Programmierung mobiler Kleingeräte

Drahtlose Kommunikation

Wolfgang Auer, Patrick Ritschel

Drahtlose Kommunikation

- *Idealerweise breiten sich elektromagnetische Wellen gleichmäßig in alle Richtungen aus*
- *Vereinfacht gesehen liegen die elektromagnetischen Wellenfronten auf Kugelfronten mit dem Sender im Zentrum*
  - *Die Intensität nimmt mit dem Quadrat zum Abstand ab*
    - *($A = 4*r^2 / \pi$)*
- *In der Realität ist die Abnahme durch unregelmäßiges Gelände, Reflexionen und elektromagnetische Störquellen stärker: mit der vierten Potenz*
  - *Wenn sich der Abstand verdoppelt muß die 16-fache Sendeleistung aufgebracht werden*

Drahtlose Kommunikation

- Frequenzbereiche elektromagnetischer Schwingungen werden in Bänder eingeteilt
  - Langwellen (50 kHz, 6 km Wellenlänge)
  - Mittelwellen (500 kHz, 600 m)
  - Kurzwellen (5 MHz, 60 m)
  - UKW, Ultrakurzwellen (50 MHz, 6 m)
  - SHF, Super High Frequency (5 GHz, 6cm)
  - Infrarot (400 THz, 750 nm)
    - Rot (750 – 650 nm)
    - Orange (650 – 585 nm)
    - Gelb (585 – 575 nm)
    - Grün (570 – 490 nm)
    - Blau (490 – 420 nm)
    - Violett (420 – 400 nm)
  - Ultraviolett (750 THz, 400 nm)
  - Röntgen (~1016 – ~1019, 10 nm – 5 pm)
  - Gammastrahlung (< 0,5 nm)

Drahtlose Kommunikation

- Kanäle können nicht isoliert werden
  - elektromagnetische Wellen verschiedener Transmissionen überlagern sich beim Empfänger, selbst wenn die Transmissionen nicht für einen bestimmten Empfänger vorgesehen sind
  - -> Algorithmen zur zeitlichen und/oder frequenten Trennung von Kanälen

- Die Funkressource ist weltweit nur ein Mal vorhanden
  - deshalb muss sie irgendwie auf verschiedene Kommunikationsverfahren und –partner aufgeteilt werden

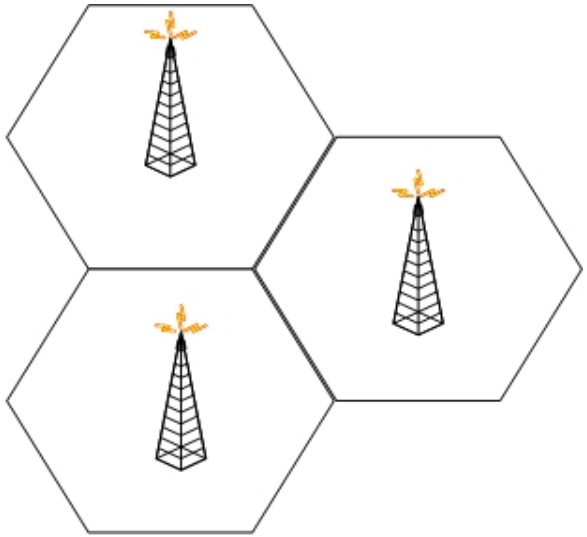
Drahtlose Kommunikation

- Duplex
  - Zwei Kommunikationspartner senden und empfangen auf eigenen „Kanälen“
  - z.B. TDD (Time Division Duplex), FDD (Frequency Division Duplex)

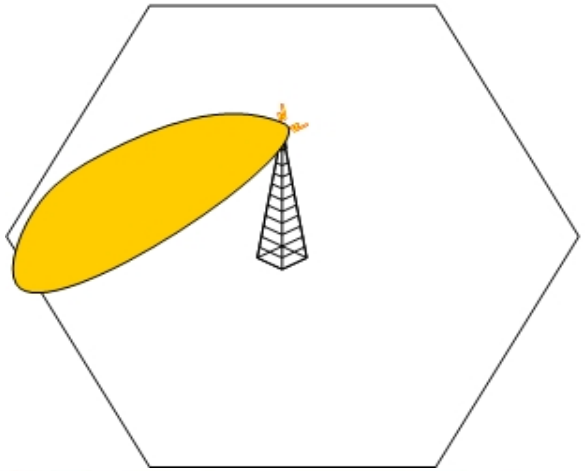
- Multiple Access
  - Das Medium wird von mehreren Sendern gleichzeitig benutzt
  - z.B. SDMA (Space Division Multiple Access), TDMA, FDMA, CDMA

Drahtlose Kommunikation

Raummultiplex



•Raum wird in mehrere Zellen aufgeteilt



•Richtungscharakteristik von Antennen kann ausgenutzt werden

Drahtlose Kommunikation
Frequenzmultiplex

- Wie im Rundfunk wird ein Frequenzband in mehrere Kanäle bestimmter Breite unterteilt
  - Dieses schmälere Band kann vom Empfänger exakt herausgefiltert werden
  - Zwischen den Kanälen braucht man einen „Sicherheitsabstand“
  - -> Es gibt nicht beliebig viele Kanäle in einem Band

- Bei Duplex (FDD) gibt es einen *Uplink*- und einen *Downlink*-Kanal

- *Frequency Hopping*

  die Frequenz eines Kanals wird oft gewechselt, damit die Störung eines Kanals keinen Ausfall der Kommunikation bewirkt

Drahtlose Kommunikation

Zeitmultiplex

- *Zeitscheibenverfahren*
  - Der Sender belegt das Medium in bestimmten Zeiträumen, *Zeitschlitze* bzw. *Slots*
  - Eine Mehrfachbelegung resultiert in einer *Kollision*
- In zentralen Verfahren teilen ausgezeichnete Sender anderen Sendern periodische *Slots* zum Senden zu
- In dezentralen Verfahren müssen die Stationen die Belegung der *Slots* miteinander aushandeln
- Bei einem TD-Duplexkanal senden *Uplink* und *Downlink* zeitversetzt

Drahtlose Kommunikation

Codemultiplex

- Codemultiplex erlaubt *gleichzeitiges* Senden auf *einer* Frequenz
  - Komplexes Verfahren; Einsatz z.B. in UMTS und GPS
  - Jeder Sender hat seinen *Spreizcode*
  - Der Empfänger kennt den Spreizcode des Senders
  - Zum Senden werden die `bin. 1` als `1`, die `bin. 0` als `-1` interpretiert
  - Anschließend werden die Daten mit dem Spreizcode multipliziert und gesendet (*Spreizen*)
  - Der Empfänger multipliziert mit dem Spreizcode des Senders, integriert und approximiert das Sendesignal

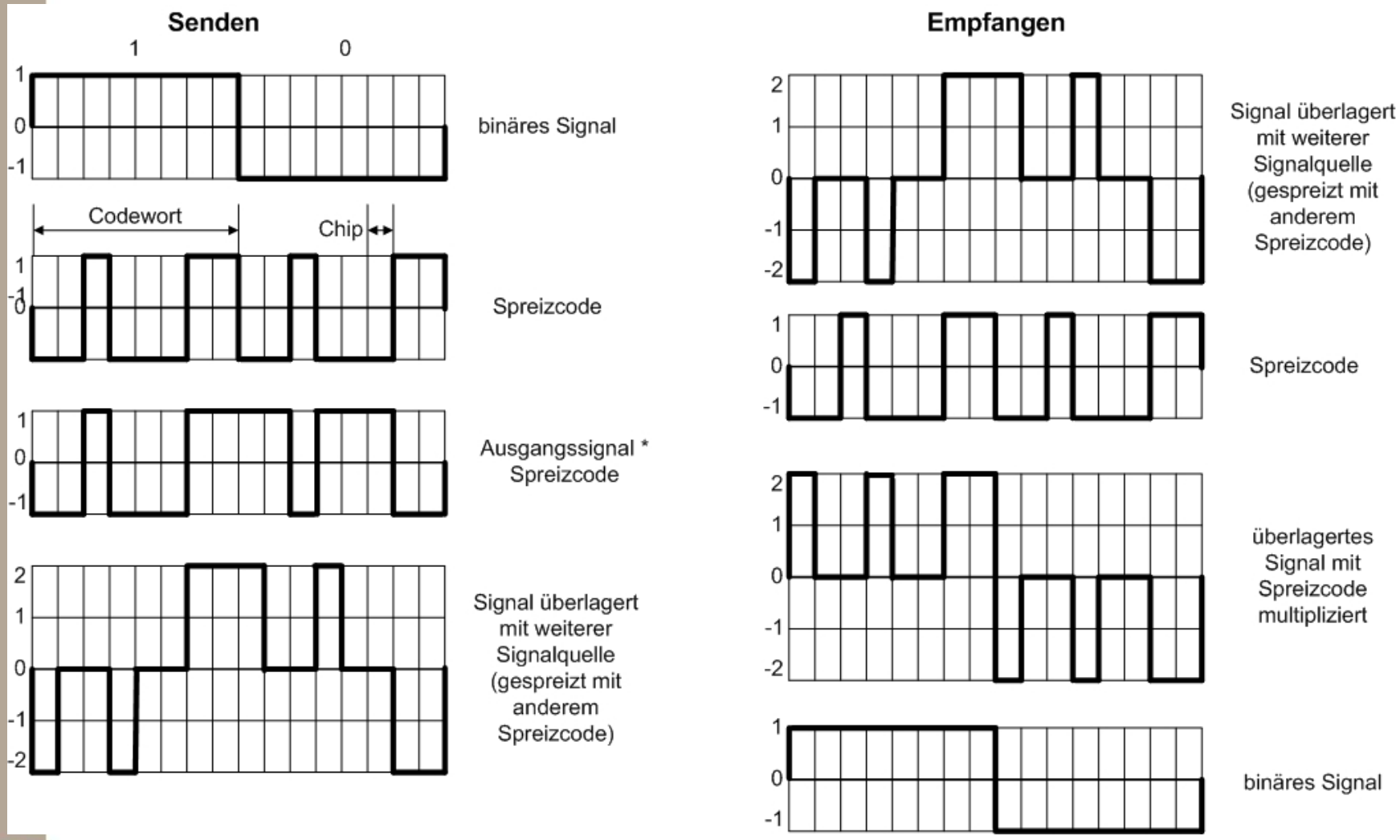
Siehe Applets unter

`www.dpunkt.de/mobile/code/cdma.html`

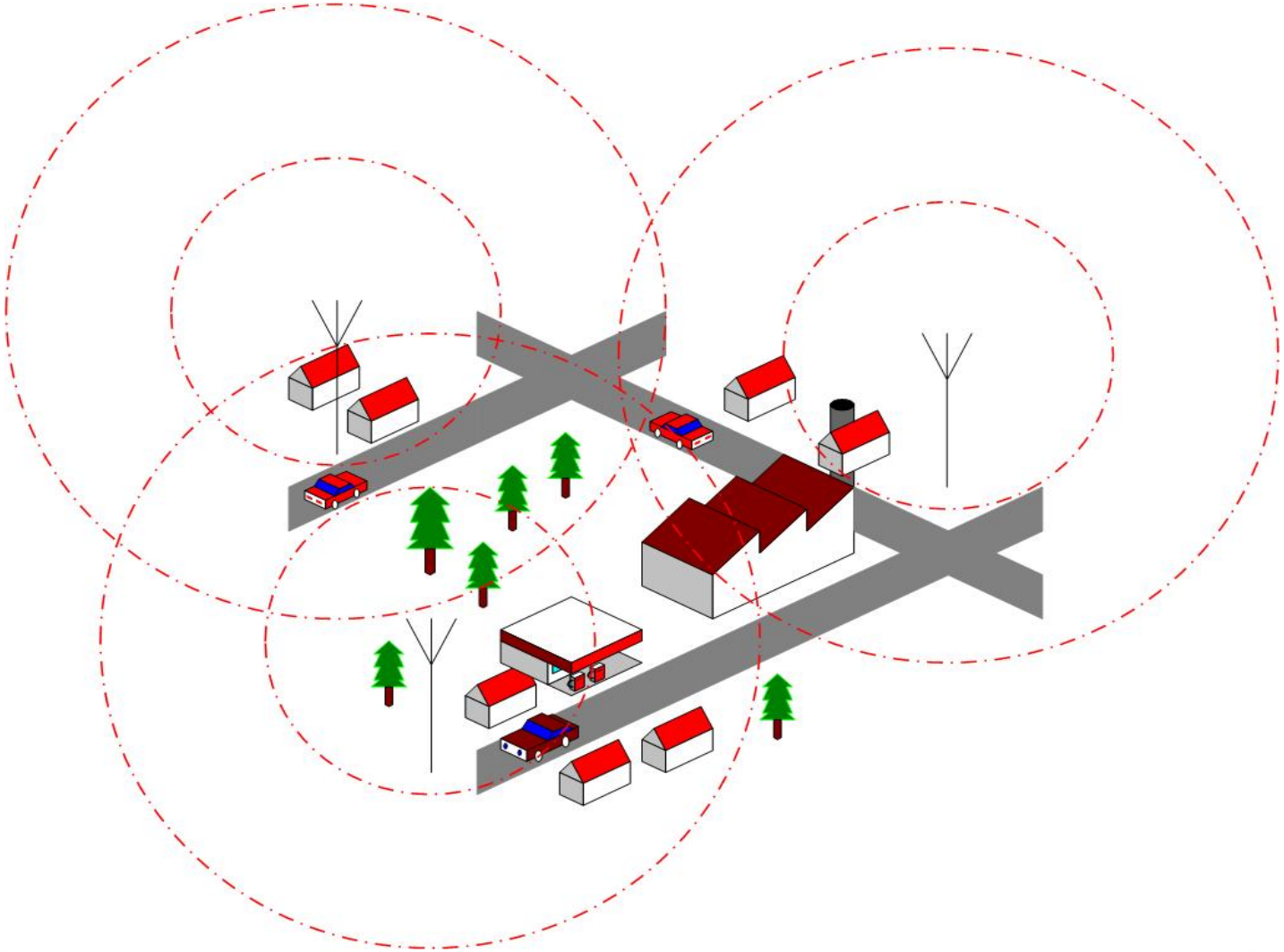
`www.dpunkt.de/mobile/code/cdma2.html`

Drahtlose Kommunikation

Codemultiplex



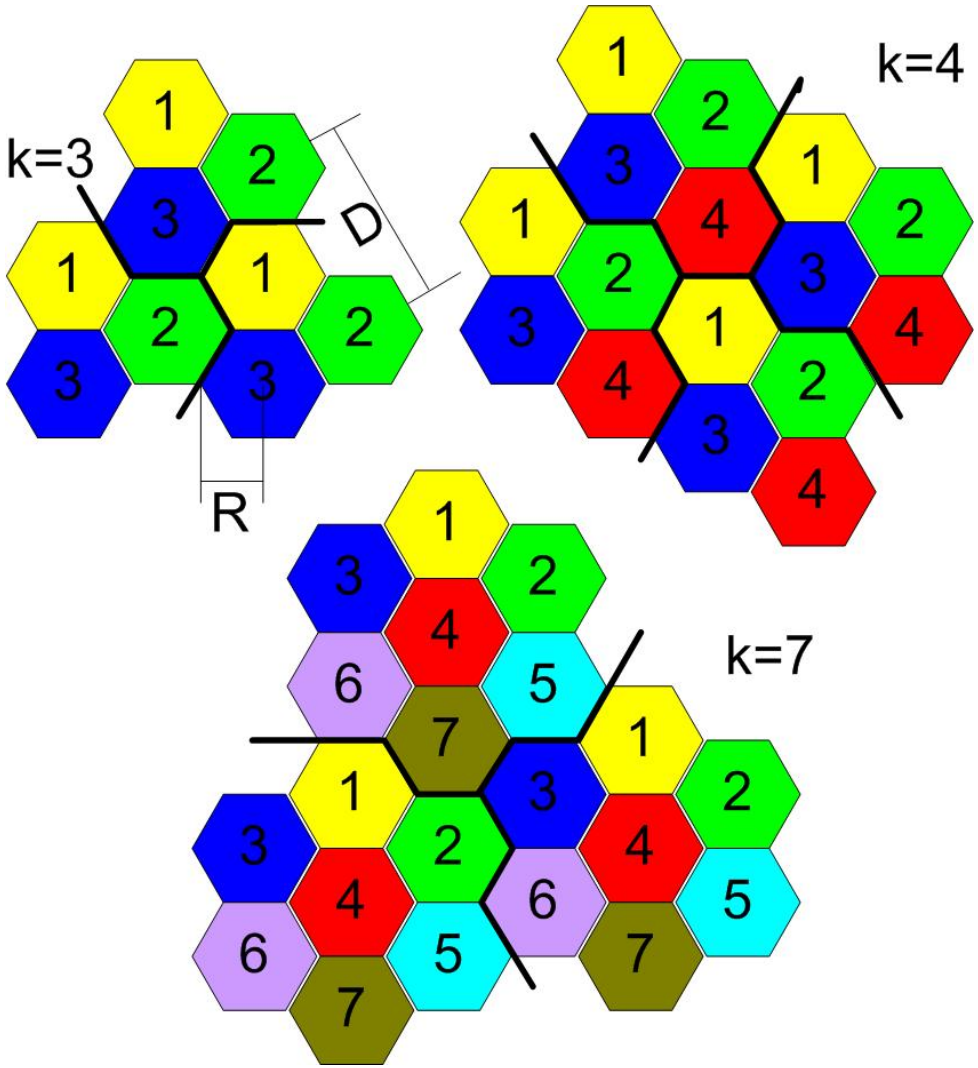
Mobiltelefonie
Zelluläre Mobilfunknetze



Mobiltelefonie
Zelluläre Mobilfunknetze

- Die gesamte Fläche wird mit einem Netz von *Zellen* abgedeckt
- Jede Zelle hat eine *Basisstation*
- Zellen haben die Vorteile
  - Zu überbrückende Sendedistanz ist gering (GSM: ~8km)
  - Ressourcen werden ökonomisch genutzt, da die Frequenzen in nicht angrenzenden Zellen wieder genutzt werden können
- Nachteile sind
  - teure Installation: in 2000 verfügte das D1-Netz über 39.000 Basisstationen

Mobiltelefonie
Clustergrössen



k…Clustergrösse
D…Clusterdimension
R…Zellenradius

$$D = R \cdot \sqrt{3k}$$

Mobiltelefonie
GSM – Einführung

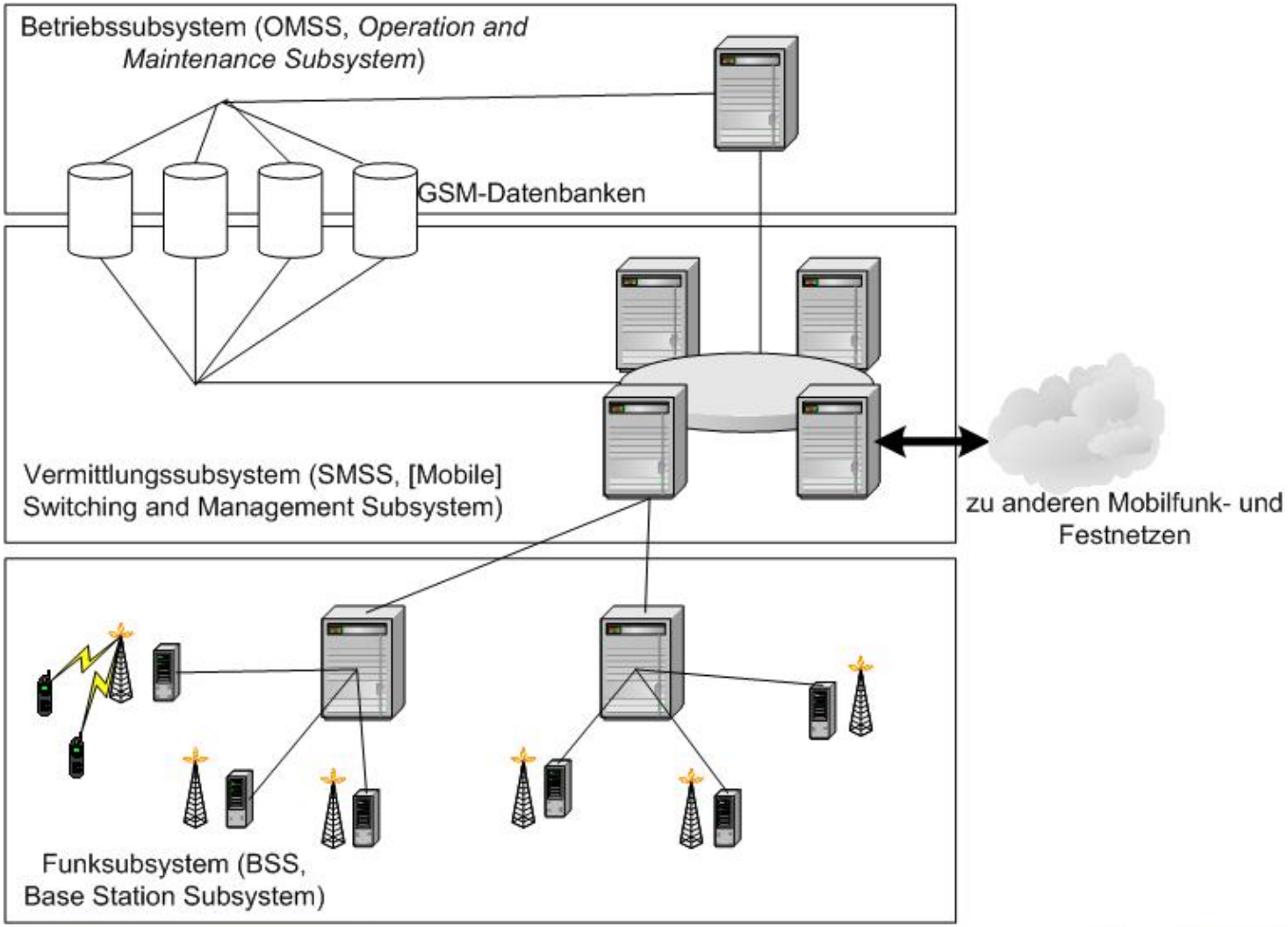
- 1982 Gründung der *Groupe Spécial Mobile*, später Benennung des Systems mit *Global System for Mobile Communication*
- 1989 wird die Gruppe als ETSI TC (Technical Committee) aufgenommen
- geplant für Massenmarkt und vollständige Gebietsabdeckung
- *Handover* zwischen Zellen ohne Unterbrechung
- *Roaming* noch mit Unterbrechung
- SMS, WAP (*Wireless Application Protocol*)
- HSCSD, GPRS, EDGE

Mobiltelefonie
GSM in der Schweiz

- 5 Netzbetreiber mit staatl. Konzession
- 6,8 Mio. Mobilfunkanschlüsse
- 99,8% der Bevölkerung versorgt (2G)
- 4 Netzbetreiber mit UMTS-Konzession
  - 3 davon aktiv
- Versorgung mit 3G beträgt über 90%
- Mobilfunk-Penetationsrate liegt mit 92% der Bevölkerung weit unter dem Durchschnitt westeuropäischer Länder

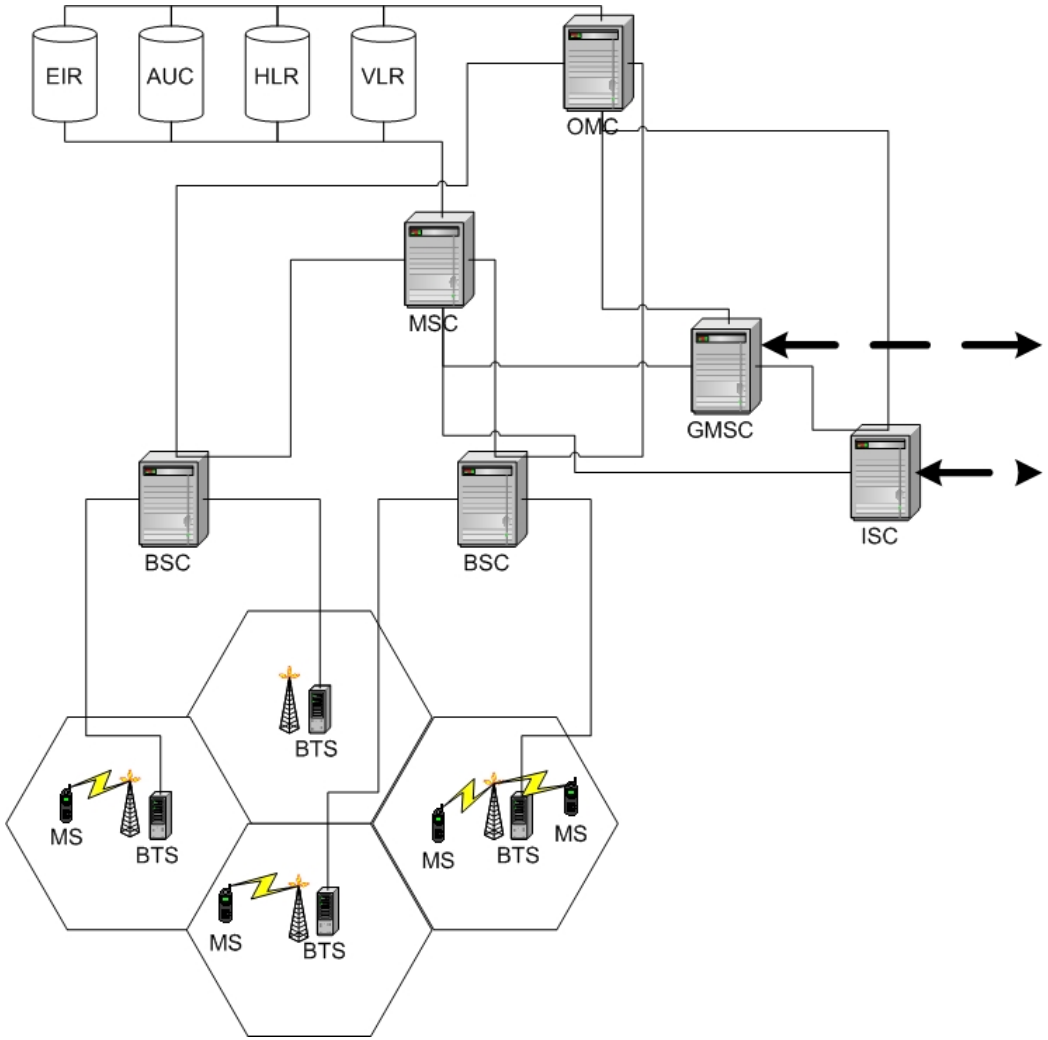
Mobiltelefonie

GSM – Architektur: Subsysteme



Mobiltelefonie

GSM – Architektur: Komponenten



MS	Mobile Station
BTS	Base Transceiver Station
BSC	Base Station Controller
MSC	Mobile Switching Center
OMC	Operation and Maintenance Center
EIR	Equipment Identifier Register
AUC	Authentification Center
HLR	Home Location Register
GMSC	Gateway MSC
ISC	International Switching Center

Mobiltelefonie
GSM

- *Mobile Station* (MS) = *Mobile Equipment* (ME) + *Subscriber Identity Module* (SIM)
  - hat vordefinierte maximale Sendeleistung
    - Autotelefone: 20W
    - tragbare Geräte: 8W
    - Handgeräte mit 5W
    - Handgeräte mit 2W
- *Equipment Identity Register* (EIR)
  - speichert IMEI (*International Mobile Equipment Identity*)
  - in *White List* sind alle registrierten Geräte
  - in *Black List* sind gesperrte Geräte
  - in *Gray List* sind veraltete Geräte gespeichert

Mobiltelefonie
GSM

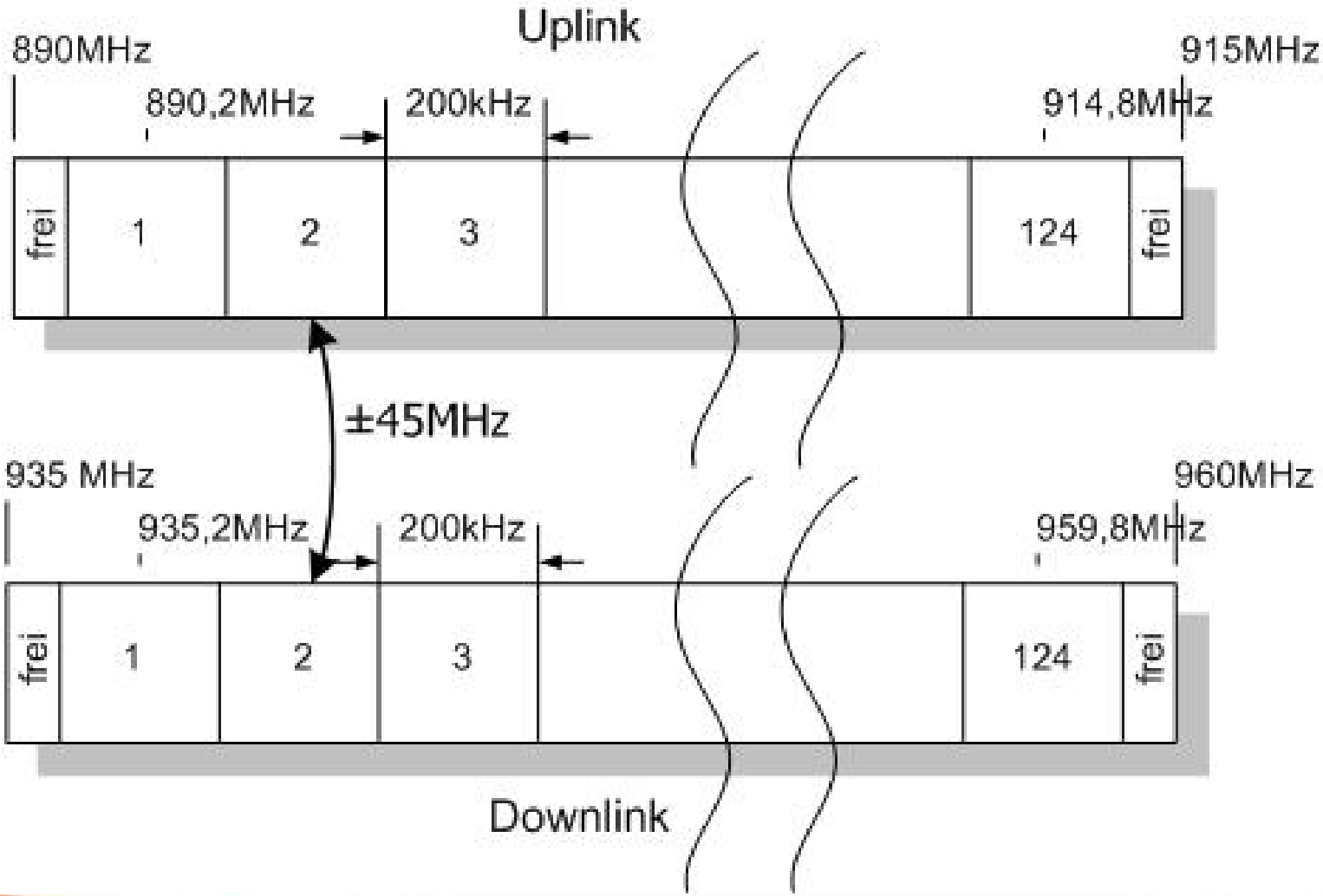
- *Home Location Register (HLR)*
  - speichert permanente und temporäre (z.B. der aktuelle Standort) Daten für jeden Kunden
- *Visitor Location Register (VLR)*
  - speichert Daten von Teilenehmern, die sich im Bereich eines MSC befinden; dies sind Kunden des Netzes und über Roaming auch Kunden anderer Netze
- *Authentication Center (AUC)*
  - speichert vertrauliche Daten über Kunden und deren Schlüssel
- *International Mobile Subscriber Identity (IMSI)*
  - identifiziert einen Kunden über eine weltweit eindeutige Nummer, die *nicht* die Telefonnummer ist

Mobiltelefonie
GSM – Die Luftschnittstelle

- GSM verwendet eine Kombination aus
  - FDMA
    - Aufteilung in ein Downlink- (MS -> BTS) und ein Uplink- (BTS -> MS) Frequenzband
    - Aufteilung eines Bandes in Kanäle (*Radio Frequency Channels, RFCH*)
    - GSM 900: 124 Kanäle, 890-915MHz (Uplink), 935-960MHz (Downlink)
    - DCS 1800: 372 Kanäle, 1710-1785MHz (Uplink), 1805-1880MHz (Downlink)
    - Mehrere Provider teilen sich die Kanäle
  - TDMA
  - SDMA (wie alle zellulären Netze)

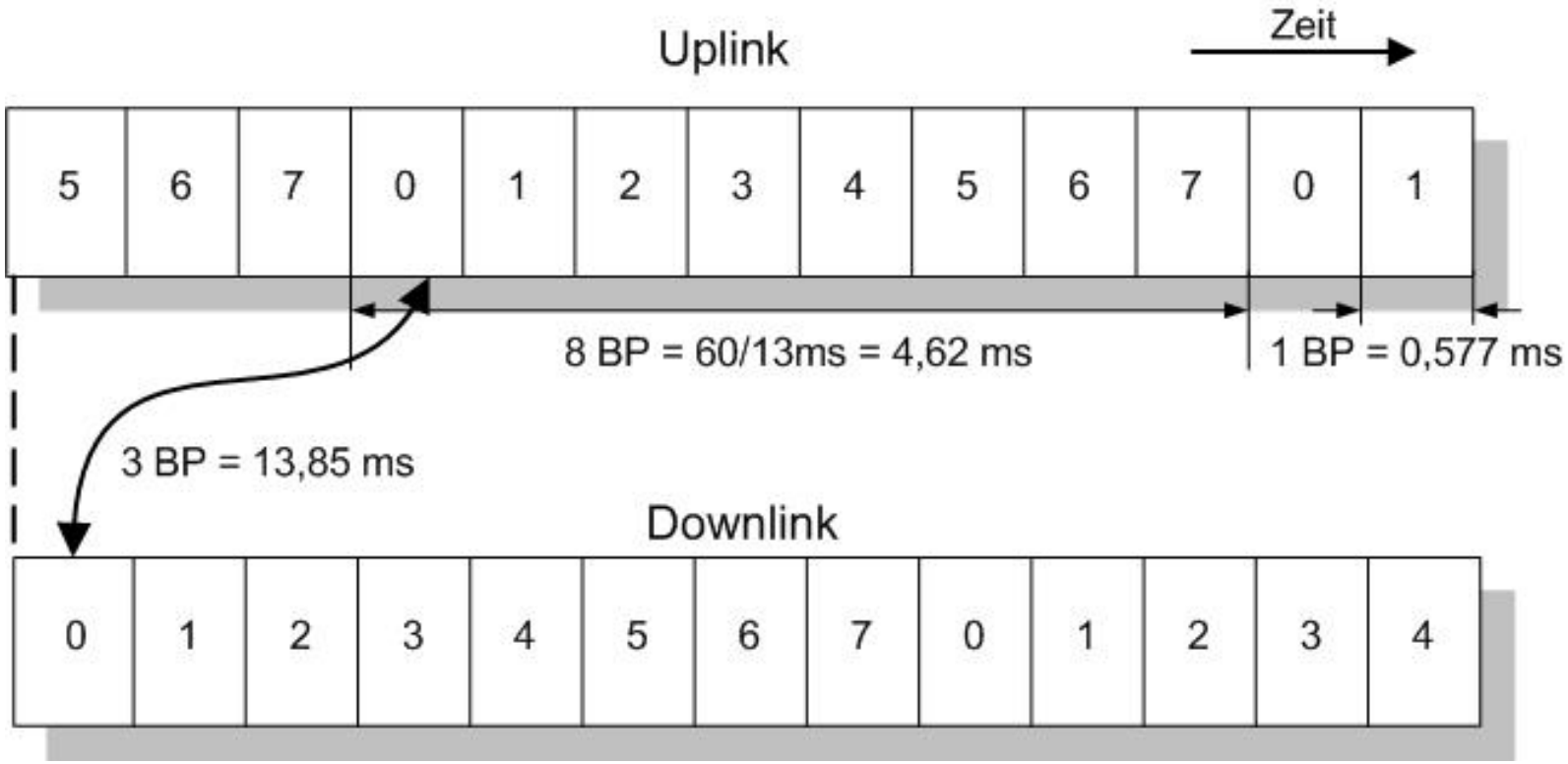
Mobiltelefonie

GSM – Kanäle in GSM 900

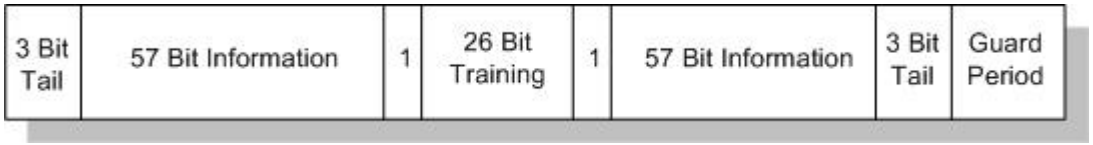


- Frequency Hopping
  - dient zum Ausgleich gestörter Kanäle
- TDMA
  - Aufteilung eines Kanals in 8 Zeitschlitze (0-7), *Burst Periods, BP*
  - Zeitschlitze zwischen Uplink und Downlink sind um 3 Zeitschlitze verschoben, damit ein Gerät nicht gleichzeitig senden und empfangen muß
  - -> ein bidirektionaler Kanal zwischen BTS und MS entsteht

Mobiltelefonie
GSM – TDMA

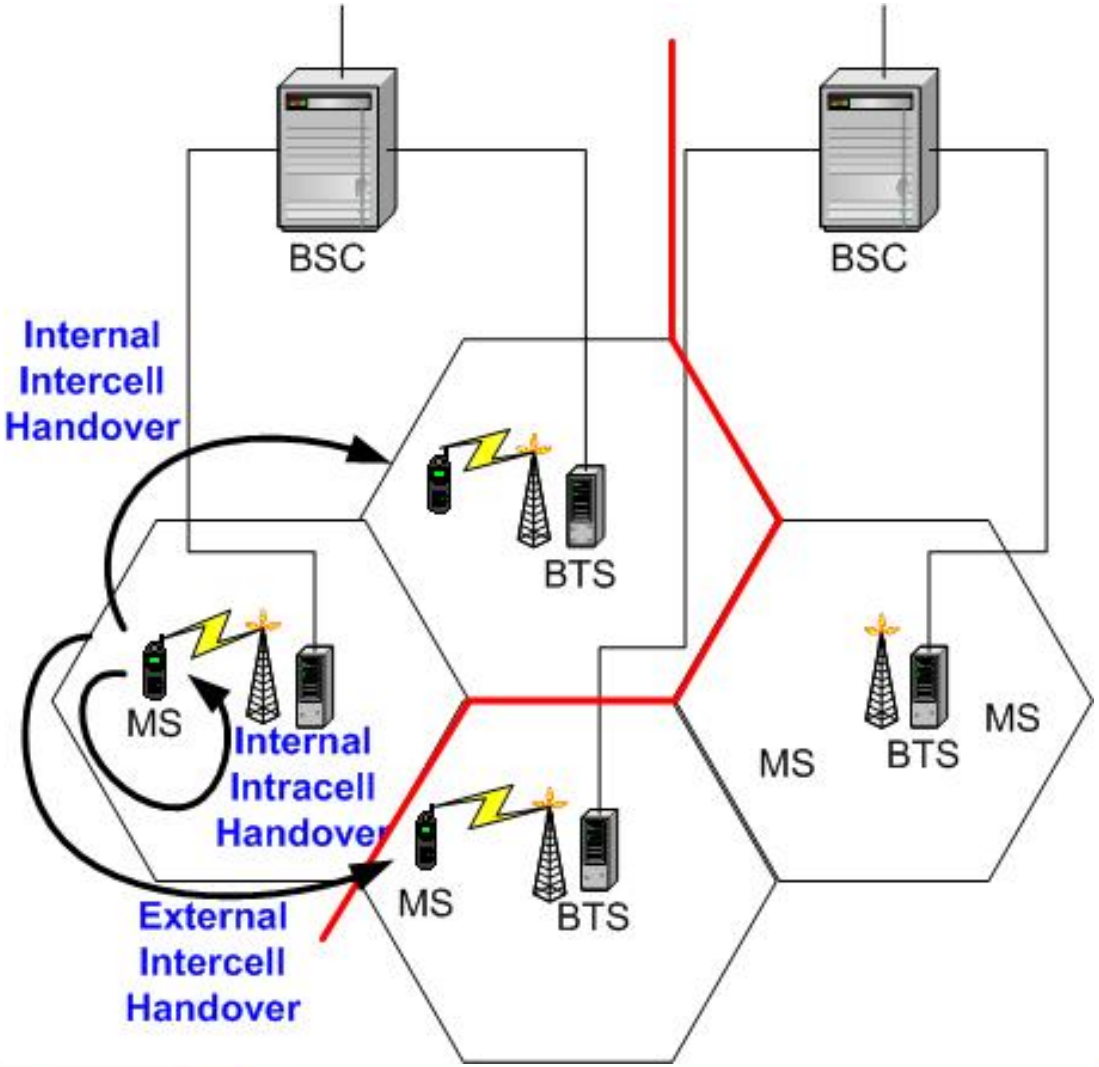


Mobiltelefonie
GSM – TDMA: Burst



- *Tail-Bits* stehen am Beginn und Ende der Übertragung
- Die Trainingssequenz erlaubt dem Empfänger, sich während der Übertragung mit dem Sender zu synchronisieren
- Ein Burst enthält 57 * 2 = 114 Bits an Nutzdaten
- 1 BP = 0,577 ms, alle 8 Slots ein Burst -> max. 24.700 Bit/s
- Da nicht nur normale Bursts gesendet werden kommt man in der Realität auf
  - 13.000 Bit/s für Sprache
  - 9.600 Bit/s für Daten

Mobiltelefonie
GSM – Handover



Mobiltelefonie
GSM – Handover & Roaming

- Beim *Handover* wird die Verbindung in eine andere Zelle verlegt
  - dies passiert abhängig von einer automatischen Entscheidung
    - bei zu kleinem Empfangspegel (< Schranke)
    - bei zu hoher Bitfehlerhäufigkeit (> Schranke)
    - bei maximaler Entfernung zwischen MS und BTS
  - Der Handover ist *network-originated*
    - Algorithmus ist hängt vom Netzbetreiber ab
    - Bei einer Algorithmusänderung müssen die MS nicht geändert werden
- *Roaming*
  - erlaubt die Nutzung des Netzes bei freigeschalteten Partnerbetreibern (meist Ausland)

Mobiltelefonie
GSM – Weiterentwicklungen (2+)

- GSM (Phase 2) hat mit 9,6 kBit/s eine zu kleine Datenrate für moderne Anwendungen
- ➔ Phase 2+
  - HSCSD (*High Speed Circuit Switched Data*)
    - Kanalbündelung mit 14,4kBit/s pro Kanal
    - Bis zu 8 Kanäle (oft Limit bei 4) mit 115,2 kBit/s (bzw. 57,5 kBit/s)
    - Nachteil: Leitungsorientertes Verfahren
  - GPRS (*General Packed Radio Service)*
    - Paketorientiertes Verfahren; „always online“
    - bis zu 171,2 kBit/s
  - EDGE (Enhanced Data Rates for GSM Evolution)
    - Neues Modulationsverfahren mit max. 473,6 kBit/s, abhängig von der Übertragungsqualität
    - zusätzlich zu HSCSD (ECSD) und GPRS (EGPRS)

Wireless Local Area Networks

Vergleich WLAN - Festnetz

- Vorteile
  - Keine kostspielige Verkabelung
  - Bereich ist nicht auf ein Gebäude beschränkt
  - Schneller Aufbau, gut für temporäre Installation
  - Geräte sind sehr mobil (praktisch z.B. in Krankenhäusern)
  - Unterwegs Netzwerkzugang mittels *Hot-Spots*
- Nachteile
  - Wesentlich geringere Bandbreite und höhere Fehlerrate
  - Frequenzen sind oft national unterschiedlich beschränkt
  - Leichte Abhörbarkeit
  - Deutlich höherer Stromverbrauch
  - Abstrahlung kann andere Geräte stören; Auswirkung auf biologische Organismen?

WLAN
Voraussetzungen

- Dienste und deren Anforderungen:

Dienst	Datenrate	Verzögerung	Paketfehlerrate
Sprache (hohe Qualität)	64 kBit/s	10 ms	10^{-3}
Sprache (mittlere Qualität)	8 kBit/s	30 ms	10^{-3}
Videokonferenz	3 MBit/s	10 ms	10^{-5}
TV (High Definition TV)	19 MBit/s	90 ms	10^{-5}
TV (Standard Definition TV)	3 MBit/s	90 ms	10^{-5}
Audio (CD-Qualität)	256 kBit/s	100 ms	10^{-5}
Daten (hohe Datenrate)	10 MBit/s	anwendungs-abhängig	0
Daten (mittlere Datenrate)	2 MBit/s		0
Daten (niedrige Datenrate)	500 kBit/s		0

WLAN
Consumer Components

Interface-Karte

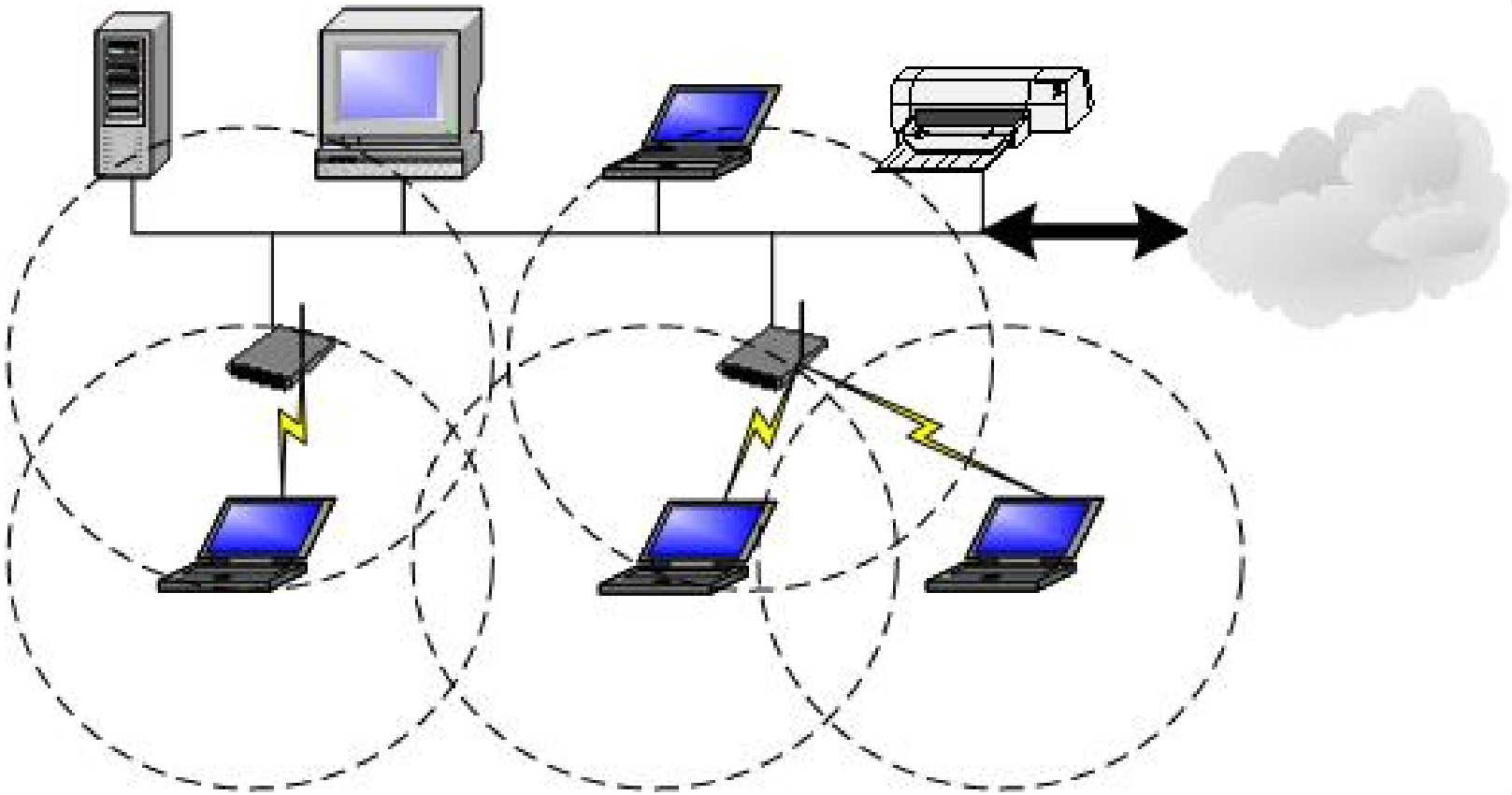
Oft in das Gerät integriert,

z.B. Centrino-Architektur

Access Point

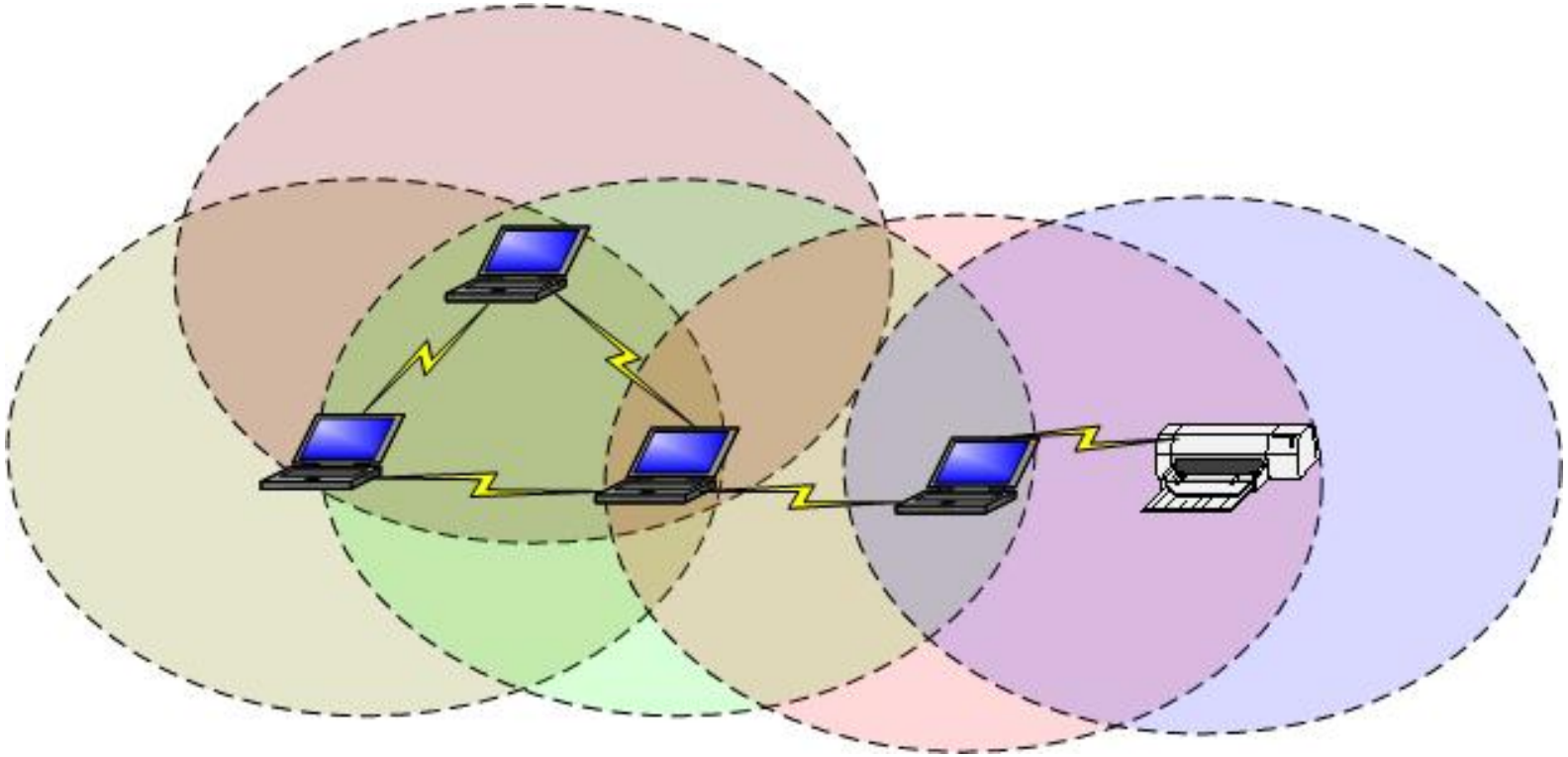
im Versorgungsbereich verteilt

WLAN
Infrastruktur-Modus



WLAN
Ad-Hoc-Modus

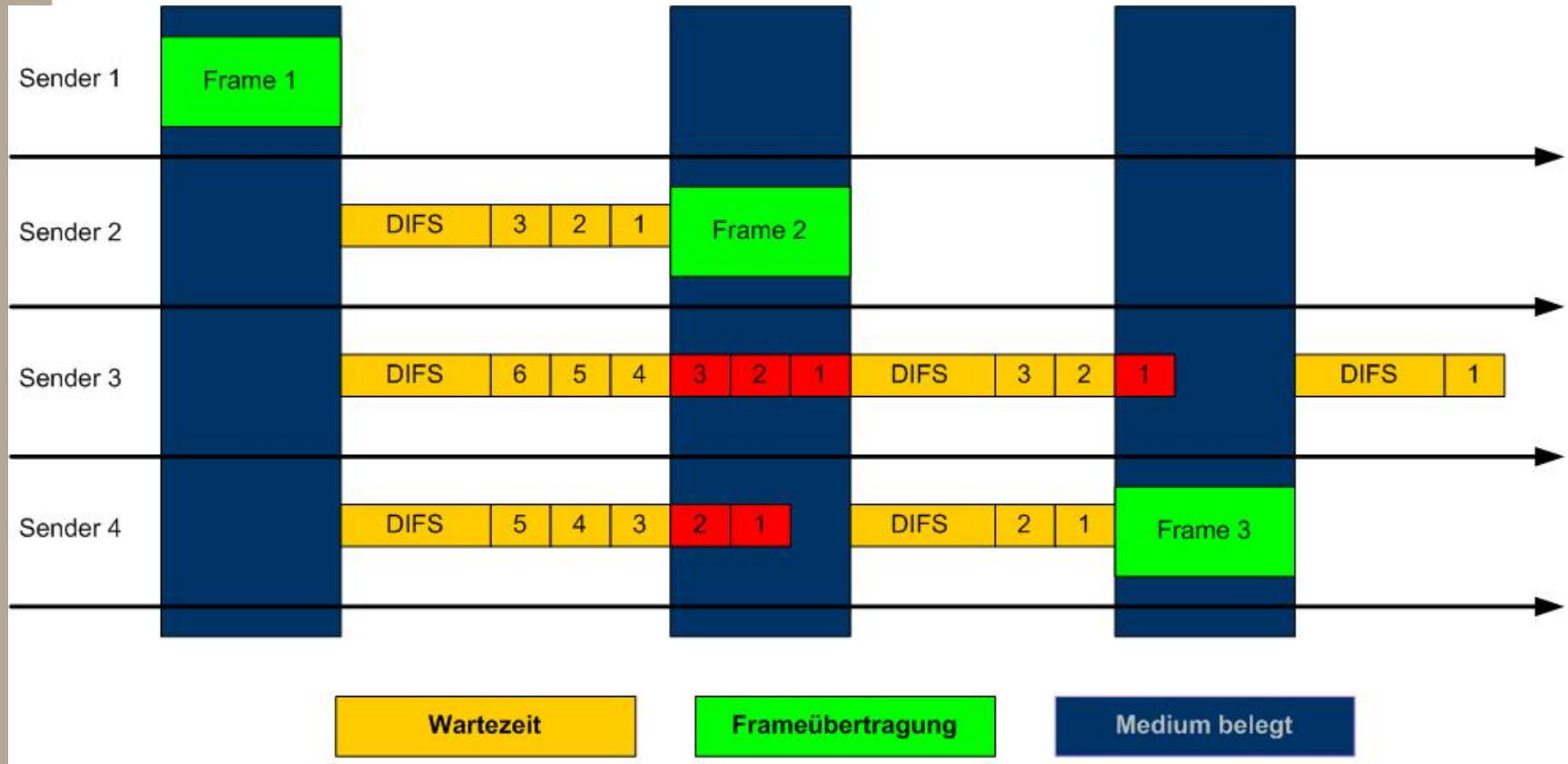
- IETF MANET (Mobile Ad-Hoc Networks)



WLAN
Zugriff auf das Funkmedium

- Die MAC-Schicht regelt den Zugriff
  - mit Entdeckung und Neusenden bei Kollisionen
  - oder mit Vermeidung von Kollisionen
- Die erste Möglichkeit geht beim Funk nicht
  - CSMA/CD (*Carries Sense Multiple Access with Collision Detection*) wird bei Ethernet eingesetzt
  - Beim Senden kann eine Station keine Kollision entdecken, da das eigene Signal die Störungen anderer in unmittelbarer Sendernähe überdeckt
- → 3 verschiedene Verfahren im Einsatz
  - CSMA/CA: CSMA with Collision Avoidance (Pflicht)
  - CSMA/CA mit RTS/CTS (Option)
  - PCF, nur im Infrastrukturmodus (Option)

WLAN
CSMA/CA Multicast

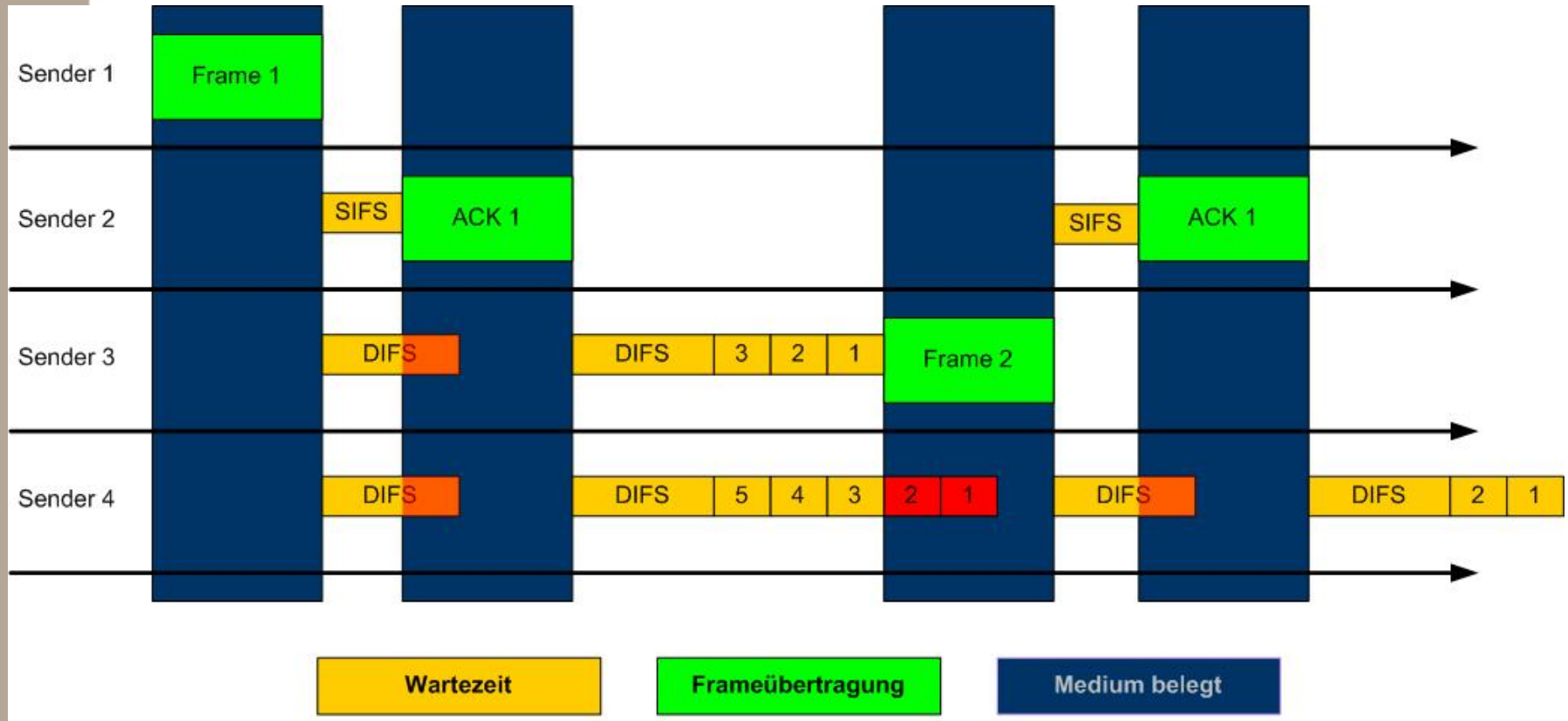


DIFS: DCF Interframe Space (Mindestabstand zwischen Frames beim Senden)

6, 5, 4, ..: Zufallsabhängige Wartezeit

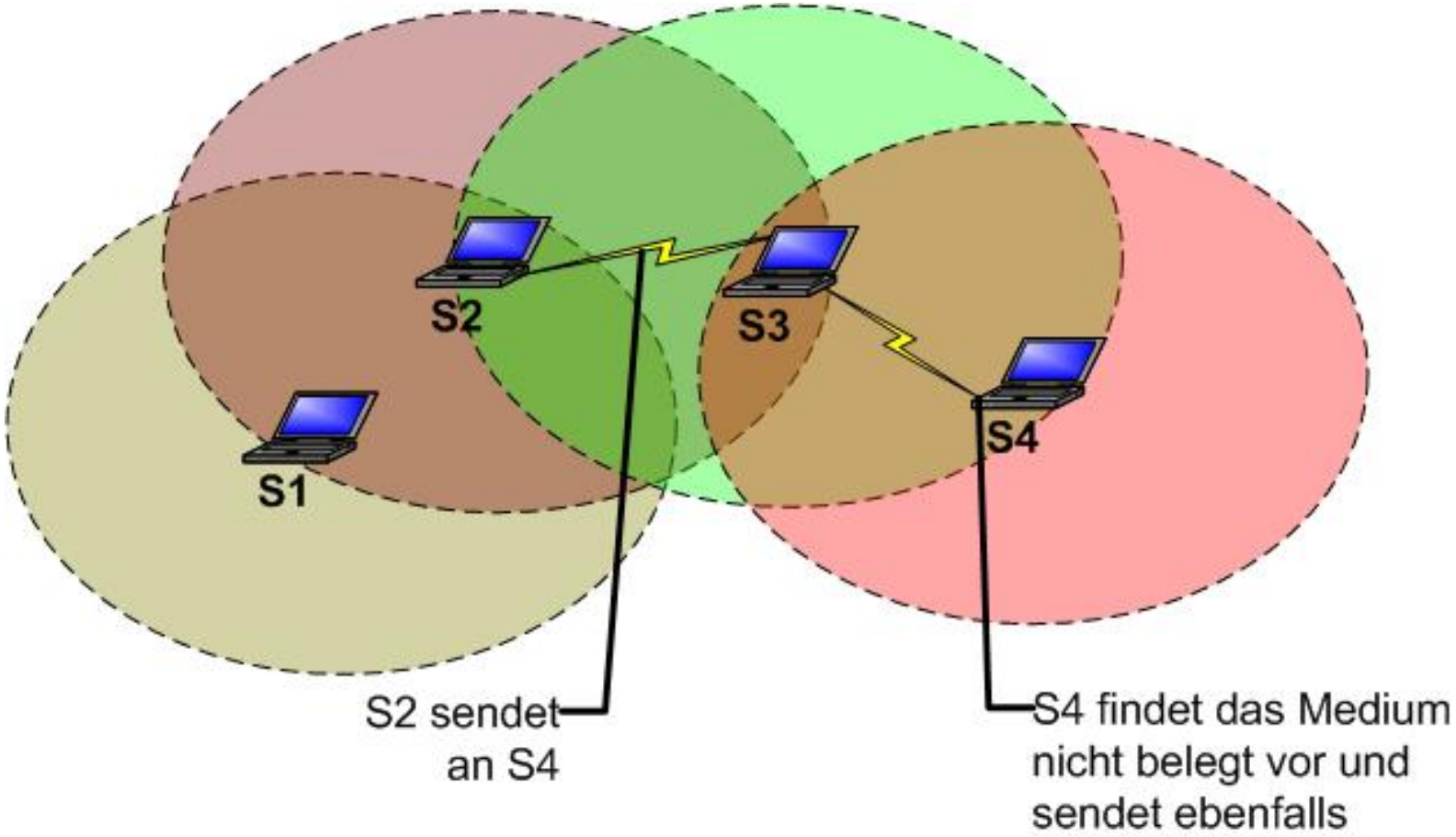
Contention Window: Wartezeit bei maximal gewählter Zufallszahl, wird im adaptiven Verfahren *Exponential Backoff* mit den Werten 7, 15, 31, 63, 127 oder 255 belegt

WLAN
CSMA/CA, Framebestätigung

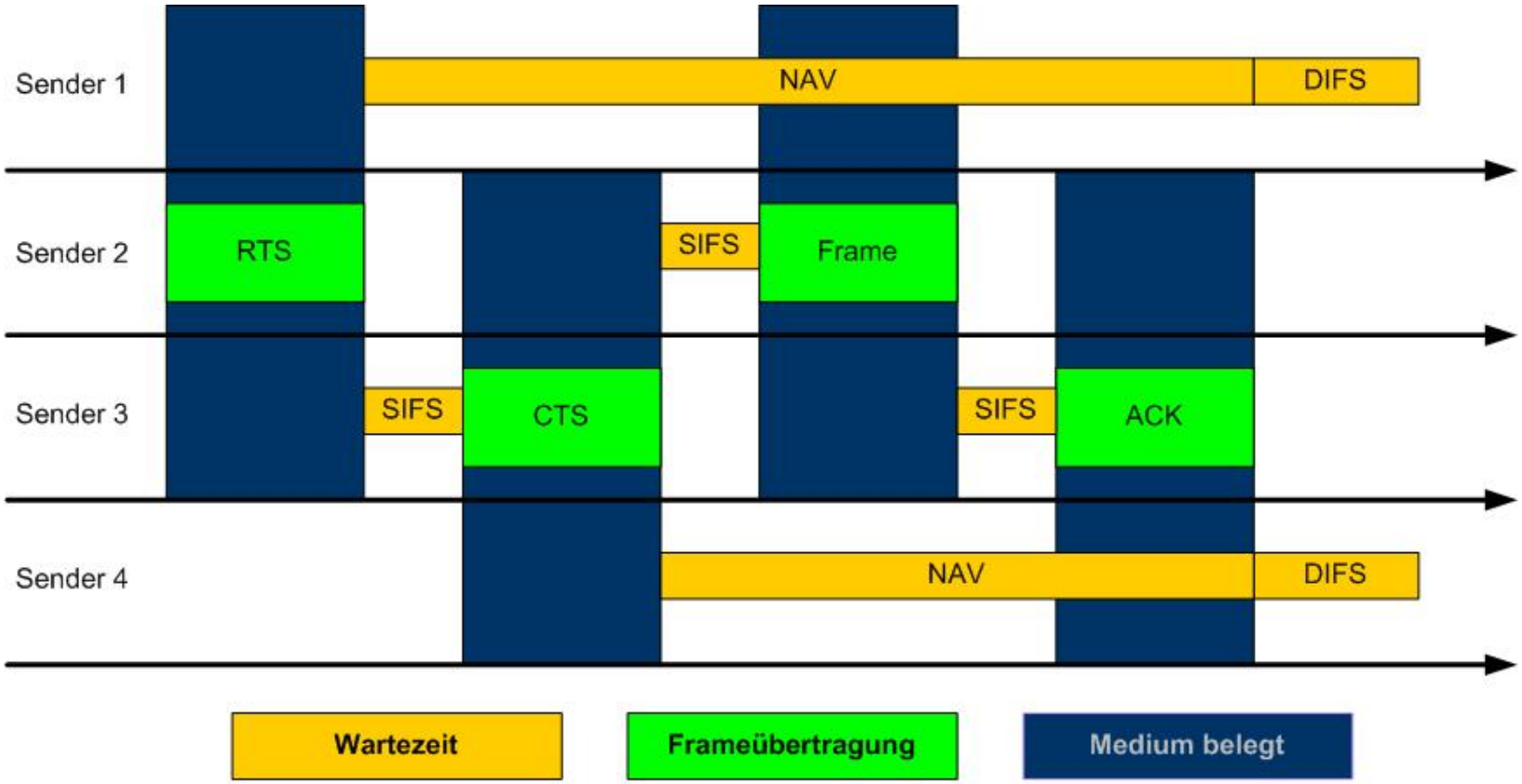


SIFS: Short Interframe Space

WLAN
Hidden Terminal Problem



WLAN
CSMA/CA mit RTS/CTS



RTS: Request To Send

CTS: Clear To Send

NAV: Net Allocation Vector; diese Wartezeit wird in den Signalen RTS und CTS mitgeschickt

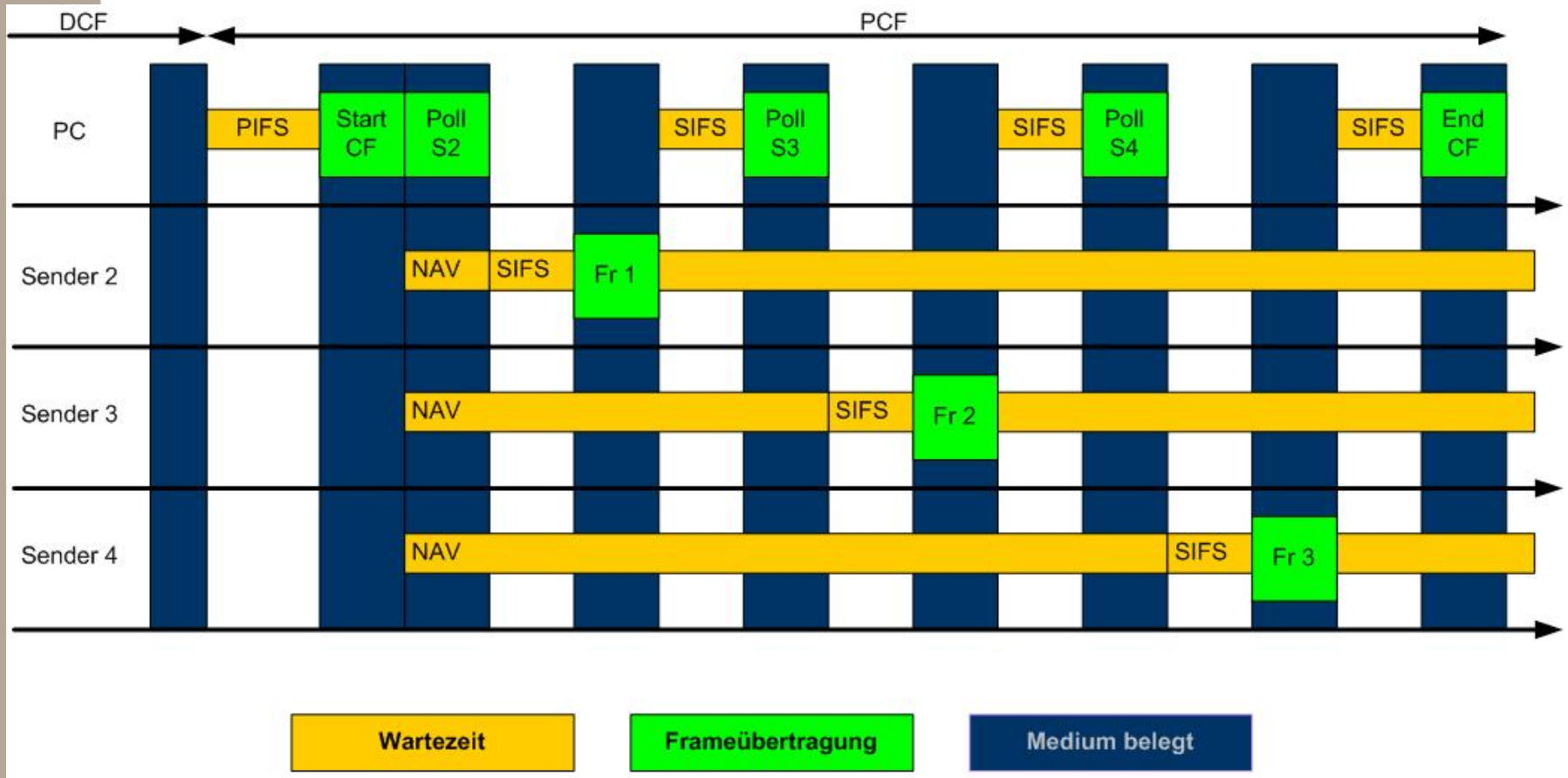
WLAN
CSMA/CA mit RTS/CTS

- *Hidden-Terminal Problem erzwingt die Strategie*
- *CSMA/CA mit RTS/CTS ist optional*
- *Über die Signale RTS und CTS wissen betroffene Stationen, daß sie die Zeit NAV (*Net Allocation Vector*) warten sollen*
- *Zusätzlicher Verwaltungsaufwand -> sinkender Nutzdatendurchsatz*
  - *Übertragung großer Frames besser, doch bei der höheren Fehlerwahrscheinlichkeit muß oft der ganze Frame neu übertragen werden*
  - *Frames können aufgeteilt werden ohne neue RTS/CTS zu senden*

WLAN
PCF Funktion

- *CSMA-Verfahren garantieren **keine***
  - *minimale Bandbreite*
  - *maximale Verzögerung*
- *Bei Kollisionshäufung erliegt die Übertragung*
- *Abhilfe: PCF (*Point Coordination Function*)*
  - *Point Coordinator*
    - *übernimmt die Koordinierung der Sender*
    - *ist nur im Infrastrukturmodus möglich*
    - *ist meist der Access Point*
    - *wechselt vom DCF in den PCF-Modus und zurück*
    - *pollt durch die Stationen (Polling-Frames können Nutzdaten enthalten) -> hoher Durchsatz*

WLAN
PCF



PIFS: PCF Interframe Space, > SIFS, < DIFS

WLAN
Uhrensynchronisation

- Genau synchronisierte Uhren sind erforderlich
  - Z.B. für Wartezeiten beim Medienzugriff
  - Beim Frequenzwechsel beim FHSS-Verfahren
- *Timing Synchronization Function* (TSF)
  - Spezieller *Beacon*-Frame wird verwendet
  - Periodische Aussendung des Frames
  - Empfangende Stationen korrigieren ihre Zeit
  - Infrastrukturnetze
    - Access Point sendet die Zeit
  - Ad-Hoc-Netze
    - Der erste Client, der senden darf, bestimmt die Zeit
  - Latenzzeit bis der Beacon-Frame gesendet wurde

WLAN
Power Management

- Awake Mode
  - benötigt recht viel Strom
- Sleep Mode
  - Sende- und Empfangselektronik wird deaktiviert
  - Station kann keine Pakete empfangen
- Periodisches Aufwachen
  - Sendende Station merkt such Pakete, sie sie an schlafende Partner senden möchte
  - Im Infrastrukturmodus
    - wachen Stationen auf, wenn sie Beacon-Frame erwarten
    - Access Point sendet im Beacon mit, auf wen Pakete warten und sendet diese dann
  - Im Ad-Hoc-Modus
    - komplizierter
    - sehr hohes Paketaufkommen nach Beginn der Beaconperiode

WLAN
Weiterentwicklungen

IEEE-Standard/ Gruppe	Beschreibung
802.11 [1997]	1-2 MBit/s; 2,4 GHz; *veraltet*
802.11a [1999]	54 MBit/s; 5 GHz; *geringe Verbreitung*
802.11b [1999]	11 MBit/s; 2,4 GHz; *noch relativ weit verbreitet*
802.11g [2003]	54 MBit/s; 2,4 GHz; *stärkste Nutzung*
802.11n [->2006]	540 MBit/s; 5 GHz; *noch nicht fertig*
802.11p [->2008]	27 MBit/s; 5 GHz; für Fahrzeug-zu-Fahrzeug geplant
802.11c	MAC-Layer-Bridging gemäß 802.1d
802.11d	Anpassungen an nationale Regelungen
802.11e	MAC-Erw.: QoS, besseres Power Management
802.11f	*Inter Access Point Protocol*
802.11h	Reichweitenanpassung *Indoor* <-> *Outdoor*; 5 GHz
802.11i	MAC-Erw.: bessere Sicherheit und Authentifikation
802.11j	4.9-5 Ghz Spezifikation für Japan
802.11s [->2008]	Mesh Netzwerke

Zusätzlich proprietäre Erweiterungen von diversen Firmen

Wireless PANs
Überblick

- *Personal Area Network*
  - Vernetzung von kleinen mobilen Geräten untereinander
  - Ersatz von Kabeln (RS 232, USB, parallel, …)

- Unterschied zu LAN
  - Kleinere Reichweite im Bereich cm bis wenige m
  - Stärkerer Fokus auf Stromsparen
  - Kostengünstige Hardware für den Massenmarkt
  - Hohe Benutzerfreundlichkeit und geringer Konfigurationsaufwand
  - Spezialisierter Einsatz (z.B. Headset für Mobiltelefone)
  - Point-to-Point Kommunikation

Wireless PANs

Beispielhafte Einsatzgebiete

- Ausdrucken von Fotos von einer Digitalkamera auf einem Fotodrucker
- Anschluß eines drahtlosen Headsets an ein Mobiltelefon
- Anschluß von Rechnerperipherie (Maus, Tastatur, Bildschirm, …)
- Vernetzung von Haushaltsgeräten
- Vernetzung von PDAs
- Zugriff auf medizinische Daten, die direkt beim Patienten ermittelt werden (Sonden, Sensoren)

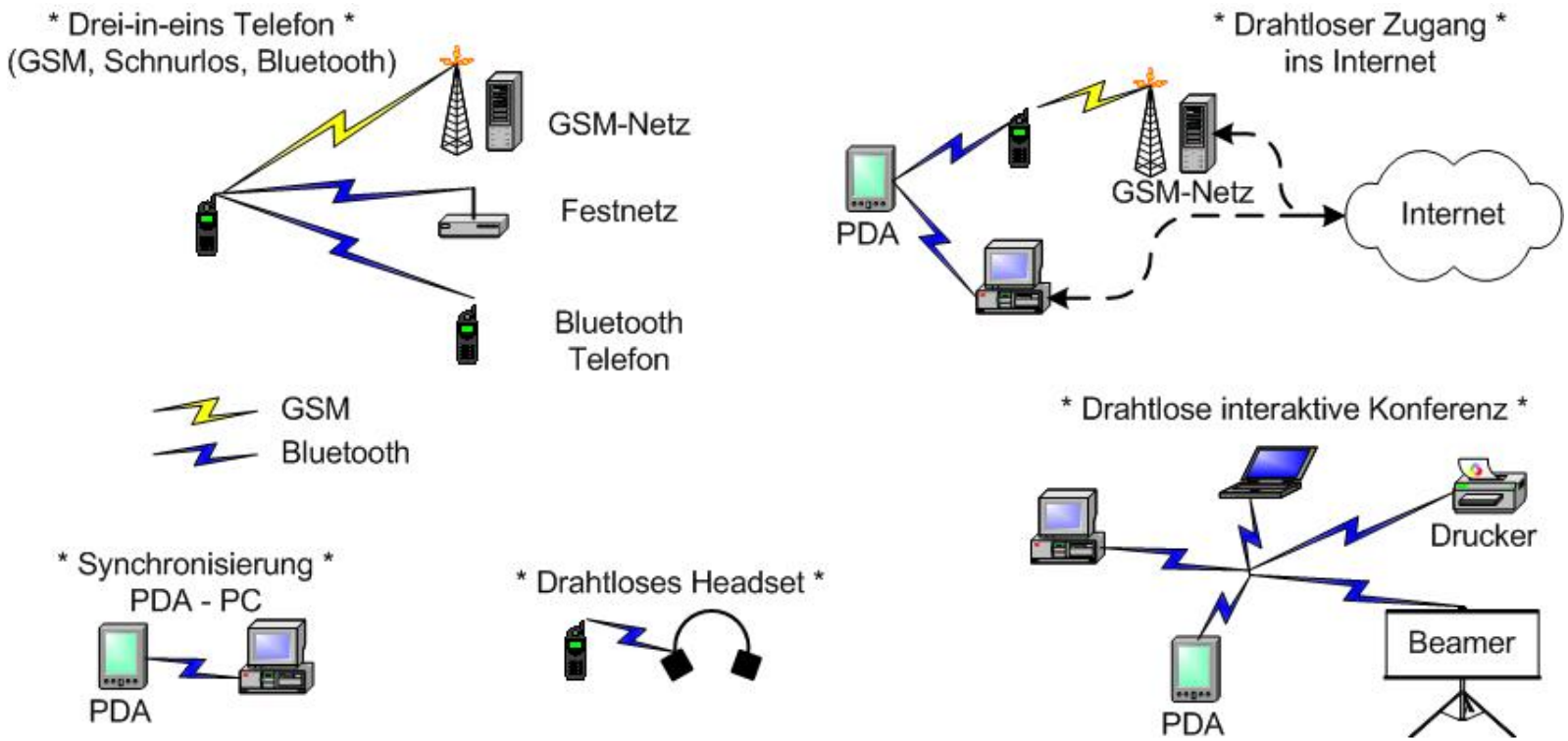
Bluetooth
Überblick

- 1994 entworfen von Ericsson zur Vernetzung von Geräten, die auch in der Kleidung getragen werden
  - Funk ist hier besser geeignet als Infrarotlicht
- 1998 Übergabe an die Bluetooth Special Interest Group (SIG)
  - bestehend aus Ericsson, Nokia, IBM, Intel und Toshiba
  - benannt nach dem Wikingerkönig Harald Blauzahn, 10. Jahrhundert (Buch „Die Abenteuer des Röde Orm“)
  - Entwicklung eines billigen Massenprodukts
    - kann preislich aber nicht mit IrDA konkurrieren
    - in großen Stückzahlen im Bereich einiger Dollar
    - Juli 1999 Bluetooth 1.0
    - Nov. 2003 Bluetooth 1.2
    - Nov. 2004 Bluetooth 2.0 + EDR
- Mehr Information unter **`www.bluetooth.org`**

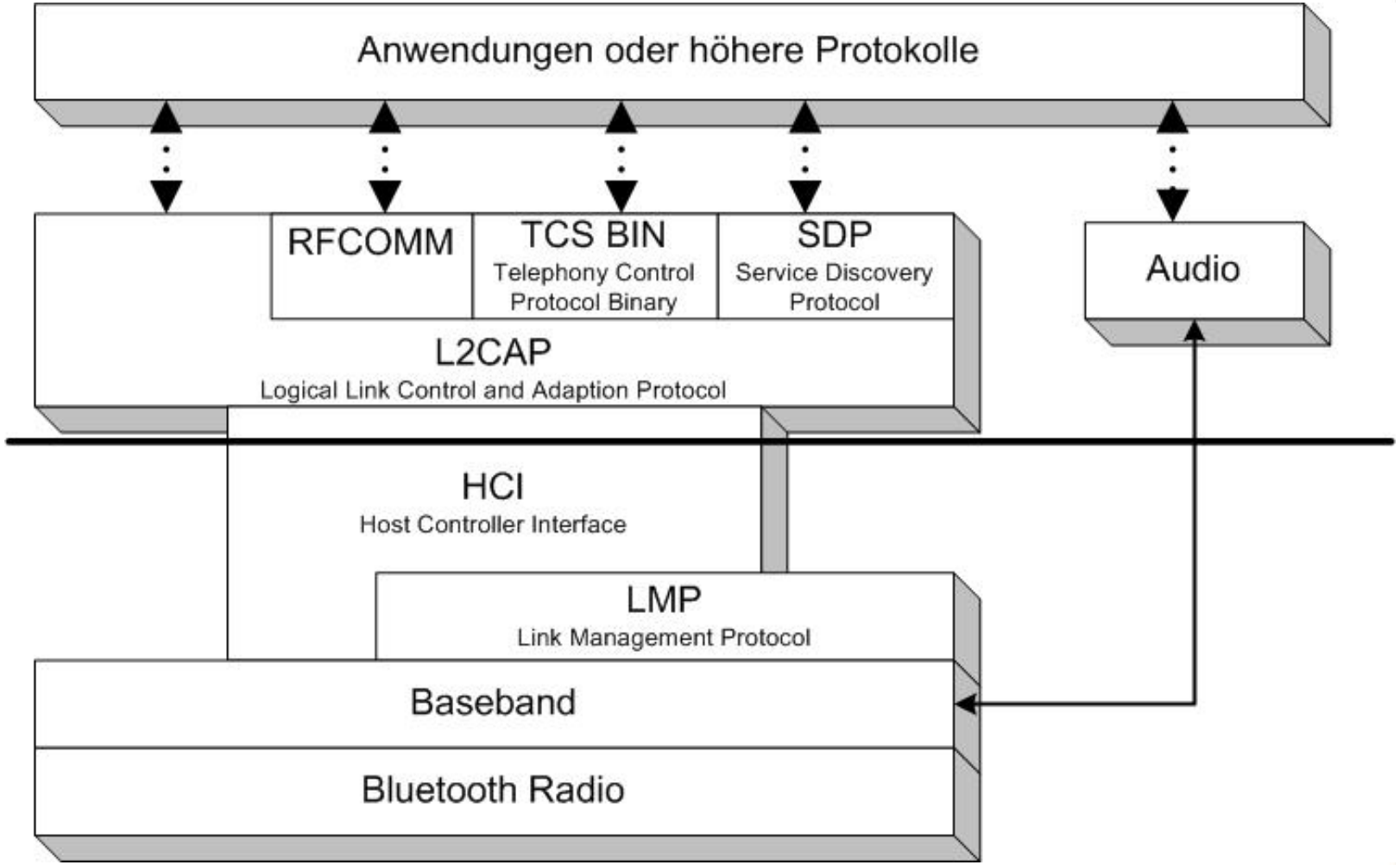
Bluetooth
Eigenschaften

- 1 MBit/s bei bis zu 10 m (bzw. 100m) Reichweite
  - ab Version 2.0 EDR (*Enhanced Data Rate*) mit 2 und 3 Mbps
- Automatische Verbindung von Geräten in Kommunikationsweite
- Suche installierter Dienste eines anderen Geräts
- Mehrere logische Kanäle zwischen zwei Geräten
- Nachrichtensenden über *Broadcast*
- Audiokanäle zwischen zwei Geräten
- Einstellen von Dienstgüteparametern
- Existenz eines Transportprotokolls mit Flusskontrolle und Segmentierung langer Nachrichten
- Emulation serieller Schnittstellen
- Integration von Authentifizierung und Verschlüsselung

Bluetooth
Anwendungsszenarien

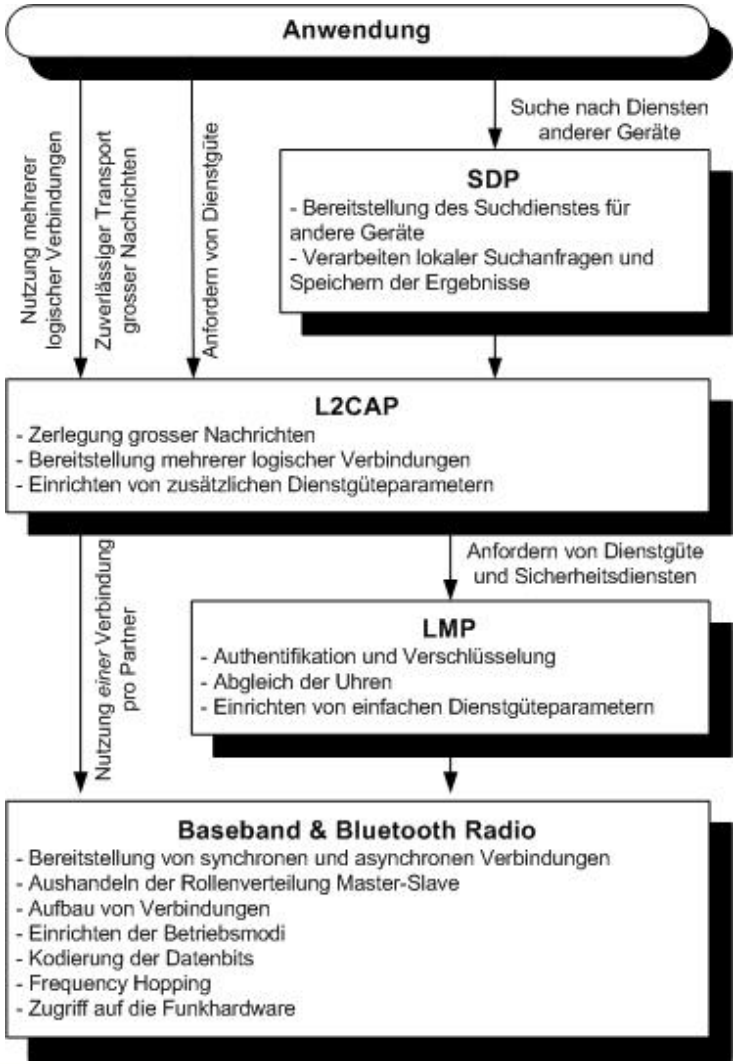


Bluetooth
Protokollstapel

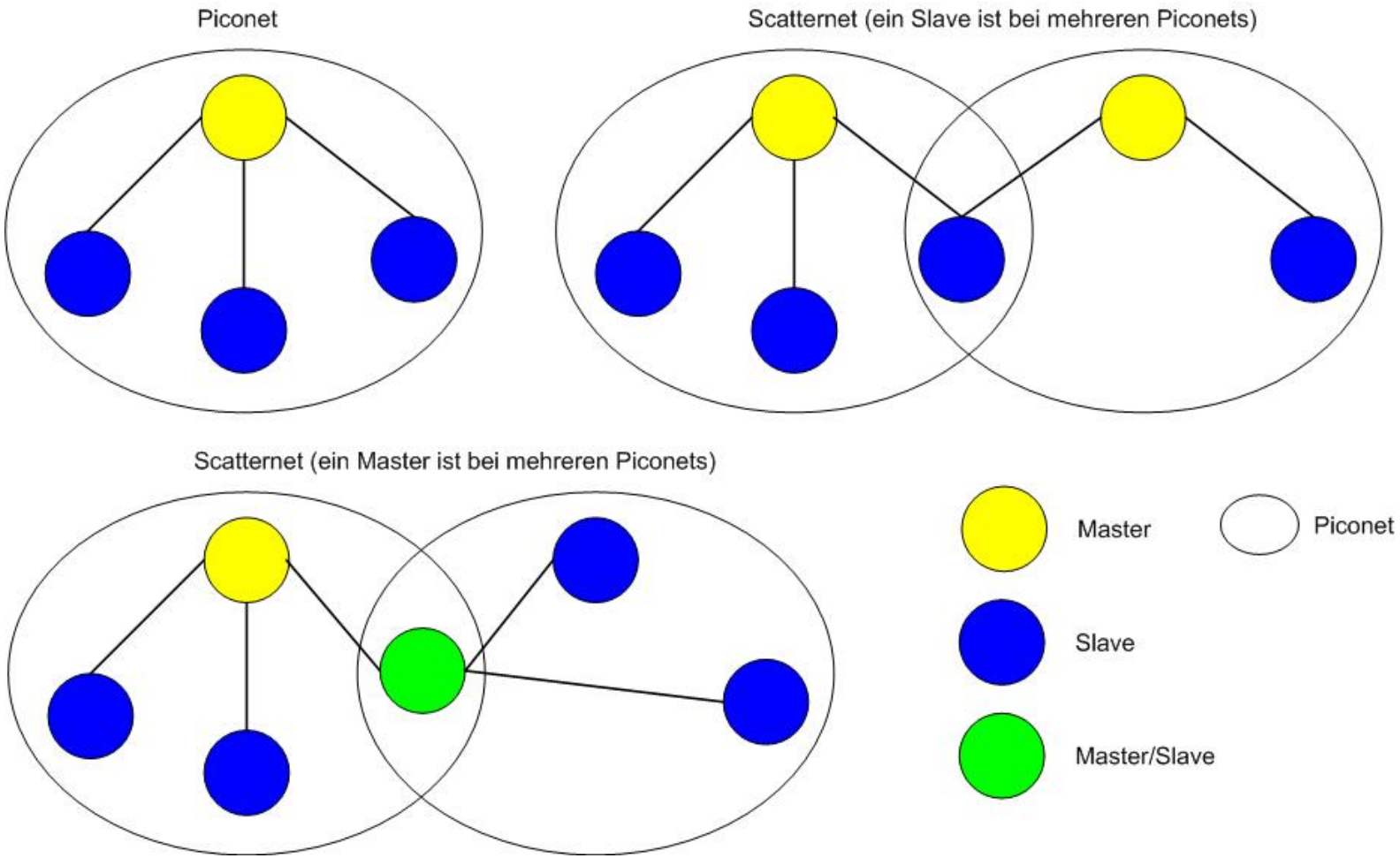


Bluetooth

Aufgaben der Protokollschichten



Bluetooth
Piconet und Scatternet



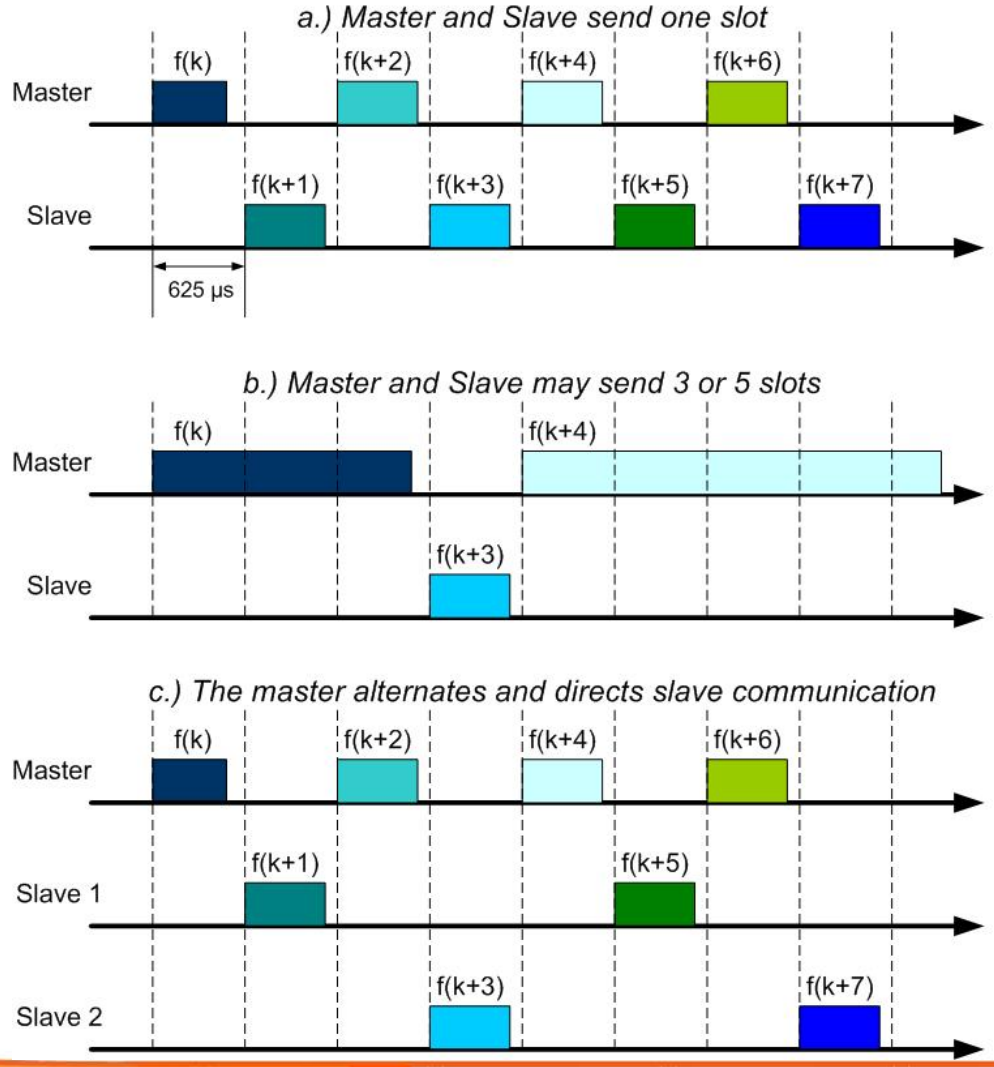
Bluetooth
Charakteristika

Eigenschaft	Wert
Reichweite	10 m (bis zu 100 m)
Ausgangsleistung (3 Klassen)	1: 1 mW – 100 mW 2: 0,25 mW – 2,5 mW (1 mW) 3: ? – 1 mW
Frequenzen	2400 – 2483,5 MHz
Datenrate	brutto 1 MBit/s, netto 723 kBit/s

- Identisch zu WLAN Aufteilung des ISM-Band in 79 Kanäle
  - in Frankreich, Spanien, Japan nur 23 verwendet
  - *Fast Frequency Hopping* mit 1600 Wechseln / Sekunde
    - 1 Slot dauert 1/1600 = 625 µs
  - Seit V1.2 *Adaptive Frequency Hopping*

Bluetooth

Master - Slave - Kommunikation



The frequencies for hopping are calculated using a common exchanged number and a standardized pseudo-random function with equal distribution to the 79 channels

Bluetooth
Links

- Mögliche Verbindungsarten sind
  - *SCO (Synchronous Connection-oriented Links)*
    - Symmetrische Point-to-Point-Verbindungen
    - Benutzen vordefinierte Slots
      - Fixe Bandbreite
      - Beschränkte Anzahl (3 pro Gerät) von SCO-Links
    - Verbindungen zwischen verschiedenen Masters und Slaves sind erlaubt
    - Pakete werden im Fehlerfall *nicht* neu gesendet
    - Verwendung hauptsächlich für Audio
  - eSCO (Extended SCO)
    - seit V1.2 für höhere Audioqualität
    - Bandbreitengarantie, aber flexibler
  - *Asynchronous Connection-less Links*
    - Benutzen die Slots, die nicht durch SCO-Links belegt sind
    - Zwischen Master und Slave existiert genau 1 ACL-Link
    - Fehlerhafte Pakete werden neu übertragen
    - Master kann ACL-Pakete auch als Broadcast an das gesamte Piconet übertragen

Bluetooth
Paketformat

- Jedes Paket besteht aus
  - *Access Code* (72 Bit = 9 Byte)
    - Eindeutige Bitsequenz markiert den Datenbeginn
    - Zieladresse des Pakets (bei bestimmtem Empfänger)
  - *Header* (54 Bit)
    - Definiert Pakettyp
    - Enthält Felder zur Flußkontrolle
    - Wird mit FEC-Rate (*Forward Error Correction*) 1/3 gesendet -> jedes Bit dreifach redundant
  - *Daten* (0 – 2744 Bit = 0 – 343 Byte)
    - Nutzlast, abhängig vom Pakettyp
    - Pakettypen sind in der Tabelle auf der folgenden Folie aufgelistet

Bluetooth
Pakettypen

Link	Typ	Nutzdaten [Bytes]	Slots	Datenheader [Bytes]	FEC	CRC	kBit/s
ACL	DM1	0-17	1	1	2/3	ja	109
ACL	DH1	0-27	1	1	-	ja	173
ACL	DM3	0-121	3	2	2/3	ja	258
ACL	DH3	0-183	3	2	-	ja	390
ACL	DM5	0-224	5	2	2/3	ja	287
ACL	DH5	0-339	5	2	-	ja	434
ACL	AUX1	0-29	1	1	-	nein	186
SCO	HV1	10 Audio	1	-	2/3	nein	64
SCO	HV2	20 Audio	1	-	1/3	nein	64
SCO	HV3	30 Audio	1	-	-	nein	64
SCO	DV	10 Audio 0.9 Daten	1	1	2/3 für Daten	nur Daten	64 58 Data

DM: Data Medium Rate, *DH*: Data High Rate
HV: High Quality Voice, *DV*: Data Voice

Bluetooth
Pakettypen

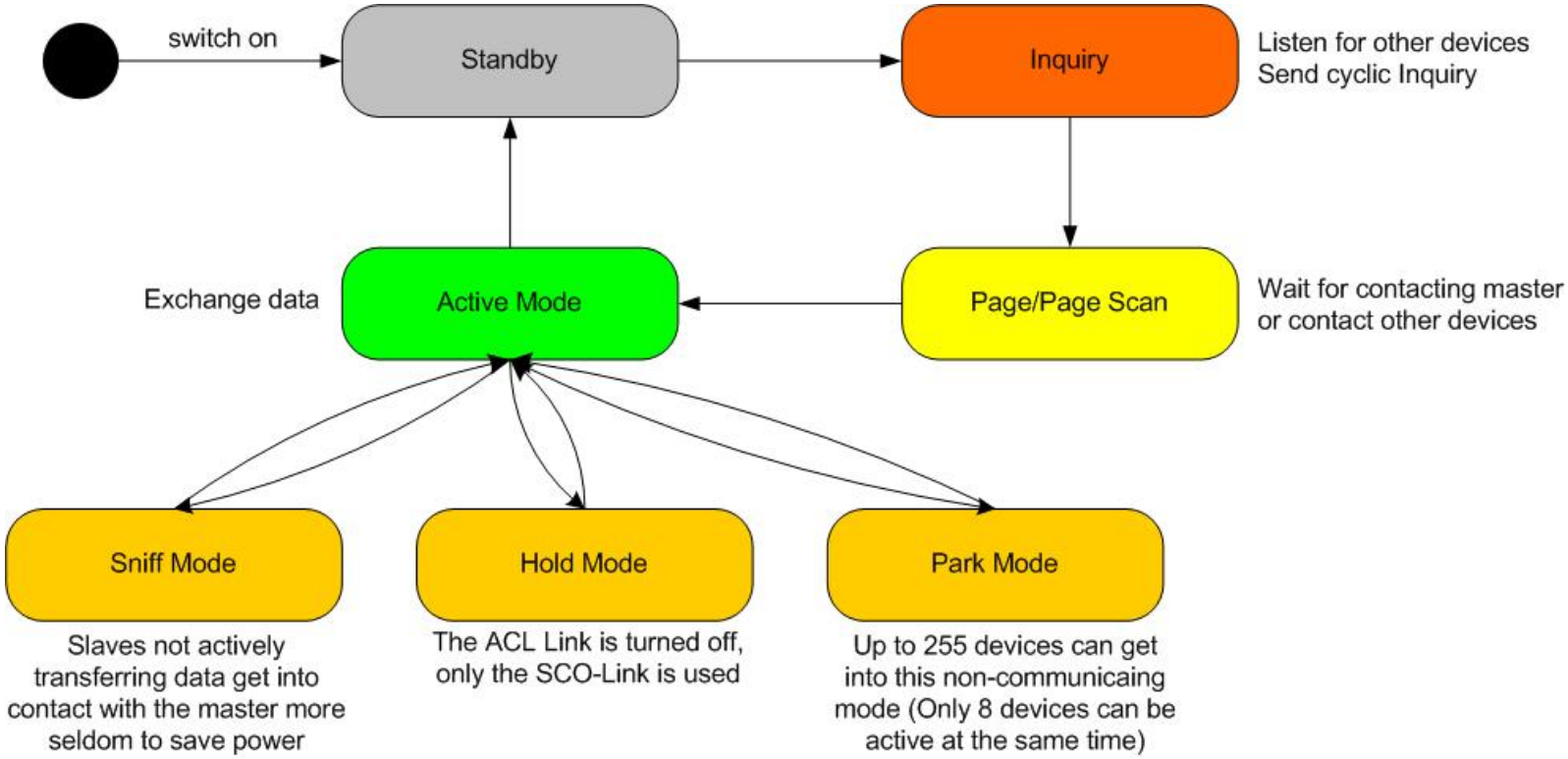
Link	Typ	Nutzdaten [Bytes]	Slots	Datenheader [Bytes]	FEC	CRC	kBit/s
eSCO	EV3	1-30	1	-	-	ja	96
eSCO	EV4	1-120	3	-	-	ja	192
eSCO	EV5	1-180	3	-	-	ja	288
eSCO	2-EV3	1-60	1	-	-	ja	192
eSCO	2-EV5	1-360	3	-	-	ja	576
eSCO	3-EV3	1-90	1	-	-	ja	288
eSCO	3-EV5	1-540	3	-	-	ja	864

EV: Extended Voice

Bluetooth
Geschwindigkeit

- Aus dem Paketaufbau resultieren folgende maximalen Datenraten (ohne EDR)
  - Datentransport mit maximal 723,2 kBit/s
    - Gegenrichtung hat in diesem Fall max. 57,6 kBit/s
    - Es ist keine zusätzliche Audioübertragung mehr möglich
  - Bei gleicher Bandbreite in beide Richtungen stehen maximal 433,9 kBit/s zur Verfügung
    - Es ist dann auch hier keine zusätzliche Audioübertragung mehr möglich
  - Eine bidirektionale Audioübertragung läuft mit 64 kBit/s
    - HV1-3 unterscheiden sich durch ihre fixe Slotbelegung
      - HV1: jeder 2. Slot, HV2: jeder 4. Slot, HV3: jeder 6.Slot
    - Übertragungsfehler wirken sich bei geringerer FEC-Rate stärker aus; hohe FEC-Rate benötigt aber mehr Slots

Bluetooth
Betriebsmodi



Bluetooth
LMP (Link Management Protocol)

- Keine *echte* Protokollschicht, da die darunterliegende Schicht *Baseband* nicht vollständig überdeckt wird
  - Obere Schichten (L2CAP) können auf Baseband zugreifen, ohne LMP zu verwenden
- Pakete über ACL-Links mit eigenem Eintrag im Header
  - Diese werden direkt in der LMP-Schicht des Empfängers ausgefiltert und verarbeitet
- LMP bietet folgende Funktionalität
  - Authentifikation und Verschlüsselung
  - Abgleich der lokalen Uhren
    - mittels Berechnung eines lokalen Offsets
  - Tausch der Master/Slave-Rollen, initiiert vom Master
  - Ändern der Verbindungszustände (Active, Sniff, Hold, Park Mode)
  - Ändern der Sendeleistung
    - Ein Gerät kann seinen Kommunikationspartner auffordern, die Sendeleistung zu erhöhen oder zu drosseln
  - Einstellen von Dienstgüteparametern (QoS)
    - über Pakettypen und Slot-zuordnungen
  - Einrichten von SCO-Links

Bluetooth
L2CAP – Funktionalität (1/2)

- Bereitstellung mehrerer logischer Kanäle pro ACL-Link
  - Verbindungsorientierte Kanäle
    - zuverlässige bidirektionale Datenverbindung
  - Verbindungslose Kanäle
    - Multicast-Möglichkeit über Benutzergruppen
- *PSM (Protocol and Service Multiplexer)*
  - Zur Identifikation von Diensten, wobei bestimmte Nummern vorbelegt sind **`(0x0001:SDP, 0x0003:RFCOMM, 0x0005:TCS-BIN)`**
  - die Werte **`0x1001-0xFFFF`** können frei vergeben werden
- Zerlegen von großen Datenpaketen beim Transport
  - Versand und Empfang von bis zu 64 KB großen Paketen
  - Es wird ein Paket fertig versendet, erst dann das nächste

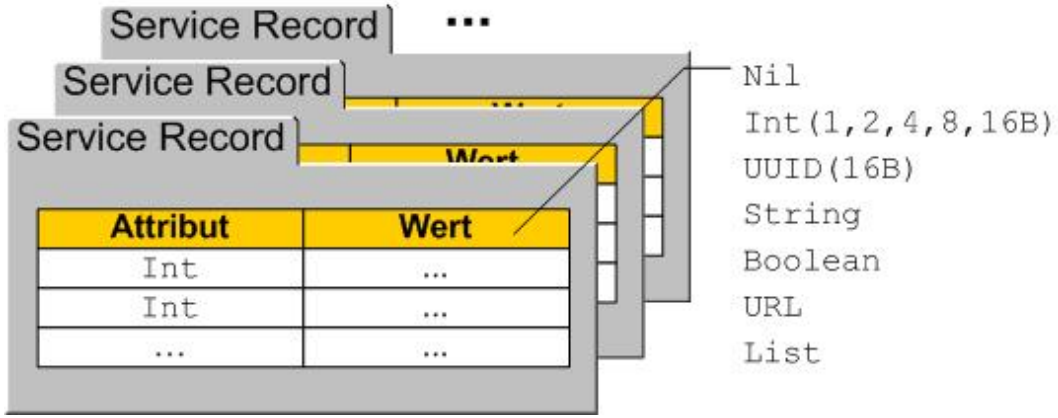
Bluetooth
L2CAP – Funktionalität (2/2)

- Zusätzliche Einstellungen von Dienstgüteeigenschaften
  - Dienstgütetyp
    - *Best Effort*, *Garantie* (Implementierung optional) oder *keine Anforderung*
  - Token Rate, Token Bucket Size
    - Datenrate beim Senden (Kredit); kurzzeitig kann schneller gesendet werden, dann wird die Anwendung blockiert
  - Maximale Bandbreite
  - Latenzzeit
    - Maximale Zeit zwischen der Datenübergabe und dem Versand
  - Verzögerungsschwankung
    - Differenz zwischen maximaler und minimaler Übertragungsdauer
- Es müssen nicht alle Parameter gesetzt werden
  - Einzelne Parameter mit **`do not care`** belegen

Bluetooth
SDP (Service Discovery Protocol)

- Suchen von Diensten
  - Nach Dienstklasse (z.B. Drucker)
  - Nach Attributen (z.B. Drucken mit 600 DPI)
  - Abfrage einer Übersicht verfügbarer Dienste
- Dienste werden über einen SDP-Server zur Verfügung gestellt, über einen SDP-Client verwendet
- Erhalt von Informationen über Dienste
  - Das Protokoll für Zugriff/Verwendung der Dienste liegt außerhalb von SDP
- Noch nicht in SDP integriert
  - Keine Weitervermittlung von Diensten (nur eigenes Gerät)
  - Keine Zugriffskontrolle
  - Keine Rechnungserstellung für Dienstnutzer
  - Keine Information über die Verfügbarkeit von Diensten

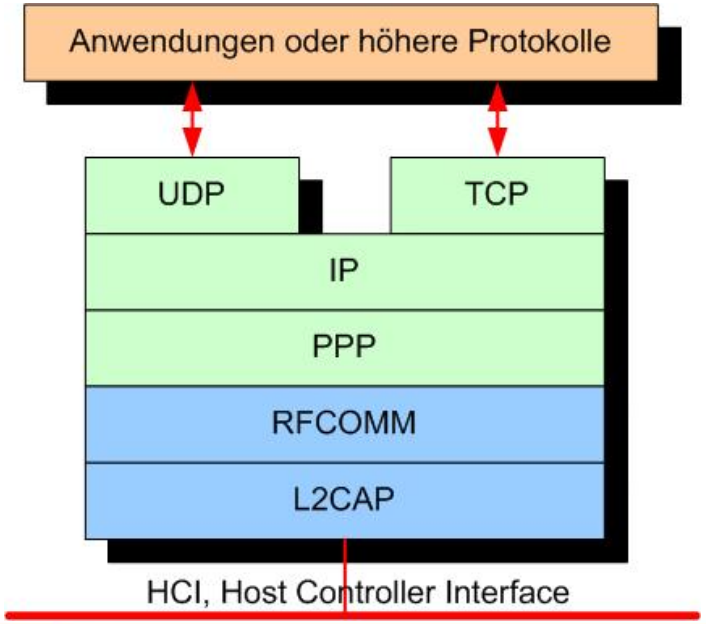
Bluetooth
SDP (Service Discovery Protocol)



Attribut ID	Wert
0x0000 (ServiceRecordHandle)	0x0A893BC1
0x0001 (ServiceClassIDList)	ID1=Headset ID2= Generic Audio
0x0004 (ProtocolDescriptionList)	Prot1=L2CAP, PSM=0x0003 Prot2=RFCOMM, CN=0x0002
0x0005 (BrowseGroupList)	ID1=PublicBrowseRoot
0x0100 (ServiceName)	„Headset“
0x1001 (VolumeControl)	true

Bluetooth
RFCOMM

- Simultaner Betrieb von bis zu 60 virtuellen seriellen Schnittstellen
- Einfache Übernahme von Protokollen und Applikationen ohne direkten Bluetooth-Support
- OBEX-Protokoll aus IrDA wurde übernommen



Bluetooth
Interessante Profile

- Advanced Audio Distribution Profile (A2DP)
  - Generic Audio/Video Distribution Profile (GAVDP)
- Audio/Video Remote Control Profile (AVRCP)
- Video Conference Profile (VCP)
  - Video Distribution Profile (VDP)
- Hands-Free Profile (HFP)
- Headset Profile (HSP)
- Phone Book Access Profile (PBAP)
- SIM Access Profile (SAP)
- Human Interface Device Profile (HID)
- File Transfer Profile (FTP)
- Personal Area Network Profile (PAN)
- Synchronization Profile (SYNCH)
- Generic Object Exchange Profile (GOEP)
- Serial Port Profile (SPP)
- Object Push Profile (OPP)

Protokolle zur spontanen Vernetzung

- Bisher behandelte Netzwerke behandeln OSI-Schichten 1 und 2
- Mobilität betrifft aber auch höhere Schichten
  - Vermittlungsschicht
    - Mobilität im Internet
      - DHCP
      - Mobile IP
    - Routing in Ad-Hoc Netzwerken
  - Transportschicht
    - Transportprotokolle für den mobilen Einsatz
      - Snoop Protocol
  - Anwendungsnahe Schichten
    - Dienstvermittlung in mobilen Umgebungen
      - JINI

Mobilität bei TCP/IP
DHCP

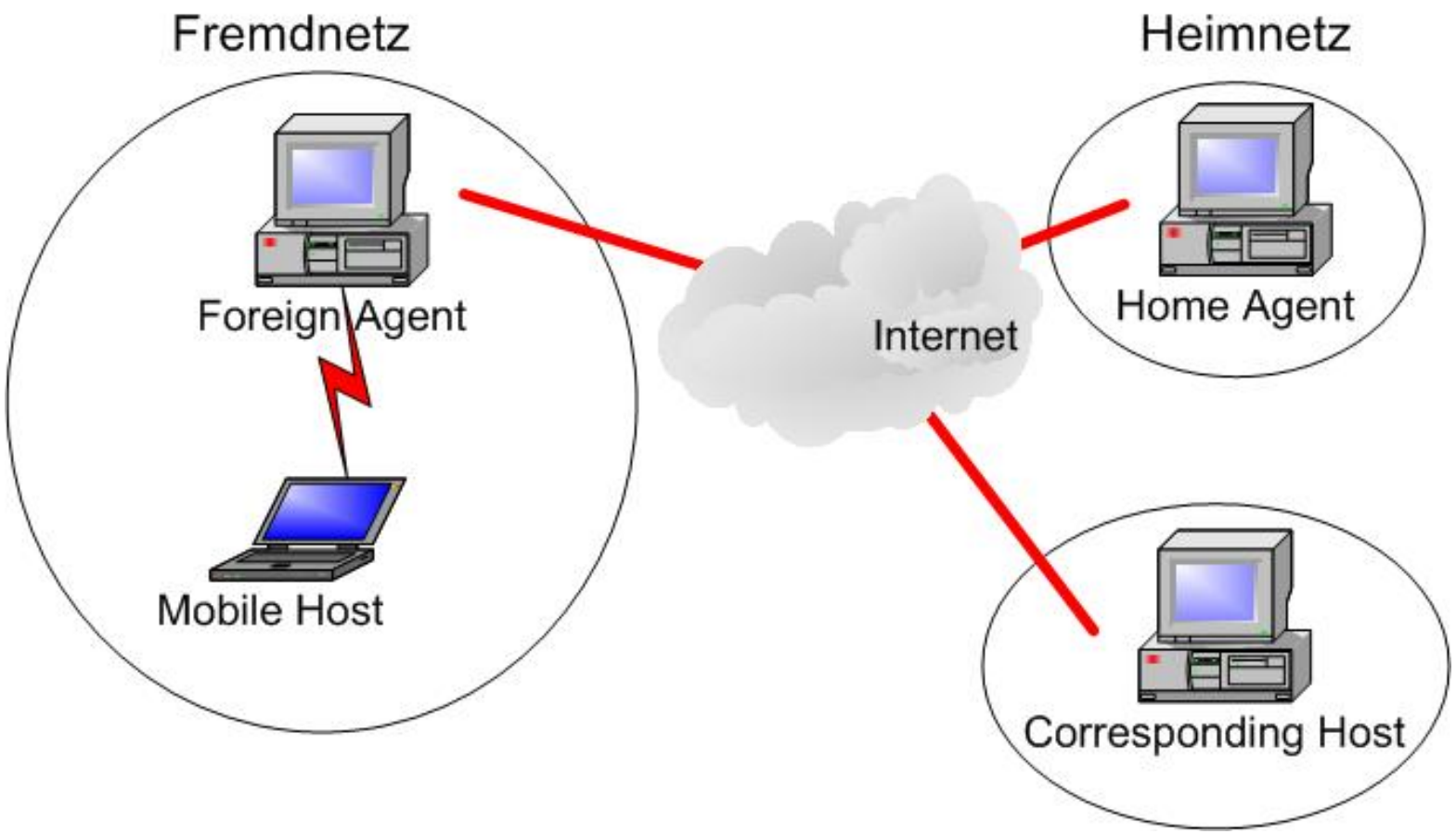
- Sicherheitsprobleme bei DHCP
  - Ungültiger Client kann sich Adresse holen
  - Ungültiger Host kann einen Client manipulieren und so dessen Verkehr abhören
  - Derzeitige Lösung mit MAC-Adressen nicht vertrauenswürdig
    - Sichere Authentifikation zwischen Client und Server ist notwendig
- Mobilitätsproblem
  - DHCP ist geeignet, an verschiedenen Stellen Zugriff auf das Internet zu erhalten
  - Rechner können keine Dienste anbieten, da sich ihre Adresse ändern kann
    - Ein Dienstnutzer könnte den Rechner nicht wiederfinden

Mobilität bei TCP/IP
Mobile IP: Rechner

- Der Rechner erhält eine IP-Adresse, die auch in anderen Netzen erhalten bleibt
- Unterscheidung verschiedener Rechnertypen
  - *Mobile Host* bewegt sich zwischen verschiedenen Subnetzen und hat eine fixe IP-Adresse
  - *Corresponding Host* ist der Rechner, der Kontakt zum mobilen Rechner aufnehmen will
  - *Home Agent* ist ein Stellvertreter im Heimnetz für den mobilen Rechner, wenn dieser sich nicht im Heimnetz befindet
  - *Foreign Agent* befindet sich im Fremdnetz, in dem sich der mobile Rechner bewegt und leitet eingehende Pakete an den mobilen Rechner weiter

Mobilität bei TCP/IP

Mobile IP: Rechner



Mobilität bei TCP/IP
Mobile IP: Adressen

- Pro mobilem Rechner existieren zwei Adressen
  - Unter der *Heimadresse* ist der mobile Rechner permanent erreichbar
    - Sie hat denselben Adresspräfix (Netzadresse und Subnetzadresse) wie der *Home Agent*
  - Die *Care-Of-Address* wird im Fremdnetz verwendet
    - *Foreign-Agent-Care-Of-Address*
      - Der Fremdagent übernimmt die Paketweiterleitung; mehrere Fremdrechner können (nicht zur selben Zeit) dieselbe Adresse haben
    - *Collocated-Care-Of-Address*
      - Adresse des mobilen Rechners im Fremdnetz. Der Heimagent kennt diese Adresse, es gibt hier keinen Fremdagenten. Jeder Fremdrechner hat eine eigene Adresse

Mobilität bei TCP/IP
Mobile IP: Agent Discovery

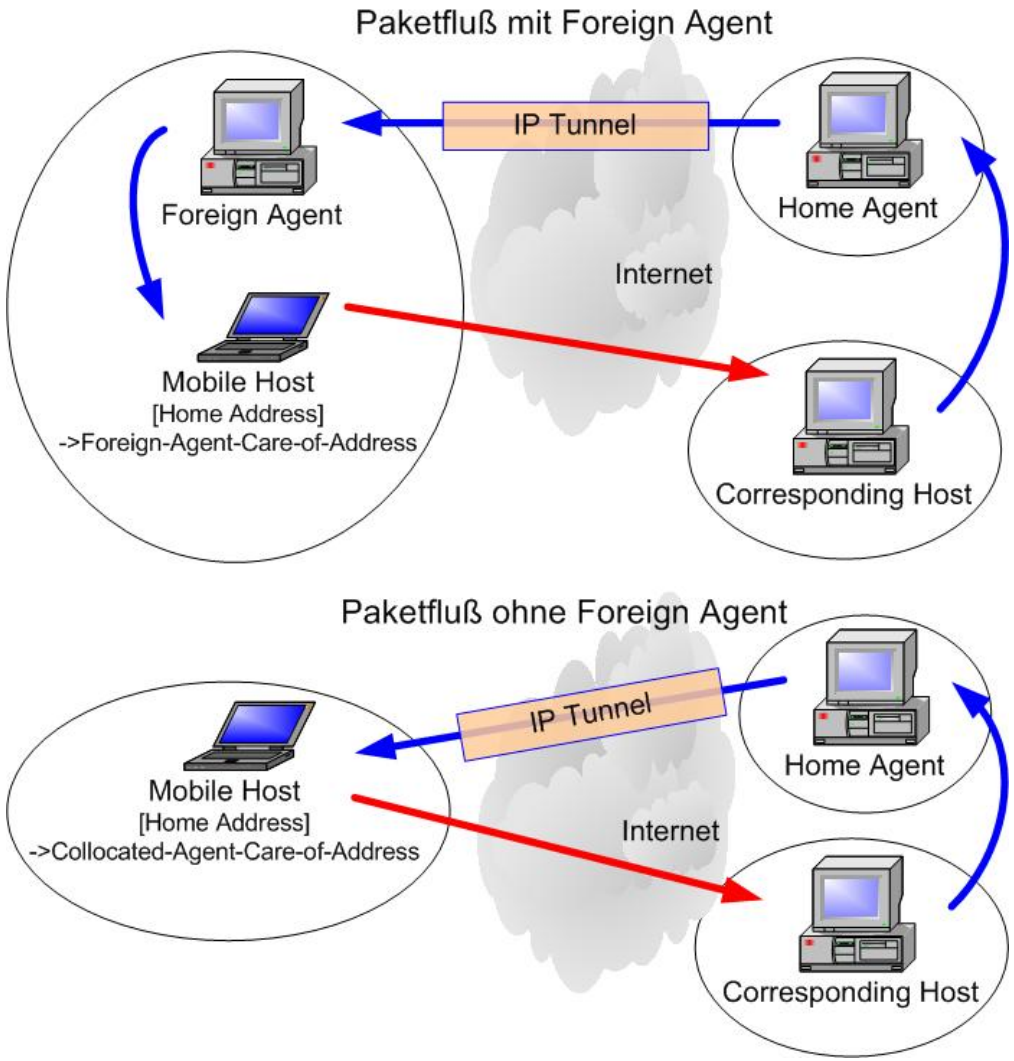
- Mittels *Agent Discovery* erfährt ein Rechner, in welchem Netz er sich befindet
  - *Agent Advertisement*: Die Agenten senden periodisch Broadcasts an ihr Subnetz. Zuhörende Rechner können so die Agenten im Subnetz finden
  - *Agent Solicitations*: Der mobile Rechner kann einen Broadcast im Subnetz verschicken, worauf alle Agenten ein *Agent Advertisement* durchführen
- Der Rechner empfängt kein Advertisement
  - Im Heimnetz nimmt er an, der *Home Agent* ist ausgefallen und er kontaktiert den Router zur Bestätigung
  - Im Fremdnetz versucht er über DHCP eine IP-Adresse zu bekommen und teilt diese dem *Home Agent* als *Collocated-Care-Of-Adresse* mit

Mobilität bei TCP/IP
Mobile IP: Registrierung

- Der mobile Rechner registriert seine *Care-Of-Adresse* beim Heimagenten
  - Der *Home Agent* besitzt eine Tabelle mit Einträgen
    - `Heimadresse | Care-Of-Adresse`
  - Zur gegenseitigen Authentifizierung besitzen der *Home Agent* und der mobile Rechner gemeinsame geheime Schlüssel
    - Ausgetauschte Nachrichten besitzen einen MAC (*Message Authentication Code*)
- Beim Austritt aus dem Fremdnetz deregistriert sich der mobile Rechner beim *Home Agent*
  - Oft werden Rechner ohne Deregistrierung ausgeschaltet
    - Registrierungen werden oft zeitlich beschränkt vorgenommen und müssen in Intervallen erneuert werden

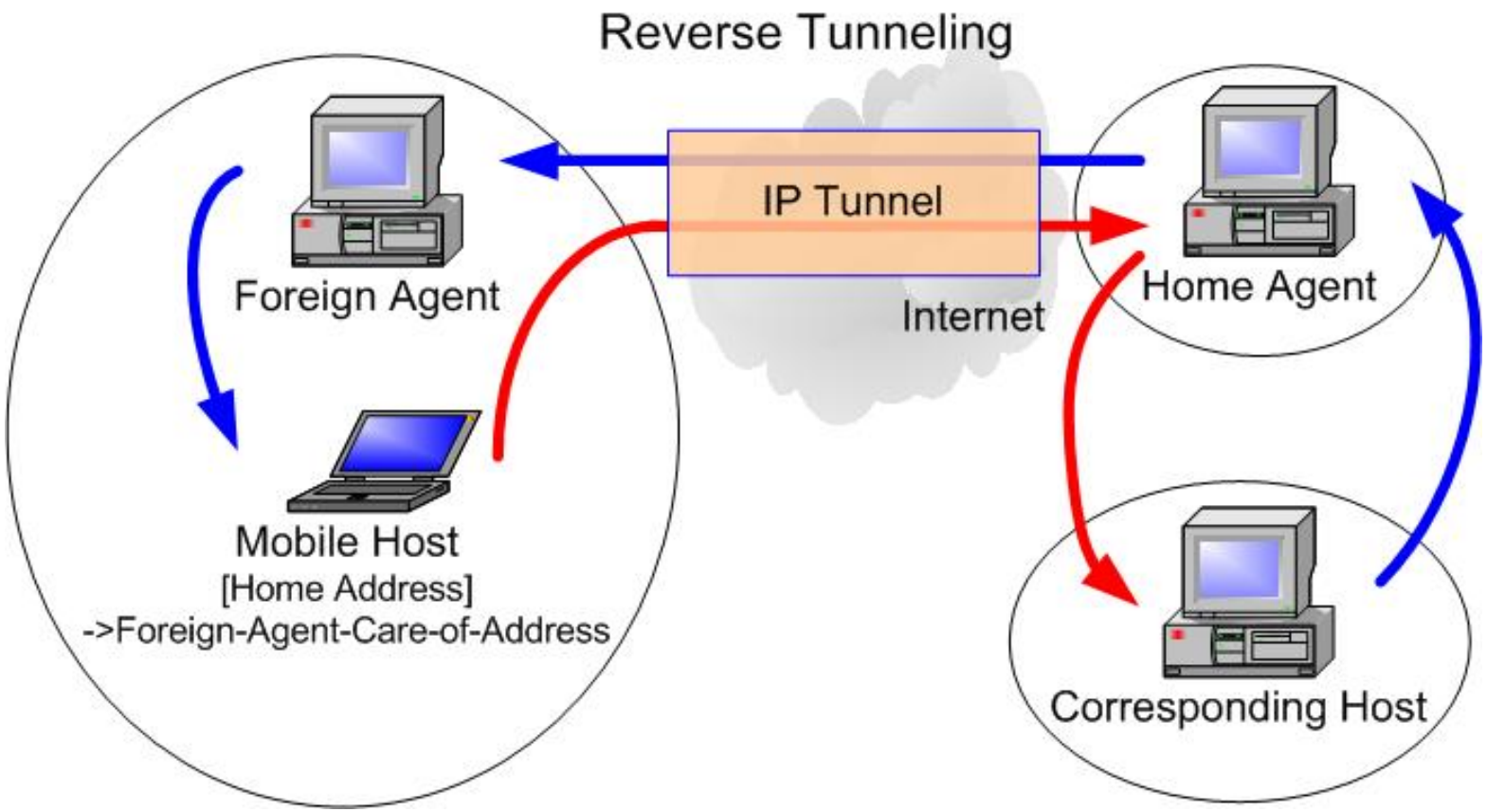
Mobilität bei TCP/IP

Mobile IP: Paketfluß



Mobilität bei TCP/IP

Mobile IP: Reverse Tunneling

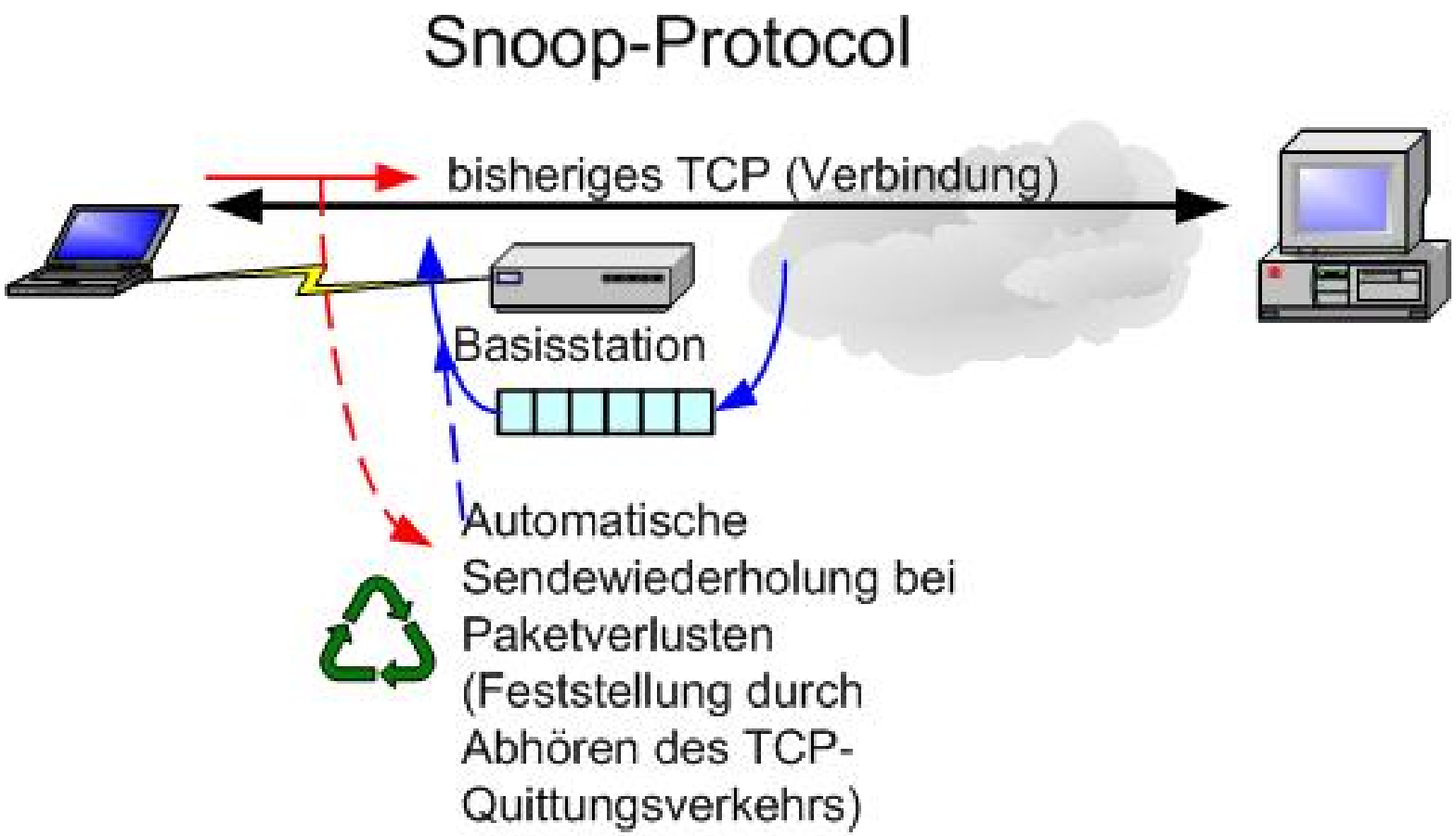


Mobilität bei TCP/IP
Mobile IP: Zukünftiges

- Mobile IP in der aktuellen Version *IPv4*
  - Erhebliche Anzahl an zusätzlichen Rechnern
    - In jedem Heimnetz ein *Home Agent*
    - U.U. in Fremdnetzen *Foreign Agents*
    - Pakete werden mitunter über lange Umwege transportiert
- Mobile IP in der Version *IPv6*
  - Mobile IP wurde direkt eingearbeitet
  - Es werden nur noch *Collocated-Care-Of Adressen* verwendet, was den *Foreign Agent* überflüssig macht
  - Die Funktionalität des Heimagenten wird direkt in die Router des Heimnetzes integriert
  - Mobile Rechner informieren die involvierten Router, was das aufwendige *Routing* über den *Home Agent* überflüssig macht

Mobilität auf Transportebene

„Abschnüffeln“ der Leitung



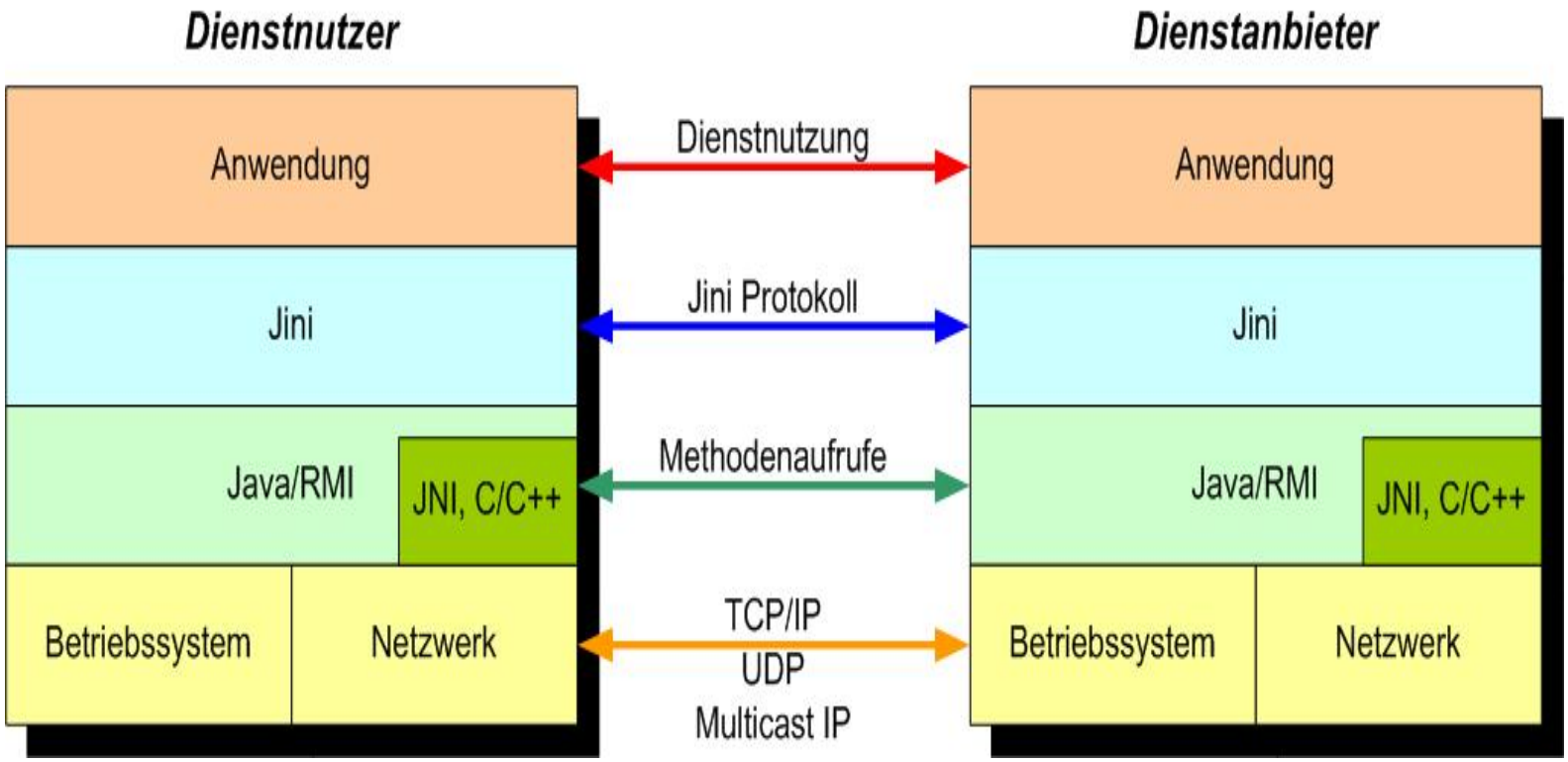
Mobilität auf Transportebene
„Abschnüffeln“ der Leitung

- *Snoop Agent* („Schnüffler“) hört den Quittungsverkehr ab
  - Hört er positive Quittungen, löscht er das betreffende Paket aus dem Puffer
  - Bei negativer Quittung wird die Quittung gelöscht und das Paket erneut gesendet
- Vorteile
  - Kommunikationsendpunkte nehmen keine Veränderung im TCP-Verhalten wahr
  - *End-to-End Semantik* bleibt erhalten
  - Ein fehlendes Paket in der Basisstation stört den Verkehr nicht
  - Der negative Quittungsverkehr muß nicht bis zum stationären Rechner durchgereicht werden
  - Wechsel zwischen Basisstationen ist unproblematisch (die neue Basisstation muß das Snoop-Protokoll nicht können)
- Nachteile
  - Bei einer verschlüsselten Übertragung kann die Sequenznummer eines Pakets nicht mehr gelesen werden (mitverschlüsselt). Der *Snoop Agent* bräuchte hier die Kommunikationsschlüssel

Dienstvermittlung
Jini

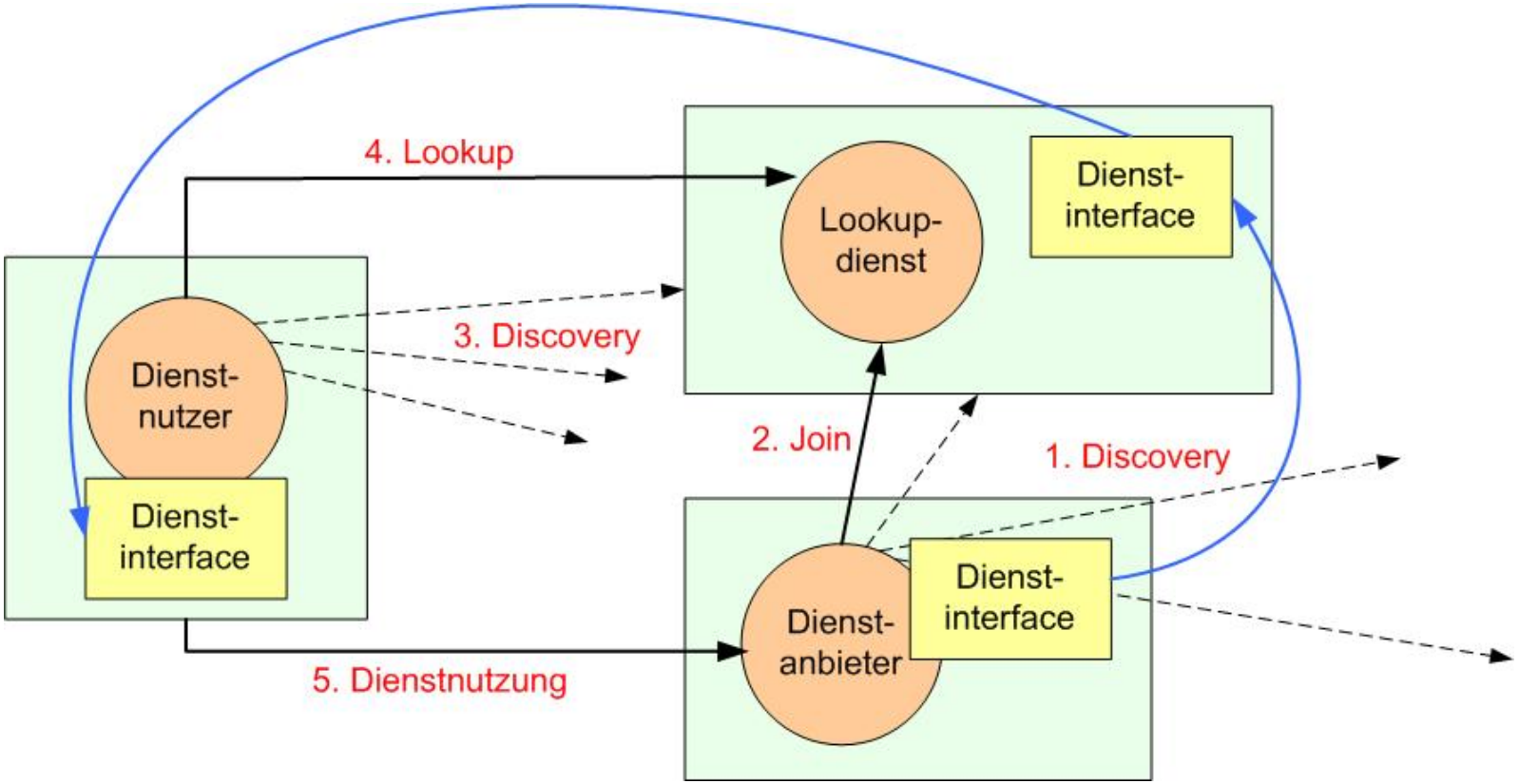
- Jini (*Java Intelligent Network Infrastructure*)
  - basierend auf Java, „natürlich“ geplante Erweiterung von Java: spontane Vernetzung von Konsumgütern
  - seit 1999 verfügbar
- Durch Java stark systemunabhängig und mächtig
  - Möglicher Einsatz von TCP, UDP und Multicast IP
  - *Object Serialization* erlaubt das Versenden komplexer Objekte
  - *RMI* erlaubt den Aufruf entfernten Codes
  - Jini steht nur auf Plattformen mit Java zur Verfügung
  - Java Microedition genügt für die aktuelle Implementierung von Jini nicht

Dienstvermittlung
Jini: Architektur



Dienstvermittlung

Jini: Registrierung und Nutzung



Dienstvermittlung
Jini: Discovery

- Lookup-Dienste werden thematisch in Gruppen eingeteilt
- Die Lookup-Dienste können auf verschiedene Arten gesucht werden
  - *Multicast Request Protocol*: In periodischen Abständen wird ein Multicast an eine bestimmte Gruppenadresse gesendet
  - *Multicast Announcement Protocol*: Ein Lookup-Dienst sendet periodisch Multicast-Pakete
  - *Unicast Discovery*: In großen Netzen kann die Rechneradresse eines Rechners mit einem bestimmten Lookup-Dienst angegeben werden

Dienstvermittlung

Jini: Join und Dienstnutzung

- Ein Join registriert einen Dienst eines Dienstanbieters. Hierfür muß angegeben werden
  - Eine weltweit eindeutige Dienstkennung (128 Bit)
  - Das Dienst-interface als Klasse(n)
  - Attribute, die den Dienst näher beschreiben
- Lookup und Dienstnutzung
  - Wird ein Dienst gefunden, kann das Dienst-interface über RMI verwendet werden
  - Das Dienst-interface implementiert hier eine Schnittstelle wie ein Gerätetreiber
- Aus Treibermangel findet Jini derzeit keine allgemeine Verbreitung