

GSM

Global System for Mobile communications

Fachhochschule Wedel
Seminar Mobile Computing
Oliver Grote
09. November 2004

- Einführung
- Systemarchitektur
- Luftschnittstelle
- Lokalisierung
- Handover
- Weiterentwicklungen

- Einführung
- Systemarchitektur
- Luftschnittstelle
- Lokalisierung
- Handover
- Weiterentwicklungen

1982 Gründung der Groupe Spéciale Mobile

- Standardisierung für den Massenmarkt
- Automatisches Handover
- Roaming über Landesgrenzen hinweg

1987 Memorandum of Understanding (MoU)

- Start mit 13 Teilnehmern aus 12 Staaten
→ schnell weitere Teilnehmer
- Gemeinsamer digitaler Mobilfunkstandard
- Aufbau eines Mobilfunknetzes (zunächst nur Europa)

1989 Koordination durch ETSI

- European Telecommunication Standard Institute
- Umbenennung des Standards in Global System for Mobile communications (GSM)
- Spezifikation umfasste mehrere Tausend Seiten
- Festlegung von Standards
 - GSM 900
 - DCS 1800 / GSM 1800
 - GSM 1900 (USA) → Triband-Handy

1992 In Deutschland gehen D1 und D2 in Betrieb

- E-Plus folgt 1994, E2 1998

Erfolgreichstes Mobilfunksystem weltweit

- 820 Mio. Teilnehmer in 190 Ländern (2003)
 - Weltweit eindeutige Nummernkreise
 - Abkommen für internationales Roaming
- Übertragung von Sprache und Daten
- Hohe Kapazität bei kleinen Funkzellen
- Handover ohne Abbruch der Verbindung
- Integriertes Sicherheitskonzept
 - Keine Ende-zu-Ende Sicherheit
 - Funkschnittstelle angreifbar
 - Datenverschlüsselung

Short Message Service (SMS)

Wireless Application Protocol (WAP)

Verbindungen in das Internet

- Nutzung von E-Mail
- Laden von Dateien

Schnelle Datenübertragung per HSCSD/GPRS

Neue Dienste

- i-mode (große, farbige Anzeigen)
- Multimedia Message Service (MMS)

- Einführung
- **Systemarchitektur**
- Luftschnittstelle
- Lokalisierung
- Handover
- Weiterentwicklungen

Architektur der Telekommunikation

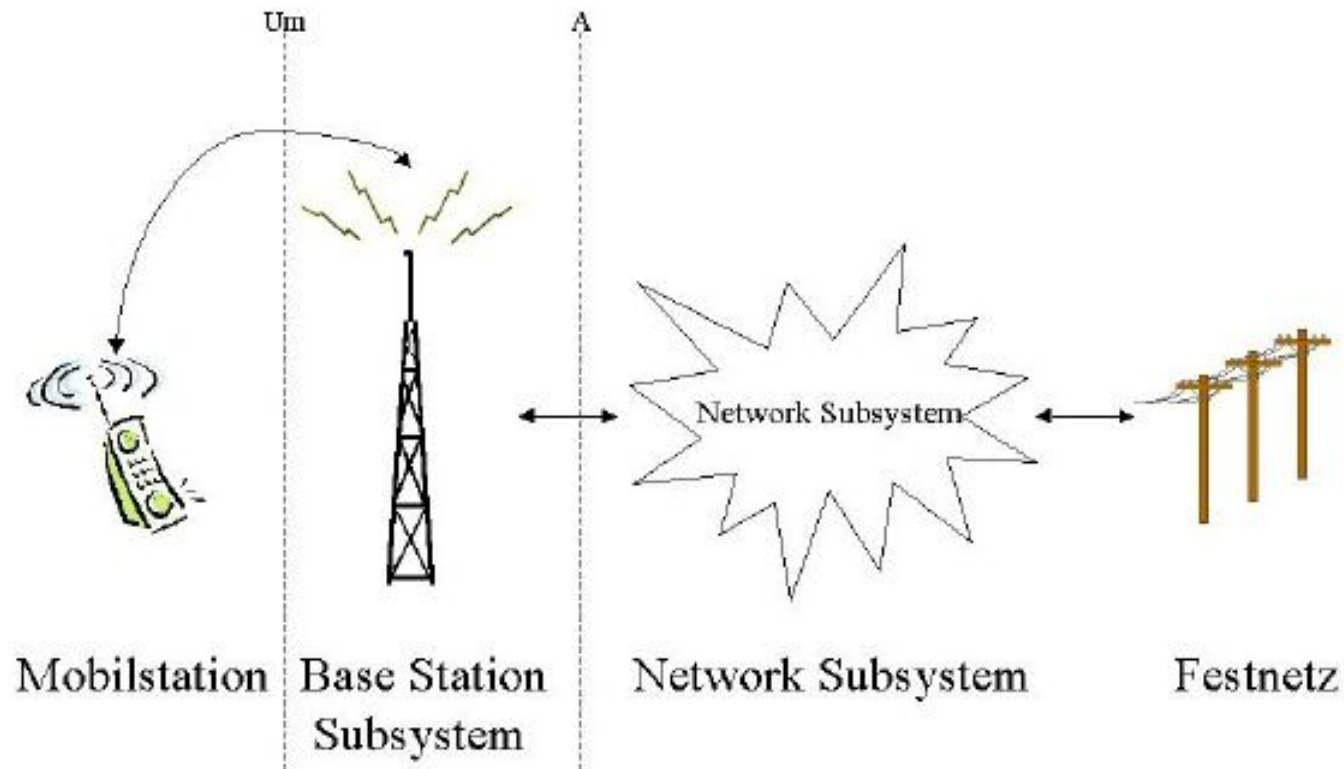
- hierarchisch
- teilweise komplex

Aufbau

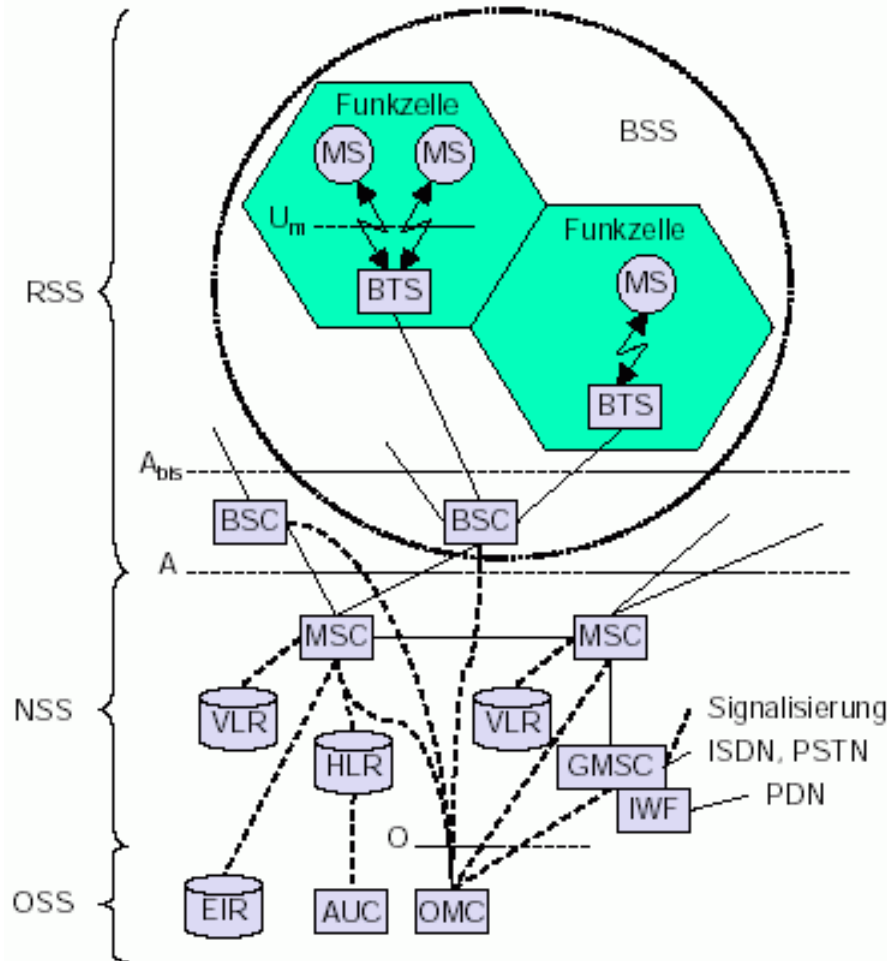
- Subsysteme
 - Funk
 - Vermittlung
 - Administration
- Schnittstellen

Standard festgelegt durch ETSI 1991

Einfaches GSM-Netz



Funktionale Architektur



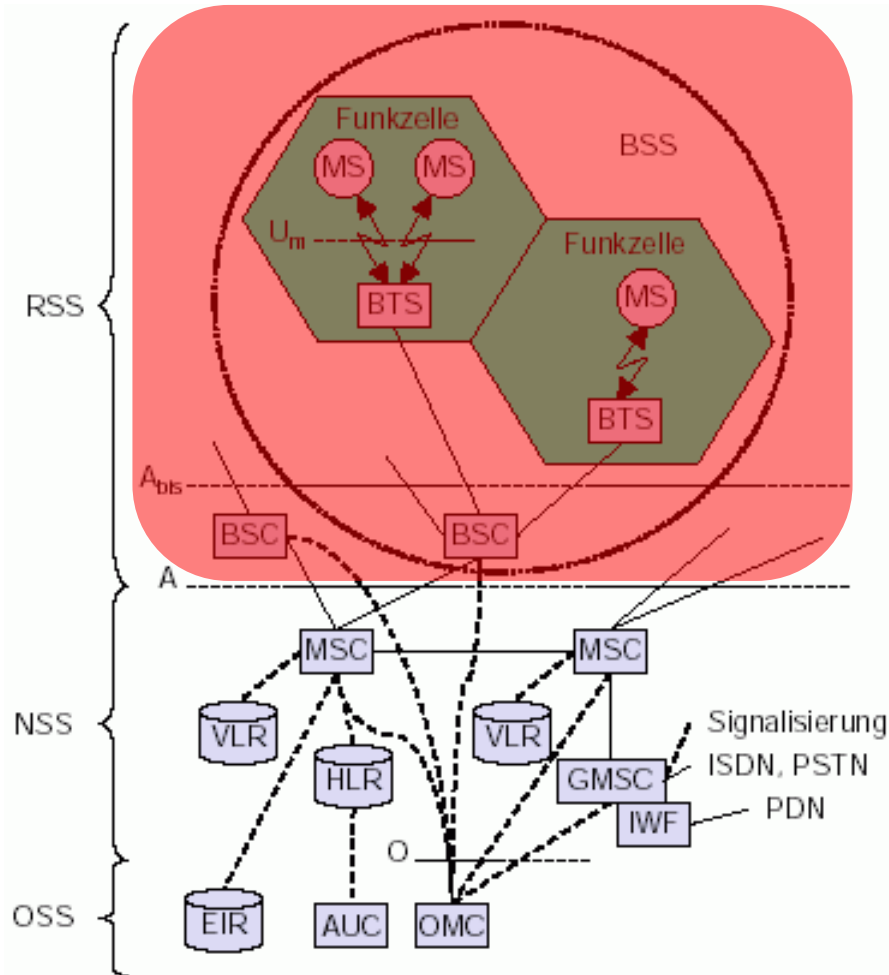
Funkspezifische Komponenten

- Mobilstationen (MS) → Handys
- Radio Access Network (RAN)
 - Base Transceiver Stations (BTS)
 - Base Station Controller (BSC)

Aufgaben

- Kommunikation per Funk
 - Signale der Mobilteilnehmer aufnehmen
 - Mobilteilnehmer mit Signalen versorgen
 - Signale den Vermittlungsstellen verfügbar machen
- Funktionen für Mobilität bereitstellen

Funk-Feststationssystem (RSS)



Feststationssystem (BSS)

- Mehrere dieser Standortbereiche bilden das RAN
- Steuerung durch einen Controller (BSC)
- Aufgaben
 - Permanente Funkverbindung zur MS realisieren
 - Sprachdaten kodieren und dekodieren
 - Datenraten vom/zum drahtlosen Netz anpassen

Sende-/Empfangsstation (BTS)

- Transceiver = „Transmitter“ + „Receiver“
→ nur wenige zusätzliche Komponenten
- Technische Einrichtungen für eine GSM-Zelle
 - Funkantennen / Verstärker
 - Elektronische Signalverarbeitung
- Realisierung der Funkverbindung zur MS
 - Funkanbindung über Luftschnittstelle
 - Daten auf Hochfrequenz modulieren
 - Setzung des TDMA-Zeitrahmens
- Zellenradius maximal 35 Kilometer

Sende-/Empfangsstation (BTS)



Zwei Netzanbieter

Funk-Feststationssystem (RSS)

Sende-/Empfangsstation (BTS)



Finde die Antenne ...

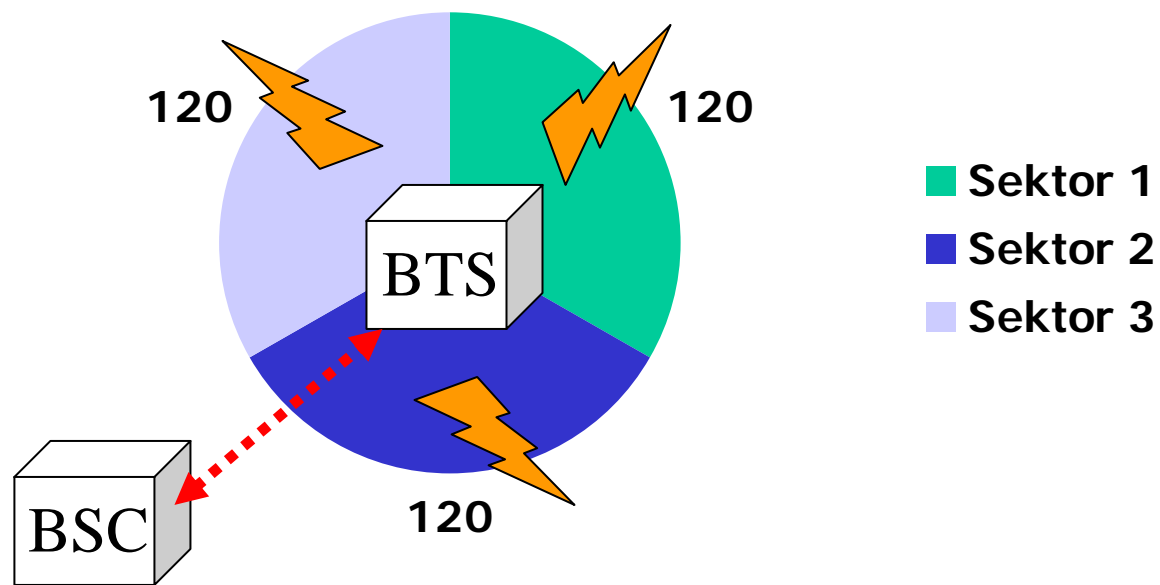
Sende-/Empfangsstation (BTS)



Insgesamt 43 Antennen

Sende-/Empfangsstation (BTS)

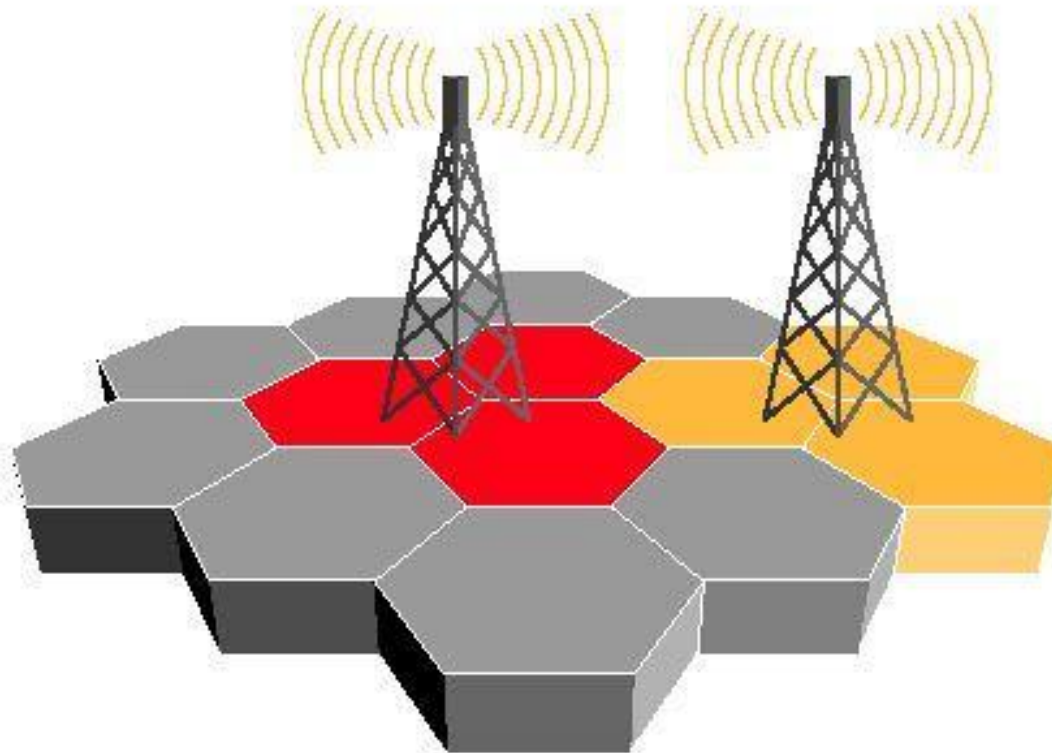
Sektorisierung



Sende-/Empfangsstation (BTS)

- Durch Sektoren kann mehr als eine Zelle durch die BTS verarbeitet werden
- Im Normalfall werden 3 Sektoren gebildet
→ Antennen mit 120° Sende-/Empfangscharakteristik
- Vorteile von Sektorbildung
 - Nur eine Schnittstelle zum BSC für mehrere Zellen
 - Nur ein Antennenmast für mehrere Sektorantennen
 - Geographisches Gebiet durch Richtcharakteristik besser konfigurierbar → Interferenzen minimieren

Sende-/Empfangsstation (BTS)



Bildung von 3 Sektoren

Feststationssteuerung (BSC)

- Kontrolleinrichtung für regionale Zusammenfassung
- Fungiert für die zugehörigen Zellen als Datenbank
- Leitet Informationen an Vermittlungsstelle weiter
- Verwaltet typischerweise 30 bis über 100 BTS
- Auslagerung wesentlicher Steuerungsaufgaben
 - Funkressourcen angeschlossener BTS managen
 - Kontrolle der Sendeleistung von MS und BTS→ Verbindungsübergabe innerhalb des BSS (Handover)
 - Multiplexing der Funkkanäle auf Festnetzverbindung

Feststationssteuerung (BSC)



Mobilstation (MS)

- Hard- und Software eines Endgeräts für die Kommunikation mit GSM
- Zwei Komponenten
 - Mobile Equipment (ME)
→ nutzerunabhängige Komponente
 - Subscriber Identity Module (SIM)
→ nutzerspezifische Einheit

Mobile Equipment (ME)

- Prinzipiell volle technische Funktionalität
- Keine GSM-Dienste (außer Notrufnummern)
- Besitzt eindeutige Gerätekennung
 - International Mobile Equipment Identity (IMEI)
- Typische Sendeleistung
 - 2 Watt bei GSM 900
 - 1 Watt bei GSM 1800
- Vielfalt von Funktionalität möglich
 - Digitale Bildaufnahme
 - Radio / MP3-Player
 - Kalender / Notizbücher
 - ...



Subscriber Identity Module (SIM)

- Unveränderliche Daten
 - Kartentyp / Seriennummer
 - Zusätzlich abonnierte Dienste
 - International Mobile Subscriber Identity (IMSI)
 - Rechnungsstellung
 - Authentifizierung
 - Roaming
 - Entsperrungsschlüssel
 - Personal Identity Number (PIN)
 - PIN Unblocking Key (PUK)
 - Verwendete Sprache



Subscriber Identity Module (SIM)

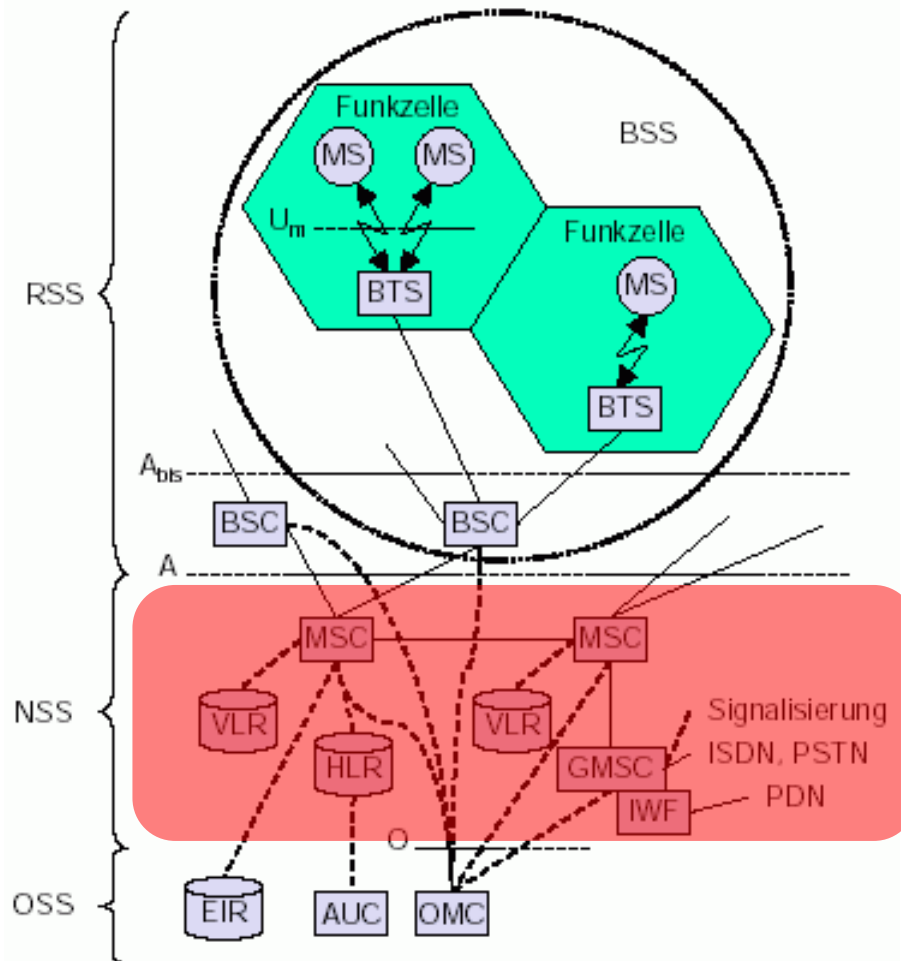
- Dynamische Daten
 - Aufenthaltsinformationen
 - Temporary Mobile Subscriber Identity (TMSI)
 - Location Area Identification (LAI)
 - Status der Aktualisierung
 - Sicherheitsdaten
 - 128 Bit Zufallszahl
 - Schlüssel zur Datenverschlüsselung K_c
 - Liste der Trägerfrequenzen für Verbindung / Handover
 - Wartezeit der MS sich in ein neues Netz einzuwählen, falls das Heimatnetz nicht erreichbar ist



Kernelement des GSM-Systems

- Verbindung der mobilen kabellosen Netze mit öffentlichen Festnetzen
- Verbindungsübergabe zwischen verschiedenen BSS
→ Handover
- Funktionen für weltweite Ortung von Teilnehmern
- Unterstützung von Roaming zwischen verschiedenen Netzbetreibern in unterschiedlichen Ländern
→ häufig keine Unterstützung von nationalem Roaming aus wirtschaftlichen Interessen
→ In Deutschland kann das GSM-900-Netz auch von Konkurrenten des GSM-1800-Netz mitbenutzt werden

Mobilvermittlungssystem (NSS)



Dienstvermittlungsstellen (MSC)

- Zuständig für mehrere BSC einer Region
- Vernetzung mit anderen MSC (Koppelnetz)
- Mobilitätsmanagement
 - Vermittlung geographisch frei beweglicher Teilnehmer
 - Routing für eine Gesprächsleitung
 - Umschaltung zwischen BSC bei Handover
- Verbindungs- und Signalisierungssteuerung mit SS7
- Unterstützung von GSM-Zusatzfunktionen
 - Anrufweiterleitung
 - Konferenzschaltung

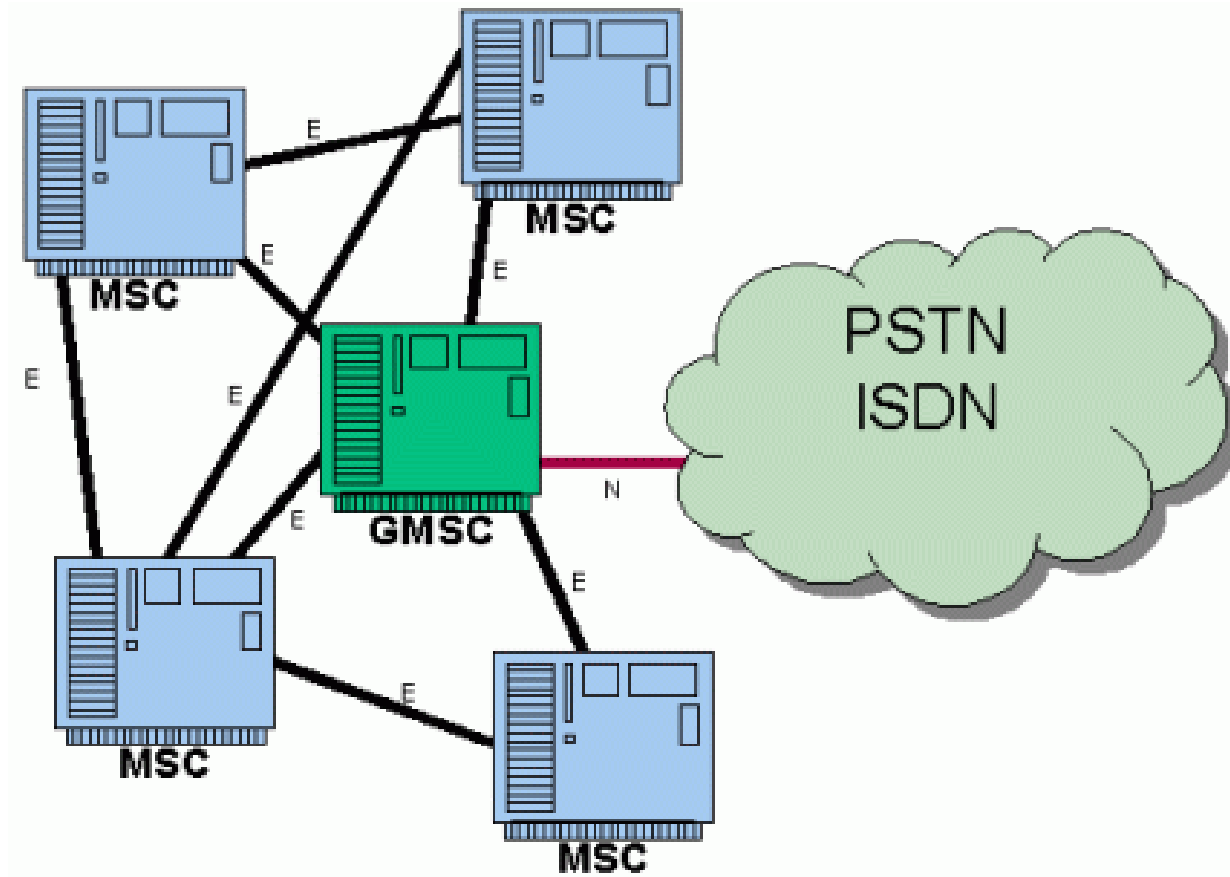
Dienstvermittlungsstellen (MSC)



Übergangsvermittlungsstelle (GMSC)

- Operiert als MSC (Gateway MSC)
- Funktionen für Kommunikation mit fremden Netzen
 - Integrated Services Digital Network (ISDN)
 - Public Land Mobile Network (PLMN) → Mobilfunk
 - Public Switched Telephon Network (PSTN) → Festnetz
 - Public Data Network (PDN)
- Auswertung der Informationen aus MSISDN-Nummer
- Zuordnung zum Teilnehmer des eigenen Netzes

Übergangsvermittlungsstelle (GMSC)



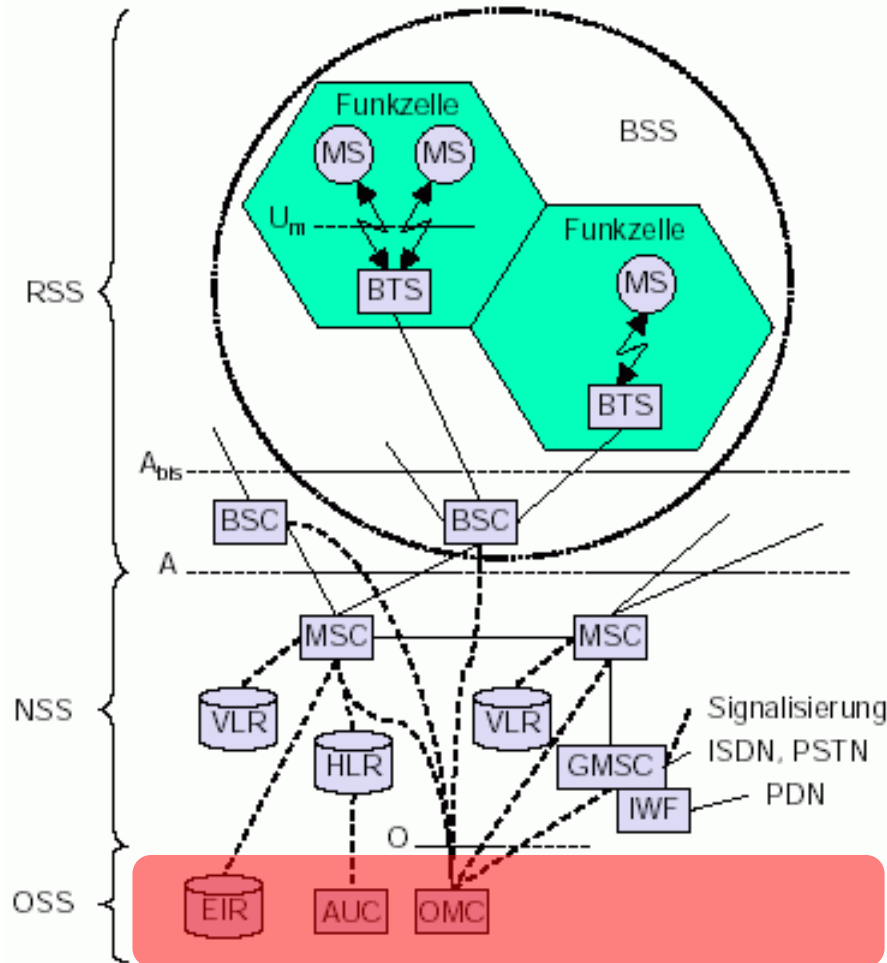
Heimatregister (HLR)

- Datenbank, die vom MSC für Routing benutzt wird
 - Hochspezialisiert mit Echtzeitanforderungen
- Enthält dauerhafte und relevante temporäre Teilnehmerdaten der Benutzer des eigenen Netzes
 - Internationale Identifizierung (IMSI)
 - Nummer des GSM-Teilnehmers (MSISDN)
 - Aufenthaltsort des Teilnehmers (LA)
 - Internationale Lokalisierung (MSRN)
- Sehr große Datenbank mit vielen Einträgen
 - Realisierung durch mehrere Module
 - Verteilte Datenbanken möglich

Besucherregister (VLR)

- Hochdynamische Datenbank mit Einträgen von allen MS im Einzugsbereich des MSC
 - MSC und VLR bilden häufig eine Einheit
- reger Datenaustausch
- Kopie der Daten vom HLR bei Eintritt einer MS in LA
 - Vergabe einer temporären IMSI (TMSI)
 - Speichern der Location Area Identity (LAI)
 - Zweck
 - Vermeidung häufiger Aktualisierungen im HLR
 - Weniger Signalisierung von Teilnehmerdaten

Betriebs-/Wartungssystem (OSS)



Betriebs- und Wartungszentrale (OMC)

- Netzkonfiguration / Netzbetrieb
- Verwaltung geschäftsrelevanter Daten
 - Kundendaten
 - Gebührenabrechnungen
 - Statistiken
- Performancemanagement
 - Überwachung des Netzverkehrs (Traffic)
 - Erstellung von Statusberichten
- Sicherheitsmanagement

Authentifizierungszentrale (AuC)

- Funksignale über Luftschnittstelle leicht angreifbar
 - Identität der Teilnehmer schützen
 - Sichere Datenübertragung gewährleisten
 - Erzeugen und Speichern vertraulicher Daten
 - Schlüssel zur Benutzerauthentifizierung generieren
 - Freischaltung registrierter Dienste
 - Parameter sind Daten aus dem HLR
- AuC kann im geschützten Bereich des HLR liegen

Geräteidentifikationsregister (EIR)

- Datenbank für alle Gerätekennungen (IMEI)
- Weiße Liste (white list)
 - Alle gültigen registrierten Gerätekennungen
- Graue Liste (gray list)
 - Geräte mit Fehlfunktionen
 - MS mit veralteter Software
- Schwarze Liste (black list)
 - Gestohlen gemeldete Geräte
 - Sonstige Gründe für Sperrung
 - Nicht immer vollständiger Abgleich zwischen verschiedenen Netzbetreibern

- Einführung
- Systemarchitektur
- **Luftschnittstelle**
- Lokalisierung
- Handover
- Weiterentwicklungen

Verbindung zwischen MS und BTS

- Realisierung der Funkübertragung
- Basiert auf Kombination FDMA/TDMA
- Standardisiert durch ETSI

Randbedingungen

- Begrenzte Bandbreite (22,8 kBit/s)
- Qualitätsbedingungen des Übertragungswegs
 - Luft, Umwelt, Wetter
 - Mobilität des Teilnehmers
- Interferenzen zwischen Nachbarzellen

Senderichtung (Uplink)

- GSM 900: 890-915 MHz
- GSM 1800: 1710-1785 MHz

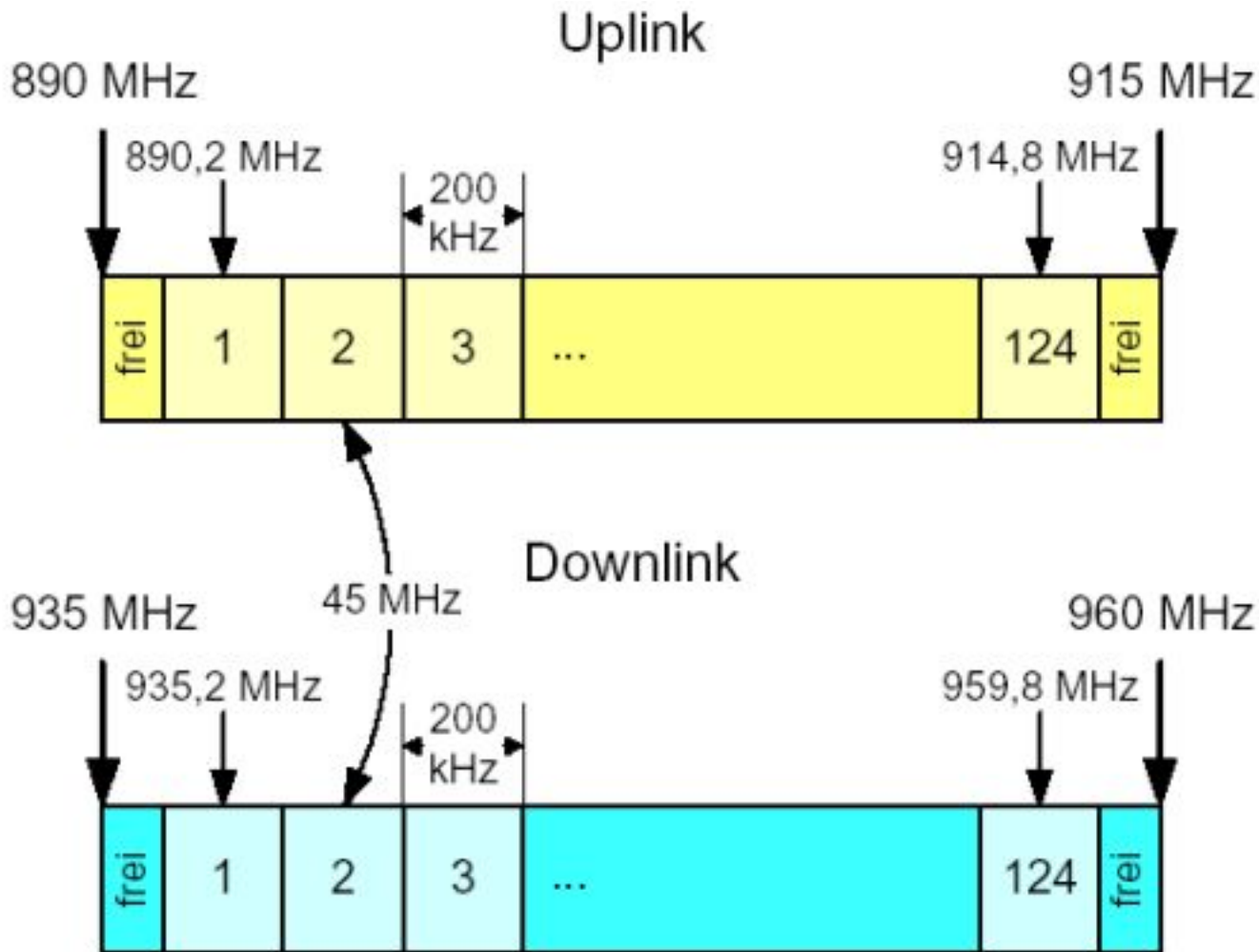
Empfangsrichtung (Downlink)

- GSM 900: 935-960 MHz
- GSM 1800: 1805-1880 MHz

Anzahl Kanäle (RFCH)

- GSM 900: 124
- GSM 1800: 372

FDMA-Schema GSM 900



Problem

- Qualitative Unterschiede benachbarter Frequenzen
- Häufig sind einige Frequenzen lokal gestört

Lösung

- Regelmäßiges Wechseln der Übertragungsfrequenz
- Jeder Burst wird auf anderer Frequenz gesendet
- Zusammenstellung aus Frequenzgruppe der Zelle
- Signalisierung an die MS durch Assignment Command
→ Schicht 3 Signalisierung

Mehrere Netzbetreiber müssen sich die zur Verfügung stehenden Kanäle teilen

Für Deutschland (GSM 900)

- D1 (57 Kanäle): 1-12, 51-80, 105-119
- D2 (57 Kanäle): 14-49, 82-102
- Reserve/Trennung (10 Kanäle)

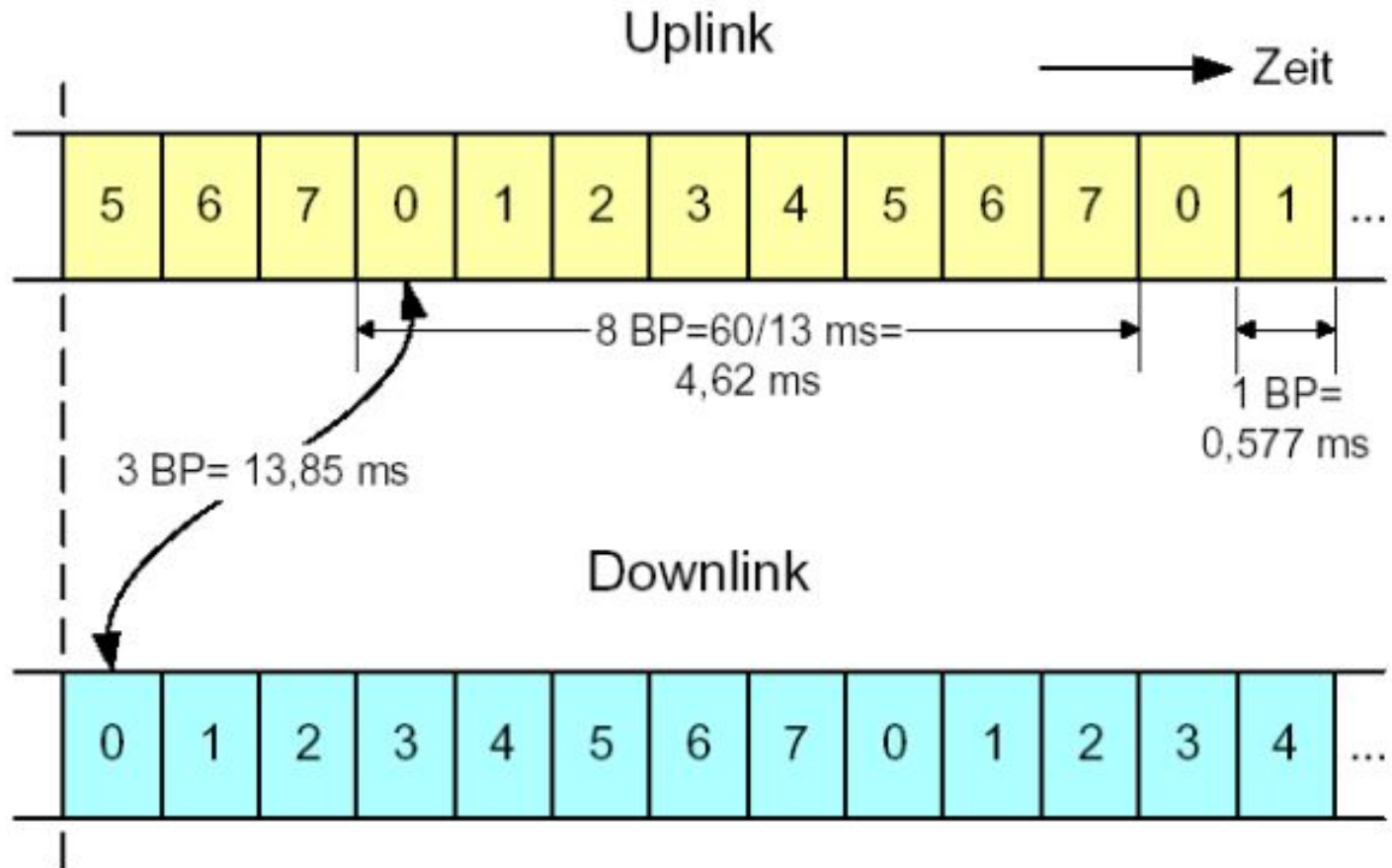
Kanäle sind knappe Ressourcen

- Basisstationen werden nur ca. 1/7 der verfügbaren Frequenzen zugeordnet
→ 8 Frequenzen für D1 / D2 pro Basisstation
- Frequenzen für Verwaltungszwecke stehen nicht für die eigentliche Datenübertragung zur Verfügung
- Viele der Teilnehmer sollen gleichzeitig telefonieren können
→ Frequenzen müssen in Zeitschlitz aufgeteilt werden

Einteilung: 1 Frequenzkanal = 8 Zeitschlitz (Slots)

- Zeitschlitz wiederholen sich zyklisch
- Nummerierung 0 bis 7
- Basisstation sendet auf einem bestimmten Zeitschlitz mit einer bestimmten Nummer
- MS antwortet auf dem Slot mit gleicher Nummer
- MS soll nicht gleichzeitig Senden und Empfangen
- Zugeordnete Up-/Downlinks um 3 Slots verschoben
- Folge von Zeitschlitz repräsentiert bidirektionalen Kanal zwischen MS und BTS

TDMA für GSM



Innerhalb eines Zeitschlitz wird ein Burst gesendet

- Dauer: 576,6 μ s (15/26 ms)
- Länge: 156,25 Bit
- Zweck der Übertragungsbursts
 - Nutzdaten transportieren
 - Verbindung aufbauen
 - Verbindung verwalten
- 5 Datenformate definiert

Datenübertragung (Verkehrs- und Steuerkanäle)



- Tail-Bits
 - Sendeleistung hoch-/ herunterfahren (logische Null)
- Stealing-Flags
 - 0: Signalisierungsinformationen, 1: Nutzdaten
- Trainings-Sequenz
 - Bitmuster für Kanalschätzung und Synchronisation
- Schutzabstand (Guard Period)
 - Vermeidung von Überlappung zeitlich benachbarter TDM-Kanäle wegen unterschiedlicher Pfadverzögerung

Dauer eines Bursts: 576,6 μ s

Nutzdaten (normaler Burst): 114 Bit

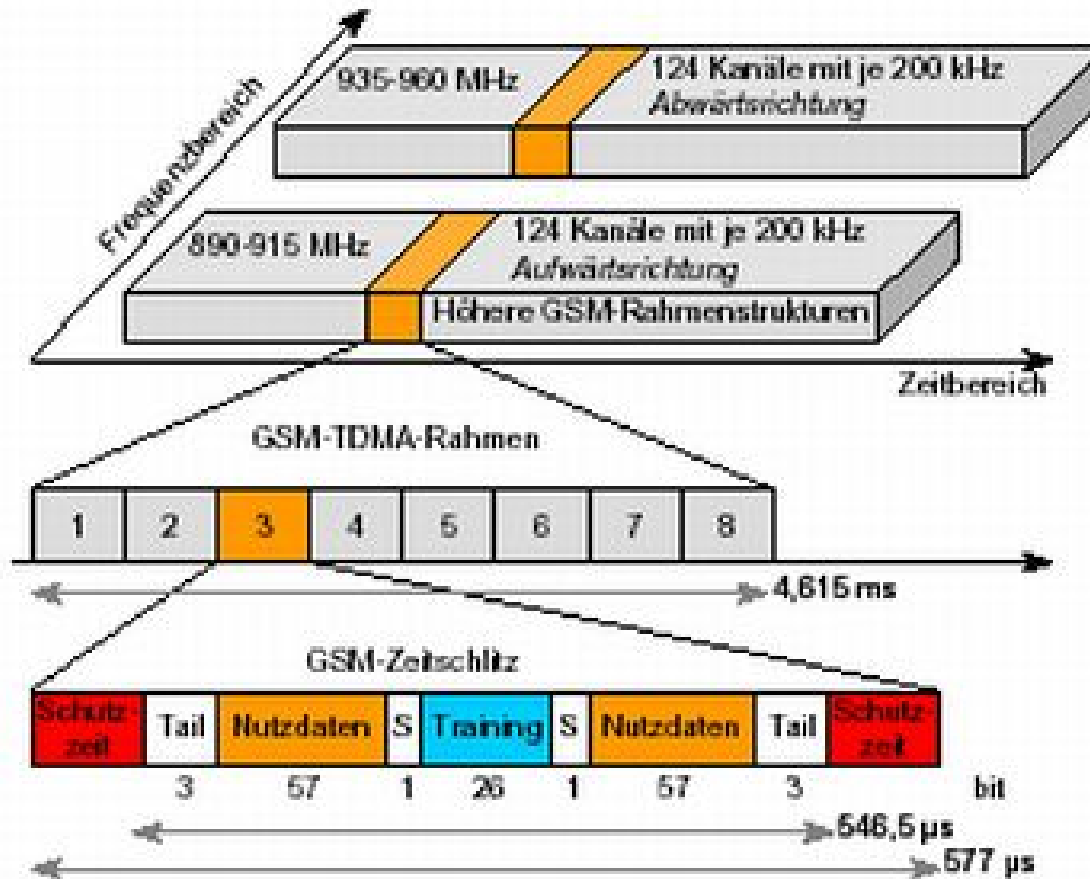
Senden eines Bursts alle 8 Zeitschlitz

→ Theoretische Obergrenze: 24700 Bit/s

In der Realität

- 13000 Bit/s für Sprache
- 9600 Bit/s für Daten

Zusammenfassung



Bursts zur Frequenzkorrektur

- Frequenzverschiebung durch Setzen der Bits auf Null

Bursts zur Synchronisation

- Zeitliche Synchronisation zwischen BTS und MS

Dummy Bursts

- Senden von nicht spezifizierten Daten, falls gerade weder Nutz- noch Verwaltungsdaten zu senden sind

Zugriffsbursts

- Verbindungsaufnahme einer MS mit einer BTS

Die MS muss ihren Burst so aussenden, daß der Zeitschlitz bei der BTS eingehalten wird

- Burst früher senden bei weiter Entfernung
- Burst später senden bei naher Entfernung

Zeitunterschiede durch Übertragungsgeschwindigkeit werden für jede MS durch die BTS ausgeglichen

- 6 Bit Wert für die Entfernung in Stufen
- Pro Stufe 555m Entfernung von der Basisstation
- Pro Stufe den Burst $3,7\mu\text{s}$ früher senden

- Einführung
- Systemarchitektur
- Luftschnittstelle
- **Lokalisierung**
- Handover
- Weiterentwicklungen

Weltweites Finden von Teilnehmern, die mit dem GSM-Netzwerk verbunden sind

- HLR kennt die Location Area (LA) der MS
 - Periodische Aktualisierung durch VLR
 - MS muss eingeschaltet sein
- Weltweite Gültigkeit der Telefonnummer

Roaming

- Wechsel zwischen zwei VLR mit permanenter Verfügbarkeit aller grundlegenden Dienste

Mobile Station International ISDN Number (MSISDN)

- Eigentliche Telefonnummer
- Verbunden mit dem SIM
- Country Code (CC) → Beispiel +49
- National Destination Code (NDC) → Beispiel 179
- Subscriber Number (SN) → Beispiel 12345678

International Mobile Subscriber Identity (IMSI)

- Interne eindeutige Kennzeichnung eines Teilnehmers
- Mobile Country Code (MCC)
- Mobile Network Code (MNC)
- Teilnehmerkennung (MSIN)

Temporary Mobile Subscriber Identity (TMSI)

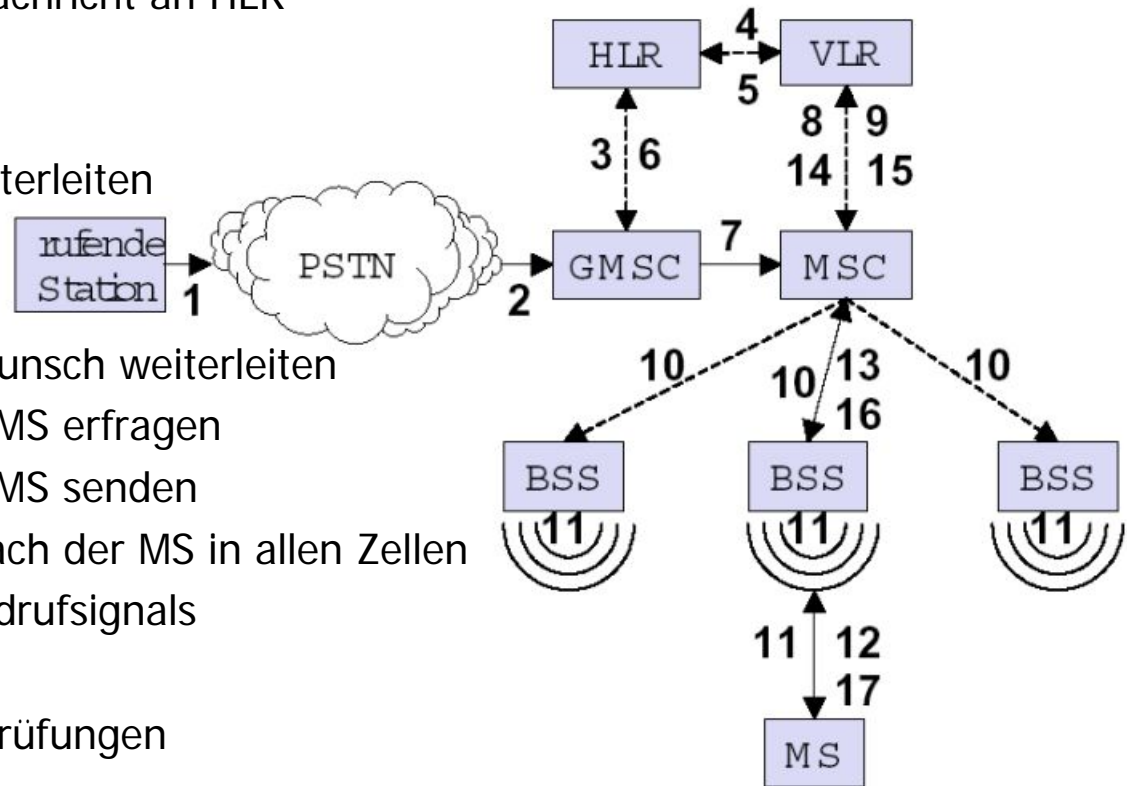
- IMSI nicht unverschlüsselt über Funk schicken
- Lokale temporäre Teilnehmerkennung (4 Byte)
- Wird vom VLR festgelegt in der Location Area der MS

Mobile Station Roaming Number (MSRN)

- Verschleierung Teilnehmeridentität/Aufenthaltort
- Vom VLR erzeugt auf Anfrage des MSC
- Visitor Country Code (VCC)
- Visitor National Destination Code (VNDC)
- MSC-Kennung + Teilnehmernummer

Mobile Terminated Call (MTC)

- 1 Nummer wählen
- 2 Weiterleitung zum GMSC, da Mobilteilnehmer
- 3 Verbindungsaufbaunachricht an HLR
- 4 Frage nach MSRN
- 5 Empfang MSRN
- 6 Zuständiges MSC weiterleiten
- 7 Verbindungsaufbauwunsch weiterleiten
- 8 Aktuellen Status der MS erfragen
- 9 Aktuellen Status der MS senden
- 10 Rundruf (Paging) nach der MS in allen Zellen
- 11 Aussenden des Rundrufsignals
- 12 13 MS antwortet
- 14 15 Sicherheitsüberprüfungen
- 16 17 Verbindungsaufbau



- Einführung
- Systemarchitektur
- Luftschnittstelle
- Lokalisierung
- Handover
- Weiterentwicklungen

Übergabe der Verbindung an eine andere BTS

- Bewegungsbereich wird nicht vollständig abgedeckt
- Zelluläre Systeme erfordern Handover-Prozeduren
- Neukonfiguration der Kommunikationsverbindung

Anzahl der Übergaben abhängig von

- Radius der Zelle (max. 35 km)
- Geschwindigkeit der Teilnehmer (max. 250 km/h)

Die laufende Verbindung darf nicht durch den Handover-Mechanismus unterbrochen werden

Network Originated Handover

- Verbindungsübergabe durch das Netzwerk initiiert
- Handover-Algorithmus kann vom Netzbetreiber unabhängig von den Endgeräten geändert werden

Dauer

- Obergrenze von ca. 60 ms kann durch entsprechende Synchronisation zwischen den Zellen für eine Übergabe der Verbindung eingehalten werden

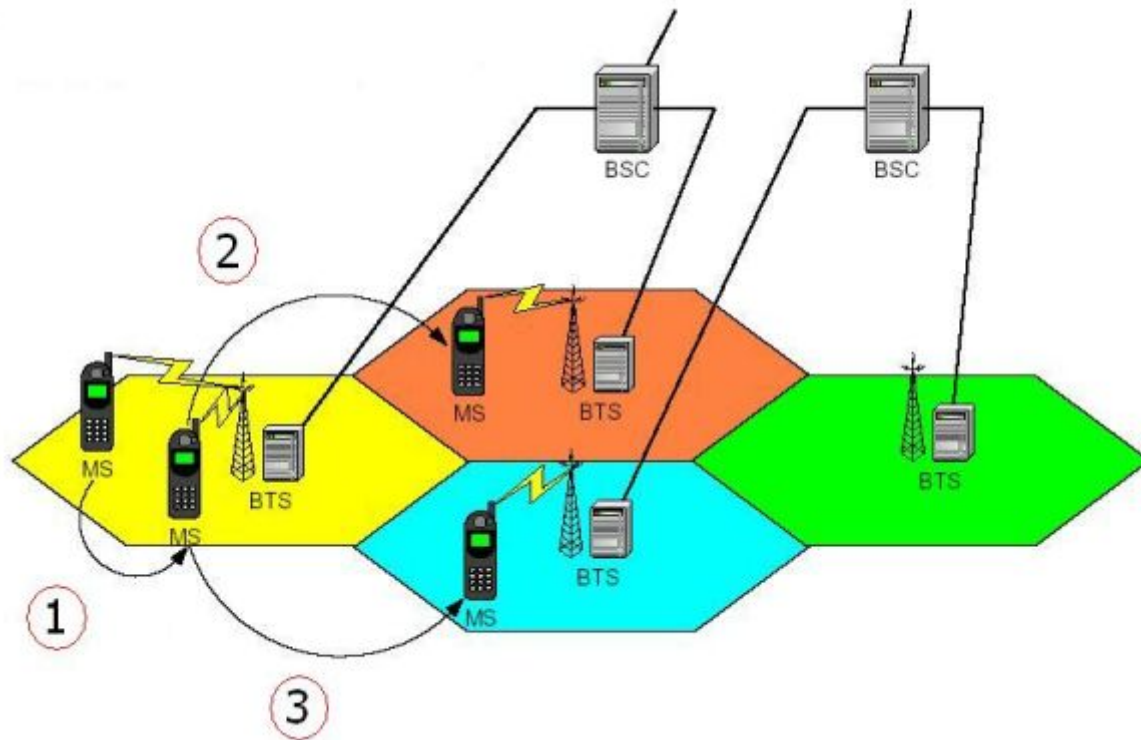
Hinausbewegen aus dem Empfangsbereich einer BTS

- Stärke des Empfangsignals nimmt kontinuierlich ab
- Signal fällt unter einen gewissen Schwellenwert
- Fehlerrate steigt wegen Interferenzen
- Abstand zu BTS wird zu groß → Timing Advance

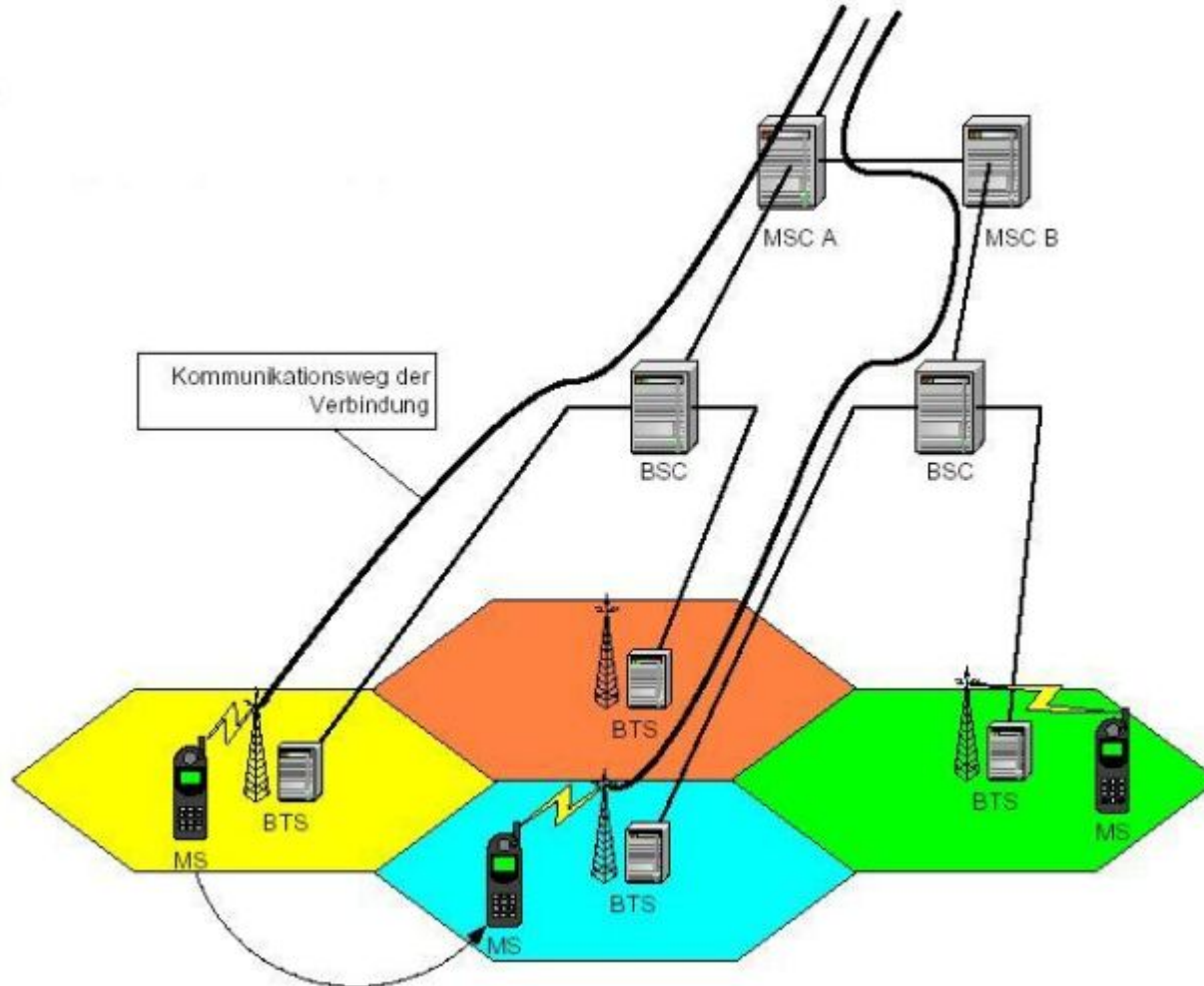
Zu hohes Verkehrsaufkommen in einer Zelle

- Aktuelle Netzlast ist zu hoch (viele Verbindungen)
- Verschiebung der Verbindung in eine weniger belastete Zelle (Lastenverteilung)

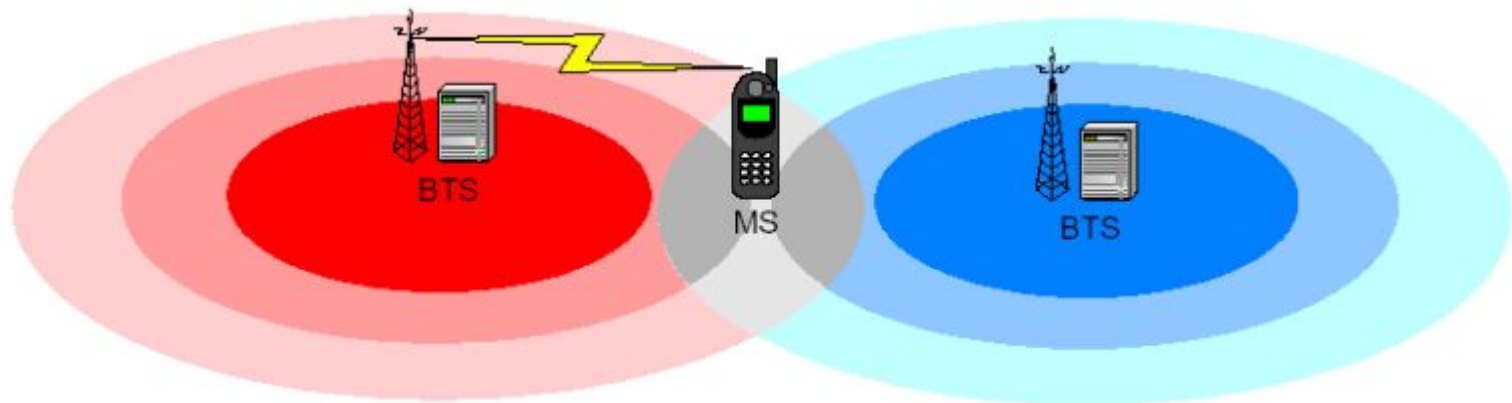
1. Intrazellenübergabe → Frequenzwechsel
2. Interzellen, Intra-BSC → Häufigster Fall
3. Inter-BSC, Intra-MSC → Anderer BSC-Bereich



4. Inter-MSC → Kontrolle weiterhin durch Anker-MSC



Problem: keine eindeutigen Zellengrenzen
MS kann häufig mehrere Zellen empfangen



Wie wird zu häufiges Hin- und Herschalten zwischen den beteiligten Basisstationen vermieden ?

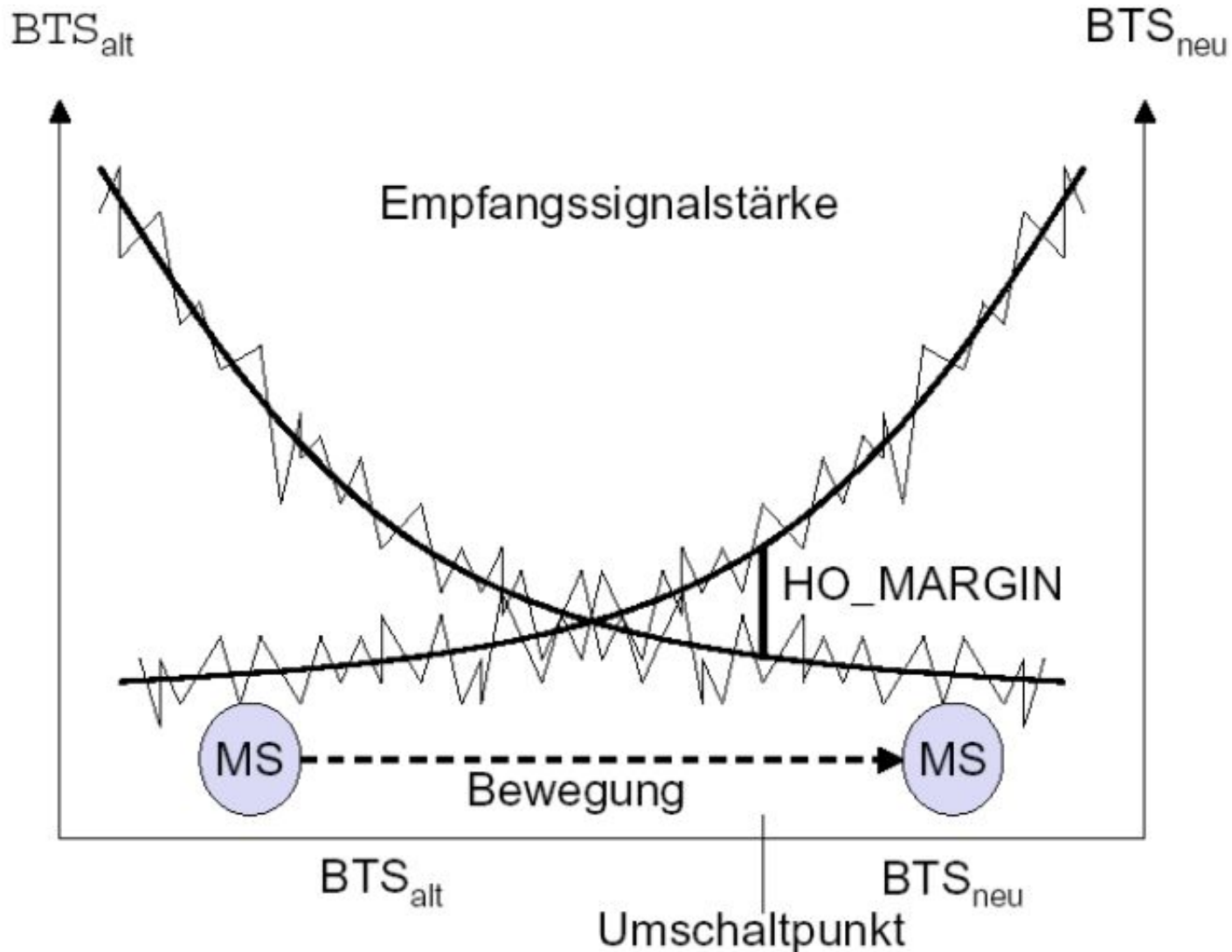
Periodische Messungen für rechtzeitige Übergabe

- Qualitätsmessungen auf Uplink und Downlink
- MS sendet Messbericht an BTS alle $\frac{1}{2}$ Sekunde

In der Realität meist mehr als ein Handover

- Schwankungen der Signalstärke
- Vergleich mit einem Schwellenwert (HO_MARGIN)
 - Berechnung des Durchschnitts durch BSC
 - HO_MARGIN zu niedrig → Gefahr ping-pong effect
 - HO_MARGIN zu hoch → Gefahr Verbindungsabbruch

Übergabeentscheidung



- Einführung
- Systemarchitektur
- Luftschnittstelle
- Lokalisierung
- Handover
- Weiterentwicklungen

Bandbreite ursprünglich nur für Sprache konzipiert

- 9,6 bis 14,4 kBit/s abhängig vom Betreiber
- Bandbreite wurde schnell nicht mehr zeitgemäß

Bandbreite nicht ausreichend für moderne Dienste

- Internetanwendungen
- Laden von Dateien
- E-Mail Austausch
- Zugang zu Datennetzen

→ Schaffung der Mobilfunkgeneration 2+

High Speed Circuit Switched Data

- Durch bessere Kodierverfahren können maximal 14400 Bit/s pro Kanal erreicht werden
- Belegung mehrerer Zeitschlitz im TDMA-Rahmen
- Bei Bündelung von maximal 8 Kanälen wären theoretisch 115,2 kBit/s möglich
- In der Praxis
 - 4 Kanäle werden gebündelt (57,6 kBit/s)
 - Bündelung muss nicht symmetrisch erfolgen
- Nur wenige Änderungen am GSM-Netzwerk
- Neue Endgeräte erforderlich

Kanalverteilung

Bisher:

2 x 9600 bit/s



HSCSD:

4 x 14.400 bit/s



1+3 - Verbindung

(z.B. für Internet-Downloads)

14.400 bit/s senden



43.200 bit/s empfangen



2+2 - Verbindung

(z.B. für E-mail Versand)

28.800 bit/s senden



28.800 bit/s empfangen



Vorteile

- Kostengünstige Installation
- Feste Übertragungsbandbreite
- Geeignet für größere Datenmengen

Nachteile

- Blockierung von Sprachkanälen
- Starke Beanspruchung des Netzes
- Unnötiger Verbrauch knapper Ressourcen
- Leitungsvermittelttes Verfahren

General Packet Radio Service

Paketvermittlung

- „Always Online“, sinnvoll für Push-Dienste
→ bessere Ausnutzung der Kapazitäten
- Kunde bezahlt nach übertragenem Volumen
- Zugang in verschiedene existierende Netze

Datenraten bis 171,2 kBit/s

- 8 gebündelte Funkkanäle, optimale Empfangsqualität
- Hängt in der Realität stark ab von
 - Datenaufkommen anderer Teilnehmer
 - Auslastung der Funkzelle

Änderungen am GSM-Netz beträchtlich

- Ausgelegt für leitungsvermittelte Kommunikation
- Verfügbar in Deutschland flächendeckend seit 2001

Neue Endgeräte notwendig

- Klasse A
 - Zeitgleicher Transfer von Daten und Sprache
- Klasse B
 - Keine Paketversand während Sprachverbindung
 - Während Datenübertragung nur Anrufmeldung
- Klasse C
 - Manuelles Umschalten in Sprach- / Datenmodus

Multislot-Klassen

→ pro Kanal 13,4 bis maximal 21,4 kBit/s

Klasse	Empfangskanäle maximal	Sendekanäle maximal	Kanäle gesamt maximal
1	1	1	2
2	2	1	3
3	2	2	3
4	3	1	4
5	2	2	4
6	3	2	4
7	3	3	4
8	4	1	5
9	3	2	5
10	4	2	5
11	4	3	5
12	4	4	5