FACHHOCHSCHULE WEDEL

SEMINARARBEIT

in der Fachrichtung

Wirtschaftsinformatik

Seminar Informatik

Oberthema: Mobile Computing

Thema:

GSM
Global System for Mobile communications

Eingereicht von:	Oliver Grote Seesrein 22 22459 Hamburg Tel. (040) 555 99 576
Erarbeitet im:	8. Semester
Abgegeben am:	16. November 2004
Referent (FH Wedel):	Prof. Dr. Sebastian Iwanowski Fachhochschule Wedel Feldstraße 143 22880 Wedel Tel. (04103) 8048 63

Inhaltsverzeichnis

Abkürzungsverzeichnis III

Abbildungsverzeichnis IV

1 Einführung 1

1.1 Geschichte 1
1.2 Eigenschaften 1
2 Systemarchitektur 2

2.1 Funk-Feststationssystem (RSS) 3
2.1.1 Feststationssystem (BSS) 3
2.1.1.1 Sende-/Empfangsstation (BTS) 3
2.1.1.2 Feststationssteuerung (BSC) 5
2.1.2 Mobilstation (MS) 5
2.1.2.1 Mobile Equipment (ME) 5
2.1.2.2 Subscriber Identity Module (SIM) 6
2.2 Mobilvermittlungssystem (NSS) 7
2.2.1 Dienstvermittlungsstellen (MSC) 7
2.2.2 Heimatregister (HLR) 8
2.2.3 Besucherregister (VLR) 9
2.3 Betriebs- und Wartungssystem (OSS) 10
2.3.1 Betriebs- und Wartungszentrale (OMC) 10
2.3.2 Authentifizierungszentrale (AuC) 10
2.3.3 Geräteidentifikationsregister (EIR) 11
3 Luftschnittstelle 11

3.1 FDMA für GSM 12
3.1.1 Frequenzbänder 12
3.1.2 Frequenzsprungverfahren 13
3.2 TDMA für GSM 13
3.2.1 Zeitschlitze (Slots) 13
3.2.2 Zeitschlitzinformationen (Bursts) 15
3.2.3 Timing Advance 16
4 Lokalisierung und Verbindungsaufbau 16

4.1 Kennungen 17
4.2 Verbindungsaufbau beim Mobile Terminated Call (MTC) 17
5 Verbindungsübergabe (Handover) 18

5.1 Gründe für Handover 19
5.2 Arten von Handover 19
5.3 Übergabeentscheidung 20
6 Weiterentwicklungen 22

6.1 HSCSD 22
6.2 GPRS 23
Literaturverzeichnis 25

Abkürzungsverzeichnis

AuC	Authentication Centre
BP	Burst Period
BSC	Base Station Controller
BSS	Base Station Subsystem
BTS	Base Transceiver Station
CC	Country Code
DCS	Digital Cellular System
EIR	Equipment Identity Register
ETSI	European Telecommunications Standards Institute
FDD	Frequency Division Duplex
FDMA	Frequency Division Multiple Access
GMSC	Gateway MSC
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HLR	Home Location Register
HSCSD	High Speed Circuit Switched Data
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
ISDN	Integrated Services Digital Network
LA	Location Area
LAI	Location Area Identification
MCC	Mobile Country Code
ME	Mobile Equipment
MNC	Mobile Network Code
MS	Mobile Station
MSC	Mobile Switching Center
MSIN	Mobile Subscriber Identification Number
MSISDN	Mobile Subscriber ISDN Number
MSRN	Mobile Station Roaming Number
MTC	Mobile Terminated Call
NDC	National Destination Code
NSS	Network and Switching Subsystem
OMC	Operation and Maintenance Centre
OSS	Operation Subsystem
PDN	Public Data Network
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
PUK	PIN Unblocking Key
RAN	Radio Access Network
RSS	Radio Subsystem
SIM	Subscriber Identity Module
SN	Subscriber Number
SS7	Signalisierungssystem Nr. 7
TDMA	Time Division Multiple Access
TMSI	Temporary Mobile Subscriber Identity
UMTS	Universal Mobile Telecommunication System
VCC	Visitor Country Code
VLR	Visitors Location Register
VNDC	Visitor National Destination Code

Abbildungsverzeichnis

Abbildung 2.1	Funktionale Architektur von GSM	2
Abbildung 2.2	Sektorisierung in der Basisstation	4
Abbildung 2.3	Übergangsvermittlungsstellen (GMSC)	8
Abbildung 3.1	FDMA-Schema bei GSM 900	12
Abbildung 3.2	Funkzellencluster bei GSM	14
Abbildung 3.3	TDMA für GSM	14
Abbildung 3.4	Aufbau eines normalen Burst	15
Abbildung 4.1	Ablauf eines Mobile Terminated Call	18
Abbildung 5.1	Übergabearten bei Handover	20
Abbildung 5.2	Übergabeentscheidung bei Handover	21
Abbildung 6.1	Verbindungsmöglichkeiten bei HSCSD	22
Abbildung 6.2	Multislot-Klassen	24

1 Einführung

GSM (Global System for Mobile communications) ist ein sehr leistungsfähiges, aber auch komplexes digitales Mobilfunksystem der 2. Generation (2G). Es bietet sehr vielfältige Dienste, gute Betriebseigenschaften und einen hohen Sicherheitsstandard.

1.1 Geschichte

1982 wurde die Groupe Spéciale Mobile gegründet. Die Gruppe hatte schon damals die Notwendigkeit eines einheitlichen Mobilfunkstandards erkannt, der für den Massenmarkt ausgelegt sein sollte. Hier wurden bereits grundlegende Dinge wie eine automatische Verbindungsübergabe oder internationales Roaming vereinbart.
1987 starteten 13 Teilnehmer aus 12 Staaten mit einem Abkommen, das „Memorandum of Understanding“ genannt wurde, in dem ein gemeinsames Mobilfunknetz zunächst nur für Europa entwickelt werden sollte. In diesem Mobilfunkstandard sollten die Überlegungen der Groupe Spéciale Mobile umgesetzt werden. Schnell unterzeichneten weitere Staaten das Abkommen, so das sich schnell ein führender Standard entwickelte.
1989 wurde der Standard in GSM umbenannt und die Koordination von der Normierungsbehörde ETSI übernommen. Schon die erste Spezifikation umfasste mehrere tausend Seiten. Hier wurden die bis heute gültigen Standards GSM 900, GSM 1800/DCS 1800 und GSM 1900 festgelegt.
1992 gingen in Deutschland die ersten auf GSM basierenden Mobilfunknetze D1 und D2 in Betrieb, E-Plus folgte 1994 und E2 1998.

1.2 Eigenschaften

GSM ist das erfolgreichste Mobilfunksystem weltweit, 2003 wurden mehr als 820 Millionen Teilnehmer in über 190 Ländern registriert und Anfang 2004 konnte man erstmals die Marke von eine Milliarde Teilnehmer übertreffen.
GSM bietet eindeutige Nummernkreise für mobile Teilnehmer und unterstützt dadurch die weltweite Ortung eines Teilnehmers mit Hilfe internationaler Roaming-

Abkommen. GSM kann neben Sprache auch Daten übertragen und bietet eine hohe Kapazität bei kleinen Funkzellen, zwischen denen die Verbindung ohne Unterbrechung übergeben werden kann. Mittlerweile unterstützt GSM mehrere z.T. moderne Datendienste wie Short Message Service (SMS), Wireless Application Protocol (WAP) oder Multimedia Message Service (MMS).
GSM hat ein integriertes Sicherheitskonzept, das zwar keine Ende-zu-Ende Sicherheit wegen der Übertragung von Daten über die Luftschnittstelle bietet, aber sicherheitsrelevante Daten angemessen verschlüsseln kann.

2 Systemarchitektur

Die Architektur von GSM ist typisch für Architekturen im Bereich der Telekommunikation. Der Aufbau ist hierarchisch, teilweise komplex und besitzt verschiedene Komponenten, die durch Schnittstellen miteinander verbunden sind.

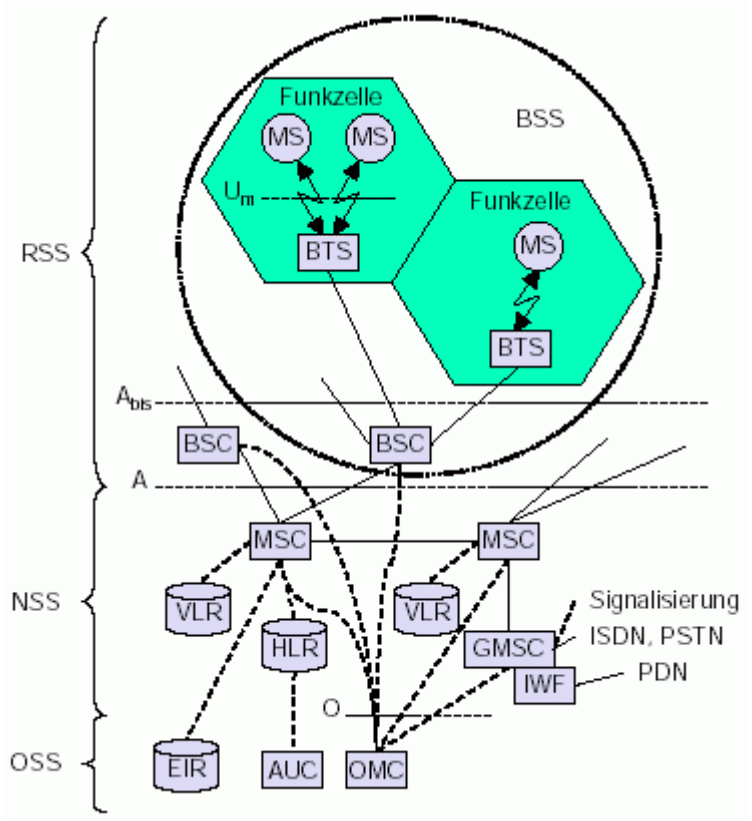

Abbildung 2.1 Funktionale Architektur von GSM

GSM wird in drei Subsysteme eingeteilt, welche für Funk (RSS), Vermittlung (NSS) und Administration (OSS) zuständig sind.

2.1 Funk-Feststationssystem (RSS)

Das RSS enthält die Komponenten, welche für die Abwicklung des Funkverkehrs zuständig sind, dabei müssen Mobilstationen (MS) über die Luftschnittstelle mit dem Radio Access Network (RAN) verbunden werden. Dieses Netzwerk besteht aus Basisstationen (BTS) und Steuerungseinheiten (BSC), welche mehrere Basisstationen verwalten können. Das Funk-Feststationssystem versorgt Mobilteilnehmer mit Signalen bzw. nimmt Signale entgegen und macht diese den angeschlossenen Vermittlungsstellen verfügbar.

2.1.1 Feststationssystem (BSS)

Das RAN besteht aus mehreren Subsystemen, den Base Station Subsystems (BSS). Jedes BSS wird durch genau einen Controller (BSC) gesteuert, der ein bestimmtes geographisches Gebiet abdeckt, das auch als Standortbereich bezeichnet wird. Durch das BSS müssen alle Funktionen bereitgestellt werden, welche für eine permanente Funkverbindung zu einer Mobilstation notwendig sind, außerdem ist das BSS noch zuständig für die Kodierung bzw. Dekodierung der Sprachdaten und muss die Anpassung der Datenraten vom bzw. zum drahtlosen Netz vornehmen.

2.1.1.1 Sende-/Empfangsstation (BTS)

Die Basisstation ist für die Kommunikation in der durch sie aufgespannten Funkzelle verantwortlich. Sie enthält die Hardware, welche zum Senden (Transmitter) bzw. Empfangen (Receiver) notwendig ist, also technische Einrichtungen wie Antennen, Verstärker und eine elektronische Signalverarbeitung. Daneben findet man nur wenige zusätzliche Komponenten, um die Basisstationen so kostengünstig wie möglich zu halten, denn bei einem Radius von typischerweise mehreren 100 Metern bis maximal 35 Kilometern abhängig von der Geländeform benötigt man schon sehr

viel Infrastruktur, um beispielsweise ein Gebiet von der Größe Deutschlands annähernd flächendeckend zu versorgen.

Die Basisstation realisiert die Funkverbindung zur Mobilstation, bietet eine Funkanbindung über die Luftschnittstelle, moduliert die Daten auf Hochfrequenz und ist verantwortlich für die Setzung des TDMA-Zeitrahmens.

Eine weitere Möglichkeit, um Kosten bei der Infrastruktur einzusparen ist die Sektorisierung: Hier wird der Basisstation nicht nur eine Zelle zur Verarbeitung zugewiesen, sondern im Regelfall kann eine BTS drei Funkzellen versorgen, die zueinander in Sektoren angeordnet sind.

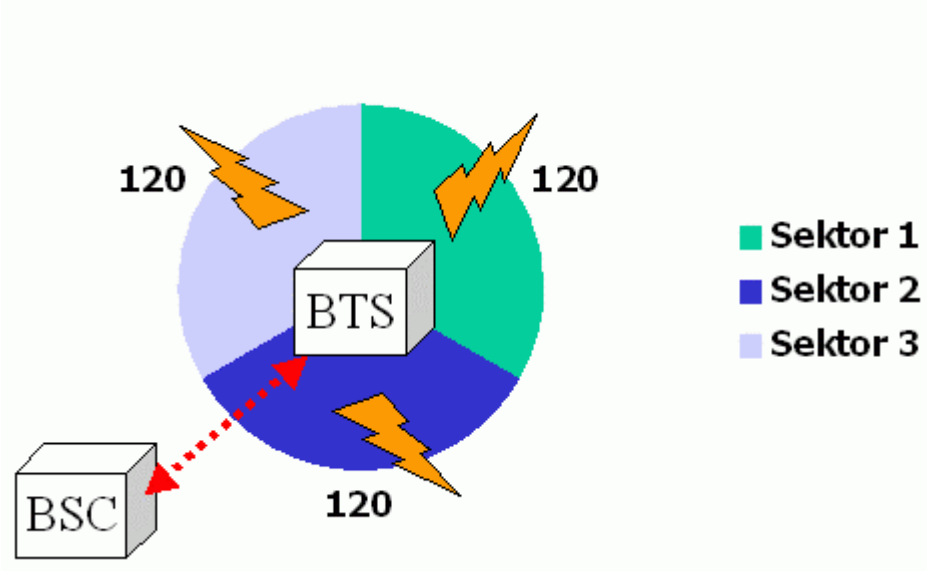

Abbildung 2.2 Sektorisierung in der Basisstation

Hierzu ist es notwendig, Antennen mit einer 120° Sende-/Empfangscharakteristik zu verwenden. Durch dieses Verfahren können so drei Zellen durch nur einen Antennenmast versorgt werden, außerdem braucht nur eine Schnittstelle zur Steuereinheit (BSC) verlegt werden. Weiterhin lässt sich durch die Bildung von Sektoren ein geographisches Gebiet mit der „schmäleren“ Richtcharakteristik besser konfigurieren, um Interferenzen zu minimieren.

2.1.1.2 Feststationssteuerung (BSC)

Ein BSC verwaltet die Funkressourcen mehrerer Basisstationen. Diese Architektur wurde deshalb so gewählt, um die eigentlichen Steuerungsaufgaben auszulagern, damit die eigentlichen Basisstationen möglichst einfach und kostengünstig gehalten werden können. Ein BSC verwaltet i.d.R. 30 bis über 100 Basisstationen, dadurch wird versucht existierende geographische Einheiten wie Bezirke, Städte oder Stadtteile von Großstädten nachzubilden, da so die Wahrscheinlichkeit am geringsten ist, das der Mobilteilnehmer sich aus dem Kontrollbereich des BSC hinausbewegt und eine aufwendige Verbindungsübergabe (Handover) eingeleitet werden muss.
Der BSC fungiert für die an ihn angeschlossenen Funkzellen als Datenbank und leitet diese Informationen an angeschlossene Vermittlungsstellen (MSC) weiter. Die Steuereinheit muss also alle Frequenzkanäle und Zeitschlitze ihrer Zellen verwalten, um zu wissen, welche Funkkanäle bereits belegt, reserviert oder vielleicht sogar gestört sind, um einen Kanal für ein neues Gespräch zu vergeben.[1]
Weiterhin ist es die Aufgabe des BSC die Sendeleistung der kommunizierenden Funkstationen, also der Mobilstation und der Basisstation, zu kontrollieren. Ebenfalls kann er eine Verbindungsübergabe (Handover) durchführen, wenn sich die neue Zelle im seinem Bereich befindet.

2.1.2 Mobilstation (MS)

Eine Mobilstation umfasst die Hard- und Software eines Endgeräts für die Kommunikation mit GSM. Im deutschen Sprachraum ist die Mobilstation fast ausnahmslos unter dem Begriff „Handy“ bekannt, der im angloamerikanischen Sprachgebrauch keine Verwendung findet. Man unterscheidet die benutzerunabhängige Komponente (ME) und eine nutzerspezifische Einheit (SIM).

2.1.2.1 Mobile Equipment (ME)

Das ME ist das technische Endgerät, welches man u.a. im Fachhandel erwerben kann. Es stellt prinzipiell die volle technische Funktionalität zur Verfügung, ist man

[1] Beispielsweise könnte eine Vermittlungsstelle einen Funkkanal beim BSC anfordern, um ein Gespräch vom Festnetz zur Mobilstation in einer angeschlossenen Zelle durchzustellen.

jedoch nicht als Kunde bei einem Netzbetreiber angemeldet, so ist eine Nutzung von GSM-Diensten eines Netzbetreibers außer einer internationale Notrufnummer nicht möglich. Die typische Sendeleistung des Endgeräts beträgt im D-Netz (GSM 900) 2 Watt, während im E-Netz (GSM 1800) 1 Watt Sendeleistung ausreichend ist, was auf den geringeren Abstand zu den Antennen bzw. den kleineren Radius der Funkzellen auf Grund des höheren Frequenzbereichs zurückzuführen ist. Mittlerweile verfügt das ME neben der reinen Übertragung von Sprachdaten über eine Reihe von zusätzlichen Funktionen, deren Charakteristik je nach Endgerät z.T. erheblich variieren kann. Beispiele für die Vielfalt von Funktionen:

- Digitale Bildaufnahme
- Radio / MP3-Player
- Kalender / Notizbücher

Für die mobilen Endgeräte wird bei der Herstellung eine Nummer vergeben (IMEI), wodurch jedes Gerät weltweit eindeutig identifiziert werden kann.

2.1.2.2 Subscriber Identity Module (SIM)

Durch das SIM wird der Zugriff auf Mobilfunkdienste überhaupt erst möglich. Die SIM-Karte speichert Daten, die für den Netzbetreiber spezifisch sind wie z.B. Rufnummern oder Identifikationsnummern. Sie kann aber nicht nur als Datenspeicher fungieren, sondern ist auch in der Lage Rechenoperationen auszuführen. Zu den Aufgaben des SIM gehören die Identifikation des Kunden, Datenverschlüsselung, Speicherung von Kundendaten und die Verwaltung netzspezifischer Daten wie z.B. der Aufenthaltsort des Teilnehmers. Nachfolgend seien einige Beispiele für permanente und temporäre Daten des SIM genannt:

Unveränderliche Daten auf dem SIM:

- Kartentyp/Seriennummer
- Zusätzlich abbonierte Dienste
- Internationale Mobile Subscriber Identity (IMSI)
  - Dient zur internationalen Identifizierung des Mobilteilnehmers
  - Wichtig für Abrechnung, Authentifizierung, Roaming
- Personal Identity Number (PIN)
- PIN Unblocking Key (PUK)
- Verwendete Sprache

Dynamische Daten auf dem SIM:

- 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 die Verbindung und Handover

2.2 Mobilvermittlungssystem (NSS)

Das NSS ist das Kernelement des GSM-Systems. Hier werden die mobilen, kabellosen Netze mit den öffentlichen, leitungsgebundenen Festnetzen verbunden. Außerdem ist das Mobilvermittlungssystem zuständig für die Verbindungsübergabe (Handover) zwischen verschiedenen BSS, d.h. das NSS muss eingreifen, wenn sich ein Mobilteilnehmer aus dem Zuständigkeitsbereich eines BSC bewegt. Im NSS ist weiterhin sämtliche Funktionalität enthalten, um einen Teilnehmer weltweit zu orten, der mit einem GSM-Netz verbunden ist.

2.2.1 Dienstvermittlungsstellen (MSC)

MSC sind für mehrere BSC einer Region zuständig, die im Prinzip die gleiche Funktionalität und Eigenschaften einer Vermittlungsstelle im Festnetz (PSTN) haben, nur müssen hier geographisch frei bewegliche Teilnehmer vermittelt werden.
Die wichtigste Aufgabe ist also das Mobilitätsmanagement, vor allem das Routing für eine Gesprächsleitung, also die wichtige Frage, welchen Weg die Signale durchlaufen müssen, um die Gesprächspartner effizient zu verbinden. Für sämtliche Signalisierung wird das Signalisierungssystem Nr. 7 (SS7) eingesetzt, welches generell der Steuerung digitaler Netze dient, weil hier beispielsweise eine zuverlässige Wegewahl garantiert wird.
Die Dienstvermittlungsstelle muss auch die Verbindungsübergabe (Handover) koordinieren, falls es beim Wechsel der Zelle erforderlich ist, auf einen anderen BSC

umzuschalten. GSM Zusatzfunktionen wie Anrufweiterleitungen und Konferenzschaltungen werden ebenfalls vom MSC unterstützt.
Besondere MSC sind die Übergangsvermittlungsstellen (GMSC), diese operieren als MSC und übernehmen noch zusätzliche Funktionalität, um mit fremden Netzen zu kommunizieren. Die GMSC sind also das Eingangs- und Ausgangstor zwischen dem eigenen Netzwerk (GSM) und anderen Telefonnetzen wie dem Festnetz (ISDN, PSTN), Mobilfunknetz (PLMN) oder sogar Datennetzen (PDN).

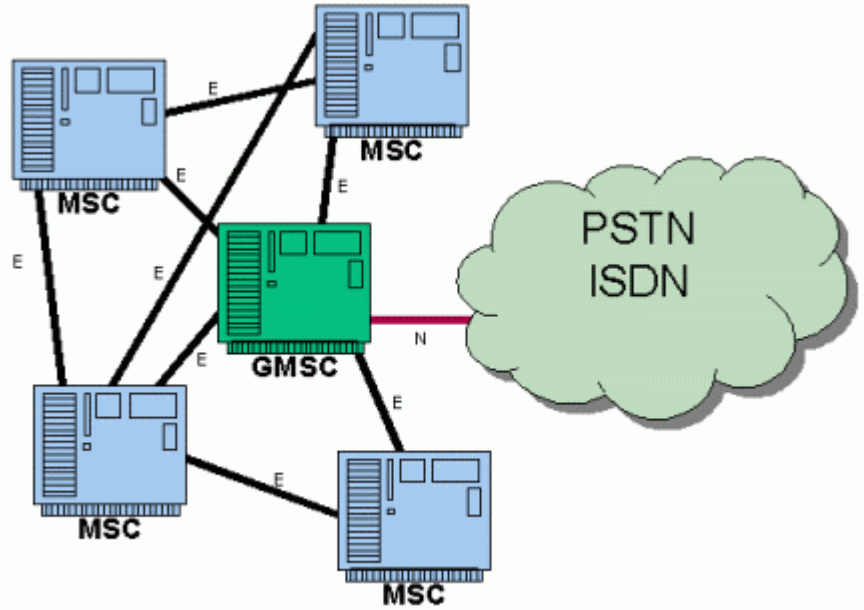

Abbildung 2.3 Übergangsvermittlungsstellen (GMSC)

Das GMSC muss bei einem kommenden Anruf die gewählte Telefonnummer (MSISDN) auswerten und unter Nutzung von Datenbanken (HLR, VLR) dem angewählten Teilnehmer aus dem eigenen Netz zuordnen. Erst danach kann das Routing in die richtige Zelle erfolgen.

2.2.2 Heimatregister (HLR)

Das HLR ist eine Datenbank, die vom MSC für die Wegfindung benutzt wird. Es enthält Daten über alle Kunden eines Netzbetreibers, kann also durchaus mehrere Millionen Einträge haben, was eine hochspezialisierte Datenbank mit

Echtzeitanforderungen erforderlich macht. Für den Verbindungsaufbau ist es unerlässlich, Anfragen innerhalb kürzester Zeitgrenzen beantworten zu können.

Das HLR speichert alle dauerhaften Teilnehmerdaten und einige relevante dynamische Daten für alle Kunden des jeweiligen Netzbetreibers.

Die wichtigsten Daten im HLR sind:

- Eine internationale Kennung (IMSI)
- Die Telefonnummer des GSM Teilnehmers (MSISDN)
- Der Aufenthaltsort des Teilnehmers (LA)
- Eine Nummer für die internationale Lokalisierung (MSRN)

Das HLR wird auf der Hardwareebene meist durch mehrere Module realisiert, die sich in den allermeisten Fällen am selben Ort befinden, hier werden aber in letzter Zeit wegen der Komplexität verstärkt verteilte Datenbanken eingesetzt. Jedes Modul bekommt eine eigene HLR-Nummer zugewiesen und kann wieder in logische Unterpartitionen eingeteilt werden.

2.2.3 Besucherregister (VLR)

Ein VLR ist eine hochdynamische Datenbank, die bis zu eine Millionen Kunden verwalten kann, nämlich die Einträge von allen Mobilstationen, die sich im Einzugsbereich des MSC befinden. Es wird eingesetzt, damit die Daten des HLR nicht zu häufig aktualisiert werden müssen, denn würde man die temporären Daten im HLR speichern, hätte das ein starkes Absinken der Performance des HLR bzgl. Antwortzeiten zur Folge. In der Praxis bilden das MSC und das VLR häufig eine Einheit, da ein reger Datenaustausch stattfindet. Der Vorteil dieser engen Kopplung ist, das man es damit vermeidet, häufig Teilnehmerdaten über eventuell lange Entfernungen zu signalisieren und damit wertvolle Leitungskapazität belegt.

Meldet sich eine Mobilstation im Verwaltungsbereich eines MSC an, werden zunächst alle relevanten Daten vom HLR kopiert. Dann wird eine temporäre IMSI vergeben, die eine Verschleierung der IMSI garantiert, damit diese nicht unverschlüsselt über die Luftschnittstelle übertragen wird.

Die wichtigsten Daten im VLR sind:

- Die genormte Identitätsnummer (IMSI)
- Eine temporäre IMSI (TMSI)
- Die Rufnummer der MS (MSISDN)
- Informationen über den Aufenthaltsort (LAI)
- Daten über unterstütze Dienste
- MSRN

2.3 Betriebs- und Wartungssystem (OSS)

Das OSS stellt die Funktionalität bereit, um einen zuverlässigen Betrieb des Netzwerks zu gewährleisten und eine leichte Wartbarkeit sicherzustellen.

2.3.1 Betriebs- und Wartungszentrale (OMC)

Mit dem OMC ist der Netzbetreiber in der Lage sein Netzwerk so zu konfigurieren, dass ein möglichst reibungsloser Netzbetrieb sichergestellt werden kann. Meistens erfolgt hier eine zentrale Verwaltung und Überwachung mit Hilfe der Führung und Auswertung diverser Statistiken.
Das OMC verwaltet geschäftsrelevante Daten, die aus der vertraglichen Beziehung zum Kunden entstanden sind. Hier erfolgt auch die Abrechnung der Gebühren für geführte Gesprächseinheiten. Besteht ein Roaming-Abkommen werden die Forderungen an den zuständigen Netzbetreiber weitergeleitet, für Kunden des eigenen Netzwerks erfolgt die Rechnungsstellung direkt.
Weiterhin wird im OMC Performancemanagement betrieben, dazu erfolgt eine Überwachung des Netzverkehrs (Traffic) und die Erstellung von Statusberichten einzelner Komponenten. Zusätzlich ist das OMC noch für das Sicherheitsmanagement verantwortlich.

2.3.2 Authentifizierungszentrale (AuC)

Im Gegensatz zum Festnetz ist die Luftschnittstelle leicht angreifbar, weil die Daten per Funk übertragen werden. Trotzdem muss die Identität des Teilnehmers so gut wie möglich geschützt werden und eine sichere Datenübertragung gewährleistet sein.

Hierzu erzeugt und speichert das AuC vertrauliche Daten, kann Schlüssel zur Authentifizierung generieren und prüfen, ob registrierte Dienste für den Benutzer freigeschaltet sind. Für die Generierung der Schlüssel werden spezielle Algorithmen angewendet. Die Authentifizierungszentrale hat eine sehr enge Beziehung zum HLR, weil dort individuelle Daten des Teilnehmers gespeichert sind. Deswegen kann das AuC in einem speziell geschützten Bereich des HLR gelegen sein.

2.3.3 Geräteidentifikationsregister (EIR)

Das EIR ist eine gesonderte Datenbank für alle Gerätekennungen. Hier speichert der Netzbetreiber die weltweit eindeutige Nummer jedes Endgeräts (IMEI). Diese Nummern werden dabei mindestens in eine der folgenden Kategorien eingeordnet:

- Die weiße Liste speichert alle gültigen registrierten Gerätekennungen
- In der grauen Liste sind alle Geräte mit Fehlfunktionen vermerkt. Hier muss i.d.R. eine Aktualisierung der Software erfolgen
- Die schwarze Liste speichert die Kennungen aller gestohlenen, verlorenen oder aus sonstigen Gründen gesperrten Geräte

Nicht immer werden diese Listen unter den Netzbetreibern vollständig abgeglichen, so das eine missbräuchliche Nutzung gestohlener Geräte nicht vollständig ausgeschlossen werden kann.

3 Luftschnittstelle

Die Luftschnittstelle ist die eigentlich interessanteste Schnittstelle im Netzwerk von GSM. Hier wird die Verbindung zwischen Basisstation und Mobilstation hergestellt.
Der eigentliche Medienzugriff basiert auf einer Kombination von FDMA und TDMA. Dieser Standard wurde für GSM von der ETSI festgelegt.
Die Anforderungen an die technische Realisierung der Luftschnittstelle sind sehr hoch, weil ähnlich hohe Anforderungen an die Sprachqualität wie beim Festnetz gestellt werden. Durch die Funkübertragung steht aber nur ein begrenzte Bandbreite von 22,8 kBit/s zu Verfügung, während bei ISDN 64 kBit/s übertragen werden können. Hinzu kommen weitere Probleme wie die sich ständig ändernden

Qualitätsbedingungen des Übertragungsweges durch die Luft, Umwelt, Wetter oder unterschiedliche Bebauungen. Auch können Interferenzen zwischen Nachbarzellen die Übertragung negativ beeinflussen.
Auf der Funkschnittstelle brauchen nur die drei untersten Schichten implementiert sein (Physical Layer, Data Link Layer und Network Layer). Obwohl die höheren Schichten die Luftschnittstelle nicht direkt betreffen, weil die Daten transparent durchgereicht werden, schreibt die ETSI ihre Implementierung vor.

3.1 FDMA für GSM

3.1.1 Frequenzbänder

Für die Senderichtung vom mobilen Gerät zur Basisstation (Uplink) verwendet GSM die Bänder 890 bis 915 MHz (GSM 900) bzw. 1710 bis 1785 MHz (GSM 1800).
Für die Empfangsrichtung von der Basisstation zum mobilen Gerät (Downlink) verwendet GSM die Bänder 935 bis 960 MHz (GSM 900) bzw. 1805 bis 1880 MHz (GSM 1800).

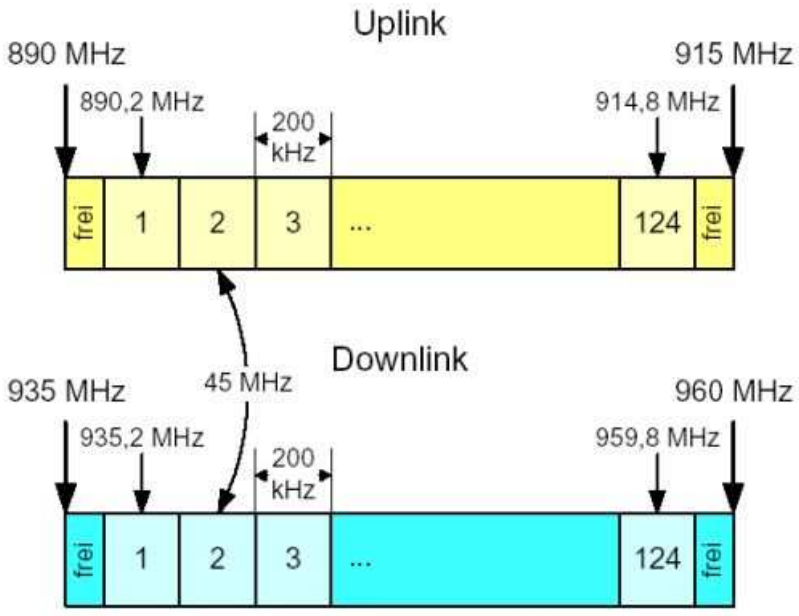

Abbildung 3.1 FDMA-Schema bei GSM 900

Abbildung 3.1 zeigt die Aufteilung der Bänder in Teilstücke mit einem Abstand von 200 KHz. Für GSM 900 stehen also insgesamt 124 Kanäle zur Verfügung, während GSM 1800 372 Kanäle für die Funkübertragung bietet. Wenn verschiedene Netzbetreiber in einer Region existieren, müssen diese Frequenzen unter den Anbietern aufgeteilt werden. Es stehen aber nicht alle Kanäle für die Funkübertragung zur Verfügung, da noch Reservefrequenzen und Trennkanäle benötigt werden. Für Deutschland ergibt sich bei GSM 900 folgende Aufteilung:

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

Die Kanäle werden durch FDD getrennt, der Sende- und Empfangskanal ist also immer um 45 MHz gegeneinander verschoben.

3.1.2 Frequenzsprungverfahren

Häufig gibt es zwischen benachbarten Frequenzen qualitative Unterschiede. Um frequenzselektive Störungen schon im Vorwege zu vermeiden, kann optional ein Frequenzsprungverfahren (Frequency Hopping) angewendet werden, bei der jeder Bit-Datenstrom auf einer anderen Frequenz gesendet wird. Die dabei verwendeten Frequenzen werden aus dem Vorrat der Funkzelle zusammengestellt und der Mobilstation über das Assignment Command (Signalisierung auf Layer 3) gesendet.

3.2 TDMA für GSM

3.2.1 Zeitschlitze (Slots)

Die Anzahl der Funkkanäle sind knappe Ressourcen, jeder Basisstation kann nur grob 1/7 der zur Verfügung stehenden Frequenzen zugeordnet werden. Für das D-Netz (GSM 900) wären das also nur ca. 8 Frequenzen pro Basisstation. Diese Aufteilung hängt mit der Grundgeometrie der Zellen zusammen, die aus k Sechsecken bestehen, wobei K = 7 bei GSM durch die ETSI festgelegt wurde.

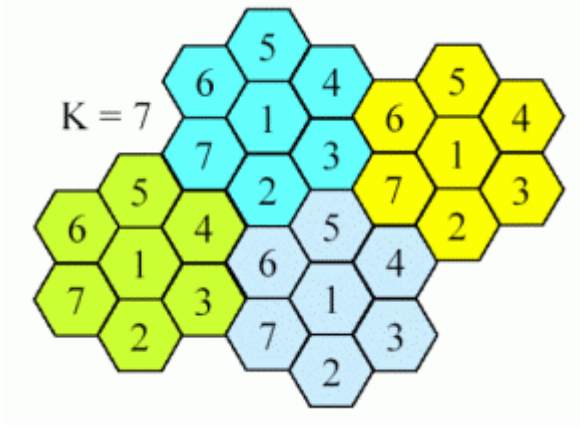

Abbildung 3.2 Funkzellencluster bei GSM

Hinzu kommt das Problem, das einige Frequenzen für Verwaltungszwecke benötigt werden und somit nicht für die eigentliche Datenübertragung zur Verfügung stehen. Die Tatsache, das trotzdem möglichst viele Teilnehmer gleichzeitig telefonieren können macht es deshalb unbedingt erforderlich, die Frequenzen in Zeitschlitze (Slots) einzuteilen. Ein Frequenzkanal aus FDMA wird dabei in 8 Zeitschlitze eingeteilt, welche von 0 bis 7 nummeriert werden und sich immer wieder zyklisch wiederholen. Sendet die Basisstation auf einem Zeitschlitz mit einer bestimmten Nummer, antwortet die Mobilstation auf dem Zeitschlitz mit der gleichen Nummer.

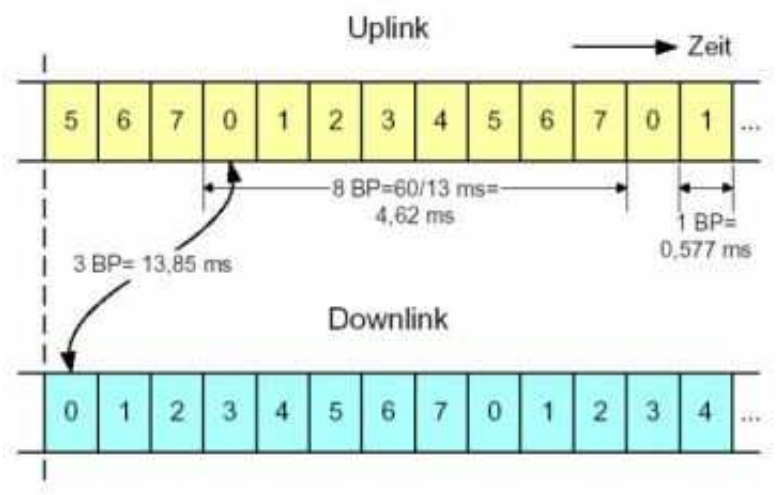

Abbildung 3.3 TDMA für GSM

Damit die Mobilstation nicht gleichzeitig Senden und Empfangen muss, sind die Zeitschlitze für den zugeordneten Uplink und Downlink um 3 Slots gegeneinander verschoben (siehe Abbildung 3.3). Die sich zyklisch wiederholende Folge von Zeitschlitzen repräsentiert so einen bidirektionalen Kanal zwischen der Mobilstation und der Basisstation.

3.2.2 Zeitschlitzinformationen (Bursts)

Innerhalb eines Zeitschlitz wird ein Burst gesendet, der 576,6 µs (15/26 ms) dauert. Dieses Zeitintervall wird auch als Burst Period (BP) bezeichnet. Den Zusammenhang zwischen Zeitschlitzen und Bursts verdeutlicht nochmals Abbildung 3.3.
Die Länge jedes übertragenen Bursts beträgt 156,25 Bit, damit sollen hauptsächlich Nutzdaten transportiert werden. Der Burst kann aber auch für den Verbindungsaufbau bzw. der Verwaltung der Verbindung dienen. Abbildung 3.4 zeigt den Aufbau eines normalen Burst.

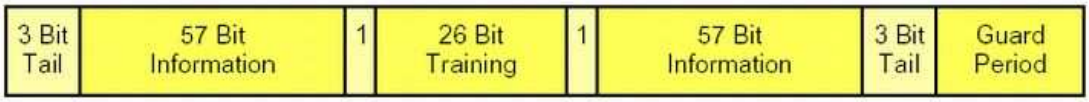

Abbildung 3.4 Aufbau eines normalen Burst

Die jeweils 3 Tail-Bits füllen die Zeitperiode aus, in der die Sendeleistung zu Beginn und am Ende eines Bursts hoch- bzw. heruntergetastet wird. Diese Zeit steht für eine korrekte Datenübertragung nicht zur Verfügung. Stealing-Flags geben an, ob Nutzdaten oder Signalisierungsdaten gesendet werden, in der Abbildung wurde dies durch eine 1 für Nutzdaten gekennzeichnet. Die Trainingssequenz besteht aus vordefinierten Bitmustern, welche für die Kanalschätzung und Synchronisation verantwortlich sind. Schließlich soll der Schutzabstand am Ende des Bursts die Überlappung zeitlich benachbarter TDM-Kanäle wegen unterschiedlicher Pfadverzögerung vermeiden.

Neben dem normalen Burst gibt es 4 weitere Datenformate:

- Bursts zur Frequenzkorrektur, dabei wird eine Frequenzverschiebung dadurch erreicht, dass die Bits auf die logische Null gesetzt werden
- Bursts zur Synchronisation, damit wird auch eine zeitliche Synchronisation zwischen Basisstation und Mobilstation ermöglicht
- Ein Dummy-Burst sendet nicht spezifizierte Daten, falls gerade weder Nutzdaten noch Verwaltungsdaten zu senden sind
- Zugriffsbursts werden eingesetzt, wenn die Mobilstation eine Verbindung mit der Basisstation aufnehmen will

Bei einem normalen Burst werden 114 Bit Nutzdaten in 15/26 ms übertragen. Daraus ergibt sich eine theoretische Obergrenze von 24700 Bit/s für die Datenübertragung, wenn alle 8 Zeitschlitze ein Burst gesendet wird. Diese Datenrate wird jedoch in der Praxis nicht erreicht, weil dazu nur normale Bursts gesendet werden müssten. Man erhält in der Realität 13000 Bit/s für Sprache und 9000 Bit/s für Daten.

3.2.3 Timing Advance

Die Mobilstation muss ihren Burst so aussenden, dass der Zeitschlitz bei der Basisstation eingehalten wird, d.h. ein Burst muss früher gesendet werden, wenn sich die Basisstation weiter entfernt befindet und später gesendet werden, wenn die Basisstation nicht so weit weg ist. Da die Übertragungsgeschwindigkeit physikalisch durch die Geschwindigkeit von Licht beschränkt ist, kann die Basisstation diese zeitlichen Unterschiede ausgleichen. Hierzu wird in regelmäßigen Abständen ein 6 Bit Wert an die MS gesendet, welcher die Entfernung in Stufen angibt. Eine Stufe entspricht dabei einer Entfernung von 555 Metern und pro Stufe muss der Burst 3,7 µs früher gesendet werden.

4 Lokalisierung und Verbindungsaufbau

Eine grundlegende Eigenschaft von GSM ist die weltweite Lokalisierung von Teilnehmern, die mit dem GSM-Netzwerk verbunden sind. Hierzu muss die Mobilstation angeschaltet sein. Das HLR kennt immer den Aufenthaltsort (LA) des Teilnehmers, welcher periodisch durch das VLR aktualisiert wird. Der Wechsel des VLR mit permanenter Verfügbarkeit aller Dienste (auch international) wird dabei als Roaming bezeichnet.

4.1 Kennungen

Für die Lokalisierung sind eine Reihe von Kennungen notwendig, um den Mobilteilnehmer im Netzwerk zu finden.
Die MSISDN ist die eigentliche Telefonnummer, welche mit dem SIM verbunden ist, sie besteht aus dem CC (Beispiel +49), dem NDC (Beispiel 179) und der SN (Beispiel 12345678).
Die IMSI kennzeichnet eindeutig den Teilnehmer im Netzwerk. Sie ist eine interne Nummer des Netzbetreibers und enthält den MCC, den MNC und die Teilnehmerkennung (MSIN).
Die TMSI wird vom VLR vergeben, um nicht die eigentliche IMSI unverschlüsselt über die Luftschnittstelle zu übertragen. Diese temporäre Teilnehmerkennung ist lokal und hat eine Länge von 4 Byte.
Die MSRN verschleiert hingegen sowohl den Aufenthaltsort (LA) als auch die Teilnehmeridentität. Sie wird ebenfalls im VLR auf Anfrage des MSC erzeugt und enthält den VCC, den VNDC und die zugehörige MSC-Kennung.

4.2 Verbindungsaufbau beim Mobile Terminated Call (MTC)

Der interessanteste Fall ist der Verbindungsaufbau zu einer Mobilstation (MTC), wie er in Abbildung 4.1 dargestellt ist. Hierbei ruft irgendein Endgerät innerhalb oder außerhalb des GSM-Netzes eine Mobilstation. Ein einfacherer Fall wäre der Mobile Originated Call (MOC), wo eine Verbindung ausgehend vom mobilen Teilnehmer aufgebaut wird. Hier entfällt aber die Suche nach der Mobilstation.

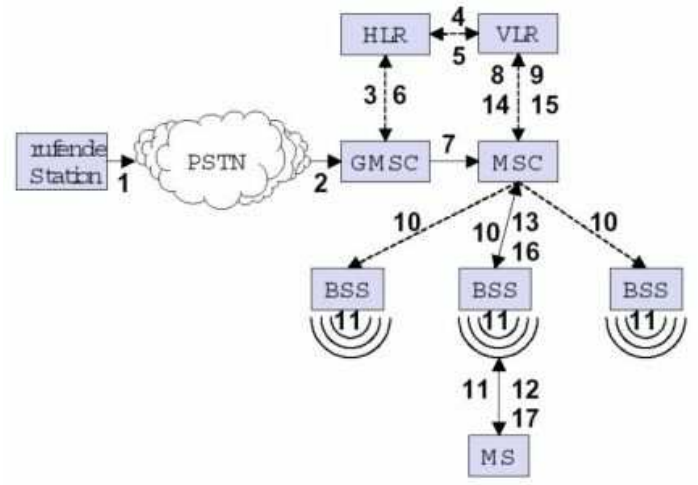

Abbildung 4.1 Ablauf eines Mobile Terminated Call

Im 1. Schritt wird die Nummer der Mobilstation gewählt. An der Telefonnummer kann erkannt werden, dass es sich um eine Mobilstation handelt, deshalb wird der Wunsch zum Aufbau der Verbindung an das GMSC weitergeleitet (Schritt 2). Im dritten Schritt sendet das GMSC eine Verbindungsaufbaunachricht zum HLR, welches bei VLR nach der MSRN fragt und diese empfängt. Dadurch weiß das GMSC, welches MSC gerade für die MS zuständig ist und kann weitervermitteln (Schritt 7). Das MSC muss nun beim VLR den aktuellen Status der MS erfragen, bevor es in Schritt 10 einen Rundruf nach der Mobilstation in allen angeschlossenen BSS starten kann (Paging). Die gezielte Suche nach der richtigen Basisstation würde zu aufwendig sein und damit zu lange dauern. In Schritt 12 und 13 antwortet die Mobilstation. Jetzt müssen in Schritt 14 und 15 die Sicherheitsüberprüfungen wie z.B. die Authentifizierung des Teilnehmers oder Generierung der Schlüssel durchgeführt werden bevor in Schritt 16 und 17 die eigentliche Verbindung aufgebaut wird.

5 Verbindungsübergabe (Handover)

Unter Handover versteht man die Übergabe der Verbindung an eine andere Basisstation (BTS), damit ist ein Neukonfiguration der Kommunikationsverbindung erforderlich. Die laufende Verbindung darf dabei nicht durch den Handover-Mechanismus unterbrochen werden.

Die Verbindungsübergabe wird durch das Netzwerk initiiert, man spricht deshalb auch von Network Originated Handover. Wesentlicher Vorteil dieses Verfahrens ist, dass der Netzbetreiber den Algorithmus für die Verbindungsübergabe selber festlegen kann und Änderungen unabhängig von den mobilen Endgeräten durchgeführt werden können.

5.1 Gründe für Handover

Durch die Struktur der zellulären Systeme kann der Bewegungsbereich des Teilnehmers nicht vollständig abgedeckt werden. Die MS bewegt sich aus dem Empfangsbereich der Basisstation hinaus, die Stärke des Signals nimmt dann kontinuierlich ab und fällt unter einen gewissen Schwellenwert.
Der zweite wesentliche Grund ist ein zu hohes Verkehrsaufkommen in einer Zelle, wenn zu viele Teilnehmer gleichzeitig telefonieren wollen, also die aktuelle Netzlast zu hoch ist. Hier kann die Verbindung in eine weniger belastete Zelle verschoben werden.

5.2 Arten von Handover

Abbildung 5.1 zeigt drei typische Arten der Verbindungsübergabe.
Im 1. Fall spricht man von Intrazellenübergabe, hier findet nur ein Wechsel der Übertragungsfrequenz statt. Fall 2 ist die häufigste Art der Verbindungsübergabe (Interzellen, Intra BSC). Die Kontrolle bleibt hier beim BSC. Beim 3. Fall (Inter BSC, Intra MSC) wechselt die Kontrolle auf einen anderen BSC, wird aber weiterhin durch das gleiche MSC verwaltet.
Ein eher seltener Fall wäre ein Wechsel des MSC (Inter MSC), hier bleibt die Kontrolle beim ursprünglichen MSC, die Verbindung wird lediglich logisch auf das andere MSC übertragen. Man spricht daher auch von einem Anker-MSC.

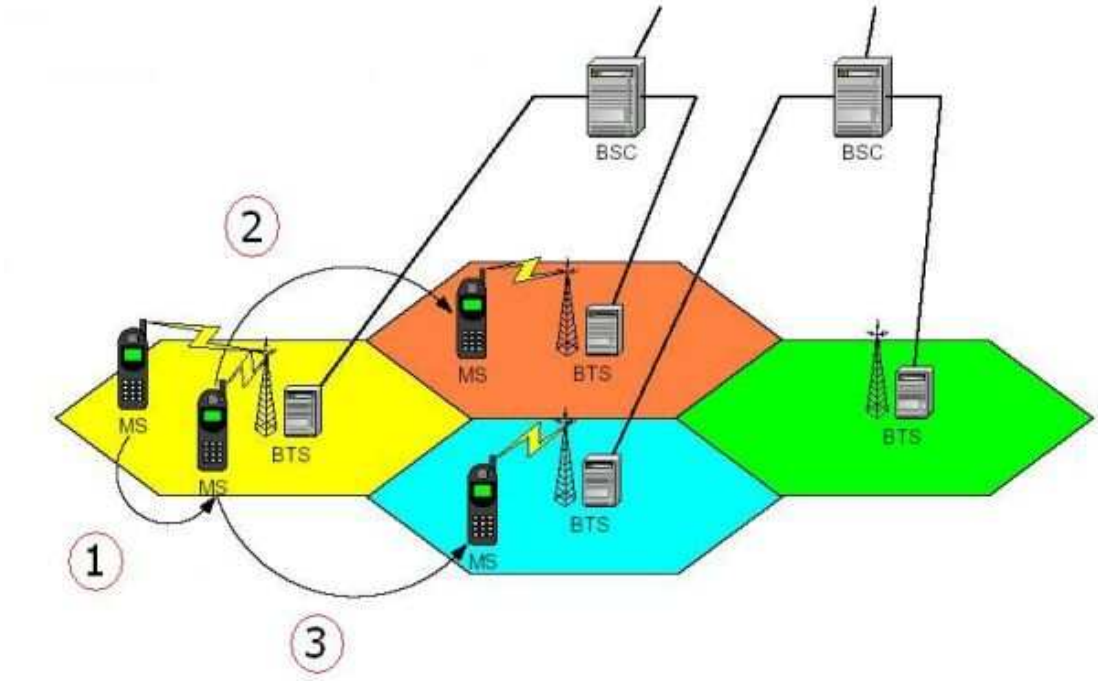

Abbildung 5.1 Übergabearten bei Handover

5.3 Übergabeentscheidung

In der Praxis hat man i.d.R. keine eindeutigen Zellengrenzen, d.h. die Mobilstation kann die Signale von mehreren Basisstationen empfangen. Ziel ist es, die Notwendigkeit eines Handovers rechtzeitig zu erkennen, damit zu häufiges Hin- und Herschalten zwischen den beteiligten Basisstationen vermieden wird. Hierfür werden periodische Messungen durchgeführt, deren Ergebnisse etwa alle ½ Sekunde von der MS an die BTS gesendet werden. Dadurch hat die Basisstation eine Kontrolle über die Sende- und Empfangsqualität auf dem Up- und Downlink.
Abbildung 5.2 zeigt einen typischen Verlauf der Messwerte für die Signalqualität.

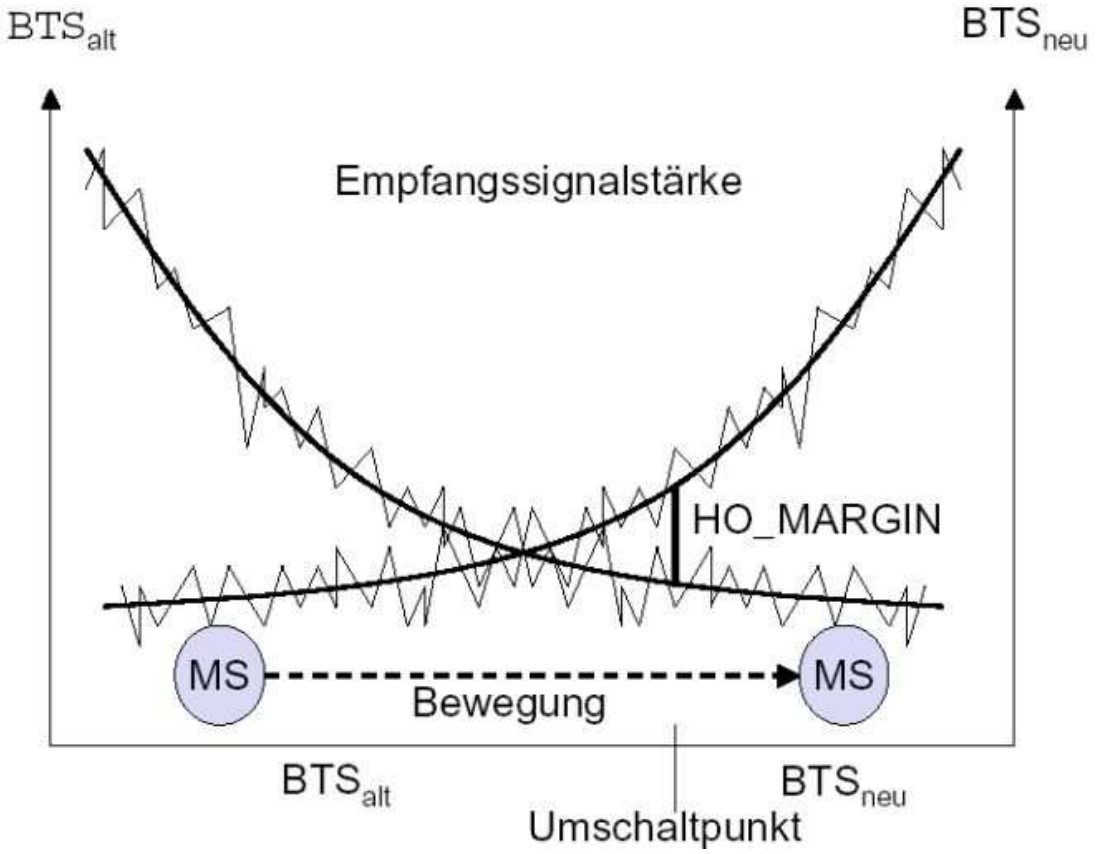

Abbildung 5.2 Übergabeentscheidung bei Handover

Die Messwerte werden mit einem Schwellenwert verglichen (HO_MARGIN). Um kurzfristige Schwankungen auszugleichen wird stets nur ein Durchschnittswert herangezogen, der durch den BSC berechnet wird. Wählt der Netzbetreiber den Schwellenwert zu niedrig, besteht die Gefahr, dass sich das System aufschaukelt und ständig hin- und hergeschaltet wird, was mit einem hohen Verwaltungsaufwand verbunden ist (Ping-Pong-Effekt). Andererseits könnte bei einem zu hohen Schwellenwert das Signal ganz verloren gehen, was einen Verbindungsabbruch zur Folge hätte.

Trotz der guten Wahl eines geeigneten Schwellenwertes findet in der Realität meist mehr als eine Verbindungsübergabe statt, weil zu viele externe Faktoren auf das System einwirken. Die Anzahl der Verbindungsübergaben hängt außerdem noch vom Zellenradius (maximal 35 km) und der Relativgeschwindigkeit des mobilen Teilnehmers ab (maximal 250 km/h).

6 Weiterentwicklungen

Die Bandbreite von GSM war ursprünglich nur für die Übertragung von Sprachdaten konzipiert. Abhängig vom Netzbetreiber können Datenraten von 9,6 bis 14,4 kBit/s realisiert werden, was für Sprache durchaus ausreichend war. Mit dem schnellen Wachstum moderner Dienste wie Internetanwendungen, Laden von Dateien, E-Mail oder Zugang zu Datennetzen, die heute mit einer modernen Mobilstation möglich sind, wurden höhere Datenraten notwendig. Diese Phase der Mobilfunkgeneration wird auch als Phase 2+ bezeichnet, damit soll der Übergang zwischen der Phase 2 (GSM) und Phase 3 (UMTS) angedeutet werden.

6.1 HSCSD

Durch bessere Kodierverfahren kann eine maximale Datenrate von 14400 Bit/s pro Kanal erreicht werden. Wird HSCSD angewendet, können mehrer Zeitschlitze im TDMA-Rahmen belegt werden, bei Bündelung von maximal 8 Kanälen könnten so theoretisch 115,2 kBit/s erreicht werden. In der Praxis werden meistens 4 Kanäle gebündelt, wobei diese Einteilung nicht zwingend ist und auch nicht symmetrisch erfolgen muss. Abbildung 6.1 zeigt die häufigsten Verbindungsmöglichkeiten.

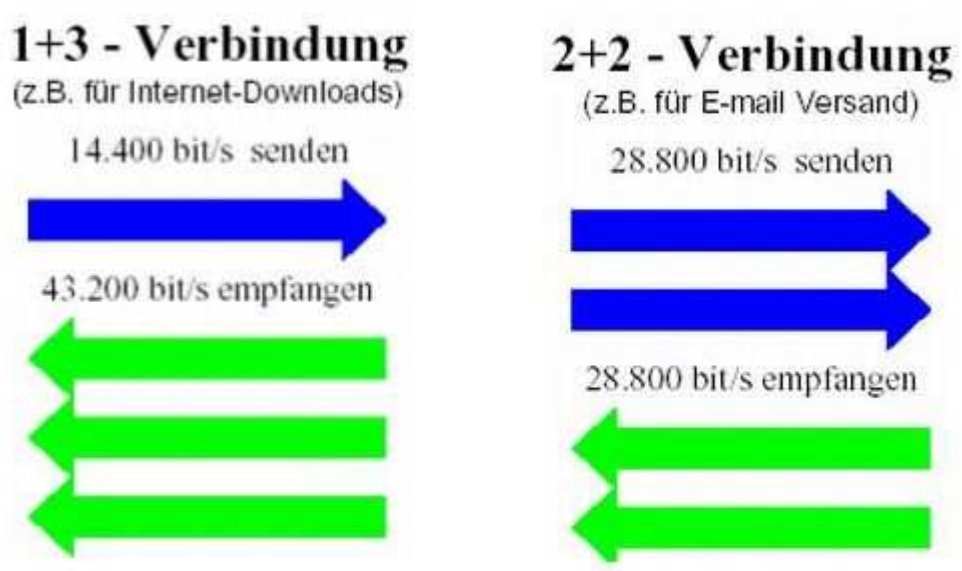

Abbildung 6.1 Verbindungsmöglichkeiten bei HSCSD

Für HSCSD sind nur wenige Änderungen am Netzwerk erforderlich. Allerdings müssen die mobilen Endgeräte diesen Datendienst unterstützen, er kann also mit älteren Endgeräten nicht genutzt werden.
Die Vorteile von HSCSD liegen in der kostengünstigen Installation und der festen Übertragungsbandbreite, mit der auch größere Datenmengen transportiert werden können. Dagegen ist die starke Beanspruchung des Netzes ein negativer Aspekt, denn durch HSCSD werden Sprachkanäle blockiert und so unnötig die knappen Funkressourcen verschwendet. Außerdem ist HSCSD ein leitungsvermitteltes Verfahren, der Kunde muss also für die ganze Zeit bezahlen, in der eine Verbindung zwischen Basisstation und Mobilstation besteht.

6.2 GPRS

General Packet Radio Service (GPRS) basiert auf einer Paketvermittlung, so das die vorhandenen Kapazitäten besser genutzt werden können. Es ist vor allem sinnvoll für sogenannte Push-Dienste, bei dem stoßartig größere Mengen an Daten übertragen werden müssen, wie es etwa dem Verhalten eines Nutzers im Internet entspricht.
Die Verbindung ist „Always Online“, der Kunde bezahlt aber nicht nach Zeit, sondern nur nach dem übertragenen Volumen.
Es besteht außerdem ein Zugang in verschiedene existierende Netze, die beispielsweise auf IP oder X.25 basieren können.
Es können Bandbreiten bis zu 171,2 kBit/s erreicht werden, hierzu bedarf es aber einer Bündelung von 8 Kanälen und einer optimalen Empfangsqualität. In der Praxis hängt die tatsächlich erreichte Datenrate stark von dem Datenaufkommen anderer Teilnehmer in der selben Funkzelle und der Auslastung des BSS ab.
Die Änderungen am Netzwerk sind beträchtlich, weil GSM ursprünglich nur für einen leitungsvermittelten Dienst ausgelegt war und damals niemand an die Möglichkeit gedacht hatte, Pakete über die Luftschnittstelle zu übertragen. Nach zahlreichen Änderungen am GSM-Netz ist GPRS flächendeckend seit 2001 in Deutschland verfügbar.
Für die Paketvermittlung sind auch spezielle Endgeräte nötig, die in verschiedene Klassen eingeteilt werden: Geräte der Klasse A können gleichzeitig Daten und Sprache übertragen, die Klasse B unterstützt diese Funktion hingegen nicht, d.h.

während eines Paketversands können keine Sprachdaten übertragen werden und ein eingehender Anruf würde lediglich gemeldet. Auf der anderen Seite können während eines Telefonats keine Pakete gesendet oder empfangen werden. Geräte der Klasse C muss man manuell in den Sprach- oder Datenmodus umschalten.
Ähnlich wie bei HSCSD kann die Bündelung der Kanäle auch asymmetrisch erfolgen, um sich an das Verhalten des Nutzers anzupassen. Hier wurden sogar spezielle Multislot-Klassen gebildet, wie sie aus Abbildung 6.2 ersichtlich sind.

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

Abbildung 6.2 Multislot-Klassen

Pro Kanal können 13,4 bis maximal 21,4 kBit/s übertragen werden, wobei die maximale Anzahl der benutzten Kanäle für Sende- und Empfangsrichtung auf 5 beschränkt ist.

Literaturverzeichnis

Bücher

David, Klaus, Benkner, Thorsten, 2003: Digitale Mobilfunksysteme, Stuttgart: Teubner Verlag

Eberspächer, Jörg, Vögel, Hans-Jörg, Bettstetter, Christian, 2001: GSM, Global System for Mobile Communication, Stuttgart: Teubner Verlag

Lipinski, Klaus, 1999: Lexikon Mobilkommunikation, Bonn: mitp

Roth, Jörg, 2002: Mobile Computing, Heidelberg: dpunkt.verlag

Schiller, Jochen, 2003: Mobilkommunikation, München: Pearson Studium

Quellen im Internet

BSI-Faltblatt: GSM-Mobilfunk
http://www.bsi.bund.de/literat/doc/gsm/index.htm

Informationszentrum für den Mobilfunk
http://www.izmf.de

Mobilfunkportal für GSM und UMTS
http://www.umtslink.at/GSM-Start.htm

Mobilkommunikation am Beispiel von GSM
http://www.fh-fulda.de/~werner/gsm2001.htm

Proseminar Rechnerkommunikation und Telefon: GSM
http://goethe.ira.uka.de/seminare/rkt/gsm/

Webseite der GSM Association
http://www.gsmworld.com/index.shtml