoT)

BLUETOOTH – IEEE 802.15.1

(Major technological improvements)

1994: Design of wireless PAN by Ericsson (name after: Danish King Harald Blåtand)

1998: Bluetooth Special Interest Group (SIG) – Ericsson, Nokia, IBM, Intel, Toshiba

2010: Bluetooth 4.0: Classic BT, **BT HS (high speed)**, **BLE (Bluetooth Low Energy),** 1 Mbit/s BLE

2016: Bluetooth 5: Improvements in range (40-400m), connectionless services, Internet of Things (IoT), 2 Mbit/s BLE

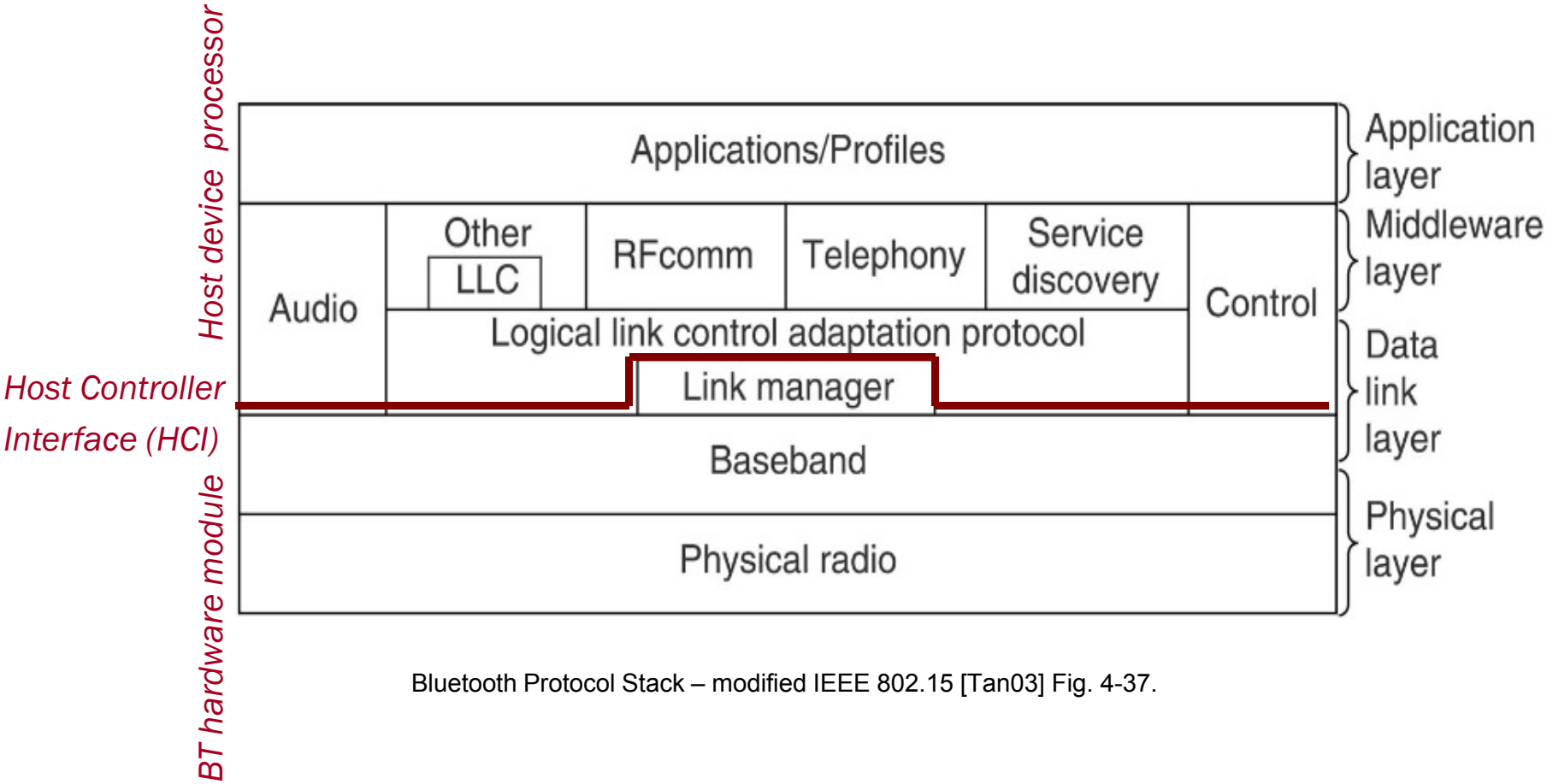
BT Version	Data rate	Frequency	
1.2	1 Mbit/s	2.4 GHz	
2.0 + EDR	3 Mbit/s	2.4 GHz	
3.0 + HS	24 Mbit/s	2.4 GHz	BT and co-used WLAN channel
4.0/4.1	24 Mbit/s	2.4 GHz	

CLASSIC BLUETOOTH VS. BLUETOOTH LE

	Classic BT (speakers, head-set)	**BLE** (wrist watch, health monitors, smart home devices)
Range	10-100 m	50m, >100m
Throughput	1-3 Mbit/s	1 Mbit/s
Latency	~ 100 ms	6 ms
Voice support	Yes	No
Peak current	< 30 mA	< 15 mA

- **Chipsets** available from: Qualcomm-Atheros, CSR, Broadcom, TI
- **Operating systems** such as Android, iOS support both Bluetooth variants

CLASSIC BLUETOOTH – PROTOCOL STACK



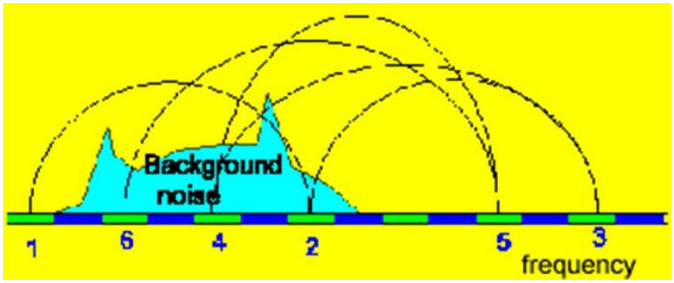
Bluetooth Protocol Stack – modified IEEE 802.15 [Tan03] Fig. 4-37.

karin_anna.hummel@jku.at

CLASSIC BLUETOOTH – RADIO

Radio layer

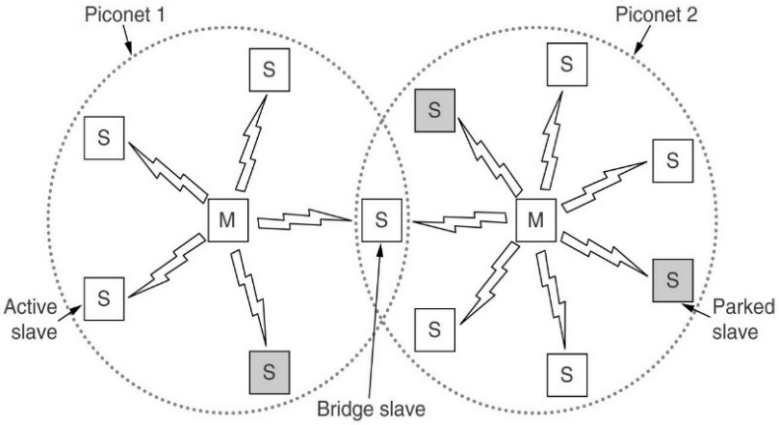
- 2.4 GHz ISM band (free, open, noisy)
- 79 channels (1 MHz)
- Low power (few mWatt, only class 1 up to 100s of mWatt)
- **Frequency Hopping Spread Spectrum** (FHSS) – fast hopping
  - 1600 hops / s (compared to WLAN-implementations 2.5 hops / s)



Baseband

- Provides in-order delivery of byte streams
- Handles frequency of hop sequence (FHSS)
- Medium access control: central Time Division Duplexing (TDD): polling by master
- Finding devices (inquiry) and setting up connections (paging)

BUILDING A BT NETWORK



Master and up to 7 active slave devices (3 bit addresses) in a piconet (additional parked slaves possible; bridging to other piconets possible to form a scatternet)

Inquiry (about finding devices)

- Station starts to inquire BT devices on different channels (frequencies); other stations listen periodically for inquiries (in “inquiry scan” state)
- If an inquiry is received, the station sends its Frequency Hopping Sequence information in a packet (i.e., clock and device ID)
- After about 10 seconds, the device should know all devices in proximity

Paging (about inviting to connect to a piconet)

- **Master** (**M**) sends a page packet to a device it knows about, **slave (S)** responds
- Master sends the Frequency Hopping Sequence information to the slave, slave responds
- Master assigns active member address to the slave and polls slave on the frequency hopping pattern of the piconet, the slave responds

CLASSIC BLUETOOTH – LINK MANAGEMENT

Link Manager

- Connection/link management: creation, management, termination of synchronous connection-oriented (SCO) and asynchronous connection-less (ACL) links (SCO: real-time voice or video; ACL: data)
- Security: no / service level-based / link level-based security; link level-based (**pairing**): use of a link key for authentication and encryption
- Clock synchronization

Logical Link Control Adaptation Protocol (L2CAP)

- Multiple logical channels to baseband layer (multiplexing)
- Segmentation/reassembly of data frames (from at max. 64kbyte to 2745 bit frames)
- Flow control
- Quality of service (QoS): none, best effort, guarantee (peak bandwidth, delay, jitter, etc.)

CLASSIC BLUETOOTH – MIDDLEWARE

Service Discovery Protocol

- Search for services of other Bluetooth devices (SDP client)
- SDP server: offer services described in an SDP database
- **Bluetooth profiles** determine the functionality

RFCOMM

- Emulates serial interface (used for connecting periphery like mouse/keyboard)

LLC (Logical Link Control)

- Introduced by IEEE for compatibility reasons

Telephony Control Protocol Specification Binary – TCS BIN

- Call control functions for telephony (Ex.: Answering the phone, hang up)

Audio / Control

- Direct access of arbitrary applications without L2CAP

BLUETOOTH – PROFILES

Profile – set of data structures, protocols to assure compatibility

Basic profiles

- GAP – Generic Access Profile: discover and establish connection; root profile
- **GATT – Generic Attribute Profile: profile discovery and description for BLE**
- GOEP – Generic Object Exchange Profile: transmission of objects (file transfer, synchronization)

and many more

Other profiles (on top of basic profiles)

- File transfer profile, headset profile, synchronization profile, and many more

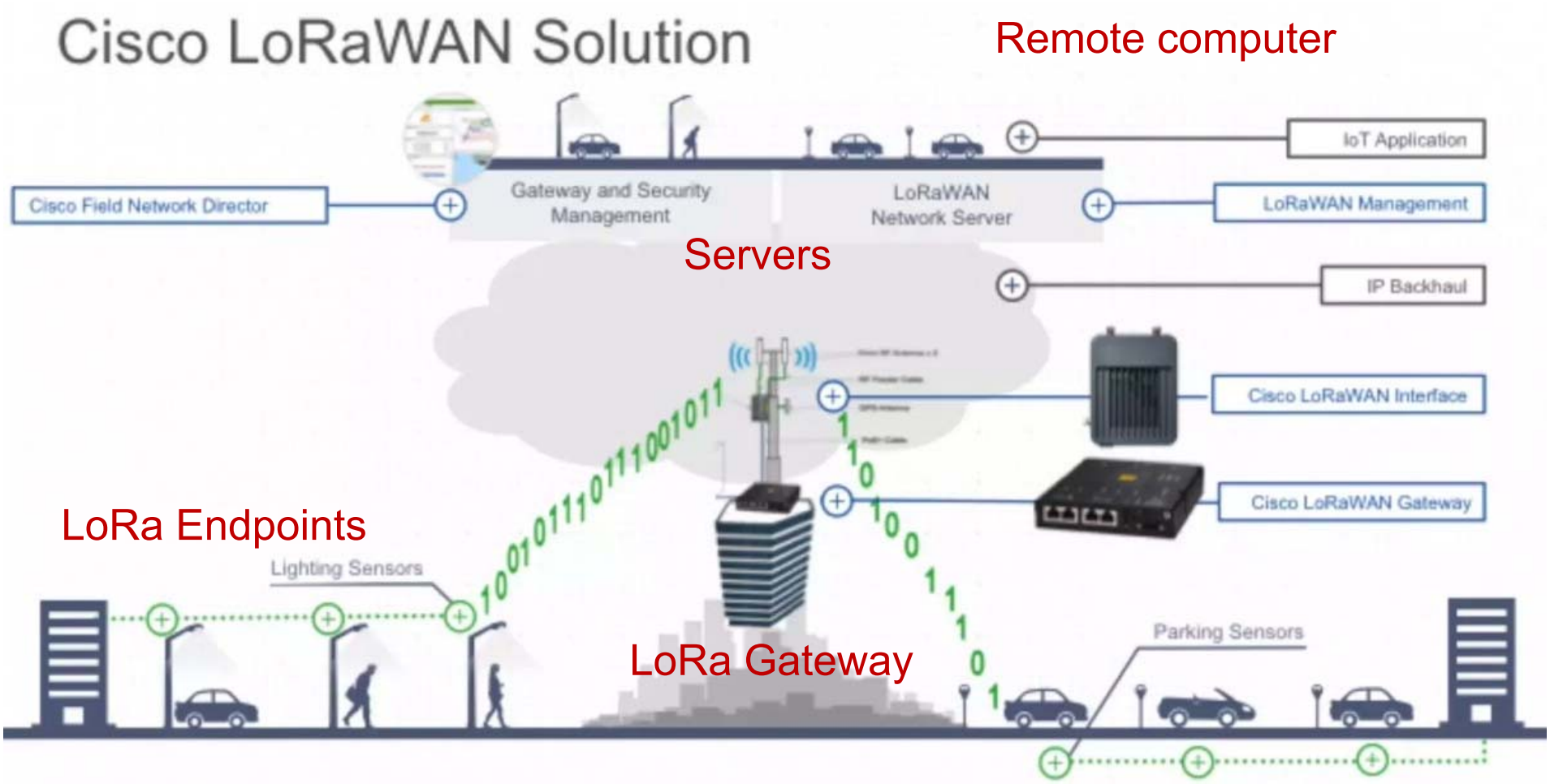
Example: Blood Pressure Sensor Features (BLE) – Blood Pressure Profile

https://www.bluetooth.com/specifications/gatt/viewer?attributeXmlFile=org.bluetooth.characteristic.blood_pressure_feature.xml&u=org.bluetooth.characteristic.blood_pressure_feature.xml

– Wireless networking in the Internet of Things (IoT)

LORA / LORAWAN – MOTIVATION

https://www.youtube.com/watch?v=m6IvwcjcxQc



karin_anna.hummel@jku.at

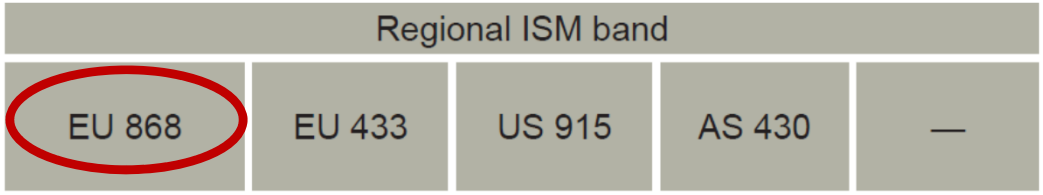
LORAWAN TECHNOLOGY

A Low Power Wide Area Network

LoRa (owner Semtech): Long range (while operating with low power)

- Lora Alliance
- Achieved by tweaking the “link budget” (potential of the link)
  - Chirp spread spectrum module (used in space and military communications)
  - 25mW, up to 50 kbit/s (Europe) – less due to channel occupancy limitations per device
- Gateway can over entire cities (100s km^2)

868 MHz



https://www.youtube.com/watch?v=hMOwbNUpDQA
https://lora-alliance.org/sites/default/files/2018-04/what-is-lorawan.pdf

Geometric operations …

POSITIONING SYSTEMS

Galileo

WLAN (fingerprinting)

Cellular network based positioning

Ultrasound

Glonass

GPS (Global Positioning System)

karin_anna.hummel@jku.at

WHY POSITIONING? – LOCATION-BASED SERVICES

Navigation
- Outdoor navigation (vehicle navigation, trekking)
- Indoor navigation (room finder)
- Traffic management (floating car data)

Information
- Tourist guide
- Restaurant finder (FourSquare)

Tracking
- Vehicle (fleet management)
- Product delivery/tracking
- Tracking for billing (toll)

Gaming
- Geocaching, Ingres, Pokemon-Go

Emergency

KEY SUCCESS FACTORS

Early location-based applications were not accepted by users (around 1990)

Second chance → 2005 revival due to

- Availability of accurate GPS
- Availability of higher data rates with 3G
- Smartphones
- Web 2.0 (user-generated content)

POSITIONING TECHNOLOGIES

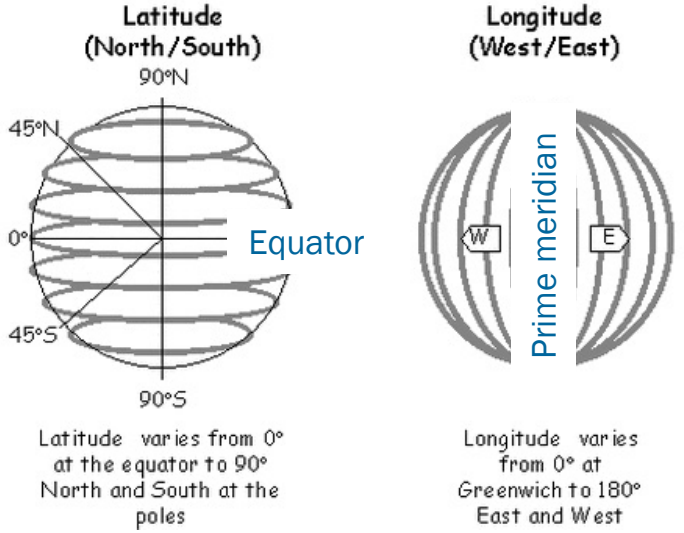
Purpose

- Locating a user/device/object (on earth)
- Indoors and outdoors

EARTH MODEL

Ideal sphere

- Meridian, line of longitude (“Längenkreis”)
  - Circle length $= 2R\pi$, $R \sim 6370$ km
- Circle of latitude (“Breitenkreis”)
  - Changing radius r (length $= 2r\pi$)



Earth-ellipsoid

- World Geodetic System 84 (WGS84) standard
  - Parameters a ~ 6378.14 km, b ~ 6356.75 km

Ex.: N 48°12’ 29.99” E 16°22’ 22.01”

karin_anna.hummel@jku.at

Assume we have

- *Some nodes at known positions*
- *Wireless technologies to send signals between nodes*

How can we leverage wireless technologies to determine distances ?

CALCULATING DISTANCE
WITH FREE SPACE PATH LOSS FORMULA

Loss in signal strength of an electromagnetic wave used to determine distance under LOS (line of sight) conditions

$$L = (\frac{4df\pi}{c})^2$$

L … free space path loss
d … distance [m]
f … frequency [Hz]
c … speed of light (speed of radio signal) $\sim 3\ x\ 10^8$ [m/s]

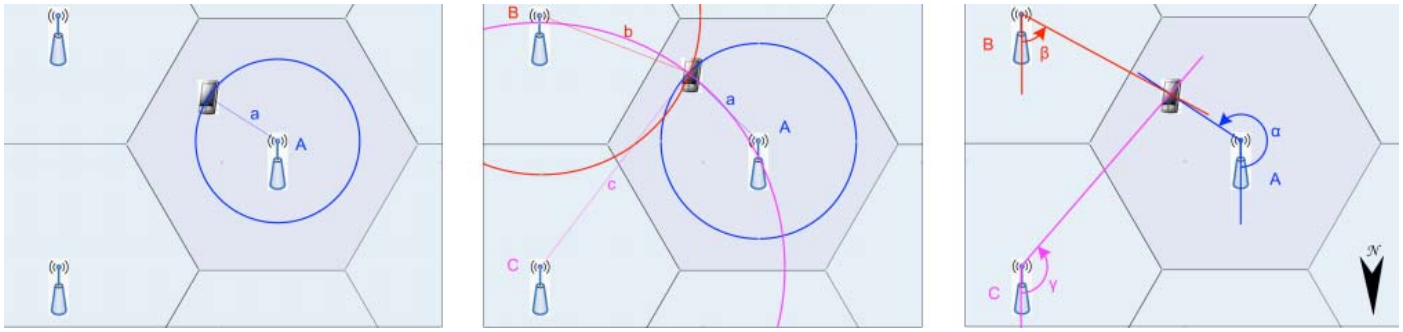
But: not practical due to disturbances and obstacles

karin_anna.hummel@jku.at

CALCULATING DISTANCE
BY GEOMETRY-BASED POSITIONING METHODS

Rely on **signal properties** and **geometry**

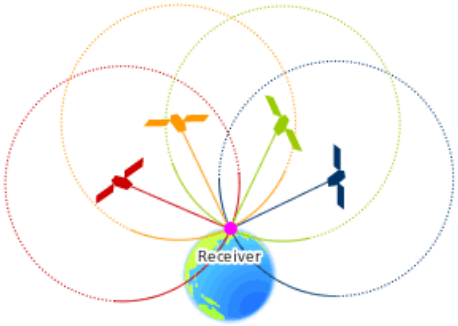
CoO **ToA** **AoA**



- **Cell of Origin (CoO) …** can be also a sector of a cell in the network
- **Time of Arrival (ToA), Time of Flight (ToF), Time Difference of Arrival (TDoA)**
  Use propagation time of signal to estimate distance of one device from different antennas
- **Angle of Arrival (AoA)**
  Use angle of received signal to device from different antennas

karin_anna.hummel@jku.at

SATELLITE-BASED POSITIONING OF A DEVICE: PRINCIPLE

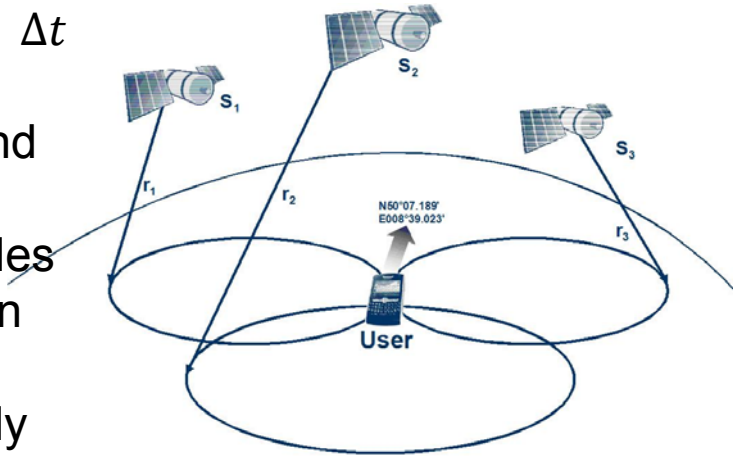


Known

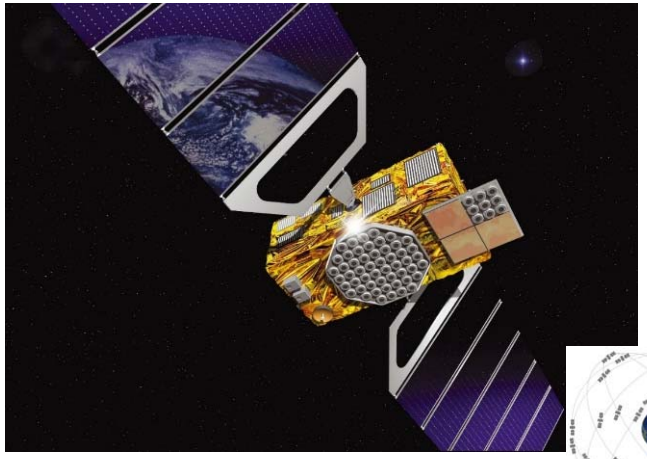
- Position of satellites (S_i) due to known orbits of satellites
- Signal runtime is measured as Δt

Use **ToA (Time of Arrival)** method

- Calculate **distances of satellites to device**: $r_{\mathrm{i}} = c \times \Delta t$
- Determine position of device in 3D by
  - Use distances r_{i} to construct three spheres around satellites S_1,S_2, S_3, spheres K_1,K_2, K_3
  - Cut each K_1,K_2, K_3 with earth sphere → three circles
  - Cut circles with one another → get device position



But: time is not accurate at the receiver (clock not perfectly synchronized) → **more satellites needed in practice!**



GLOBAL NAVIGATION SPACE SYSTEMS

Satellite-based Positioning

- **GPS** http://www.gps.gov/
- **GLONASS** (**ГЛОНАСС** - Глобальная навигационная спутниковая система) operational since 1996, 23 satellites available [24.11.2015] http://www.glonass-ianc.rsa.ru/en/
- **GALILEO** (scheduled for 2019?) http://www.esa.int/

COMPASS (People's Republic of China), IRNSS (India)

…

karin_anna.hummel@jku.at

GLOBAL POSITIONING SYSTEM (GPS)

US Project (DoD – Department of Defense, DoTransportation, NASA)

1970 NAVSTAR GPS (Navigation System Timing and Ranging – GPS)
1995 fully operational

Main facts

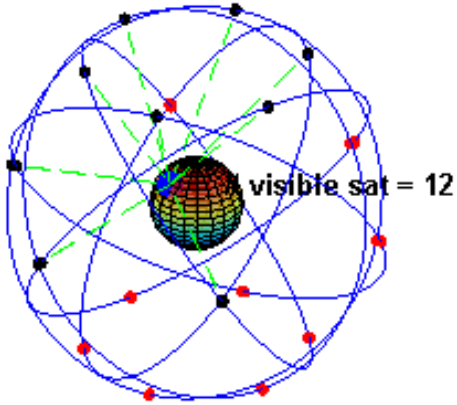
24 satellites (with additional spare ones)
6 orbits (Medium Earth Orbit (MEO)) consisting of 4 satellites each
Altitude: about 20'180 km
Full earth orbit: 12 hours
Threats: valleys, narrow streets, buildings, indoors

Satellite

Availability: ~7.5 years, Weight: 1.5 - 2 tons
Autonomous energy supply via solar panels
CPU:16 MHz; operating system consists of approx. 25'000 lines of code in Ada

GPS current constellation: U.S. Naval Observatory Web site
http://tycho.usno.navy.mil/gpscurr.html

GPS SYSTEM ARCHITECTURE



User segment

GPS receiver

Manufacturers: Garmin, Magellan, TomTom, etc.

Receives signal and estimates travel time

Space segment

Satellites

Control segment

Monitoring stations: at known positions; receive signals (system time, position, orbit data), calculate correction data and send it to *master control station*

Master control station (@ Colorado Springs, USA): calculates correction data for satellites; uses uplink to all satellites (special frequency band “S-band”) to transfer clock corrections and to setup new satellites

GPS ACCURACY

Dependent on pulse of signal → higher, more accurate
Clock errors, deviations of the orbit, disturbances: satellite position (gravitation influence of moon/sun), disturbances in the atmosphere (weather, air pressure), disturbances in the **ionosphere** (electrically loaded particles) and troposphere, **multipath** fading (reflection in the surrounding of the receiver), **satellite clock**

Vertical: ≤ 4.684 m (95%)
Horizontal: ≤ 3.351 m (95%)

According to:
GPS performance analysis (FAA report):
http://www.nstb.tc.faa.gov/reports/PAN86_0714.pdf#page=22

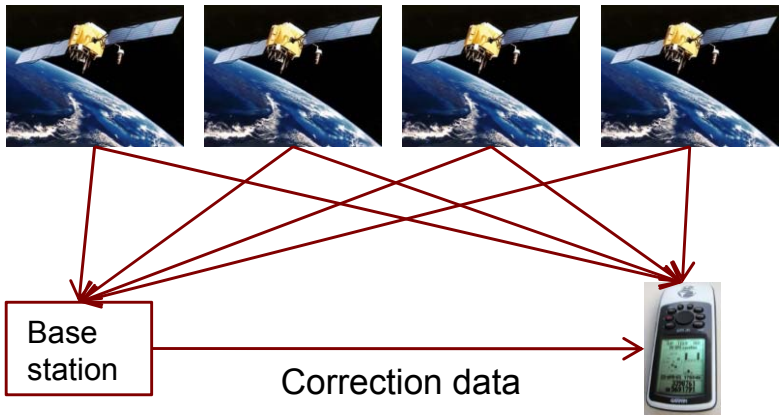
DIFFERENTIAL GPS (DGPS) - PRINCIPLE

DGPS Equipment

… improving accuracy with a little help from the ground

Adding terrestrial stations to the system

Base station (BS): **known position → distance to satellite known**; calculates correction data; transmits to receivers in proximity (unidirectional transmission)
Assumption: BS and user device experience same error → sub-meter accuracy (10s of cm)



karin_anna.hummel@jku.at

OTHER OPTIONS: CELLULAR NETWORK-BASED POSITIONING

Utilizing existing infrastructure and apply “Cell ID”, ToA, AoA

GSM/3G/LTE

1) Cell ID (Cell of Origin), signal strength; problem: size of a cell varies <1 km (cities) – 35 km (country side)
2) Sectoral cells → sectors
3) ToA, TDoA, AoA

(range of 10s to 100s of meters)

Possible to use also indoors!

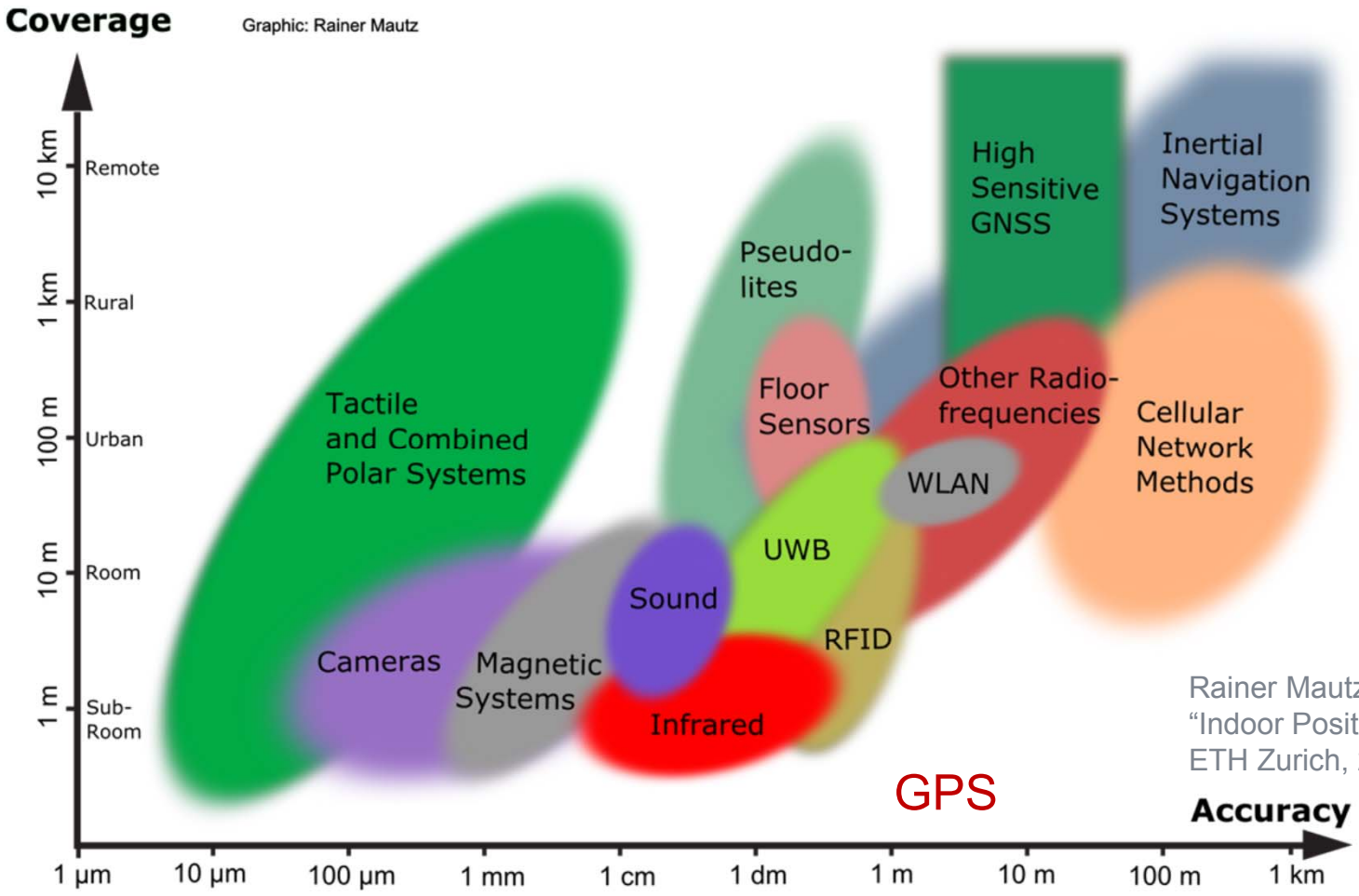
FCC E911 Requirement

2D error for a given set of measurements:

67% ‹ 50m

95% ‹150m

POSITIONING TECHNOLOGIES



Rainer Mautz, Habilitation Thesis
"Indoor Positioning Technologies"
ETH Zurich, 2012

karin_anna.hummel@jku.at

ADD-ON SLIDES

CALCULATION OF MAX. DTR

Harry Nyquist (1924)

Each channel has a limited transmission capacity, limited Data Transfer Rate (DTR)

$$DTR_{max} = 2 \times H \ \log_2 V \ [\text{bit/s}]$$

V … number of discrete levels; H … bandwidth

Ex.: Assume noiseless **3 kHz channel**, **binary signal** (two levels) should be transmitted

Rate of 7 kbit/s – possible?

$$DTR_{max} = 2 \times 3 \ \log_2 2 = 6 \ [\text{kbit/s}]$$

SIGNAL AND NOISE

Claude Shannon (1948)
Channel disturbed by thermodynamics (noise), molecules collide

Thus … quality of a channel described by **Signal-to-Noise Ratio (SNR)** = *S*/*N*

$$DTR_{max} = H \log_2\left(1 + \frac{S}{N}\right) \text{ [bit/s]}$$

H is the bandwidth

Ex.: $H = 3$ kHz, $S/N = 30$ dB (typical for analog telephone part);
by approximating $\log_2(1 + S/N) \sim 10$ → $DTR_{max} = 30$ [kbit/s]

DEZIBEL, DB

Describes the relation of two values of physical quantities in logarithmic scale.

$$x = 10 \times \log_{10} \frac{P}{Q} \text{ [dB]}$$

$$x = 10 \times \log_{10} \frac{P}{1\text{mW}} \text{ [dBm]}$$

P/Q	... in dB
10	10
100	20
1000	30

Examples

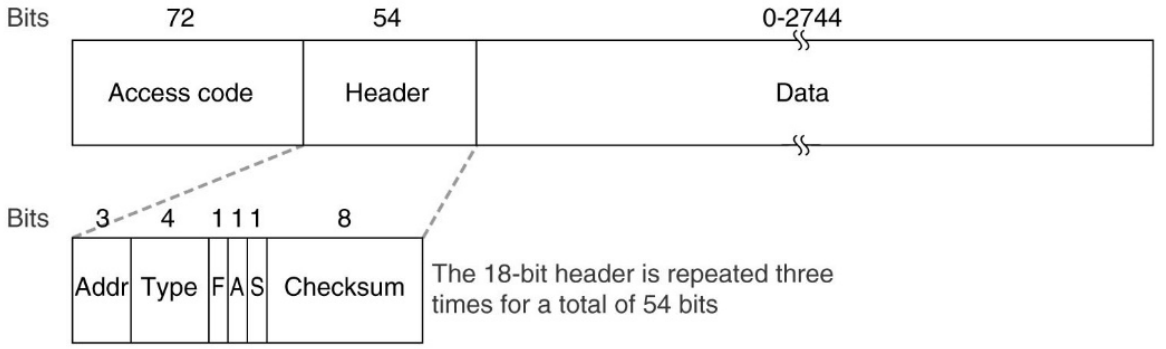
CLASSIC BLUETOOTH – FRAME STRUCTURE

Access Code: Unique bit sequence, piconet address (from master)

(Packet) **Header**

- Type, F/A/S – flags (flow control, acknowledge indication, sequence), checksum
- Every bit transmitted 3 times (FEC – Forward Error Correction)

Data, Payload: Content



[Tan03] Fig. 4-38.

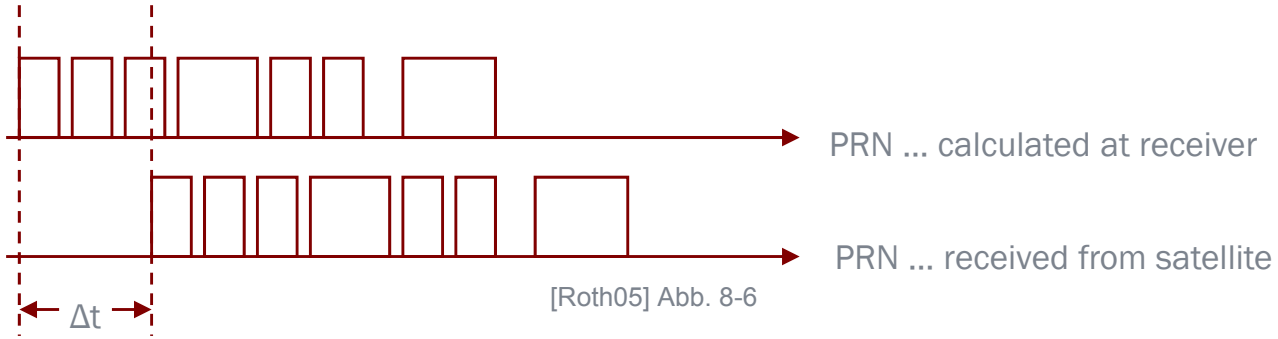
karin_anna.hummel@jku.at

GPS SIGNALS

Power: 20 W
Frequencies: L1 1.57542 GHz (civilian, military), L2 1.2276 GHz (military)

Code Division Multiple Access (CDMA) with Pseudo Random Noise (PRN)

- Receiver knows all (unique) PRNs
- Receiver adapts/shifts PRN until it matches PRN of satellite (time offset Δt), determines runtime of signal
- Data rates: 50 bit/s, Pulse: civilian – 1023 (repeated every millisecond), military – 2.35 10^{10} pulses (repeated after 38 weeks)
- Almanac: position of satellite, orbit data of other satellites



[Roth05] Abb. 8-6

DGPS CORRECTION

Deviation of BS clock to system time

Actual distance to satellite

Positioning error

Pseudo-distance to satellite i

$$p_{bi} = r_{bi} + E_{bi} + c \times \delta_{bi}$$

Base station Δp_{bi} 

BS sends correction values for each satellite to near mobile GPS receivers:

$$\Delta p_{bi} = p_{bi} - r_{bi} = E_{bi} + c \times \delta_{bi}$$

Calculation at user device:

$$p_{ui} - \Delta p_{bi} = r_{ui} + E_{ui} + c \times \delta_{ui} - E_{bi} - c \times \delta_{bi}$$

Positioning errors are almost equal

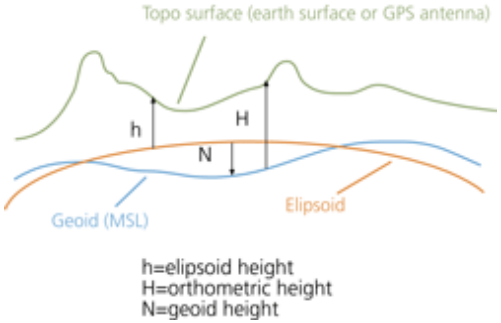
NMEA POSITIONING FORMAT

National Marine Electronics Association 0183

[after:http://www.gpsinformation.org/dale/nmea.htm#GGA]

Ex.: $GPGGA,123519,4807.038,N,01131.000,E,1,08,0.9,545.4,M,46.9,M,,*47

GGA	Global Positioning System Fix Data
123519	Fix taken at 12:35:19 UTC
4807.038,N	Latitude 48 deg 07.038' North
01131.000,E	Longitude 11 deg 31.000' E
1	Fix quality: 0 = invalid 1 = GPS fix (SPS) 2 = DGPS fix 3 = PPS fix 4 = Real Time Kinematic 5 = Float RTK 6 = estimated (dead reckoning) (2.3 feature) 7 = Manual input mode 8 = Simulation mode
08	Number of satellites being tracked
0.9	Horizontal dilution of position
545.4,M	Altitude, meters, above mean sea level, H
46.9,M	Height of geoid (mean sea level) above WGS84 ellipsoid, N
(empty field)	time in seconds since last DGPS update
(empty field)	DGPS station ID number
***47**	the checksum data, always begins with *



karin_anna.hummel@jku.at