Technische Hochschule Ingolstadt
Fakultät Informatik

Kapitel 5: Mobilfunk-Netze - Grundlagen und GSM

CASE_SMN WS 2023

Vorlesung „Sicherheit moderner Netze“

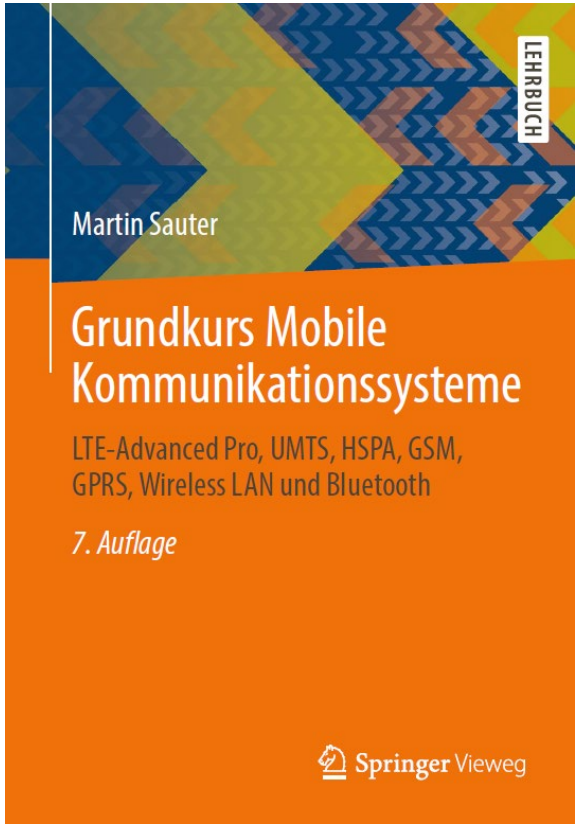
29.11.2023

Literatur

Mobilfunk-Systeme:

- **Sauter, Martin:**
  Grundkurs Mobile Kommunikationssysteme : LTE-Advanced, UMTS, HSPA, GSM, GPRS, Wireless LAN und Bluetooth
  von Martin Sauter
  7., überarb. Aufl. 2018
  Online-Ressource der thi Bibliothek !!!!

Guter Überblick über alle Funksysteme, aktuell



Mobilfunk – Was ist hier anders?

Einige wesentliche Unterschiede Mobilfunknetz ⇔ Festnetz

- **Teilnehmerauthentifizierung**
  - Festnetz: Trust by wire
  - Mobilfunk: Eigenes Verfahren / sicheres Protokoll
- **Verwalten und finden des mobilen Teilnehmers (Mobilitätsverwaltung)**
  - Festnetz: eigene Teilnehmer-VSt; durch Rufnummer definiert (Ortsbezogene Rufnummer)
  - Mobilfunk: Heimat-Datenbank (HLR), Besuchs-Datenbank (VLR)
- **Mobilität des Teilnehmers:**
  - Teilnehmer können während des Gesprächs die Funkzelle wechseln.
  - Gespräch wird weitergereicht (Handover)
- **Nutzung von Fremdnetzen (Roaming)**

Mobilfunk – Was ist hier anders?

Einige wesentliche Unterschiede Mobilfunknetz ⇔ Festnetz

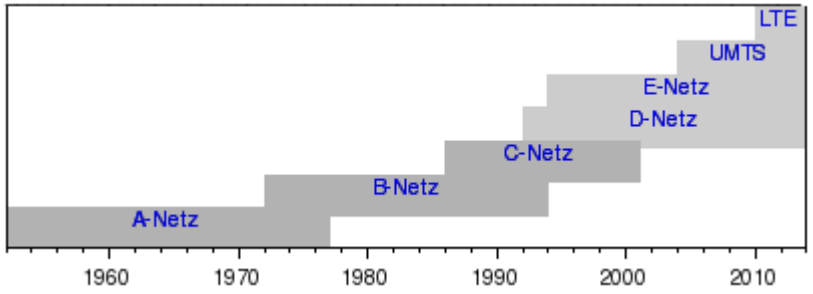
- **Kanalzugriffsverfahren**
  - Nutzung derselben Frequenzen mit vielen anderen Teilnehmern in derselben Funkzelle
  - „Shared medium“

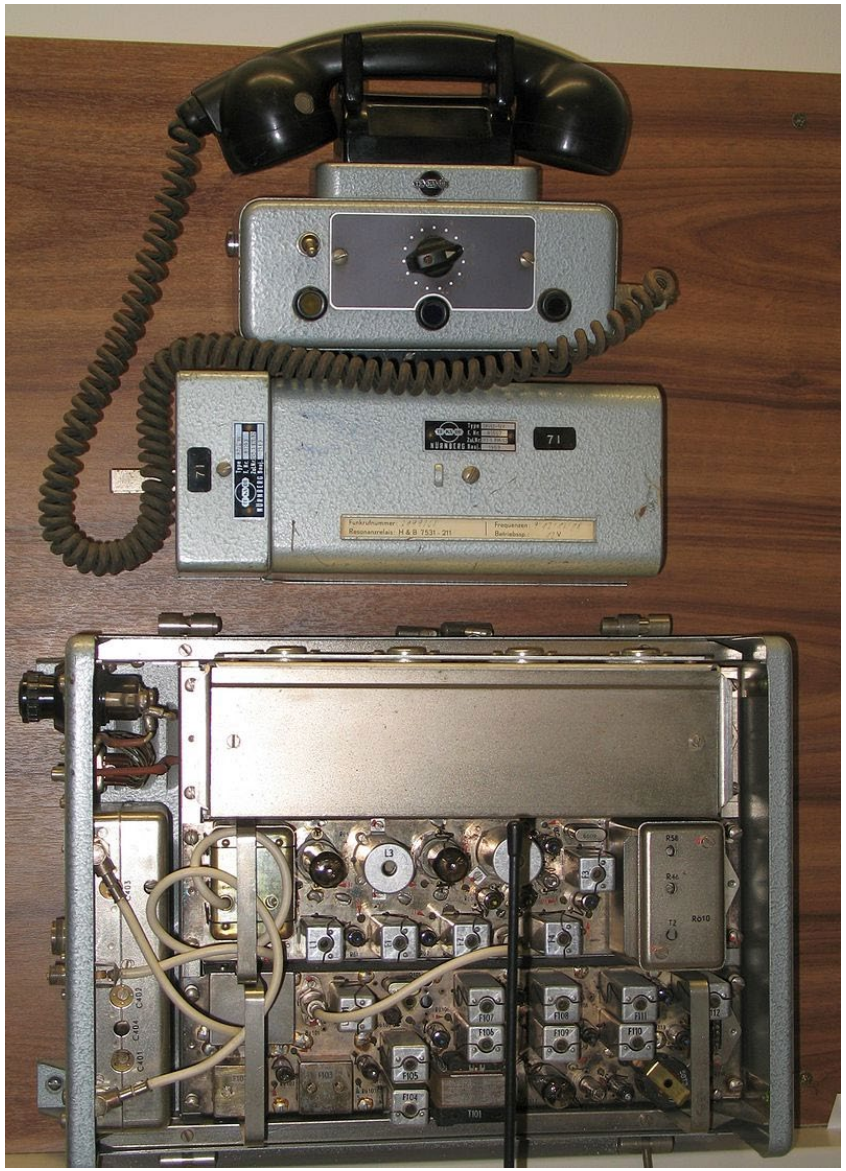
- **Effiziente Ressourcenausnutzung**
  Frequenz-Spektrum ist die knappe Ressource im Netz, daher müssen die Nutzdaten (Sprache) sehr stark komprimiert werden.

- **Energie**
  Mobiltelefone haben nur eine begrenzte Akkukapazität. Daher müssen Dauer und Form der Kommunikation sehr energiesparsam designed werden, z.B.:
  - Einfachere Codierung für Uplink
  - Stand-by mit wenig Statusmeldungen
    (aber der Standort muss für Anrufe immer bekannt sein!)

Historie der Mobilfunknetze in Deutschland

- **A-Netz:**
  - Analoger Mobilfunk für Telefonie 1958 – 1977:
    „öffentlicher beweglicher Landfunkdienst“ (öbL) der Deutschen Bundespost
  - Nationaler Standard
  - Handvermittlung, Gespräch nur in einer Funkzelle möglich
  - Frequenzbereich: 156 -174 MHz, Sendeleistung 10 W, Frequenzmodulation
  - Endausbau: 136 Funkverkehrsbereiche mit zusammen über
    317 Funkkanälen
  - 10.500 Teilnehmer (Kapazitätsgrenze)
  - Mobil => Schuhkarton-Größe => „Auto-Telefon“
  - Abgelöst ab 1972 durch B-Netz





A-Netz-Funktelefon Typ B72 (Hersteller: TeKaDe Nürnberg, 1963).

Oben das Bedienteil mit Hörer; im Kofferraum war das noch mit Elektronenröhren bestückte Sende-/Empfangsteil (unten) untergebracht.

Quelle: Wikipedia

Historie der Mobilfunknetze in Deutschland

- **B-Netz:**
  - Analoger Mobilfunk für Telefonie 1972 – 1994, unverschlüsselt
  - Nationaler Standard, kompatibel nur mit A, NL, Lux
  - Selbstwählvermittlung, Gespräche vom und zum Mobilteilnehmer
  - Gespräch nur in einer Funkzelle möglich
  - Wahl zum Standort des Teilnehmers => Vorwahl des „Funkverkehrsbereiches“ (158 Zonen in Deutschland)
  - Frequenzbereich: 148 – 163 MHz, Sendeleistung 10 W, Frequenzmodulation
  - 75 Sprechkanäle
  - 850 Funkkanäle
    (mit Wiederverwendung des Kanals bei genügen großer Entfernung)
  - Endausbau: 136 Funkverkehrsbereiche
  - 27.000 Teilnehmer (1986)

Historie der Mobilfunknetze in Deutschland

- **C-Netz:**
  - Analoges, zellulares Mobilfunknetz für Telefonie 1985 – 2000
  - Betreiber DeTeMobil, nationaler Standard, kein Roaming möglich
  - Großzellen (Radius etwa 15–20 km) und Kleinzellen (2–3 km) in den Ballungsräumen
  - Frequenzbereich: 450 – 465 MHz, Sendeleistung bis 15 W im Auto, Phasenmodulation
  - 287 Funkkanäle ab 1991
  - 850.000 Teilnehmer
  - Abgelöst ab 1992 durch GSM (D-Netz)
- **C-Netz-Besonderheiten:**
  - Teilnehmer wird im Netz gefunden, nur Netzvorwahl (0161)
  - unterbrechungsfreier Wechsel von einer Funkstation zur nächsten (Handover)
  - Teilnehmeridentität mit Karte (Magnetstreifen)
- **Mehr Info zur Geschichte: oebl.de**

C-Netz-Funktelefon

Mobiltelefon C3 portable von Siemens, Bauzeit 1989 – 1993

Quelle: Stuttgarter Zeitung online, „25 Jahre Mobiltelefone, Vom Knochen zum schlanken Handy“

C-Netz-Funktelefon

C-Netz-Funktelefon

Siemens C3:

- Bauzeit: 1989-1993
- Kanäle: 1989: 237 / 1991: 287
- max. Sendeleistung: 16 Watt / mobil 2,5 Watt

Abmessungen und Gewicht:

- 210mm breit x 170mm Hoch x 80mm tief / Gesamtgewicht: 2,5kg
- davon der Hörer 0,31kg / Tragerahmen 0,7kg / Akku 0,5kg / Funkteil 0,99kg

Historie der Mobilfunknetze in Deutschland

- **D-Netz:**
  - Erster Internationaler Standard (GSM), weltweites Roaming möglich!
  - Digitale Übertragung der Sprache / Daten
  - In Deutschland: 2 Betreiber im Wettbewerb:
    - DeTeMobil (D1) und
    - Mannesmann (D2 privat), später Vodafone D2
  - Start 1992
  - Frequenzbereich 900 MHz

- **E-Netz**
  - GSM-Standard
  - Frequenzbereich 1800 MHz
  - Start 1994 mit E-plus (Vebacom und Thyssen Telecom), dann KPN, seit 2015 Telefonica
  - 1997 E2-Netz mit Viag-Interkom, dann O2 (erst BT, jetzt Telefonica)

- **UMTS, LTE, LTE Advanced,…..**

Mobilfunk-Systeme
der 2. Generation

➔ GSM
Teil 1: Funknetz

Mobilfunk 2. Generation: GSM

- **GSM: Global System for Mobile Communications**
  - 1. Internationaler Standard für digitale Mobilfunknetze
  - Standardisierung durch ETSI,
    später Gründung von 3GPP:
    3rd Generation Partnership Project
  - Ziele:
    - Europaweite Mobilität
    - Kompatibel mit Festnetztelefonie
    - Anpassung an die Anforderungen moderner Mobilfunksysteme (vorherige Folien)

- **Generelle Struktur:**
  - Funknetz
  - „Luftschnittstelle“ (Übertragung auf der Funkstrecke, Air Interface)
  - Netzarchitektur

Ausbreitungseigenschaft der Funkwellen:

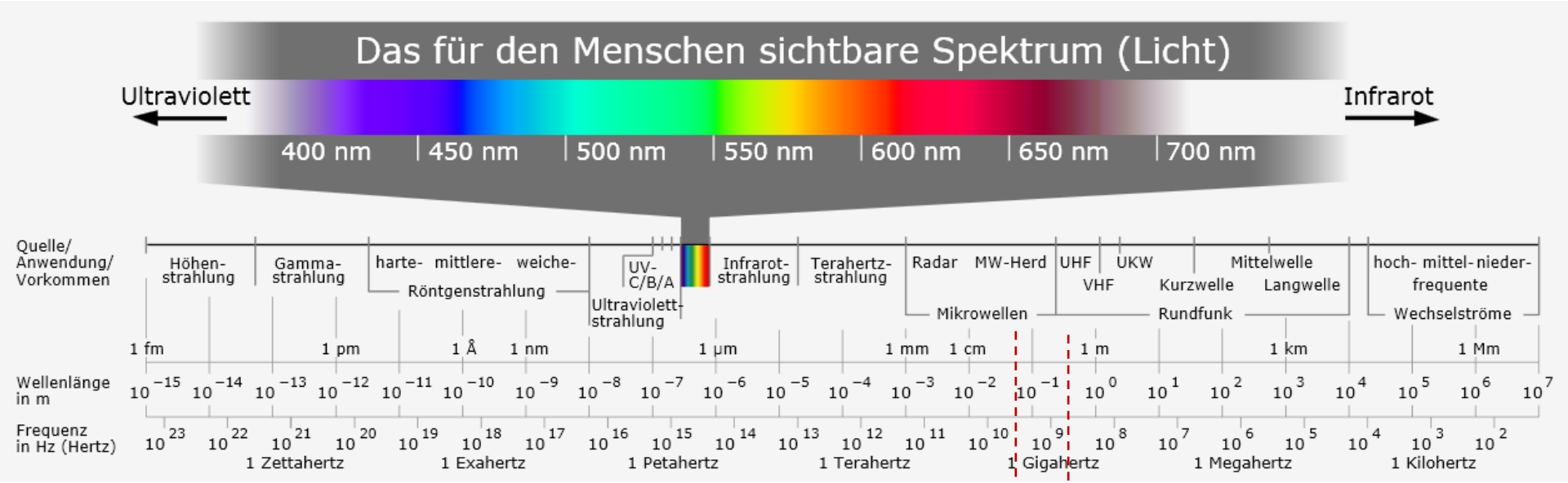
- **Dämpfung der Funkwellen im freien Raum:**
  „Freiraumdämpfung“,
  als Funktion der Frequenz bzw. Wellenlänge:
  - f = Frequenz, λ = Wellenlänge, c = Lichtgeschwindigkeit, r = Abstand
  - **Freiraumdämpfung F:**

$$F = \left(\frac{4\pi r}{\lambda}\right)^2$$

$$F = \left(\frac{4\pi r \cdot f}{c}\right)^2$$

- **Problem mit sehr hohen Frequenzen** (keine Rundstrahler-Antennen mehr sinnvoll)
- **Weitere Effekte, speziell bei höheren Frequenzen:**
  - Dämpfung in der Atmosphäre
  - Störung in der Wellenausbreitung (Hindernisse)
  - Reflexionen und Beugungen
  - Dämpfung durch Gebäude / Wände (=> „indoor-coverage“)
- **In Zukunft:** gerichtete Strahlung (Aktive Antennen), Mehrfache Antennen (MIMO)

Elektromagnetisches Spektrum



Frequenzen für Mobilfunk, WLAN
700 MHz … 5 GHz (in Zukunft auch höher), 5G betrachtet auch 26 -28 GHz

Wichtige Aspekte der Funksignale:

- Frequenz: Reichweite / Durchdringung
- Bandbreite eines Kanals (x MHz ⇔ n*x Mbit/s)
- Regulierung: Lizensiert (Mobilfunk) oder frei mit Rahmenbedingungen (WLAN)

Grafik von Horst Frank / Phrood / Anony - Horst Frank, Jailbird and Phrood, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=3726606

Ausbreitung der Radiowellen (Mobilfunk)

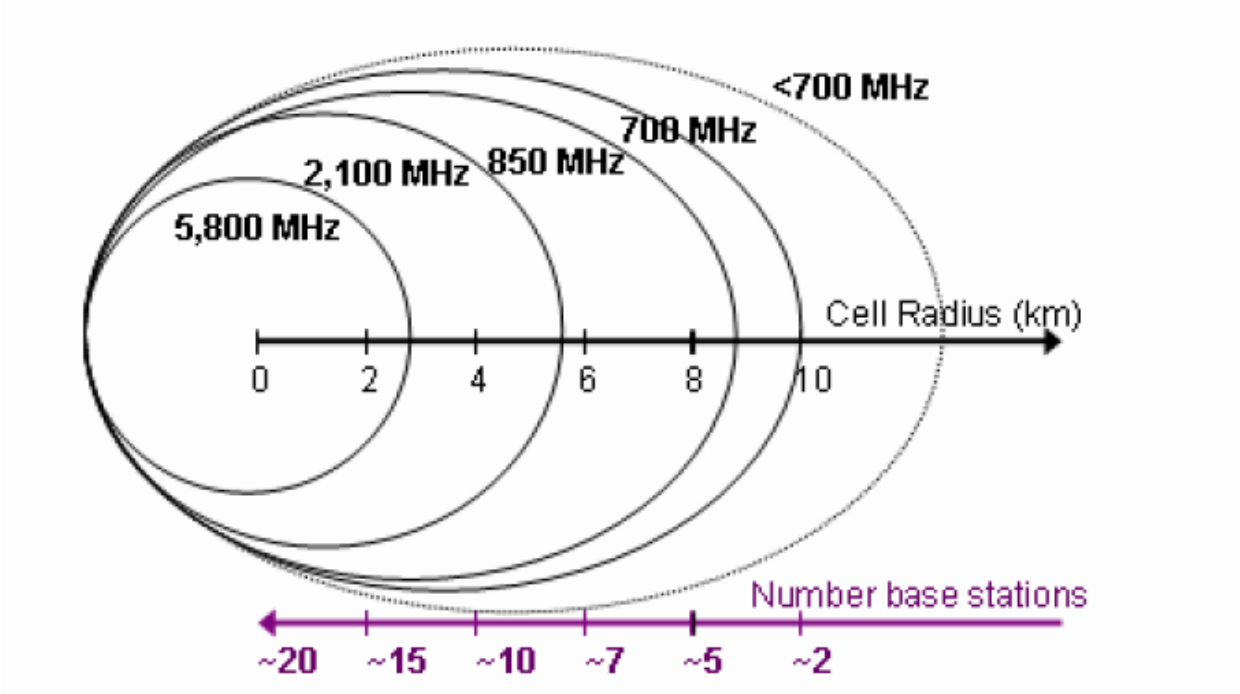


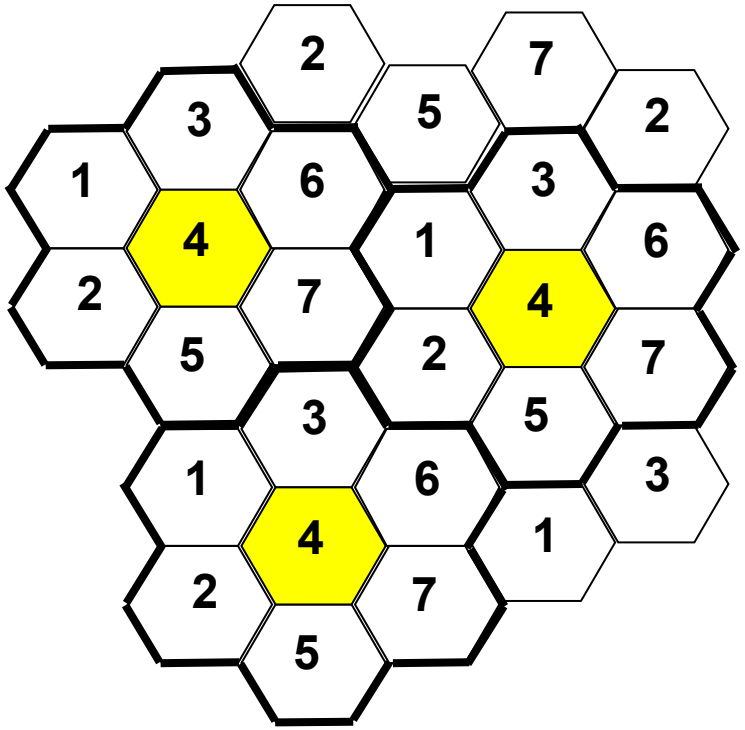
Figure 2. The propagation characteristics of spectrum

Source: BBC R&D.

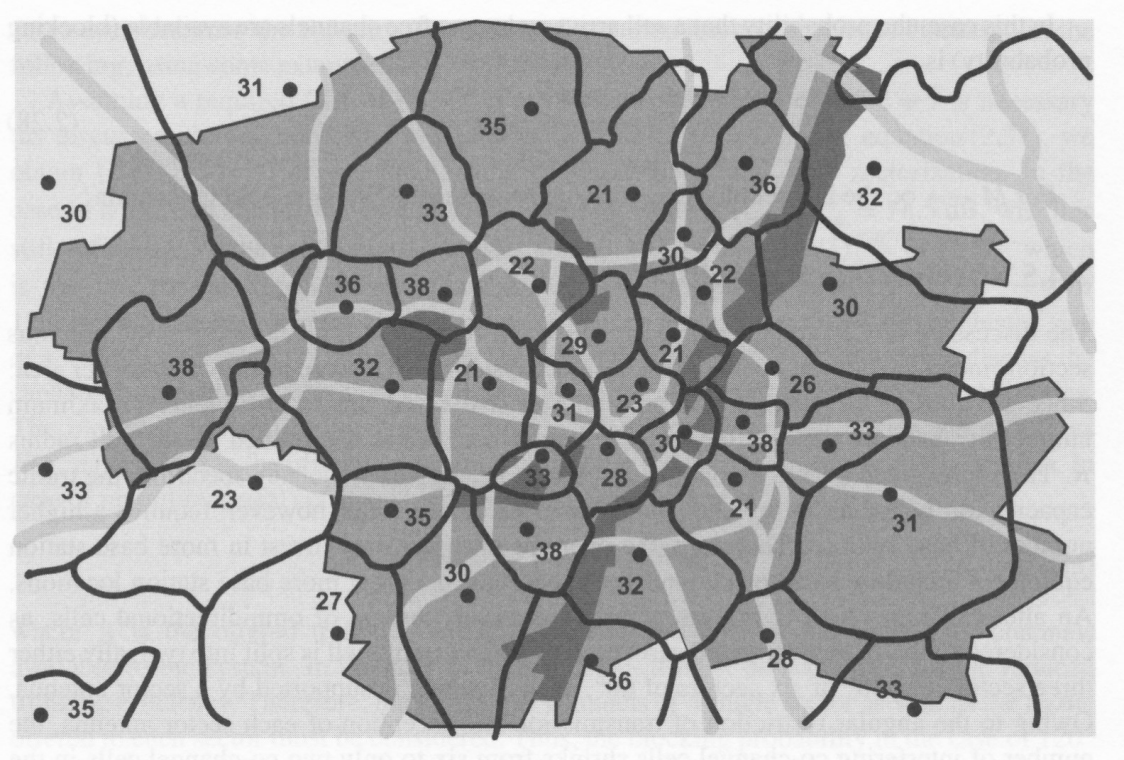
- Ausbreitungseigenschaft in Abhängigkeit von der Frequenz (bei gleicher Leistung)
- Anmerkung: Die Durchdringung von Gebäuden nimmt bei höheren Frequenzen stark ab („Indoor Coverage“)

Mobil-Funk-Netz

- **Randbedingungen:**
  - Begrenzte Reichweiten der Funkstrecke (Ausbreitung der Wellen begrenzt)
  - Begrenztes Spektrum für den Mobilfunkdienst
    (Funk-Spektrum ist eine stark begrenzte Ressource => Versteigerungen!!)
- **Lösung:**
  - Zellulares Netz
  - Einmalige Vergabe der verfügbaren Frequenzen in einem Cluster (1 – 7)
  - Nachbarzellen benutzen andere Frequenzen
  - Wiederholung der Frequenzen in den anderen Clustern
  - Hexagonale Zellenstruktur für Planung



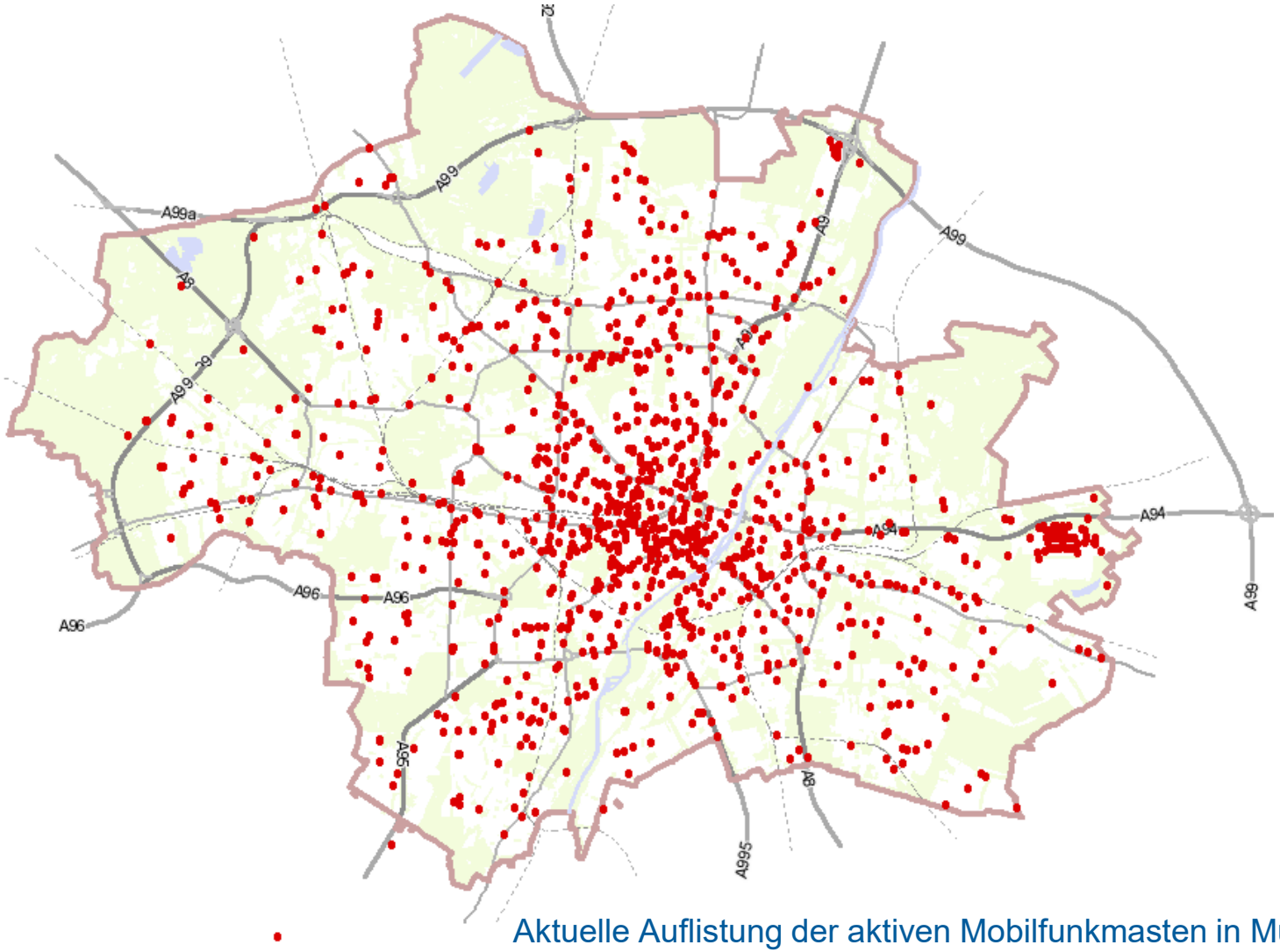
Mobilfunkstationen in München (Stand ca. 2000)



- **Die reale Größe der Funkzellen wird neben der maximalen Ausbreitung / Reichweite auch stark vom Bedarf /Anzahl aktiver Nutzer bestimmt**

[Quelle: Eberspächer, GSM…, 2009]

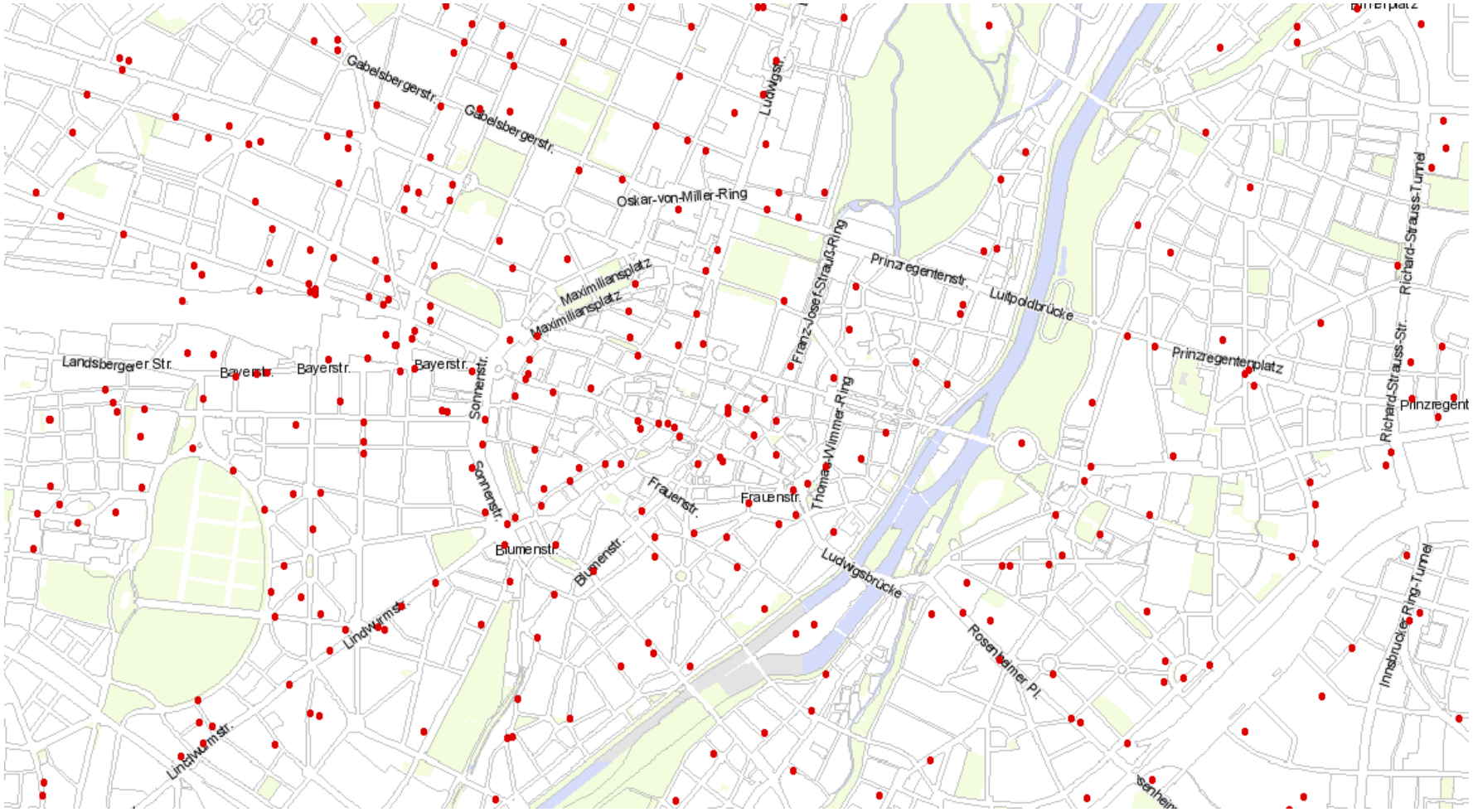
Aktueller Stand der Mobilfunkstationen in Mch



Aktuelle Auflistung der aktiven Mobilfunkmasten in München: (Stand 05/2015) mit Angabe der Betreiber, Systeme (GSM / UMTS / LTE) und Frequenzen

http://maps.muenchen.de/rgu/mobilfunkstationen (2019: nicht mehr verfügbar)

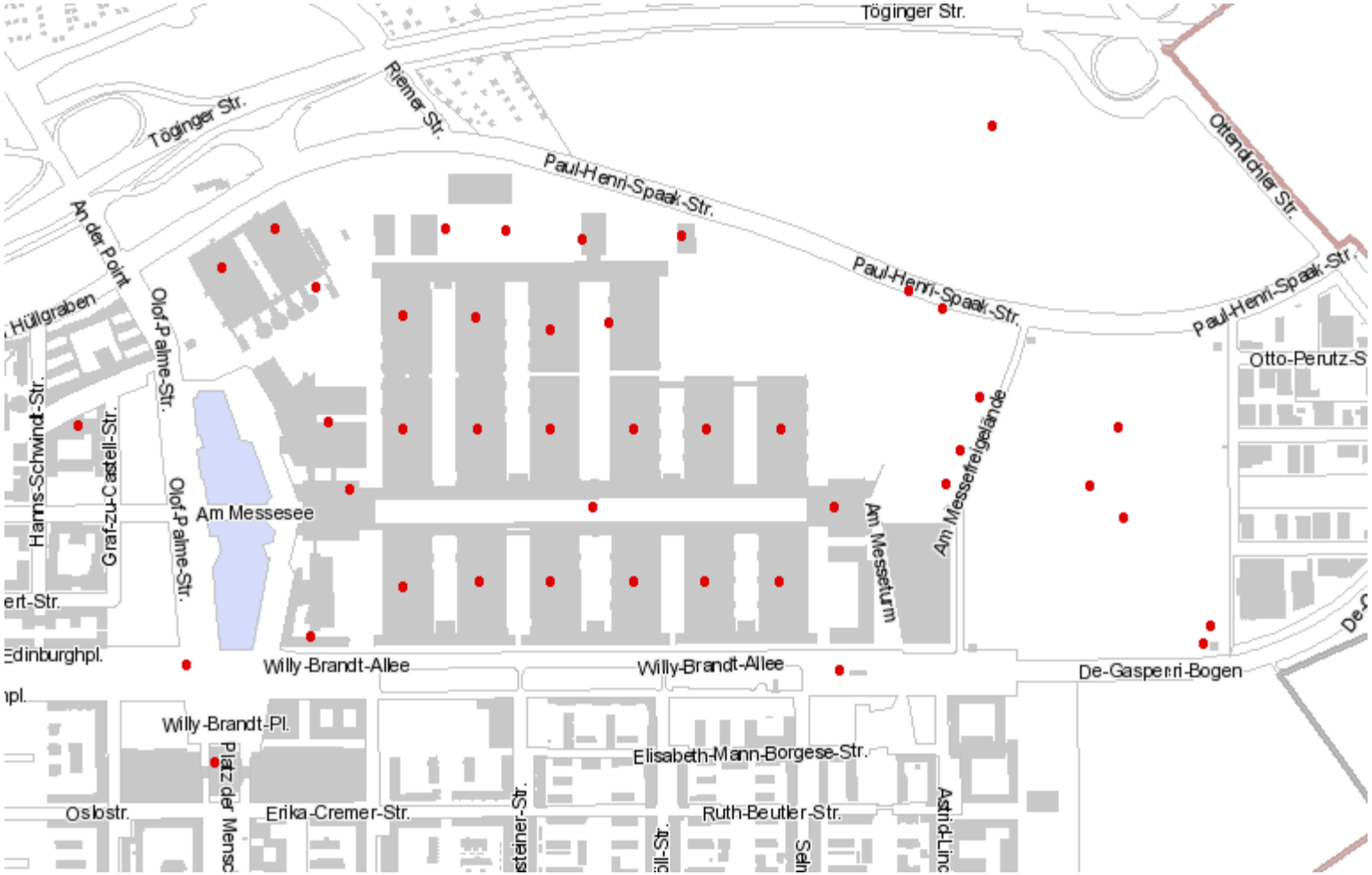
Mobilfunkmasten am Beispiel München Innenstadt



Aktuelle Auflistung der aktiven Mobilfunkmasten in München: (Stand 5/2015)
mit Angabe der Betreiber, Systeme (GSM / UMTS / LTE) und Frequenzen

http://maps.muenchen.de/rgu/mobilfunkstationen

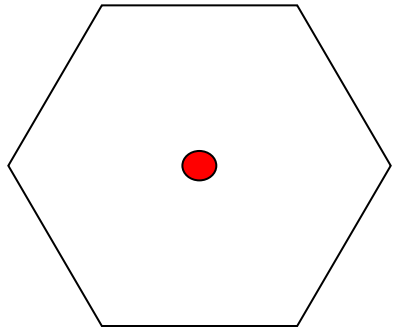
Mobilfunkmasten am Beispiel Messe München



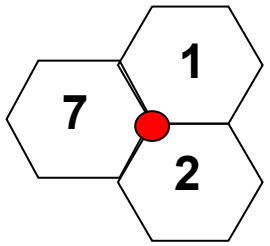
Aktuelle Auflistung der aktiven Mobilfunkmasten in München: (Stand 5/2015)
mit Angabe der Betreiber, Systeme (GSM / UMTS / LTE) und Frequenzen
http://maps.muenchen.de/rgu/mobilfunkstationen

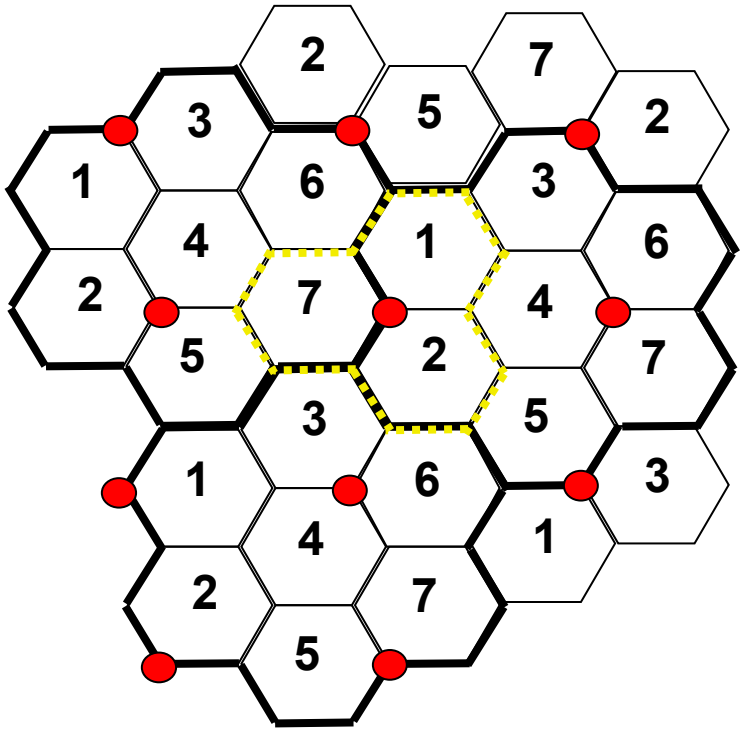
Mobil-Funk-Netz

- **1 Funkzelle = 1 Funkmast ?**



- **Meist 3 Sektoren je Mast =>**





- **Heute: auch 6 Sektoren / Mast**

Mobil-Funk-Netz

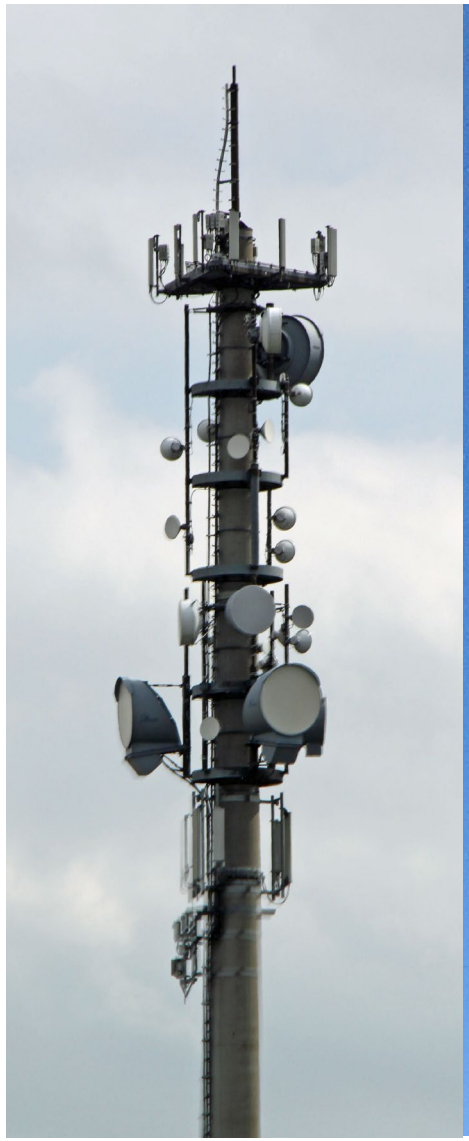
- **An einem Funkmast (Site) befinden sich meist**
  - mehrere Sektoren (Antennen)
  - für mehrere Frequenzbänder
  - für mehrere Mobilfunktechniken
  - Und manchmal auch von mehreren Betreibern
    (site sharing)

- **Beispielfoto (Telekom)**
  - 3 * GSM
  - 3 * UMTS
  - 3 * LTE

- **Mobilfunkstandorte der DT:**
  - 27.000 in 2017
  - 33.000 in 2021

Beispiele

Neben den Mobilfunk-Antennen sind oft auch Richtfunk-Antennen an den Masten zur Anbindung an das Netz => „Mobile Backhaul“



Installation 3 Sektor-Antennen

Beispiel für eine Mobilfunk-Installation in Hamburg.

Ungeschützt stehen die Systemteile der 3 Antennen-Sektoren am Boden, verbunden über Koax-Kabel mit den Antennen auf dem Dach. (Nokia)

Fotografiert im Dez 2019

Multiplex Technik bei GSM

- Trennung von Sende- und Empfangsrichtung:

  ➔ **Frequenz-Multiplex**

- Trennung der Daten einzelner Teilnehmer:

  ➔ **Zeitmultiplex**

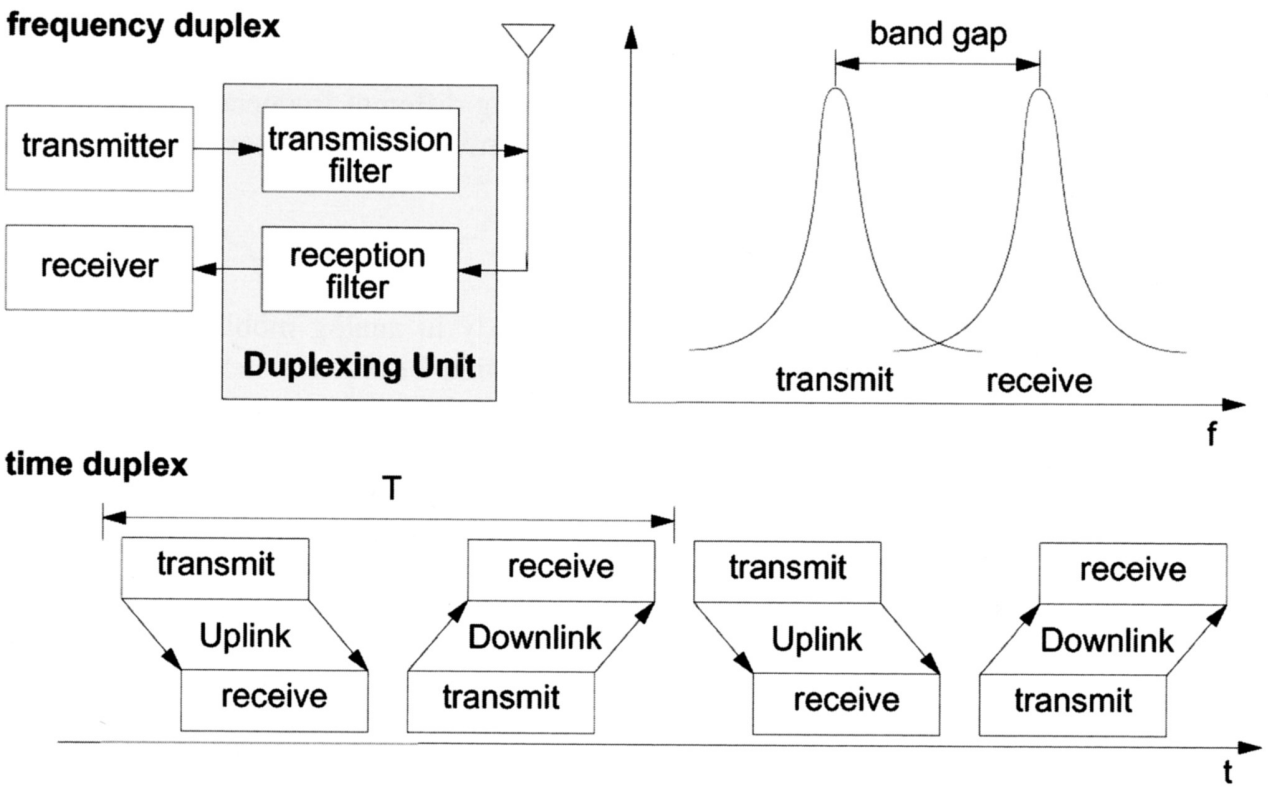


Figure 2.3 Frequency and time duplex.

[Quelle: Eberspächer, GSM…, 2009]

Eckwerte der GSM Funktechnik

Stand 2010 in D

	GSM 900	GSM 1800
Frequenzband (Empfang)	925 – 960 MHz	1805 – 1880 MHz
Frequenzband (Senden)	880 – 915 MHz	1710 – 1785 MHz
Kanalraster	200 kHz	200 kHz
Anzahl Kanäle	175 Paare	375 Paare
Zeitlage pro Kanal	8	8
Duplexabstand	45 MHz	95 MHz
Modulation	GMSK (1 Bit / Symbol)	
Zugriffsverfahren	FDMA (Richtung), TDMA (Kanal)	
Max. Übertragungsrate / Kanal	270,88 kbit/s	
Max. Zellgröße	30 – 35 km	< 8 km

Gesamtkapazität des E-GSM 900 Bands: 2 * 47,4 Mbit/s / GSM 1800: 2 * 101,6 Mbit/s
Die Nutzbare Datenrate ist aber deutlich kleiner
Aufteilung der Frequenzen auf alle Netzbetreiber => Folie

Modulation: GSMK: Gaussian Minimum Shift Keying:
digitale Phasenmodulation mit konstanter Amplitude

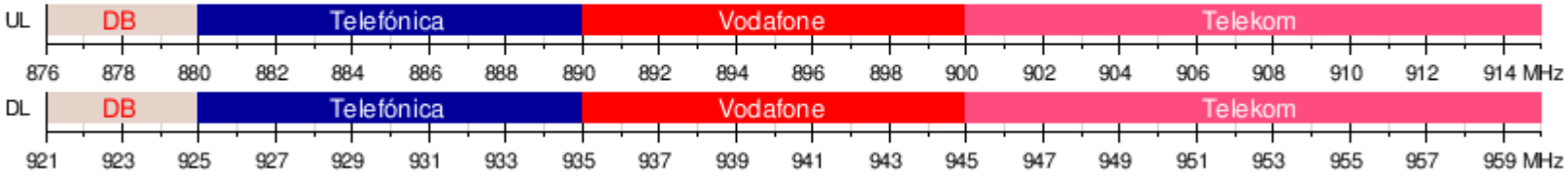
Nutzung der Mobil-Funk-Frequenzen in D

- **Vergabe der Frequenzblöcke durch die Bundesnetzagentur (BNetzA) in Form von Versteigerungen**
- **Aktuelle Belegung nach Versteigerung 8/2015:**

GSM 900

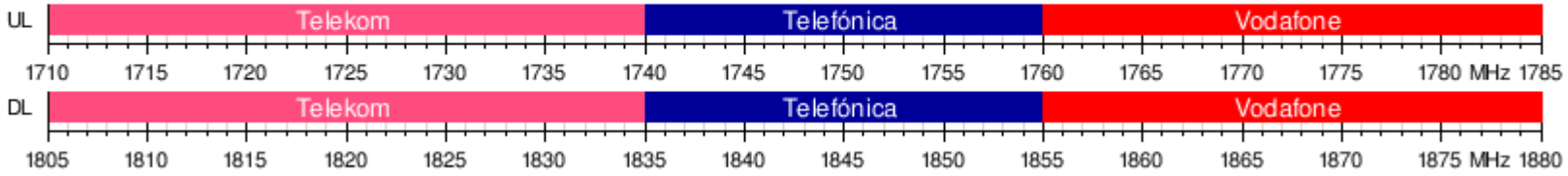
E-GSM Band in Europa: 880 – 915 / 925 – 960 MHz

R-GSM, E-GSM (GSM 900), E-UTRA Band 8



GSM 1800

DCS 1800 (GSM 1800) E-UTRA Band 3



DCS 1800 Band in Europa, Amerika, Asien, Afrika, Australien: 1710 – 1785 / 1805 – 1880 MHz

[Quelle: BNetzA, Wikipedia, GSM, 4/2019]

Versteigerung der Frequenzen 2015:

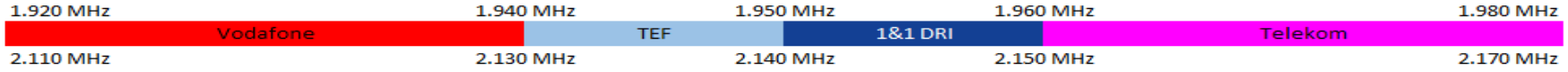
Telefónica Deutschland GmbH & Co. OHG	**700 MHz: 900 MHz: 1800 MHz:**	**2 x 10 MHz 2 x 10 MHz 2 x 10 MHz**	**1.198.238.000 €**
Telekom Deutschland GmbH	**700 MHz: 900 MHz: 1800 MHz: 1500 MHz:**	**2 x 10 MHz 2 x 15 MHz 2 x 15 MHz 20 MHz**	**1.792.156.000 €**
Vodafone GmbH	**700 MHz: 900 MHz: 1800 MHz: 1500 MHz:**	**2 x 10 MHz 2 x 10 MHz 2 x 25 MHz 20 MHz**	**2.090.842.000 €**
Gesamt	**270 MHz**		**5.081.236.000 €**

[Quelle: www.bundesnetzagentur.de 6/2015]

Versteigerung der Frequenzen 2019:

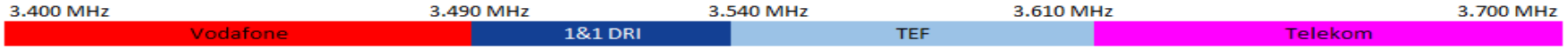
Im Bereich bei 2 GHz

Bandlage 01.01.2021 bis 31.12.2025



Bandlage 01.01.2026 bis 31.12.2040

Im Bereich bei 3,6 GHz



Bandlage im Bereich 3,6 GHz

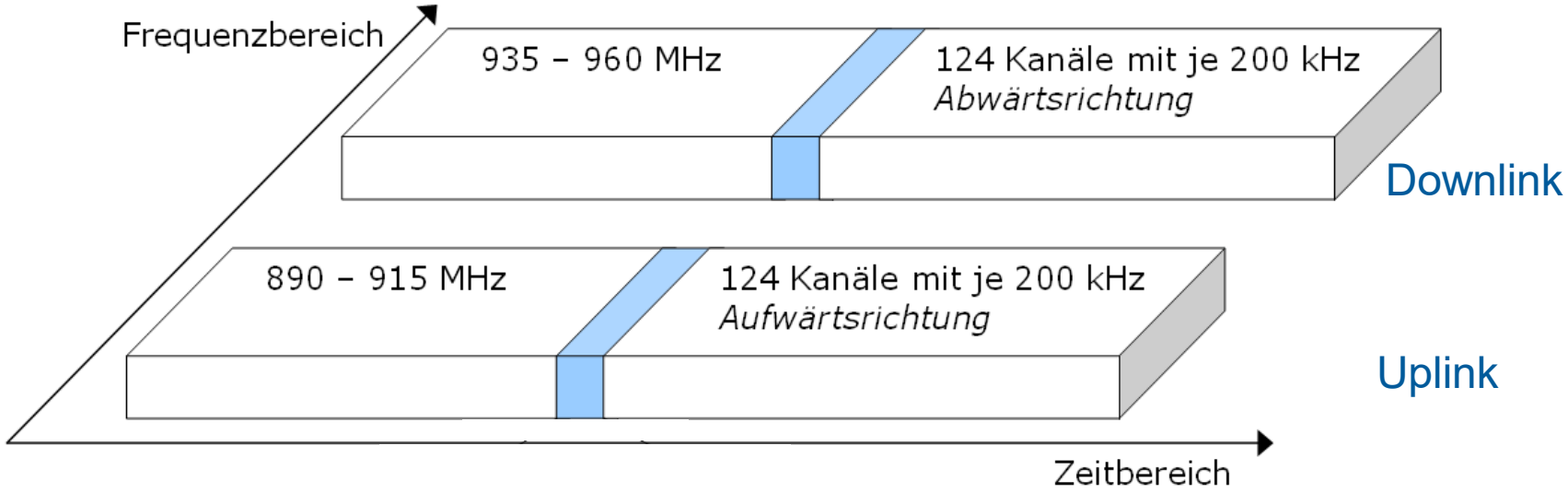
	Drillisch Netz AG	Telefónica Germany GmbH & Co. OHG	Telekom Deutschland GmbH	Vodafone GmbH
2 GHz	2 x 10 MHz	2 x 10 MHz	2 x 20 MHz	2 x 20 MHz
3.6 GHz	50 MHz	70 MHz	90 MHz	90 MHz
Summe	70 MHz	90 MHz	130 MHz	130 MHz

Die Auktion endetet nach 497 Runden bei 6.549.651.000 €.

[Quelle: www.bundesnetzagentur.de 8/2019]

[https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/OeffentlicheNetze/Mobilfunknetze/mobilfunknetze-node.html]

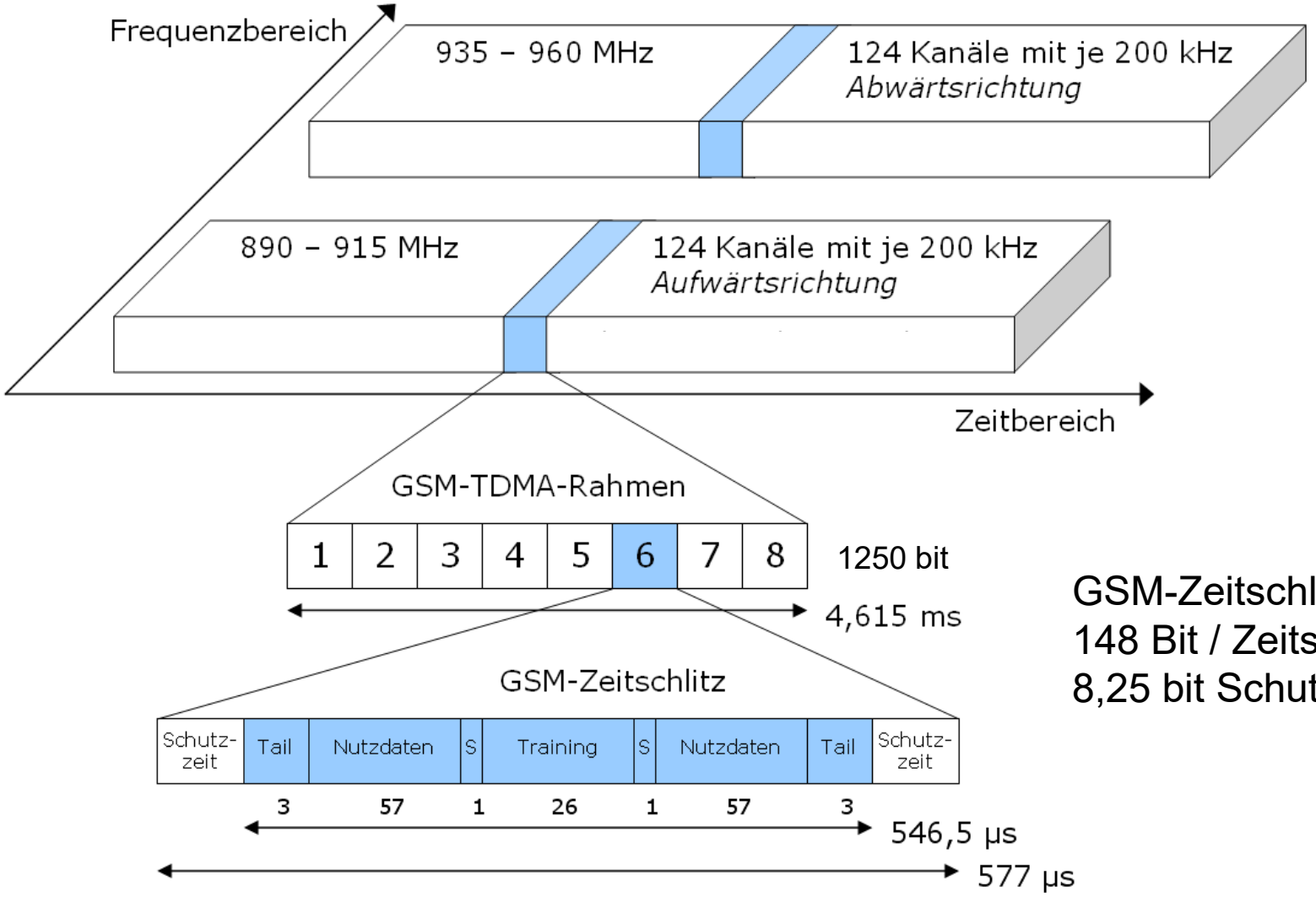
Struktur der GSM-Daten (900 MHz-Band)



- Trennung von Sende- und Empfangsrichtung durch unterschiedliche Frequenzbereiche (Bänder)
- Frequenzabstand Uplink – Downlink: 45 MHz (Fest, sog. Duplexabstand)
- In jedem Frequenzband liegen 124 Kanäle (GSM 900), später erweitert auf 175 Kanäle im Bereich 880 – 915 MHz, bzw. 925 – 960 MHz
- In jedem Kanal liegen die TDMA-Rahmen mit den einzelnen Slots für einen Teilnehmer

[Quelle: Wikipedia, GSM, 5/2014]

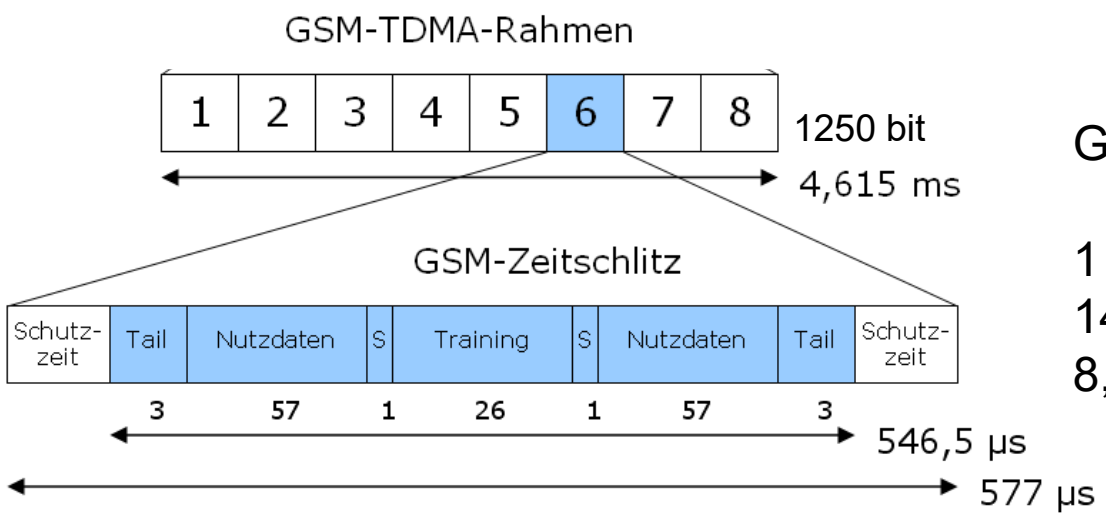
Struktur der GSM-Daten (900 MHz-Band)



GSM-Zeitschlitz = Burst
148 Bit / Zeitschlitz
8,25 bit Schutzzeit

[Quelle: Wikipedia, GSM, 5/2014]

Struktur der GSM-Daten



GSM-Zeitschlitz = Burst

1 Kanal =
148 Bit / Zeitschlitz (Burst)
8,25 bit Schutzzeit

- Nutz-Datenrate / Kanal: 114 bit / 4,615 ms => 24,7 kbit/s
- Signalisierung + Synchronisation + Guard Time: 42,25 bit / 4,615 ms => 9,2 kbit/s
- Signalisierung (z.B. beim Handover) wird als Nutzdaten übertragen und mit den „Stealing Flag“ S angezeigt
- Weitere Burst (Zeitschlitzformate) für
  - Frequency Correction: Frequenzabgleich / Taktsynchronisation
  - Synchronisation: des TDMA-Musters / der Zeitschlitze
  - Dummy: Periodische Lokalisierung und Leistungsmessung
  - Access: Erster Vielfachzugriffskanal (Slotted Aloha) für Gesprächswunsch

[Quelle: Wikipedia , GSM, 5/2014]

Ablauf der Datenübertragung – 1 –

- TDM-Verfahren erfordern eine **Zeit-Synchronisation** für den Datenaustausch
  - Die Mobilfunkstation werden über das Netz synchronisiert (SDH, in Zukunft auch über Ethernet, auch GPS)
  - Spezieller Synchronisations-Burst für Mobiltelefon
  - Synchronisations-Muster („Training“) in jedem Burst

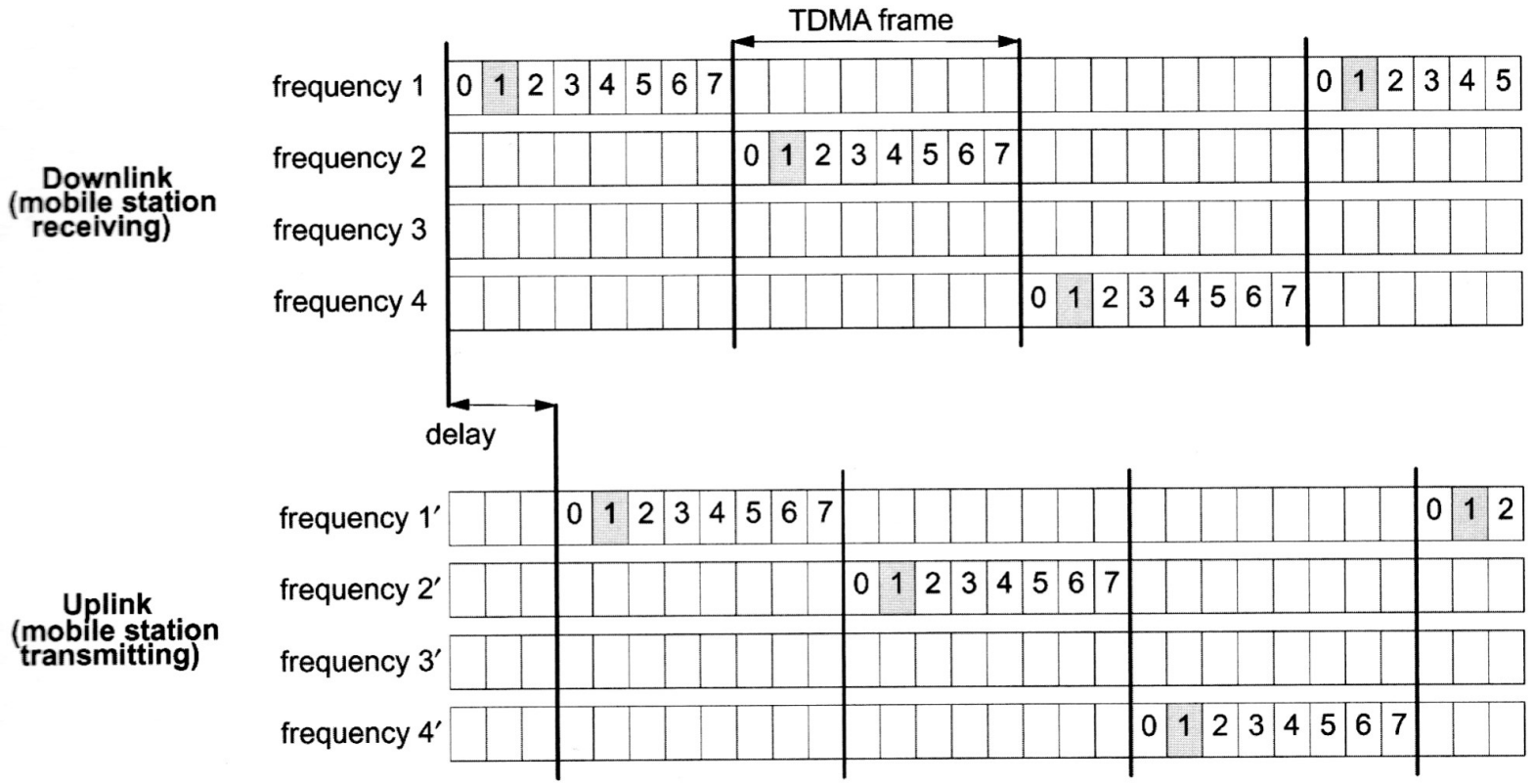
- Wechsel der Frequenz nach jedem Rahmen (Frequency Hopping)
  - Erhöhung der Störfestigkeit
  - 217 Frequenzsprünge / sec (alle 4,615 ms, also nach jedem TDMA Rahmen)

- Anpassung der Sendeleistung an den Bedarf:
  - BS steuert Leistung des MS
  - Reduzierte Störungen der Nachbarzellen und Kanäle
  - Minimaler Energieverbrauch des Mobiltelefons

BS: Base Station
MS: Mobile Station

Ablauf der Datenübertragung – 2 –

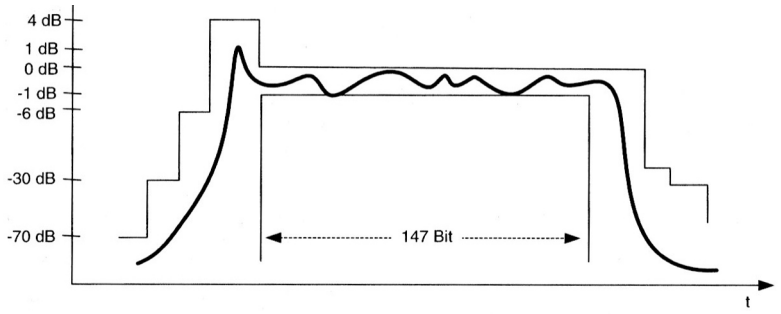
- Mobiltelefon (MS) empfängt Burst mit seine Daten
- Im Uplink ist ein Kanal um 3 Zeitschlitze zum Downlink versetzt.



[Quelle: Eberspächer, GSM…, 2009]

Ablauf der Datenübertragung – 3 –

- Im Uplink ist ein Kanal um 3 Zeitschlitze zum Downlink versetzt.
  - MS kann zeitversetzt Senden und Empfangen => 1 Antenne reicht aus
  - Schutzzeit (Guard Time) zwischen den TDM-Rahmen von 8,5 Bit-Zeiten
  - Timing Advance: BS kann MS einen Zeitversatz für das Senden in Abhängigkeit von der Laufzeit / Entfernung BS – MS mitteilen (n * 1 Bit => n * 550 m Entfernung)
    ➔ Guard Time ist ausreichend für alle MS im Bereich einer BS
  - Bitmuster in jedem Burst (Training) für Synchronisation und Entzerrung



BS: Base Station
MS: Mobile Station

Maske für den Signalverlauf eines Burst
Quelle: Duque-Antón, 2002

GSM-Kanalstruktur

200 kHz-Kanäle

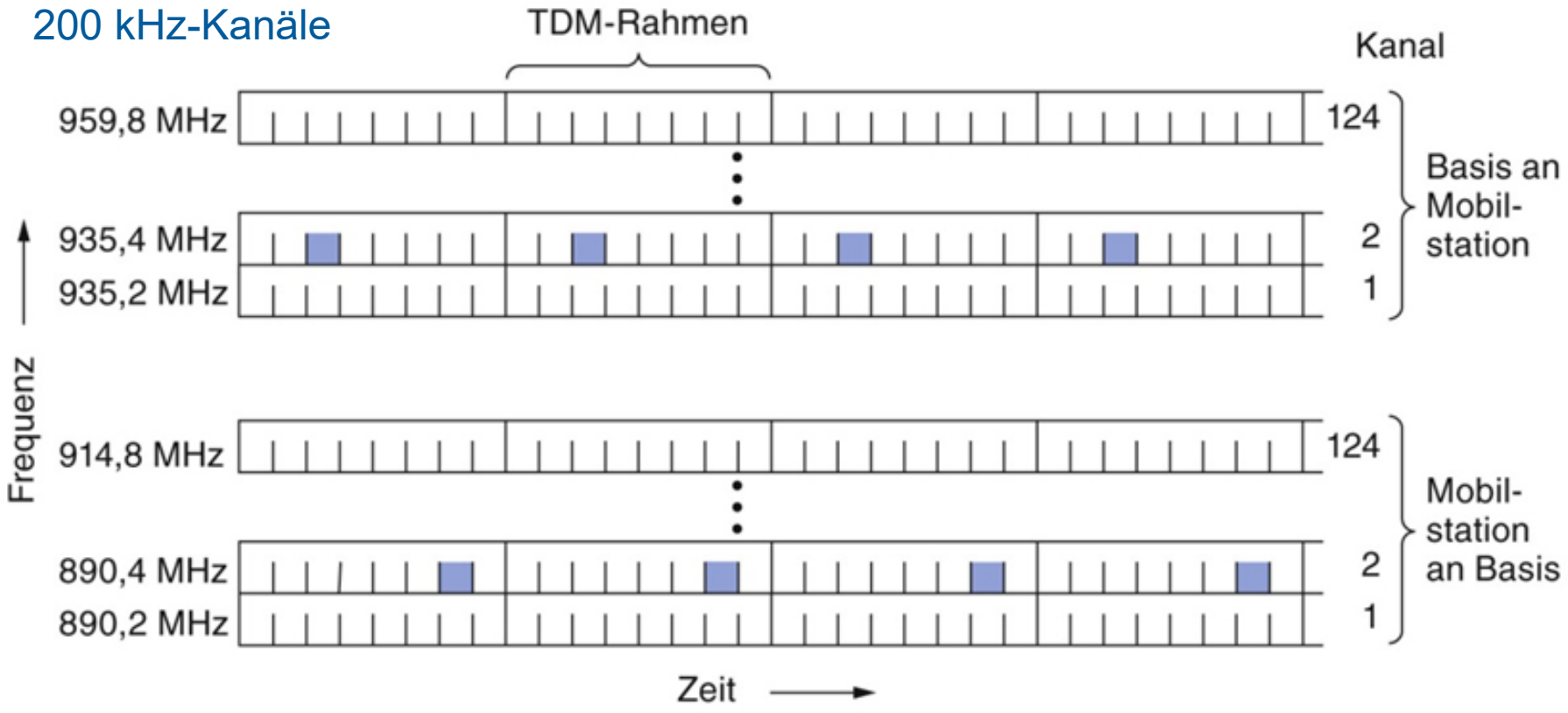


Abbildung 2.47: GSM nutzt 124 Frequenzkanäle, wobei jeder Kanal ein TDM-System mit acht Zeitscheiben verwendet.

[Quelle: Tanenbaum, 2012]

GSM-Kanalstruktur – Multiframe in jedem Frequenz-Kanal

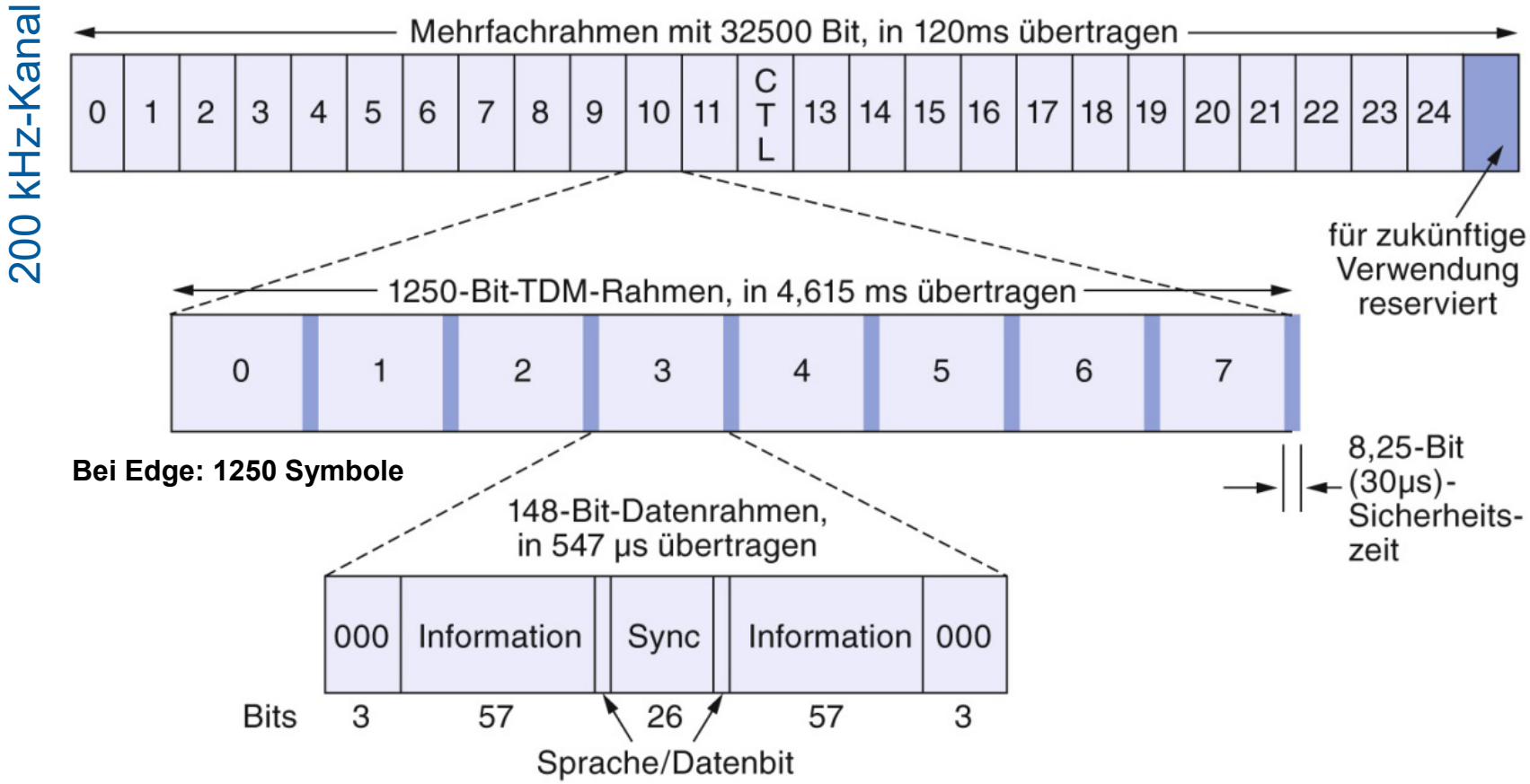


Abbildung 2.48: Teil der GSM-Rahmenstruktur.

2 Burst von 26 übertragen Signalisierung und Steuerinformationen

[Quelle: Tanenbaum, 2012]

Kanalstruktur bei GSM

- **2 Kanalgruppen bei GSM:**
  - **Traffic Channels (TCH)**
    für Bearer Services (Nutzverkehr: Sprache oder Daten)
    - Full Rate TCH mit 22,8 kbit/s (B_m)
    - Half Rate TCH mit 11,4 kbit/s (L_m)

  - **Control Channel (D_m):**
    - **Broadcast Control Channel BCCH**:
      - Allg. Daten über Netz, Basisstation,
      - Frequenzen, Nachbarfrequenzen, Frequenzhopping
    - **Common Control Channel CCCH:**
      - Verbindungsaufbau BS → MS mit Paging Channel
      - Verbindungsaufbau MS → BS mit Random Access Channel
    - **Dedicated Control Channel DCH:**
      - Steuerdaten vor und während des Gesprächs
  - Die Control Channel werden in komplexe und lange Rahmenstrukturen eingebettet („GSM-Multiframe“)
  - 2 von 26 Kanälen (im Multiframe) werden zur Übertragung der Signalisierungskanäle verwendet

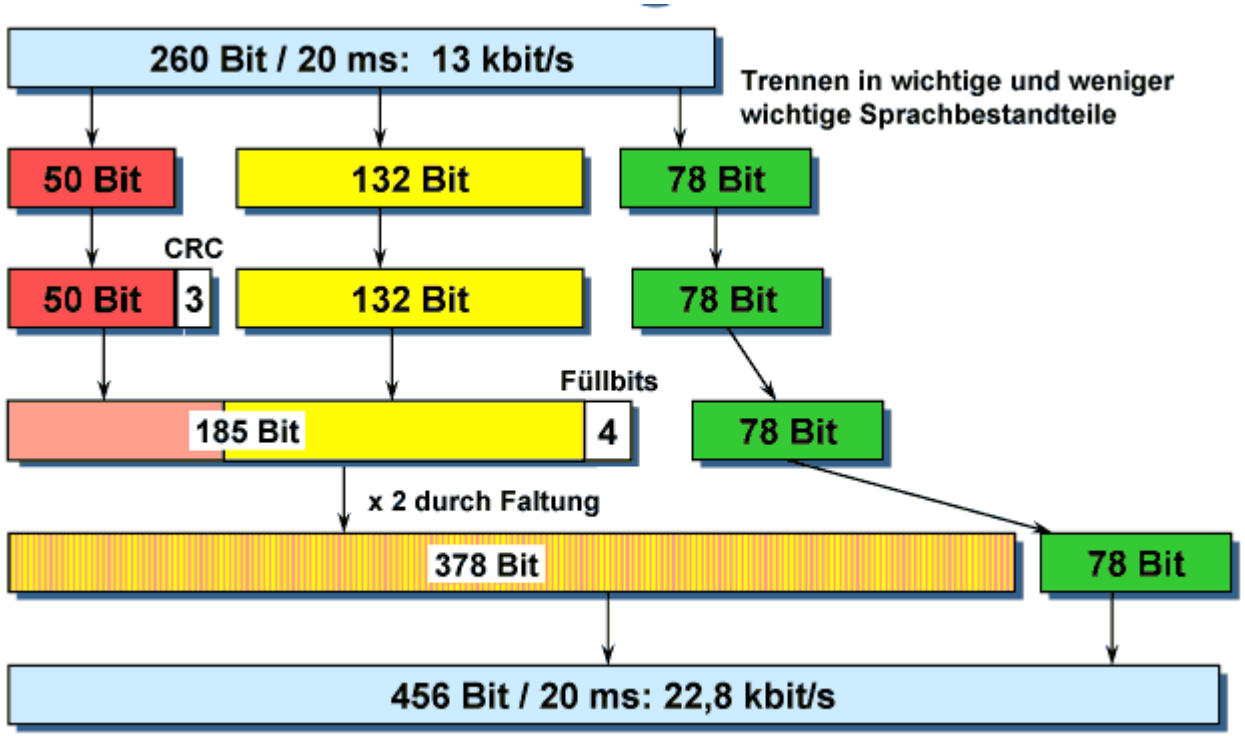
BS: Base Station
MS: Mobile Station

Sprachübertragung bei GSM

- **Sprache in Telefon-Netz = 64 kbit/s PCM**
- **Bei GSM muss diese Sprache sehr stark komprimiert werden:**
  - Nutzkanal = 22,8 kbit/s
  - Daten für Fehlererkennung und Korrektur ~ 10 kbit/s
  - Mögliche Datenrate für Sprache ~ 13 kbit/s (Full Rate)
  - Funktion im Netz: **TRAU** (Transcoding and Rate Adaption Unit)
- **Verfahren beim Full Rate Codec:**
  - Mischung aus Langzeit- und Kurzzeit-Prädiktion
  - Ausnutzung der natürlichen Eigenschaften der Sprache
  - RPE/LTP-LPC Sprachkompression: *Linear Predictive Coding*, *Long Term Prediction*, *Regular Pulse Excitation*
- ***Weitere Verfahren:***
  - Half Rate Codec (für half rate TCH) ➔ 2 Gespräche pro Kanal ➔ Schlechte Sprachqualität, nur bei Überlastung einer Funk-Zelle
  - Mehrere verbesserte und adaptive Verfahren (Bessere Sprachqualität und / oder verbesserte Fehlerkorrektur), z.B. „HD-Voice“

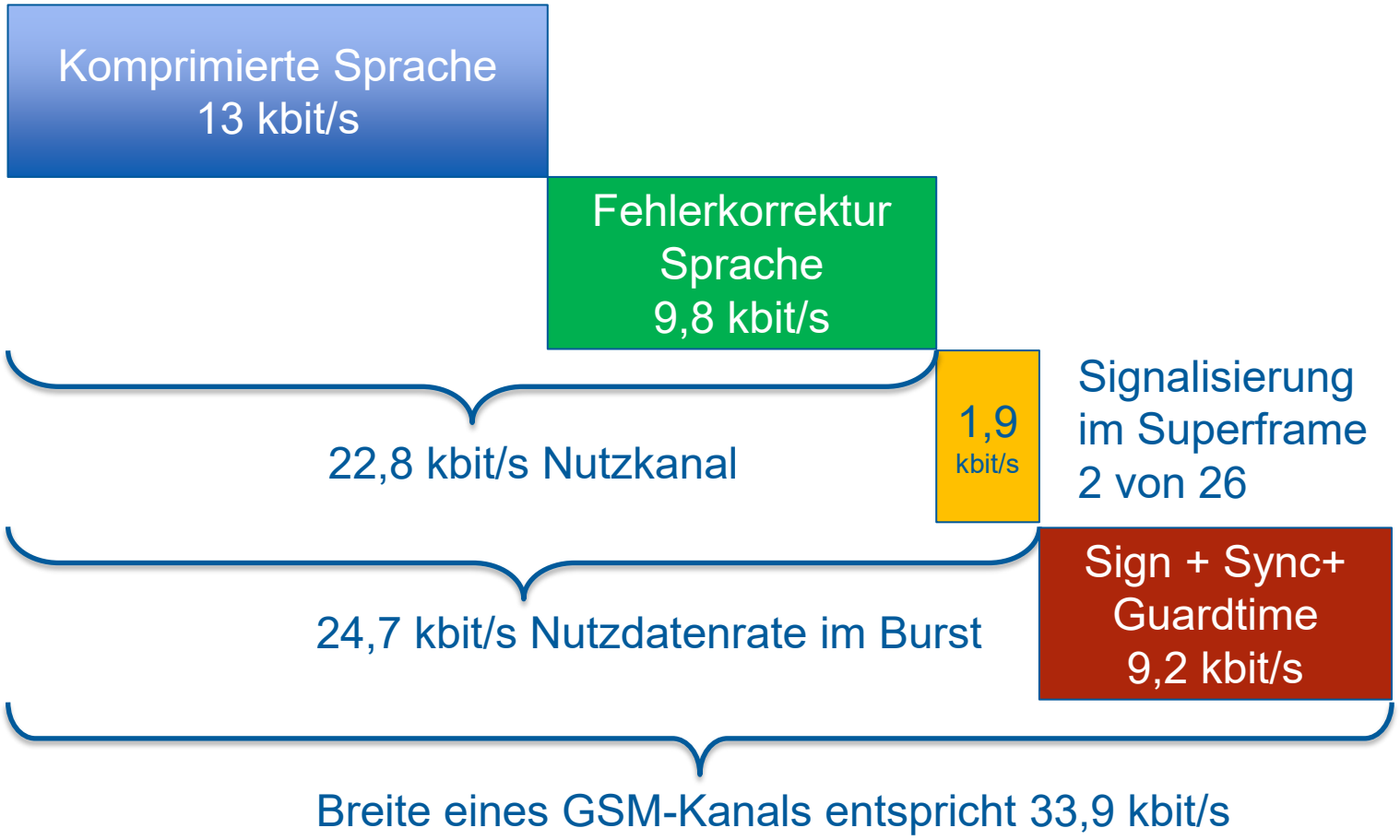
Sprachcodierung im GSM-Full Rate Codec

- Kompression im Codec ergibt 13 kbit/s (260 Sprachbit / 20 ms)
- Trennen in wichtige und weniger wichtige Sprachbestandteile:
- Klasse Ia =>
  50 + 3 bit CRC
  ggfs. Werte des
  vorh. Pakets
- Klasse Ia + Ib=>
  Faltungscodierung
  zur Forward Error
  Correction
- Ergebnis:
  Gute Fehlererkennung
  bei Einzelfehlern oder
  kurzen Burststörungen
- Ergebnis:
  456 bit / 20 ms = 22,8 kbit/s



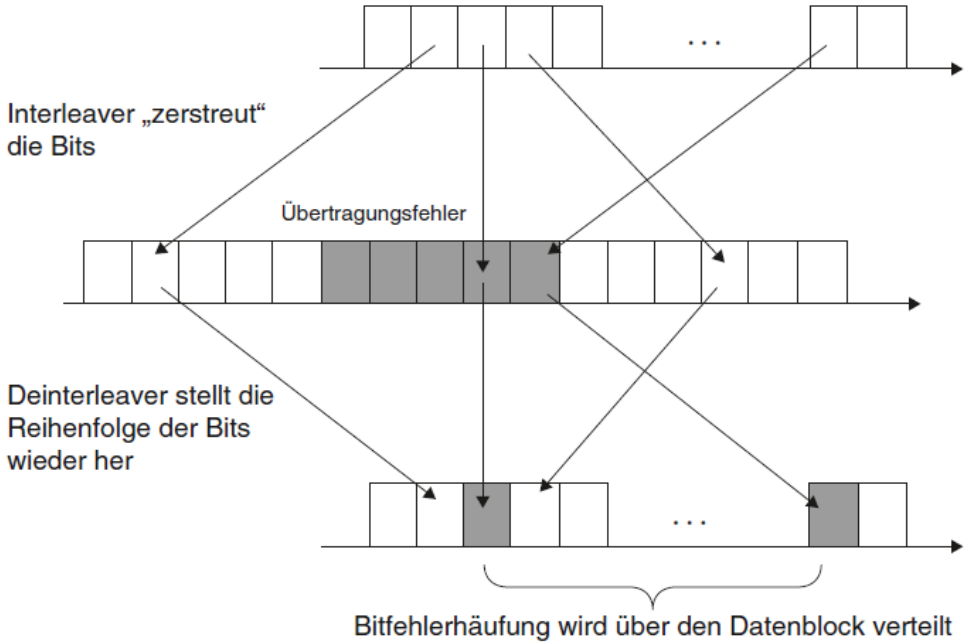
[Quelle: Wikipedia, GSM, 5/2014]

Aufteilung der Bandbreite bei GSM-Sprache (Full Rate)



Reduktion von Störungen: Interleaving

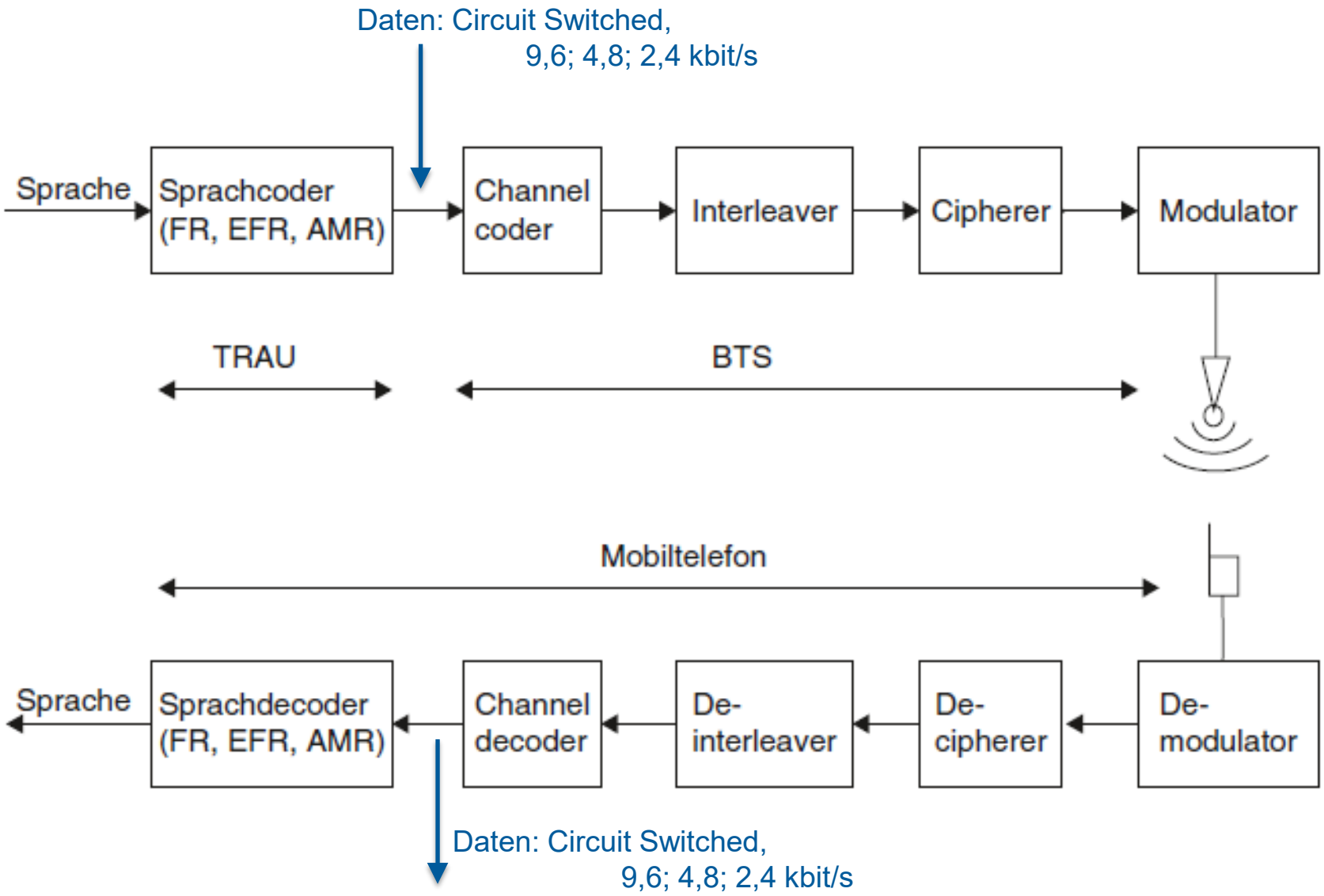
- **Störungen / Fading auf Funkkanälen betreffen oft viele Bits in Folge:**
  - Verschachteln der 57 Bit Datenpakete über mehrere Zeitschlitze



  - Sprachblock wird über 8 Burst verteilt (anstatt 4),
  - weitere 40 ms Verzögerung (Interleaver) und 20 ms für Codec

Quelle: Sauter, 2018

Verarbeitungsschritte bei der Übertragung

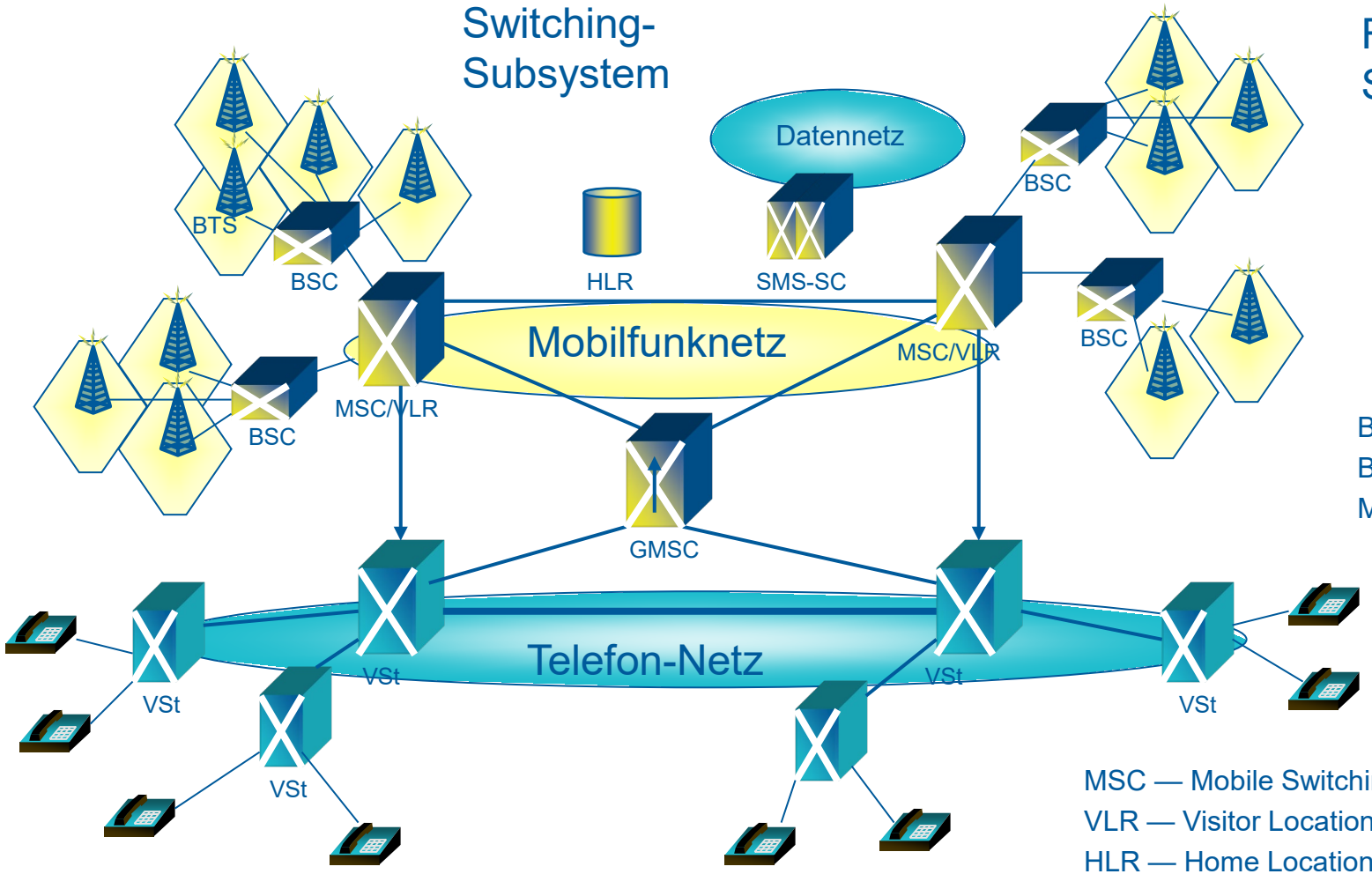


Quelle: Sauter, 2018

Mobilfunk-Systeme
der 2. Generation

➔ GSM
Teil 2: Netzarchitektur

Architektur des GSM-Netzes

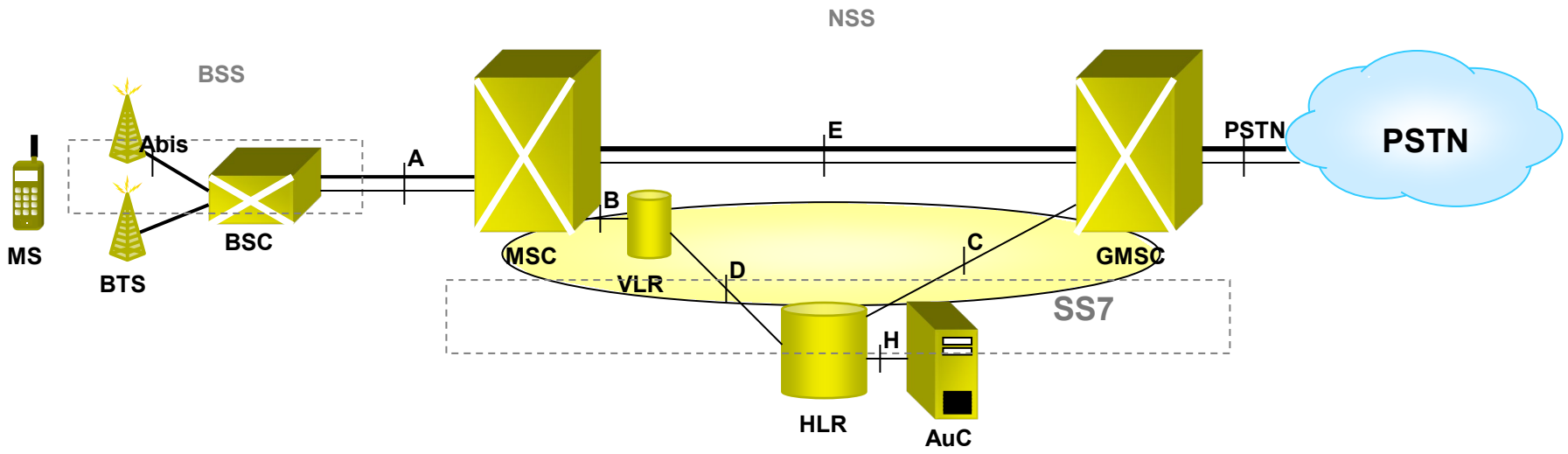


BTS — Base Transceiver Station
BSC — Base Station Controller
MS – Mobile Station

MSC — Mobile Switching Center
VLR — Visitor Location Register
HLR — Home Location Register
GMSC – Gateway MSC
SMS-SC: SMS Service Center

[Quelle: Brough Turner & Marc Orange, 3G Tutorial]

GSM-Architektur - Voice only

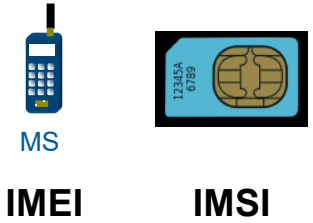


BSS — Base Station System
BTS — Base Transceiver Station
BSC — Base Station Controller
MS — Mobile Station

NSS — Network Sub-System
MSC — Mobile-service Switching Centre
VLR — Visitor Location Register
HLR — Home Location Register
AuC — Authentication Server
GMSC — Gateway MSC

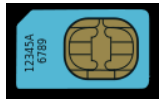
[Quelle: Brough Turner & Marc Orange, 3G Tutorial]

Identitäten im GSM-Netzes: SIM-Karte



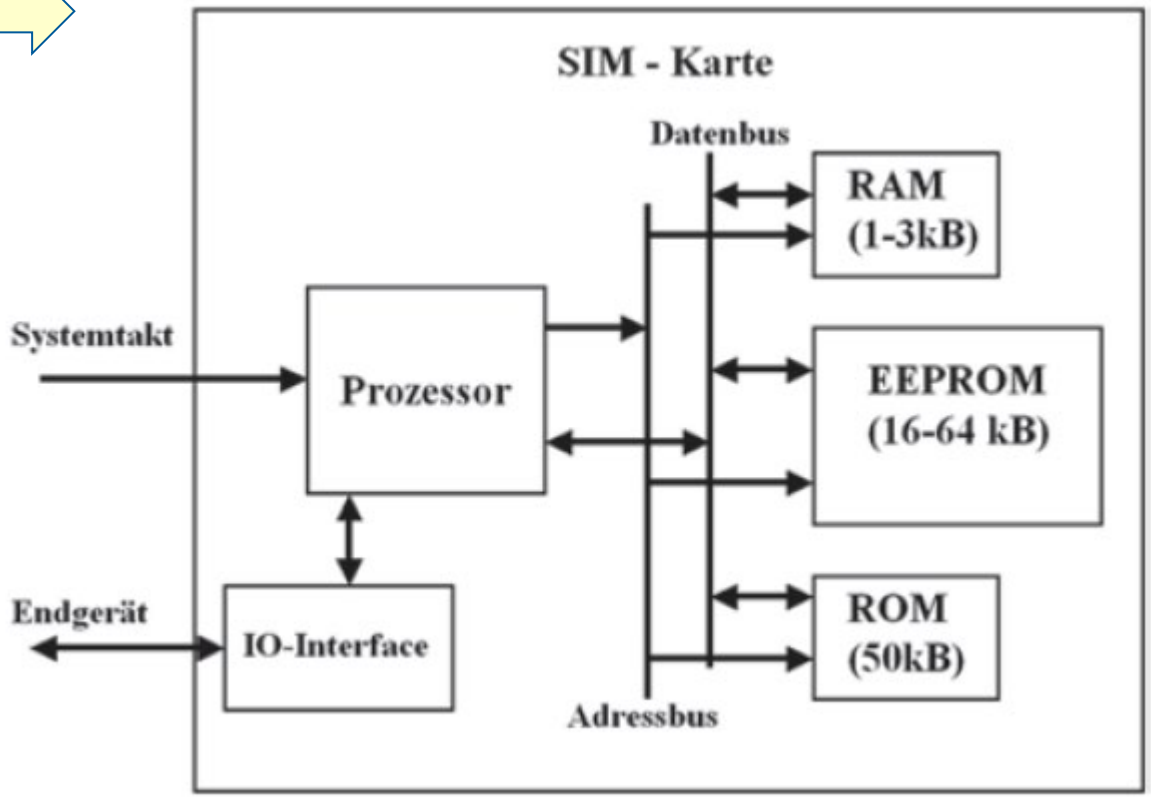
- **IMEI: International Mobile Station Equipment Identity**
  - 15 stellige Seriennummer des Mobilen Geräts
- **SIM-Karte (Subscriber Identity Module)**
  - Identität des Nutzers im GSM-Netz,
  - Mit PIN geschützte Authentifikation
  - Enthält Prozessor und Schlüssel für die Verschlüsselung der Daten
  - Location Area der letzten Verbindung
  - **IMSI (International Mobile Subscriber Identity)**
    - Weltweit eindeutige Nummer
    - Zuordnung zu einem Land und einem Betreiber
    - Benötigt für die Zuordnung des Teilnehmers zu einem Ort (Location Registration / Location Update)

Identitäten im GSM-Netzes: SIM-Karte



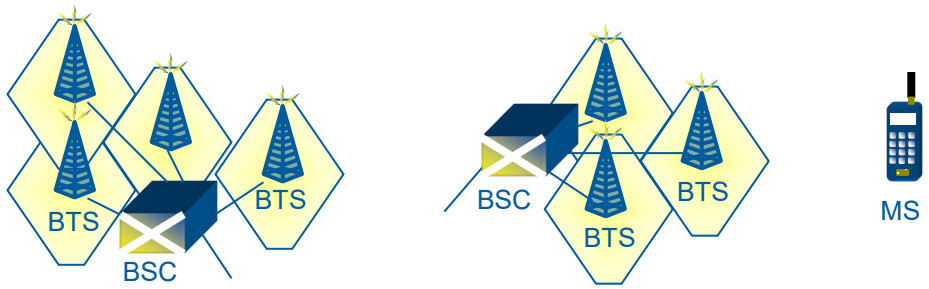
Blockschaltbild einer SIM-Karte

- Zugriff auf die Daten im EEPROM nur über den Prozessor (z.B. auf die Schlüssel)
- Dateisystem mit Zugriffsrechten
- Zugriff erfordert vorher PIN-Eingabe
- Weitere Applikationen möglich mit SIM Application Toolkit (SAT)



[Quelle: Martin Sauter, Grundkurs Mobile Kommunikationssysteme, 6. Aulf, 2015]

Architektur des GSM-Netzes: Radio-Subsystem BSS



Radio-Subsystem (BSS: Base Station Subsystem)

- **Abwicklung des Funkverkehrs von / zu MS**
- **BTS — Base Transceiver Station („Basisstation“)**
  - Signalverarbeitung für die Funkschnittstelle
  - Kommunikation mit der Mobile Station (Mobiltelefon)
  - Eine BTS je Zelle / Sektor
- **BSC — Base Station Controller**
  - Steuert 10 ..100 BTS
  - Verbindungsaufbau,
  - Auswahl Funkkanal,
  - Handover,
  - Leistungsregelung der MS

MSC: Mobile Switching Centre

Vermittlungsstelle im GSM-Mobilfunknetz

- Schnittstelle zwischen dem Funknetz (Base Station Controller) und dem Telefonnetz
- Eine MSC ist für ein bestimmtes Gebiet zuständig (Serving Area), damit
- feste Zuordnung einiger (10 … 100…) BSC mit ihren BTS zu einer MSC
- **Aufgaben der MSC:**
  - Steuerung des Gesprächsaufbaus und –abbaus (Call Control)
  - Vermittlung der Sprachkanäle
  - Steuerung des Transcoders (TRAU, Umsetzung 64 kbit/s ⇔ 13 kbit/s)
  - Standort-Verwaltung / Lokalisierung der Teilnehmer
  - Steuerung des Handover
  - Lokale Verwaltung der Teilnehmer-Profile (im Visitor Location Register (VLR))
  - Erheben von Gesprächsdaten zur Gebührenabrechnung
  - Kommunikation mit anderen Komponenten des Mobilfunknetzes
  - Authentisierung

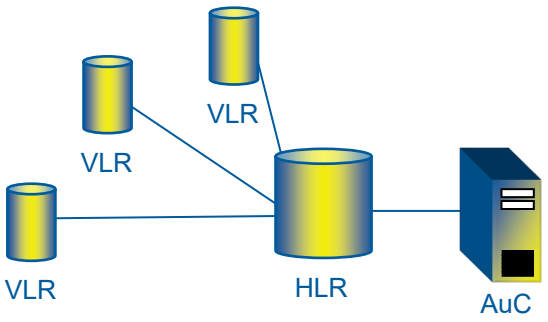
MSC: Mobile Switching Centre

Vermittlungsstelle im GSM-Mobilfunknetz

- **Schnittstellen eines MSC:**
  - Zu den anderen MSC eine Netzes
  - Zum HLR (Home Location Register)
  - Signalisierungsnetz (SS7)
  - Dienste-Zentralen (SMS, Voice-Mailbox)

- **Gateway-MSC: zusätzlich Schnittstellen zu anderen Netzen (Fest / Mobil)**

Datenbanken im GSM-Netz



- **Teilnehmerdaten werden im HLR (Home Location Register) gehalten**
  - Zuordnung Rufnummer – IMSI (Rufnummer = MSISDN; Mobile Subscriber ISDN Number)
  - Aktueller Aufenthaltsort (Roaming Information)
  - Alle permanenten Teilnehmerdaten + Tarifdaten
  - Aktuelle Gebührendaten
- **VLR (Visitor Location Register), meist je MSC**
  - Einbuchen des Teilnehmers bei Aufenthalt in der Location Area eines VLR
  - Abgleich der Daten mit HLR (HLR kennt das aktuelle VLR)
  - VLR enthält alle für den Betrieb / Datenaustausch notwendigen Daten
- **AuC: Authentication Center**
  - Enthält die geheimen Schlüssel der Teilnehmer, Zuordnung zur IMSI
  - Zur Identifizierung und Authentifizierung der Teilnehmer
  - Schlüssel für die Nutzdatenverschlüsselung

Teilnehmerdaten werden im HLR (Home Location Register) gehalten

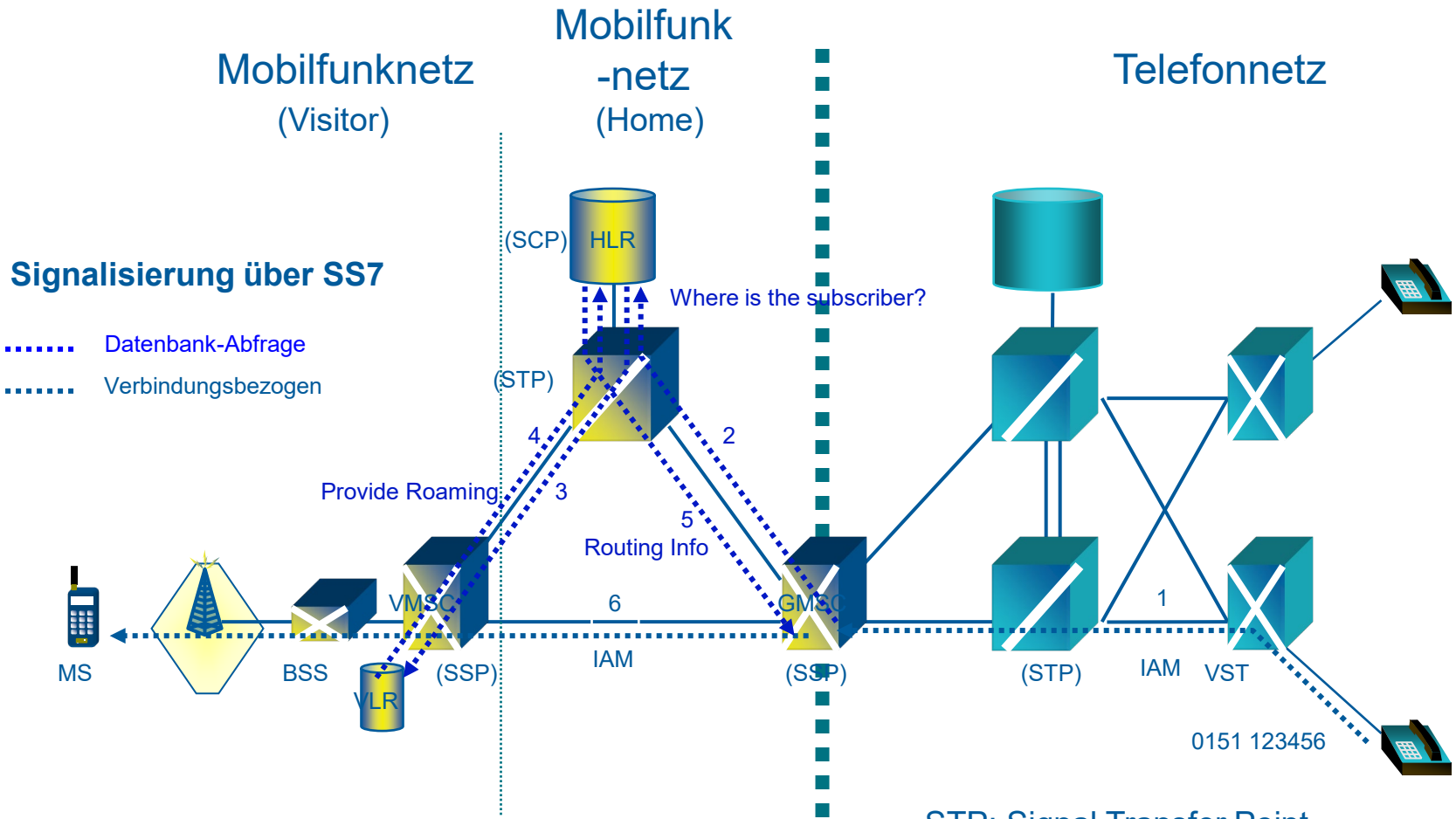
- **Semipermanente Daten**
  - International Mobile Subscriber Identity (IMSI)
  - Mobile Subscriber ISDN Number (MSISDN)
  - gebuchtes Dienstprofil (Anrufweiterleitung, Dienstsubskription, Dienstrestriktionen usw.)
- **Temporäre Daten**
  - Adresse des Visitor Location Registers (VLR)
  - Adresse des Mobile-services Switching Centre (MSC)
  - Authentication Set (aus mehreren Authentication Triples bestehend)
  - Gebührendaten

Datenbanken im GSM-Netz im Detail: VLR

VLR (Visitor Location Register), meist je MSC

- **Einbuchen des Teilnehmers bei Aufenthalt in der Location Area eines VLR**
- **Abgleich der Daten mit HLR (HLR kennt das aktuelle VLR)**
- **VLR enthält alle für den Betrieb / Datenaustausch notwendigen Daten:**
  - International Mobile Subscriber Identity (IMSI)
  - Mobile Subscriber ISDN Number (MSISDN, „internationale Rufnummer“)
  - Temporary Mobile Subscriber Identity (TMSI)
  - Mobile Station Roaming Number (MSRN)
  - Location Area Identification (LAI)
  - Adresse des Mobile-services Switching Centre (MSC-Adresse)
  - Adresse des Home Location Register (HLR-Adresse)
  - Daten des gebuchten Dienstprofils
  - Verkehrsdaten, die zur Weiterleitung an die Billing-Center entstehen

Verbindungsaufbau zu einem Mobilen Teilnehmer



IAM: Initial Address Message
(Signalisierung zum Verbindungsaufbau)

STP: Signal Transfer Point
SSP: Service Switching Point
SCP: Service Control Point

[Quelle: Brough Turner & Marc Orange, 3G Tutorial]

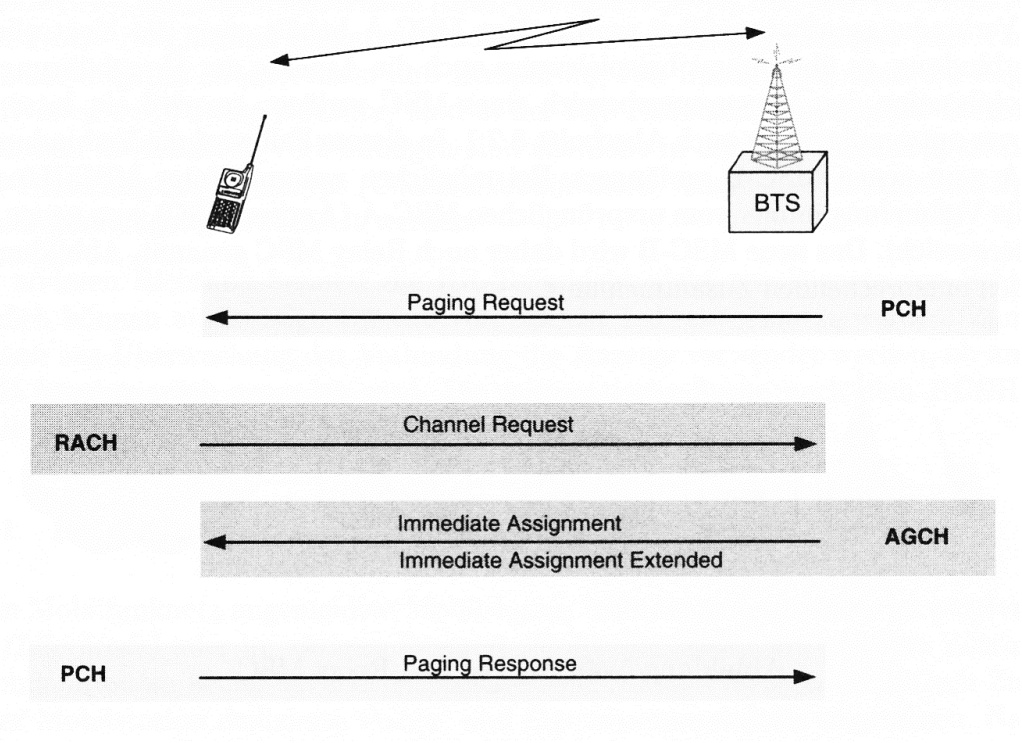
Radio-Ressource Management

- **Die Protokolle des Radio-Ressource-Layers (RR) steuern die Verbindung zwischen der Mobile Station und dem MSC (Ursprungs-MSC / Anchor-MSC)**

- **Aufgaben des RR-Layers:**
  - Steuerung des Funkkanals
    - Kanalzuweisung (Channel Assignment)
    - Kanalwechsel (Handover)
    - Kanalabbau (Channel Release)
  - Messungen des Funkstrecke (Signalqualität)
  - Leistungsregelung (Power Control)
  - Aktivieren der Verschlüsslung
  - Kanaltyp (Sprach- / Datenübertragung)

Verbindungsaufbau – Zuordnung eines „Kanals“

- Im Ruhezustand sind einer MS keine Frequenzen zugeteilt, aber
- MS „kennt“ das Netz und hat eine Liste mit den Broadcast Control Channels (BCCH-Kanäle) gespeichert, oder
- MS muss alle Frequenzen nach BCCH absuchen und die Empfangsfeldstärken messen.
- Ständige Überwachung der BCCH (Broadcast Control Channels).
- Festlegen der „eigenen“ BTS,
  - hier wird der Paging-Kanal (PCH) für Anrufe abgehört und
  - Auf dem Random Access Kanal (RACH) kann eine Verbindung (freier Zeitschlitz) angefordert werden



[Quelle: Duque-Antón, 2002]

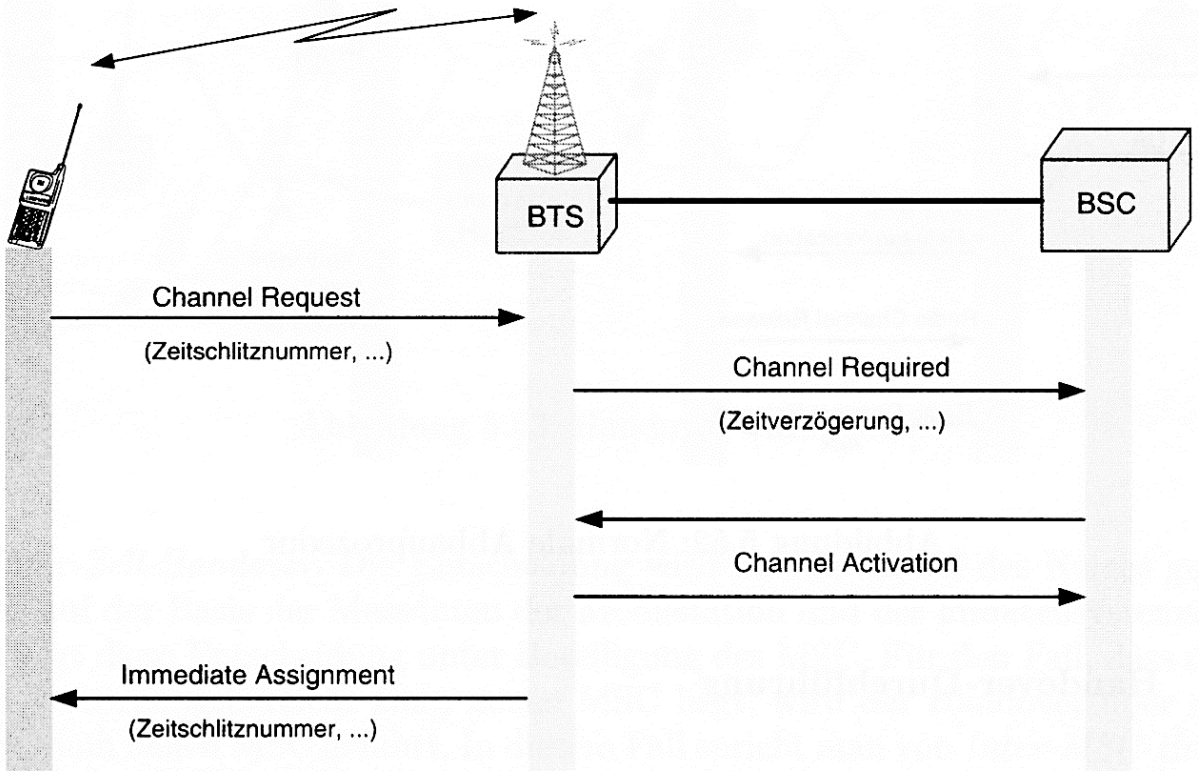
Etablieren der Verbindung mit dem Mobilfunknetz:

- Das mobile Endgerät (ME) versucht ständig an einer Basisstation (BTS) in Reichweite angemeldet zu sein, damit Anrufe oder SMS-Nachrichten jederzeit empfangen bzw. versendet werden können. Dieser Betriebszustand, bei dem keine aktive Verbindung besteht, wird als „Idle-Mode“ bezeichnet. Das ME empfängt und verarbeitet jedoch ständig Daten aus folgenden Funkkanälen der Luftschnittstelle Um der BTS:
  - **BCCH**: Broadcast Control Channel zur Identifikation des Netzes (BSIC) und Übermittlung aller nötigen Parameter, um die Kommunikation mit der Basisstation aufzunehmen.
  - **CBCH**: Cell Broadcast Channel überträgt aktuelle Nachrichten, z.B. Wetterdaten oder die lokale Verkehrssituation.
  - **PCH**: Paging Channel kündigt eingehende Anrufe oder SMS an (Downlink).
  - **RACH**: Random Access Channel wird genutzt um sich bei der BTS anzumelden (Shared Uplink).
  - **AGCH**: (Access Grant Channel) dieser Kanal ist dem ME als Downlink zugewiesen. Auf diesem Frequenzband können Signale empfangen werden.
- Ist das ME noch gar nicht am Funknetz angemeldet, scannt es nach verfügbaren Stationen, indem es sich zunächst mit einem Sender synchronisiert und dann den BCCH ausliest. Auf diesem Broadcast Channel werden Systeminformationen der BTS gesendet.
- An die Station mit der höchsten Sendeleistung wird dann ein „Access Burst“ gesendet, der aus einer „Channel Request Message“ auf dem RACH besteht.
- Danach wird dem ME eine Frequenz (ARF Channel) und ein „Time-Slot“ zugewiesen, damit es sich über den SDCCH bei dem Netzwerk anmelden kann. Hierzu sendet das Mobilteil ein „Location Update Request“, in dem die IMSI und LAI im Klartext an das Mobilfunknetz gesendet werden.

[Quelle: Marcus Prem, http://smartphone-attack-vector.de]

Verbindungsaufbau MS – BTS - BSC

- Die Zuteilung des Funkkanals / Zeitschlitz erfolgt nur durch die BSC
- BSC wählt einen freien Kanal aus
  - Nutzkanal (TCH) und
  - Zugeordneten Signalisierkanal (SACCH)
- MS kann damit die Kommunikation konfigurieren und beginnen.

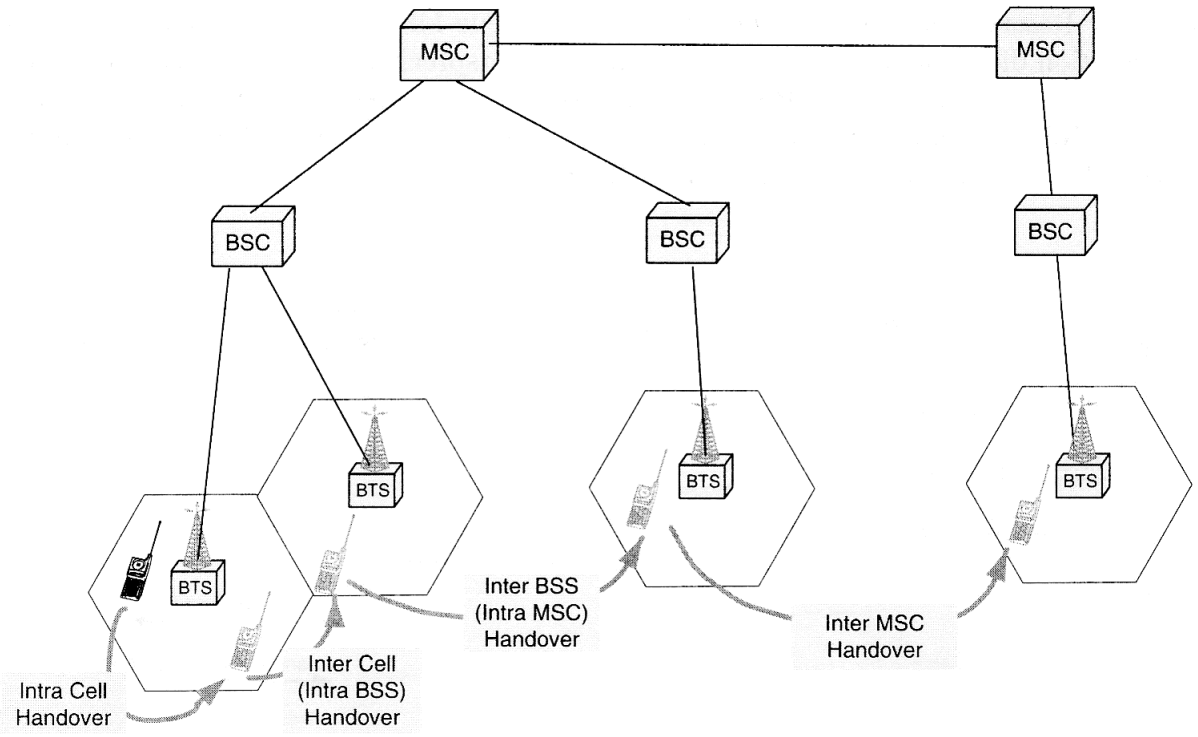


TCH: Traffic Channel
SACCH: Slow Associated Control Channel (dedicated Channel)

[Quelle: Duque-Antón, 2002]

Handover

- Handover: „Weitereichen“ der bestehenden Verbindung von einer Funkzelle zur nächsten Funkzelle: BTS (alt) ➔ BTS (neu)
- Je nach Netzstruktur:
  - Intra-Cell Handover (BTS bleibt): neue Frequenz / neuer Zeitschlitz (Administrative bedingt)
  - Inter-Cell Handover: neue BTS am gleichen BSC
  - Inter-BSS-Handover: neue BTS an anderem BSC, gleichen MSC
  - Inter-MSC-Handover: neues MCS und BCS
  - Definition des Anchor-MSC beim Verb.-Aufbau

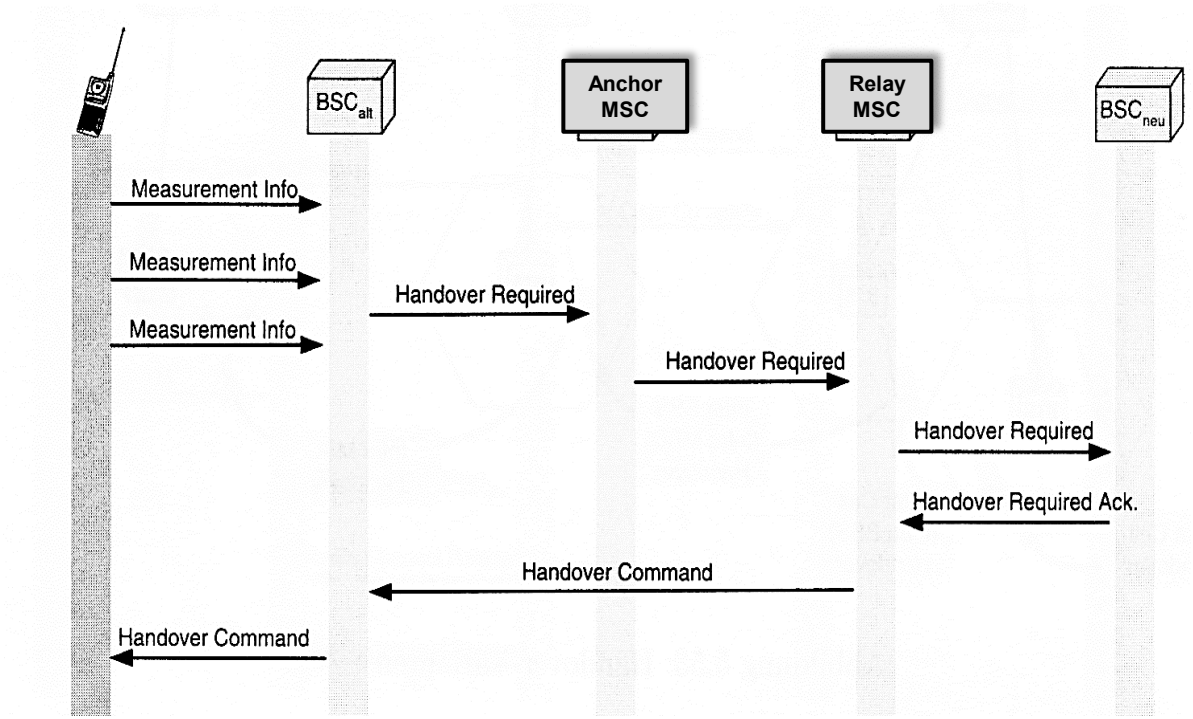


[Quelle: Duque-Antón, 2002]

Handover

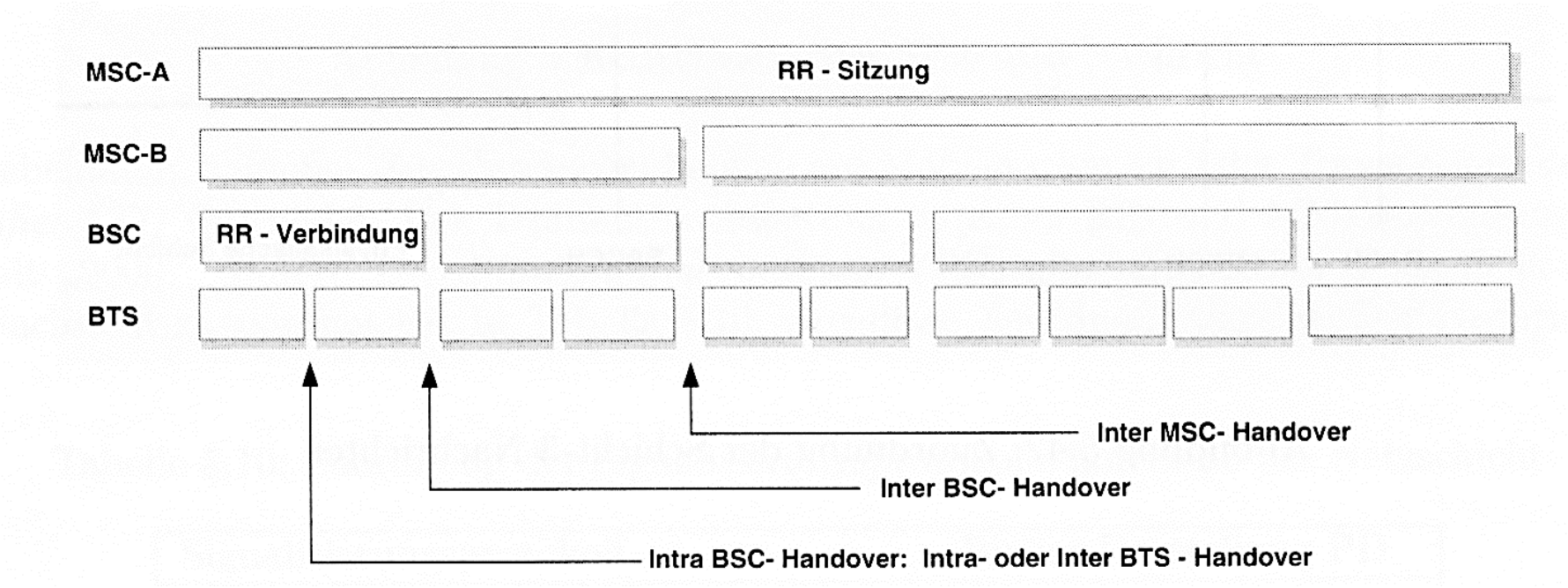
Handover:

- MS: Ständige Messung der Funkverbindungen zu allen Nachbar BTS (Signalstärke und Signalqualität)
- BSC entscheidet über Handover
- MSC wird über Messergebnisse informiert
- Inter-MSC Handover: Neue (Relay-) MSC übernimmt die Verbindung



[Quelle: Duque-Antón, 2002]

Das Anchor-MSC behält die Verbindung



- **Während einer Verbindung bleibt die Radio Ressource Session im ersten MSC bestehen ➔ „Anchor MSC“**

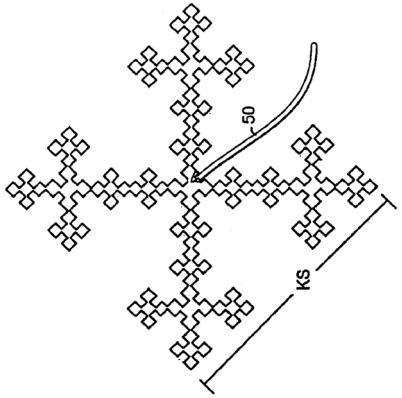
[Quelle: Duque-Antón, 2002]

Mobile Station – vom Handy zum Smartphone

- Die ersten Handys hatten 1 Antennen - zum ausziehen - für 1 Frequenz (nur GSM 900, Bsp. Siemens S4)
- Aktuelle Mobiltelefone müssen Antennen für mehrere Frequenzen besitzen (Bsp., Auszug)
  - 2G/2.5G – GSM/GPRS/EDGE: 850/900/1800/1900 MHz
  - 3G – WCDMA: 800/850/900/1900/2100 MHz
  - 4G – LTE: 700/800/850/900/1800/1900/2600 MHz
  - Wi-Fi®: IEEE 802.11 a/b/g/n/ac (2,4 und 5 GHz)
  - Bluetooth® 4.0 (2,45 GHz)
  - GPS (1.575,42; 1.227,60 und 1.176,45 MHz)
  - NFC (13,56 MHz)

Mobile Station – vom Handy zum Smartphone

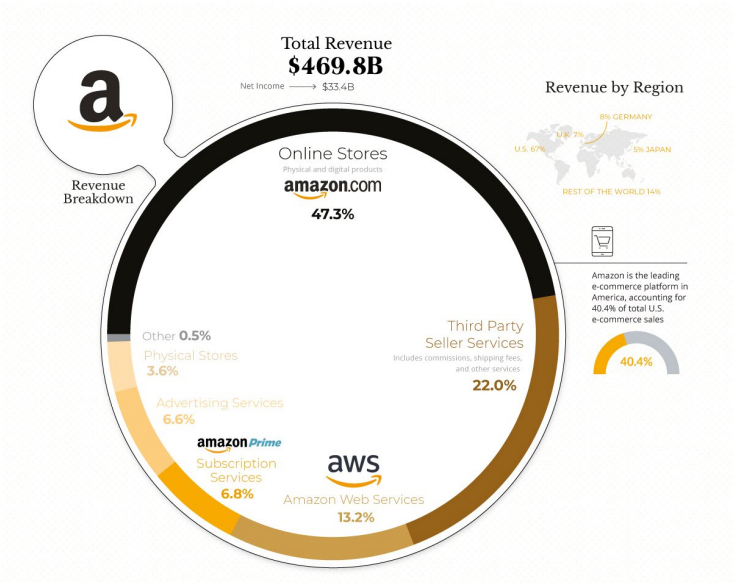
- Heute werden meist Fraktal-Antennen verwendet:
  - Wegen der Selbstähnlichkeit eines Fraktals ist für jede Wellenlänge ein Bereich mit gutem Wirkungsgrad vorhanden.
  - Ein weiterer Vorteil ist die Möglichkeit der Miniaturisierung der Antenne, die fraktale Struktur bringt eine äußerst große Kantenlänge auf sehr geringer Fläche unter, so dass auch relativ lange Wellen mit einer kleinen Antenne abgestrahlt bzw. empfangen werden können
  - Erfunden 1995

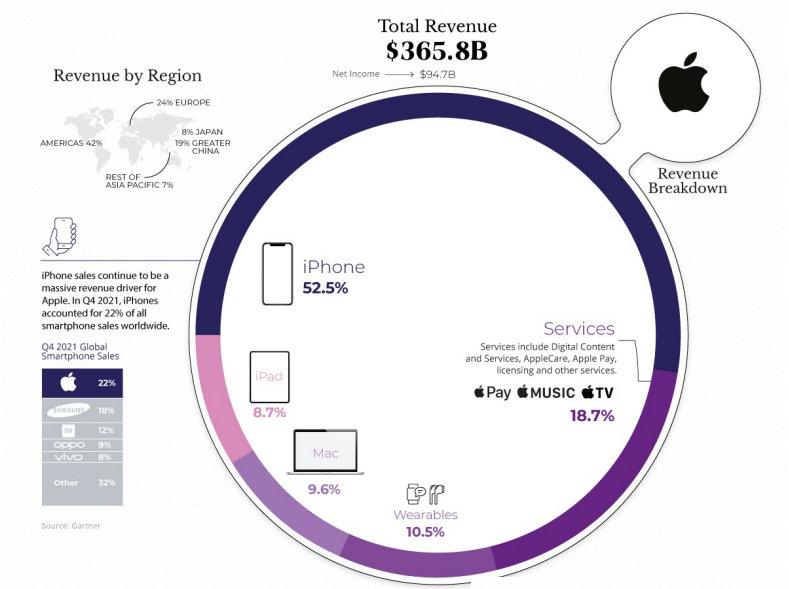


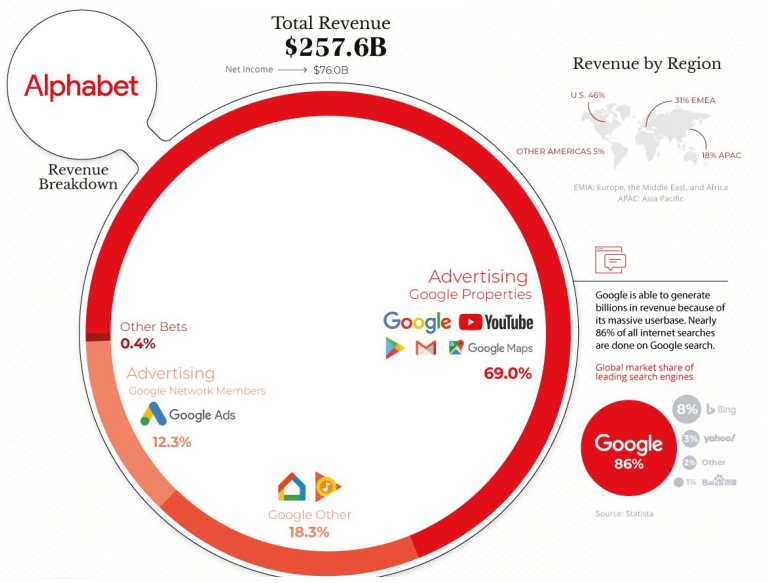
http://www.fractenna.com/our/our.html#fractalantennas

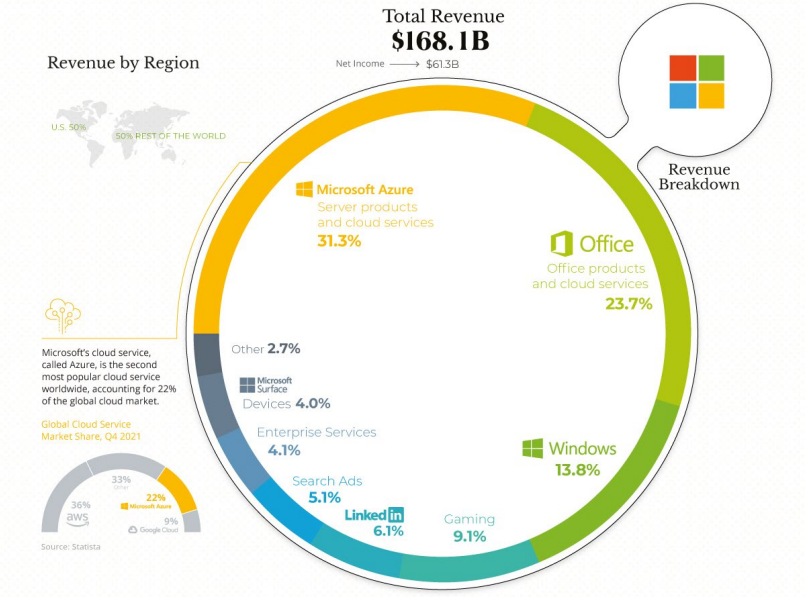
https://www.youtube.com/watch?v=g6wDRiE8JaM

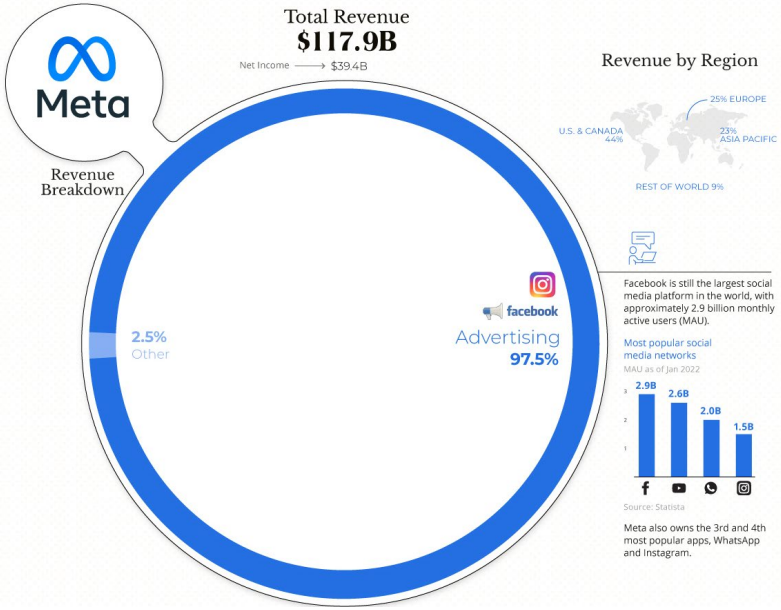
Wo kommt das Geld der Tech-Konzerne her?











https://www.visualcapitalist.com/how-big-tech-makes-their-billions-2022/

Mobilfunk-Systeme
der 2. Generation

➔ GSM
Teil 3: Sicherheitsaspekte

Grundprinzip der Sicherheit bei GSM - 1

- **Authentifizierung des Nutzers durch**
  - SIM-Karte (Besitz)
  - PIN zur SIM-Karte (Wissen)
  - Keine Bindung an das Gerät
- **Authentifizierungsverfahren**
  - Challenge / Response (Zufallszahl RAND / signierte Antwort SRES)
- **Quelle des initialen Schlüssel K_i eines Nutzers:**
  - SIM-Karte (von außen nicht lesbar)
  - AuC (Authentication Center, geschützter Bereich)
  - Der initialen Schlüssel K_i wird **nie** im Netz übertragen!
  - K_i = 128 bit Schlüssel
- **SIM-Karte enthält:**
  - Initialisierungsschlüssel K_i
  - Authentifikationsalgorithmus A3 (nicht auslesbar)
  - Verfahren A8 zur Generierung der Schlüssel K_C für Daten (Stromchiffre A5)

Grundprinzip der Sicherheit bei GSM - 2

- **Verarbeitungsweg:**
  - Das AuC erzeugt für einen Nutzer aktuelle Werte zur Authentifizierung (Werte für Challenge/ Response sowie temporären Sitzungsschlüssel K_c zur Verschlüsselung der Daten / Sprache)
  - => Authentifizierungstriplet; Authentifizierungsvektors

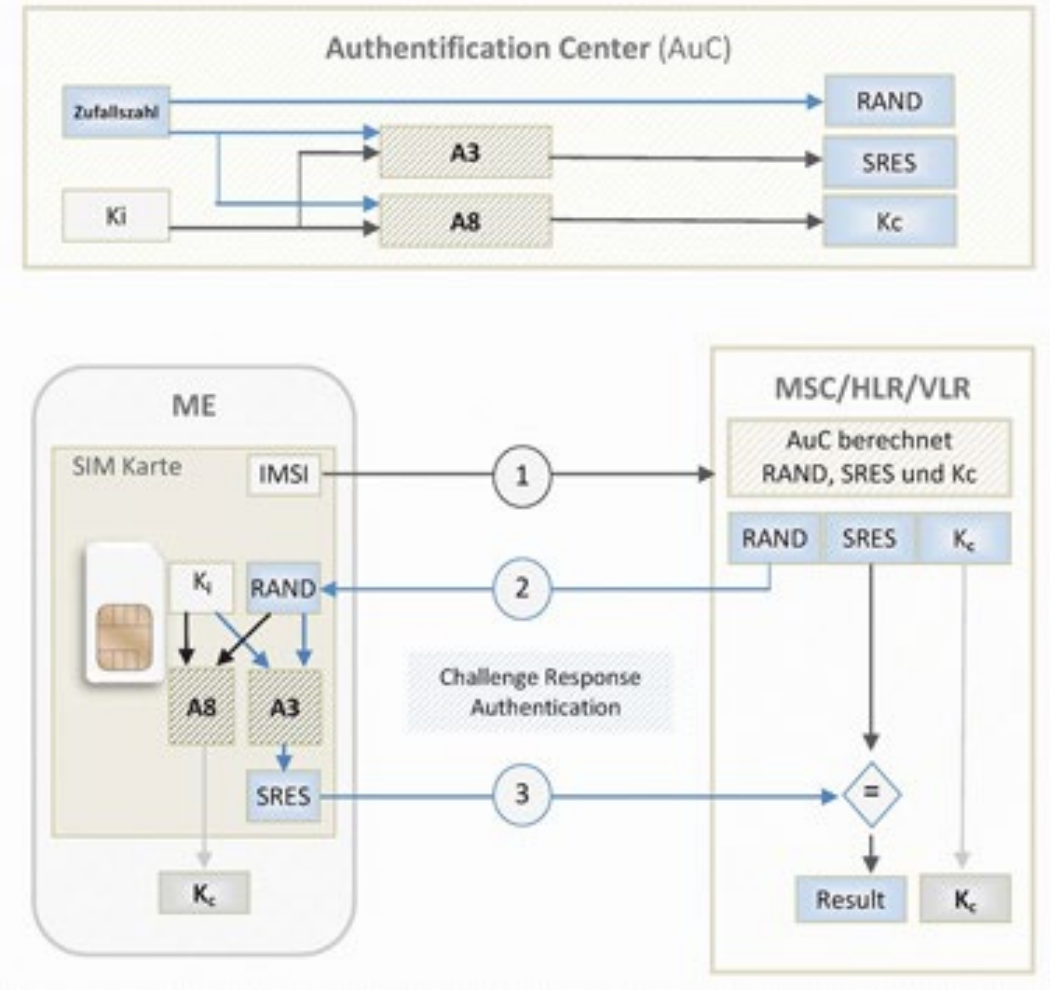
- **Ablauf beim Anmelden eines Nutzers („Einbuchen ins Netz“):**
  - Identifikation des Nutzers über die IMSI (International Mobile Subscriber Identity)
  - MSC fragt bei HLR über IMSI die Teilnehmerdaten ab (Authentifizierungstriplet von AuC)
  - Nach erfolgreicher Authentifizierung wird dieser Teilnehmer im VLR eingetragen und der aktuelle Standort dem HLR mitgeteilt.
  - Nach den erfolgreichen einbuchen wird die TMSI (Temporary Mobile Subscriber Identity) verschlüsselt an SIM übermittelt.
  - Weiter Identifikation des Nutzes / SIM nur über TMSI – damit sollen Bewegungsprofile verschleiert werden.
  - IMSI wird nicht mehr übertragen
  - TMSI wird immer wieder vom Netz gewechselt

Grundprinzip der Sicherheit bei GSM - 3

- **Verschlüsselungsalgorithmen**
- **A3:** im ROM der Sim-Karte, nicht kopierbar
  - Authentifikationsalgorithmus, Einwegfunktion, Erzeugt SRES:

  SRES = A3 (RAND, K_i)
- **A8:** im ROM der Sim-Karte, nicht kopierbar
  - Erzeugt Sitzungsschlüssel K_C:
  - K_C = A8 (RAND, K_i)
  - A3 und A8 werden vom Netzbetreiber ausgewählt
- **A5:** Verschlüsselung der Nutzdaten mit Sitzungsschlüssel K_C:
  - Verschiedene standardisierte Algorithmen:
    - A5/1 für starke Verschlüsselung
    - A5/2 für schwache Verschlüsselung (wird aktuell nicht mehr unterstützt)
    - A5/3 neu für stärkere Verschlüsslung (von UMTS übernommen)
    - A5/0 für <u>keine</u> Verschlüsselung
  - A5/2 wurde durch Reverse Engineering bekannt und 2003 wurde ein Angriff auf A5/2 vorgestellt

Anmeldeprozedur an einem GSM-Mobilfunknetz



1. Das Mobilteil sendet die IMSI an das Mobilfunknetz das seinerseits den passenden geheimen Schlüssel Ki heraussucht und daraus im Authentication Center (AuC) die Authentifikations-Triplets (RAND, SRES, Kc) berechnet.

2. Das ME erhält zunächst nur die Zufallszahl RAND. Durch die gleichen Algorithmen (A3 und A8) im AuC kann auch die SIM Karte den Hash-Wert SRES berechnen und zurücksenden.

3. Ist das Ergebnis von SRES korrekt, hat sich das ME gegenüber dem Mobilfunknetz erfolgreich Authentifiziert.

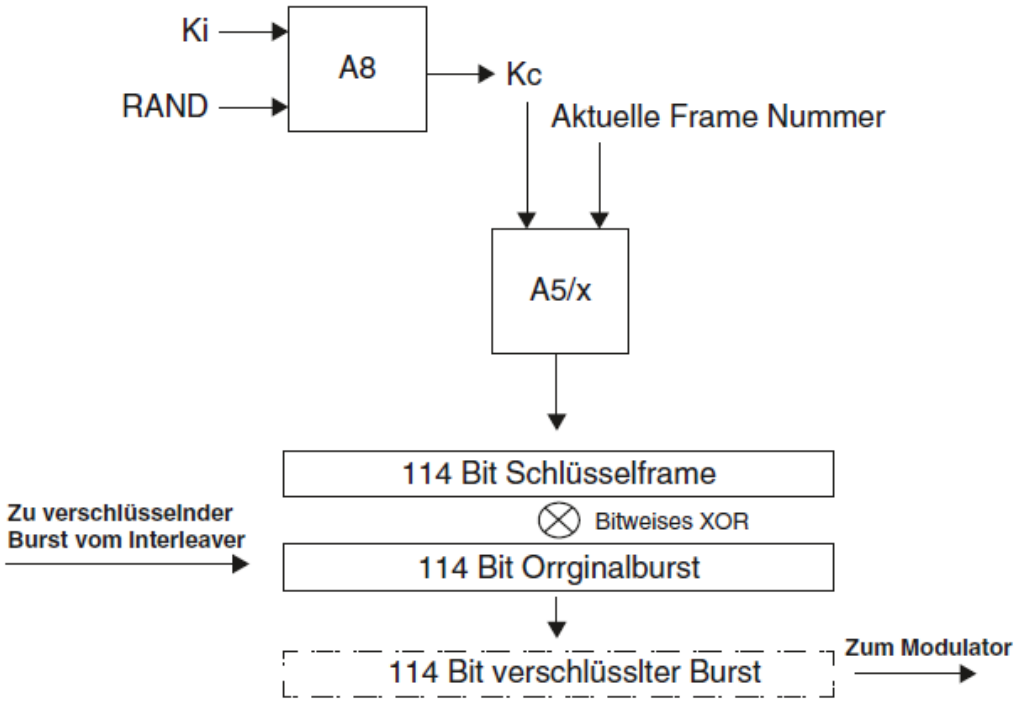
Legende:

Algorithmus | Fest-Werte | Variablen

[Quelle: Marcus Prem, http://smartphone-attack-vector.de]

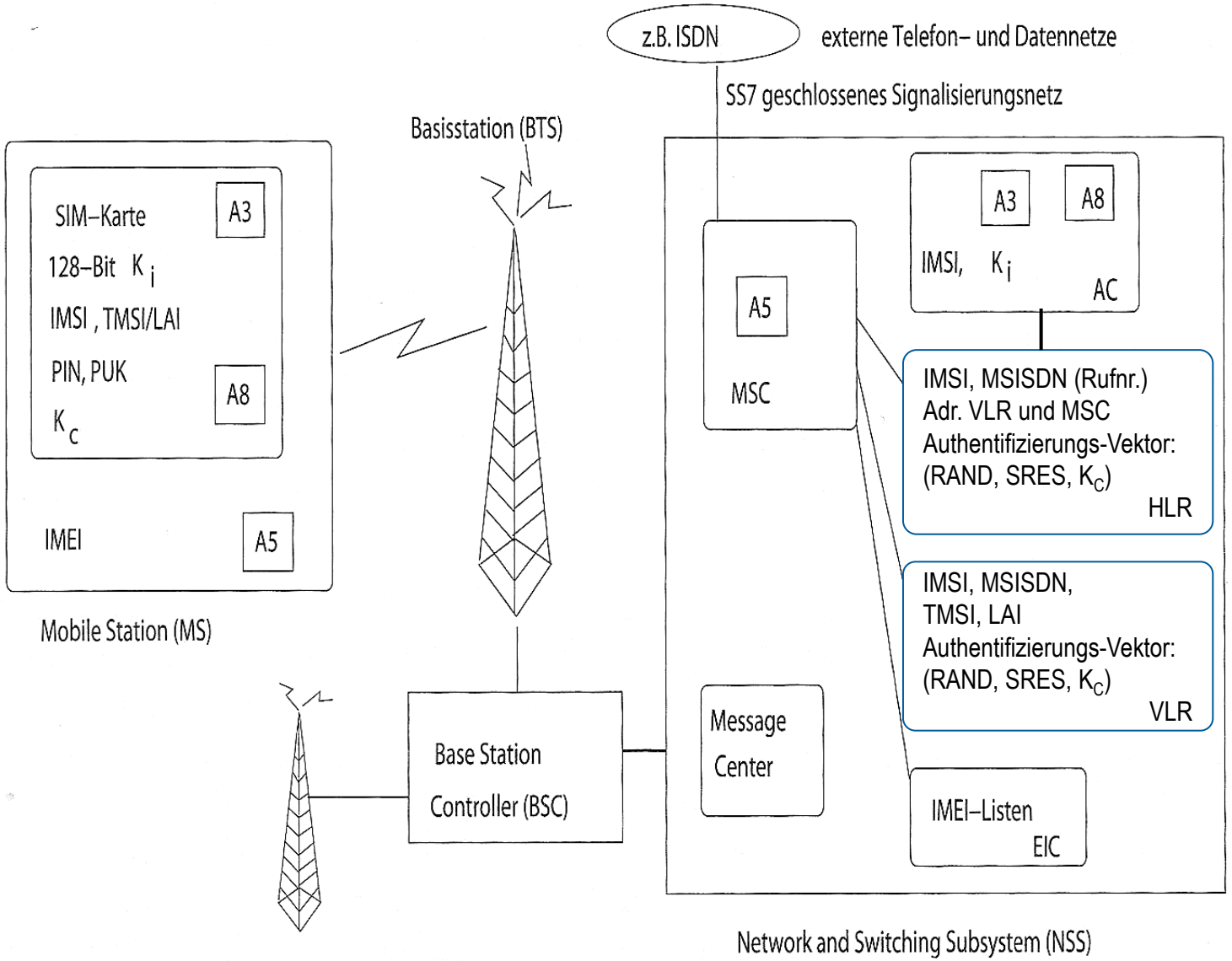
Verschlüsselung der Daten-/Sprachübertragung

- **Die codierten Sprachpaket werden vor den Senden verschlüsselt. Der initiale Schlüssel Ki ist**
  - Auf der SIM-Karte und
  - im Authentication Center im Netz
- **Aus Ki wird der Session-Key Kc errechnet. Dieser wird**
  - Der Basisstaion mitgeteilt
  - In der SIM-Karte errechnet
- Synchronisation über die aktuelle Frame Nummer
- Verschlüsselung kann optional abgeschaltet werden (wird meist nicht mehr unterstützt, da zu unsicher)



Quelle: Sauter, 2018

GSM-Architektur aus Sicht der Sicherheit



[Quelle: nach Claudia Eckert: IT-Sicherheit, 7. Aufl., korr]

GSM-Schwachstellen aus Sicht der Sicherheit

- **Nur einseitige Authentifizierung**
  - Handy kann nicht prüfen ob es mit dem richtigen Netz kommuniziert.
- **Man-in-the-middle Angriff: „IMSI-Catcher“**
  - Starkes Mobilfunksignal an Handy => Handy bucht sich ein
  - Abfangen der IMSI
  - Ausschalten der Verschlüsselung (sofern noch möglich)
  - Evtl. geknackte Verschlüsselung zum Netz nutzen
  - SMS und Signalisierung sind nicht verschlüsselt
- **Problem SS7**
  - Internationales Signalisiersystem für Telefonie (und Mobilfunk)
  - In Netz keine Überwachung (Konzept der Trusted Partner = Netzbetreiber)
  - Lokalisierungsdaten / Autorisierungsdaten (temp. Authorisierungsvektoren) werden unverschlüsselt übertragen.
  - Betreiber können Standorte der Nutzer abfragen (=> Vortrag Tobias Engel, CCC)
  - Zugriff auf SS7 ist über „dubiose Kanäle“ kaufbar
  - Betreiber versuchen die Angriffe durch Plausibilitätschecks einzugrenzen (Dank CCC)

GSM-Angriffsvektoren - 1

- **Modem / Baseband:**
  - Angriffsmethoden auf den Baseband-Prozessor werden in den letzten Jahren immer häufiger veröffentlicht. Zunächst muss eine Verbindung zum Smartpone hergestellt werden. Hierfür gibt es bekannte Lösungen (➔ „IMSI-Catcher“). Damit kann der Angreifer auch aus großer Entfernung auf das Smartphone zugreifen.
- **Roving Bug:**
  - Die als „Roving-Bug“ bekannte Angriffsmethode wurde im Jahre 2006 das erste Mal offiziell eingesetzt [Fraunhofer-Instituts für Sichere Informationstechnologie (SIT) und auch im BSI-Gefährdungskatalog beschrieben]. Hierbei wird das Mikrofon des Mobiltelefons aktiviert und die Audiosignale an einen Server übertragen. Evtl wurde dieser Angriff über “Firmware-over-the-air” (FOTA) realisiert und dadurch der Schadcode installiert.
- **COO-Ortung:**
  - Die vom Mobilfunknetz initiierte Ortung dient unter anderem zur Messung der Signalqualität am aktuellen Standort des Smartphones.
  - Details: Bei einem Anruf über die Notrufnummer “112” muss der Anrufer unmittelbar und zuverlässig geortet werden. Dies wird mittels E-OTD (Enhanced Observed Time Difference) Messungen realisiert. E-OTD berechnet den zeitlichen Unterschied beim Eintreffen der Broadcasts der Basisstationen beim Mobilteil. Bei UMTS wird das System als „Observed Time Difference of Arrival“ (OTDOA) bezeichnet. Es gibt keinerlei Sicherheitsmechanismen, damit eine sofortige Messung nicht verzögert oder gar verhindert wird.

[Quelle: Marcus Prem, http://smartphone-attack-vector.de]

GSM-Angriffsvektoren - 2

- **IMSI/LAI im Klartext:**
  - Das Smartphone sendet, z.B. bei der ersten Verbindungsaufnahme die unverschlüsselte IMSI der SIM -Karte und die LAI (Location Area Identifer) der letzten Verbindung mit einer Basisstation.
- **Störfunk/Jammer**
  - Durch das Stören der UMTS-Frequenzbänder wir der Wechsel auf GSM Standard erzwungen. (Teilfunktion bei Semi-Aktiven Abhöranlagen)
  - Es ist aber auch ein kompletter „Denial of Service“ aller Funkverbindungen möglich.
- **Stille SMS**
  - Eine Stille SMS (Silent SMS, Stealth-SMS) ist für den Empfänger nicht zu erkennen. (nicht auf dem Display angezeigt und auch kein akustisches Signal). Wie bei einem Ping auf eine Netzwerkadresse, antwortet das mobile Endgerät mit einer Quittung. Zur Ortung eines Smartphones benötigt man jedoch die dabei angefallenen Verbindungsdaten.
  - Diese Methode wird sehr häufig von Behörden genutzt um den Aufenthaltsort von Personen fest zu stellen. Es können aber auch " Denial of Service" (DoS) Angriffe durchgeführt werden.
- **“Location Leaks” und SS7:**
  - Eine Stille SMS kann zur Ortung eingesetzt werden, wie oben beschrieben. Um die Verbindungsdaten auswerten zu können, muss jedoch ein weiterer Zugriffspunkt direkt beim Provider bestehen. Damit könnte die aktuelle Cell-ID ermittelt werden, in der sich das Smartphone gerade befindet.
- **… und weitere …**

[Quelle: Marcus Prem, http://smartphone-attack-vector.de]

Mobilfunk-Systeme
der 2,5. Generation

➔ GPRS, EDGE

Weiterentwicklung von GSM

- **GSM**
  - Designed und optimiert für Sprachverbindungen
  - bietet nur durchschalte-vermittelte Kanäle bis 9,6 kbit/s
  - mit fester Bandbreite und
  - Abrechnung nach Nutzungs**dauer** (wie Telefondienst)
  - Modulation (GSMK) ist zwar robust und für große Entfernungen geeignet, hat aber eine schlechte spektrale Effizienz (~1 bit/Hz)
  - Erster „schneller“ Datenservice durch Kanalbündelung: HSCSD mit bis zu 64 kbit/s (High Speed Circuit Switched Data)
- **Anforderungen der Nutzer (Internetzugang):**
  - Datenverkehr, Internetzugang, IP
  - Burstartiger Verkehr
  - Lange Onlinezeiten
  - Sporadische Nutzung
  - Mehrere parallele Sessions
  - Abrechnung nach Datenvolumen, nicht nach online Zeit erwünscht

Weiterentwicklung von GSM: GPRS

- **Entwicklung vom General Packet Radio Service (GPRS):**
  - Paketvermittlung mit virtuellen Verbindungen
  - Neue Struktur für die Funkkanäle definiert:
    - Größere Bandbreite durch Zusammenlegen der vorhandenen Kanäle (1 – 8)
    - Kompatibel zur vorhandenen Kanalstruktur durch Bündelung der TDMA-Kanäle eines Frequenz-Kanals
    - Packet Data Traffic Channel (PDTCH) besteht aus 4 aufeinader folgenden Timeslots,
    - Diese wurden jeweils einem Teilnehmer für die Datenpaket-Übertragung zugeteilt.
    - Gleichzeitige Nutzung dieses Kanals durch mehrere Teilnehmer auf Anforderung
    - Adaptive Anpassung (dynamisch / administrativ) Voice / Data
    - Verzögerung der Kapazitätszuweisung im Paketkanal 500…700 ms
  - Neues Codierschema
    - Qualität der Funkverbindung bestimmt Codierschema (Anteil Prüfbits zur Fehlerkorrektur)
      4 Codierschema:
      bis max. 171 kbit/s / Kanal
  - Multislot-Klassen
    (auch asymmetrisch)
  - Modulation: GSMK: 1 Bit/Symbol

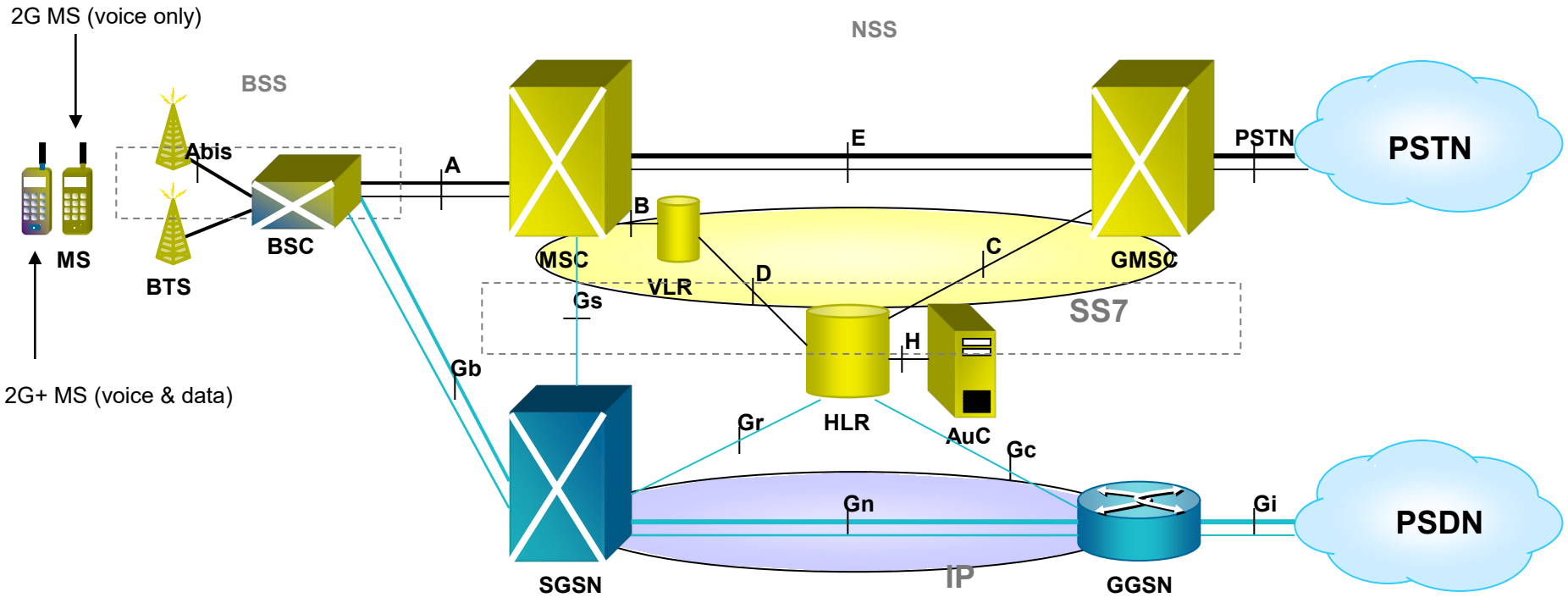
Codier-schema	Coderate	Pro Zeitlage	Max (8 Zeitlagen)
CS-1	0,5	9,05 kbit/s	72,4 kbit/s
CS-2	0,66	13,5 kbit/s	107,2 kbit/s
CS-3	0,75	15,6 kbit/s	124,8 kbit/s
CS-4	1,00	21,4 kbit/s	171,2 kbit/s

Weiterentwicklung von GPRS: EDGE

- **Erhöhung der Datenrate von GPRS mit EDGE (EDGE: Enhanced Data Rates for GSM Evolution)**
- **Änderung der Modulation (GMSK => 8-PSK)**
  - 8-PSK überträgt 3 Bit / Symbol
  - Signalamplitude trägt auch Information => genau Leistungsregelung ist erforderlich
  - Guter Übertragungsweg und wenig Störungen (kleiner Funk-Zellen) erlauben hohe Datenraten
  - Konstante Messung der Signal-Stärke und Signal-Qualität und genaue Anpassung der Modulation und des Coding Schemes (MSC)
  - BSS verteilt alle Kanäle:
    - GSM für Voice
    - GPRS / EDGE in den Kanälen für Daten die zu Packet Data Channel (PDCH) zusammengefasst werden.
    - Zahlreiche Kanalkombinationen sind möglich

	Modulation	Geschwindigkeit pro Timeslot
EDGE MSC-1	GMSK	8,8 kbit/s
EDGE MSC-4	GMSK	17,6 kbit/s
EDGE MSC-5	8-PSK	22,4 kbit/s
EDGE MCS-9	8-PSK	59,2 kbit/s

GPRS-Erweiterung für den Datenverkehr



BSS — Base Station System
BTS — Base Transceiver Station
BSC — Base Station Controller

NSS — Network Sub-System
MSC — Mobile-service Switching Controller
VLR — Visitor Location Register
HLR — Home Location Register
AuC — Authentication Server
GMSC — Gateway MSC

SGSN — Serving GPRS Support Node
GGSN — Gateway GPRS Support Node

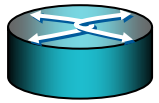
GPRS — General Packet Radio Service

[Quelle: Brough Turner & Marc Orange, 3G Tutorial]

Serving GPRS Support Node, SGSN

- Die BSC koppeln die GPRS-Paketdaten in der Packet Contol Unit (PCU) aus und leiten diese über IP-Verbindungen an den zuständigen Serving GPRS Support Node (SGSN) weiter. Jeder SGSN verwaltet den GPRS-Datenverkehr für eine größere Anzahl von BSCen.
- Ein SGSN hat für GPRS-Datenkommunikation eine ähnliche Funktion wie ein MSC für Sprachkommunikation. Der SGSN organisiert das Einbuchen von Teilnehmern für GPRS-Dienste, organisiert den Wechsel von Funkzellen und SGSN-Bereichen (GPRS-Routing Area Update bzw. GPRS-Cell Reselection) und organisiert das Routing von GPRS-Daten.
- SGSN-Schnittstellen:
  - IP-Schnittstellen zu den BSC (früher auch ATM-Schnittstelle)
  - SS7- und SIGTRAN-Strecken (SS7 over IP) zum eigenen Signalisierungsnetz, um z. B. mit Hilfe der HLR Teilnehmerdaten und -standorte zu verwalten und Service-Knoten des GSM-Netzes ansprechen zu können.
  - IP-Strecken zu weiteren GPRS-Netzelementen, wie z. B. dem GGSN um Daten mit dem Internet, Firmennetzen, usw. austauschen zu können.

Gateway GPRS Support Node, GGSN



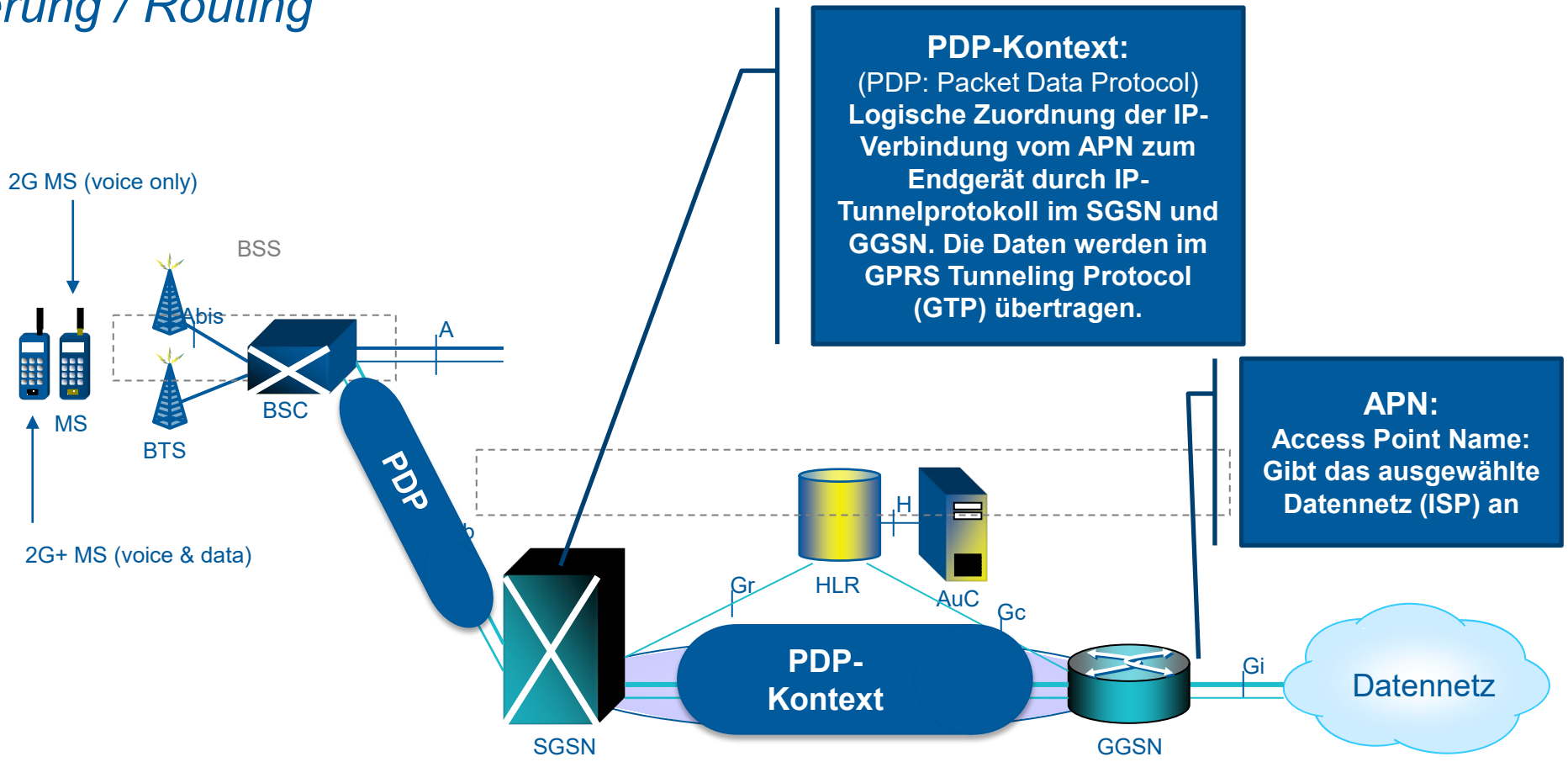
GGSN

- Die **GGSN (Gateway GPRS Support Node)** stellen die GPRS-Datenverbindungen zu netzinternen Diensteplattformen oder zu Datennetzen her.

- **GGSN-Schnittstellen:**
  - Schnittstellen zu den SGSN des eigenen Netzes
  - Schnittstellen zu den SGSNs ausländischer GPRS-Netze, um den eigenen Teilnehmern die Nutzung der GPRS-Dienste vom Ausland aus zu ermöglichen.
  - Schnittstellen zu Online-Abrechnungssystemen (Traffic Analyser, Charging Gateway), um GPRS-Benutzung mengenmäßig oder auch zielspezifisch abrechnen zu können.
  - Schnittstellen zu GPRS-Diensteplattformen (z. B. WAP-Server, MMSC)
  - Schnittstellen zu Datennetzen (Internet, Firmennetze)

- Der Zugang zum GPRS-Netz erfolgt über einen Zugangspunkt, der **APN** (Access-Point-Name) genannt wird. Die Zuordnung von APN zu einem Teilnehmer erfolgt über die Teilnehmerdaten, die im HLR gespeichert werden. Ein Teilnehmer kann dabei mehrere APN nutzen.

IP-Adressierung / Routing



PDP-Kontext:
(PDP: Packet Data Protocol)
Logische Zuordnung der IP-Verbindung vom APN zum Endgerät durch IP-Tunnelprotokoll im SGSN und GGSN. Die Daten werden im GPRS Tunneling Protocol (GTP) übertragen.

APN:
Access Point Name: Gibt das ausgewählte Datennetz (ISP) an

BSS — Base Station System
BTS — Base Transceiver Station
BSC — Base Station Controller

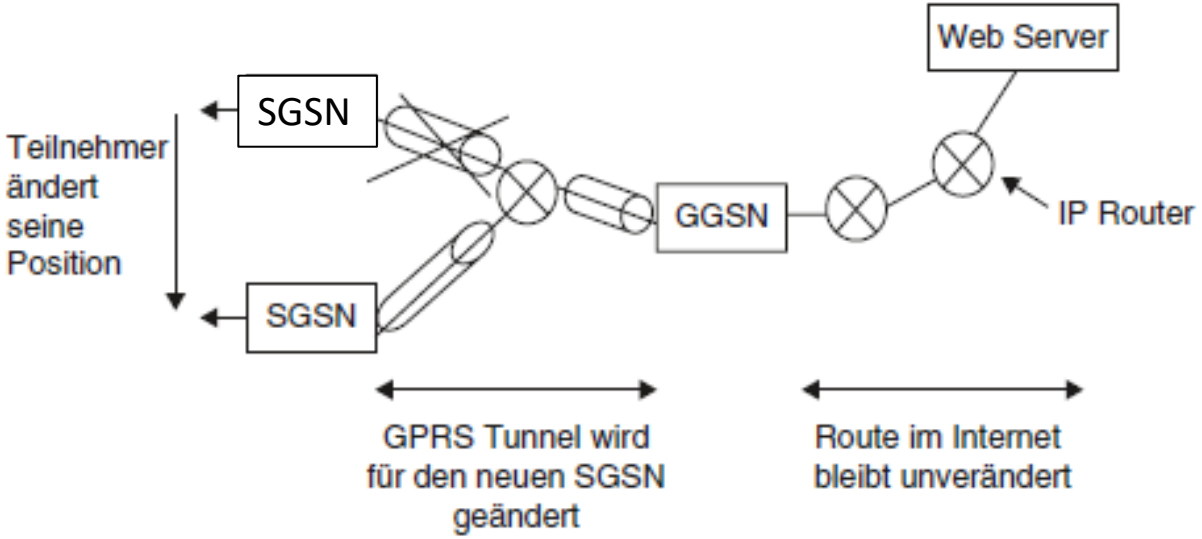
NSS — Network Sub-System
MSC — Mobile-service Switching Controller
VLR — Visitor Location Register
HLR — Home Location Register
AuC — Authentication Server
GMSC — Gateway MSC

SGSN — Serving GPRS Support Node
GGSN — Gateway GPRS Support Node

GPRS — General Packet Radio Service

[Quelle: Brough Turner & Marc Orange, 3G Tutorial]

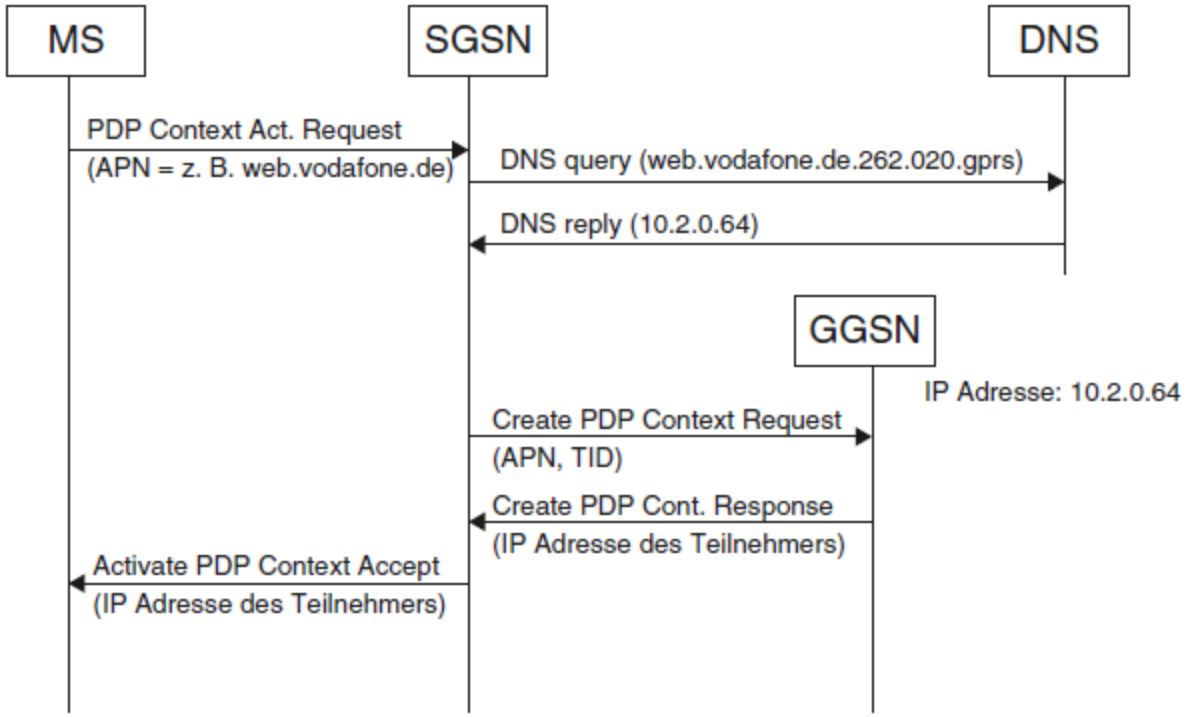
PDP-Context Aktivierung durch Smartphone



- GGSN bleibt stabil (Anchor Point) für eine IP-Verbindung
- Der PDP-Tunnel wird zum aktuellen SGSN weitergereicht
- Mobilität des Teilnehmers ist im Internet nicht sichtbar

[Quelle: Sauter, 2018]

PDP-Context Aktivierung durch Smartphone



- APN: Access Point Name (international eindeutiger Name des IP-Netzzugangs für Mobilfunkteilnehmer, Bsp: internet.telekom.de)
- TID: Tunnel ID (Kennzeichnung des „PDP-Tunnels“ im Mobilfunknetz (vereinfacht)

[Quelle: Sauter, 2018]

Grundprinzip der Sicherheit bei GPRS

- **Nutzdaten (IP)** werden in Datenframes (wie Voice) aufgespalten und unabhängig voneinander übertragen
- Reassembly zu IP-Paketen im SGSN
- Verschlüsselung der Nutzdaten entspricht GSM Voice und enthält die aktuelle Frame-Nummer
- Entschlüsselung der Nutzdaten erst im SGSN (nicht Basisstation wie bei Voice), da durch das parallele Senden in mehreren Timeslots die Reihenfolge / Framenummer erkannt werden muss.
- Einbuchen bei GPRS: wie bei GSM – aber beim SGSN!!
- SGSN empfängt vom HLR das Authentifizierungstriplet und verwaltet diese Info.
- Prozedur wie bei GSM
- Temporäre Teilnehmerkennung TLLI (Temporary Logical Link Identifier) anstatt TMSI
- GPRS verwendet zur Verschlüsslung der Nutzdaten den A5/3
- Gefahr: Jedes Smartphone hat eine IP-Adresse und ist i.a. ständig online

=> Angriffe aus dem Internet sind möglich