1 GSM

Mit GSM, dem Global System for Mobile Communication begann Anfang der 90'er Jahre ein beispielloser Wandel in der mobilen Kommunikation. Hatte das Vorläufersystem C-Netz in seiner Glanzzeit in Deutschland knapp eine Million Teilnehmer, brachten es die vier GSM Netze im Jahre 2007 auf über 65 Millionen. Dies ist vor allem einer stetigen Weiterentwicklung in allen Bereichen der Telekommunikation und dem anhaltenden Preisverfall der digitalen Technik sowie der Mobiltelefone zu verdanken. Das erste Kapitel dieses Buches beschäftigt sich ausführlich mit der Technik dieses Systems, das die Grundlage für die paketdatenorientierte Erweiterung GPRS und das Nachfolgesystem UMTS bildet.

1.1 Leitungsvermittelnde Datenübertragung

Verbindungsmatrix

GSM Mobilfunknetze zählen genauso wie drahtgebundene Fernsprechnetze, auch Festnetze genannt, zu den leitungsvermittelnden Kommunikationsnetzen (Circuit Switched Networks). Beim Beginn eines Gespräches wird dabei vom Netzwerk eine Leitung direkt von Teilnehmer zu Teilnehmer geschaltet, die diese dann exklusiv für sich verwenden können. In der Vermittlungsstelle (Switching Center) befindet sich dafür, wie in Abb. 1.1 gezeigt, eine Verbindungsmatrix (Switching Matrix), die einen beliebigen Eingang mit einem beliebigen Ausgang verbinden kann. Nachdem die Verbindung aufgebaut wurde, werden alle Signale transparent über die Verbindungsmatrix zwischen den Teilnehmern ausgetauscht. Erst wenn einer der beiden Teilnehmer die Verbindung beendet, wird die Vermittlungsstelle wieder aktiv und baut die Verbindung in der Verbindungsmatrix wieder ab. Diese Vorgehensweise ist in einem Festnetz und einem Mobilfunknetz identisch.

Drahtgebundene Fernsprechnetze wurden anfangs nur für die Sprachdatenübertragung konzipiert, und es wurde ein analoger Kanal zwischen den Teilnehmern aufgebaut. Mitte der 80'er Jahre wurden diese Netze in Deutschland digitalisiert. Dies bedeutet, dass die Sprache heute nicht mehr analog von Ende zu Ende übertragen wird, sondern in der Vermittlungsstelle digitalisiert

und danach digital weiter übertragen wird. Am anderen Ende werden die digitalen Sprachdaten wieder in ein analoges Signal umgewandelt und über die Telefonleitung zum Endteilnehmer geschickt. Bei einem ISDN Anschluss findet diese Unwandlung von analog nach digital und zurück bereits im Endgerät (z.B. Telefon) statt, und die Sprache wird Ende zu Ende digital übertragen.

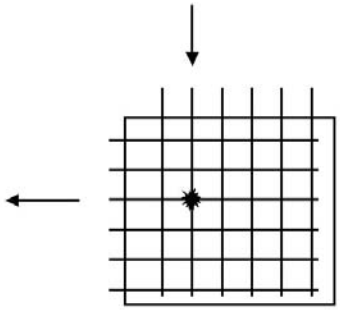

Abb. 1.1: Verbindungsmatrix in einer Vermittlungsstelle

An dieser Stelle sei angemerkt, dass manche Netzbetreiber inzwischen dazu übergehen, in der Vermittlungsstelle die Verbindungsmatrix durch ein so genanntes Media Gateway zu ersetzen. Damit wird erreicht, dass Sprachverbindungen im Kernnetzwerk nicht mehr leitungsvermittelnd sondern über IP oder ATM Paketnetzwerke übertragen werden. Dieser Ansatz ist unter dem Namen Bearer Independent Core Network bekannt und in Kapitel 3.1.2 näher beschrieben. In GSM Radionetzwerk wird jedoch weiterhin die in diesem Kapitel beschriebene leitungsvermittelnde Technik verwendet.

Gleiche Hardware unterschiedliche Systeme

Für GSM wurde das Rad nicht neu erfunden. Statt ein komplett neues System zu entwickeln, wurde auf die bereits vorhandene Festnetztechnik in Form von Vermittlungsstellen und Weitverkehrsübertragungstechnik zurückgegriffen. Neu entwickelt werden musste jedoch die Technik für den eigentlichen Anschluss der Teilnehmer. Im Festnetz ist der Teilnehmeranschluss sehr einfach, für jeden Teilnehmer werden lediglich zwei Kabel benötigt. In einem Mobilfunknetzwerk jedoch kann der Teilnehmer seinen Standort frei wählen. Somit ist es nicht mehr möglich, ein Gespräch immer über den gleichen Anschluss der Verbindungsmatrix zu einem Teilnehmer durchzuschalten.

Da ein Mobilfunknetzwerk wie ein Festnetz viele Vermittlungsstellen besitzt, die jeweils ein begrenztes geographisches Gebiet

versorgen, ist in einem Mobilfunknetzwerk nicht einmal gewährleistet, dass ein Teilnehmer immer über die gleiche Vermittlungsstelle zu erreichen ist. Somit kann auch die im Festnetz verwendete Software für die Teilnehmerverwaltung und Gesprächsvermittlung für ein Mobilfunknetzwerk nicht weiterverwendet werden. Statt einer statischen 1:1 Zuweisung von Teilnehmer und Leitung wurde die Software in der Vermittlungsstelle um eine Mobilitätsmanagementkomponente erweitert. Diese verwaltet alle Teilnehmer und kennt den aktuellen Aufenthaltsort jedes erreichbaren Teilnehmers.

Da ein Teilnehmer auch während eines Gespräches den Aufenthaltsort ändern kann und somit eventuell das Gespräch auf eine andere Leitung geschaltet werden muss, ist auch die Gesprächsverwaltung neu entwickelt worden.

Weiterverwendet werden im Mobilfunknetzwerk jedoch fast die komplette Hardware einer Festnetzvermittlungsstelle, sowie die unteren Softwareschichten, die für das Schalten der Verbindungsmatrix und die Signalisierung zuständig sind. Somit ist es auch nicht weiter verwunderlich, dass alle großen Netzwerkhersteller wie z.B. Siemens, Nortel, Ericsson, Nokia oder Alcatel heute ihre Hardwareplatform für Vermittlungsstellentechnik sowohl für Festnetze, als auch für Mobilfunknetze anbieten. Einzig die Software entscheidet darüber, für welchen Zweck die Vermittlungsstelle eingesetzt wird.

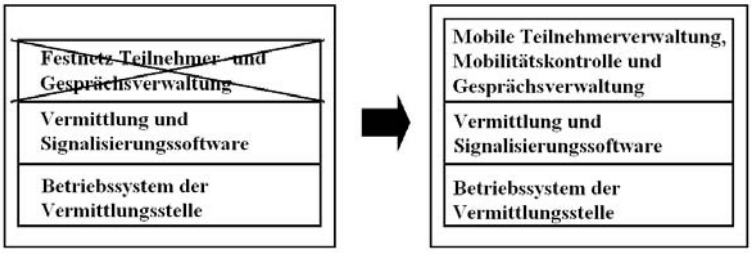

Abb. 1.2: Softwareänderungen von Festnetz- zu Mobilfunkvermittlung

1.2 Standards

Da sich im weltweiten Markt für Telekommunikationsnetzwerke viele Firmen um Aufträge der Netzwerkbetreiber bemühen, ist eine Standardisierung der Schnittstellen und technischen Vorgänge notwendig. Ohne diese Standards, die unter anderem von der

ITU

International Telecommunication Union (ITU) definiert wurden, wäre eine länderübergreifende Telefonie nicht möglich, und Netzwerkbetreiber wären fest an einen Netzwerklieferanten gebunden.

Einer der wichtigsten ITU Standards ist das in Kapitel 1.4 vorgestellte Signalisierungssystem SS-7 für die Gesprächsvermittlung. Viele ITU Standards repräsentieren jedoch nur den kleinsten gemeinsamen internationalen Nenner. Jedes Land behielt sich vor, nationale Erweiterungen vorzunehmen. Dies verursacht in der Praxis enorme Kosten bei der Softwareentwicklung, da für jedes Land spezielle Erweiterungen nötig sind. Auch der Übergang zwischen Netzen unterschiedlicher Länder wird dadurch sehr erschwert.

ETSI / 3GPP

Mit GSM wurde zum ersten Mal ein einheitlicher Standard in Europa für die mobile Kommunikation geschaffen, der später auch von vielen Ländern außerhalb Europas übernommen wurde. Diesem Umstand ist es zu verdanken, dass Teilnehmer heute weltweit in allen GSM Netzen, die ein sogenanntes Roamingabkommen mit seinem Heimatnetz abgeschlossen haben, telefonieren und mobil Daten übertragen können. Auch wurde es so möglich, die Entwicklungskosten wesentlich zu reduzieren, da die Systeme ohne große Modifikationen in alle Welt verkauft werden können. Dem European Telecommunication Standards Institute (ETSI), das neben GSM auch noch viele weitere Telekommunikationsstandards für Europa spezifiziert hat, kam dabei eine wesentliche Rolle bei der Erarbeitung dieser Standards zu. Die ETSI GSM Standards umfassen dabei eine Vielzahl von unterschiedlichen Standarddokumenten, auch Technical Specifications (TS) genannt, die jeweils einen Teil des Systems beschreiben. Da GSM heute international verwendet wird und es zu Beginn der UMTS Standardisierung absehbar war, dass auch dieser über Europa hinaus große Bedeutung erlagen würde, gründete ETSI zusammen mit weiteren internationalen Standardisierungsgremien aus aller Welt das 3rd Generation Partnership Project (3GPP). Dieses Gremium ist seither für die Standardisierung von GSM und UMTS verantwortlich. In den nachfolgenden Kapiteln befinden sich für eine weitere Vertiefung einzelner Themen Verweise auf diese Spezifikationen, die auf http://www.3gpp.org kostenlos abgerufen werden können.

1.3 Übertragungsgeschwindigkeiten

DS0

Die kleinste Geschwindigkeitseinheit in einem Telekommunikationsnetzwerk ist der Digital Signal 0 (DS0) Kanal. Dieser hat eine feste Übertragungsgeschwindigkeit von 64 kbit/s. Über einen solchen Kanal können Sprache oder auch Daten übertragen werden. Aus diesem Grund wird üblicherweise nicht von einem Sprachkanal, sondern allgemein von einem Nutzdatenkanal gesprochen.

E-1

Die Referenzeinheit in einem Telekommunikationsnetzwerk ist die E-1 Verbindung, die zumeist über Twisted Pair oder Koaxialkabel geführt wird. Die Bruttodatenrate einer E-1 Verbindung beträgt 2.048 MBit/s. Diese Bruttodatenrate ist in 32 Zeitschlitze (Timeslots) à 64 kbit/s aufgeteilt, in denen jeweils unabhängige Datenströme (DS0s) übertragen werden.

Ein Zeitschlitz pro E-1 wird für die Synchronisation benötigt und kann somit keinen DS0 übertragen. Somit stehen pro E-1 Verbindung 31 Zeitschlitze zur Verfügung. Davon können beispielsweise 29 oder 30 Zeitschlitze für die Nutzdatenübertragung verwendet werden und ein oder zwei für die nötigen Signalisierungsdaten. Mehr zu Signalisierungsdaten in Kapitel 1.4 über das SS-7 Protokoll.

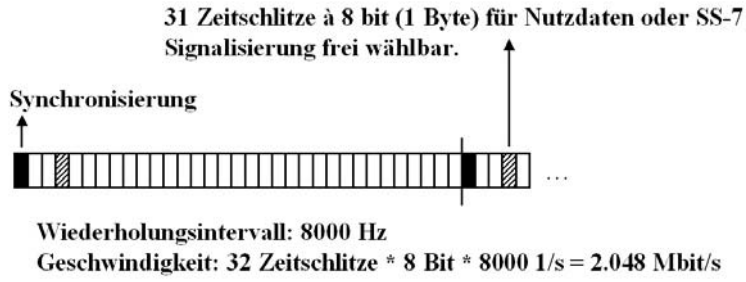

Abb. 1.3: Zeitschlitzarchitektur einer E-1Verbindung

Zumeist reicht ein E-1 mit 31 DS0s nicht für Verbindungen zwischen Vermittlungsstellen aus. Für diesen Fall gibt es die E-3 Verbindung, ebenfalls über Twisted Pair oder Koaxialkabel mit einer Geschwindigkeit von 34.368 MBit/s. Dies entspricht 512 DS0s.

STM

Für höhere Übertragungsgeschwindigkeiten und für große Übertragungsdistanzen werden optische Systeme verwendet, die nach

dem Synchronous Transfer Mode (STM) Standard arbeiten. Die nachfolgende Tabelle zeigt einige Übertragungsraten und die Anzahl der Nutzdatenkanäle à 64 kbit/s (DS0s), die pro Glasfaserpaar übertragen werden können.

Typ	Geschwindigkeit	Anzahl 64 kbit/s Verbindungen (ca.)
STM-1	155.52 MBit/s	2.300
STM-4	622.08 MBit/s	9.500
STM-16	2488.32 MBit/s	37.000
STM-64	9953.28 MBit/s	148.279

Die hier vorgestellten Übertragungssysteme und Übertragungsgeschwindigkeiten werden in den meisten Ländern dieser Welt verwendet. Lediglich Nordamerika und Japan bilden eine Ausnahme und verwenden eigene Übertragungsstandards.

1.4 Das Signalisierungssystem Nr. 7

Teilnehmersignalisierung

Für den Aufbau, den Erhalt und den Abbau einer Verbindung müssen zwischen den Geräten Signalisierungsinformationen ausgetauscht werden. Bei Teilnehmern mit analogem Festnetztelefon findet diese Signalisierung durch Abnehmen oder Auflegen des Handapparats statt, die gewünschte Rufnummer wird dem Netzwerk dann per Pulswahl oder der schnelleren und heute üblichen Dual Tone Multi Frequency (DTMF) Tonwahl übermittelt. Bei ISDN Festnetz- und auch bei GSM Mobiltelefonen erfolgt diese Signalisierung über einen eigenen Signalisierungskanal. Die Informationen wie zum Beispiel die Telefonnummer werden digital in Nachrichtenpaketen übertragen.

Netzwerksignalisierung

Sind mehrere Netzwerkkomponenten wie z.B. mehrere Vermittlungsstellen am Verbindungsaufbau beteiligt, müssen zwischen diesen ebenfalls Signalisierungsinformationen ausgetauscht werden. Für diese Signalisierung wird in digitalen Fernsprechnetzwerken das Signalisierungssystem Nummer 7 (SS-7) verwendet. Auch der GSM Mobilfunkstandard verwendet SS-7, wobei jedoch zusätzliche SS-7 Protokolle bei ETSI standardisiert wurden, die für die zusätzlichen Aufgaben eines Mobilfunknetzwerkes notwendig sind.

Grundsätzlich gibt es bei SS-7 drei unterschiedliche Netzwerkknoten:

SSP Service Switching Points: SSPs sind Vermittlungsstellen, also Netzwerkelemente, über die Daten- und Sprachverbindungen aufgebaut, zugestellt oder weitergeleitet werden können.

SCP Service Control Points: SCPs sind Datenbanken mit dazugehörender Software, die den Aufbau einer Verbindung beeinflussen können. Bei GSM werden SCPs z.B. für die Speicherung des aktuellen Aufenthaltsorts jedes Teilnehmers verwendet. Bei einem Verbindungsaufbau zu einem mobilen Teilnehmer müssen dann die Vermittlungsstellen zuerst dort nachfragen, wo sich der Teilnehmer befindet. Mehr hierzu im Abschnitt 1.6.3 über das Home Location Register.

STP Signaling Transfer Points: STPs sind für das Weiterleiten von Signalisierungsnachrichten zwischen SSPs und SCPs notwendig, da nicht jeder Netzwerkknoten eine dedizierte Verbindung zu jedem anderen Knoten unterhalten kann. Von der prinzipiellen Funktionsweise kann man diese Knoten mit IP Routern im Internet vergleichen, die ebenfalls Pakete in unterschiedliche Netze an unterschiedliche Geräte weiterleiten. Im Gegensatz zu diesen befördern STPs aber keine Nutzdaten wie Datenrufe oder Telefongespräche, sondern nur die zum Aufbau, Abbau oder Aufrecherhaltung einer Verbindung notwendigen Signalisierungsinformationen.

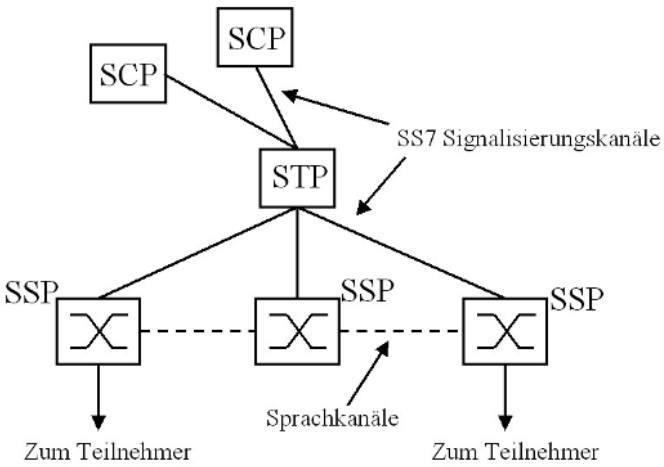

Abb. 1.4: Ein SS-7 Netzwerk mit einem STP, zwei SCP Datenbanken und 3 Vermittlungsstellen

1.4.1 Allgemeiner SS-7 Protokoll Stack

Das Signalisierungssystem Nummer 7 (SS-7) basiert auf einer Anzahl von Protokollen, die schichtweise aufeinander aufgebaut sind. Das bekannteste und meistverwendete Modell zur Erklärung der Protokolle auf den unterschiedlichen Schichten ist dabei das OSI 7 Schichten Modell.

MTP

Das Message Transfer Part – 1 (MTP-1) Protokoll beschreibt auf Schicht 1 des OSI Modells die Eigenschaften des Übertragungsmediums. Diese Schicht wird auch Physical Layer genannt. Dazu gehört unter anderem die Definition der möglichen Kabelarten, die zu verwendenden Signalpegel, mögliche Übertragungsgeschwindigkeiten, etc.

Auf Schicht 2, dem Data Link Layer, werden Nachrichten in Pakete eingepackt und mit einer Start- und Endekennung versehen.

Der Network Layer auf Schicht 3 ist für die Weiterleitung von Datenpaketen zuständig. Jedes Paket wird dazu mit einer Quell- und Zieladresse versehen. Auf diese Weise können Netzwerkknoten Datenpakete weiterleiten (routen), die nicht für sie selber bestimmt sind. Im SS-7 Protokollstapel ist das MTP-3 Protokoll hierfür zuständig. Für Leser, die bereits Kenntnisse in der TCP/IP Welt haben, sei an dieser Stelle erwähnt, dass das MTP-3 Protokoll sehr gut mit dem IP Protokoll verglichen werden kann. Statt einer IP Adresse verwendet das MTP-3 Protokoll aber so genannte Point Codes, um Quelle und Ziel einer Nachricht eindeutig zu identifizieren.

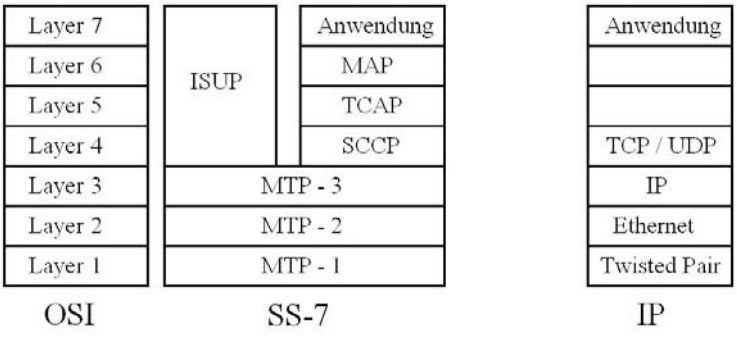

Abb 1.5: SS-7 Protokollstack im Vergleich zum IP Protokollstack

ISUP

Auf Layer 4-7 kommen nun je nach Bedarf unterschiedliche Protokolle zum Einsatz. Dient die Signalisierungsnachricht zum Auf- oder Abbau eines Übertragungskanals, wird das ISDN User Part (ISUP) Protokoll verwendet.

ISUP Messages

Abb. 1.6 zeigt, wie ein Gespräch zwischen zwei Teilnehmern aufgebaut wird. Teilnehmer A ist dabei ein Mobilfunkteilnehmer und B ein Festnetzteilnehmer. Während A über eine Mobilfunkvermittlungsstelle verbunden ist, die auch Mobile Switching Center (MSC) genannt wird, ist B ein Festnetzteilnehmer.

Um Teilnehmer B zu erreichen, übermittelt A seiner MSC die Telefonnummer von B. Anhand der Vorwahl von B erkennt die MSC, dass B ein Festnetzteilnehmer ist. Für die Sprachübertragung gibt es in Abbildung 1.6 dorthin eine direkte Verbindung. Dies kann auch durchaus in der Praxis vorkommen, wenn zum Beispiel von einem Mobiltelefon in München ein Festnetztelefon ebenfalls in München angerufen wird.

IAM

Da es sich bei B um einen Festnetzteilnehmer handelt, muss die MSC nun einen Nutzdatenkanal für die Sprachübertragung zur Festnetzvermittlungsstelle aufbauen. Dies geschieht über das ISUP Protokoll mit einer Initial Address Message (IAM). Diese Nachricht enthält unter anderem die Telefonnummer von B, sowie die Information, welcher Nutzdatenkanal zwischen den zwei Vermittlungsstellen für das Gespräch verwendet werden soll. Die IAM wird dabei nicht direkt zwischen den Vermittlungsstellen ausgetauscht, sondern läuft über einen STP.

ACM

Die Festnetzvermittlungsstelle empfängt diese Nachricht, analysiert die darin enthaltene Rufnummer und stellt die Verbindung zu Teilnehmer B her. Sobald dessen Telefon klingelt, wird eine Address Complete Message (ACM) an die MSC zurückgeschickt. Die MSC weiß somit, dass die Rufnummer korrekt war und Teilnehmer B gerufen wird.

ANM

Beantwortet Teilnehmer B den Anruf durch Abnehmen des Telefonhörers, schickt die Festnetzvermittlungsstelle eine Answer Message (ANM) an die MSC zurück, und das Telefongespräch beginnt.

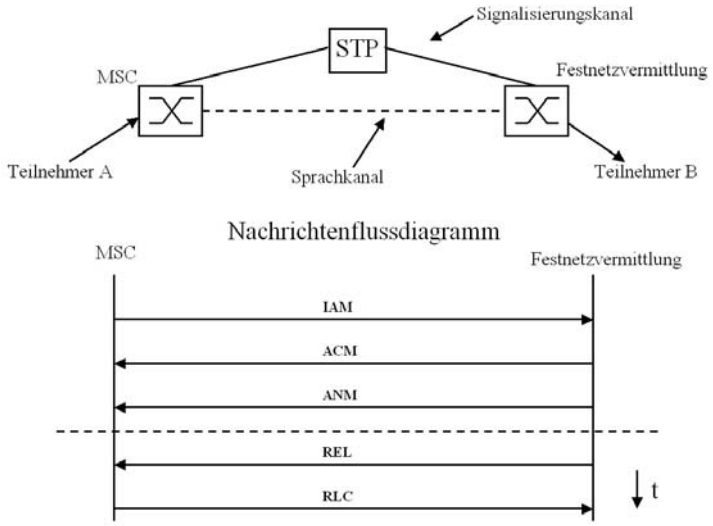

Abb. 1.6: Aufbau einer Verbindung zwischen Vermittlungsstellen

REL, RLC

Legt Teilnehmer B am Ende des Gespräches auf, schickt die Festnetzvermittlungsstelle eine Release Message (REL) an die MSC. Diese schickt daraufhin eine Release Complete Message (RLC) als Quittung zurück. Beendet Teilnehmer A das Gespräch, laufen diese Nachrichten in die jeweils andere Richtung.

SCCP

Für die Kommunikation zwischen Vermittlungsstellen (SSPs) und Datenbanken (SCPs) kommt auf Schicht 4 das Signalling Connection and Control Part (SCCP) zum Einsatz. Seine Funktionsweise ist in weiten Teilen sehr ähnlich zum TCP und UDP Protokoll in der IP Welt. Über Protokolle der Schicht 4 können unterschiedliche Anwendungen auf einem System unterschieden werden. In TCP und UDP gibt es dazu so genannte Ports. Wird ein PC z.B. als Web Server und gleichzeitig als FTP Server verwendet, sind diese Server zwar über die gleiche IP Adresse erreichbar, verwenden aber unterschiedliche Port Nummern. Anhand dieser Port Nummer kann dann der Protokollstapel entscheiden, an welche Applikation das Datenpaket weitergegeben wird. In der SS-7 Welt wird diese Aufgabe von SCCP erledigt. Statt Port Nummern werden hier jedoch Subsystem Nummern (SSNs) an unterschiedliche Applikationen vergeben.

TCAP

Für den Zugriff auf Datenbanken wurde für SS-7 das Transaction Capability Application Part (TCAP) entwickelt. Dies stellt für SCP Datenbankabfragen eine Anzahl von unterschiedlichen Nachrichtenbausteinen bereit, um Abfragen möglichst einheitlich zu gestalten.

1.4.2 Spezielle SS-7 Protokolle für GSM

Neben den bereits genannten SS-7 Protokollen die sowohl in einem Festnetz, wie auch im GSM Mobilfunknetz verwendet werden, sind für ein GSM Mobilfunknetz eine Reihe weiterer Protokolle notwendig, um den zusätzlichen Aufgaben eines Mobilfunknetzwerkes Rechnung zu tragen.

MAP

Das Mobile Application Part (MAP) Protokoll: Dieses Protokoll ist in ETSI TS 09.02 spezifiziert und wird für die Kommunikation zwischen einer MSC und dem Home Location Register (HLR) verwendet, das Teilnehmerinformationen verwaltet. Das HLR wird zum Beispiel gefragt, wenn eine MSC eine Verbindung zu einem mobilen Benutzer herstellen soll. Das HLR liefert in einem solchen Fall der MSC die Information zurück, wo sich der gewünschte Teilnehmer gerade aufhält. Mit dieser Information kann dann die MSC das Gespräch zur aktuellen Vermittlungsstelle dieses Teilnehmers mit den in Abbildung 1.6 beschriebenen ISUP Nachrichten herstellen.

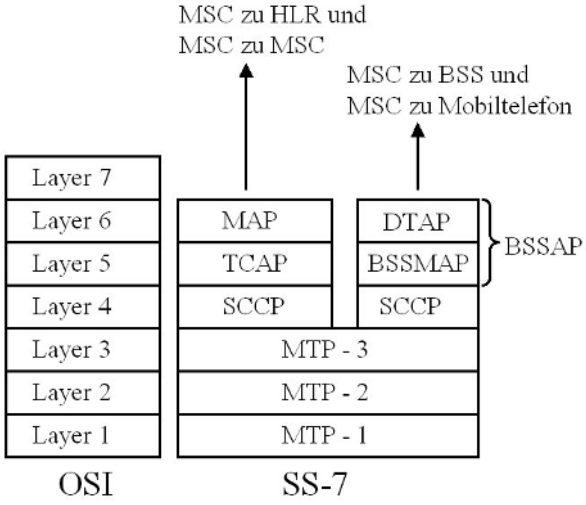

Abb. 1.7: Erweiterungen des SS-7 Protokollstacks für GSM

MAP wird außerdem zwischen MSCs verwendet, wenn sich ein Teilnehmer während eines Gesprächs in das Versorgungsgebiet einer anderen MSC bewegt und die Verbindung dorthin weitergeleitet werden muss.

Wie in Abb. 1.7 dargestellt ist, setzt das MAP Protokoll auf die bereits beschriebenen TCAP, SCCP und MTP Protokolle auf.

BSSMAP Das Base Station Subsystem Mobile Application Part (BSSMAP): Dieses Protokoll dient der Kommunikation zwischen MSC und dem Radionetzwerk. Es wird zum Beispiel verwendet, um dem Radio Netzwerk die Anweisung zu geben, einen dedizierten Funkkanal für eine neue Verbindung zu einem Mobilfunkteilnehmer herzustellen. Da es sich hier nicht um Datenbankabfragen wie beim MAP Protokoll handelt, setzt BSSMAP nicht auf TCAP, sondern direkt auf SCCP auf.

DTAP Direct Transfer Application Part (DTAP): Über dieses Protokoll kann ein Endgerät, im englischen auch Mobile Station (MS) genannt, direkt mit einer MSC Nachrichten austauschen. Um eine Verbindung zu einem anderen Teilnehmer aufzubauen, wird beispielsweise die SETUP Nachricht verwendet. Diese enthält unter anderem die Telefonnummer des Gesprächspartners. Alle Netzwerkelemente zwischen Endgerät und MSC leiten diese Nachrichten transparent weiter.

1.5 Die GSM Subsysteme

Ein GSM Netzwerk wird in 3 unterschiedliche Subsysteme eingeteilt:

BSS Das Basestation Subsystem (BSS), auch Radio Netzwerk genannt, enthält alle Elemente und Funktionen, die für die Verbindung zwischen Netzwerk und mobilen Teilnehmern über die Funkschnittstelle, die auch Luftschnittstelle genannt wird, notwendig sind.

NSS Das Network Subsystem (NSS), auch Core Network oder Kernnetzwerk genannt, enthält alle Komponenten für die Vermittlung von Gesprächen, für die Teilnehmerverwaltung und das Mobilitätsmanagement.

IN Das Intelligent Network Subsystem (IN), besteht aus SCP Datenbanken, die zusätzliche Dienste zur Verfügung stellen. Einer der wichtigsten IN Dienste in einem Mobilfunknetzwerk ist beispielsweise der Prepaid Service, der das Abtelefonieren eines zuvor eingezahlten Guthabens in Echtzeit erlaubt.

1.6 Das Network Subsystem

Die wichtigste Aufgabe des NSS ist der Verbindungsaufbau, Verbindungskontrolle und Vermittlung von Verbindungen zwischen unterschiedlichen mobilen Vermittlungsstellen (MSC) und anderen Netzwerken. Andere Netzwerke können z.B. das nationale Festnetz, das im englischen auch Public Standard Telefone Network (PSTN) genannt wird, internationale Festnetze sowie andere nationale und internationale Mobilfunknetze sein. Außerdem umfasst das NSS die Teilnehmerverwaltung. Die dazu notwendigen Komponenten und Prozesse werden in den nächsten Abschnitten beschrieben und werden schematisch in Abb. 1.8 dargestellt.

1.6.1 Die Mobile Vermittlungsstelle (MSC)

MSC

Die Mobile Vermittlungsstelle, auch Mobile Switching Center (MSC) genannt, ist das zentrale Element eines Mobilfunknetzwerkes, das auch Public Land Mobile Network (PLMN) genannt wird.

Call Control

Alle Verbindungen zwischen Teilnehmern, auch wenn diese sich in der gleichen Funkzelle befinden, werden immer über eine MSC geleitet und kontrolliert. Diese Aufgabe wird Call Control (CC) genannt und umfasst folgende Aufgaben:

- Registrieren des Teilnehmers (Registration): Beim Einschalten des Endgeräts registriert sich dieses im Netzwerk und ist anschließend für alle Teilnehmer erreichbar.
- Der Verbindungsaufbau (Call Routing) zwischen zwei Teilnehmern.
- Weiterleiten von Kurznachrichten (SMS).

Mobility Management

Da sich Teilnehmer im Mobilfunknetzwerk frei bewegen können, ist die MSC auch für die Mobilitätskontrolle (Mobility Management) zuständig. Man unterscheidet zwei Zustände:

- Authentifizieren des Teilnehmers bei Verbindungsaufnahme (Authentication): Dies ist notwendig, da ein Teilnehmer nicht mehr wie im Festnetz anhand der verwendeten Leitung identifiziert werden kann. Weitere Information über die Teilnehmerauthentifizierung im Zusammenhang mit dem Authentication Center sind in Kapitel 1.6.4 zu finden.

- Besteht keine aktive Verbindung zwischen Netzwerk und Endgerät, muss das Endgerät eine Änderung seiner Position dem Netzwerk mitteilen, um für den Fall eines eingehenden Anrufs oder einer Kurzmitteilung (SMS) auffindbar zu sein. Dieser Vorgang wird Location Update genannt und in Kapitel 1.8.1 näher beschrieben.
- Bewegt sich ein Teilnehmer während einer bestehenden Verbindung, sorgt die MSC dafür, dass die Verbindung nicht abbricht und in die jeweils geeigneten Zellen weitergegeben wird. Dieser Vorgang wird Handover genannt und in Kapitel 1.8.3 näher beschrieben

Um mit anderen MSCs und Netzwerkkomponenten zu kommunizieren, ist die MSC mit diesen über standardisierte Schnittstellen verbunden. Dies ermöglicht, dass die Netzwerkkomponenten von unterschiedlichen Netzwerkherstellern stammen können.

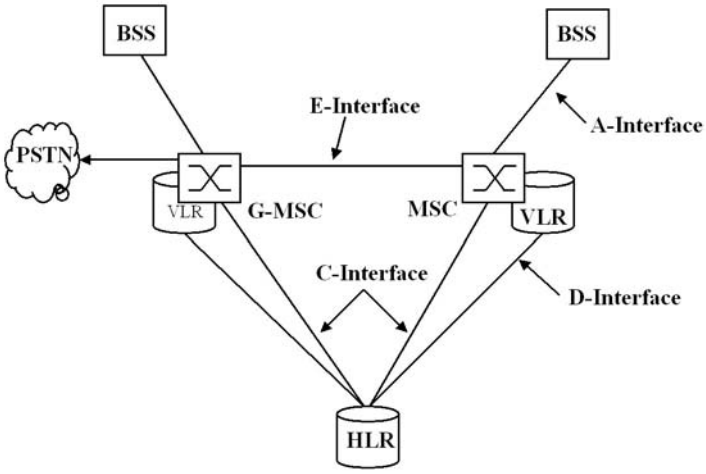

Abb. 1.8: Schnittstellen und Komponenten im NSS

A-Interface

Das BSS, über das alle Teilnehmer mit dem Mobilfunknetzwerk kommunizieren, wird über eine Anzahl von 2 MBit/s E-1 Leitungen mit einer MSC verbunden. Diese Verbindung wird A-Interface genannt. Wie in Kapitel 1.4 bereits gezeigt, werden auf dem A-Interface das BSSMAP und DTAP Protokoll verwendet. Da eine E-1 Verbindung nur maximal 31 Nutzdatenverbindungen übertragen kann, werden pro MSC viele E-1 Verbindungen ver-

wendet. In der Praxis bedeutet das, dass diese gebündelt und dann über eine optische Verbindung wie z.B. STM-1 zum BSS weitergeleitet werden. Dies ist auch deshalb sinnvoll, da elektrische Signale nur mit großem Aufwand über weite Strecken transportiert werden können. So kann es durchaus vorkommen, dass MSC und BSS hundert Kilometer oder mehr voneinander entfernt sind.

E-Interface

Da eine MSC nur eine begrenze Vermittlungsleistung und Rechenkapazität besitzt, besteht ein großes Mobilfunknetzwerk normalerweise aus dutzenden oder sogar hunderten voneinander unabhängiger MSCs. Jede MSC versorgt dabei einen eigenen geographischen Bereich. Auch zwischen den MSCs werden E-1 Verbindungen verwendet, die wieder optisch gebündelt und weitergeleitet werden. Da sich ein Teilnehmer während eines Gesprächs auch über die geographische Versorgungsgrenze einer MSC hinaus bewegen kann, muss das Gespräch entsprechend an die für dieses Gebiet zuständige MSC weitergeben werden können. Diese Gesprächsweitergabe wird auch Handover genannt. Die dafür notwendigen Signalisierungs- und Sprachverbindungen werden E-Interface genannt. Als Protokoll zwischen den MSCs kommt ISUP für die Verbindungskontrolle und MAP für die Signalisierung des Handovers zum Einsatz. Näheres hierzu in Kapitel 1.8.3.

C-Interface

Über das C-Interface ist die MSC mit der Teilnehmerdatenbank, dem Home Location Register (HLR) des Mobilfunknetzwerkes verbunden. Während zum A-Interface und dem E-Interface immer auch zwingend Sprachkanäle gehören, ist das C-Interface eine reine Signalisierungsverbindung. Sprachkanäle sind für das C-Interface nicht notwendig, da an einem Ende eine Datenbank angeschlossen ist, die keine Sprachverbindungen vermittelt oder gar annehmen kann. Trotzdem werden auch für diese Schnittstelle E-1 Verbindungen verwendet. Alle Zeitschlitze werden dabei für die Signalisierung verwendet, bzw. bleiben leer.

Sprachübertragung

Wie im Kapitel 1.3 beschrieben, wird in digitalen leitungsvermittelnden Festnetz- und Mobilfunksystemen ein Sprachkanal im Kernnetz in einem 64 kbit/s E-1 Zeitschlitz übertragen. Ein analoges Sprachsignal muss dazu aber zuerst digitalisiert werden. Bei einem analogen Festnetzanschluß erfolgt dies in der Vermittlungsstelle, bei einem ISDN Anschluss und bei einem GSM Teilnehmer bereits im Endgerät.

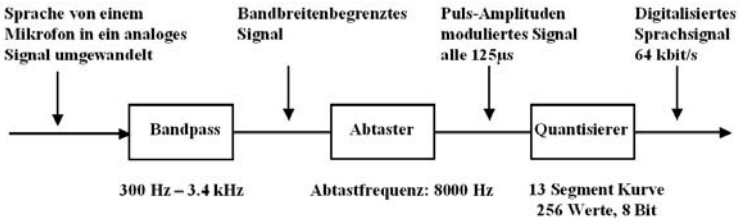

Abb. 1.9: Sprachdigitalisierung

Ein analoges Sprachsignal wird dabei in 3 Schritten digitalisiert: Im ersten Schritt wird die Bandbreite des analogen Signals auf 300 Hz – 3.400 Hz begrenzt, damit dies später auch in einem 64 kbit/s Timeslot übertragen werden kann. Danach wird das analoge Signal 8.000 mal pro Sekunde abgetastet und der Wert einem Quantisierer übergeben. Der Quantisierer wandelt nun den analog abgetasteten Wert in einen 8 bit digitalen Wert von 0 – 255 um.

Je höher die Amplitude des abgetasteten Wertes, also je lauter das Sprachsignal, desto größer der digitale Wert. Um auch leise Töne möglichst gut zu übertragen, erfolgt die Quantisierung nicht linear im gesamten Bereich, sondern nur abschnittsweise. Für kleine Amplituden, also leise Sprache, werden dabei wesentlich mehr digitale Werte verwendet, als für laute Töne.

PCM

Das so digitalisierte Signal wird Pulse Code Modulated (PCM) Signal genannt. Für welche Lautstärke welcher digitale Wert zugeordnet ist, beschreibt in Europa der a-Law Standard, in Nordamerika der µ-Law Standard. Die Verwendung unterschiedlicher Standards erschwert natürlich die Sprachübertragung zwischen Netzen, die jeweils den anderen Standard verwenden. Zwischen Deutschland und Nordamerika muss das Sprachsignal deshalb an den Netzübergängen entsprechend umkodiert werden.

Billing

Da die MSC alle Verbindungen kontrolliert, ist sie auch für die spätere Abrechnung (Billing) zuständig. Zu diesem Zweck erstellt die MSC für jedes Gespräch einen so genannten Billing Record, der nach dem Gespräch gespeichert und zum Abrechnungssystem übertragen wird. Der Billing Record enthält dabei unter anderem die Informationen über die Nummer des Anrufers, Nummer des Angerufenen, die ID der Funkzelle bei Gesprächsbeginn, Zeitpunkt des Gesprächsbeginns, Dauer des Gesprächs und vieles mehr.

Prepaid Billing

Verbindungen von Prepaid Teilnehmern werden hingegen schon während der laufenden Verbindung von einem Billing Dienst

abgerechnet, der sich auf einem IN System und nicht in der MSC befindet. Mehr hierzu in Kapitel 1.11.

1.6.2 Das Visitor Location Register (VLR)

VLR

Jeder MSC ist eine Visitor Location Register (VLR) Datenbank zugeordnet, die Informationen über alle aktuellen Teilnehmer in deren Versorgungsbereich verwaltet. Diese Daten sind jedoch nur eine temporäre Kopie der Originaldaten, die sich im Home Location Register (HLR) befinden, das im nächsten Abschnitt behandelt wird. Das VLR wird hauptsächlich verwendet, um die Signalisierung zwischen MSC und HLR zu reduzieren. Bewegt sich ein Teilnehmer in den Bereich einer MSC, werden die Daten einmalig aus dem HLR in das VLR kopiert und stehen somit lokal bei jeder Verbindungsaufnahme von oder zu Teilnehmern für eine Überprüfung zur Verfügung. Die Überprüfung der Teilnehmerdaten bei jedem Verbindungsaufbau ist notwendig, da jedem Teilnehmer individuell Dienste aktiviert oder gesperrt werden können. So ist es zum Beispiel möglich, ausgehende Anrufe eines Teilnehmers zu sperren oder Missbrauch zu unterbinden.

Kombiniertes MSC und VLR

Während es die ETSI Standards ermöglichen, das VLR als eine eigenständige Hardwarekomponente zu implementieren, haben alle Hersteller diese jedoch als Softwarekomponente in die MSC integriert. Dies ist möglich, da MSC und VLR über unterschiedliche SCCP Subsystemnummern (vgl. Kapitel 1.4.1) angesprochen werden.

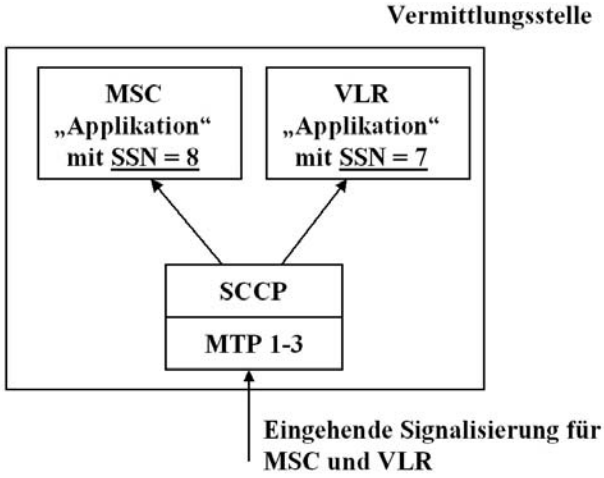

Abb. 1.10: Vermittlungsstelle mit integriertem VLR

Bewegt sich ein Teilnehmer aus dem Versorgungsbereich einer MSC, werden die Daten des Teilnehmers aus dem HLR in das VLR der neuen MSC kopiert und danach aus dem alten VLR gelöscht.

D-Interface

Für die Kommunikation mit dem HLR wurde in den GSM Standards das D-Interface spezifiziert, das zusammen mit den Schnittstellen der MSC in Abb. 1.8 im Überblick dargestellt ist.

1.6.3 Das Home Location Register (HLR)

HLR

Das Home Location Register (HLR) ist die Teilnehmerdatenbank eines GSM Mobilfunknetzwerkes. Es enthält für jeden Teilnehmer Informationen, welche Dienste des Mobilfunknetzwerkes diesem zur Verfügung stehen.

IMSI

Die International Mobile Subscriber Identity, kurz IMSI genannt, ist eine weltweit eindeutige Nummer, die einen Teilnehmer identifiziert und bei fast allen teilnehmerbezogenen Signalisierungsvorgängen im GSM Netzwerk verwendet wird. Neben der SIM Karte wird die IMSI auch im HLR gespeichert und ist dort der Schlüssel zu allen Informationen eines Teilnehmers.

Die IMSI besteht aus folgenden Teilen:

- Dem Mobile Country Code (MCC): Dieser gibt an, aus welchem Land der Teilnehmer stammt. Nachfolgend eine Tabelle mit einigen MCCs:

MCC	**Land**
262	Deutschland
232	Österreich
228	Schweiz
208	Frankreich
310	USA
604	Marokko
505	Australien

- Dem Mobile Network Code (MNC): Dieser bestimmt, aus welchem Netzwerk der Teilnehmer stammt. Dies ist notwendig, da es in einem Land mehrere unabhängige

Mobilfunknetzwerke geben kann. In Deutschland gibt es z.B. folgende Mobile Network Codes: 01 für T-Mobile, 02 für Vodafone, 03 für E-Plus und 07 für O2 Deutschland.

- Der Mobile Subscriber Identification Number (MSIN): Diese Nummer ist im nationalen Netzwerk eindeutig.

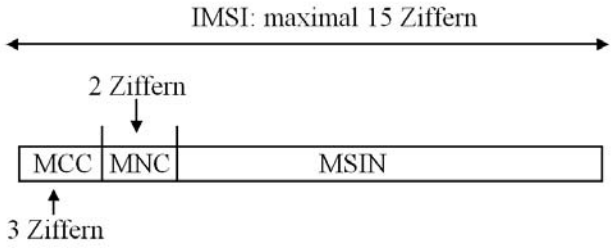

Abb. 1.11: Die IMSI

Da die IMSI international eindeutig ist, kann mit einem Mobiltelefon auch im Ausland telefoniert werden. Beim Einschalten übermittelt das Mobiltelefon die auch auf der SIM-Karte des Teilnehmers gespeicherte IMSI an die dortige Mobilfunkvermittlungsstelle. Anhand der ersten Ziffern erkennt die Vermittlungsstelle, aus welchem Land (MCC) und aus welchem Netzwerk (MNC) dieser Teilnehmer stammt und kann somit das HLR im Heimnetzwerk des Teilnehmers nach dessen Daten befragen.

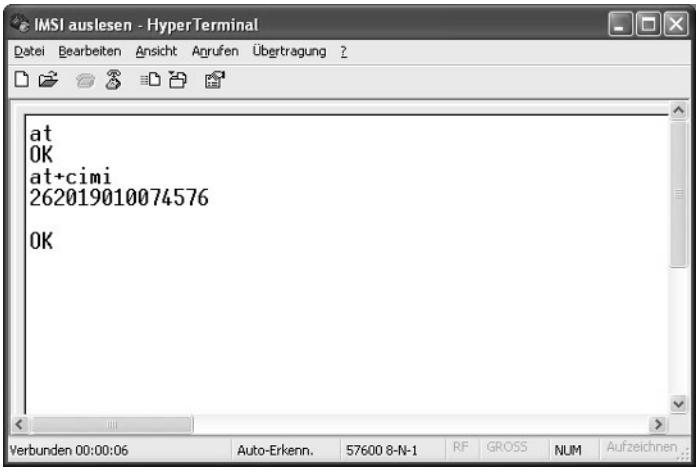

Abb. 1.12: IMSI per PC aus einer SIM Karte auslesen

Die IMSI kann auch mit einem PC und einem geeigneten seriellen Mobiltelefonkabel ausgelesen werden. Über ein Terminalprogramm wie z.B. HyperTerminal muss dem Mobiltelefon dafür der in ETSI TS 07.07 standardisierte Befehl ‚at+cimi' übergeben werden. Wie in Abbildung 1.12 zu sehen ist, liest das Mobiltelefon die IMSI aus der SIM Karte aus und gibt diese als Antwort auf den Befehl zurück.

MSISDN

Die eigentliche Telefonnummer eines Teilnehmers, die auch Mobile Subscriber ISDN Number (MSISDN) genannt wird, darf maximal 15 Stellen lang sein. Sie besteht aus:

- dem Country Code, also der internationalen Vorwahl des Landes, wie z.B. (+)49 für Deutschland
- dem National Destination Code (NDC), der nationalen Vorwahl des Netzbetreibers, normalerweise 3 Stellen lang
- einer eindeutigen Nummer innerhalb eines Mobilfunknetzwerks

Zwischen der IMSI und der MSISDN besteht ein 1:1 oder 1:N Zusammenhang, der im HLR festgelegt wird. Normalerweise bekommt ein Mobilfunkkunde nur eine Telefonnummer für seinen Mobilfunkanschluss. Da jedoch die IMSI und nicht die MSISDN einen Teilnehmer eindeutig identifiziert, ist es auch möglich, mehrere Telefonnummern pro Teilnehmer zu vergeben.

Ein weiterer Vorteil der IMSI als Schlüssel für alle Teilnehmerinformation ist, dass die Telefonnummer eines Teilnehmers jederzeit geändert werden kann, ohne dass die SIM Karte getauscht werden muss. Hierfür muss lediglich im HLR eine neue MSISDN für den Benutzer eingetragen werden, die IMSI bleibt unverändert. Da auf der SIM Karte nur die IMSI, nicht jedoch die MSISDN gespeichert ist, sind hier keine Änderungen notwendig. Dies bedeutet auch, dass das Endgerät seine eigene Telefonnummer nicht kennt. Dies ist auch nicht notwendig, da diese bei einem abgehenden Telefonanruf von der MSC automatisch in die Nachrichten für den Verbindungsaufbau eingefügt wird, damit sie beim angerufenen Teilnehmer angezeigt werden kann.

Mobile Number Portability

Seit der Einführung der Mobile Number Portability (MNP) in Deutschland kann über die nationale Vorwal (NDC) nicht mehr ermittelt werden, zu welchem Netzbetreiber ein Teilnehmer ge-

hört. Dies hat zwar den großen Vorteil für den Kunden, seine Rufnummer bei einem Wechsel zu einem anderen Netzbetreiber mitnehmen zu können, verursacht aber einen großen Mehraufwand bei Signalisierung, Routing und Billing. Statt das Gespräch über den NDC (Vorwahl) zum richtigen Mobilfunknetzwerk weiterzuleiten, muss jetzt zuvor eine Mobile Number Portability Datenbank befragt werden.

Basic Services

Neben der IMSI und MSISDN enthält das HLR für jeden Teilnehmer eine Menge weiterer Informationen über Dienste, die dieser verwenden darf. In der nachfolgenden Tabelle sind einige grundsätzliche Dienste (Basic Services) aufgeführt, die für einen Teilnehmer aktiviert werden können:

Basic Service	**Aufgabe**
Telefonie	Gibt an, ob ein Teilnehmer für die Sprachtelefonie freigeschaltet ist.
Short Message Service (SMS)	Gibt an, ob ein Teilnehmer für den Kurznachrichtendienst SMS freigeschaltet ist.
Datendienste	Gibt an, welche leitungsvermittelnden Datendienste (z.B. 2.4 kbit/s, 4.8 kbit/s, 9.6 kbit/s und 14.4. kbit/s) der Teilnehmer verwenden darf.
FAX	Aktiviert oder sperrt FAX Übertragungen für einen Teilnehmer.

Supplementary Services

Neben diesen grundsätzlichen Diensten bietet ein GSM Netzwerk seinen Teilnehmern eine Menge weiterer Dienste an, die ebenfalls einzeln freigeschaltet oder gesperrt werden können. Da dies zusätzliche Dienste sind, werden diese auch Supplementary Services genannt:

Supplementary Service	**Zweck**
Call Forward Unconditional (CFU)	Erlaubt einem Benutzer das Setzen und Löschen einer sofortigen Gesprächsweiterleitung.

	Ist diese konfiguriert, wird der Ruf automatisch weitergeleitet, ohne dass das Telefon klingelt.
Call Forward Busy (CFB)	Gibt dem Benutzer die Möglichkeit, ein Gespräch an eine andere Telefonnummer weiterzuleiten, wenn während eines laufenden Gesprächs ein weiterer Anruf eingeht.
Call Forward No Reply (CFNRY)	Leitet ein Gespräch weiter, wenn der Teilnehmer das Gespräch nach einer bestimmten Zeit nicht angenommen hat. Das Intervall kann vom Benutzer vorgegeben werden (z.B. 25 Sekunden)
Call Forward Not Reachable (CFNR)	Leitet ein Gespräch weiter, wenn das Mobiltelefon ausgeschaltet ist, oder keinen Netzempfang hat.
Barring of All Outgoing Calls (BAOC)	Sperren aller abgehenden Anrufe. Kann auch vom Netzwerkbetreiber gesetzt werden, wenn der Teilnehmer seine Rechnung nicht bezahlt hat.
Barring of All Incoming Calls (BAIC)	Ankommende Anrufe werden zum Teilnehmer nicht durchgestellt.
Call Waiting (CW)	Das Anklopfen. Ermöglicht die Signalisierung eines weiteren ankommenden Gesprächs. Das erste Gespräch kann dann auf Halten (HOLD) gelegt werden, um das Zweite anzunehmen. Kann vom Netzbetreiber erlaubt oder gesperrt sein und vom Teilnehmer an- oder abgeschaltet werden.
Call Hold (HOLD)	Zum Halten eines Gesprächs um ein zweites eingehendes Gespräch anzunehmen oder um

	ein zweites Gespräch zu beginnen.
Calling Line Identification Presentation (CLIP)	Anzeige der Rufnummer des Anrufers.
Calling Line Identification Restriction (CLIR)	Mit CLIR kann ein Anrufer die Anzeige seiner Rufnummer beim Gesprächspartner unterdrücken.
Connected Line Presentation (COLP)	Zeigt dem Anrufer, auf welche Telefonnummer sein Anruf umgeleitet wird, wenn eine Anrufweiterleitung aktiviert ist.
Connected Line Presentation Restriction (COLR)	Unterdrückung des COLP Service.
Multiparty (MPTY)	Erlaubt dem Teilnehmer, Konferenzen mit mehreren anderen Teilnehmern zu führen. Üblich sind Konferenzbrücken mit 3 oder 6 Teilnehmern.

Die meisten Supplementary Services sind vom Netzwerkbetreiber an- und abschaltbar und ermöglichen ihm somit, für einzelne Dienste eine zusätzliche Gebühr zu verlangen. Während die meisten Dienste in Deutschland kostenlos sind, ist es in Frankreich beispielsweise durchaus üblich, für die Anzeige der Rufnummer oder Telefonkonferenzen eine zusätzliche Grundgebühr zu bezahlen.

Die meisten dieser Dienste können vom Benutzer über das Mobiltelefon konfiguriert werden, wenn diese vom Netzbetreiber freigeschaltet sind. Meist bieten Endgeräte dafür eine Menüstruktur an. Hinter diesen Menüs, die den Umgang mit diesen Diensten wesentlich vereinfachen, verbergen sich jedoch Zahlencodes, die mit einem ‚*' Zeichen beginnen und zwischen Endgerät und Netzwerk ausgetauscht werden. Diese Codes sind im GSM Standard 22.030 festgelegt und somit in allen Netzwerken und in allen Endgeräten gleich. Diese Codes kann ein Benutzer auch selber über die Tastatur eingeben. Nach Drücken der Ruftaste wird der eingegebene Zahlencode dann über die MSC zum HLR

übertragen, wo der gewünschte Dienst aktiviert oder deaktiviert wird. Um zum Beispiel eine Anrufweiterleitung bei besetzt (CFB) auf die Nummer 0170992333 zu setzten, muss der Code **67*0170992333# + Ruftaste eingegeben werden.

1.6.4 Das Authentication Center (AC)

Authentication Center

Ein weiterer wichtiger Bestandteil des HLR ist das Authentication Center. In ihm ist für jeden Teilnehmer ein geheimer Schlüssel Ki abgelegt, von dem nur eine weitere Kopie auf der SIM Karte des Teilnehmers existiert. Dieser ist im Authentication Center und besonders auf SIM Karte so gespeichert, dass er nicht ausgelesen werden kann.

Authentication Triplets

Bei vielen Vorgängen im Netzwerk, wie z.B. beim Beginn eines Gesprächs wird der Teilnehmer mit Hilfe dieses Schlüssels authentifiziert. Somit kann sichergestellt werden, dass kein Missbrauch durch Dritte stattfindet. Abbildungen 1.13 und 1.14 zeigen diesen Vorgang.

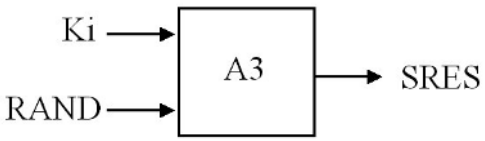

Abb. 1.13: Erzeugen der Signed Response (SRES)

Bei einer Verbindungsaufnahme zwischen Netzwerk und einem Teilnehmer fordert die MSC beim HLR/Authentication Center so genannte Authentication Triplets an. Teil dieser Anforderung ist die IMSI des Teilnehmers. Das Authentication Center sucht anhand der IMSI den Ki des Teilnehmers und den zu verwendenden Authentifizierungsalgorithmus, der A3 genannt wird. Mit Ki wird dann das Authentication Triplet gebildet, das aus folgenden drei Werten besteht:

RAND, SRES, Kc

- RAND: Eine 128 Bit Zufallszahl.
- SRES: Die Signed Response SRES wird aus Ki und RAND mit dem Authentifizierungsalgorithmus A3 erzeugt und hat eine Länge von 32 Bit.
- Kc: Auch der Ciphering Key Kc wird aus Ki und RAND erzeugt. Er wird für die Verschlüsselung des Datenver-

kehrs nach erfolgreicher Authentifizierung verwendet. Mehr dazu in Kapitel 1.7.5.

RAND, SRES (und Kc) werden anschließend der MSC übergeben, die die eigentliche Authentifizierung des Teilnehmers vornimmt. Wichtig ist hierbei, dass der geheime Schlüssel Ki das Authentication Center nicht verlässt.

Um nachfolgende Verbindungsaufnahmen zu beschleunigen, schickt das Authentication Center normalerweise gleich mehrere Authentication Triples in einer Nachricht zur MSC zurück. Diese werden dann in der MSC/VLR für die nächsten Verbindungsaufnahmen zwischengespeichert.

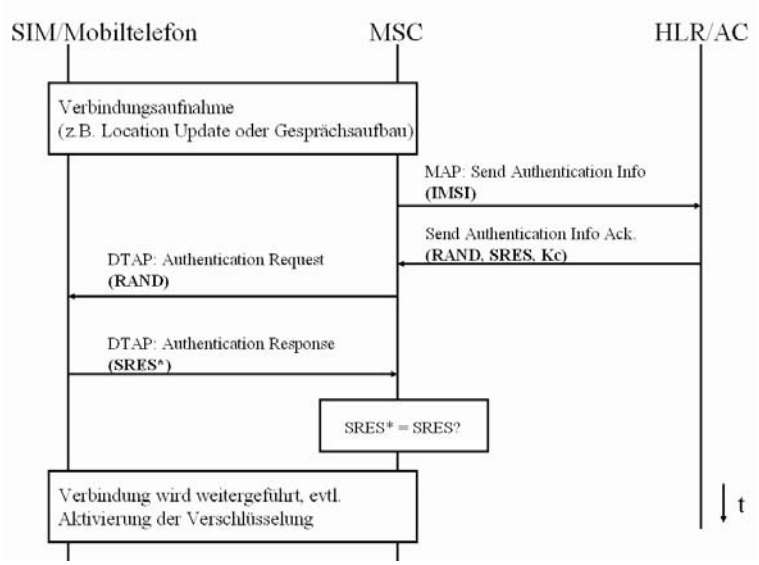

Abb. 1.14: Nachrichtenfluss während einer Authentifizierung

Im nächsten Schritt sendet die MSC dem Endgerät die Zufallszahl (RAND) in einer Authentication Request Nachricht. Das Endgerät übergibt die Zufallszahl der SIM Karte, die dann mit der Kopie von Ki und dem Authentifizierungsalgorithmus A3 die Antwort, also die Signed Response (SRES*) berechnet. Diese wird dann dem Endgerät zurückgegeben und von diesem in einer Authentication Response Nachricht zur MSC zurückgeschickt. Stimmen SRES und SRES* überein, ist der Teilnehmer erfolgreich authentifiziert und hat somit die Berechtigung, das Netzwerk zu verwenden.

Da der geheime Schlüssel Ki zu keiner Zeit im potentiell abhörgefährdeten Netzwerk oder per Funk übertragen wird, ist es

einer dritten Person nicht möglich, SRES zu berechnen. Da bei der nächsten Authentifizierung eine neue Zufallszahl verwendet wird, ist auch das Abhören der zuvor gesendeten SRES nutzlos.

Abbildung 1.15 zeigt Ausschnitte aus einer Authentication Request und einer Authentication Response Nachricht. Neben den Formaten von RAND und SRES ist auch sehr interessant, welche Protokolle des SS-7 Stacks zum Einsatz kommen (vgl. hierzu auch Kapitel 1.4.2)

Ausschnitt aus einer dekodierten Authentication Request Nachricht

```
SCCP MSG: Data Form 1
DEST. REF ID: 0B 02 00
DTAP MSG      LENGTH: 19
PROTOCOL DISC.: Mobility Management
DTAP MM MSG: Auth. Request
Ciph. Key Seq.: 0
RAND in hex: 12 27 33 49 11 00 98 45
             87 49 12 51 22 89 18 81 (16 Byte = 128 Bit)
```

Ausschnitt aus einer dekodierten Authentication Response Nachricht

```
SCCP MSG: Data Form 1
DEST. REF ID: 00 25 FE
DTAP MSG      LENGTH: 6
PROTOCOL DISC.: Mobility Management
DTAP MM MSG: Auth. Response
SRES in hex: 37 21 77 61 (4 Byte = 32 Bit)
```

Abb. 1.15: Authentifizierung zwischen Netzwerk und Endgerät

1.6.5 Das Short Message Service Center (SMSC)

SMSC

Ein weiteres wichtiges Netzwerkelement ist das Short Message Service Center (SMSC), das für die Weiterleitung und Speicherung von Kurznachrichten (SMS) zuständig ist. Erst etwa 4 Jahre nach dem Start der ersten GSM Netze wurde dieser Dienst in Betrieb genommen. Binnen kurzer Zeit jedoch erfreute er sich so enormer Popularität, dass Netzbetreiber heute einen zweistelligen Prozentsatz ihres Umsatzes mit diesem Dienst erwirtschaften.

Der SMS Dienst ermöglicht sowohl den direkten Austausch von Kurznachrichten zwischen Teilnehmern, als auch automatisch generierte SMS Nachrichten als Reaktion auf eingehende eMails oder weitergeleitete Gespräche zur Sprachbox (Voice Mail Sys-

tem). Das Prinzip der Übertragung einer SMS ist jedoch in beiden Fällen identisch:

Senden einer SMS

Der Sender erstellt eine SMS und überträgt diese zur MSC über einen Signalisierungskanal. Eine SMS ist somit nichts anderes als eine DTAP SS-7 Nachricht, wie z.B. eine Location Update Nachricht oder eine Setup Nachricht zum Aufbau eines Gesprächs. Inhalt der SMS ist der Nachrichtentext selber, sowie die Telefonnummer (MSISDN) des Zielteilnehmers. Die MSC leitet die SMS ohne weitere Bearbeitung direkt an das Short Message Service Center (SMSC) weiter. Das SMSC bestätigt dem Sender daraufhin den korrekten Empfang der SMS. Dies wird dann auch auf dem Display des Teilnehmers angezeigt.

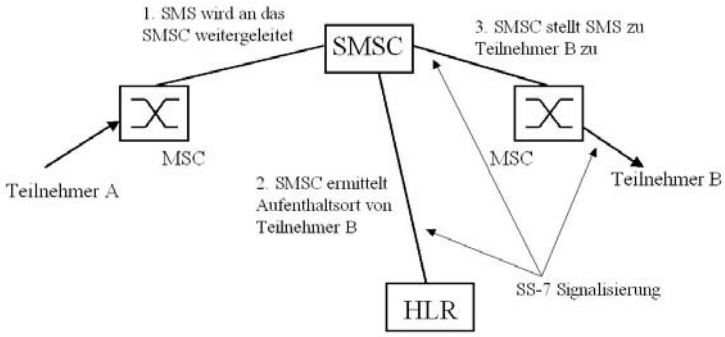

Abb. 1.16: Zustellungsprinzip einer SMS

Zustellen einer SMS

Für die Zustellung einer SMS analysiert das SMSC die MSISDN des Empfängers und befragt das entsprechende HLR nach dessen aktuellen Aufenthaltsort (MSC). Danach wird die SMS an diese MSC geschickt. Ist der Teilnehmer in dieser MSC als aktiv angemeldet (attached), versucht die MSC Kontakt mit ihm aufzunehmen und die SMS zuzustellen. Die korrekte Zustellung wird dem SMSC quittiert, und die SMS kann daraufhin im SMSC gelöscht werden.

Nicht erreichbarer Teilnehmer

Ist der Teilnehmer nicht erreichbar (z.B. Akku leer, keine Netzabdeckung, Endgerät ausgeschaltet, etc.) kann die SMS nicht sofort zugestellt werden. Daraufhin wird im VLR Eintrag des Empfängers das Message Waiting Flag gesetzt, und die SMS wird im SMSC zwischengespeichert. Sobald sich der Empfänger wieder meldet, sieht die MSC dieses Flag und kann das SMSC davon

unterrichten. Daraufhin versucht das SMSC erneut, die SMS zuzustellen.

Da auch im HLR ein Message Waiting Flag gesetzt wird, erreicht die SMS einen Empfänger auch dann noch, wenn dieser sein Mobiltelefon z.B. in Frankfurt ausgeschaltet hat und sich während der SMS Zustellung gerade im Flugzeug nach Paris befindet. Beim Einschalten des Mobiltelefons in Paris meldet die dortige MSC dem Heimat HLR des Teilnehmers dessen neue Position (Location Update). Das HLR schickt daraufhin dem neuen MSC/VLR eine Kopie der Teilnehmerdaten inklusive des Message Waiting Flags, und die SMS kann wiederum korrekt zugestellt werden.

Ende zu Ende Empfangsbestätigung

Die in GSM spezifizierten Mechanismen zur SMS Zustellung enthalten leider keine Ende zu Ende Empfangsbestätigung für den Sender der SMS. Dieser bekommt nur signalisiert, dass die SMS korrekt beim SMSC eingetroffen ist. Ob die SMS auch korrekt zum Zielteilnehmer zugestellt werden konnte, wird nicht mitgeteilt. Hier haben einige Hersteller von SMSCs eigene Lösungen entwickelt. Einige Hersteller verwenden dabei einen Code, der vom Benutzer am Anfang des SMS Textes eingegeben werden kann. Bei einigen deutschen Netzbetreibern ist dies ‚*T#'. Erkennt das SMSC diesen Code am Anfang des Nachrichtentextes, wird dieser vor der Zustellung der SMS gelöscht und die Nachricht dann an den Empfänger übermittelt. Nachdem die SMS erfolgreich übermittelt wurde, schickt das SMSC im letzten Schritt eine Bestätigung in Form einer SMS an den Absender zurück.

1.7 Das Base Station Subsystem (BSS)

Während ein Großteil der zusätzlichen Funktionalität für den Mobilfunk im NSS durch neue Software implementiert wurde, musste im Radio Netzwerk ein Großteil der Hard- und Software neu entwickelt werden. Dies wurde schon alleine deswegen nötig, da alle Vorgängertechnologien noch auf analoger Technik für die Funkübertragung basierten.

1.7.1 Frequenzbereiche

Frequenzbereiche

In Europa wurde GSM zunächst im 900 MHz Frequenzband von 890–915 MHz im Uplink und von 935-960 MHz im Downlink spezifiziert. Uplink ist dabei die Senderichtung von Mobiltelefon zu Netzwerk, Downlink die Senderichtung von Netzwerk zu Mobiltelefon. Die Bandbreite von 25 MHz ist dabei in 125 Kanäle mit einer Bandbreite von jeweils 200 kHz aufgeteilt. Diese Kanä-

le teilen sich in Deutschland die Mobilfunkbetreiber T-Mobile (vormals D1) und Vodafone (vormals D2).

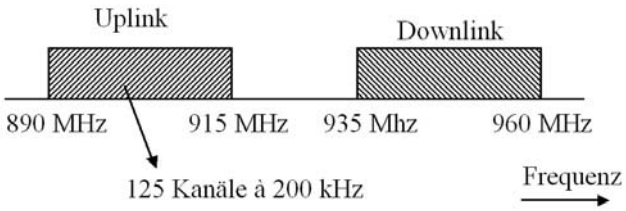

Abb. 1.17: Uplink und Downlink im 900 MHz Frequenzband

Schon bald war abzusehen, dass diese Kanalanzahl für den schnell wachsenden Mobilfunkverkehr in vielen europäischen Ländern nicht ausreichend sein würde. Deshalb wurde in einem zweiten Schritt ein Frequenzband im Frequenzbereich von 1710-1785 MHz im Uplink und 1805-1880 im Downlink für GSM in Europa geöffnet. Statt einer Bandbreite von 25 MHz wie im 900 MHz Bereich steht hier eine Bandbreite von 75 MHz zur Verfügung. Dies entspricht 375 zusätzlichen Kanälen. Ein Teil dieser Kanäle wird heute in Deutschland von E-Plus verwendet, ein weiterer Teil von O2-Deutschland. Da vor allem in Großstädten das 900 MHz Band nicht mehr genug Kapazität für T-Mobile und Vodafone bot, kauften diese noch nachträglich von der Regulierungsbehörde für Telekommunikation und Post (RegTP) zusätzliche Frequenzen im 1800 MHz Band. Die Funktionsweise von GSM ist auf beiden Frequenzbändern identisch, sie unterscheiden sich lediglich durch andere Kanalnummern, die Absolute Radio Frequency Channel Number (ARFCN) genannt werden.

Von Europa breitete sich der GSM Standard in kurzer Zeit über die ganze Welt aus, nur in wenigen Ländern wie Japan und Südkorea gibt es heute keine GSM Netze.

GSM Frequenzen in Nordamerika

Während in Nordamerika zunächst die alten analogen Mobilfunknetze weiter betrieben wurden, etablierte sich GSM neben anderen digitalen Techniken auch dort. Da sowohl das 900 MHz, als auch das 1800 MHz Band schon von anderen Funkdiensten genutzt wurden, musste man hier auf Frequenzen im 1900 MHz Band ausweichen. Dies hat den gravierenden Nachteil, dass viele Mobiltelefone aus den USA und Kanada in Europa nicht funktionieren und umgekehrt. Nur so genannte Tri-Band Mobiltelefone, die sowohl den 900,1800 und 1900 MHz Frequenzbereich unterstützten, können auf beiden Seiten des Atlantiks verwendet wer-

den. Diese werden aber von Firmen wie Motorola, Nokia, Siemens und anderen vermehrt angeboten. Da auch im 1900 MHz Band die Frequenzen knapp wurden, wurde ein weiteres Band im 850 MHz Bereich für den nordamerikanischen Markt geöffnet. Auch dieses ist zum 900 MHz Band, das in den meisten anderen Ländern verwendet wird, inkompatibel. Um weltweit in GSM Netzen erreichbar zu sein, sind somit Quad-Band Mobiltelefone nötig, die das 850, 900, 1800 und 1900 MHz Band unterstützen. Während die Endgeräte Software dafür nur wenig modifiziert werden muss, erhöhen sich jedoch die Hardwarekosten der Sende- und Empfangseinheit.

Name	**ARFCN**	**Uplink (MHz)**	**Downlink (MHz)**
GSM 900 (Primary)	0-124	890-915	935-960
GSM 900 (Extended)	975-1023, 0-124	880-915	925-960
GSM 1800	512-885	1710-1785	1805-1880
GSM 1900 (Nordamerika)	512-810	1850-1910	1930-1990
GSM 850 (Nordamerika)	128-251	824-849	869-894
GSM-R	0-124 955-1023	876-915	921-960

GSM-R

Neben öffentlichen GSM Netzen etabliert sich für die europäischen Eisenbahnen eine neue digitale Zugfunkgeneration, die auf dem GSM Standard basiert. Zusätzlich zu den GSM Funktionalitäten wurden spezielle für Eisenbahnen benötigte Dienste wie z.B. Gruppenrufe entwickelt. Dieser Standard wurde GSM for Railways, kurz GSM-R genannt. Da es sich hier nicht um öffentliche, sondern um private Netzwerke handelt, wurde den GSM-R Netzen auch ein eigenes Frequenzband unmittelbar unterhalb des öffentlichen 900 MHz GSM Bands zugeteilt. Um GSM-R zu nutzen, sind Mobiltelefone mit leichten Hardwaremodifikationen notwenig, um in diesem Frequenzbereich senden und

empfangen zu können. Um eisenbahnspezifische Dienste wie z.B. Gruppenrufe verwenden zu können, wurde zusätzlich die Mobiltelefonsoftware erweitert. In Deutschland sind bereits alle wesentlichen Bahnstrecken mit GSM-R ausgerüstet, Neubaustrecken werden ausschließlich mit der neuen digitalen Technik betrieben. Mehr zum Thema GSM-R ist unter http://gsm-r.uic.asso.fr zu finden.

1.7.2 Base Transceiver Station (BTS)

Basisstationen, auch Base Transceiver Station (BTS) genannt, sind durch Ihre Antennen die wohl sichtbarsten Netzwerkelemente eines GSM Mobilfunksystems. Diese ersetzten im Vergleich zum Festnetz die kabelgebundene Verbindung mit dem Benutzer durch eine Funkverbindung, die auch Luftschnittstelle oder Air Interface genannt wird. Laut Presseberichten hat jeder Netzwerkbetreiber in Deutschland einige zehntausend dieser Basisstationen.

Abb. 1.18: Eine typische Antenne einer GSM Basisstation. Die zusätzliche optionale Richtfunkantenne (runde Antenne unten) verbindet die Basisstation mit dem GSM Netzwerk.

Reichweite

Theoretisch kann eine BTS eine Fläche mit einem Radius von bis zu 35 km abdecken. Dieses Gebiet wird auch Zelle genannt. Da eine BTS aber nur mit einer begrenzten Anzahl an Nutzern gleichzeitig kommunizieren kann, sind Zellen vor allem in städti-

schen Bereichen wesentlich kleiner. Sie reichen dort von 3-4 km Radius in Wohngebieten bis zu wenigen 100 Metern und sehr kleiner Sendeleistung in Innenstädten. Aber auch auf dem Land sind Zellen mit einem Radius von mehr als 15 km nur sehr selten anzutreffen. Hier ist die maximale Sendeleistung der Endgeräte von 1-2 Watt der begrenzende Faktor.

Grundsätzlich gilt, dass die von einer Basisstation verwendeten Sendefrequenzen nicht von Nachbarstationen verwendet werden dürfen, da diese sich sonst gegenseitig stören (Interferenz). Da eine Basisstation wie in Abbildung 1.19 normalerweise mehrere Nachbarstationen besitzt, können nur eine sehr begrenzte Anzahl an Frequenzen pro Basisstation verwendet werden.

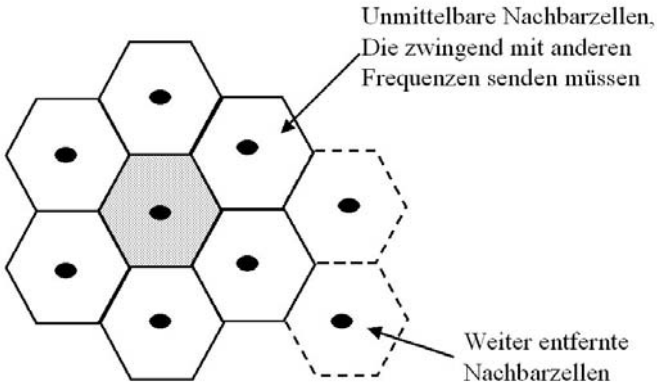

Abb. 1.19: Zelle mit Nachbarzellen

Sektorisierung

Um die Kapazität einer BTS zu steigern, wird das abgedeckte Gebiet oft in zwei oder drei Sektoren eingeteilt, die jeweils von einer eigenen Sende- und Empfangshardware der BTS auf unterschiedlichen Frequenzen abgedeckt werden. Somit können die Frequenzen im zweidimensionalen Raum gesehen öfters wieder verwendet werden. Jeder Sektor ist dabei eine eigenständige Zelle.

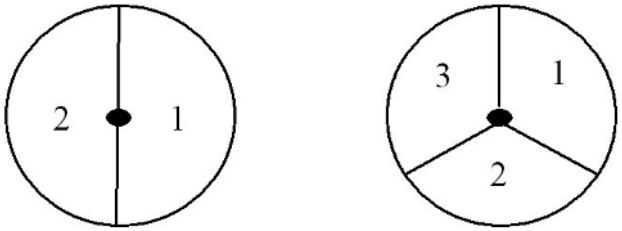

Abb. 1.20: Sektorisierte Zellkonfigurationen

1.7.3 Die GSM Luftschnittstelle

Um

Der Übertragungsweg zwischen BTS und Mobilfunkteilnehmer wird bei GSM als Luftschnittstelle, Air Interface oder Um-Interface bezeichnet.

Frequenz Multiplex

Damit eine BTS mit mehreren Teilnehmern gleichzeitig kommunizieren kann, werden bei GSM zwei Verfahren angewandt. Das erste Verfahren ist der Frequenzmultiplex (Frequency Division Multiple Access, FDMA), also die gleichzeitige Nutzung mehrer Frequenzen pro Zelle.

Zeitmultiplex

Das zweite Verfahren ist der Zeitmultiplex, auch Time Division Multiple Access (TDMA) genannt. Bei GSM können pro Trägerfrequenz mit 200 kHz Bandbreite bis zu 8 Teilnehmer gleichzeitig kommunizieren.

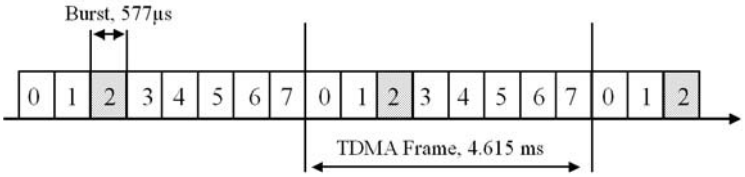

Abb. 1.21: Ein GSM TDMA Frame

Dazu werden auf dem Träger 4.615 ms lange Frames übertragen. Jeder Frame enthält 8 voneinander unabhängige physikalische Zeitschlitze (Timeslots) für die Kommunikation mit unterschiedlichen Teilnehmern. Das Zeitintervall eines Timeslots wird Burst genannt und beträgt 577 µs. Bekommt ein Endgerät beispielsweise Timeslot Nr. 2 eines Frames für ein Telefongespräch zugeteilt, darf es in jedem Frame in diesem Timeslot senden und empfan-

gen. Danach muss es den restlichen Frame abwarten, bevor es erneut an der Reihe ist.

Kapazitätsbetrachtung

Nachdem die grundsätzlichen Mehrfachzugriffsverfahren nun bekannt sind, kann in grober Nährung die Gesamtkapazität einer BTS ermittelt werden. Für nachfolgendes Beispiel wird eine BTS mit 3 sektorisierten Zellen betrachtet, die jeweils über 2 Frequenzen verfügen, eine in der Praxis übliche Konfiguration. Pro Sektor stehen somit 2*8 = 16 Timeslots zur Verfügung. Von diesen müssen 2 Timeslots für Signalisierungsaufgaben abgezogen werden. Somit bleiben 14 Timeslots pro Sektor. Von diesen werden meist 4 oder mehr Timeslots für den paketorientierten Datendienst GPRS verwendet, der im nächsten Kapitel beschrieben wird. Somit bleiben pro Sektor 10, pro BTS somit 30 Kanäle für die Sprachübertragung. Das bedeutet also, dass in der Praxis 30 Teilnehmer gleichzeitig pro BTS kommunizieren können.

Eine BTS versorgt jedoch wesentlich mehr Teilnehmer eines Netzwerkes, da nicht alle Teilnehmer gleichzeitig telefonieren. Mobilfunknetzbetreiber gehen davon aus, dass im Durchschnitt ein Teilnehmer pro Stunde 1 Minute telefoniert. Somit versorgt eine BTS in grober Nährung etwa 60 mal mehr passive als aktive Teilnehmer. In diesem Beispiel versorgt die BTS also etwa 1800 Teilnehmer.

Teilt man die gesamte Nutzerzahl eines Netzwerkes, im Falle von Vodafone in Deutschland 2004 etwa 25 Millionen durch diesen Wert, so kommt man auf etwa 14.000 Basisstationen, die für diese Anzahl Teilnehmer im gesamten Bundesgebiet benötigt werden. Diese Zahl ist im Bereich der von den Netzwerkbetreibern veröffentlichten Werten und vermittelt einen ersten Eindruck über die Dimensionen eines großen Netzwerkes. Da in einem Netzwerk jedoch auch Basisstationen mit mehr oder weniger Kapazität verwendet werden, ist diese Rechnung jedoch nur eine sehr grobe Näherung.

Burstaufteilung

Jeder Burst eines TDMA Frames ist wie in Abb. 1.22 gezeigt in unterschiedliche Bereiche aufgeteilt:

Guard Time

Während einer durch die Guard Time festgelegte Zeit am Anfang und Ende jedes Frames werden keine Daten übertragen. Dies ist notwendig, da sich Teilnehmer auch während der Dauer einer Verbindung bewegen und sich der Abstand zur BTS ständig ändern kann. Da sich die Funkwellen ‚nur' mit Lichtgeschwindigkeit ausbreiten, treffen die Daten eines weiter entfernten Teilnehmers erst später als die Daten eines Teilnehmers ein, der sich näher an der Basisstation befindet. Um Überlappungen zu ver-

meiden, sind diese Pausenzeiten nötig. Die Guard Time ist jedoch sehr kurz, da durch eine aktive Sendezeitregelung, die Timing Advance genannt wird, diese Unterschiede weitestgehend ausgeglichen werden. Mehr zum Timing Advance im Laufe dieses Kapitels.

Training Sequence

In der Mitte des Bursts befindet sich die Training Sequence mit einem immer gleichen Bitmuster. Diese ist notwendig, da sich das Signal bei der Funkübertragung durch verschiedene Phänomene wie Reflexion, Absorption und Mehrfachausbreitung verändert. Diese Effekte müssen auf der Empfängerseite wieder ausgeglichen werden. Der Empfänger vergleicht dazu das ihm bekannte Bitmuster mit dem empfangen Signal und kann daraus schließen, wie aus dem empfangenen Signal die Originaldaten wieder rekonstruiert werden können.

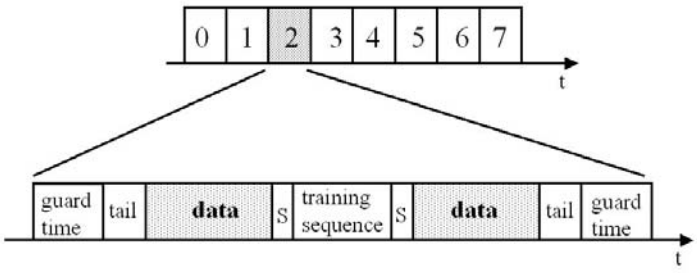

Abb. 1.22: Ein GSM Burst

Tail

Am Anfang und Ende des Bursts wird ebenfalls ein bekanntes Bitmuster gesendet, damit der Empfänger den Beginn und das Ende des Bursts korrekt erkennen kann. Diese Felder werden Tail genannt.

Nutzdaten

Die eigentlichen Nutzdaten des Bursts, also z.B. digitalisierte Sprache, werden in zwei Nutzdatenfelder (data) mit jeweils 57 Bit Länge übertragen. Somit werden pro 577 µs Burst genau 114 Bit Nutzdaten übertragen.

Stealing Flags

Schließlich gibt es vor und nach der Training Sequence noch jeweils zwei Bits, die Stealing Flags genannt werden. Sind sie gesetzt, befinden sich in den Datenfeldern keine Nutzdaten, sondern dringende Signalisierungsinformationen. Werden Signalisierungsdaten in diesen Feldern übertragen, gehen die Nutzdaten verloren.

Kanäle auf der Luftschnittstelle

Zur Übertragung von Nutzdaten oder Signalisierungsdaten werden die Zeitschlitze in logische Kanäle eingeteilt. Ein Nutzdatenkanal für die Übertragung von Sprachdaten ist z.B. ein logischer Kanal. Auf der ersten Trägerfrequenz einer Zelle werden die ersten beiden Timeslots üblicherweise für allgemeine logische Signalisierungskanäle reserviert, die restlichen können für 6 unabhängige Nutzkanäle oder GPRS verwendet werden. Da es wesentlich mehr logische Signalisierungskanäle als physikalische Kanäle (Timeslots) für die Signalisierung gibt, wurden im GSM Standard 45.002 für die Signalisierung 51 Frames zu einem Multiframe zusammengefasst. In einem solchen Multiframe, der sich ständig wiederholt, ist genau festgelegt, in welchen Bursts von Timeslot 0 und 1 welche logischen Kanäle übertragen werden. Über diese Vorschrift werden also viele logische Kanäle auf wenige physikalische Kanäle übertragen. Für Timeslots, die für Nutzdatenübertragung (also z.B. Sprache) verwendet werden, wird ein 26 Multiframe Muster verwendet.

Um dies grafisch darzustellen, werden alle Bursts eines Timeslots untereinander angeordnet, die 8 Timeslots eines Frames nebeneinander. Abbildung 1.23 zeigt dieses Prinzip, mit dem dann in Abbildung 1.24 die Zuordnung der logischen Kanäle zu physikalischen Kanälen dargestellt ist.

Logische Kanäle

Logische Kanäle werden in zwei Gruppen eingeteilt. Sind Daten auf einem logischen Kanal nur für einen einzelnen Nutzer bestimmt, handelt es sich um einen Dedicated Channel. Werden auf einem Kanal Daten für mehrere Benutzer übertragen, wird dieser Common Channel genannt.

Dedicated Channels

Im Anschluss werden nun zuerst die Dedicated Channels betrachtet:

TCH

Der Traffic Channel (TCH) ist ein Nutzdatenkanal in GSM. Über diesen können entweder digitalisierte Sprachdaten oder leitungsvermittelnde Datendienste mit bis zu 14.4 kbit/s oder 9.6 kbit/s FAX übertragen werden.

FACCH

Der Fast Associated Control Channel (FACCH) wird auf dem gleichen Timeslot wie der TCH übertragen. Er dient zur Übermittlung dringender Signalisierungsnachrichten wie z.B. einem Handover Kommando. Da dringende Signalisierungsnachrichten nur selten zu übertragen sind, wurden dem FACCH keine eigenen Bursts zugeteilt. Bei Bedarf werden Nutzdaten aus einzelnen Bursts des Timeslots entfernt und FACCH Daten übertragen. Um dies dem Endgerät bzw. dem Netzwerk zu signalisieren, werden die in Abb. 1.22 gezeigten Stealing Flags eines Bursts entspre-

chend gesetzt. Aus diesem Grund ist der FACCH in Abbildung 1.24 auch nicht dargestellt.

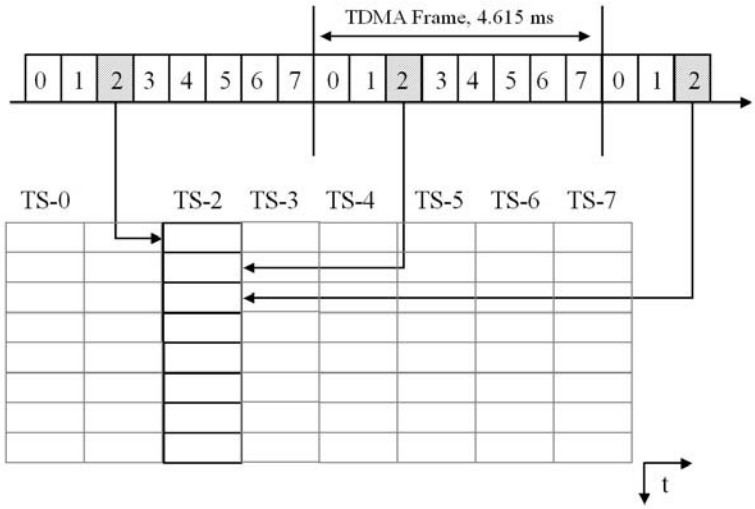

Abb. 1.23: Zusammenhängende Anordnung von Bursts eines Timeslots für die Darstellung der logischen Kanäle in Abb. 1.24

SACCH

Der Slow Associated Control Channel (SACCH) ist ebenfalls einem aktiven Benutzer zugeordnet. Dieser wird im Uplink verwendet, um während der aktiven Verbindung ständig Messergebnisse der Signalpegelmessungen der aktiven Zelle, sowie der Nachbarzellen an das Netzwerk zu senden. Die Messergebnisse werden vom Netzwerk dann für die Handover Entscheidung sowie für die Leistungsregelung verwendet. Im Downlink werden auf dem SACCH im Gegenzug Befehle für die Leistungsregelung der Mobilstation übermittelt. Außerdem erhält das Endgerät über den SACCH Informationen für die Timing Advance Regelung, die in Kapitel 1.7.4 und Abbildung 1.29 näher beschrieben werden. Da diese Daten keine hohe Priorität haben und die Datenrate sehr gering ist, werden nur wenige Bursts für diesen logischen Kanal in einem 26 Multiframe verwendet.

SDCCH

Der Standalone Dedicated Control Channel (SDCCH) ist ein reiner Signalisierungskanal, der während des Gesprächsaufbaus verwendet wird, solange einem Teilnehmer noch kein eigener

TCH zugeordnet ist. Außerdem wird dieser Kanal für Signalisierungsdaten verwendet, die nicht zum Aufbau eines Gesprächs und somit auch zu keiner Zuteilung eines TCH führen. Dies sind z.B. ein Location Update oder das Senden oder Empfangen einer SMS.

Common Channels

Neben diesen teilnehmerbezogenen Kanälen gibt es eine Reihe von Common Channels, die von allen Teilnehmern abgehört werden:

SCH

Der Synchronization Channel (SCH) wird von Endgeräten bei der Netzwerk- und Zellsuche verwendet.

FCCH

Der Frequency Correction Channel (FCCH) wird von Endgeräten für die Kalibrierung ihrer Sende- und Empfangseinheiten verwendet und dient außerdem dazu, den Anfang eines 51-Multiframes zu finden.

BCCH

Der Broadcast Common Control Channel (BCCH) überträgt in verschiedenen SYS_INFO Nachrichten eine Vielzahl von Systeminformationen, über die alle Teilnehmer die am Netzwerk angemeldet aber nicht aktiv sind (Idle Mode) stets informiert sein müssen. Dazu gehören unter anderem:

- Mobile Country Code (MCC) und Mobile Network Code (MNC) der Zelle.
- Identifikation der Zelle bestehend aus dem Location Area Code (LAC) und der Cell ID.
- Um Endgeräten die Suche nach Nachbarzellen zu vereinfachen, werden auf dem BCCH jeder Zelle die verwendeten Frequenzen der Nachbarzellen ausgestrahlt. Somit muss das Mobiltelefon nicht ständig das komplette Frequenzband nach Nachbarzellen durchsuchen.

FN	TS-0	TS-1
0	FCCH	SDCCH/0
1	SCH	SDCCH/0
2	BCCH	SDCCH/0
3	BCCH	SDCCH/0
4	BCCH	SDCCH/1
5	BCCH	SDCCH/1
6	AGCH/PCH	SDCCH/1
7	AGCH/PCH	SDCCH/1
8	AGCH/PCH	SDCCH/2
9	AGCH/PCH	SDCCH/2
10	FCCH	SDCCH/2
11	SCH	SDCCH/2
12	AGCH/PCH	SDCCH/3
13	AGCH/PCH	SDCCH/3
14	AGCH/PCH	SDCCH/3
15	AGCH/PCH	SDCCH/3
16	AGCH/PCH	SDCCH/4
17	AGCH/PCH	SDCCH/4
18	AGCH/PCH	SDCCH/4
19	AGCH/PCH	SDCCH/4
20	FCCH	SDCCH/5
21	SCH	SDCCH/5
22	SDCCH/0	SDCCH/5
23	SDCCH/0	SDCCH/5
24	SDCCH/0	SDCCH/6
25	SDCCH/0	SDCCH/6
26	SDCCH/1	SDCCH/6
27	SDCCH/1	SDCCH/6
28	SDCCH/1	SDCCH/7
29	SDCCH/1	SDCCH/7
30	FCCH	SDCCH/7
31	SCH	SDCCH/7
32	SDCCH/2	SACCH/0
33	SDCCH/2	SACCH/0
34	SDCCH/2	SACCH/0
35	SDCCH/2	SACCH/0
36	SDCCH/3	SACCH/1
37	SDCCH/3	SACCH/1
38	SDCCH/3	SACCH/1
39	SDCCH/3	SACCH/1
40	FCCH	SACCH/2
41	SCH	SACCH/2
42	SACCH/0	SACCH/2
43	SACCH/0	SACCH/2
44	SACCH/0	SACCH/3
45	SACCH/0	SACCH/3
46	SACCH/1	SACCH/3
47	SACCH/1	SACCH/3
48	SACCH/1	free
49	SACCH/1	free
50	free	free

FN	TS-2	…	TS-7
0	TCH		TCH
1	TCH		TCH
2	TCH		TCH
3	TCH		TCH
4	TCH		TCH
5	TCH		TCH
6	TCH		TCH
7	TCH		TCH
8	TCH		TCH
9	TCH		TCH
10	TCH		TCH
11	TCH		TCH
12	SACCH		SACCH
13	TCH		TCH
14	TCH		TCH
15	TCH		TCH
16	TCH		TCH
17	TCH		TCH
18	TCH		TCH
19	TCH		TCH
20	TCH		TCH
21	TCH		TCH
22	TCH		TCH
23	TCH		TCH
24	TCH		TCH
25	free		free
0	TCH		TCH
1	TCH		TCH
2	TCH		TCH
3	TCH		TCH
4	TCH		TCH
5	TCH		TCH
6	TCH		TCH
7	TCH		TCH
8	TCH		TCH
9	TCH		TCH
10	TCH		TCH
11	TCH		TCH
12	SACCH		SACCH
13	TCH		TCH
14	TCH		TCH
15	TCH		TCH
16	TCH		TCH
17	TCH		TCH
18	TCH		TCH
19	TCH		TCH
20	TCH		TCH
21	TCH		TCH
22	TCH		TCH
23	TCH		TCH
24	TCH		TCH
25	free		free

Abb. 1.24: Nutzung der Timeslots im Downlink, in Anlehnung an Darstellung 7.7 in „GSM-Signalisierung verstehen und praktisch Anwenden“, ISBN 3-7723-5774-1

PCH

Der Paging Channel (PCH) wird verwendet, um nicht aktive Teilnehmer bei eingehenden Anrufen oder SMS Nachrichten zu rufen (pagen). Da das Netzwerk nur weiß, in welcher Location Area sich ein Teilnehmer befindet, wird dieser auf dem Paging Channel jeder Zelle in dieser Location Area gerufen. Wichtigster Teil der Nachricht ist seine IMSI oder eine temporäre ID, die Temporary Mobile Subscriber Identity (TMSI) genannt wird. Diese wird z.B. nach dem Einschalten einem Teilnehmer zugewiesen und kann von Netzwerk dann bei beliebigen Netzwerkzugriffen nach aktivieren der Datenverschlüsselung wieder geändert werden. Somit muss der Teilnehmer nur in wenigen Fällen mit seiner IMSI identifiziert werden, während Daten unverschlüsselt übertragen werden. Dies erhöht die Anonymität der Teilnehmer im Netzwerk und vereitelt externen Beobachtern, Bewegungsprofile von Teilnehmern zu erstellen.

RACH

Der Random Access Channel (RACH) ist der einzige Common Channel vom Endgerät in Richtung Netzwerk. Erhält das Endgerät über den PCH eine Nachricht, dass das Netz mit ihm Kontakt aufnehmen will, oder möchte der Benutzer ein Gespräch beginnen, eine SMS senden, usw., nimmt das Endgerät über den RACH mit dem Netzwerk Kontakt auf. Dies geschieht mit einer Channel Request Nachricht. Diese muss über den „Zufallskanal“ gesendet werden, da die Teilnehmer einer Zelle nicht untereinander synchronisiert sind. Somit ist nicht gewährleistet, dass nicht zwei Endgeräte versuchen, zur selben Zeit auf das Netzwerk zuzugreifen. Erst wenn auf die Channel Request Anfrage ein dedizierter Kanal (SDCCH) vom Netzwerk zugeteilt worden ist, können keine Kollisionen mehr auftreten. Tritt eine Kollision beim Zugriff auf den RACH auf, gehen die kollidierenden Nachrichten verloren, und die Teilnehmer erhalten vom Netzwerk keine Antwort. Nach unterschiedlich langen Wartezeiten müssen sie danach ihre Kanalanforderung wiederholen.

AGCH

Sendet ein Teilnehmer auf dem RACH eine Channel Request Nachricht, reserviert das Netzwerk daraufhin einen SDCCH oder in Ausnahmefällen direkt einen TCH und benachrichtigt den Teilnehmer daraufhin auf dem Access Grant Channel (AGCH) mit einer Immediate Assignment Nachricht. Diese Nachricht enthält dann die Information, welchen SDCCH oder TCH der Teilnehmer verwenden darf.

Abbildung 1.25 zeigt das Zusammenspiel von PCH, AGCH und SDCCH beim Aufbau einer Signalisierungsverbindng. Der in der Abbildung gezeigte Base Station Controler (BSC) ist für die Ver-

gabe aller SDCCH und TCH Kanäle einer BTS zuständig und wird im Kapitel 1.7.4 näher beschrieben.

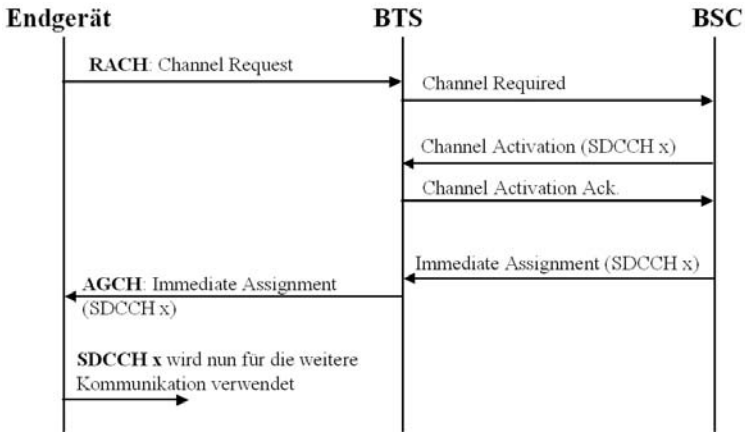

Abb 1.25: Aufbau einer Signalisierungsverbindung

Leere Bursts

Wie in Abbildung 1.24 auch zu sehen ist, werden nicht alle Bursts von Timeslot 2 bis 7 für Traffic Channels (TCH) verwendet. In jedem Timeslot wird jeweils der 12. Burst für den zum TCH zugehörigen Slow Associcated Control Channel (SACCH) verwendet. Außerdem werden im 25. Burst keine Daten übertragen. Diese Lücke wurde geschaffen, um dem Endgerät die Möglichkeit zu geben, auch während einer aktiven Verbindung Messungen der Signalstärken der Nachbarzellen auf anderen Frequenzen durchzuführen. Dies ist nötig, damit das Netzwerk die Verbindung eines aktiven Teilnehmers ggf. in eine andere Zelle umschalten kann (Handover), falls dort die Übertragungsbedingungen besser als die der aktuellen Zelle werden.

Frequency Hopping

Der GSM Standard bietet zwei Möglichkeiten der Frequenznutzung. Der einfachste Fall, von dem hier bisher ausgegangen wurde, ist die Verwendung einer konstanten Trägerfrequenz (ARFCN). Um die Übertragungsqualität zu steigern, wurde auch ein Verfahren zum Wechsel der Frequenzen während einer Verbindung, im englischen Frequency Hopping genannt, standardisiert. Wird Frequency Hopping in einer Zelle angewandt, wird nach der Übertragung jedes Bursts die Trägerfrequenz (carrier frequency) gewechselt. Auf diese Weise kann die Wahrscheinlichkeit erhöht werden, nur wenige Daten zu verlieren, wenn in

einem Frequenzbereich eine Störung das Nutzdatensignal überlagert. Im schlimmsten Fall ist davon nur ein Burst betroffen, da der nächste Burst eines Teilnehmers schon wieder auf einer anderen Frequenz übertragen wird. Maximal können pro BTS 64 Frequenzen für das Frequency Hopping verwendet werden. Eine Mobilstation bekommt dazu beim Aufbau einer Verbindung in der Immediate Assignment Nachricht mitgeteilt, welche Frequenzen für seinen Kanal verwendet werden und mit welchem Muster diese gewechselt werden.

Für Carrier, auf denen Broadcast Kanäle wie SCH, FCCH und BCCH ausgestrahlt werden, darf kein Frequency Hopping verwendet werden. Dies ist zwingend erforderlich, da sonst Endgeräte die Nachbarzellen auf Grund des ständigen Frequenzwechsels nicht finden könnten. In der Praxis zeigt sich, dass Netzbetreiber ihre Zellen sowohl mit, als auch ohne Frequency Hopping betreiben.

Abis Interface

Von der BTS werden die Daten aller logischen Kanäle über das Abis Interface und eine E-1 Verbindung an den Base Station Controller weitergeleitet. Die Übertragung erfolgt jedoch in einer gänzlich anderen Rahmenstruktur. Für sämtliche Common Channels sowie die SDCCH und SACCH Kanäle wird mindestens ein gemeinsamer 64 kbit/s E-1 Timeslot verwendet. Dies ist möglich, da hier nur Signalisierungsdaten übertragen werden, die nicht zeitkritisch sind. Dieser Signalisierungskanal verwendet auf dem BTS – BSC Interface das LAPD Protokoll. LAPD steht dabei für Link Access Protocol D-Channel und wurde mit wenigen Modifikationen aus der ISDN Welt übernommen.

Für Traffic Channels, die wie wir später noch sehen, 13 kbit/s an Sprachdaten übertragen, wird jeweils ¼ E-1 Timeslot verwendet. Für alle 8 Timeslots eines Air Interface Frames werden somit nur 2 Timeslots auf dem E-1 Interface benötigt. Eine 3 Sektor Zelle mit jeweils 2 Carrier pro Sektor benötigt somit auf dem Abis Interface 12 Timeslots + 1 Timeslot für die LAPD Signalisierung. Die restlichen Timeslots können für die Kommunikation zwischen der BSC und einer oder mehreren anderen Basisstationen verwendet werden. Für diesen Anwendungsfall werden diese dann über eine E-1 Leitung in Reihe geschaltet.

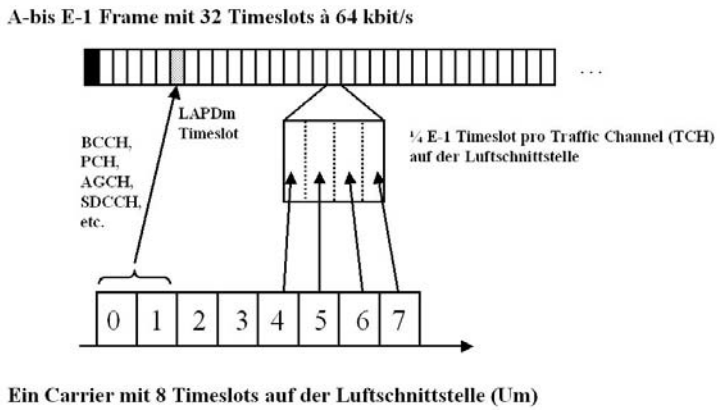

Abb. 1.26: Übertragung der logischen Luftschnittstellenkanäle auf dem A-bis Interface zum BSC.

1.7.4 Der Base Station Controller (BSC)

Während die Basisstationen die Schnittstellenelemente zu den Endgeräten darstellen, ist der Base Station Controller (BSC) für den Aufbau, Abbau und Aufrechterhaltung sämtlicher Verbindungen zu den Endgeräten über alle Basisstationen in seinem Bereich zuständig.

Aufbau eines Signalisierungskanals

Möchte ein Teilnehmer ein Gespräch beginnen, eine SMS abschicken etc., schickt sein Endgerät dazu wie in Abbildung 1.25 dargestellt eine Channel Request Nachricht an die BSC. Die BSC überprüft daraufhin, ob ein freier Signalisierungskanal (SDCCH) vorhanden ist und aktiviert diesen in der BTS. Danach schickt die BSC auf dem Access Grant Channel (AGCH) eine Immediate Assignment Nachricht mit der Nummer des zugeteilten SDCCH zum Endgerät zurück. Über die so aufgebaute Signalisierungsverbindung können nun DTAP Nachrichten transparent zur MSC weitergeleitet werden.

Der zweite Fall für den Aufbau eines Signalisierungskanals ist eine ankommende Verbindung, wie z.B. ein Telefongespräch oder eine SMS. In diesem Fall empfängt der BSC eine Paging Nachricht von der MSC. Die Paging Nachricht enthält die IMSI, die TMSI sowie die Location Area, in der sich der gewünschte Teilnehmer momentan aufhält. Die Zellen, die sich in dieser Location Area befinden, sind der Location Area Datenbank im BSC bekannt. Der BSC leitet daraufhin die Paging Nachricht an

alle Zellen weiter, die sich in dieser Location Area befinden. Nach Empfang der Paging Nachricht meldet sich das Endgerät beim Netzwerk wiederum wie im ersten Fall gezeigt mit einer Channel Request Nachricht.

Aufbau eines Sprachkanals

Der Aufbau eines Sprachkanals wird sowohl für ein abgehendes, wie auch für ein ankommendes Gespräch immer von der MSC bei der BSC beantragt. Nachdem sich MSC und Endgerät über die Signalisierungsverbindung (SDCCH) über den Aufbau einer Sprachverbindung verständigt haben, schickt die MSC wie in Abbildung 1.27 gezeigt, eine Assignment Request Nachricht an die BSC.

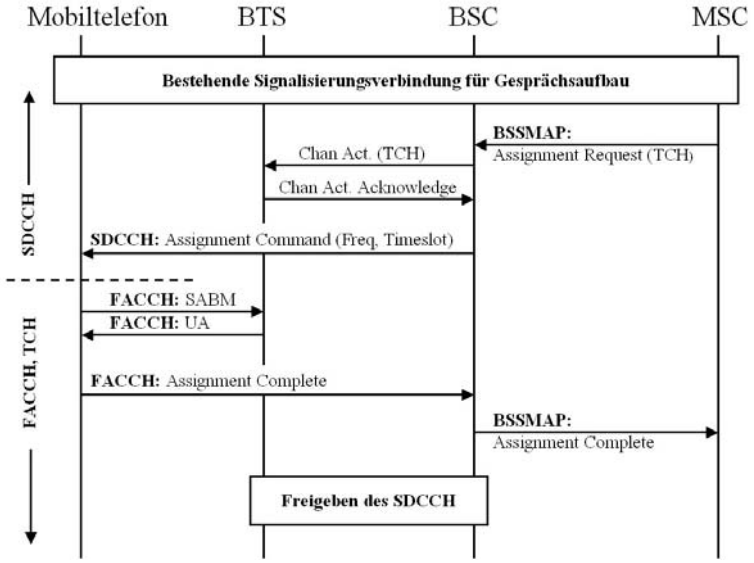

Abb. 1.27: Aufbau eines Sprachkanals (TCH)

Die BSC überprüft daraufhin, ob in der gewünschten Zelle ein freier Traffic Channel (TCH) vorhanden ist und aktiviert diesen in der BTS. Danach wird das Endgerät über den SDCCH benachrichtigt, dass ein TCH für die weitere Kommunikation zur Verfügung steht. Das Endgerät wechselt dann auf den TCH und FACCH und sendet ein SABM Frame zur BTS. Diese sendet daraufhin ein UA Frame als Bestätigung über die korrekte Verbindungsaufnahme an das Endgerät zurück. Danach sendet das Mobiltelefon ein Assignment Complete an die BSC zurück, die diese Nachricht auch an die MSC weitergibt.

Handover

Neben dem Auf- und Abbau ist auch die Aufrechterhaltung einer Verbindung eine wichtige Aufgabe des Base Station Controllers. Da Teilnehmer auch während einer Verbindung ihren Standort ändern können, kommt es während einer Verbindung durchaus vor, dass sich Teilnehmer aus dem Versorgungsbereich ihrer aktuellen Zelle hinausbewegen. In diesem Fall muss die BSC einen Wechsel der Verbindung in eine Zelle mit besserer Funkversorgung veranlassen. Dieser Vorgang wird Handover genannt. Um einen Handover durchzuführen, benötigt die BSC Messergebnisse über die Signalqualität auf der Luftschnittstelle. Die Messergebnisse für die Signalqualität im Downlink erhält die BSC vom Endgerät, das die Signalqualität laufend misst und über den SACCH dem Netzwerk mitteilt. Die Uplink Signalqualität wird ständig von der BTS gemessen und ebenfalls dem BSC mitgeteilt. Neben der Signalqualität der aktuellen Zelle ist es für das Netzwerk weiterhin wichtig zu wissen, wie gut die Nachbarzellen von einem Teilnehmer empfangen werden können. Dazu teilt das Netzwerk dem Endgerät über den SACCH die Frequenzen der Nachbarzellen mit, die vom Endgerät dann in den Sendepausen überprüft werden. Auch diese Messergebnisse werden dem Netzwerk über den SACCH mitgeteilt.

Aufgrund dieser Messergebnisse trifft die BSC dann bei Bedarf die Entscheidung, in welche Zelle ein Handover erfolgen soll. Dazu wird als erstes wie in Abbildung 1.29 dargestellt in der neuen Zelle ein TCH aktiviert. Danach schickt die BSC dem Endgerät über die alte Zelle ein Handover Command über den Fast Associated Control Channel (FACCH). Wichtige Informationen in dieser Nachricht sind die neue Frequenz und die Nummer des Timeslots des neuen TCH. Das Endgerät ändert dann seine Sende/Empfangsfrequenz, synchronisiert sich ggf. mit der neuen Zelle und sendet in vier aufeinander folgenden Bursts des Timeslots eine Handover Access Nachricht. Im fünften Burst des Timeslots wird eine SABM Nachricht gesendet. Hat die BTS den Handover korrekt erkannt, schickt diese eine Establish Indication Nachricht zum BSC und eine UA Nachricht zum Endgerät. Die BSC kann daraufhin die Sprachverbindung in die neue Zelle schalten.

Aus Sicht des Endgeräts ist der Handover damit beendet. Die BSC muss jedoch noch den TCH in der alten Zelle abbauen und dem MSC eine Nachricht über den erfolgten Handover schicken. Diese Nachricht ist jedoch nur informativ und hat auf der MSC keinen Einfluss auf den weiteren Verbindungsablauf.

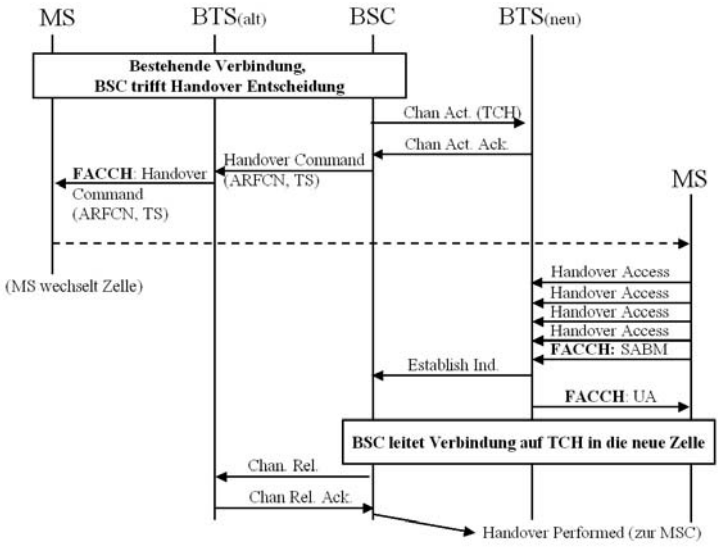

Abb. 1.28: Nachrichtenfluss während eines Handovers

Leistungsregelung

Um Interferenzen möglichst gering zu halten, kontrolliert die BSC während einer Verbindung für jeden Teilnehmer die Sendeleistung auf der Luftschnittstelle. Für Endgeräte hat dies auch den positiven Effekt, dass bei guter Verbindung die Sendeleistung reduziert werden kann und sich somit die Akkulaufzeit erhöht. Die Regelung erfolgt dabei mit Hilfe der Signalqualitätsmessungen der BTS. Muss die Sendeleistung erhöht oder abgesenkt werden, sendet die BSC eine entsprechende Änderungsinformation einmalig zur BTS. Die BTS sendet diese dann periodisch am Anfang jedes SACCH Frames zur Mobilstation. Wie sich in der Praxis zeigt, wird eine Leistungsanpassung etwa alle 1-2 Sekunden durchgeführt, sofern sich die Signalqualität ändert. Bei Verbindungsaufbau wird dazu immer erst mit einer hohen Sendeleistung begonnen, die dann Schritt für Schritt abgesenkt, bzw. wieder erhöht werden kann. Die nachfolgende Tabelle gibt eine Übersicht über die bei GSM möglichen Leistungsklassen für Endgeräte. Dabei wird zwischen Leistungsklassen für das 900 MHz Band und das 1800 MHz Band unterschieden. Während die maximale Sendeleistung für Mobiltelefone im 900 MHz Band 2 Watt beträgt, ist diese im 1800 MHz Band auf 1 Watt begrenzt. Für stationäre Geräte oder Autotelefone mit Außenantenne ist im 900

MHz Bereich eine Sendeleistung bis zu 8 Watt definiert. Die Leistungsangaben in der Tabelle beziehen sich auf die Leistung, die während der Übertragung in einem einzelnen Timeslot von einem Endgerät erreicht wird. Da das Endgerät aber nur in einem von 8 Timeslots sendet, ist für die gemittelte Leistung der angegebene Wert durch 8 zu Teilen. Die maximale durchschnittliche Sendeleistung bei einer Sendeleistung von zwei Watt ist somit nur 250 mW.

GSM 900 Power Level	GSM 900 Leistung	GSM 1800 Power Level	GSM 1800 Leistung
(0-2)	*(8W)*		
5	2W	0	1W
6	1.26W	1	631 mW
7	794 mW	2	398 mW
8	501 mW	3	251 mW
9	316 mW	4	158 mW
10	200 mW	5	100 mW
11	126 mW	6	63 mW
12	79 mW	7	40 mW
13	50 mW	8	25 mW
14	32 mW	9	16 mW
15	20 mW	10	10 mW
16	13 mW	11	6.3 mW
17	8 mW	12	4 mW
18	5 mW	13	2.5 mW
19	3.2 mW	14	1.6 mW
		15	1.0 mW

Auch die Sendeleistung der BTS kann von der BSC geregelt werden. Hierfür werden Signalstärke Messergebnisse des Endgeräts verwendet. Dies ist jedoch in den Standards nur als optional definiert. Die Leistungsregelung im Downlink ist außerdem nur für Timeslots auf Frequenzen möglich, die keine Broadcastkanäle

(FCH, SCH, BCCH…) einer Zelle aussenden. Auf solchen Frequenzen muss die Sendeleistung konstant bleiben, damit Teilnehmer in anderen Zellen eine korrekte Nachbarschaftszellenmessung durchführen können. Dies wäre bei einer schwankenden Signalamplitude über die unterschiedlichen Timeslots hinweg nicht möglich.

Timing Advance

Entfernt sich ein Teilnehmer während einer aktiven Verbindung von einer Basisstation, benötigen die Funkwellen eines Bursts aufgrund der begrenzten Ausbreitungsgeschwindigkeit der Funkwellen für den längeren Weg mehr Zeit. Würde hier nicht gegengesteuert werden, würde sich der Burst eines Teilnehmers bei zu großer Entfernung trotz der in Abb. 1.22 beschriebenen Guard Time mit dem Burst des Teilnehmers im nächsten Zeitschlitz überschneiden. Aus diesem Grund muss der Sendezeitpunkt für alle Teilnehmer ständig überwacht und angepasst werden. Dabei gilt, dass je weiter ein Teilnehmer entfernt ist er umso früher seinen Burst senden muss, damit dieser zur richtigen Zeit bei der Basisstation eintrifft. Dieses Verfahren wird Timing Advance Regelung genannt.

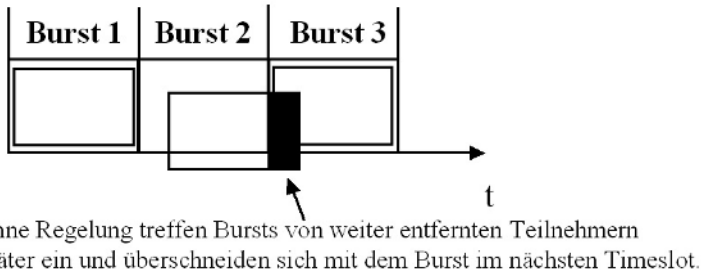

Abb. 1.29: Zeitverschiebung eines Bursts ohne Timing Advance Regelung

Timing Advance Regelung

Die Regelung erfolgt dabei in 64 Schritten von 0 bis 63. Pro Schritt kann die Entfernung zur Basisstation um 550 Meter angepasst werden. Die maximale Distanz zwischen einer Basisstation und einem mobilen Teilnehmer kann somit theoretisch 64*550m = 35.2 km betragen. In der Praxis wird eine solche Distanz jedoch nur sehr selten erreicht, da Basisstationen in besiedelten Gebieten wesentlich näher zusammenliegen. Auch reicht die Sendeleistung des Endgeräts nicht aus, diese Entfernung zu über-

brücken, da zumeist auch keine direkte Sichtverbindung zwischen Mobiltelefon und Basisstation besteht. Dieser Wert kann allenfalls in Küstennähe von einem Schiff erreicht werden.

Die Regelung des Timing Advance beginnt schon beim ersten Zugriff des Mobiltelefons auf das Netzwerk mit der Channel Request Nachricht. Diese Nachricht verwendet einen sehr kurzen Burst, der nur sehr wenig Nutzdaten enthalten kann, dafür aber sehr große Guard Periods an Anfang und Ende. Dies ist notwendig, da am Anfang das Mobiltelefon nicht wissen kann, wie weit es von der Basisstation entfernt ist und somit auch noch keinen Timing Advance einstellen kann. Beim Eintreffen der Channel Request Nachricht bei der BTS misst diese die zeitliche Verzögerung des Bursts. Anschließend leitet die BTS die Channel Request Nachricht inklusive der gemessenen Verzögerungszeit in Form eines Timing Advance Wertes an die BSC weiter. Wie in Abbildung 1.25 gezeigt wurde, schickt die BSC als Antwort auf die Channel Request Nachricht eine Immediate Assignment Nachricht an die Mobilstation zurück. Neben der Nummer des zugeteilten Signalisierungskanals (SDCCH) enthält die Nachricht auch den ersten Timing Advance Wert, den die Mobilstation für die weitere Kommunikation verwenden soll. Nach erfolgreicher Verbindungsaufnahme über den SDCCH und später evtl. über den TCH misst die BTS ständig die Zeitverzögerung der eintreffenden Bursts und meldet diese in Form eines Timing Advance Wertes der BSC weiter. Ändert sich der Timing Advance Wert, informiert die BSC über den SACCH das Endgerät, das daraufhin seinen Timing Advance Wert entsprechend korrigiert.

Erweiterter Zellradius

Für Anwendungsfälle wie Küstenkommunikation enthält der GSM Standard noch eine weitere Timeslotkonfiguration, um die maximale Entfernung zur Basisstation auf bis zu 120 km auszudehnen. Um dies zu ermöglichen, wird in einer Zelle nur jeder zweite Timeslot verwendet und bewusst akzeptiert, dass der Burst sich in den nächsten Timeslot verschiebt. Dies erweitert zwar den Abdeckungsbereich einer Zelle erheblich, dies geht aber sehr zu lasten der Anzahl der verfügbaren Kommunikationskanäle. Mobiltelefone, die wie heute üblich auf ein Watt (1800 MHz Band) oder zwei Watt (900 MHz Band) begrenzt sind, mögen zwar den BCCH empfangen können, aufgrund ihrer Sendeleistung wird das Uplink Signal die Basisstation aber nicht erreichen. Aus diesem Grund können Zellen in solcher Entfernung nur von fest eingebauten Mobiltelefonen verwendet werden, die mit einer Leistung von bis zu 8 Watt senden können.

1.7.5 Die TRAU für Sprachdatenübertragung

Bandbreite eines TCH

Für die Übertragung eines Sprachdatenkanals über die Luftschnittstelle dient in GSM der in 1.7.3 beschriebene Traffic Channel (TCH). Dieser verwendet wie in Abb. 1.24 gezeigt alle Bursts eines 26 Multiframe mit Ausnahme eines Burst für den Slow Associated Control Channel und einen Burst, der für die Nachbarzellen Pegelmessung leer bleibt. Wie im letzten Kapitel außerdem gezeigt wurde, kann ein Burst, der alle 4.615 ms übertragen wird, genau 114 Bit Nutzdaten aufnehmen. Dies entspricht unter Berücksichtigung der zwei nicht für den TCH verwendeten Bursts pro 26-Multiframe einer Bruttodatenrate von 22.8 kbit/s. Wie wir im Laufe dieses Kapitels noch genauer betrachten werden, wird von dieser Bruttodatenrate ein großer Teil für die Fehlererkennung und Fehlerkorrektur verwendet, so dass für die reinen Sprachdaten nur eine Bandbreite von etwa 13 kbit/s zur Verfügung steht.

Komprimierung der Sprachdaten

Dies ist ein Problem, da im Kernnetzwerk immer ein 64 kbit/s E-1 Timeslot für einen Sprachkanal verwendet wird und auch der in Kapitel 1.6.1 vorgestellte PCM Sprachkodierer diese Bandbreite voll ausnutzt.

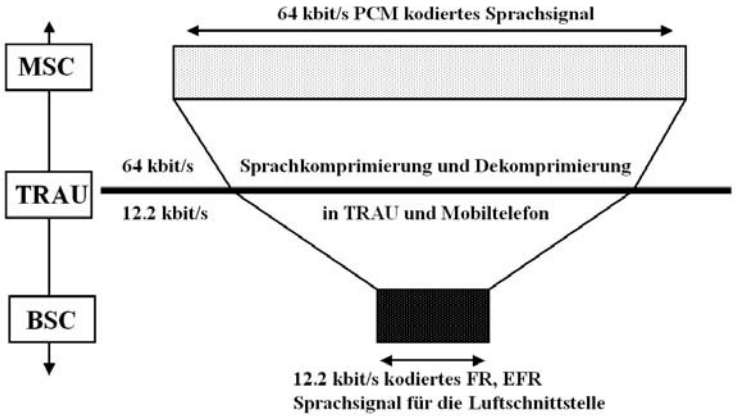

Abb. 1.30: GSM Sprachdatenkomprimierung

Um dieses Problem erst gar nicht entstehen zu lassen, hätte der GSM Standard auch 64 kbit/s Sprachkanäle auf der Luftschnittstelle definieren können. Die Wahl eines Kanals mit weit geringerer Bandbreite wurde aber ganz bewusst getroffen, um möglichst viele Sprachkanäle über die knappen Ressourcen auf der

Luftschnittstelle übertragen zu können. Dies wurde auch deshalb möglich, da zu Beginn der Standardisierung in den 80'er Jahren absehbar war, dass die technischen Möglichkeiten zur Komprimierung der Sprachdaten von 64 kbit/s auf 13 kbit/s in Echtzeit durch neue Hardwareentwicklungen möglich wurde.

TRAU

Im Mobilfunknetzwerk wird die Komprimierung und Dekomprimierung der Sprachdaten durch die Transcoding and Rate Adaptation Unit (TRAU) durchgeführt. Diese wird zwischen eine MSC und einen BSC geschaltet und von der BSC kontrolliert. Die MSC schickt dabei die Sprachdaten im 64 kbit/s PCM Format in Richtung Radionetzwerk. In der TRAU wird das Sprachsignal dann auf etwa 13 kbit/s komprimiert und zur BSC weitergeschickt. In der Gegenrichtung dekomprimiert die TRAU das von der BSC erhaltene 13 kbit/s Sprachsignal wieder in das 64 kbit/s PCM Format und gibt es an die MSC weiter. Im Endgerät auf der anderen Seite der Luftschnittstelle sind die Algorithmen für die Komprimierung und Dekomprimierung des Sprachsignals ebenfalls implementiert.

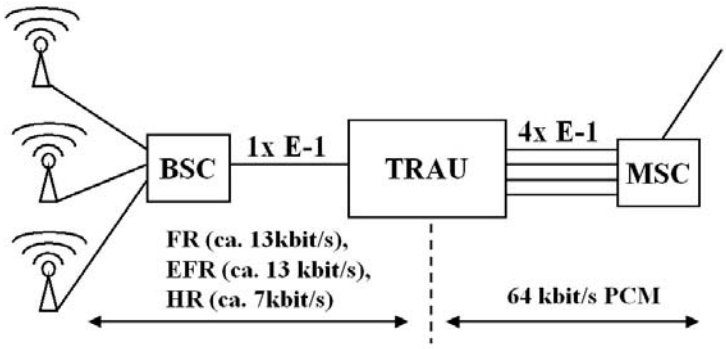

Abb. 1.31: Sprachkompression in Verhältnis 4:1 in der TRAU

Obwohl die TRAU eine logische Komponente des BSS ist, wird diese in der Praxis normalerweise direkt neben einer MSC aufgestellt. Dies hat den Vorteil, dass nach der Komprimierung des Sprachdatensignals vier Sprachkanäle mit je 13 kbit/s auf einem einzigen E-1 Timeslot übertragen werden können. Jeder Sprachkanal belegt damit einen 16 kbit/s Subtimeslot. Somit wird nur ¼ der Übertragungskapazität zwischen MSC und BSC benötigt. Da die BSCs normalerweise in größerer Entfernung zur MSC aufgestellt werden, ergibt sich dadurch eine deutliche Kosteneinsparung für den Netzbetreiber.

Full Rate

Die TRAU bietet eine Anzahl unterschiedlicher Algorithmen für die Sprachkomprimierung. Diese werden auch Sprachcodecs oder Codecs genannt. Der als erstes implementierte Codec wurde Full Rate Codec (FR) genannt und komprimiert das Sprachsignal in Echtzeit auf etwa 13 kbit/s.

Enhanced Full Rate

Ende der 90'er Jahre wurde ein weiterer Codec eingeführt, der sich Enhanced Full Rate Codec (EFR) nennt und heute im Grossteil der in Betrieb befindlichen Netze bevorzugt verwendet wird. Auch der EFR Codec komprimiert das Sprachsignal auf etwa 13 kbit/s, bietet aber eine bessere Sprachqualität. Nachteil ist der wesentlich komplexere Komprimierungsalgorithmus, der deutlich mehr Rechenkapazität benötigt. Dies spielt aber bei heutigen Mobiltelefonen auch im Niedrigpreissegment aufgrund der gestiegenen Prozessorleistung keine Rolle mehr.

Half Rate

Neben diesen zwei Codecs gibt es den Half Rate Codec (HR), der nur 7 kbit/s Bandbreite benötigt. Während beim Enhanced Full Rate Codec fast kein Unterschied zum original 64 kbit/s PCM Signal zu hören ist, ist die Sprachqualität beim Half Rate Codec deutlich schlechter. Vorteil für den Netzbetreiber ist jedoch, dass sich die Anzahl der möglichen Sprachverbindungen über eine BTS verdoppelt. Auf einem Timeslot, der normalerweise für einen TCH (EFR) benötigt wird, können auf diese Weise zwei TCH (HR) übertragen werden. In der Praxis scheinen die Netzbetreiber den Half Rate Codec jedoch nicht oft einzusetzen. Selbst bei großen Veranstaltungen wie Messen mit vielen zehntausend Teilnehmern auf engstem Raum wird vorwiegend ein normaler TCH (FR) oder TCH (EFR) für eine Sprachverbindung verwendet.

Adaptive Multi Rate

Die neueste Sprachcodec Entwicklung ist der Adaptive Multi Rate Algorithmus, auch AMR genannt. Statt sich wie bei FR, EFR und HR bei Beginn der Sprachverbindung auf einen Codec festzulegen, erlaubt der Adaptive Multi Rate Algorithmus den Wechsel des verwendeten Codecs auch während der Verbindung. Ein wesentlicher Vorteil dieses Verfahrens ist, bei einer schlechten Verbindung auf einen Sprachcodec mit höherer Kompression umzuschalten und dafür die Anzahl der Bits für Fehlererkennung und Fehlerkorrektur zu erhöhen. Andererseits kann bei einer guten Verbindung die Kapazität der Zelle gesteigert werden, in dem ein Codec mit niederer Bitrate gewählt wird und nur ein Timeslot in jedem zweiten Frame für ein Gespräch verwendet wird. Während dieses Verfahren bei GSM optional ist, wird bei UMTS ausschließlich AMR für die Sprachübertragung verwendet. Ob sich AMR bei GSM in Europa durchsetzten wird ist fraglich,

da Netzwerkbetreiber in Zukunft hauptsächlich in den Ausbau ihrer UMTS Netzwerke investieren werden. Weitere Informationen über AMR sind im Kapitel über UMTS zu finden.

Sprach-kompression

Während der bereits vorgestellte PCM Algorithmus im wesentlichen analoge Pegel über eine vorgegebene Kurve in digitale Werte umwandelt, ist die GSM Sprachdigitalisierung wesentlich komplexer aufgebaut, um die gewünschte Kompression zu erreichen. Im Falle des Full Rate Codecs, der im GSM Standard 06.10 spezifiziert ist, erfolgt die Komprimierung durch Nachbildung der menschlichen Spracherzeugung. Als mathematische Grundlage dient ein Quelle–Filter Modell. Die menschliche Spracherzeugung im Kehlkopf und mit den Stimmbändern wird in diesem Modell durch die Quelle repräsentiert. Die Filter repräsentieren die Signalformung, die beim Mensch im Rachen und Mundraum stattfindet.

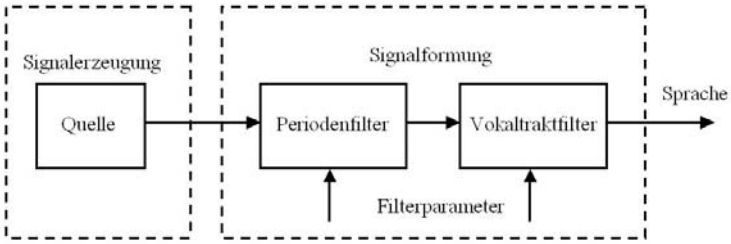

Abb 1.32: Quelle-Filter Modell des Full Rate Codecs

Mathematisch wird die Sprachformung durch zwei zeitvariante Filter nachgebildet. Der Periodenfilter bildet dabei die periodischen Vibrationen der menschlichen Sprache nach, der Vokaltraktfilter simuliert die Hüllkurve der menschlichen Sprache. Die für die Filter notwendigen Parameter werden aus dem Eingangssignal gebildet. Um menschliche Sprache zu digitalisieren und zu komprimieren, wird dieses Modell wie in Abbildung 1.32 gezeigt in umgekehrter Reihenfolge angewandt. Da zeitvariante Filter schwer nachzubilden sind, wird das Modell noch deutlich vereinfacht, in dem die Filterparameter für die Zeit von 20 ms als konstant betrachtet werden.

Als Eingangssignal dient dem Kompressionsalgorithmus ein nach dem PCM Verfahren digitalisiertes Sprachsignal, das wie bereits gezeigt pro Wert 8 (oder 13) Bit verwendet. Da der PCM Algorithmus pro Sekunde 8000 Werte liefert, benötigt der Full Rate

Codec für die Berechnung der Filterparameter alle 20 ms genau 160 Werte. Bei 8 Bit pro Wert ergibt dies 8 Bit * 160 Werte = 1280 Eingangsbits, bei 13 Bits pro Wert entsprechend mehr. Für den Periodenfilter wird aus diesen Eingangsbits dann ein 36 Bit langer Filterparameter berechnet. Danach wird dieser Filter auf das Eingangssignal angewandt. Mit dem daraus entstandenen Ergebnis wird ein weiterer 36 Bit langer Filterparameter für den Vokaltraktfilter berechnet und der Filter daraufhin wieder entsprechend auf das Signal angewandt. Das so entstandene Restsignal wird in insgesamt 188 Bit kodiert.

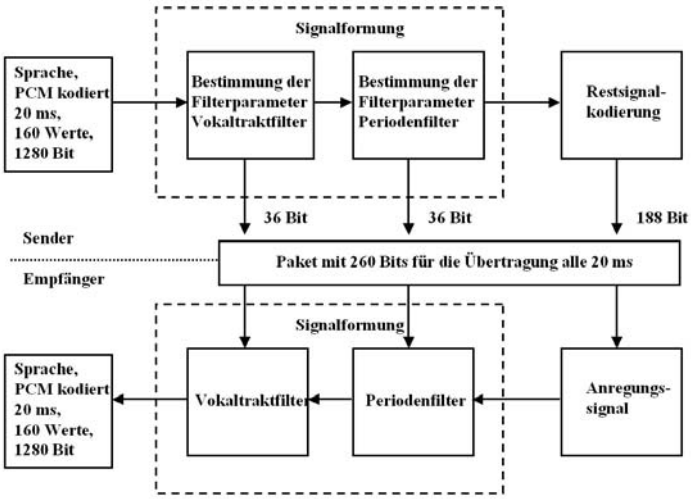

Abb. 1.33: Komplette Übertragungskette mit Sender und Empfänger des GSM Full Rate Codec

Verlustbehaftete Kompression

Übertragen werden anschließend die Filterparameter mit jeweils 36 Bit Länge, sowie das in 188 Bit kodierte Restsignal. Somit werden statt den ursprünglichen 1280 Eingangsbits nur 36+36+188 = 260 Bits übertragen. Auf der Gegenseite wird der Filtervorgang in umgekehrter Reihenfolge auf das Restsignal durchgeführt und das ursprüngliche Sprachsignal somit wiederhergestellt. Da das Verfahren verlustbehaftet arbeitet, ist das wiederhergestellte Signal nicht mehr mit dem Original identisch. Dies ist der Grund, warum sich ein mit dem Full Rate Decoder komprimiertes und wieder dekomprimiertees Sprachsignal hörbar vom ursprünglichen PCM Signal unterscheidet. Mit dem En-

hanced Full Rate Coder, der nach einem komplexeren Algorithmus arbeitet, ist dieser Unterschied jedoch fast unhörbar geworden.

Übertragungskette

Bevor dieses 260 Bit Datenpaket alle 20 ms über die Luftschnittstelle übertragen wird, durchläuft es noch eine Reihe von weiteren Verarbeitungsschritten, die nicht in der TRAU, sondern in der Basisstation durchgeführt werden. Diese sind im Überblick in Abbildung 1.34 dargestellt.

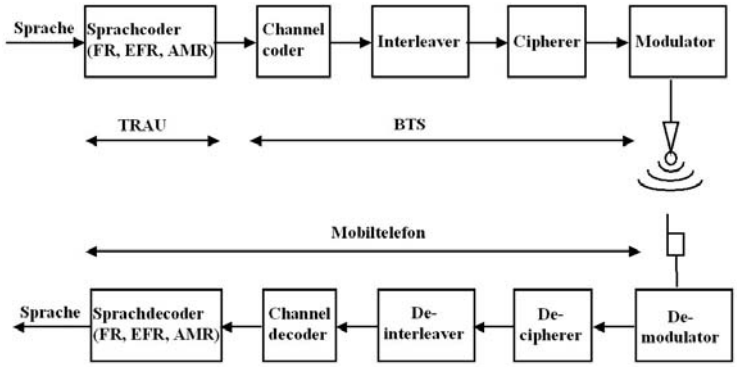

Abb. 1.34: Übertragungsschritte im Downlink zwischen Netzwerk und Mobiltelefon.

Kanalkodierer

Im Kanalkodierer werden dem eigentlichen Nutzdatenstrom Fehlererkennungs- und Fehlerkorrekturinformationen hinzugefügt. Dies ist sehr wichtig, da die Übertragung über die Luftschnittstelle aufgrund der sich ständig ändernden Bedingungen sehr störanfällig ist. Ausserdem machen sich aufgrund der stark komprimierten Sprachdatenübertragung schon wenige Fehler später deutlich hörbar bemerkbar. Um dies zu vermeiden, werden die 260 Bits des Sprachdatenblocks wie in Abbildung 1.35 gezeigt in drei unterschiedliche Klassen eingeteilt:

50 Bits des 260 Bit Sprachpakets werden zur ersten Klasse (Class Ia) gezählt. Sie sind extrem wichtig und dürfen unter keinen Umständen bei der Übertragung verfälscht werden. Solche Bits sind z.B. die höherwertigen Bits der FR Coder Filterparameter. Um dies zu gewährleisten, wird eine 3 Bit CRC Checksumme gebildet und in den Datenstrom eingefügt. Wird auf der Empfängerseite festgestellt, dass hier ein Fehler aufgetreten ist, wird das komplette Datenpaket verworfen.

Die 132 Bits der zweiten Klasse (Class Ib) sind auch wichtig, werden aber nicht durch eine Checksumme geschützt. Um später

eine vorgegebene Anzahl an Bits am Ausgang des Kanalkodieres zu erhalten, werden am Ende der Klasse Ib vier Füllbits eingefügt. Die Bits der Klasse Ia, die CRC Checksumme, die Bits der Klasse Ib und die vier Füllbits werden dann einem Faltungskodierer übergeben, der den Daten Redundanz hinzufügt. Für jedes Eingangsbit berechnet der Faltungskodierer, im englischen Convolutional Coder genannt, zwei Ausgangsbits. Für die Berechnung der zwei Ausgangsbits wird nicht nur der Wert des aktuellen Bits herangezogen, sondern auch die der vorangegangenen Bits. Da für jedes Eingangsbit genau zwei Ausgangsbits berechnet werden, spricht man auch von einem ½-Rate Convolutional Coder.

Zur dritten Klasse (Class II) gehören 78 Bits des ursprünglichen 260 Bit Datenpakets. Diese werden ohne Checksumme und ohne Redundanz übertragen. Fehler, die hier auftreten, können weder erkannt, noch korrigiert werden.

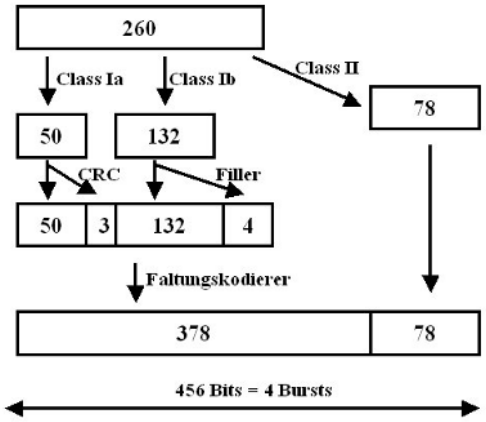

Abb. 1.35: GSM Kanalkodierer für FR Sprachdaten

Aus den ursprünglichen 260 Bits erstellt der Kanalkodierer somit 456 Bits. Da pro Burst auf der Luftschnittstelle 114 Bits an Daten übertragen werden, entspricht dies somit genau 4 Bursts. Da ein Burst eines TCHs alle 4.6152 ms übertragen wird, ergibt dies somit in etwa wieder 20 ms. Um exakt auf eine Übertragungszeit von 20 ms für diese Daten zu kommen, muss noch der Burst für den SACCH und der leere Burst für die Nachbarzellenmessung eines 26 Multiframe in die Rechnung einbezogen werden.

Interleaver

Durch die im Kanalkodierer hinzugefügte Redundanz ist es möglich, auch eine größere Anzahl an Fehlern pro Datenblock zu korrigieren. Der Faltungskodierer hat jedoch eine Schwachstelle: Werden direkt aufeinander folgende Bits während der Übertragung auf der Luftschnittstelle verfälscht, kann der Faltungsdekodierer auf der anderen Seite die ursprünglichen Daten nicht korrekt wiederherstellen. Dieser Effekt tritt aber sehr häufig bei ungünstigen Übertragungsbedingungen auf, da Übertragungsstörungen dann meist länger als eine Bitperiode dauern.

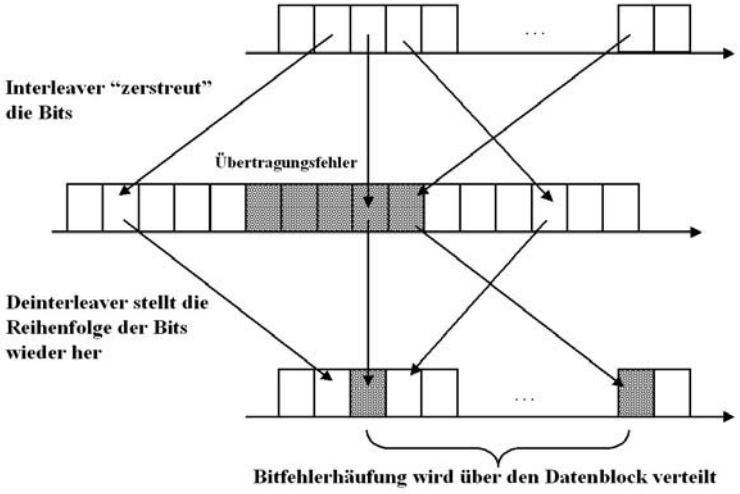

Abb. 1.36: Funktionsweise des Interleavers

Um diesen Effekt zu vermeiden, verteilt der Interleaver die Bits eines 456 Bit Datenblocks nach einem vorgegebenen Muster über insgesamt 8 Bursts. Aufeinanderfolgende Datenblöcke greifen somit ineinander. Auf der Empfängerseite werden die Datenbits dann wieder durch den Deinterleaver in die richtige Reihenfolge gebracht. Werden nun an einer Stelle viele Bits hintereinander verfälscht, verteilt der Deinterleaver diese somit über das ganze Datenpaket, und der Faltungskodierer kann dies entsprechend korrigieren.

Ein Nachteil dieses Verfahrens ist jedoch eine längere Verzögerung (Delay) des Sprachsignals. Zusätzlich zu den 20 ms des Full Rate Coders, kommen im Interleaver noch weitere 40 ms hinzu, da ein Sprachblock nun über 8 Bursts verteilt wird und nicht direkt in 4 Blocks übertragen wird. Bei einem Gespräch von

Mobiltelefon zu Festnetzanschluß ergibt sich dadurch somit mindestens eine Verzögerung von 60 ms. Von Mobiltelefon zu Mobiltelefon sind es dagegen schon mindestens 120 ms, da hier die Kette zweimal durchlaufen wird.

Cipherer

Als nächster Schritt in der Übertragungskette folgt der Cipherer, der vom Interleaver erhaltene Datenpakete verschlüsselt. GSM verwendet dazu wie bei den meisten Kommunikationssystemen üblich einen Stream Cipher Algorithmus. Dazu wird im Authentication Center und auf der SIM Karte aus einer Zufallszahl (RAND), dem geheimen Schlüssel Ki und dem Algorithmus A8 der Ciphering Key Kc errechnet. Zusammen mit der GSM Framenummer, die nach der Übertragung jedes Frames erhöht wird, bildet Kc die Eingangsparameter für den Verschlüsselungsalgorithmus A5. Dieser berechnet nun eine 114 Bit lange Sequenz, mit der die Originaldaten für einen Burst dann Bit für Bit Exklusiv Oder (XOR) verknüpft werden. Da sich die Frame Nummer bei jedem Burst ändert ist gewährleistet, dass sich auch die 114 bit Schlüsselsequenz für jeden Burst ändert und somit die Sicherheit des Verfahrens weiter erhöht wird.

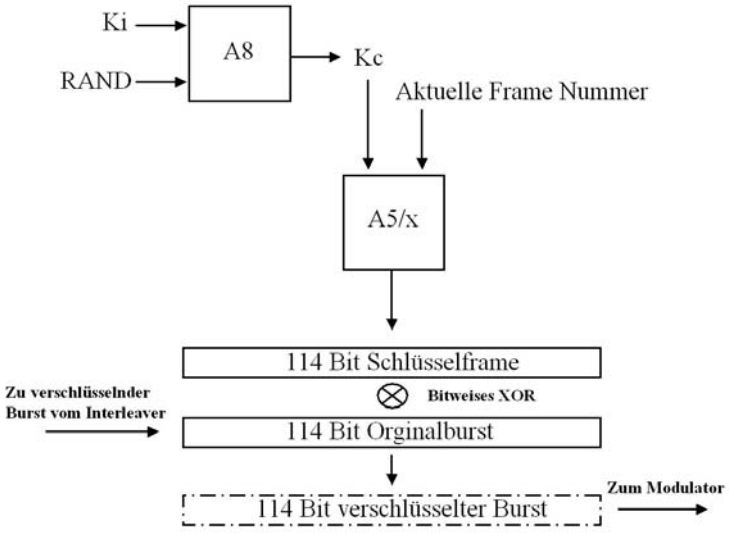

Abb. 1.37: Verschlüsselung eines Datenbursts

Um möglichst flexibel zu sein, wurden bei GSM mehrere Ciphering Algorithmen spezifiziert, die A5/1, A5/2, A5/3… genannt wurden. Somit ist es möglich, GSM Netze auch in Länder zu exportieren, in die manche Verschlüsselungsalgorithmen nicht

exportiert werden dürfen. Auch ist es möglich, in einem bestehenden Netzwerk jederzeit einen neuen Verschlüsselungsalgorithmus einzuführen und eventuell gefundene Sicherheitsprobleme durch die Verwendung eines neuen Algorithmus zu lösen. Die Wahl des verwendeten Algorithmus hängt jedoch auch vom Endgerät ab. Damit das Netzwerk einen geeigneten Verschlüsselungsalgorithmus für eine Verbindung wählen kann, informiert das Endgerät dafür bei Verbindungsaufnahme das Netzwerk über die unterstützten Algorithmen.

Aktivieren der Verschlüsselung

Da bei Beginn der Kommunikation die Identität des Teilnehmers dem Netzwerk nicht bekannt ist, muss sich das Endgerät vor dem Aktivieren der Verschlüsselung zuerst authentifizieren. Dieser Vorgang wurde in Kapitel 1.6.4 beschrieben. Die Aktivierung der Verschlüsselung erfolgt danach mit einer Ciphering Command Nachricht durch die MSC. Diese Nachricht enthält unter anderem Kc, der von der BTS für die Verschlüsselung verwendet wird. Bevor die Nachricht zum Mobiltelefon weitergeleitet wird, entfernt das BSS jedoch Kc aus der Nachricht, da dieser nicht über die Luftschnittstelle übertragen werden darf. Die Übermittlung von Kc an das Mobiltelefon ist auch nicht notwendig, da die SIM Karte diesen selber errechnen kann. In Abbildung 1.40 wird gezeigt, wie bei der Kommunikation für ein Location Update die Verschlüsselung aktiviert wird.

Schwachstellen

Leider weist die Art der Verschlüsselung bei GSM ein paar Schwachstellen auf. Eine gravierende Schwachstelle ist zum Beispiel, dass die Verschlüsselung nur als optional in den Standards definiert wurde und somit an- und abschaltbar ist. Manche Mobiltelefone wie z.B. die S-Reihe von Siemens zeigen auf dem Display an, ob die Verschlüsselung aktiviert oder deaktiviert ist. Ist sie deaktiviert, erscheint im Display ein ‚*!*' Symbol. Da dem Autor dieses Symbol jedoch bisher nur im Labor bei speziellen Tests begegnet ist, darf davon ausgegangen werden, dass die Verschlüsselung in öffentlichen Netzen immer eingeschaltet ist. Eine weitere Schwachstelle der Verschlüsselung ist der Umstand, dass der Datenverkehr nur zwischen der BTS und dem Teilnehmer verschlüsselt wird. Alle anderen Übertragungsschnittstellen, wie z.B. von der BTS zum BSC, zur TRAU und zur MSC sind nicht geschützt. Da viele Netzbetreiber Basisstationen per Richtfunk mit der BSC verbinden, ist das Abhören an dieser Schnittstelle ohne Eingriff in das Netzwerk möglich.

Modulation

Als letzter Schritt in der Übertragungskette steht der Modulator. Dieser überträgt die digitalen Daten auf einen Träger (Carrier)

mit einer Bandbreite von 200 kHz durch Änderung der Trägerfrequenz. Da die Trägerfrequenz nicht beliebig schnell geändert werden kann, kommt hierfür ein Verfahren namens Gaussian Minimum Shift Keying (GMSK) zum Einsatz, das die Flanken der Frequenzänderung abrundet. Dieses Verfahren wurde zum einen aufgrund seiner Modulations- und Demodulationseigenschaften gewählt, die einfach in Hardwarekomponenten umzusetzen ist und zum anderen, weil es nur geringe Interferenzen auf Nachbarkanälen erzeugt.

Discontinuous Transmission

Um die Interferenz auf der Luftschnittstelle zu reduzieren und die Akkulaufzeiten in den Endgeräten zu erhöhen, werden nur Datenbursts gesendet, wenn auch tatsächlich gesprochen wird. Dieses Verfahren wird Discontinuous Transmission (DTX) genannt und kann unabhängig im Uplink und Downlink aktiviert werden. Da üblicherweise nur ein Gesprächspartner zu einer Zeit spricht, kann somit fast immer die Übertragung zumindest in einer der beiden Richtungen abgeschaltet werden. Dies wird von der TRAU im Downlink und vom Endgerät im Uplink durch die Voice Activity Detection (VAD) gesteuert.

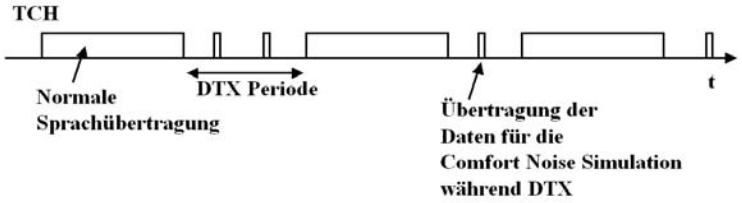

Abb. 1.38: Discontinuous Transmission (DTX)

Würde jedoch der Übertragungskanal einfach abgeschaltet, hätte das eine sehr unangenehme Nebenwirkung. Da nichts mehr übertragen wird, hört der Teilnehmer auch das Hintergrundrauschen des Gesprächspartners nicht mehr. Dies kann sehr irritierend sein, vor allem wenn das Hintergrundrauschen des Gesprächsteilnehmers aufgrund einer Zug- oder Autofahrt sehr laut ist. Deshalb ist es notwendig, während solcher Übertragungspausen ein künstliches Rauschen einzuspielen, das Comfort Noise genannt wird. Da Hintergrundgeräusche jedoch sehr verschieden sind und sich auch mit der Zeit ändern können, analysiert dazu das Mobiltelefon bzw. das Netzwerk das Hintergrundrauschen auf dem Kanal und berechnet eine Approximation. Diese Approximation wird dann nur alle 480 ms zwischen den Teilnehmern

ausgetauscht. Außerdem sind diese Frames für Signalstärke und Timing Advance Messungen notwendig. Wie gut dieses Verfahren arbeitet ist schon daran zu erkennen, dass die Simulation so gut wie nicht vom Original zu unterscheiden ist.

Nicht korrigierbare Übertragungsfehler

Trotz ausgefeilter Mechanismen zur Fehlerkorrektur kann nicht ausgeschlossen werden, dass Daten bei der Übertragung unwiederbringlich zerstört werden. In solchen Fällen wird der komplette 20 ms Sprachdatenblock vom Empfänger verworfen und stattdessen der vorige Datenblock nochmals verwendet. Meist bleiben Fehler, die mit diesem Trick ausgebessert werden, unhörbar. Dieser Trick funktioniert aber nicht auf Dauer. Wird auch nach 320 ms kein korrekter Datenblock empfangen, wird der Sprachkanal stumm geschaltet und weiter versucht, ein Datenblock korrekt zu dekodieren. Wird innerhalb der nächsten Sekunden dann weiterhin kein korrekter Datenblock empfangen, wird die Verbindung abgebrochen.

GSM Datenübertragung

Viele der vorgestellten Verfahren wurden speziell für Sprachdaten entwickelt. Für leitungsvermittelnde Datenverbindungen müssen diese modifiziert werden bzw. können gar nicht angewandt werden. Die im letzten Absatz besprochenen Verfahren bei nicht korrigierbaren Übertragungsfehlern können beispielsweise nicht für die Datenübertragung angewandt werden. Werden Bits nicht korrekt übertragen, müssen diese von neuem Übertragen werden, da ein Datenverlust von den meisten Anwendungen im Unterschied zur Sprachübertragung nicht akzeptiert werden kann. Um die Wahrscheinlichkeit für die korrekte Widerherstellung der Daten zu erhöhen, wird ein Datenblock über wesentlich mehr als 8 Bursts vom Interleaver gestreut. Auch der Kanalkodierer, der die Bits in Klassen nach deren Wichtigkeit sortiert, muss für die Datenübertragung modifiziert werden, da hier alle Bits gleich wichtig sind und somit der Faltungskodierer auf alle Bits angewandt werden muss. Schließlich kann auch keine Datenreduktion wie bei der Sprache stattfinden, die TRAU verhält sich somit bei Datenübertragungen transparent. Sollten die Daten komprimierbar sein, ist dies von der jeweiligen Anwendung vor der Übertragung selber durchzuführen.

Hörbare Bursts

Mit einem Radioempfänger bzw. Stereoanlagenverstärker können die in den vorangegangenen Absätzen beschriebenen Sendezustände während eines Gesprächs auch gehört werden. Dies ist möglich, da das An- und Abschalten des Senders im Endgerät Störungen in der Verstärkerstufe verursachen. Hält man ein GSM Telefon nahe an ein eingeschaltetes Radio oder einen Verstärker,

ist beim Gesprächsaufbau zuerst das typische Geräuschmuster zu hören, das ein GSM Telefon auf einem Signalisierungskanal (SDCCH) verursacht. Bei Aufbau eines Sprachkanals ist dann der Wechsel auf einen Traffic Channel (TCH) deutlich zu hören. Da für einen TCH alle 4.615 ms ein Brust gesendet wird, wird der Sender mit einer Frequenz von etwa 217 Hz kontinuierlich an- und abgeschaltet. Sind die Hintergrundgeräusche gering oder wird das Mikrofon abgeschaltet, wechselt das Endgerät nach kurzer Zeit in den DTX Zustand. Auch dies kann gehört werden, da dann statt dem kontinuierlichen 217 Hz Rauschen nur noch etwa alle 0.5 Sekunden Bursts gesendet werden.

Bei ankommenden Gesprächen kann man mit dieser Methode auch feststellen, dass das Mobiltelefon schon 1-2 Sekunden vor dem eigentlichen ‚Klingeln' auf dem SDCCH aktiv wird. Diese Verzögerung kommt dadurch zustande, da das Endgerät den Benutzer erst nach erfolgreicher Authentifizierung, Aktivierung der Verschlüsselung und Aufbau eines Traffic Channels über den Anruf informieren kann. Dies ist auch der Grund, warum der Gesprächsaufbau zu einem mobilen Endgerät länger dauert als zu einem Endgerät im Festnetz.

Netzmonitor

Diverse Endgerätetypen verfügen auch über Netzmonitorfunktionen, die über das normale Menü nicht zugänglich sind. Mit einem solchen Netzmonitor können dann viele der in diesem Kapitel vorgestellten Abläufe und Parameter wie Timing Advance, Kanalzuteilung, Leistungsregelung, Cell-ID, Nachbarzelleninformation, Handover, Cell Reselections und vieles mehr beobachtet werden. Im Internet gibt es zahlreiche Websites die beschreiben, wie dieser Monitormode aktiviert werden kann. Da dies nicht bei allen Endgerätetypen möglich ist und sich die Aktivierungsprozedur von Typ zu Typ unterscheidet, kann hier keine allgemeingültige Anleitung gegeben werden. Im Internet sind jedoch Anleitungen für diverse Endgeräte mit Suchbegriffen wie „GSM Netzmonitor", „GSM Netmonitor", „GSM monitoring mode", etc. zu finden.

1.8 Mobility Management und Call Control

Nachdem in den vorangegangenen Abschnitten nun alle Komponenten eines Mobilfunknetzwerkes vorgestellt wurden, zeigt dieser Abschnitt nun einige Vorgänge, um die Mobilität der Teilnehmer zu gewährleisten. In einem GSM Mobilfunknetzwerk gibt es dazu drei wesentliche Abläufe:

1.8.1 Location Area und Location Area Update

Damit das Netzwerk eingehende Verbindungen an einen Teilnehmer weitervermitteln kann, muss dessen Aufenthaltsort bekannt sein. Direkt nach dem Einschalten meldet sich das Endgerät beim Netz an. Damit kennt das Netzwerk den genauen Aufenthaltsort des Teilnehmers, der sich aber danach jederzeit ändern kann. Besteht zu dieser Zeit keine aktive Sprach- oder Datenverbindung, muss sich das Endgerät beim Netzwerk melden. Um zu vermeiden, dass dies bei jedem Zellwechsel geschehen muss, werden mehrere Zellen in einer Location Area zusammengefasst. Über den Broadcast Channel (BCCH) informiert das Netzwerk alle Teilnehmer, zu welcher Location Area die aktuelle Zelle gehört. Dazu wird neben der Cell-ID der Zelle auch ständig die Location Area ID ausgestrahlt.

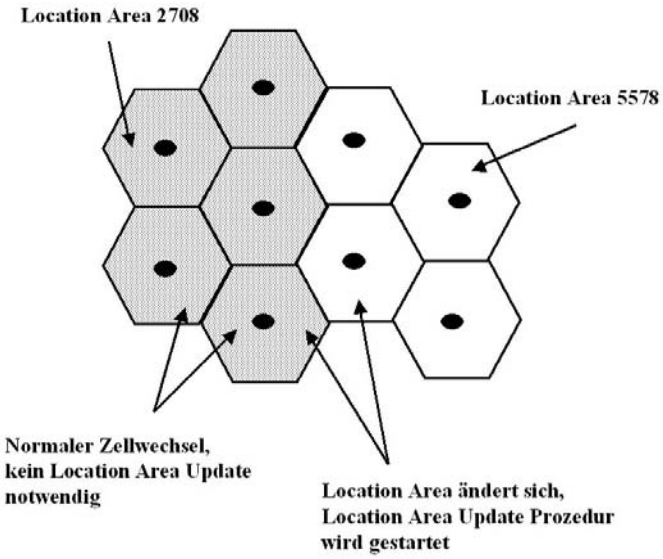

Abb. 1.39: Zellen in verschiedenen Location Areas

Wenn das Endgerät in eine Zelle einer anderen Location Area wechselt, muss dem Netzwerk dies mit einer Location Area Update Nachricht mitgeteilt werden. Dieses Verfahren reduziert zum einen die Signalisierungslast des Netzwerkes deutlich und spart zum anderen auch Energie im Endgerät. Nachteil ist jedoch, dass das Netzwerk nur noch die aktuelle Location Area des Teilnehmers kennt, nicht aber die aktuelle Zelle. Bei einem ankommen-

den Gespräch oder einer SMS muss das Netzwerk dann den Teilnehmer in allen Zellen einer Location Area suchen (Paging). Die Größe der Location Areas kann vom Netzwerkbetreiber festgelegt werden. In der Praxis zeigt sich, dass ein guter Kompromiss für die meisten Anwendungsfälle etwa 20 Zellen pro Location Area ist.

Abbildung 1.40 zeigt einen solchen Location Area Update. Nach erfolgreicher Verbindungsaufnahme, sendet das Endgerät eine Location Update Request Nachricht an das Netzwerk. Bevor das Netzwerk diese bearbeitet, wird der Teilnehmer zuerst authentifiziert und danach die Verschlüsselung (Ciphering) aktiviert.

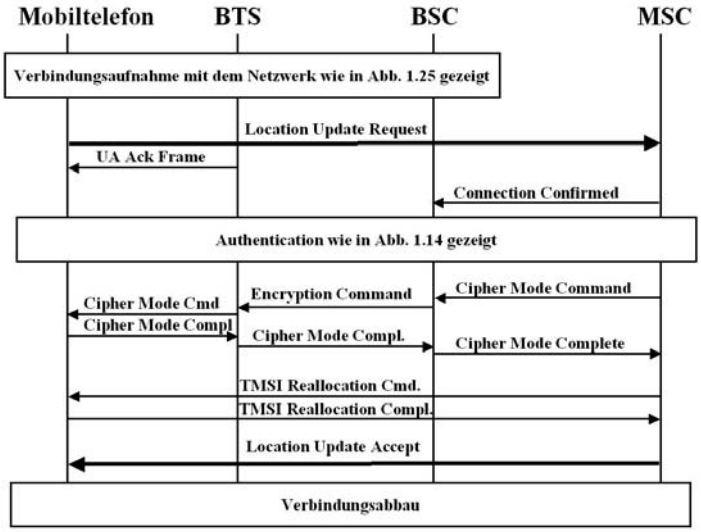

Abb. 1.40: Location Update

Nachdem die Verbindung so gegen Abhörversuche gesichert ist, wird dem Endgerät eine neue Temporäre ID (TMSI) zugeteilt, die auf der Luftschnittstelle beim Verbindungsaufbau und Paging statt der IMSI verwendet wird. Da eine ständig wechselnde TMSI den Teilnehmer beim nächsten Verbindungsaufbau identifiziert ist sichergestellt, dass die Identität des Teilnehmers auch während des nicht verschlüsselten Teils der Kommunikation geschützt ist. Nachdem auch diese Prozedur erfolgreich ausgeführt wurde, wird dem Endgerät der erfolgreiche Location Area Update bestätigt und die Verbindung beendet.

Inter MSC Location Update

Für den Fall, dass die alte und neue Location Area von zwei unterschiedlichen MSC/VLR verwaltet werden, sind noch weitere

Schritte notwendig. In diesem Fall muss das neue MSC/VLR das HLR über den Wechsel des Teilnehmers in die neue Area informieren. Das HLR löscht die Daten des Teilnehmers daraufhin im alten MSC/VLR. Dieser Vorgang wird Inter MSC Location Update genannt.

1.8.2 Mobile Terminated Call

Ein Anruf, der bei einem mobilen Teilnehmer eingeht, wird bei GSM als Mobile Terminated Call bezeichnet. Ein wesentlicher Unterschied zwischen Mobilfunknetz und Festnetz ist dabei, dass die Telefonnummer des Teilnehmers keinen Aufschluss mehr über den Aufenthaltsort des Gesprächspartners enthält. Im Mobilfunknetz muss deshalb über das Home Location Register der aktuelle Aufenthaltsort des Teilnehmers ermittelt werden, bevor das Gespräch weitervermittelt werden kann.

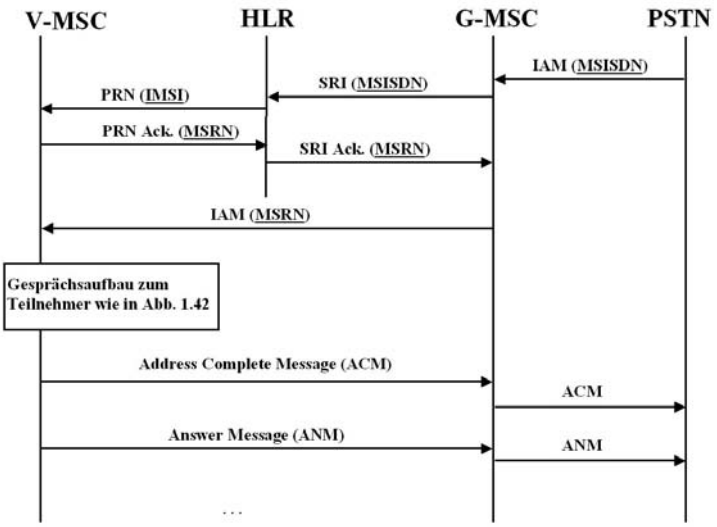

Abb. 1.41: Gesprächsaufbau zu einem mobilen Teilnehmer, Teil 1

SRI

Abbildung 1.41 zeigt den ersten Teil eines Mobile Terminated Calls, der in diesem Beispiel von einem Festnetzteilnehmer ausgelöst wird. Aus dem Festnetz bekommt dabei die Gateway-MSC (G-MSC) über die schon in Abbildung 1.6 gezeigte ISUP Signalisierung und die IAM Nachricht die Telefonnummer (MSISDN) des Gesprächspartners übermittelt. Eine G-MSC wie in diesem Beispiel gezeigt ist eine normale MSC mit zusätzlichen Verbin-

dungen in andere Netze. Die G-MSC sendet nach Erhalt der IAM Nachricht eine Send Routing Information (SRI) Nachricht an das Home Location Register (HLR), um die aktuelle MSC des Teilnehmers zu ermitteln. Die aktuelle MSC des Teilnehmers wird auch Visited MSC (V-MSC) genannt.

MSRN

Das HLR ermittelt anhand der übergebenen MSISDN die IMSI des Teilnehmers und findet somit auch seine aktuelle V-MSC und deren VLR. Daraufhin sendet das HLR eine Provide Roaming Number Nachricht an das V-MSC/VLR, um diese über den ankommenden Anruf zu informieren. Im V-MSC/VLR wird die übergebene IMSI einer temporären Mobile Station Roaming Number (MSRN) zugeordnet, die dann an das HLR zurückgegeben wird. Das HLR gibt die MSRN schließlich transparent an die G-MSC zurück.

IAM mit MSRN

Die G-MSC verwendet die so erhaltene MSRN für die Weitervermittlung des Gesprächs an die V-MSC. Dies ist möglich, da die MSRN nicht nur temporär den Teilnehmer in der V-MSC/VLR identifiziert, sondern auch so aufgebaut ist, dass die V-MSC eindeutig identifiziert werden kann. Zwischen G-MSC und V-MSC wird dazu wiederum die ISUP Signalisierung verwendet. Statt der ursprünglichen MSISDN des Teilnehmers enthält diese IAM Nachricht jedoch die MSRN. Die MSISDN kann hier nicht mehr verwendet werden, da zwischen G-MSC und V-MSC durchaus noch mehrere weitere Vermittlungsstellen geschaltet sein können.

International Call Routing

Da die MSRN nicht nur im nationalen Netz, sondern auch International eindeutig ist, kann über dieses Verfahren auch ein Teilnehmer erreicht werden, der sich gerade im Ausland aufhält. Für das Netzwerk macht es also keinen Unterschied, ob sich ein Teilnehmer im eigenen Netzwerk oder im Ausland befindet. Da die MSRN für die spätere Abrechnung im Billing Record gespeichert wird ist es auch möglich, dem Teilnehmer eine Gebühr für die Weitervermittlung ins Ausland in Rechnung zu stellen und einen Teil dieser Gebühr an den ausländischen Netzbetreiber zu überweisen.

Paging des Teilnehmers

In der V-MSC/VLR wird die MSRN dann verwendet, um die IMSI des Teilnehmers und seine Daten im VLR zu finden. Dies ist möglich, da bei der Zuteilung der MSRN bei der Anfrage des HLR diese Beziehung gespeichert wurde. Nachdem die Teilnehmerdaten im VLR gefunden wurde, wird nun der Teilnehmer von der MSC in der Location Area im Radionetzwerk gesucht, die in seinem VLR Eintrag gespeichert ist. Dieser Vorgang wird Paging

genannt und ist in Abbildung 1.42 dargestellt. Dazu schickt die V-MSC eine Paging Nachricht an die entsprechende BSC. Die BSC wiederum schickt daraufhin in jede Zelle der betreffenden Location Area eine Paging Nachricht, die dann auf dem Paging Channel (PCH) ausgestrahlt wird. Meldet sich der Teilnehmer nicht innerhalb weniger Sekunden, wird die Paging Nachricht wiederholt.

Aufbau der Signalisierungsverbindung

Nachdem sich das Endgerät beim Netzwerk gemeldet hat, finden wie beim Location Update wieder eine Authentifizierung und Aktivierung der Verschlüsselung statt. Erst danach wird das Endgerät über den eingehenden Anruf über eine Setup Nachricht informiert. Teil dieser Nachricht ist z.B. die Telefonnummer des Anrufers falls dieses Dienstmerkmal aktiviert ist (CLIP) und nicht von der Anruferseite unterdrückt wird (CLIR).

Aufbau der Sprachverbindung.

Bestätigt das Endgerät den eingehenden Anruf mit einer Call Confirmed Nachricht, beantragt die MSC bei der BSC den Aufbau eines Sprachkanals (TCH).

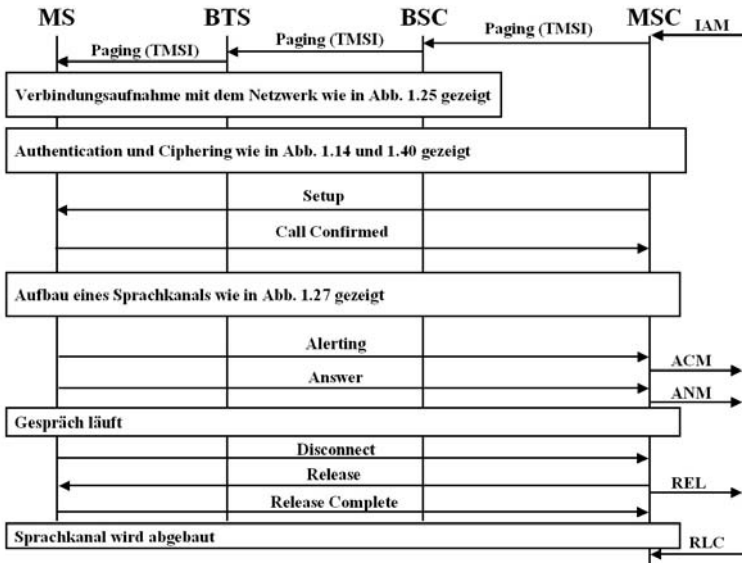

Abb. 1.42: Gesprächsaufbau zu einem mobilen Teilnehmer, Teil 2

Nach erfolgreichem Aufbau des Sprachkanals schickt das Endgerät eine Alerting Nachricht zur MSC und teilt ihr dadurch mit, dass der Teilnehmer über den eingehenden Anruf informiert wird (das Telefon „klingelt“). Die V-MSC ihrerseits gibt diese

Information über die Address Complete Nachricht (ACM) an die G-MSC weiter. Auch diese gibt die Information über eine ACM Nachricht an das Festnetz weiter.

Nimmt der mobile Teilnehmer das Gespräch an, schickt das Endgerät eine Answer Nachricht zur V-MSC. Diese leitet die Information dann über eine Answer Nachricht (ANM) zur G-MSC weiter. Von dort aus wird dann das Festnetz wiederum durch eine ISUP ANM darüber informiert, dass das Gespräch durchgeschaltet wurde.

Signalisierung während der Verbindung

Auch während der eigentlichen Sprachverbindung werden ständig Signalisierungsnachrichten ausgetauscht. Am häufigsten werden zweifellos Nachrichten mit Messergebnissen zwischen Endgerät, BTS und BSC ausgetauscht. Wenn nötig, kann die BSC während der bestehenden Verbindung ein Handover zu einer anderen Zelle veranlassen. Mehr dazu in Kapitel 1.8.3.

Beenden der Verbindung

Beendet einer der beiden Teilnehmer das Gespräch, schickt die jeweilige Seite eine Disconnect Nachricht. Nach Abbau des Sprachkanals zum Endgerät und dem Senden einer ISUP Release Complete Nachricht ist die Verbindung dann komplett beendet.

Teilnehmer befindet sich bei der Gateway MSC

In diesem Beispiel wurde davon ausgegangen, dass sich der mobile Teilnehmer nicht im Bereich der G-MSC aufhält. Dies kann aber durchaus vorkommen, wenn z.B. ein Gespräch von einem Festnetzteilnehmer zu einem Mobilfunkteilnehmer aufgebaut wird, der sich in der gleichen Region befindet. Da Festnetzvermittlungsstellen das Gespräch aus Kostengründen meist an die nächstgelegene Mobilfunkvermittlungsstelle weitergeben, kann somit die G-MSC auch gleichzeitig die V-MSC sein. Dies erkennt die G-MSC nach Erhalt der MSRN in der SRI Acknowledge Nachricht. In diesem Fall wird das Gespräch dann gleich intern behandelt, und die ISUP Signalisierung (IAM, ACM, ANM…) entfällt.

1.8.3 Handoverszenarien

Verschlechtert sich der Empfang während einer Verbindung z.B. aufgrund einer Positionsänderung des Teilnehmers zusehends, leitet die BSC einen Handover ein. Das grundsätzliche Verfahren und die dazu notwendigen Nachrichten wurden bereits in Abbildung 1.28 dargestellt. Im Netzwerk werden folgende Handoverfälle unterschieden:

Intra BSC Handover

Beim Intra BSC Handover sind die aktuelle Zelle und die neue Zelle an der gleichen BSC angeschlossen. Diese Situation ist in Abbildung 1.28 dargestellt.

Inter BSC Handover

Bei einem Wechsel in eine Zelle einer anderen BSC kann der Handover nicht durch die aktuelle BSC gesteuert werden, da keine direkte Signalisierungsverbindung zwischen den BSCs existiert. Deshalb beantragt die aktuelle BSC den Handover in die neue Zelle bei ihrer MSC über eine Handover Request Nachricht. Teil dieser Nachricht ist die Cell-ID und der Location Area Code (LAC) der neuen Zelle. Da die MSC eine Liste aller LACs und Cell-IDs seiner Zellen hat, kann sie die dazugehörige BSC ermitteln, dort einen Sprachkanal in der gewünschten Zelle aufbauen und die BSC sowie die neue Zelle auf den Handover vorbereiten. Nachdem der Sprachkanal vorbereitet wurde, schickt die MSC ein Handover Kommando zum Endgerät über die noch existierende alte Verbindung. Das Endgerät wechselt daraufhin in die neue Zelle. Erkennt die neue BTS und BSC den erfolgreichen Handover, wird dies der MSC mitgeteilt und die MSC kann den Sprachkanal auf die neue Verbindung umschalten. Danach wird der Sprachkanal in der alten BTS und BSC abgebaut, der Handover ist beendet.

Inter MSC Handover

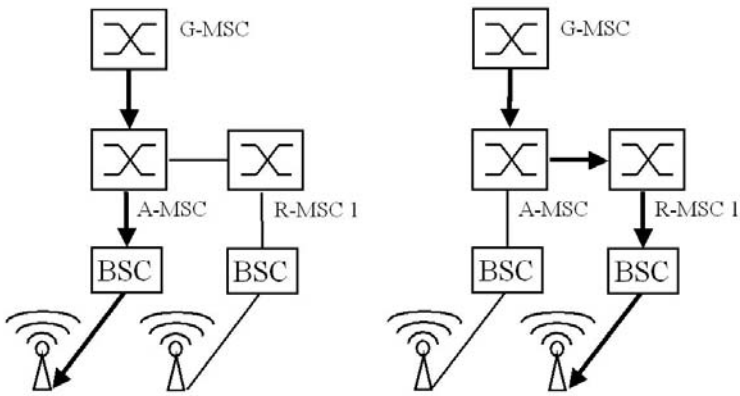

Abb. 1.43: Inter-MSC Handover

Noch aufwändiger wird es, wenn sich die neue Zelle nicht im Bereich der aktuellen MSC befindet. Aufgrund der Handover Request Nachricht des aktuellen Base Station Controllers erkennt die MSC, dass sich die Location Area der neuen Zelle nicht in ihrem Versorgungsgebiet befindet. Über eine weitere Datenbank

der MSC, die alle Location Areas der benachbarten MSCs enthält, kann die für diese Zelle verantwortliche MSC gefunden werden. Die aktuelle MSC wird in diesem Szenario auch als Anchor MSC (A-MSC) bezeichnet, die für die neue Zelle zuständige MSC wird Relay MSC (R-MSC) genannt.

Um den Handover durchzuführen, schickt die Anchor MSC der ermittelten Relay MSC eine Handover Nachricht über das MAP Protokoll. Die Relay MSC baut daraufhin in der gewünschten Zelle einen Sprachkanal für den Handover auf und meldet dies der Anchor MSC. Die Anchor MSC leitet daraufhin den Handover durch Senden einer Handover Command Nachricht an das Endgerät ein.

Nach erfolgreichem Handover in die neue Zelle meldet die Relay MSC der Anchor MSC den erfolgreichen Handover. Diese kann daraufhin den Sprachkanal zur Relay MSC durchstellen. Danach wird der Sprachkanal zur alten Zelle abgebaut.

Subsequent Inter MSC Handover

Wechselt ein Teilnehmer nach einem Inter-MSC Handover in eine Zelle, die von einem dritten MSC verwaltet wird, spricht man von einem Subsequent Inter MSC Handover.

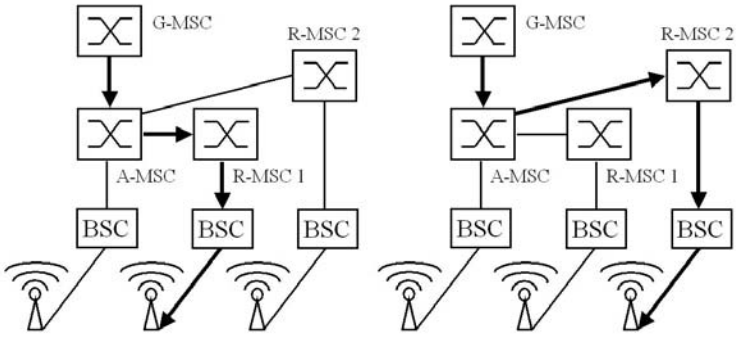

Abb. 1.44: Subsequent Inter-MSC Handover

Für diesen Fall meldet die aktuelle Relay MSC (R-MSC 1) der Anchor MSC, dass ein Subsequent Inter MSC Handover zu einer anderen Relay MSC (R-MSC 2) notwenig ist. Die Anchor MSC beauftragt dann R-MSC 2 mit dem Aufbau der nötigen Ressourcen. Nachdem die neue Zelle vorbereitet wurde, schickt die Anchor MSC über R-MSC 1 den Handover Befehl an das Endgerät. Dieses wechselt in die Zelle von R-MSC 2 und meldet den erfolgreichen Handover der Anchor MSC über die neue Verbindung.

Diese kann dann R-MSC 1 anweisen, den nicht mehr benötigten Sprachkanal abzubauen. Auf diese Weise wird erreicht, dass es keine weitere Verkettung von MSCs gibt. An einem Gespräch sind somit immer nur die ursprüngliche Gateway MSC, die Anchor MSC und maximal eine Relay MSC beteiligt. Die Gateway und Anchor MSCs bleiben damit während des ganzen Gespräches unter Umständen die einzigen festen Komponenten.

Subsequent Handback

Und schließlich gibt es auch noch den Fall, dass der Teilnehmer aus dem Gebiet der Relay MSC wieder in das Gebiet der Anchor MSC zurückkehrt. Nach einem solchen Handover ist die Anchor MSC neben der Gateway MSC wieder die einzige an der Verbindung beteiligte MSC. Da die Relay MSC das Gespräch wieder an die Anchor MSC zurückgibt, wird in diesem Fall von einem Subsequent Handback gesprochen.

Handover aus Endgerätesicht

Aus Sicht des Endgeräts unterscheiden sich die vorgestellten Handovervarianten nicht, da die Handover Nachricht für alle Fälle identisch ist.

Um einen Handover jedoch so schnell wie möglich durchzuführen, gibt es in GSM die Möglichkeit, Synchronisationsinformationen zwischen aktueller und neuer Zelle in der Handover Nachricht zu übermitteln. Dies ermöglicht der Mobilstation, sofort auf den ihr zugeteilten Timeslot in der neuen Zelle zuzugreifen, statt sich zuerst auf die neue Zelle zu synchronisieren. Dazu müssen jedoch die aktuelle und neue Zelle synchronisiert sein, was z.B. bei einem Inter-MSC Handover nicht möglich ist, da die zwei Zellen von unterschiedlichen MSCs und BSCs verwaltet werden. Da aber auch zwei Zellen die mit der gleichen BSC verbunden sind nicht unbedingt synchronisiert sein müssen, kann das Endgerät auch daran nicht erkennen, um welche Art Handover es sich im Netzwerk handelt.

1.9 Die Mobile Station

Durch die fortschreitende Miniaturisierung war es Mitte der 80'er Jahre erstmals möglich, alle für ein Mobiltelefon nötigen Bauteile in einem tragbaren Gerät unterzubringen. Wenige Jahre später konnte man Mobiltelefone dann soweit verkleinern, dass der limitierende Faktor für die Größe eines Mobiltelefons nicht mehr unbedingt die Größe der elektronischen Bauteile ist. Vielmehr wird die Größe eines Endgeräts heute hauptsächlich durch die notwendige Größe der Bedienteile wie Tastatur und Display bestimmt. Durch die ständige Weiterentwicklung und Miniaturisierung der elektronischen Bauteile ist es jedoch möglich, immer

mehr Funktionalitäten und Bedienkomfort in ein Mobiltelefon zu integrieren. Wurden Mobiltelefone anfangs hauptsächlich zum telefonieren verwendet, geht der Trend heute zu „Geräten mit eingebautem Mobiltelefon“ für unterschiedliche Nutzergruppen:

- PDA mit Mobiltelefon für Sprach- und Datenkommunikation.
- Spielekonsolen mit integriertem Mobiltelefon für Sprach- und Datenkommunikation (z.B. Multiuserspiele mit Echtzeitdatenaustausch per Internet und Mobilfunk).
- Mobiltelefone für Sprachkommunikation mit Bluetooth Kurzstreckenfunk für die Internetanbindung von anderen tragbaren Geräten wie PDAs oder Notebooks.

Grundsätzliche Architektur

Unabhängig ihrer Größe und enthaltenem Funktionsumfang haben jedoch alle Mobiltelefone eine ähnliche Grundarchitektur, die in Abbildung 1.45 dargestellt ist.

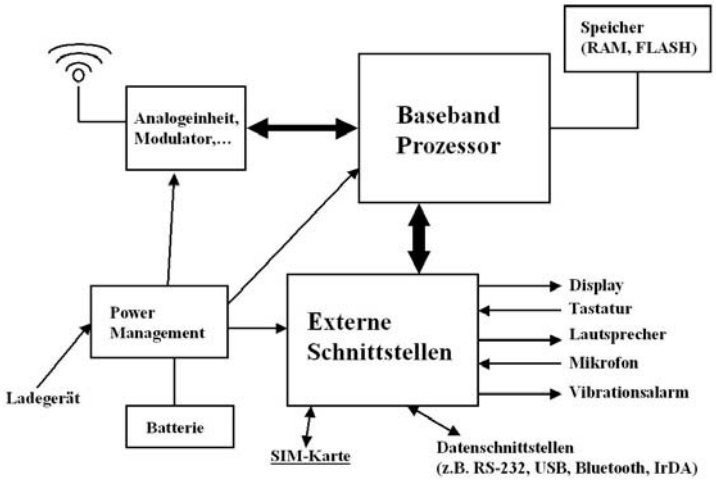

Abb. 1.45: Grundsätzlicher Aufbau eines Mobiltelefons

Kern jedes Mobiltelefons ist der Baseband Prozessor, der eine RISC CPU und einen Digitalen Signalprozessor (DSP) enthält.

RISC Einheit

Der RISC Prozessor kümmert sich dabei um:

- Die Verarbeitung der Informationen, die auf den Signalisierungskanälen (BCCH, PCH, AGCH, PCH, etc.) empfangen werden.

- Die Gesprächssignalisierung (DTAP)
- GPRS Management und GPRS Daten
- Teile der Datenübertragungskette: Kanalkodierer, Interleaver, Cipherer (evtl. eigene Hardwareeinheit)
- Mobility Management (Netzwerksuche, Cell Reselection, Location Update, Handover, Timing Advance, etc.)
- Kommunikation mit externen Schnittstellen wie Bluetooth, RS-232, IrDA, USB
- Userinterface (Tastatur, Display, Bedienungssoftware)

Multitasking Betriebssystem

Da viele dieser Aufgaben gleichzeitig zu bearbeiten sind, kommt auf dem RISC Prozessor ein echtzeitfähiges Embedded Multitasking Betriebssystem zum Einsatz. Die Echtzeitfähigkeit ist notwendig, da der Prozessor zur richtigen Zeit Daten für die Übertragung über die GSM Rahmenstruktur zur Verfügung stellen und auch empfangen muss. Die restliche Peripherie wie Tastatur oder Display sowie die Usersoftware hat dagegen eine niedrigere Priorität. Dies kann bei vielen Mobiltelefonen während einer GPRS Datenübertragung beobachtet werden. Hier ist die RISC CPU nicht nur für die Signalisierung, sondern auch für die Weiterleitung der Daten zwischen externem Gerät (z.B. Notebook) und dem Netzwerk verantwortlich. Bei einer hohen Übertragungsgeschwindigkeit reagiert das Mobiltelefon dann auf Benutzereingaben über die Tastatur nur recht zögerlich.

Prozessorleistung und Speicher

Die Rechenleistung des RISC Prozessors beeinflusst heute im wesentlichen, welche Applikationen auf dem Mobiltelefon implementiert werden können. So wird z.B. für die Aufzeichnung und Wiedergabe von digitalen Bildern oder Videofilmen eine hohe Rechenleistung benötigt. Eine RISC Architektur, die in GSM und auch UMTS Telefonen verwendet wird, ist z.B. die ARM-7 Architektur, die mit einer Prozessorgeschwindigkeit von 50 MHz und mehr betrieben werden kann. Kehrseite schnellerer Prozessoren ist jedoch der steigende Leistungsverbrauch, der sich ein Wettrennen mit steigenden Batteriekapazitäten und ausgeklügelten Power Management Funktionen liefert.

Digitaler Signalprozessor

Der Digitale Signalprozessor (DSP) ist ein weiterer wichtiger Bestandteil eines GSM und UMTS Chipsatzes. Seine Hauptaufgabe ist die Sprachdatenkomprimierung mit den unterschiedlichen Sprachcodecs wie FR, EFR, HR oder AMR. Daneben wird er in Empfangsrichtung eingesetzt, um das empfangene Signal, das

bereits digitalisiert wurde vor der Dekodierung zu bearbeiten. Dazu verwendet der DSP die Trainingssequenz eines Bursts, die in Kapitel 1.7.3 vorgestellt wurde. Da dem DSP die Bits der Trainingssequenz bekannt sind, kann dieser einen Filter berechnen, der auf den restlichen Burst angewandt wird, um die darin enthaltenen Daten zu rekonstruieren. Als DSP Einheit wird zum Beispiel ein DSP 56600 mit 104 MHz Prozessortakt verwendet.

Abbildung 1.46 zeigt, welche Aufgaben der RISC Prozessor und der DSP in einem Endgerät übernehmen. Vergleicht man die Bearbeitungskette des Sprachsignals im Mobiltelefon mit der im Netzwerk, stellt man fest, dass die Aufgabe der TRAU zum größten Teil vom DSP und den analogen Bauelementen im Endgerät übernommen werden. Alle anderen Bearbeitungsschritte wie die Kanalkodierung etc., die im Netzwerk von der BTS durchgeführt werden, finden ihr Gegenstück in der RISC CPU des Endgeräts.

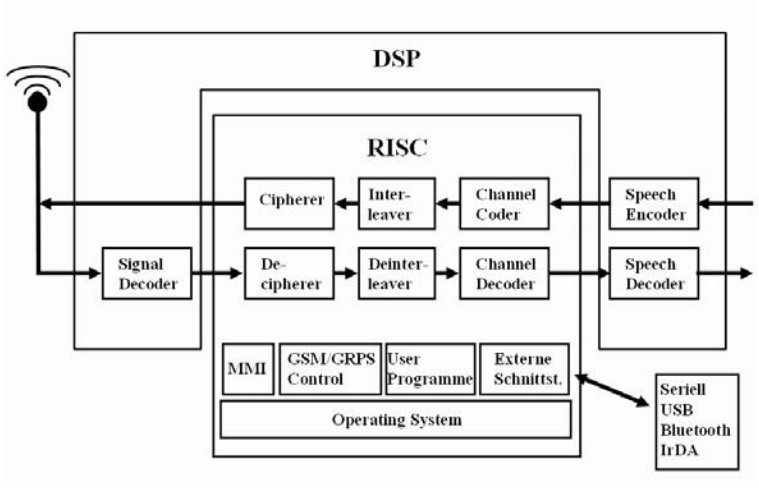

Abb. 1.46: RISC und DSP Funktionen im Überblick

Chipsatzhersteller

Da pro Jahr viele Millionen Endgeräte verkauft werden, ist auch das Angebot an Chipsätzen sehr groß. Dabei muss der Chipsatzhersteller nicht unbedingt der Hersteller des Mobiltelefons sein. Während Motorola eigene Chipsätze produziert, verwendet z.B Nokia unter anderem Chipsätze von STMicroelectronics und Texas Instruments. Weitere GSM Chipsatzhersteller sind auch Infineon, Analog Devices, Philipps und zahlreiche Firmen aus dem fernen Osten.

Software

Auch ein Teil der Anwendungssoftware eines Endgeräts kommt häufig nicht aus der Hand des Mobiltelefonherstellers. So verwendet z.B. Siemens den WAP Browser von OpenWave für seine Endgeräte, der auch in Endgeräten anderer Hersteller verwendet wird. Dies macht deutlich, dass an der Entwicklung der Hardware und Software eines Endgeräts nicht nur der aufgedruckte Hersteller, sondern noch eine Vielzahl anderer Firmen beteiligt sind.

Erfreulicherweise ist auch zu beobachten, dass in immer mehr Mobiltelefonen auch eine großteils geräteunabhängige Java Virtual Machine zum Einsatz kommt. Dies fördert besonders die Entwicklung von Programmen, die mit nur wenig oder keinem Aufwand auf eine große Zahl unterschiedlicher Mobiltelefone angepasst werden können.

1.10 Die SIM Karte

Trotz ihrer geringen Größe ist auch die SIM Karte ein wichtiger Bestandteil des GSM Netzwerkes. Da sie alle Daten eines Teilnehmers enthält, kann der Teilnehmer mit seiner SIM Karte jedes beliebige GSM Endgerät verwenden. Ausnahmen sind Endgeräte mit SIM Sperre, die nur mit einer einzigen SIM-Karte funktionieren. Dies ist aber keine GSM Einschränkung, sondern wurde von den Mobilfunkbetreibern eingeführt, um ein subventioniertes Endgerät nur mit der eigenen SIM Karte zu betreiben.

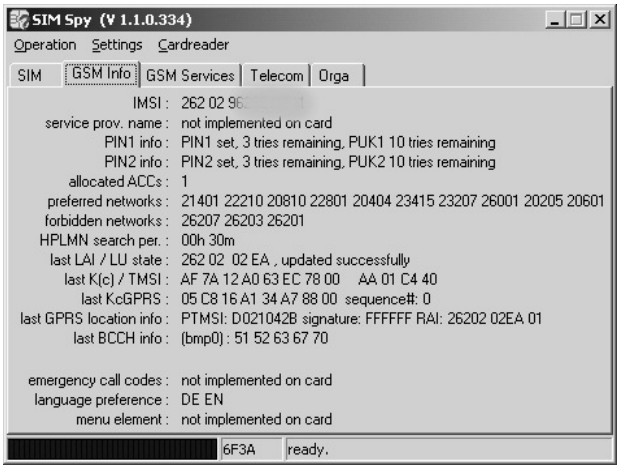

Abb. 1.47: Beispiel eines Tools zum Auslesen der Daten auf der SIM-Karte

Die wichtigsten Informationen auf der SIM Karte sind unter anderem die International Mobile Subscriber Identity (IMSI) des Teilnehmers, sowie dessen geheimer Schlüssel (Ki), der für die Authentifizierung und Generierung des Verschlüsselungskeys Kc benötigt wird.

Mit diversen im Internet kostenlos erhältlichen Tools können alle nicht lesegeschützten Informationen ausgelesen werden. Abbildung 1.47 zeigt ein solches Tool. Sensitive Informationen, wie z.B. der geheime Schlüssel Ki können jedoch auch mit diesen Tools nicht ausgelesen werden.

SIM Mikrokontroller

Erstaunlicherweise ist eine SIM Karte jedoch weit mehr als nur eine einfache Speicherkarte, denn sie enthält ein komplettes Mikrokontrollersystem, dessen Basisdaten in der folgenden Tabelle gezeigt werden:

CPU	8 oder 16 Bit CPU
Größe des ROM	40-100 kByte
Größe des RAM	1-3 kByte
EEPROM Größe	16-64 kByte
Taktfrequenz	10 MHz, wird aus Mobiltelefontakt generiert.
Betriebsspannung	3V oder 5V

Wie in Abbildung 1.48 gezeigt wird, kann von extern nur über die CPU auf die nichtflüchtigen Daten im EEPROM zugegriffen werden. Somit ist sichergestellt, dass von außerhalb kein direkter Zugriff auf die Daten erfolgen kann und somit sensitive Daten geschützt sind. Weiterhin wird der SIM Prozessor verwendet, um die Signed Response (SRES) aus der Zufallszahl (RAND) zu generieren, die bei der Authentifizierung (vgl. Kapitel 1.6.4) an das Mobiltelefon übermittelt wird. Die Berechnung von SRES muss zwingend in der SIM Karte und nicht im Mobiltelefon durchgeführt werden, da sonst der geheime Schlüssel Ki an das Endgerät übergeben werden müsste. Könnte das Endgerät jedoch Ki auslesen, wäre dies auch mit anderen Geräten oder der in Abbildung 1.47 gezeigten Software möglich und wäre somit ein großes Sicherheitsrisiko.

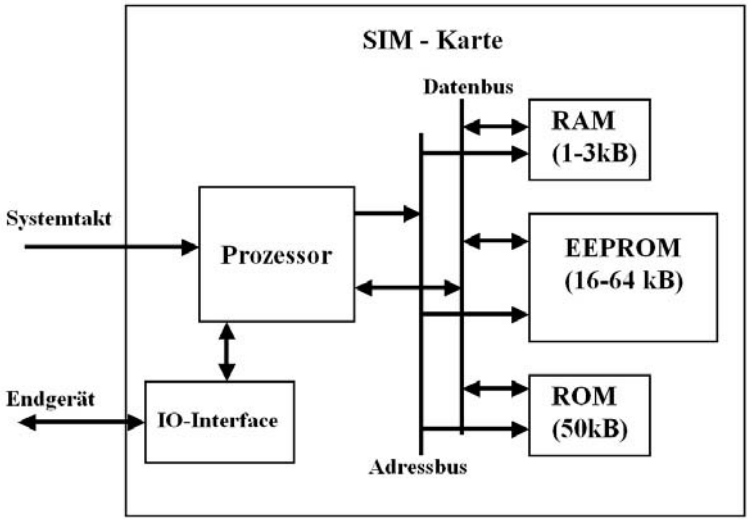

Abb. 1.48: Blockschaltbild der Komponenten einer SIM Karte

Das SIM Application Toolkit

Außerdem kann der Microcontroller auf der SIM Karte auch Programme ausführen, die vom Netzwerkbetreiber in die SIM Karte übertragen wurden. Über die SIM Application Toolkit Schnittstelle, die in der ETSI Spezifikation 11.14 standardisiert ist, können diese Programme auch auf diverse Funktionen des Mobiltelefons zugreifen und z.B. auf Benutzereingaben reagieren oder Texte oder Menüs auf dem Display darstellen.

T-Mobile in Deutschland nutzt das SIM Application Toolkit beispielsweise, um ein T-Mobile spezifisches Menü in die Menüstruktur des Mobiltelefons einzublenden. In diesem Menü kann dann unter anderem ein aktueller Nachrichtenüberblick angefordert werden. Navigiert der Benutzer durch dieses Menü, werden alle Tastatureingaben des Benutzers dem Programm auf der SIM Karte übergeben. Dieses generiert dann mit den erhaltenen Informationen des Benutzers eine SMS zum Anfordern der gewünschten Nachrichten und sendet diese automatisch an das Netzwerk.

Eine weit komplexere Applikation für das SIM Application Toolkit hat sich O2-Deutschland mit ihrem Genion Service ausgedacht. Hat man diesen Dienst abonniert, kann man in einem bestimmten Bereich zum Beispiel rund um seinen Wohnort billiger telefonieren. Die SIM Karte enthält dabei Informationen über Größe und geographische Position dieser verbilligten Nutzungs-

zone. Um den Benutzer zu informieren, ob er sich dort aufhält, werden der SIM Karte vom Mobiltelefon laufend Informationen über die Position der aktuellen Zelle übergeben, die diese auf einem Broadcast Kanal periodisch aussendet. Das Programm auf der SIM Karte vergleicht diese Daten dann mit der geographischen Position und Größe der ‚billigeren' Zone des Benutzers. Befindet sich der Benutzer innerhalb der Zone, weisst das SIM Programm das Endgerät an, den Text „home" oder „city" auf dem Display darzustellen.

Datenspeicher auf der SIM Karte

Die Daten auf einer GSM SIM Karte werden aus logischer Sicht ähnlich wie bei einer Festplatte in Verzeichnissen und Dateien verwaltet. Die Datei- und Verzeichnisstruktur ist dabei fest vorgegeben und im ETSI Standard 11.11 spezifiziert. Das Hauptverzeichnis (Root Directory) wird darin unglücklicherweise Main File (MF) genannt, ein Unterverzeichnis wird als Dedicated File (DF) bezeichnet und eine normale Datei wird Elementary File (EF) genannt. Da auf der SIM Karte nur wenig Speicherplatz zur Verfügung seht, haben die einzelnen Dateien und Verzeichnisse keine Datei- und Verzeichnisnamen, sondern nur 4-stellige Hex Nummern mit einer Länge von 2 Bytes. Diesen wurden in der Spezifikation dann Namen gegeben, die jedoch nicht auf der SIM Karte gespeichert sind. So wurde zum Beispiel dem Root Directory die ID 0x3F00 gegeben, dem GSM Unterverzeichnis die ID 0x7F20 und der Datei, die die IMSI enthält, die ID 0x6F07. Um die IMSI auszulesen, muss das Endgerät somit auf folgenden Pfad zugreifen: \\0x3F00\0x7F20\0x6F07.

SIM Dateiformate

Um den Umgang mit Daten auf der SIM Karte für das Endgerät so einfach wie möglich zu halten, kann jede Datei auf der SIM Karte eine der folgenden drei Dateiformate haben:

- Transparent: Die Datei enthält nur eine Sequenz aus Bytes. Die Datei für die IMSI verwendet zum Beispiel dieses Format. Wie das Endgerät den Inhalt dieser Datei zu interpretieren hat, um die IMSI zu erhalten, ist wiederum im ETSI Standard 11.11 festgelegt.
- Linear Fixed: Diese Datei enthält Einträge (Records), die eine feste Länge besitzen. Dieses Format wird zum Beispiel für das Telefonbuch der SIM Karte verwendet. Jeder Telefonbucheintrag ist dabei in einem Record der Telefonbuchdatei abgelegt.

- Cyclic: Ähnlich wie Linear Fixed, das Format enthält jedoch einen Zeiger auf den zuletzt geschriebenen Record. Ist das Ende der Datei erreicht wird der Zeiger automatisch wieder auf den ersten Record gesetzt. Dieses Format wird z.B. für die Datei verwendet, die die zuletzt angerufenen Telefonnummern enthält.

Zugriffsrechte

Um Dateien zu schützen, ist jede Datei mit Zugriffsrechten ausgestattet. Dabei kann individuell kontrolliert werden, ob eine Datei gelesen oder geschrieben werden darf. Grundsätzlich ist der Zugriff auf die Dateien der SIM Karte nur möglich, wenn sich der Teilnehmer zuvor per PIN authentifiziert hat. SIM Karten mancher Netzbetreiber bieten jedoch die Möglichkeit, diesen Schutz zu deaktivieren, damit die PIN beim Einschalten des Endgeräts nicht eingegeben werden muss.

Nach Übergabe der PIN an die SIM Karte kann dann das Lesen und Schreiben einzelner Dateien freigegeben oder gesperrt sein. So ist zum Beispiel trotz korrekter PIN das Lesen oder gar Schreiben der Datei für den geheimen Schlüssel Ki nicht möglich.

Kommunikation mit der SIM Karte

Neben der Dateistruktur der SIM Karte legt die ETSI Spezifikation 11.11 auch fest, wie mit der SIM Karte kommuniziert wird. Auf Layer 2 wurden dazu Kommando- und Antwortnachrichten spezifiziert, die ganz allgemein als Application Protocol Data Units (APDU) bezeichnet werden. Sollen Daten zwischen einem Endgerät und einer SIM Karte ausgetauscht werden, sendet das Endgerät eine Command APDU an die SIM Karte. Diese muss darauf mit einer Response APDU antworten. Die SIM Karte nimmt bei dieser Kommunikation eine passive Rolle ein, da sie nur Response APDUs schicken kann.

Daten von der SIM lesen

Sollen Daten gelesen werden, enthalten die Command APDUs unter anderem die Datei ID sowie die Anzahl der zu lesenden Bytes oder die Nummer des gewünschten Records. In Response APDUs werden dann die gewünschten Daten zurückgegeben.

Daten auf die SIM schreiben

Sollen Daten auf die SIM Karte geschrieben werden, enthalten die Command APDUs neben der Datei ID die zu schreibenden Daten. In den Response APDUs befinden sich dann Statusmeldungen, ob der Schreibvorgang erfolgreich war.

Command APDU

Abbildung 1.49 zeigt das Format einer Command APDU. Das erste Feld ist dabei die Class of Instruction und enthält bei GSM immer den Wert 0xA0. Das Instruction Feld enthält die ID des Befehls, der von der SIM Karte ausgeführt werden soll.

Abb. 1.49: Command APDU

Die nachfolgende Tabelle zeigt einige Befehle und deren IDs. Die Felder P1 und P2 dienen zur Übergabe von Parametern für den gewählten Befehl. P3 gibt die Länge des nachfolgenden Datenfeldes an, das z.B. bei einem Schreibbefehl die zu schreibenden Daten enthält.

Befehl	**ID**	**P1**	**P2**	**Länge**
SELECT (Datei öffnen)	A4	00	00	02
READ BINARY (Datei lesen)	B0	Offset High	Offset Low	Länge
UPDATE BINARY (Datei schreiben)	D6	Offset High	Offset Low	Länge
VERIFY CHV (PIN Eingabe)	20	00	ID	08
CHANGE CHV (PIN ändern)	24	00	ID	10
RUN GSM ALGORITHM (RAND, SRES, Kc…)	88	00	00	10

Response APDU

Das Format einer Response PDU ist in Abbildung 1.50 dargestellt. Neben einem Datenfeld enthält die Response APDU auch die Felder SW1 und SW2. Diese werden von der SIM Karte verwendet, um dem Endgerät mitzuteilen, ob der zuvor gesendete Befehl korrekt ausgeführt werden konnte.

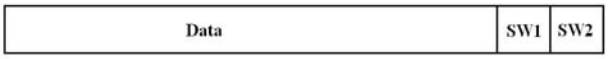

Abb. 1.50: Response APDU

Beispiel

Um eine Datei für das Lesen oder Schreiben von Daten zu öffnen, sendet das Endgerät ein SELECT Kommando an die SIM Karte. Die SELECT APDU hat dabei den wie in Abbildung 1.51 dargestellten Inhalt.

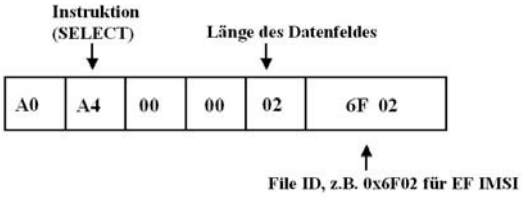

Abb 1.51: Select Command

Als Antwort bekommt das Endgerät von der SIM Karte eine Response APDU, die unter anderem folgende Datenfelder enthält:

Byte	Description	Länge
3-4	**File Size**	2
5-6	**File ID**	2
7	**Type of File** **(Transparent, Linear Fixed, Cyclic)**	1
9-11	**Zugriffsberechtigungen**	3
12	**Dateistatus**	1

Für eine vollständige Auflistung der zurückgegebenen Informationen siehe ETSI 11.11.

Im nächsten Schritt kann dann z.B. mit einer READ BINARY oder WRITE BINARY APDU die Datei gelesen oder modifiziert werden.

Physikalisches Interface

Um mit der SIM Karte zu kommunizieren, hat diese auf ihrer Oberfläche 6 Kontaktstellen. Eine GSM SIM Karte verwendet davon jedoch nur 4 für folgende Zwecke:

- C1: Spannungsversorgung
- C2: Resetleitung
- C3: Takt (1-5 MHz)
- C7: Input/Output Leitung

Da nur eine Leitung für Ein- und Ausgabe von Command und Status APDUs verwendet wird, erfolgt die Übertragung der Kommandos seriell und nur abwechselnd im Halbduplexverfahren. Die Taktgeschwindigkeit für die Datenübertragung ist dabei mit C3 Takt / 372 definiert worden. Bei einem C3 Takt von 5 MHz beträgt somit die Übertragungsgeschwindigkeit 13 440 bit/s.

1.11 Das Intelligent Network Subsystem und CAMEL

Alle bisher in diesem Kapitel beschriebenen Komponenten sind zwingend für den Betrieb eines Mobilfunknetzwerkes notwendig. Mobilfunkbetreiber bieten jedoch über die grundsätzliche Kommunikation hinaus heute zusätzliche Dienste an, für die zusätzliche Logik und Datenbanken notwenig sind. Dazu zählen insbesondere:

- Location Based Services (LBS), die vor allem in Deutschland von der Mehrzahl der Netzbetreiber in diversen Varianten angeboten werden. Eine Variante von LBS ist beispielsweise, einen günstigeren Tarif zu Festnetzanschlüssen im Ortsnetz anzubieten, in dem sich ein Mobilfunkteilnehmer momentan aufhält. Für die Tarifberechnung prüft dabei ein LBS Dienst im Netzwerk, ob aktueller Standort des Teilnehmers und die gewählte Festnetznummer im gleichen geographischen Gebiet liegen. Wenn ja, fügt der Dienst dem Billing Record darüber eine Information hinzu und das Gespräch kann im Abrechnungssystem entsprechend abgerechnet werden.
- Prepaid Dienste: Diese erfreuen sich seit deren Einführung Mitte der 90er Jahre großer Beliebtheit. Statt einmal im Monat eine Rechnung zu erhalten, besitzt ein Prepaid Kunde ein Konto bei seinem Mobilfunkbetreiber, das er vorab aufladen kann. Für die aufgeladene Summe kann dann telefoniert werden. Während jedes Gespräches wird dabei der Kontostand laufend aktualisiert und nach dem Aufbrauchen des Verbindungsguthabens beendet. Weiterhin ist das Prepaid System auch mit dem SMSC und dem GPRS Netzwerk verbunden, und kann somit auch für die sofortige Abrechnung von Kurznachrichten und für die Abrechnung von GPRS Verbindungen verwendet werden.

Diese und viele andere Dienste können mit Hilfe des Intelligent Network (IN) Subsystem gelöst werden. Die Logik und die entsprechenden Datenbanken befinden sich dabei auf einem Servi-

ce Control Point (SCP), dessen grundsätzliche Funktionsweise schon in Kapitel 1.4 kurz vorgestellt wurde.

Proprietäre IN Protokolle

In den Anfangsjahren der GSM Entwicklung wurde für diese Dienste in Ermangelung eines Standards auf herstellerspezifische Entwicklungen gesetzt. Großer Nachteil dieser Lösungen war jedoch, dass sie nur zwischen Komponenten des gleichen Herstellers verwendet werden konnten. Dies bedeutet, dass die Dienste im Ausland nicht funktionierten, wenn die Komponenten dort von anderen Herstellern stammten. Dies war z.B. für den Prepaid Dienst sehr ärgerlich, da Prepaid Teilnehmer somit vom International Roaming ausgeschlossen waren.

CAMEL

Um die Interoperabilität zwischen Netzwerkkomponenten unterschiedlicher Hersteller und zwischen unterschiedlichen Mobilfunknetzen zu gewährleisten, wurde von ETSI/3GPP in TS 23.078 ein Protokoll und Verfahren spezifiziert, die den Namen CAMEL tragen. CAMEL steht dabei für ‚Customized Applications for Mobile network Enhanced Logic', ist aber in seinen Grundzügen deutlich einfacher, als sein Name suggeriert.

Während CAMEL auch Funktionalitäten für SMS und GPRS bietet, wird nachfolgend jedoch nur auf die grundsätzliche Funktionsweise für leitungsvermittelnde Verbindungen eingegangen.

CAMEL selbst ist keine Applikation oder Dienst, sondern die Grundlage, Dienste (Customized Applications) auf einem SCP zu entwickeln, die mit Netzwerkelementen anderer Hersteller national und international kompatibel sind. Diese Eigenschaft lässt sich z.B. mit dem HTTP Protokoll vergleichen. HTTP wird für die Übertragung von Web Seiten zwischen einem Web Server und einem Web Client verwendet. Dabei stellt HTTP sicher, dass jeder beliebige Web Server mit jedem beliebigen Web Client Daten austauschen kann. Ob es sich bei den Daten nun um Web Seiten oder Bilder handelt ist HTTP egal, denn die Interpretation ist Sache des Web Clients, bzw. Web Server.

CAMEL spezifiziert dazu im Wesentlichen das Protokoll zwischen den Netzwerkelementen wie MSC und SCP, sowie ein Zustandsmodell für einen Verbindungsablauf.

Zustandsmodell BCSM

Dieses Zustandsmodell wird bei CAMEL Basic Call State Model (BCSM) genannt. Ein Verbindungsablauf wird dabei in eine Anzahl Zustände unterteilt. Für den Anrufer (Originator BCSM) gibt es unter anderem folgende Zustände:

- Anrufaufbau
- Analyse der Zielrufnummer

- Routing der Verbindung
- Benachrichtigen des Ziels (Alerting)
- Gespräch läuft (Active)
- Beenden der Verbindung (Disconnect)
- Keine Antwort des Zielteilnehmers
- Zielteilnehmer besetzt

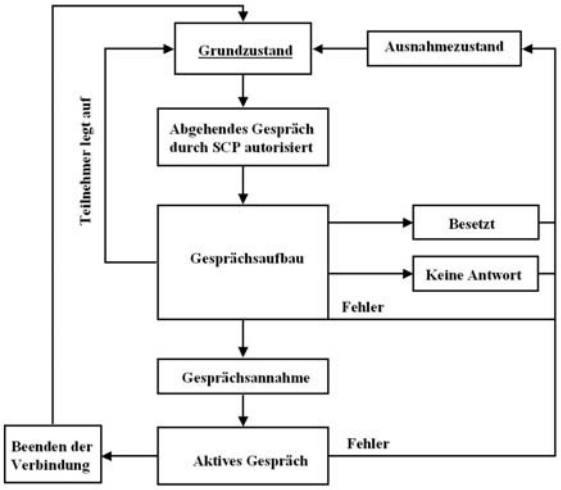

Abb. 1.52: Vereinfachtes Anrufer Zustandsmodell (O-BCSM) nach ETSI/3GPP TS 23.078

Auch für einen angerufenen Teilnehmer (Terminator) gibt es ein Zustandsmodell, das entsprechend T-BCSM genannt wird. Das T-BCSM wird z.B. für Prepaid Teilnehmer im Ausland benötigt, um die Weiterleitung des Gesprächs ins Ausland steuern und abrechnen zu können.

Detection Points

Beim Übergang zwischen den Zuständen definiert CAMEL Detection Points (DPs). Ist ein Detection Point für einen Teilnehmer aktiviert, wird der SCP über den Zustandsübergang informiert. Teil dieser Nachricht sind die IMSI des Anrufers, seine aktuelle Position (Cell ID), Zielrufnummer und vieles mehr. Ob ein DP für einen Teilnehmer aktiviert ist, wird im HLR für jeden Teilnehmer individuell eingetragen. Der SCP hat dann bei Empfang einer solchen Nachricht aufgrund der enthaltenen Daten die Möglichkeit, den weiteren Ablauf des Gesprächs zu beeinflussen. Der SCP hat zum Beispiel die Möglichkeit, das Gespräch zu be-

enden, die Zielrufnummer zu ändern oder Informationen an die MSC zurückzugeben, die in den Billing Record aufgenommen werden und somit später Einfluss auf die Gesprächsabrechnung haben.

Beispiel Prepaid

Für einen Prepaid Dienst kann das Zustandsmodel und das CAMEL Protokoll zwischen MSC und SCP wie folgt verwendet werden:

Ein Teilnehmer möchte ein Gespräch aufbauen. Die MSC stellt am Anfang des Gesprächsaufbaus fest, dass der Detection Point ‚Authorize Origination' in dessen HLR Eintrag gesetzt ist und sendet daraufhin eine Nachricht zum SCP. Anhand der darin enthaltenen IMSI und der gewünschten CAMEL Dienstnummer erkennt der SCP, dass es sich um einen Prepaid Teilnehmer handelt. Mit der übergebenen Zielrufnummer, der aktuellen Uhrzeit, etc., ermittelt der SCP dann den Minutenpreis für das Gespräch. Hat der Teilnehmer noch genug Guthaben auf seinem Konto, gestattet der SCP den Gesprächsaufbau und teilt der MSC mit, für wie viele Minuten diese Freigabe Gültigkeit hat. Die MSC verbindet daraufhin das Gespräch. Nach Ende des Gesprächs schickt die MSC erneut eine Nachricht zum SCP und teilt ihm die Dauer des Gesprächs mit. Der SCP aktualisiert daraufhin das Guthaben des Teilnehmers entsprechend.

Läuft die vom SCP übergebene Zeit während des Gesprächs ab, benachrichtigt die MSC wiederum den SCP. Dieser hat dann die Möglichkeit, der MSC eine weitere Zeitspanne für die Weiterführung des Gesprächs zu übergeben. Der SCP kann die MSC jedoch auch anweisen, das Gespräch zu beenden oder einen Ton oder eine Ansage einzuspielen. Im Prepaid Fall kann dieser Ton zum Beispiel ein Hinweis sein, dass das Guthaben fast erschöpft ist.

Beispiel Location Dependant Billing

Auch Location Based Services (LBS) können mit CAMEL realisiert werden. Hierfür ist wiederum im HLR Eintrag eines Teilnehmers der „Authorize Origination" Detection Point aktiviert. In diesem Fall stellt jedoch der SCP anhand der IMSI und der CAMEL Dienstnummer fest, dass es sich um einen Teilnehmer handelt, der einen LBS Dienst abonniert hat. Dieser Dienst auf dem SCP ermittelt dann anhand der aktuellen Zelle des Teilnehmers und der Vorwahl der Zielrufnummer, welcher Tarif für die Verbindung angewandt werden soll. Dies teilt der SCP dann der MSC in einer „Furnish Charging Information" (FCI) Nachricht mit. Die MSC übernimmt die Informationen in den Billing Record des

Gesprächs und ermöglicht es so später dem Abrechnungssystem, den entsprechenden Tarif für das Gespräch anzuwenden.

1.12 Fragen und Aufgaben

1. Mit welchem Verfahren und typischen Übertragungsgeschwindigkeiten werden Sprachdaten in einem leitungsvermittelten Netzwerk übertragen?
2. Welche wichtigen Komponenten gibt es im GSM Network Subsystem (NSS) und welche Aufgaben erfüllen sie?
3. Welche wichtigen Komponenten gibt es im GSM Radionetzwerk (BSS) und welche Aufgaben erfüllen sie?
4. Mit welchen Verfahren kann eine BTS gleichzeitig mit mehreren Teilnehmern kommunizieren?
5. Welche Verarbeitungsschritte durchläuft die menschliche Sprache in einem Mobiltelefon, bevor sie über die GSM Luftschnittstelle versandt werden kann?
6. Was ist ein Handover und welche Komponenten können daran beteiligt sein?
7. Wie wird bei einem eingehenden Gespräch der aktuelle Aufenthaltsort eines Teilnehmers ermittelt und wie wird das Gespräch im Netzwerk zugestellt?
8. Wie wird eine SMS Nachricht zwischen zwei Teilnehmern ausgetauscht?
9. Wie wird ein Teilnehmer im GSM Netzwerk Authentifiziert? Warum ist eine Authentifizierung notwendig?
10. Welche Aufgaben haben der RISC Prozessor und der DSP in einer Mobile Station?
11. Wie werden Daten auf einer SIM Karte abgelegt?
12. Was ist CAMEL und für welche Dienste wird es verwendet?