Martin Sauter

Grundkurs Mobile Kommunikationssysteme

Leserstimmen zu vorangegangenen Auflagen:

„Leicht verständliche und übersichtliche Darstellung mit hoher Praxisrelevanz. Als Lernhilfe mit Fragen und Aufgaben (und gut gepflegtem Online-Service mit Antworten) bestens geeignet."

Achim Büge, Berufskolleg Mühlheim

„Eine echte Einführung! Gut strukturiert, passende Tiefe, angenehmer Umfang. Ich werde das Buch auf der nächsten IT-Lehrerfortbildung vorstellen."

Jürgen Schumacher, Erich-Gutenberg-Berufskolleg Köln

„Gute Einführung und Nachschlagewerk zu den derzeitigen digitalen mobilen Kommunikationssystemen für Studierende und Praktiker."

Prof. Dr.-Ing. Bernhard Hoier, FH Brandenburg

„Klare Struktur und verständliche Sprache bei gleichzeitig tiefgehendem Wissen zu den wesentlichen mobilen Kommunikationssystemen machen dieses Buch auch zu einem gelungenen Nachschlagewerk."

Prof. Dr. Bettina Schnor, Universität Potsdam

„Endlich ein Buch, das NICHT-Elektrotechnikern, z. B. Informatikern, den Einstieg in mobile Kommunikationstechnologien ermöglicht."

Prof. Dr. Gernot Bauer, FH Münster

„Alle mobilen Technologien in einem Buch."

Prof. Dr. Jörg Keller, Fernuniversität Hagen

„Das Buch besticht durch seine Aktualität und die Praxisnähe des Autors. Ich bin begeistert!"

Prof. Dr. Johannes Maucher, HDM Stuttgart

„Dieses Buch bietet dem Leser praxis- und detailgerechtes Wissen zu mobilen Kommunikationssystemen. Vom derzeitigen GSM und GPRS über UMTS bis hin zu WLANs und Bluetooth werden die technischen Konzepte, Standards und Protokolle verständlich dargestellt."

Prof. Dr. Jürgen Scherff, FH Furtwangen

Martin Sauter

Grundkurs Mobile Kommunikationssysteme

Von UMTS und HSDPA, GSM und GPRS zu Wireless LAN und Bluetooth Piconetzen

Mit 196 Abbildungen

3., erweiterte Auflage

vieweg

Bibliografische Information Der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der
Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über
<http://dnb.d-nb.de> abrufbar.

1. Auflage 2004
2. Auflage 2006
3., erweiterte Auflage 2008

Lektorat: Sybille Thelen / Andrea Broßler

Der Vieweg Verlag ist ein Unternehmen von Springer Science+Business Media.
www.vieweg.de

Umschlaggestaltung: Ulrike Weigel, www.CorporateDesignGroup.de
Druck und buchbinderische Verarbeitung: MercedesDruck, Berlin
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.
Printed in Germany

ISBN 978-3-8348-0397-9

Vorwort zur dritten Auflage

Zwischen der zweiten und dritten Auflage dieses Buches hat sich in nur 12 Monaten wieder einiges in der Mobilfunkwelt getan und die aktuelle Auflage enthält wiederum zahlreiche Erweiterungen. Während eine der wichtigsten Neuerungen der zweiten Auflage die Beschreibung des UMTS Turbo „HSDPA“ war, ist in der Zwischenzeit auch „HSUPA“, eine Technik für schnellere Geschwindigkeiten im Uplink, verfügbar und darf deshalb in diesem Buch nicht fehlen.

Zum Erstaunen vieler Experten erfreuen sich die schon recht lange in der Praxis betriebenen GSM/GPRS Netze weiterhin weltweit eines starken Wachstums und der GPRS Beschleuniger EDGE wird mittlerweile auch in Deutschland von zwei Netzbetreibern angeboten. Schnelle Internetverbindungen sind somit nun auch in ländlichen Gebieten möglich, in denen es noch keine UMTS/HSPA Versorgung gibt. Diesem Trend wurde schon in der zweiten Auflage Rechnung getragen. Die dritte Auflage enthält nun auch Informationen über neue GPRS und EDGE Endgeräteklassen, die noch höhere Übertragungsgeschwindigkeiten unterstützen.

Während Wireless LAN bei Erscheinen der ersten Auflage nur wenig verbreitet war, hat es seither einen wahren Ansturm auf diese Art der Heim- und Bürovernetzung gegeben. Außerdem nimmt die Verbreitung von Wireless LAN Hotspots in Hotels, Flughäfen und Cafés weiter zu. Während heute der 802.11g Standard mit etwa 20 MBit/s auf Anwendungsebene üblich ist, gibt es mittlerweile eine stabile Vorversion des 802.11n Standards mit Datenraten auf Anwendungsebene von 150 MBit/s und mehr. In dieser Auflage wurde das Wireless LAN Kapitel deshalb stark erweitert und enthält jetzt eine Beschreibung von 802.11n sowie der 802.11e Quality of Service Erweiterung, die auch unter dem Namen Wireless Multimedia (WMM) bekannt ist. Schließlich hat sich auch beim Thema WLAN Sicherheit seit dem Erscheinen der ersten Auflage einiges getan und Kapitel 4 enthält nun eine ausführlichere Beschreibung zu Authentifizierung und Verschlüsselung mit WPA und WPA2.

Auch beim Bluetooth Standard gibt es zahlreiche Neuerungen. Vermehrt bieten heute Smartphones und auch Mobiltelefone im

mittleren Preissegment eine MP-3 Player Funktion, für die eine Verbindung zu einem Kopfhörer über das Headset- oder Handsfree Profil keine ausreichende Klangqualität bietet. Deshalb setzen Endgerätehersteller vermehrt auf das Advanced Audio Distribution Profil (A2DP), das nun im Bluetooth Kapitel beschrieben ist. Die in 2007 erschienene Bluetooth 2.1 + EDR Erweiterung brachte zudem neue Pairing Protokolle, um gefundene Schwachstellen zu beseitigen. Eine Beschreibung dieser Protokolle und anderer Verbesserungen wie z.B. die Verwendung von Near Field Communication (NFC) Tags sowie neuer Stromsparmechanismen ist nun ebenfalls enthalten.

Bleibt mir noch, Ihnen an dieser Stelle viel Freude beim Studium dieses Buches, und beim Experimentieren und Nutzen mobiler Kommunikation zu wünschen.

Paris, im August 2007 Martin Sauter

Vorwort

Mobile Kommunikationssysteme wie GSM, GPRS, UMTS, Wireless LAN und Bluetooth bieten heute eine große Vielfalt von Anwendungsmöglichkeiten. Um einen Einblick in die Technik dieser Systeme zu gewinnen, gibt es eine große Anzahl von Publikationen. In Buchform sind diese jedoch meist sehr umfangreich und für eine Einführung oft zu komplex. Publikationen im Internet hingegen sind meist nur sehr kurz und oberflächlich oder beschäftigen sich nur mit einer speziellen Eigenschaft eines Systems. Aus diesem Grund konnte ich während meiner Vorlesungen zu diesem Thema keine einzelne Publikation empfehlen, die eine Einführung in diese Systeme mit der nötigen Detailtiefe geboten hätte. Mit dem vorliegenden Buch möchte ich dies ändern.

Jedes der fünf Kapitel gibt eine detaillierte Einführung und Überblick über jeweils eines der zu Anfang genannten Systeme. Besonders wichtig ist mir auch, einen Eindruck zu vermitteln, welche Gedanken hinter der Entwicklung der unterschiedlichen Systeme standen. Neben dem „Wie“ ist also auch das „Warum“ zentraler Bestandteil jedes Kapitels. Außerdem wird durch zahlreiche Vergleiche zwischen den unterschiedlichen Technologien deutlich, wo die Anwendungsgebiete der einzelnen Systeme liegen. In manchen Fällen konkurrieren die Systeme miteinander, in vielen Fällen jedoch ergibt erst eine Kombination mehrerer Systeme eine interessante Anwendung. Abgerundet wird jedes Kapitel durch einen Fragen- und Aufgabenkatalog zur Lernzielkontrolle und Wiederholung.

Um einen tieferen Einblick in das eine oder andere System zu gewinnen, sind in den Kapiteln zahlreiche Verweise auf die entsprechenden Standards zu finden. Sie bilden eine ideale Ergänzung für einen tieferen Einblick in die einzelnen Systeme und sollten mit Hilfe der Hintergrundinformationen in diesem Buch auch etwas einfacher zu interpretieren sein.

Den Entschluss, mein Wissen zu diesen Themen als Buch zu veröffentlichen, fasste ich nach vielen theoretischen Gedankenspielen ganz spontan in einer Pariser Buchhandlung. Dort stieß ich zufällig auf ein Buch mit einem ganz anderen Themenschwerpunkt, mit dessen Autor ich jedoch den Umstand gemeinsam habe, dass wir für die gleiche Firma arbeiten. Ich nahm

Kontakt mit ihm auf, und er schilderte mir während eines ausgedehnten Mittagessens, wie man von der ersten Idee zu einem fertigen Buch kommt. An dieser Stelle möchte ich mich deshalb sehr herzlich bei Pierre Lescuyer bedanken, dessen Tipps mir beim Start meines eigenen Buchprojekts sehr weitergeholfen haben.

Außerdem gebührt mein großer Dank auch Berenike, die mir mit Ihrer Liebe und Freundschaft während dieses Projekts immer inspirierend zur Seite stand.

Weiterhin gebührt mein Dank auch Thomas Kempf, Christophe Schmid, Markus Rösch, Thomas Ehrle und ganz besonders Jörg Becker. Mit ihrem Wissen und großen Einsatz ihrer privaten Zeit haben sie mich vor einigen Fehlern bewahrt und in zahlreichen Gesprächen wichtige Anregungen und Verbesserungsvorschläge gegeben.

Nicht zuletzt gilt mein Dank auch Dr. Reinald Klockenbusch, der dieses Buchprojekt von Anfang an begleitet hat und an der Ausrichtung des Buches maßgeblich beteiligt war.

Paris, im Juni 2004 Martin Sauter

Inhaltsverzeichnis

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.

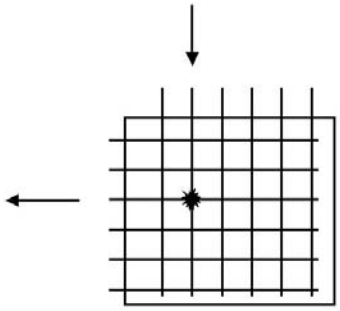

Abb. 1.1: Verbindungsmatrix in einer Vermittlungsstelle

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.

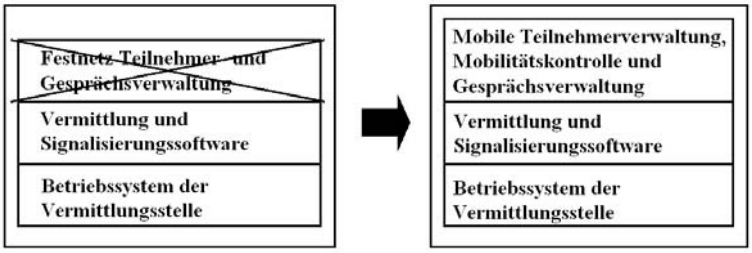

Abb. 1.2: Softwareänderungen von Festnetz- zu Mobilfunkvermittlung

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.

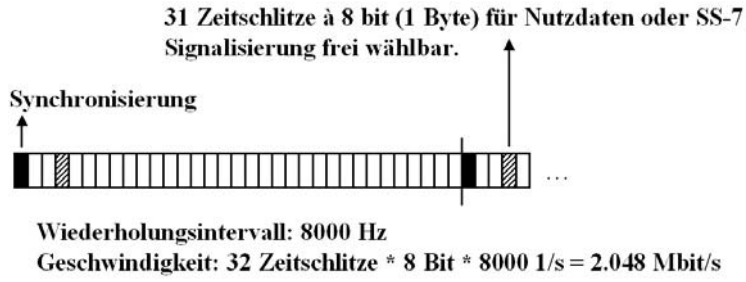

Abb. 1.3: Zeitschlitzarchitektur einer E-1Verbindung

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.

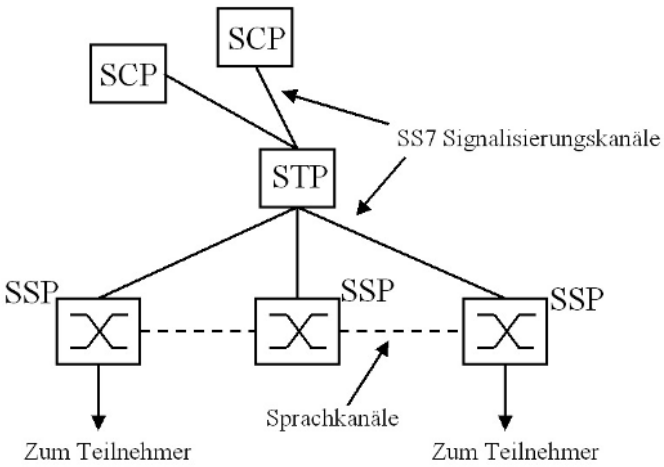

Abb. 1.4: Ein SS-7 Netzwerk mit einem STP, zwei SCP Datenbanken und 3 Vermittlungsstellen

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.

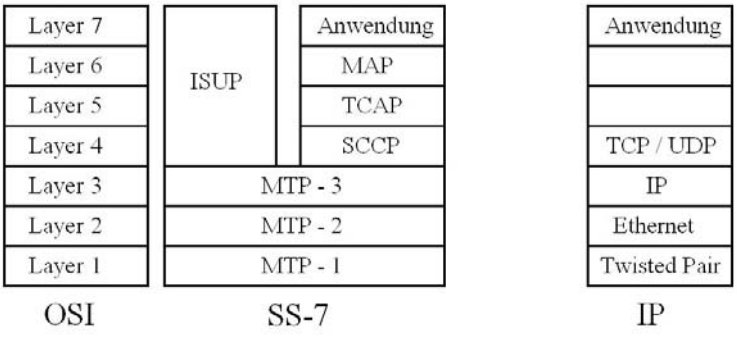

Abb 1.5: SS-7 Protokollstack im Vergleich zum IP Protokollstack

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.

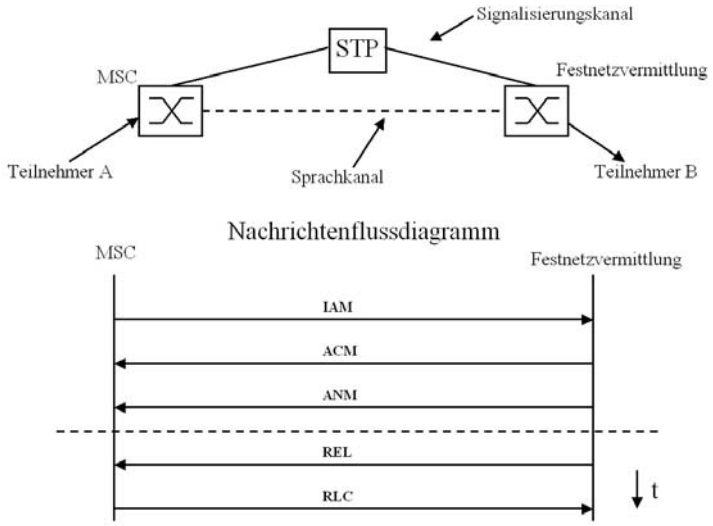

Abb. 1.6: Aufbau einer Verbindung zwischen Vermittlungsstellen

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.

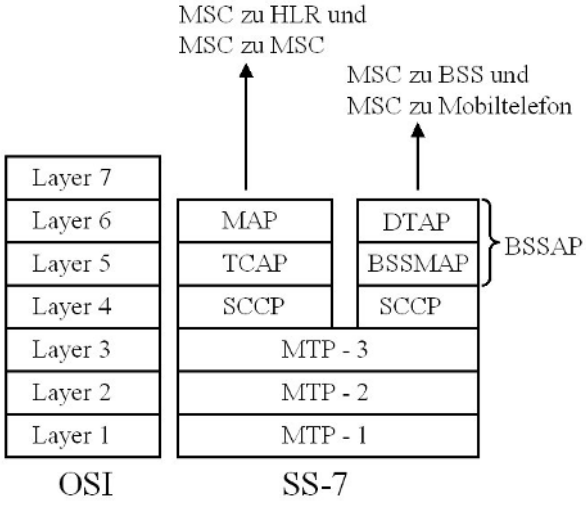

Abb. 1.7: Erweiterungen des SS-7 Protokollstacks für GSM

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.

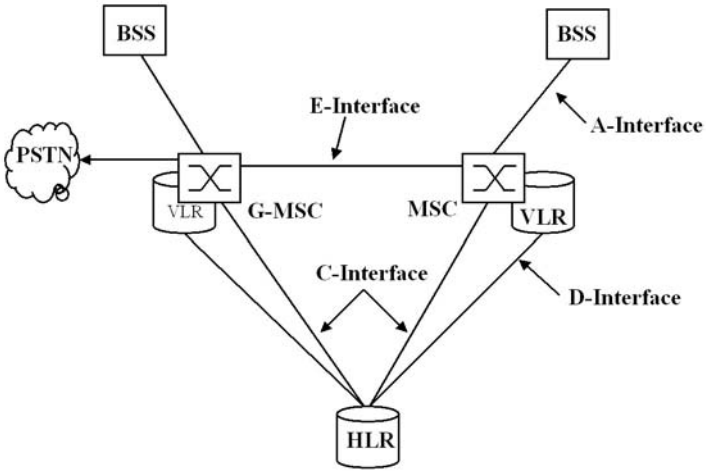

Abb. 1.8: Schnittstellen und Komponenten im NSS

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.

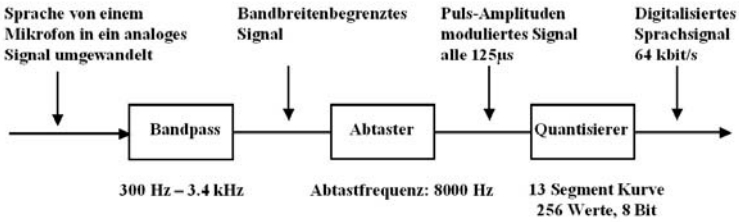

Abb. 1.9: Sprachdigitalisierung

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.

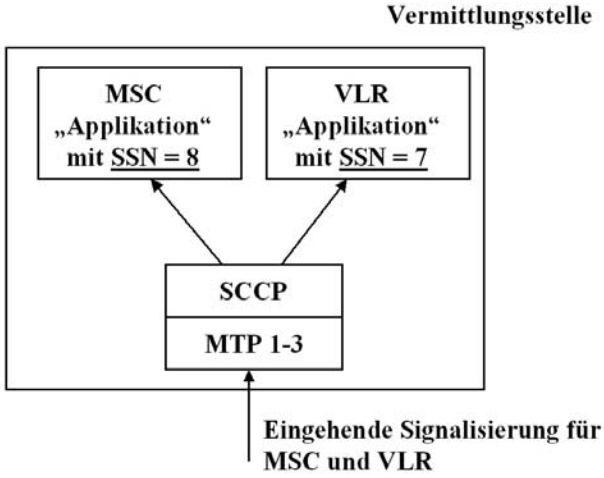

Abb. 1.10: Vermittlungsstelle mit integriertem VLR

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.

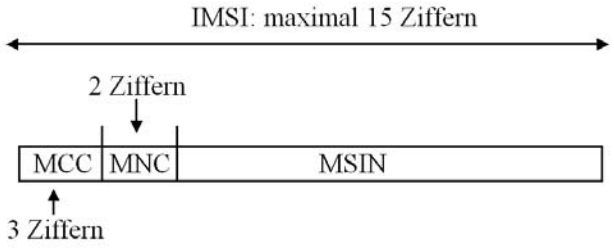

Abb. 1.11: Die IMSI

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.

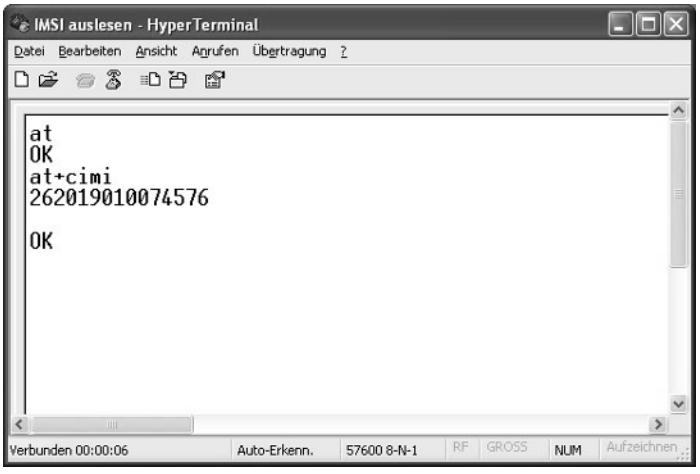

Abb. 1.12: IMSI per PC aus einer SIM Karte auslesen

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.

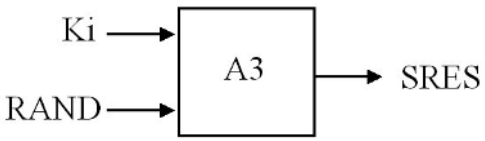

Abb. 1.13: Erzeugen der Signed Response (SRES)

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.

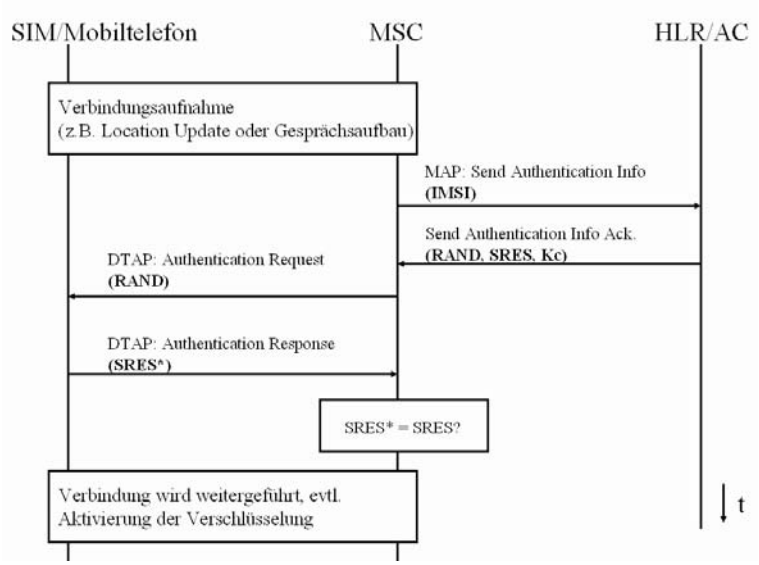

Abb. 1.14: Nachrichtenfluss während einer Authentifizierung

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.

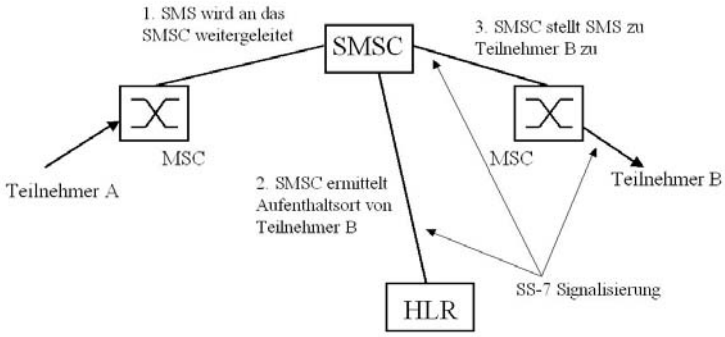

Abb. 1.16: Zustellungsprinzip einer SMS

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).

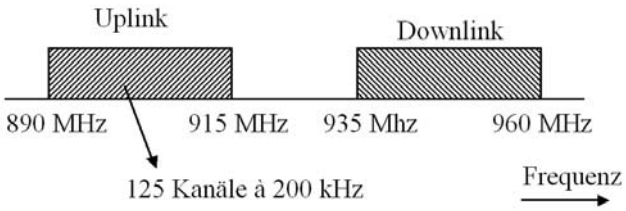

Abb. 1.17: Uplink und Downlink im 900 MHz Frequenzband

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.

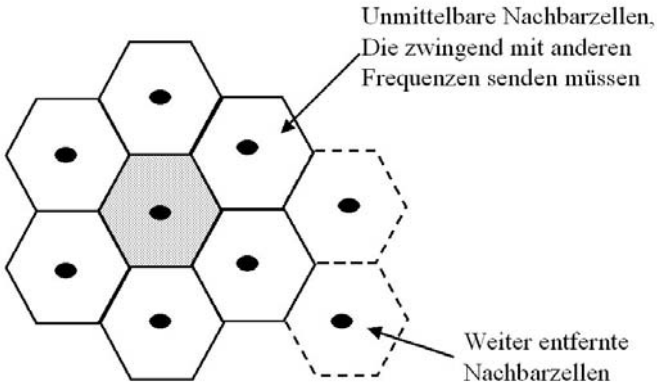

Abb. 1.19: Zelle mit Nachbarzellen

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.

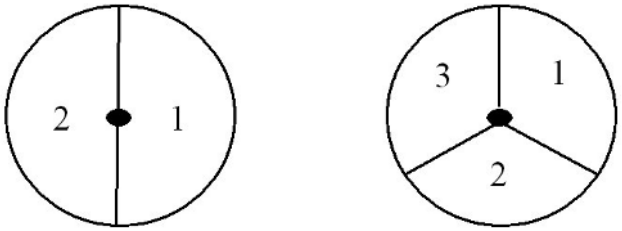

Abb. 1.20: Sektorisierte Zellkonfigurationen

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.

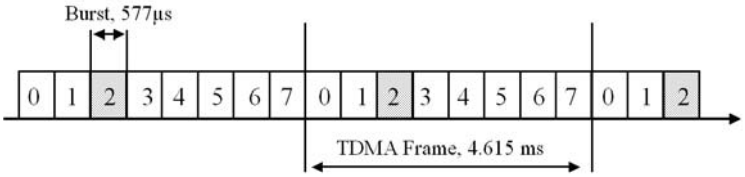

Abb. 1.21: Ein GSM TDMA Frame

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.

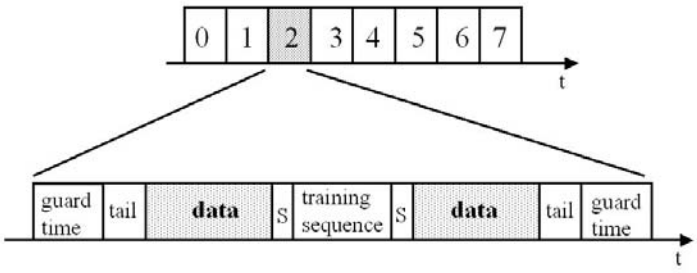

Abb. 1.22: Ein GSM Burst

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.

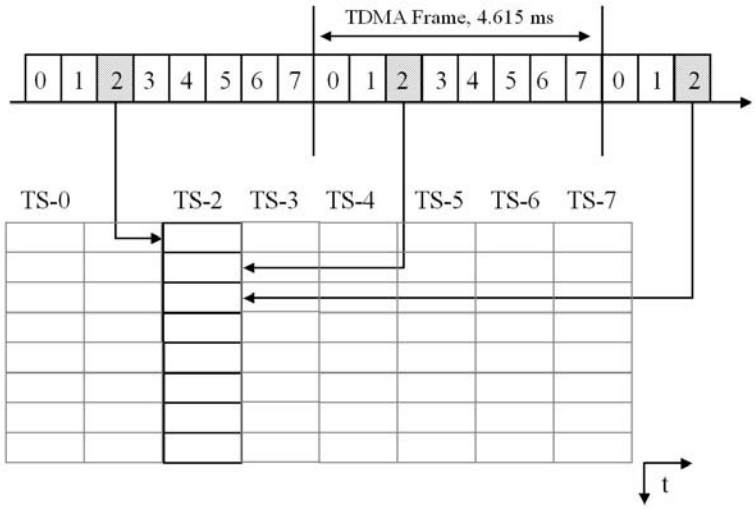

Abb. 1.23: Zusammenhängende Anordnung von Bursts eines Timeslots für die Darstellung der logischen Kanäle in Abb. 1.24

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.

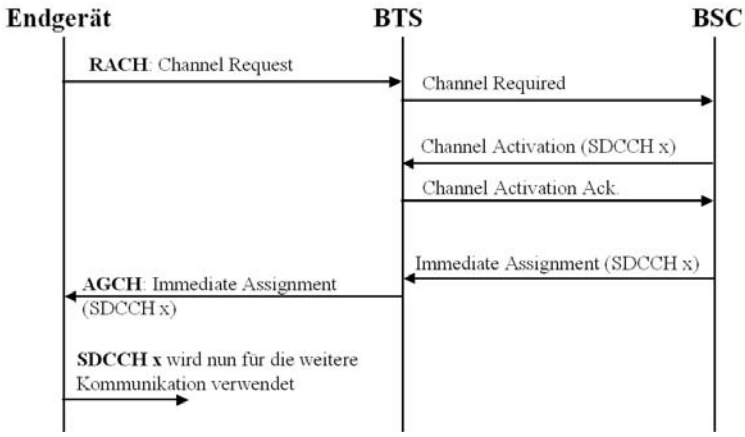

Abb 1.25: Aufbau einer Signalisierungsverbindung

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.

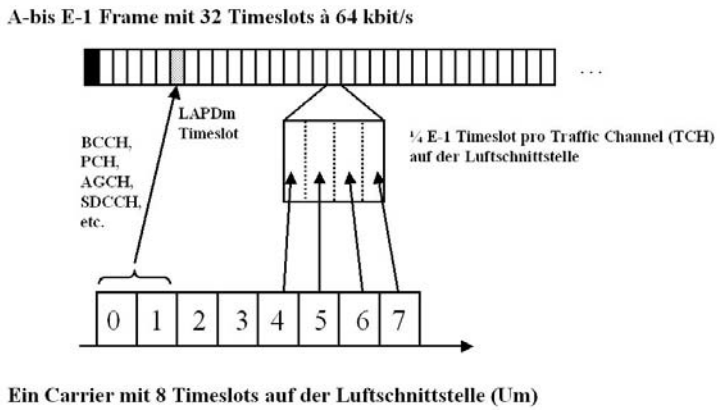

Abb. 1.26: Übertragung der logischen Luftschnittstellenkanäle auf dem A-bis Interface zum BSC.

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.

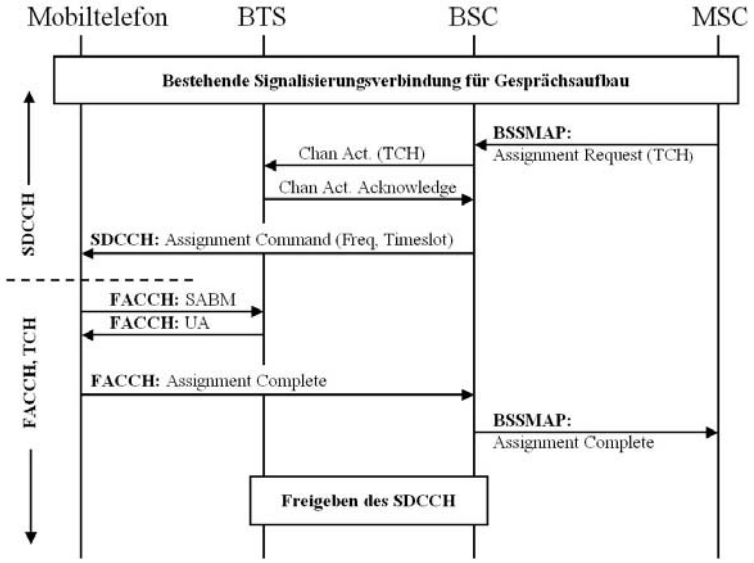

Abb. 1.27: Aufbau eines Sprachkanals (TCH)

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.

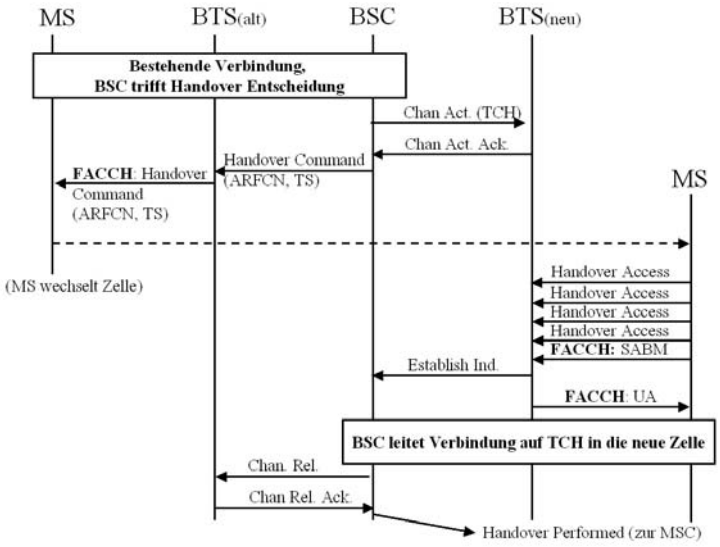

Abb. 1.28: Nachrichtenfluss während eines Handovers

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.

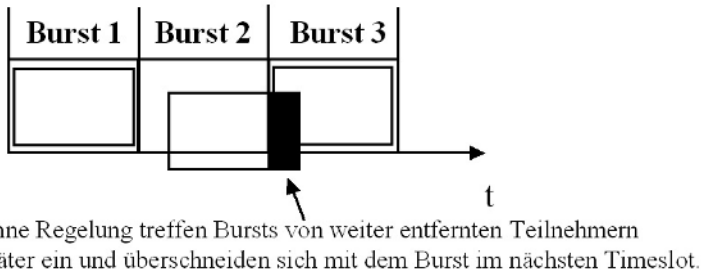

Abb. 1.29: Zeitverschiebung eines Bursts ohne Timing Advance Regelung

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.

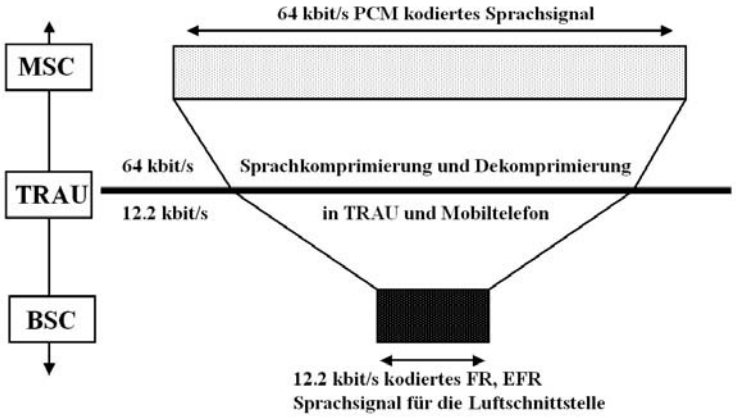

Abb. 1.30: GSM Sprachdatenkomprimierung

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.

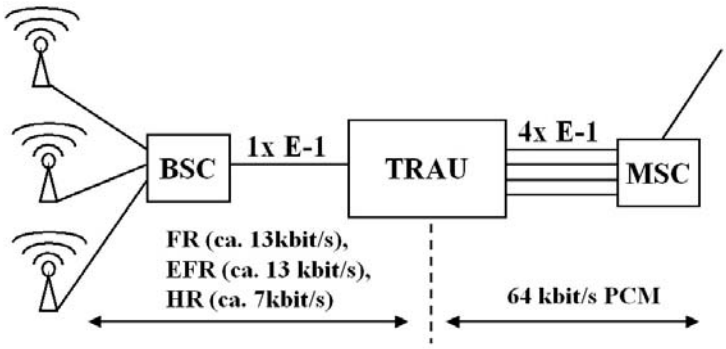

Abb. 1.31: Sprachkompression in Verhältnis 4:1 in der TRAU

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.

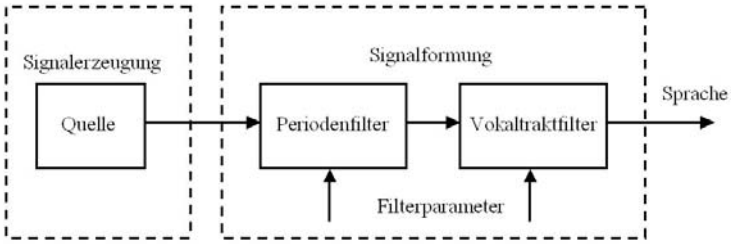

Abb 1.32: Quelle-Filter Modell des Full Rate Codecs

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.

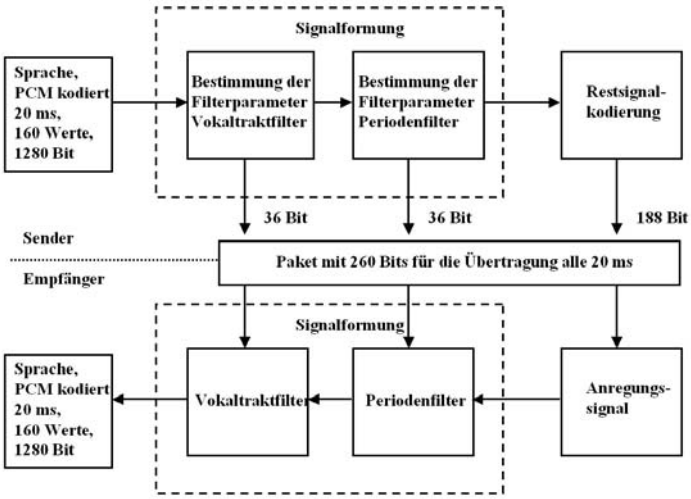

Abb. 1.33: Komplette Übertragungskette mit Sender und Empfänger des GSM Full Rate Codec

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.

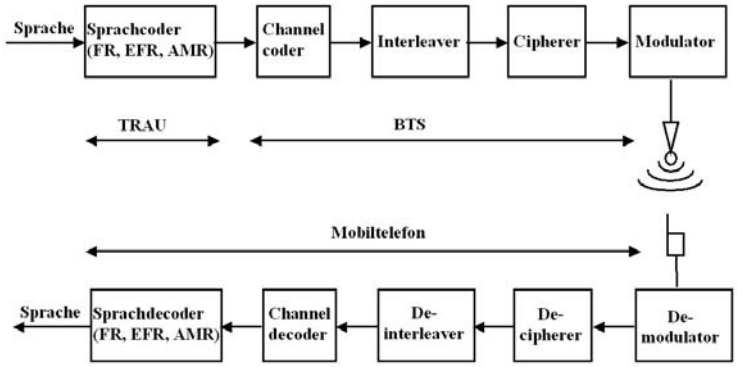

Abb. 1.34: Übertragungsschritte im Downlink zwischen Netzwerk und Mobiltelefon.

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.

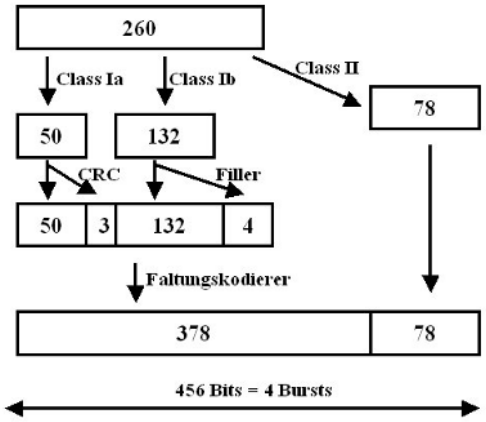

Abb. 1.35: GSM Kanalkodierer für FR Sprachdaten

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.

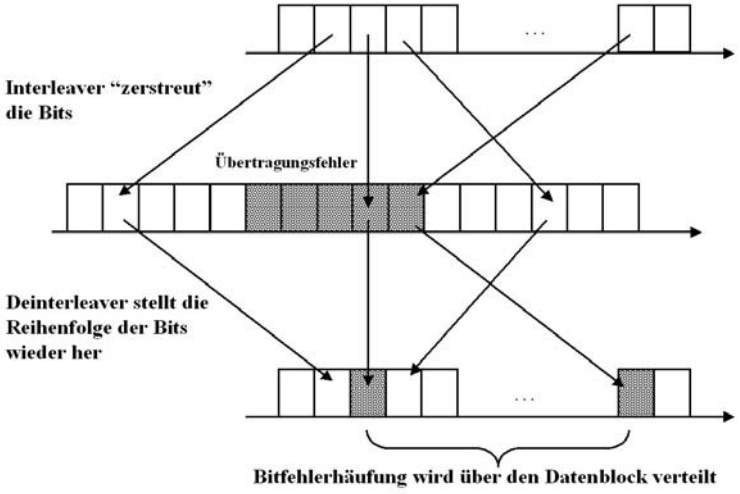

Abb. 1.36: Funktionsweise des Interleavers

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.

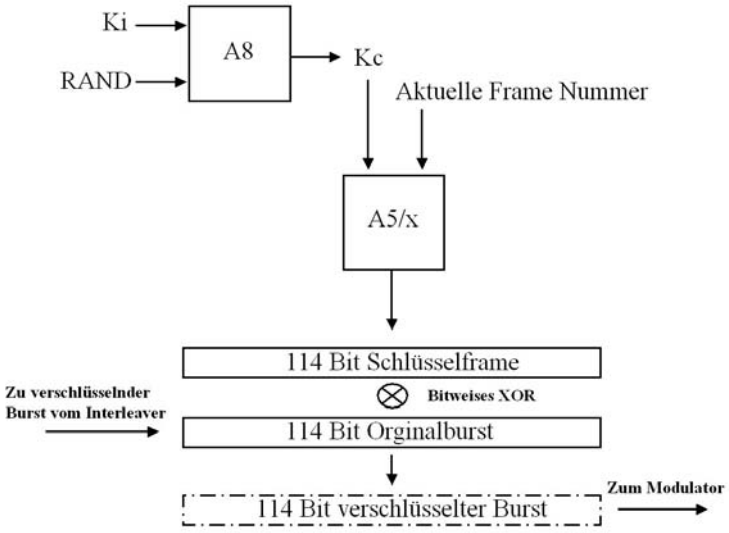

Abb. 1.37: Verschlüsselung eines Datenbursts

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.

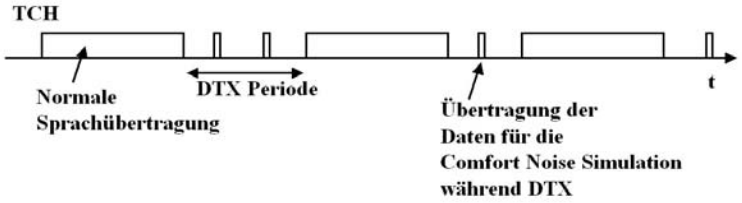

Abb. 1.38: Discontinuous Transmission (DTX)

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.

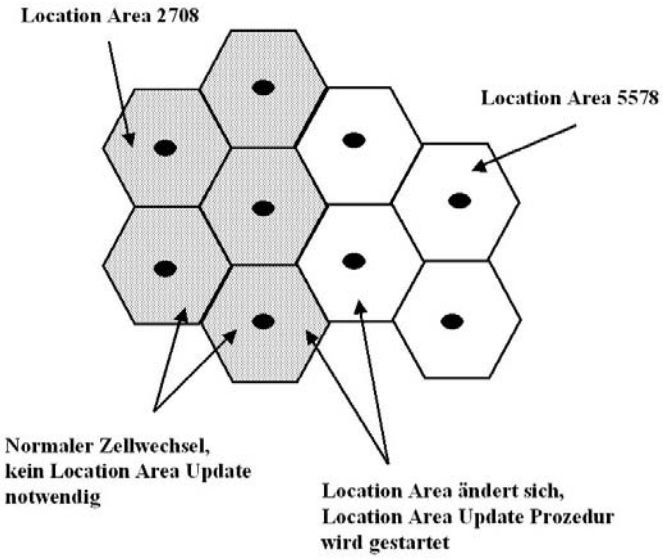

Abb. 1.39: Zellen in verschiedenen Location Areas

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.

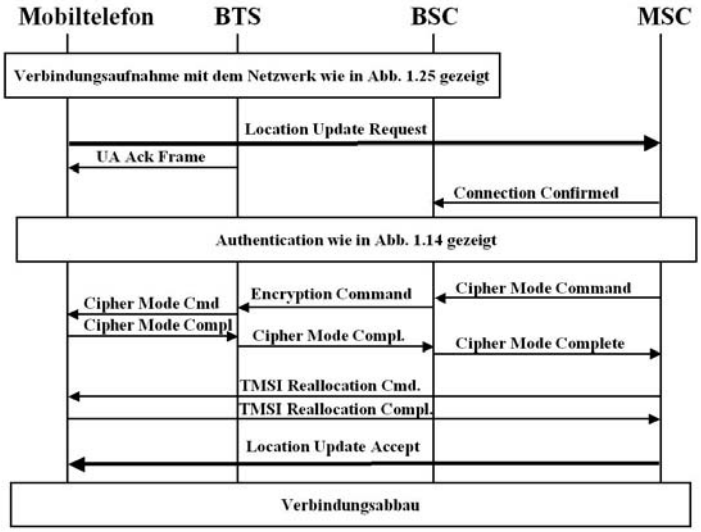

Abb. 1.40: Location Update

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.

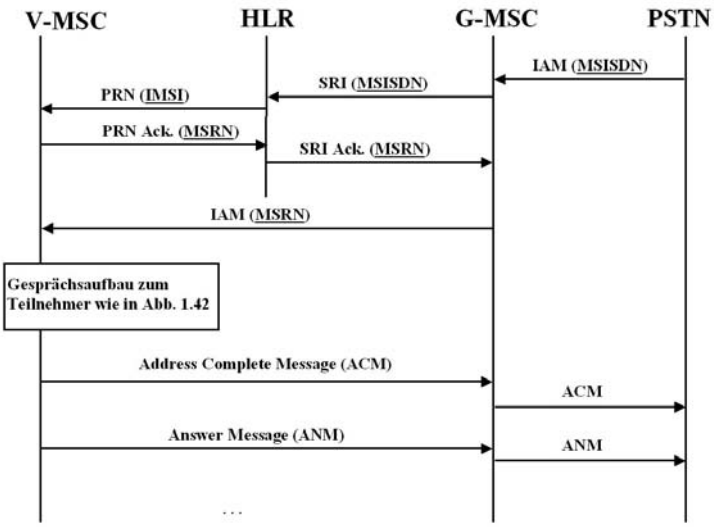

Abb. 1.41: Gesprächsaufbau zu einem mobilen Teilnehmer, Teil 1

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).

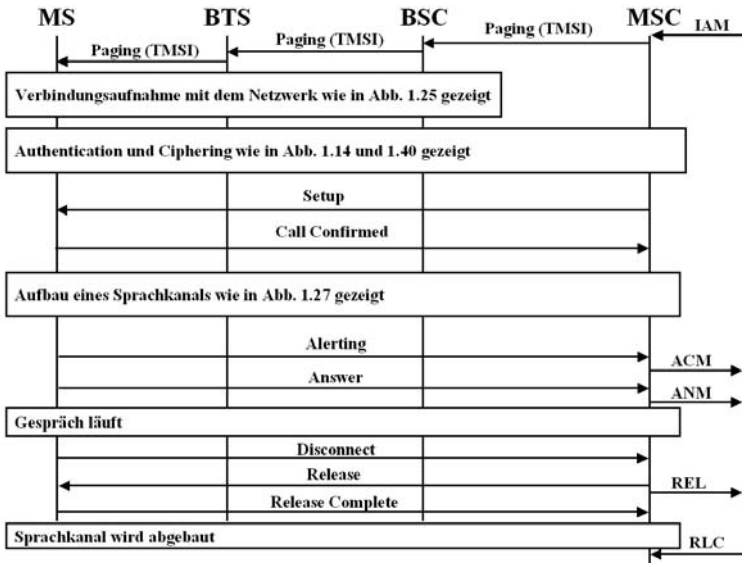

Abb. 1.42: Gesprächsaufbau zu einem mobilen Teilnehmer, Teil 2

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

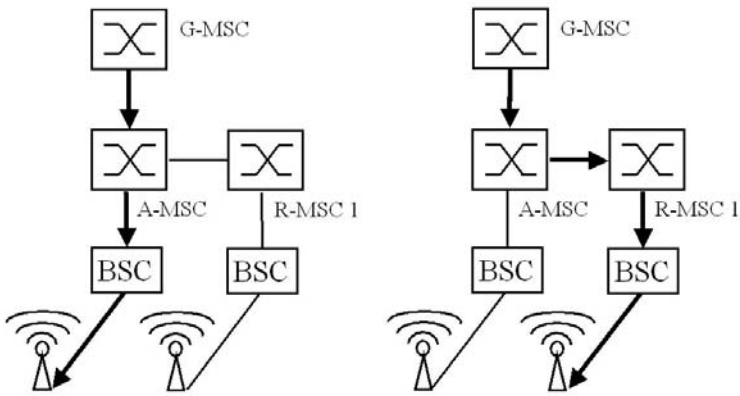

Abb. 1.43: Inter-MSC Handover

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.

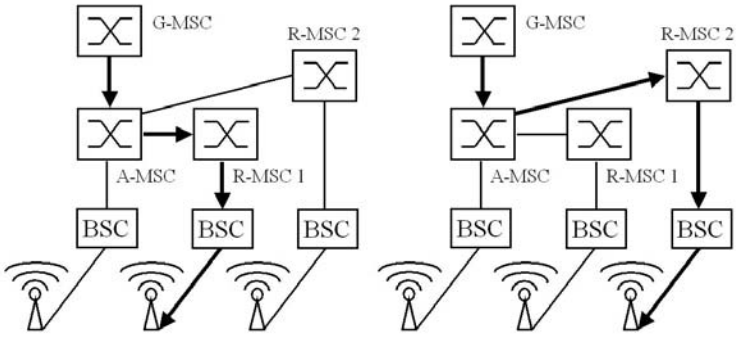

Abb. 1.44: Subsequent Inter-MSC Handover

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.

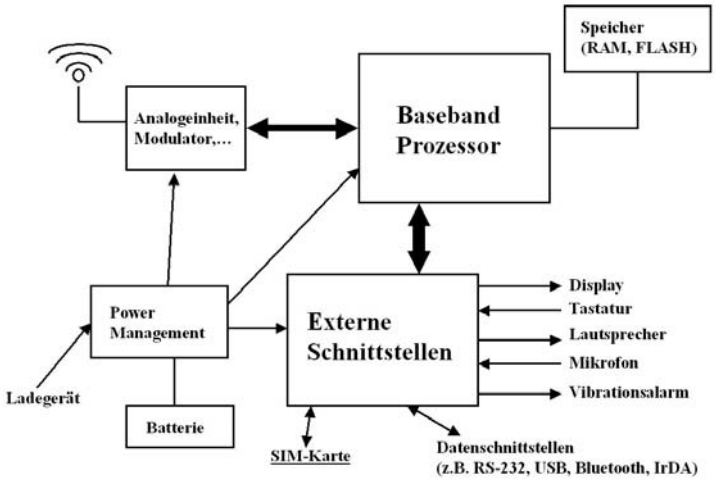

Abb. 1.45: Grundsätzlicher Aufbau eines Mobiltelefons

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.

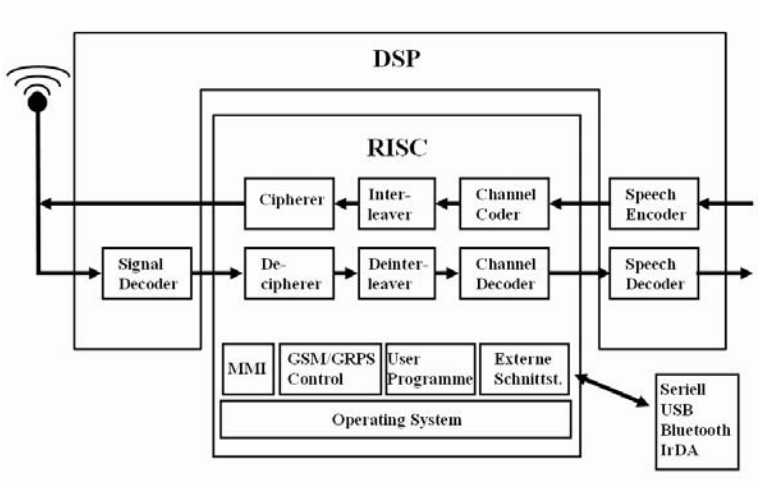

Abb. 1.46: RISC und DSP Funktionen im Überblick

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.

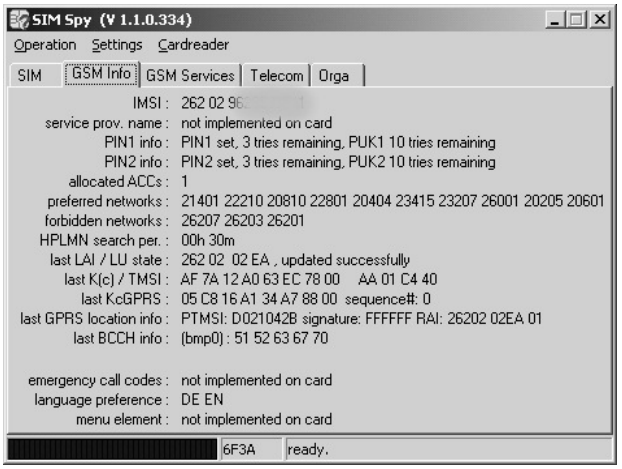

Abb. 1.47: Beispiel eines Tools zum Auslesen der Daten auf der SIM-Karte

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.

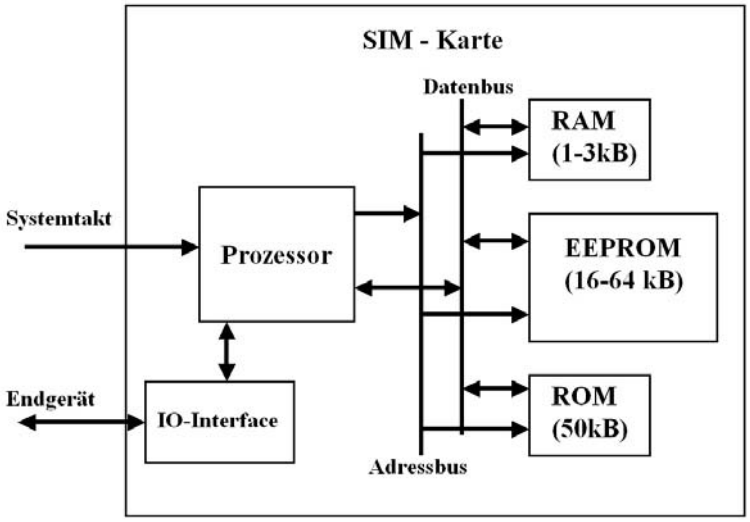

Abb. 1.48: Blockschaltbild der Komponenten einer SIM Karte

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.

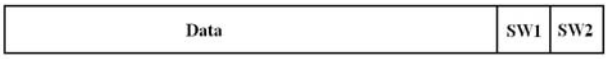

Abb. 1.50: Response APDU

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.

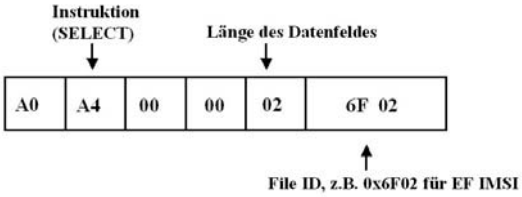

Abb 1.51: Select Command

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

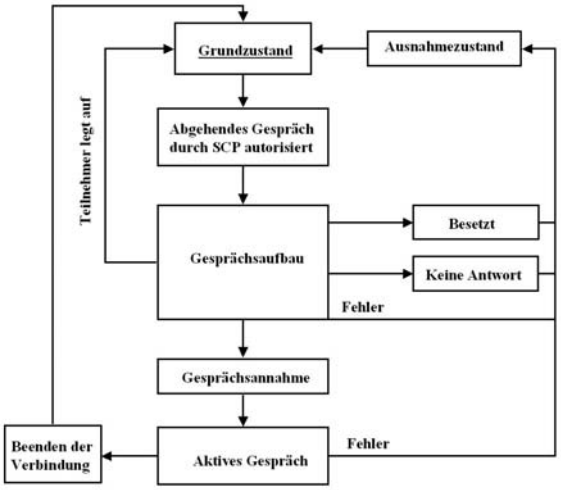

Abb. 1.52: Vereinfachtes Anrufer Zustandsmodell (O-BCSM) nach ETSI/3GPP TS 23.078

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?

2 GPRS und EDGE

Mitte der 80'er Jahre war die Sprachübertragung die wichtigste Anwendung für drahtgebundene und mobile Netzwerke. Aus diesem Grund wurde das GSM Netz auch hauptsächlich für die Sprachübertragung konzipiert und optimiert. Seite Mitte der 90'er Jahre spielt jedoch das Internet und somit die Datenübertragung eine immer größere Rolle. GPRS, der General Packet Radio Service, erweitert den GSM Standard für eine effiziente Datenübertragung und ermöglicht somit mobilen Geräten den Zugriff auf das Internet. Im ersten Teil dieses Kapitels werden die Vor- und Nachteile von GPRS gegenüber der GSM Datenübertragung und der Datenübertragung in drahtgebundenen Netzen erläutert. Teil zwei des Kapitels beschreibt dann, wie diese Datenübertragungstechnik standardisiert und in der Praxis implementiert wurde.

2.1 Leitungsvermittelte Datenübertragung

Da das GSM Netzwerk ursprünglich als leitungsvermittelndes Netzwerk konzipiert wurde, wird für eine herkömmliche Sprach- oder Datenverbindung zwischen zwei Teilnehmern ein exklusiver Kanal geschaltet. Dieser kann während der Verbindung nur von den zwei miteinander verbundenen Teilnehmern verwendet werden.

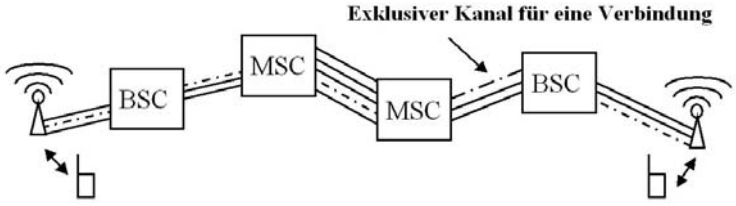

Abb. 2.1: Exklusive Verbindung bei der Leitungsvermittlung

Exklusive Verbindung

Dieser exklusive Kanal hat eine konstante Bandbreite und eine konstante Verzögerungszeit. Für den Anwender hat dies eine Reihe von Vorteilen:

Kein Overhead

Nach Aufbau der Verbindung können Daten in beide Richtungen ohne weitere Signalisierungsinformationen für das Weiterleiten der Daten (Routing) gesendet werden. Da die Verbindung fest geschaltet ist, leitet jede Komponente im Netzwerk die Daten über den für die Verbindung reservierten Kanal transparent an die nächste Komponente weiter.

Konstante Bandbreite

Der zugeteilte Kanal hat eine konstante Bandbreite, die Geschwindigkeit der Datenübertragung variiert also nicht. Dies ist besonders für die Sprachdatenübertragung wichtig, da hier die Daten nicht in Netzwerkelementen zwischengepuffert werden sollten oder gar in Überlastsituationen verworfen werden dürfen.

Konstante Verzögerungszeit

Eine weitere wichtige Eigenschaft einer leitungsvermittelten Verbindung für die Sprachübertragung ist die konstante Verzögerungszeit. Die Verzögerungszeit ist dabei die Zeit zwischen dem Senden und Empfangen eines Bits oder eines Datenblocks. Ohne eine konstante Verzögerungszeit müsste beim Empfänger ein Empfangspuffer vorhanden sein, der die schwankenden Verzögerungszeiten ausgleicht. Dies ist vor allem für Sprache sehr unerwünscht, da diese so schnell wie möglich am anderen Ende empfangen und wiedergegeben werden soll.

Während die Leitungsvermittlung ideal für die Sprachübertragung geeignet ist, gibt es jedoch einen großen Nachteil für die Datenübertragung mit variablen Übertragungsraten:

Keine Flexibilität

Das Webbrowsen im Internet ist eine typische Datenanwendung mit variablen Übertragungsraten. Während der Anforderung einer Webseite sollte dem Anwender eine möglichst große Bandbreite zur Verfügung stehen, um die Webseite möglichst schnell zu empfangen. Während des anschließenden Lesens der Webseite werden dann für einige Zeit keine Daten übertragen. Da bei einer leitungsvermittelten Verbindung die Bandbreite weder erhöht noch während des Lesens wieder freigegeben werden kann, ist die Leitungsvermittlung für diese Art der Datenübertragung nicht ideal geeignet. Vor allem die ungenutzte Bandbreite während des Lesens der Webseite ist für ein Mobilfunknetzwerk problematisch, da auf der Luftschnittstelle die Übertragungskapazität sehr begrenzt ist.

2.2 Paketorientierte Datenübertragung

Freigabe von Ressourcen

Für Anwendungen wie dem Webbrowsen ist es viel effizienter, wenn der Übertragungskanal nur während der eigentlichen Übertragung der Daten für einen Teilnehmer verwendet wird und danach wieder für andere freigegeben wird. Um dies zu errei-

chen, wird bei der paketorientierten Datenübertragung der Übertragungskanal nicht mehr in kleinere Kanäle für einzelne Benutzer aufgeteilt und fest zugeordnet. Stattdessen werden die Daten der unterschiedlichen Benutzer in Datenpaketen nacheinander über den Übertragungskanal gesendet. Zwar kann zu einer Zeit nur ein Teilnehmer senden oder empfangen, die Datenpakete werden dafür aber schneller übertragen, da die Bandbreite des gesamten Übertragungskanals zur Verfügung steht. Da bei dieser Übertragung nicht Leitungen vermittelt werden, sondern einzelne Pakete, wird diese Art der Datenübertragung Paketvermittlung oder Packet Switching genannt.

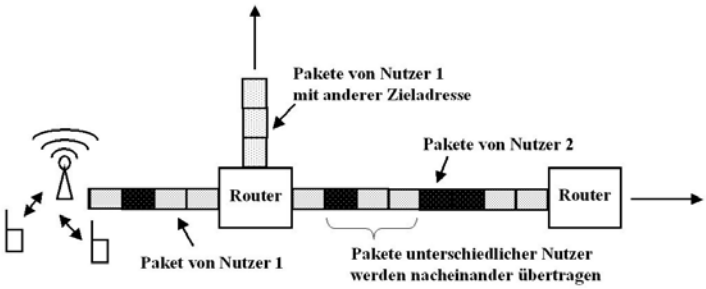

Abb. 2.2: Paketorientierte Datenübertragung

Pakete mit Quell- und Zieladresse

Da es bei der Paketvermittlung keine festen Kanäle gibt, muss jedes Paket eine Information über Absender (Source) und Empfänger (Destination) enthalten. Die Empfängeradresse, auch Zieladresse genannt, wird dann innerhalb des Netzwerkes für die Weiterleitung der Datenpakete an den richtigen Empfänger verwendet. Auf diese Weise wird z.B. auch eine Webseite im Internet übertragen. Die Webseite wird dazu vom Webserver (Sender) in mehrere IP Pakete aufgeteilt und danach zum Webbrowser (Empfänger) übertragen.

N:N Verbindungen möglich

Die paketorientierte Übertragung hat außerdem den Vorteil, dass ein Webbrowser auch Webseiten von verschiedenen Servern empfangen kann, ohne dafür wie bei der Leitungsvermittlung mehrere physikalische Verbindungen (Leitungen) explizit nacheinander aufzubauen.

GPRS für die mobile Paketvermittlung

Um die Paketdatenübertragung auch in GSM Netzwerken zu ermöglichen, wurde der General Packet Radio Service (GPRS) entwickelt. Dabei wurde besonderen Wert darauf gelegt, dass für GPRS keine neuen Basisstationen (BTS'en) notwendig sind.

Dies war eine wichtige Voraussetzung, um die paketorientierte Übertragung kostengünstig in bereits existierenden Netzwerken einzuführen.

GPRS bietet durch seinen paketorientierten Ansatz für mobile Applikationen mit dynamischer Bandbreitennutzung außerdem folgende Vorteile gegenüber der Leitungsvermittlung:

Höhere Datenraten

Flexible Zuteilung der Bandbreite auf der Luftschnittstelle: Da mehr als nur ein Zeitschlitz pro Teilnehmer zugeteilt werden kann, übertrifft die GPRS Übertragungsgeschwindigkeit die eines leitungsvermittelten Kanals von 9.6 oder 14.4 kbit/s bei weitem. GPRS bietet eine Übertragungsgeschwindigkeit von theoretisch 170 kbit/s, in der Praxis werden Geschwindigkeiten von etwa 50 kbit/s erreicht. Dies entspricht etwa der Geschwindigkeit eines Festnetzmodems.

Mit EDGE (Enhanced Data Rates for GSM Evolution), das den GPRS Standard unter anderem um eine neue Modulationsart erweitert, kann in der Praxis die Übertragungsgeschwindigkeit auf bis zu 230 kbit/s gesteigert werden. Da EDGE auch Neuerungen für den leitungsvermittelten Teil des Netzwerkes bringt, werden die GPRS Erweiterungen als EGPRS bezeichnet. Im täglichen Umgang dominiert jedoch die Abkürzung EDGE.

Während GPRS heute flächendeckend verfügbar ist, wird EDGE wegen des parallelen UMTS Ausbaus nicht von allen Netzbetreibern nachgerüstet. Somit ist EDGE (EGPRS) nicht in jedem Land und bei jedem Netzbetreiber verfügbar, der GPRS anbietet.

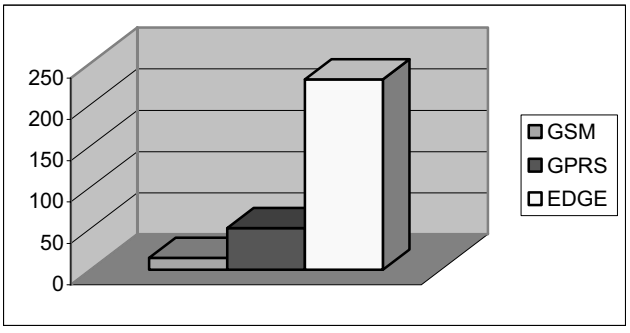

Abb. 2.3: Geschwindigkeit von GSM, GPRS und EDGE in kbit/s

Abrechnung nach Volumen

Bei GPRS kann nach Datenvolumen statt Onlinezeit abgerechnet werden. Großer Vorteil hierbei ist, dass z.B. beim Websurfen „nur“ für das übertragene Datenvolumen bezahlt werden muss und nicht für die Zeit, in der die Webseite gelesen wird. Da während des Lesens keine Daten übertragen werden, kann die frei gewordene Bandbreite für andere Nutzer verwendet werden. Dies ist bei der Leitungsvermittlung grundsätzlich nicht möglich.

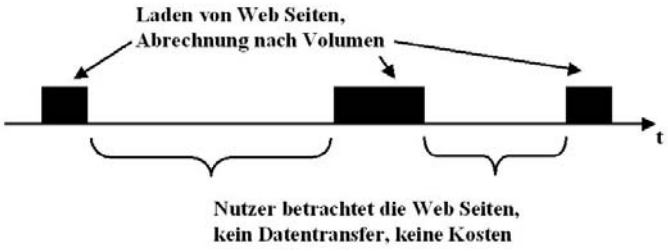

Abb. 2.4: Abrechnung nach Volumen und nicht nach Onlinezeit

Schnellerer Verbindungsaufbau

GPRS reduziert die Zeit für die Interneteinwahl erheblich. Während eine GSM leitungsvermittelte Internetverbindung ähnlich einer analogen Modemverbindung im Festnetz bis zu 20 Sekunden für den Verbindungsaufbau benötigt, kann eine GPRS Verbindung in weniger als 5 Sekunden aufgebaut werden. Dies ist vor allem ein großer Vorteil, wenn ein Nutzer möglichst schnell z.B. über den im Endgerät eingebauten WAP Browser die neuesten Nachrichten abrufen möchte.

Always On

Da der Benutzer nicht für die Zeit bezahlt, in der keine Daten übertragen werden, muss die Internetverbindung auch bei langen Übertragungspausen nicht abgebaut werden. Dieser „Always On“ Modus ermöglicht viele neue Anwendungen wie z.B. eMail-Programme, die automatisch neue eMail-Nachrichten empfangen oder Mobile Messaging Clients wie den Yahoo- oder MSN Messenger, die ständig auf neue Nachrichten warten können.

Keine Verbindungsabbrüche

Während einer Zug- oder Autofahrt kommt es häufig zu schlechtem Empfang oder sogar zu Empfangsverlust. In solchen Fällen brechen leitungsvermittelte Internetverbindungen ab und müssen vom Anwender erneut aufgebaut werden. GPRS Verbindungen dagegen werden bei Empfangsverlust nicht abgebrochen, da die logische Verbindung unabhängig von der Verfügbarkeit der physikalischen Verbindung weiterhin besteht. Wurden bei Emp-

fangsverlust gerade Daten übertragen, kann der Transfer sofort wieder aufgenommen werden, sobald das Endgerät eine neue Zelle des Netzwerks entdeckt. Da jedoch beim Webbrowsen die meiste Zeit für das Lesen der Webseiten verwenden wird und somit die meiste Zeit keine Daten übertragen werden, bemerkt ein Anwender einem Empfangsverlust oft gar nicht. Während leitungsvermittelte Datenverbindungen in Zügen oder Autos aufgrund der ständigen Verbindungsabbrüche in der Praxis nicht nutzbar sind, zeigt GPRS hier eine seiner größten Stärken, da es das mobile Internet in solchen Umgebungen erst ermöglicht.

2.2.1 GPRS und das IP Protokoll

GPRS wurde ursprünglich für die Übertragung von verschiedenen paketorientierten Protokollen entworfen. Mit dem großen Erfolg des Internets, das ausschließlich auf dem paketorientierten Internet Protokoll (IP) basiert, ist IP auch das einzige Protokoll, das GPRS heute unterstützt. Deshalb werden Begriffe wie „Nutzdatenübertragung“, „paketorientierte Datenübertragung“ oder „packet swichting“ in diesem Kapitel als Synonyme für „Übertragung von IP Paketen“ verwendet.

2.2.2 GPRS im Vergleich zur Datenübertragung im Festnetz

Hohe Übertragungskosten für GPRS

Trotz Kosteneinsparungen für den Benutzer, die durch die Freigabe nicht benötigter Ressourcen auf der Luftschnittstelle erreicht werden, ist die Datenübertragung per GPRS und EDGE noch immer um ein vielfaches teurer als die Datenübertragung im Festnetz. Durch den Einzug von EDGE und UMTS ist jedoch zu beobachten, dass aufgrund der schnelleren Datenraten und der ständig fallenden Kosten für Übertragungsstrecken auch die Datenratenübertragung per Funk zunehmend billiger wird.

Webseiten für mobile Geräte

Erfreulicherweise bieten viele Websites ihre Informationen heute auch in einem PDA freundlichen Format an. Da die Displaygröße eines PDAs wesentlich kleiner als ein PC Display ist, sind diese Webseiten auch wesentlich kleiner und kompakter. Dies bedeutet, dass auch das Datenvolumen der Seiten und der darin enthaltenen Bilder deutlich reduziert ist und somit die höheren Übertragungskosten etwas ausgleichen werden. Da Webseiten für PDAs ganz normale HTML Seiten sind, können sie auch mit einem Webbrowser eines Notebooks gelesen werden. Somit ist es möglich, auch mit größeren Endgeräten mobil im Internet zu einem erträglichen Preis zu browsen.

Zusammenfassend lässt sich sagen, dass GPRS und EDGE aus Kosten- und Geschwindigkeitsgründen ähnlich schnelle Festnetztechnologien wie Modems oder ISDN nicht verdrängen können. Für ‚klassische' Internetapplikationen wie Webbrowsen oder eMail sind GPRS und EDGE jedoch ideale Technologien, wenn keine Festnetzverbindung unterwegs zur Verfügung steht. Neben der Übertragung ‚klassischer' Internetapplikationen in die mobile Welt bildet GPRS auch die Grundlage für völlig neue Anwendungen wie mobile Messaging Clients etc., die durch die ‚Always On' Funktionalität erst möglich werden.

2.3 GPRS auf der Luftschnittstelle

Nach einem Überblick im letzten Abschnitt über die grundsätzliche Funktionsweise von GPRS zeigt dieser Abschnitt nun, welche Verfahren die paketdatenorientierte Datenübertragung über die Luftschnittstelle des GSM Mobilfunknetzwerkes ermöglichen.

2.3.1 GPRS Timeslot Nutzung im Vergleich zu GSM

PDTCH vs. TCH

Wie im ersten Kapitel gezeigt wurde, verwendet GSM Zeitschlitze (Timeslots) auf der Luftschnittstelle für die Kommunikation mit mehreren Teilnehmern. Während einer leitungsvermittelten Verbindung bekommt ein Teilnehmer einen logischen Traffic Channel (TCH) fest zugeteilt, der auf einem physikalischen Timeslot übertragen wird. Dieser kann nicht für andere Teilnehmer verwendet werden, auch wenn darauf für eine gewisse Zeit keine Daten übertragen werden.

Ressourcezuteilung

GPRS ist bei der Zuteilung der physikalischen Ressourcen sehr viel flexibeler. Die kleinste physikalische Ressource, die bei GPRS einem Teilnehmer zugeteilt werden kann ist ein Block, der aus 4 Bursts eines Packet Data Traffic Channel (PDTCH) besteht. Ein logischer PDTCH ist dem logischen TCH sehr ähnlich, da auch er auf einem physikalischen Timeslot übertragen wird. Möchte ein Teilnehmer weitere Daten übertragen, kann das Netzwerk auch die nachfolgenden Blocks des PDTCH dem Teilnehmer zuweisen. Die nachfolgenden Blocks können aber auch an andere Teilnehmer vergeben oder für Kontrollinformationen verwendet werden. Abbildung 2.5 zeigt auf der linken Seite, wie die Blocks eines PDTCH unterschiedlichen Teilnehmern dynamisch zugewiesen werden können. Die Darstellungsweise entspricht dabei dem Prinzip aus Abbildung 1.23.

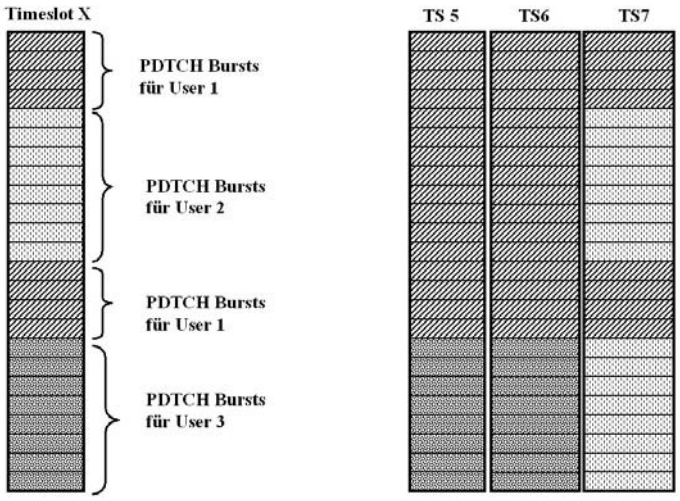

Abb. 2.5: PDTCH Vergabe und Timeslot Aggregation

GPRS 52 Multiframe

GPRS verwendet ähnlich wie GSM eine Rahmenstruktur für die Anordnung der Frames. Statt jedoch 26 bzw. 51 Frames zu einem Multiframe zu gruppieren, werden bei GPRS 52 Frames zu einem Multiframe zusammengefasst. In einem GPRS 52 Multiframe werden fast alle Frames für den logischen PDTCH sowie für Kontrollinformationen verwendet. Ausnahmen bilden lediglich Frame 24 und 51, die von aktiven Endgeräten für die Pegelmessung von Nachbarzellen verwendet werden. Frame 12 und 38 schließlich werden für Timing Advance Berechnungen verwendet. Details über den PDTCH und andere logische GPRS Kanäle werden in Kapitel 2.2.6 beschrieben.

Mutlislot Übertragung

Um die Übertragungsgeschwindigkeit eines Teilnehmers zu steigern, können wie im rechten Teil von Abbildung 2.5 gezeigt, mehrere Zeitschlitze gleichzeitig verwendet werden. Sind Daten für einen Teilnehmer zu übertragen, entscheidet das Netzwerk anhand der verfügbaren Timeslots und technischen Möglichkeiten des Endgeräts, wie viele Timeslots verwendet werden können. Dieses Verfahren wird Multislot Datenübertragung oder auch Timeslot Aggregation genannt.

Multislot-Klassen

Die Anzahl der Timeslots, die einem Endgerät gleichzeitig zugeteilt werden können, ist von seinen technischen Eigenschaften wie z.B. der Prozessorgeschwindigkeit abhängig. Endgeräte werden deshalb in unterschiedliche Multislot-Klassen eingeteilt, von denen die wichtigsten in Abbildung 2.6 dargestellt sind. In Ab-

hängigkeit der Multislot Klasse können dann 3, 4 oder mehr Timeslots für die Datenübertragung vom Netzwerk an ein Endgerät zugewiesen werden. Da bei Anwendungen wie dem Webbrowsen statistisch gesehen die unterschiedlichen Anwender in einer Zelle zu unterschiedlichen Zeiten Daten übertragen, erhöht sich so für jeden Teilnehmer die Übertragungsgeschwindigkeit und die Ressourcen werden besser genutzt. Die meisten heute erhältlichen Mobiltelefone unterstützen mindestens Multislot-Klasse 10. Geräte dieser Klasse können bis zu 4 Timeslots im Downlink und bis zu 2 Timeslots im Uplink bündeln. Das bedeutet, dass die maximale Übertragungsgeschwindigkeit im Uplink wesentlich geringer als im Downlink ist. Für viele Internet Anwendungen ist dies kein Problem, da z.B. beim Webbrowsen große Datenmengen meistens nur zum Endgerät, also in Downlink Richtung übertragen werden. Für andere Anwendungen wie z.B. dem Versenden von MMS Nachrichten mit Bildern oder Videosequenzen wären mehr Timeslots in Uplink Richtung wünschenswert. Geräte der gehobenen Preiskategorie unterstützen deshalb heute auch Multislot-Klasse 32, mit der 5 Timeslots im Downlink und 3 Timeslots im Uplink gebündelt werden können. Gleichzeitig nutzbar sind 6 Timeslots. Das Netzwerk kann somit dynamisch folgende Downlink + Uplink Kombinationen wählen: 5+1, 4+2 oder 3+3.

	Multislot	Mögliche Zeitschlitze		
	Klasse	Rx	Tx	Summe
	1	1	1	2
	2	2	1	3
	3	2	2	3
	4	3	1	4
	5	2	2	4
	6	3	2	4
	7	3	3	4
	8	4	1	5
	9	3	2	5
→	**10**	**4**	**2**	**5**
	11	4	3	5
	12	4	4	5
→	**32**	**5**	**3**	**6**

Abb. 2.6: Beispiele für GPRS Multislot-Klassen aus 3GPP TS 45.002, Annex B.1

Flexible Rekonfiguration

In Multislot Klasse 10 ist die Summe der gleichzeitig nutzbaren Timeslots im Uplink und Downlink zusammen maximal 5. Sind 4 Timeslots im Downlink zugeteilt, kann das Endgerät nur einen Timeslot für die Datenübertragung im Uplink verwenden. Bemerkt das Netzwerk, dass auch Daten in Uplink Richtung zu übertragen sind, wird die Timeslot Zuteilung allerdings automatisch neu konfiguriert. Das Endgerät bekommt dann 3 Timeslots in Downlink Richtung und 2 Timeslots in Uplink Richtung zugewiesen. Beendet das Endgerät die Übertragung im Uplink und werden weiterhin Daten im Downlink übertragen, ändert das Netzwerk erneut die Zuweisung, und es werden wieder 4 Timeslots im Downlink zugewiesen. Dieser Effekt kann zum Beispiel bei der Übertragung von Webseiten beobachtet werden. Neben der eigentlichen Webseite werden im Downlink auch die in der Seite enthaltenen Bilder übertragen, die aber extra angefordert werden müssen. Um die Seite möglichst schnell aufzubauen, werden diese Anforderungen noch während der Übertragung von anderen Elementen gesendet und profitieren somit besonders von dieser Methode.

MS Radio Access Capabilities

Damit das Netzwerk für jeden Teilnehmer die richtige Anzahl Timeslots zuweisen kann, teilt das Endgerät bei Anforderung eines Uplinkkanals dem Netzwerk seine Mobile Station Radio Access Capabilites mit. Teil dieser Information ist auch die unterstützte Multislot Klasse. Im Netzwerk wird die Multislot Klasse des Endgeräts gespeichert und kann somit später wieder verwendet werden, wenn Ressourcen im Downlink zugeteilt werden.

2.3.2 Gleichzeitige Nutzung einer Basisstation von GSM und GPRS

Da GPRS als Erweiterung eines GSM Netzwerks entwickelt wurde, teilen sich GSM und GPRS Netz auch die 8 Timeslots pro Frequenz einer Basisstation (BTS). Die maximale GPRS Datenrate hängt also auch davon ab, wie viele Timeslots einer BTS für Sprachkanäle verwendet werden. Es bleibt dabei dem Netzwerkbetreiber überlassen, wie viele Timeslots für welchen Dienst verwendet werden. Auch eine dynamische Zuordnung ist möglich. Bei geringem Sprachaufkommen können viele Timeslots für GPRS verwendet werden, die aber jederzeit für die Sprachübertragung dem GPRS Netzwerk entzogen werden können. In der Praxis wird üblicherweise eine Mischkonfiguration verwendet. Das bedeutet, dass für GPRS eine gewisse Anzahl an Timeslots

zur Verfügung steht, die nicht für Sprachkanäle verwendet werden dürfen. Neben diesen festen Timeslots werden weitere Timeslots dynamisch zugeteilt und können je nach Verkehrsaufkommen entweder für GPRS oder für leitungsvermittelte Verbindungen verwendet werden. So ist sichergestellt, dass trotz hohem Verkehrsaufkommen weiterhin ein Datentransfer mit GPRS möglich ist.

Abbildung 2.7 zeigt ein Beispiel für eine gemischte GSM/GPRS Konfiguration einer Zelle. Wie in Kapitel 1.7.3 gezeigt wurde, besteht in der Praxis eine BTS meist aus mehreren Zellen, in denen zur Kapazitätssteigerung mehrere Frequenzen verwendet werden.

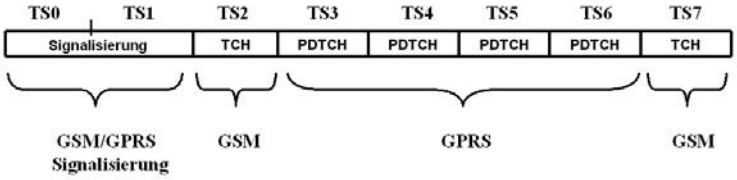

Abb. 2.7: Gemeinsame Nutzung einer Zelle von GSM und GPRS

2.3.3 Coding Schemes

Variable Geschwindigkeit

Eine weitere Möglichkeit die Übertragungsgeschwindigkeit der Teilnehmer zu steigern, ist die Anpassung der Bits pro Block für die Fehlerkorrektur an die jeweiligen Übertragungsbedingungen. Zu diesem Zweck wurden in GPRS vier Kodierungsverfahren (Coding Schemes) mit einem unterschiedlichen Verhältnis von Nutzdatenbits zu Fehlerkorrekturbits definiert. Bei schlechten Übertragungsbedingungen kann mit Coding Scheme 1 oder 2 eine Nettodatengeschwindigkeit von 8 bzw. 12 kbit/s pro Timeslot erreicht werden. Bei guten Übertragungsbedingungen können Coding Scheme 3 oder 4 verwendet werden und so Übertragungsraten von bis zu 20 kbit/s pro Timeslot erreicht werden.

Probleme mit CS-3 und CS-4

Während CS-1 und CS-2 in allen Netzwerken verwendet werden, haben die meisten Netzwerkkomponenten, die vor der Entstehung des GPRS Standards entwickelt wurden, ein Problem mit CS-3 und CS-4. Bei diesen Coding Schemes übersteigt die Datenrate inklusive Netzwerksignalisierungsinformationen die Bandbreite eines 16 kbit/s Timeslots auf dem Abis Interface. Um im Netzwerk CS-3 und CS-4 verwenden zu können, muss deshalb

die starre Zuordnung von Timeslots auf der Luftschnittselle und Timeslots auf dem Abis Interface aufgehoben werden. Dies erfordert in vielen Fällen nicht nur angepasste Software, sondern auch neue Hardware. Beim Kauf neuer GSM Hardware gehen die Netzbetreiber statt CS-3 und 4 deshalb lieber gleich auf das nachfolgend noch genauer beschriebene EDGE Verfahren über. Viele Netzbetreiber überspringen jedoch auch diesen Schritt und forcieren stattdessen ihren UMTS Ausbau.

	Modulation	**Geschwindigkeit pro Timeslot**
GPRS CS-1	GMSK	8 kbit/s
GPRS CS-2	GMSK	12 kbit/s
GPRS CS-3	GMSK	14.4.kbit/s
GPRS CS-4	GMSK	20 kbit/s
EDGE MCS-1	GMSK	8.8 kbit/s
EDGE MCS-2	GMSK	11.2 kbit/s
EDGE MCS-3	GMSK	14.8 kbit/s
EDGE MCS-4	GMSK	17.6 kbit/s
EDGE MCS-5	8PSK	22.4 kbit/s
EDGE MCS-6	8PSK	29.6 kbit/s
EDGE MCS-7	8PSK	44.8 kbit/s
EDGE MCS-8	8PSK	54.4 kbit/s
EDGE MCS-9	8PSK	59.2 kbit/s

Abb. 2.8: GPRS Coding Schemes (CS) und EDGE Modulation and Coding Schemes (MCS) im Überblick

CS-2, CS-3, Convolutional Coding und Punktierung

In Abbildung 2.9 ist dargestellt, wie Nutzdaten mit Coding Scheme 2 und 3 für die Übertragung über die Luftschnittstelle vorbereitet werden. Das Verfahren ist dabei sehr ähnlich wie die Kodierung der Sprachdaten, die bereits in Kapitel 1.7.5 vorgestellt wurde. Während der Half Rate Convolutional Coder bei Sprachdaten nur für eine Auswahl an Bits verwendet wird, wird dieser

hier auf alle Datenbits angewandt. Dies ist auch sinnvoll, da bei der Datenübertragung alle Bits gleich wichtig sind und somit auch alle Bits gleichermaßen geschützt werden müssen. Ergebnis dieser Codierung sind 588 (CS-2) bzw. 676 Bits (CS-3), die dann innerhalb eines Blocks übertragen werden sollen. Da aber in einem Block (= 4 Bursts) nur genau 4*114 Bits = 456 Bits übertragen werden können, muss der so erzeuge Datenstrom vor der Übertragung aber noch angepasst werden. Dies geschieht durch weglassen einzelner Bits (Punktierung). Da der Empfänger weiß, welche Bits punktiert, also nicht übertragen wurden, kann dieser an den geeigneten Stellen ‚Dummy' Bits einfügen, die der Convolutional Decoder dann als Fehler betrachtet und entsprechend wieder korrigieren kann. Unterschied zwischen CS-2 und CS-3 sind die Anzahl der punktierten Bits. Je mehr punktierte Bits, desto weniger ‚richtige' Fehler dürfen während der Übertragung im Datenblock auftreten. Das in Abbildung 2.9 gezeigte USF (Uplink State Flag) Precoding in 6 Bits dient den unterschiedlichen Teilnehmern als Sendeerlaubnis und wird in Kapitel 2.5 zusammen mit dem dort eingeführten RLC/MAC Header ausführlicher beschrieben.

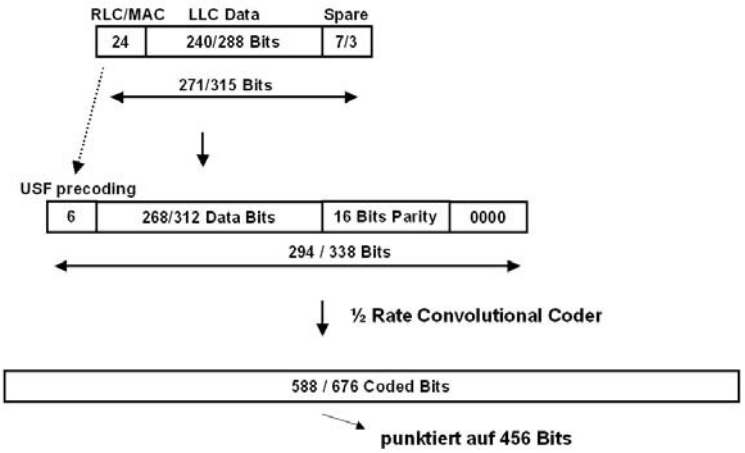

Abb. 2.9: CS-2 und CS-3 Kodierung von GPRS Daten

2.3.4 EDGE (EGPRS)

Um die GPRS Übertragungsgeschwindigkeit noch weiter zu steigern, wurde für GPRS als nächste Ausbaustufe ein neues Modu-

lationsverfahren nach dem 8PSK Prinzip unter dem Namen EDGE (Enhanced Data Rates for GSM Evolution) standardisiert.

EDGE Modulation und Coding Schemes

Statt 1 Bit pro Übertragungsschritt wie bei der bisher für GSM und GPRS verwendeten GMSK Modulation, werden mit EDGE 3 Bits pro Übertragungsschritt gesendet. Zusammen dem höchsten der insgesamt 9 Coding Schemes sind Übertragungsraten von bis zu 60 kbit/s pro Timeslot möglich. Ähnlich wie bei CS-3 und CS-4 sind jedoch auch hierfür neue Hardwarekomponenten im Radionetzwerk erforderlich. Darüber hinaus sind wegen des neuen Modulationsverfahrens auch neue Endgeräte notwendig. Ein weiterer Vorteil von neun unterschiedlichen Modulation Coding Schemes (MCS) gegenüber den vier GPRS Coding Schemes ist eine exakte Verwendung der für die aktuelle Übertragungsqualität geeigneten Modulation und Kodierung. Da sich Netzwerk und Endgerät im Gegensatz zu GPRS auch ständig gegenseitig über die Signalqualität beim Empfang der vorhergehenden Datenpakete informieren, kann somit schnell auf geänderte Übertragungsbedingungen reagiert werden. Dies senkt die Fehlerrate und ermöglicht bei jeder Signalqualität die optimale Geschwindigkeit. Durch diesen Regelmechanismus ist es auch in der Praxis tatsächlich möglich, MCS-8 und 9 bei guten Übertragungsbedingungen zu verwenden.

Incremental Redundancy

Trotz schneller Reaktion auf sich ändernde Übertragungsbedinungen ist es natürlich weiterhin möglich, dass Datenblocks nicht korrekt empfangen werden. Auch hier wurde mit EDGE der GPRS Standard erweitert, um den Datentransfer auf höheren Schichten nicht ins Stocken geraten zu lassen. Um Übertragungsfehler zu beheben, kann z.B. ein Verfahren namens „Incremental Redundancy“ eingesetzt werden. Wie zuvor schon bei den GPRS Coding Schemes gezeigt, werden nicht alle berechneten Fehlerkorrekturbits auch tatsächlich gesendet (puncturing). Tritt ein Übertragungsfehler auf, wird mit Incremental Redundancy das Paket nicht einfach erneut übertragen, sondern es werden nun Fehlerkorrekturbits gesendet, die vorher nicht übertragen wurden. Auf der Empfängerseite können dann die Fehlerkorrekturbits vom ersten und zweiten Übertragungsversuch kombiniert werden. Da nun mehr Fehlerkorrekturbits zur Verfügung stehen, steigen die Chancen, die Übertragungsfehler im Paket zu korrigieren.

Re-Segmentation

Statt Incremental Redundancy ist es mit EDGE auch möglich, den Inhalt eines fehlerhaft empfangenen Paketes, dass zuvor mit einem hohen MCS gesendet wurde auf zwei Pakete aufzuteilen

mit niedrigerem MCS aufzuteilen. Diese Methode wird Re-Segmentation genannt.

Verbesserungen beim Interleaving

Auch beim Interleaving, also dem Mischen von Bits um punktuelle Übertragungsfehler über den Block zu streuen (vgl. Kapitel 1.7.5), wurden mit EDGE Erweiterungen am Standard vorgenommen. Bei GPRS wird ein Datenblock unabhängig vom Coding Scheme immer über 4 Bursts gesendet. Bei den EDGE MCS 7-9 jedoch wurde die Länge eines Blocks auf zwei Bursts reduziert und somit das Interleaving verkürzt. Somit müssen bei einem Übertragungsfehler nur zwei Bursts neu übertragen werden und nicht vier. Dies ist vor allem bei der Verwendung von Frequency Hopping ein großer Vorteil. Dieses Verfahren wird verwendet, um nicht konstant auf einer Frequenz zu senden, die gestört oder für die aktuellen Übertragungsbedingungen ungeeignet ist. Während Frequency Hopping für die Sprachübertragung aufgrund der Kaschierung von kleinen Fehlern im Sprachdecoder gut geeignet ist, lassen sich viele falsche Bits in einem Burst bei der Datenübertragung nicht verstecken und der fehlerhafte Block muss komplett neu übertragen werden.

2.3.5 Mobile Station Classes

Class C

Der GPRS Standard sieht drei verschiedene Endgeräteklassen vor: Endgeräte der Mobile Station Class C können entweder im leitungsvermittelnden GSM Netzwerk oder im paketvermittelnden GPRS Netzwerk angemeldet sein. Diese Klasse macht vor allem für Endgeräte Sinn, die nur für die Datenübertragung gedacht sind.

Class B

Die häufigste Mobile Station Class die derzeit für Endgeräte verwendet wird, ist Mobile Station Class B. Endgeräte dieser Klasse können gleichzeitig im GSM leitungsvermittelnden Netz und dem GPRS paketvermittelnden Netz angemeldet sein und beide Dienste ohne explizites Umschalten nutzen. Einschränkend gilt jedoch, dass während eines Telefongesprächs keine Daten per GPRS gesendet oder empfangen werden können. Umgekehrt bedeutet dies auch, dass während einer laufenden Datenübertragung keine Telefonate geführt werden können. Baut der Anwender während einer GPRS Datenübertragung ein Telefongespräch auf, wird die GPRS Datenübertragung unterbrochen. Nach Ende des Gesprächs wird die Datenübertragung ohne erneute Verbindungsaufnahme weitergeführt. Dies kann vor allem dann eine Einschränkung sein, wenn das Endgerät neben dem Telefo-

nat noch zusätzlich von einem Endgerät wie z.B. einem Notebook für die Datenübertragung verwendet wird.

PCH kann nicht gelesen werden

Da ein Endgerät der Klasse B während einer GPRS Datenübertragung den Paging Channel (PCH) nicht beobachten kann, werden in dieser Zeit ankommende Telefongespräche oder SMS Nachrichten nicht empfangen. Bei burstartiger Datenübertragung wie dem Internet Browsing oder dem WAP Browsing ist die Chance jedoch recht hoch, das eingehende Gespräch oder die SMS trotzdem zu empfangen. Bei diesen Anwendungen werden immer nur kurzzeitig Daten übertragen und die Nachrichten auf dem Paging Channel werden zumindest einmal wiederholt. Dennoch kann nicht ausgeschlossen werden, dass die Paging Nachricht nicht gesehen wird. Abhilfe schafft hier der Network Operation Mode 1 (NOM 1), der im nächsten Abschnitt vorgestellt wird.

Class A

Schließlich gibt es noch die Mobile Station Class A. Endgeräte dieser Klasse können ebenso wie Endgeräte der Klasse B gleichzeitig am GSM und GPRS Teil des Netzwerkes angemeldet sein. Wichtiger Unterschied ist jedoch, dass telefonieren im leitungsvermittelnden Teil und Datenübertragung im paketvermittelnden Teil des Netzwerkes gleichzeitig möglich ist. Voraussetzung dafür ist aber eine aufwändigere Hardware in den Endgeräten.

2.3.6 Network Operation Mode (NOM)

Ähnlich der verschiedenen Endgeräteklassen mit unterschiedlicher Komplexität gibt es auch für das Netzwerk unterschiedliche Betriebsmodi, die Network Operation Mode (NOM) 1, 2 und 3 genannt werden.

NOM 2

Der Network Operation Mode 2 (NOM 2) ist der einfachste der drei Netzwerk Modi und wurde deshalb bei der Einführung fast aller GPRS Netze in der Praxis verwendet. Auch heute ist dieser Modus noch bei den meisten Netzwerken anzutreffen. NOM 2 verwendet für einen Teil der Signalisierung die schon vorhandenen GSM Signalisierungskanäle wie den RACH, den AGCH und den PCH. Nachrichten auf diesen Kanälen werden vom BSC transparent zwischen Endgerät und GPRS Netzwerk weitergegeben. Mehr dazu in Kapitel 2.4. Um diesen Mode so einfach wie möglich zu halten, gibt es zwischen den GSM und GPRS Kernnetzen keine Verbindung. Dies führt wie schon erwähnt dazu, dass eingehende Telefongespräche und SMS Nachrichten während einer aktiven GPRS Datenübertragung mit einem Mobile Station Class B Endgerät nicht empfangen werden können.

NOM 3

Der Network Operation Mode 3 bietet zusätzlich zu den Fähigkeiten des NOM 2 eigene GPRS Signalisierungskanäle. Statt die bereits für GSM verwendeten BCCH, RACH, AGCH und PCH Kanäle für GPRS mitzuverwenden, gibt es bei NOM 3 dafür eigene GPRS Kanäle, die PBCCH, PRACH, PAGCH und PPCH genannt werden. ‚P' steht dabei jeweils für ‚Packet'. Zwar bedeuten diese zusätzlichen Kanäle für das Endgerät einen zusätzlichen Aufwand, dafür können jedoch die leitungsvermittelnden Signalisierungskanäle des Radionetzwerkes entlastet werden. Außerdem wird die BSC entlastet, da diese bei NOM 3 keine GPRS Signalisierungsnachrichten zwischen Teilnehmer und GPRS Netzwerk weiterleiten muss. Der Timeslot, auf denen sich diese Packet Signalisierungskanäle befinden, werden über die Switching Matrix in der BSC zum GPRS Netzwerk getunnelt, was mit wesentlich weniger Aufwand verbunden ist, als einzelne Signalisierungsnachrichten weiterzugeben.

NOM 1

Und schließlich gibt es noch den Network Operation Mode 1 (NOM 1). Dieser verwendet entweder die GSM Signalisierungskanäle (wie bei NOM 2) oder optional die GPRS Signalisierungskanäle (wie bei NOM 3).

Zusätzlich wird in NOM-1 das Gs Interface zwischen der MSC im leitungsvermittelnden GSM Teil des Netzwerkes und dem SGSN (Serving GPRS Support Node) im GPRS Teil des Netzwerkes eingeführt. Der SGSN ist dabei das paketvermittelnde Gegenstück der MSC und ist neben dem Vermitteln von Datenpaketen auch für das Mobility Management und Session Management der Teilnehmer zuständig. Mehr dazu in Kapitel 2.7.

Über das Gs Interface ist es möglich, GSM und GPRS Signalisierungsvorgänge zu synchronisieren und zusammenzufassen. Dies hat folgende Vorteile:

- Bei eingehenden Gesprächen sucht die MSC den Teilnehmer nicht direkt über die BSC mit einer Paging Nachricht, sondern schickt die Paging Nachricht stattdessen an den SGSN, der dann seinerseits den Teilnehmer benachrichtigt. Dies hat den großen Vorteil, dass auch ein Endgerät der Mobile Station Class B während eines aktiven GPRS Datentransfer über das eingehende Gespräch informiert werden kann.
- Location Area Update und Routing Area Update müssen nicht mehr getrennt für GSM und GPRS durchgeführt werden. Bei Bedarf erfolgt ein Combined Location Update mit dem SGSN. Der SGSN gibt die Daten während

des Vorgangs dann auch an das MSC/VLR weiter. Während der Vorgang im Netzwerk dadurch etwas komplizierter wird, vereinfacht sich der Vorgang für das Endgerät, da die Prozedur statt zweimal nur noch einmal durchgeführt werden muss. Außerdem werden weniger Signalisierungsressourcen im Radionetzwerk benötigt.

Gs MAP Signalisierung

Die Signalisierung auf dem Gs Interface erfolgt über das in Kapitel 1.4.2 vorgestellte MAP Protokoll, das für diese Zwecke erweitert wurde.

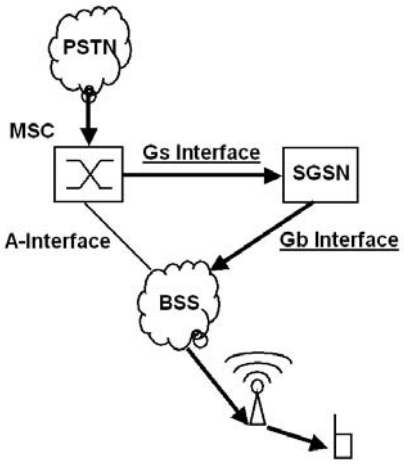

Abb. 2.10: Paging für ein eingehendes Gespräch über das Gs Interface

Während bei der Einführung von GPRS im Feld zunächst bei den meisten Netzwerkbetreibern auf NOM 2 gesetzt wurde, werden mit der Zeit die meisten GSM Netze auch das Gs Interface durch einen Softwareupdate der MSC und SGSN nutzten können. Da die Verwendung dieses Interfaces sowohl für den Kunden wie auch für den Netzbetreiber zahlreiche Vorteile bringt ist zu erwarten, dass die meisten Netzwerke mit der Zeit auf diesen GPRS Netzwerkmodus umschalten werden. Vorreiter ist hier z.B. T-Mobile in Österreich, der NOM 1 als einer der ersten Netzwerkbetreiber bereits seit 2003 einsetzt.

Welcher Network Operation Mode vom Netzwerk verwendet wird, erfahren die Endgeräte über den Broadcast Kanal (BCCH bzw. PBCCH) der Zelle in der SYS_INFO 13 Nachricht.

2.3.7 GPRS Kanalstruktur auf der Luftschnittstelle

Mit GPRS wurden für die Datenübertragung und Signalisierung folgende neue logische Kanäle auf der Luftschnittstelle eingeführt:

PDTCH Wichtigster Kanal aus Endnutzersicht ist sicherlich der Packet Data Traffic Channel (PDTCH), welcher bei GPRS die eigentlichen Nutzdaten überträgt. Dieser Kanal wird in Uplink wie auch in Downlinkrichtung verwendet. Up- und Downlinkrichtung werden jedoch unabhängig voneinander vom Netzwerk zugewiesen. Der PDTCH verwendet ähnlich einem leitungsvermittelten GSM Traffic Channel (TCH) bis auf wenige Ausnahmen alle Bursts eines Timeslots (GPRS 52 Multiframe).

PACCH Zu jedem PDTCH gehört auch ein Packet Associated Control Channel (PACCH). Der PACCH ist ein bidirektionaler Kanal und wird für die Übertragung von Signalisierungsnachrichten verwendet. Diese sind zum Beispiel notwendig, um den korrekten Empfang von Datenpaketen zu bestätigen. Außerdem wird die Ressourcezuteilung (also die Zuweisung von Blocks eines PDTCH an einen Teilnehmer) mit Uplink und Downlink Assignment Nachrichten über diesen Kanal gesteuert. Ein PACCH wird auf den gleichen Timeslots wie ein PDTCH übertragen. Um den PACCH und den PDTCH zu unterscheiden, gibt es im Header jedes Datenpakets wie in Abbildung 2.11 dargestellt, ein Payload Type Feld.

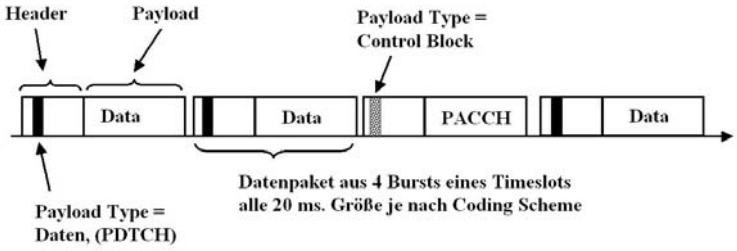

Abb. 2.11: PDTCH und PACCH werden wahlweise auf dem gleichen Timeslot gesendet.

PTCCH Der Packet Timing Advance Control Channel (PTCCH) wird für die Timing Advance Kontrolle von aktiven Endgeräten verwendet. In vom Netzwerk vorgegebenen Intervallen senden die aktiven Endgeräte in Uplink Richtung des PTCCH einen kurzen Burst, der vom Netzwerk für die Berechnung des Timing Advan-

ce verwendet wird. Das Ergebnis wird dann den Endgeräten in Downlinkrichtung des PTCCH mitgeteilt.

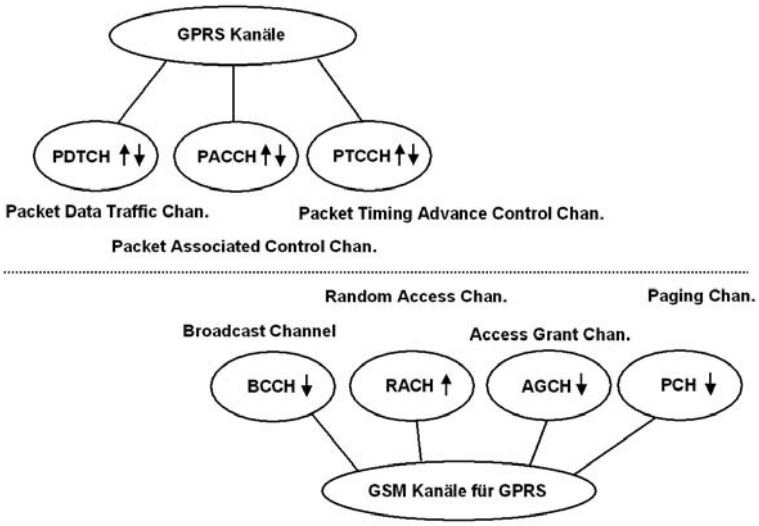

Abb. 2.12: Logische Kanäle in NOM 2 für GPRS

Im Network Operation Mode 2 werden neben diesen Kanälen auch folgende bereits existierende GSM Kanäle verwendet (vgl. Kapitel 1.7.3):

RACH Der Random Access Channel (RACH) wird bei GPRS für die Anforderung von Uplink Ressourcen (Blocks auf dem Uplink PDTCH) verwendet. Statt einer GSM Channel Request Nachricht wird dafür jedoch eine Packet Channel Request Nachricht gesendet.

AGCH Der PACCH kann nur für die Ressourcezuteilung an ein Endgerät verwendet werden, wenn diesem bereits Datenblocks in der jeweils anderen Richtung zugeteilt wurden. Für eine neue Ressourcezuteilung wird der GSM Access Grant Channel (AGCH) verwendet.

Abbildung 2.13 zeigt die Verwendung von RACH, AGCH und PACCH bei der Zuteilung von Uplink Ressourcen und die anschließende Datenübertragung über den PDTCH. Weitere Details hierzu in Kapitel 2.5 über das Radio Resource Management.

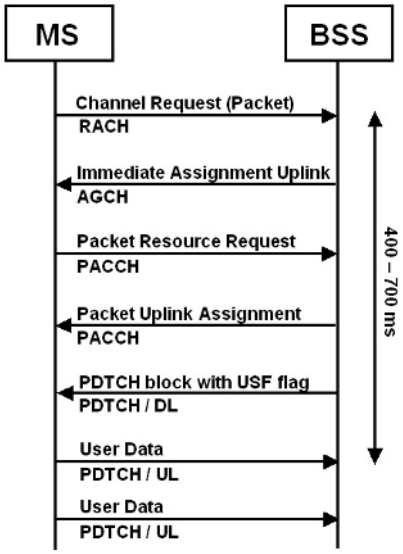

Abb. 2.13: Anforderung einer Uplink Ressource in NOM 2

PCH

Ist ein Endgerät für längere Zeit inaktiv, geht es in den Standby Mode über, der in Kapitel 2.3 näher beschrieben wird. Im Standby Mode ist es nicht mehr möglich, dem Endgerät unmittelbar Ressourcen über den AGCH zuzuteilen. In diesem Zustand muss deshalb das Endgerät zunächst über den Paging Channel gerufen werden.

SYS_INFO 13

Auch der Broadcast Kanal (BCCH) wird für GPRS verwendet. Neben den schon bisher bekannten SYS_INFO Nachrichten mit GSM Systeminformationen wird für GPRS nun noch zusätzlich die GPRS spezifische SYS_INFO 13 Nachricht ausgestrahlt. Diese enthält alle für das Endgerät wichtigen GPRS Parameter wie zum Beispiel den Network Operation Mode oder den Routing Area Code.

PCCCH (optional)

Neben diesen Kanälen gibt es noch eine Reihe weiterer Kanäle, die nur in NOM 3 und optional auch in NOM 1 verwendet werden. Diese Kanäle dienen vor allem der Entlastung von RACH, AGCH und PCH und werden entsprechend PRACH, PAGCH und PPCH genannt, wobei ‚P' jeweils für Packet steht. Zusammengefasst werden diese Kanäle auch als Packet Common Control Channel (PCCCH) bezeichnet. Da der PCCCH nicht von der BSC kontrolliert wird, bedeutet dessen Verwendung auch eine Entlastung der BSC. Nachteil ist jedoch, dass der PCCCH in der Praxis

einen eigenen Timeslot benötigt und somit die Bandbreite einer Zelle für Nutzdaten reduziert. In der Praxis scheint die Signalisierungslast für die BSC nicht kritisch zu sein und so wird der PCCCH in den meisten in Betrieb befindlichen Netzwerken nicht verwendet.

PBCCH (optional)

Ist in einer Zelle der PCCCH aktiviert, reicht der Platz in der SYS_INFO 13 Nachricht auf dem BCCH nicht aus, um dem Endgerät alle GPRS Informationen mitzuteilen. Deshalb muss bei Aktivierung des PCCCH im Radionetzwerk auch ein Packet Broadcast Control Channel (PBCCH) verwendet werden.

2.4 GPRS Zustandsmodell

Bei GSM befindet sich ein am Netzwerk angemeldetes Endgerät entweder im Idle Mode oder im Dedicated Mode. Im Idle Mode gibt es keine Verbindung zwischen Endgerät und Netzwerk und das Endgerät überprüft nur von Zeit zu Zeit den Paging Kanal. Im Dedicated Mode hingegen existiert zwischen Endgerät und Netzwerk eine aktive Verbindung (z.B. ein Telefongespräch) und es werden in regelmäßigen Abständen Daten gesendet und empfangen. Für GPRS wurde dieses Zustandsmodell für die Anforderungen der Paketdatenübertragung etwas modifiziert:

Idle State

Im Idle State ist das Endgerät nicht am GPRS Netzwerk angemeldet, der Aufenthaltsort des Teilnehmers ist nicht bekannt. Somit kann der Teilnehmer keine Daten übertragen, es ist keine GPRS Session (auch PDP Kontext genannt, siehe Kapitel 2.7.2) aktiv. Leider birgt die Bezeichnung Idle State bei GPRS ein großes Verwechslungsrisiko mit dem GSM Idle Mode. Während im GSM Idle Mode das Endgerät eingebucht aber im Ruhezustand ist und somit jederzeit erreicht werden kann, ist ein Endgerät im GPRS Idle State nicht eingebucht und kann auch vom Netzwerk nicht angesprochen werden.

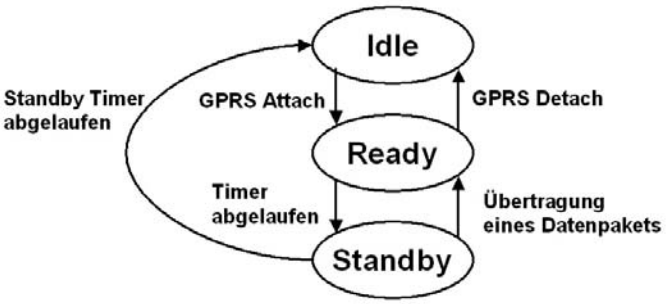

Abb. 2.14 GPRS Zustandsdiagramm

Ready State

Möchte sich ein Endgerät im GPRS Netzwerk einbuchen, wechselt es in den GPRS Ready State mit der Übertragung der Packet Channel Request Nachricht wie in Abbildung 2.13 gezeigt. Im Ready State kann das Netzwerk jederzeit Downlinkressourcen über den AGCH zuweisen und Daten an das Endgerät schicken. Dies ist möglich, da dem GPRS Netzwerk die Zelle bekannt ist, in dem sich der Teilnehmer gerade aufhält. Dies bedeutet umgekehrt aber auch, dass das Endgerät jeden Zellwechsel dem Netzwerk durch eine Cell Update Nachricht mitteilen muss. Das Endgerät bleibt im Ready State, solange entweder Signalisierungsnachrichten oder Nutzdaten übertragen werden, sowie noch für einige Zeit nach dem Ende der Übertragung. So wird sichergestellt, dass nachfolgende Datenpakete ohne große Verzögerung zugestellt werden können. Über den Ready Timer wird die Zeit bestimmt, die ein Endgerät nach einer Datenübertragung noch im Ready State verbleibt. Sein maximaler Wert, auf den der Ready Timer nach jeder Datenübertragung zurückgestellt wird, ist Teil der GPRS Systeminformationen, die auf dem BCCH oder PBCCH ausgestrahlt werden. Ein typischer Wert des Ready Timers, der in vielen Netzwerken verwendet wird, ist 44 Sekunden. Nach Ablauf des Ready Timers wechselt das Endgerät in den Standby State.

Der Ready State macht keine Aussage darüber, ob ein Teilnehmer Daten von und zum Internet übertragen kann. Hierfür wird ein sogenannter PDP Kontext benötigt, der in Kaptitel 2.7.2 beschrieben wird. Der Ready State bedeutet für das Endgerät und Netzwerk lediglich, dass Daten und Signalisierungsnachrichten sofort ohne vorheriges Paging an das Endgerät zugestellt werden können.

Mobility Management im Ready State

Der GPRS Ready State ähnelt stark dem GSM Dedicated Mode, da beide Zustände für die Übertragung von Daten gedacht sind. Im Falle des GSM Dedicated Mode sind dies vorwiegend Signalisierungs- und Sprachdaten, im GPRS Ready State hingegen neben der Signalisierung hauptsächlich IP Pakete. Während jedoch im GSM Dedicated Mode das Mobility Management durch die BSC (vgl. Handover) kontrolliert wird, bleibt diese Aufgabe im GPRS Ready State dem Endgerät überlassen.

Cell Update

Wie bei GSM führt das Endgerät auch bei GPRS Signalstärkemessungen der aktuellen Zelle sowie aller Nachbarzellen durch. Bei Bedarf startet das Endgerät dann ohne Hilfe oder Anweisung des Netzwerkes einen Zellwechselvorgang, der Cell Update genannt

wird. Nach Wechsel in die neue Zelle werden zunächst die Systeminformationen der Zelle aus deren Broadcast Kanal (BCCH oder PBCCH) ausgelesen. Danach nimmt das Endgerät über den RACH Kontakt zum Netzwerk auf und sendet ein leeres Datenpaket. Hieran erkennt das Netzwerk, dass der Teilnehmer die Zelle gewechselt hat und ändert die Route für nachfolgende Datenpakete entsprechend. Der komplette Cell Update Vorgang benötigt etwa 2 Sekunden. Wird ein Cell Update Vorgang während einer laufenden Datenübertragung durchgeführt, entsteht dadurch natürlich eine Unterbrechung der Übertragung von mindestens zwei Sekunden. Daten, die in Downlink Richtung während des Cell Updates in der alten Zelle übertragen wurden, müssen erneut gesendet werden. Für Anwendungen wie z.B. dem Webbrowsing stellt der Cell Update kein großes Problem dar, da die meiste Zeit keine Daten übertragen werden und somit die meisten Cell Updates in Zeiten ohne Übertragungsaktivität fallen. Problematisch sind diese Unterbrechungen jedoch für Echtzeitdienste wie z.B. Voice over IP.

NACC

Um die Unterbrechungen bei Cell Updates so kurz wie möglich zu halten, wurde in den GPRS Standards nachträglich noch ein Verfahren eingebracht, das sich Network Assisted Cell Change, kurz NACC nennt. Bei diesem Verfahren kündigt das Endgerät einen bevorstehenden Zellwechsel dem Netzwerk an. Dieses kann dann die Systeminformationen der neuen Zelle an das Endgerät schicken und eine laufende Datenübertragung in Downlink Richtung anhalten. Das Endgerät wechselt danach in die neue Zelle und sendet ein neues Datenpaket. Somit reduziert sich die Unterbrechungszeit wesentlich, da der BCCH der neuen Zelle nicht gelesen werden muss und auch keine Daten im Downlink verloren gehen, die in der neuen Zelle erneut gesendet werden müssten. Für dieses optionale Verfahren muss jedoch die Software sowohl im Netzwerk als auch im Endgerät entsprechend erweitert werden. Da NACC erst mit der GSM Release 4 spezifiziert wurde, sind bei Drucklegung dieses Buches zwar schon einige Endgeräte erhältlich die dieses Verfahren unterstützen, auf der Netzwerkseite ist diese Funktionalität jedoch noch nicht sehr weit verbreitet.

Standby State

Nach Ablauf des Ready Timers wechselt das Endgerät in den Standby State. In diesem Zustand informiert das Endgerät das Netzwerk nur noch über einen Zellwechsel, wenn die neue Zelle zu einer neuen Routing Area gehört. Nachteil ist jedoch, dass bei ankommenden Daten der Teilnehmer erst über den PCH in der gesamten Routing Area gesucht werden muss. Eine Routing Area

ist ein Teil einer Location Area, besteht also auch aus einer Anzahl Zellen. Eigentlich hätten auch die Location Areas auch für GPRS weiterverwendet werden können. Durch die feinere Unterteilung einer Location Area in eine oder mehrere Routing Areas gibt man den Netzbetreibern aber die Möglichkeit, die richtige Balance zwischen Nutzung des Paging Channels bei ankommenden Daten und die Häufigkeit der Routing Area Updates unabhängig von GSM zu kontrollieren.

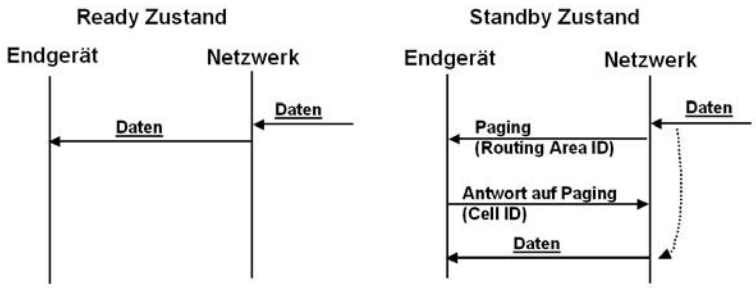

Abb. 2.15: Unterschied zwischen Ready und Standby Zustand

Routing Area Update

Ändert sich bei einem Zellwechsel nur die Routing Area, führt das Endgerät einen Routing Area Update mit dem GPRS Netzwerk durch. Ändert sich neben der Routing Area auch gleichzeitig die Location Area, führt das Endgerät zusätzlich noch einen Location Area Update durch. Auch im Ready State ist bei einem Zellwechsel statt eines Cell Updates ein Routing und Location Area Update notwendig, wenn sich diese bei einem Zellwechsel ändern.

Paging im Standby State

Vorteil des Standby State ist der geringere Signalisierungsaufwand und somit für die Endgeräte eine längere Akkulaufzeit. Für das Netzwerk hat dies den Vorteil, dass knappe Signalisierungsressourcen auf dem RACH, AGCH und PDTCH gespart werden. Nachteil ist jedoch, dass bei ankommenden Daten das Endgerät erst über den Paging Channel gerufen werden muss, was zusätzlich Zeit kostet. Da bei üblichen Ready Timer Werten von z.B. 44 Sekunden in den meisten Fällen keine Daten mehr nachkommen, muss der Paging Channel in der Praxis nicht sehr oft verwendet werden.

In Uplink Richtung gibt es keinen Unterschied zwischen Ready und Standby State. Möchte ein Endgerät im Standby State Daten schicken, geht das Endgerät mit dem Senden des ersten Pakets automatisch wieder in den Ready State über.

2.5 GPRS Netzwerkelemente

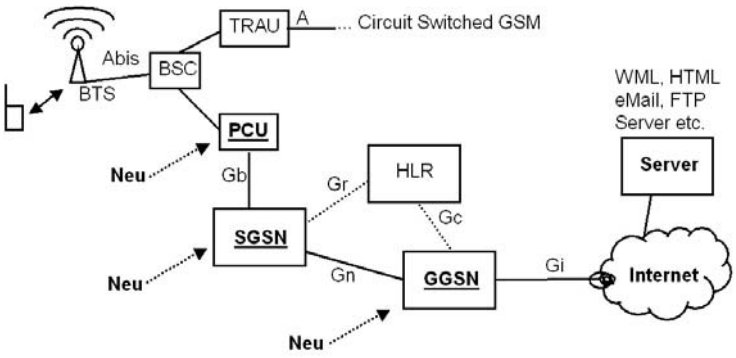

Abb. 2.16: GPRS Netzkomponenten

Durch Einteilung der Timeslots für GSM und GPRS im Radionetzwerk ist es möglich, beide Dienste über die gleichen Basisstationen zu betreiben. Hierzu ist lediglich ein Softwareupdate für die Basisstationen und BSCs notwendig. Aufgrund der großen Unterschiede zwischen Leitungs- und Paketvermittlung wurde es jedoch notwendig, drei neue Netzwerkkomponenten für GPRS in das vorhandene Netzwerk zu integrieren. Diese werden in Abb. 2.16 gezeigt und in diesem Abschnitt näher beschrieben.

2.5.1 Die Packet Control Unit (PCU)

Der Base Station Controller (BSC) ist Teil des leitungsvermittelnden GSM Netzwerkes und verbindet Endgeräte über 16 kbit/s Kanäle mit der MSC im Kernnetzwerk. Außerdem ist der BSC für das Handover der Verbindungen zuständig. Da GPRS Teilnehmer jedoch keine dedizierte 16 kbit/s Verbindung mehr mit dem Netzwerk haben, ist die Architektur der BSC nicht für GPRS geeignet. Aus diesem Grund wurde die Packet Control Unit (PCU) im Netzwerk eingeführt, die das paketvermittelnde Gegenstück zur BSC im Radionetzwerk darstellt. Die PCU hat folgende Aufgaben:

PDTCH Management

Die Vergabe von Timeslots, respektive PDTCHs in Up- und Downlink Richtung an die einzelnen Teilnehmer: In NOM 2 werden Uplinkressourcen mit einer Packet Channel Request Nachricht über den RACH angefordert. Die BSC empfängt diese

Nachrichten und leitet sie an die PCU weiter. Dieser Umweg ist notwendig, da über den RACH auch GSM Kanalanforderungen gesendet werden, die von der BSC selber bearbeitet werden. In NOM 3 hingegen wird für Packet Channel Request Nachrichten der PRACH verwendet. Dieser ist direkt mit der PCU ohne Zwischenstop über die BSC verbunden, da hier nur GPRS Signalisierung übertragen wird.

Flusskontrolle

Da über eine Zelle viele Teilnehmer gleichzeitig Daten übertragen können, ist die PCU auch für die Flusskontrolle der Daten in Up- und Downlink Richtung zuständig, sowie für die Priorisierung der unterschiedlichen Datenströme.

Fehlerkorrektur

In Uplinkrichtung überprüft die PCU die ankommenden Datenblocks und fordert bei Übertragungsfehler ggf. die Daten erneut beim Endgerät an.

Paging

Befindet sich ein Teilnehmer im Standby State, ist die PCU auch für das Paging verantwortlich, wenn vom Netzwerk neue Daten für die Übertragung bereitstehen.

Timing Advance Management

Um sicherzustellen, dass Datenpakete von Endgeräten in ihren vorgesehenen Zeitfenstern an der BTS eintreffen, ist die PCU auch für das grundsätzliche Timing Advance Management zuständig. Bei Vergabe von Up- und Downlinkressourcen teilt die PCU dem Endgerät mit, wann es den Packet Timing Advance Control Channel (PTCCH) für Timing Advance Messungen verwenden darf. Die eigentlichen Timing Advance Messungen auf dem PTCCH sowie die Berechnung und Übertragung der Werte an das Endgerät werden jedoch von der BTS autonom ausgeführt.

Wie in Abb. 2.16 zu sehen ist, ist die PCU mit dem BSC über E-1 Leitungen verbunden. Die für GPRS reservierten Timeslots für PDTCHs werden zwischen BSC und PCU über transparente 16 kbit/s E-1 Subtimeslots geleitet. Signalisierungsnachrichten von und zu den logischen Signalisierungskanälen RACH, AGCH und PCH werden separat über LAPD Signalisierungskanäle (siehe auch Ende Kapitel 1.7.3) zwischen PCU, BSC und BTS transportiert.

Aufzeichnen der Signalisierung

Im GSM Radionetzwerk ist es sehr einfach, Signalisierungsnachrichten für die Fehleranalyse und Lastmessungen aufzuzeichnen. Jedes Paket, das auf dem für LAPD reservierten Timeslot übertragen wird, ist dabei eine Signalisierungsnachricht. Wenn bekannt ist, auf welchem Timeslot der LAPD Kanal übertragen wird, kann dieser mit Hilfe eines Netzwerkanalysetools wie z.B. von Tektro-

nix, Acterna oder NetHawk überwacht werden. Diese Tools funktionieren sehr ähnlich wie Ethernet Netzwerkanalyseprogramme wie z.B. Ethereal. Einzige Hürde für das Monitoring ist dabei das Anzapfen der E-1 Leitung mit spezieller Hardware, die aufgrund der geringen Stückzahl und hohen Entwicklungskosten sehr teuer ist.

Bei GPRS ist die Aufzeichnung der Signalisierungspakete jedoch deutlich schwieriger geworden. Neben der Signalisierung auf dem RACH, AGCH und PCH werden die meisten Signalisierungsnachrichten in PACCHs gesendet. Diese werden zusammen mit PDTCHs für Nutzdaten über die gleichen Timeslots übertragen. Erschwerend ist außerdem, dass Signalisierungspakete je nach Multislot Klasse des Endgeräts über mehrere Timeslots gleichzeitig übertragen werden. Das Netzwerkanalysetool kann nun nicht mehr einfach alles aufzeichnen, sondern muss aus den Datenströmen die Signalisierungsnachrichten extrahieren und zusammenfügen.

Interface zwischen PCU und BSC

Einzige Schnittstelle die bei GPRS nicht standardisiert ist, ist die Schnittstelle zwischen PCU und BSC. Dies bedeutet, dass der Hersteller der BSC auch automatisch der Lieferant der PCU sein muss. Während manche Hersteller wie z.B. Siemens die PCU als zusätzliche Baugruppe in ihre BSC integrieren, haben andere Hersteller die PCU als eigenständige Komponente entwickelt, die aufgrund ihrer Leistungsfähigkeit auch Basisstationen von mehreren BSCs versorgen kann.

2.5.2 Der Serving GPRS Support Node (SGSN)

Der Serving GPRS Support Node (SGSN) ist das Gegenstück zur leitungsvermittelnden MSC im paketorientierten GPRS Netzwerk. Er erfüllt im wesentlichen die gleichen Aufgaben, die sich in die Teilbereiche User Plane und Signalling Plane unterteilen lassen:

User Plane

Die User Plane ist für die Übertragung von Nutzdatenpaketen zwischen Teilnehmern und externen Netzwerken wie dem Internet oder einem Firmenintranet zuständig. Alle Pakete, die beim SGSN für einen Teilnehmer eingehen, werden an die für die aktuelle Zelle des Teilnehmers zuständige PCU weitergeleitet (‚geroutet'). Liefert die PCU Pakete eines Teilnehmers, reicht der SGSN diese an den nächsten Netzwerkknoten, den Gateway GPRS Support Node (GGSN) weiter, der im nächsten Abschnitt beschrieben wird.

IP im Kernnetz

Im GPRS Kernnetz wird zwischen den unterschiedlichen Netzwerkkomponenten IP als Transportprotokoll verwendet. Dies hat den großen Vorteil, dass eine Vielzahl unterschiedlicher Übertragungstechnologien verwendet werden können. Für kurze Distanzen zwischen den GPRS Netzwerkknoten können zum Beispiel 100 MBit/s Ethernetverbindungen verwendet werden. Für die Übertragung über weite Strecken ist hingegen ATM über optische STM Übertragungssysteme (z.B. STM-1 mit 155 MBit/s, vgl. Kapitel 1.3) besser geeignet. Die Verwendung von IP im Kernnetz stellt also sicher, dass bei steigender GPRS Nutzung das Kernnetz auch in Zukunft flexibel ausbaubar bleibt.

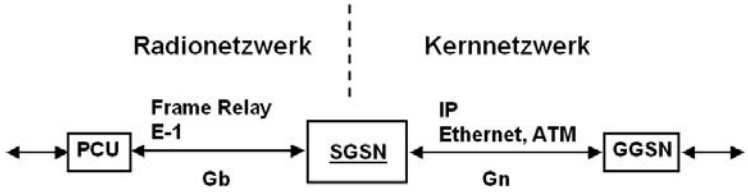

Abb. 2.17: Schnittstellen und Protokolle des SGSN auf Layer 2+3

Frame Relay zur PCU

Von und zur PCU wurde das Frame Relay Protokoll für den Transport der Userdatenpakete gewählt. Die Entscheidung, hier nicht auch das IP Protokoll zu verwenden, ist aus heutiger Sicht nur schwer nachvollziehbar. Die Wahl auf Frame Relay fiel unter anderem deswegen, da Datenpakete zwischen SGSN und PCU wie im BSS üblich über E-1 Leitungen transportiert werden sollten. Frame Relay mit seiner paketorientierten Architektur und vielen Ähnlichkeiten zu ATM eignet sich gut für die Übertragung über 2 MBit/s E-1 Kanäle und wird seit vielen Jahren in der Weitverkehrstechnik eingesetzt. Nachteil ist allerdings neben einer komplizierteren Netzwerkarchitektur auch, dass der SGSN Datenpakete von der PCU aus einem Frame Relay Paket extrahieren und danach per IP weiter an den GGSN schicken muss und umgekehrt. Dies hat sich zwischenzeitlich auch in der Praxis gezeigt, weshalb bei UMTS zwischen Radionetz und Kernnetz nicht mehr auf Frame Relay sondern auf ATM und IP gesetzt wird.

Verschlüsselung

Während bei GSM leitungsvermittelte Verbindungen nur die Übertragung auf der Luftschnittstelle zwischen Endgerät und BTS verschlüsselt wird, werden GPRS Datenpakete zwischen Endgerät und SGSN durchgehend geschützt. Dies hat den Vorteil, dass

nun auch das Abis Interface geschützt ist, das oft über eine Mikrowellenverbindung läuft und somit leicht abhörbar ist. Nachteil ist jedoch, dass die Rechenleistung für die Verschlüsselung im Netzwerk nicht mehr über viele Basisstationen verteilt werden kann, sondern im SGSN konzentriert ist. Zwar gibt es in großen Mobilfunknetzwerken viele SGSN's, deren Anzahl ist jedoch bedeutend kleiner als die Anzahl der Basisstationen. Deshalb bieten SGSN Hersteller auch optionale Hardwarebaugruppen für die Verschlüsselung der Datenpakete an und steigern so die Routingkapazität eines SGSNs.

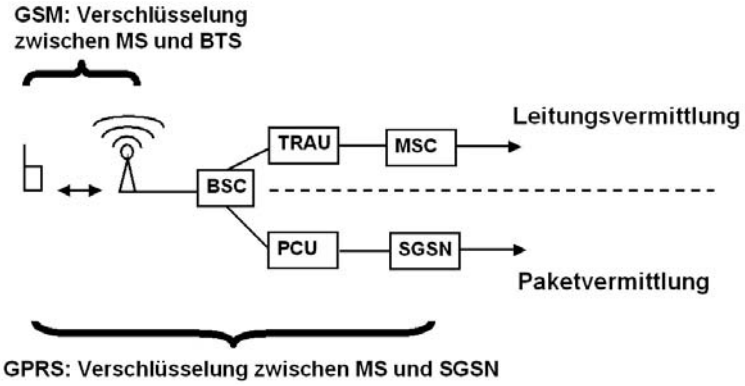

Abb. 2.18: Verschlüsselung in GSM und GPRS im Vergleich

Abgeschaltete Verschlüsselung in der Praxis

Wiedereinmal wurde in den Standards jedoch an der Sicherheit gespart und die Verschlüsselung als optional deklariert. Dies nutzen auch viele Netzbetreiber und verwenden keine GPRS Verschlüsselung. Vorteil der abgeschalteten Verschlüsselung für sie ist die höhere Teilnehmerkapazität pro SGSN.

Signalling Plane

Neben dem Weiterleiten von Daten zwischen mobilem Teilnehmern und dem GGSN ist eine weitere wichtige Aufgabe des SGSNs die Teilnehmersignalisierung. Diese Aufgabe wird von der Signalling Plane übernommen, die in zwei Bereiche aufgeteilt ist:

Session Management und PDP Context

Um als mobiler Teilnehmer Daten mit dem Internet auszutauschen, muss zunächst über das GPRS Netzwerk eine Datenverbindung aufgebaut werden. Diese Prozedur wird Packet Data Protocol (PDP) Context Activation genannt und ist Teil des Session Managements des SGSN. Aus Anwendersicht wird während der PDP Context Activation Prozedur dem Endgerät eine IP Adresse zugeteilt.

Mobility Management

Um am Netzwerk angemeldete Teilnehmer jederzeit erreichen zu können, ist der SGSN auch für die Verwaltung der Position jedes Teilnehmers in seinem Versorgungsbereich zuständig. Diese Aufgabe wird GPRS Mobility Management (GMM) genannt und ist dem Mobility Management der MSC sehr ähnlich. Zusammen mit der Session Management (SM) Komponente wird das zugehörige Protokoll auch GMM/SM genannt.

Billing

Um GPRS Dienste in Rechnung stellen zu können, sammelt der SGSN und der im Anschluss beschriebene GGSN die dazu nötigen Billing Information in Call Detail Records (CDR). Diese werden an einen Billing Server weitergeleitet. Die CDRs des SGSN sind vor allem bei Teilnehmern wichtig, die in einem ausländischen Netz roamen. Wie wir in Kapitel 2.7.2 noch genauer betrachten werden, ist bei einer GPRS Verbindung im Ausland der SGSN die einzige Komponente, die im ausländischen Netz einen CDR generieren kann. In diesem Fall dienen die CDRs des SGSN dem Netzbetreibern für die Abrechnung des Datenverkehrs des fremden Teilnehmers. Für Teilnehmer, die sich im Heimnetzwerk befinden, erzeugt hingegen auch der GGSN einen CDR und die Billing Informationen des SGSN sind somit nicht unbedingt erforderlich.

2.5.3 Der Gateway GPRS Support Node (GGSN)

Während der SGSN das Bindeglied zwischen Radionetzwerk und GPRS Kernnetz darstellt sowie die Mobilität der Teilnehmer verwaltet, verbindet der GGSN das GPRS Netzwerk mit dem Internet. Für Geschäftskunden kann der GGSN das GPRS Netzwerk auch direkt mit dem Intranet einer Firma verbinden.

Anchor Point der IP Verbindung

Der GGSN ist am Aufbau einer Internetverbindung, also dem Aufbau eines PDP Kontextes beteiligt und vergibt die IP Adressen. Danach fungiert der GGSN als fester Bezugspunkt (Anchor Point) der Verbindung. Bewegt sich ein Teilnehmer mit einem aktiven PDP Kontext in das Gebiet eines anderen SGSN, ändert das GPRS Netzwerk entsprechend das Routing der Datenpakete zwischen dem GGSN und dem neuen SGSN. Im Internet ist dies jedoch nicht sichtbar, da der GGSN während der Verbindung niemals gewechselt wird. Dies ist auch notwendig, da Router im Internet Datenpakete für eine IP Adresse immer an das gleiche Ziel weiterleiten und ihre Routing Tabellen für mobile Teilnehmer nicht anpassen können. Durch den GGSN wird also die Mobilität des Teilnehmers vor dem Internet versteckt. Abbildung

2.19 zeigt, wie sich eine Positionsänderung des Teilnehmers im GPRS Netzwerk auswirkt.

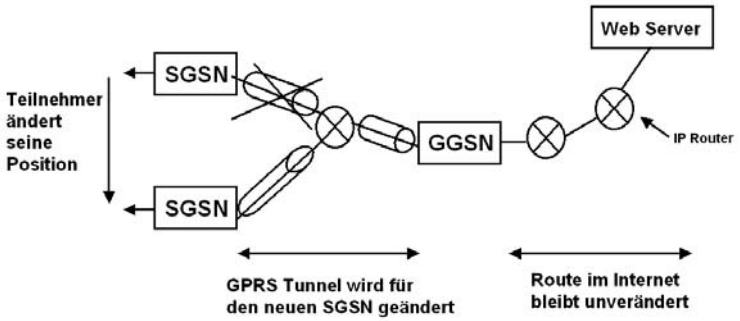

Abb. 2.19: Änderung des Aufenthaltsorts eines GPRS Teilnehmers

2.6 GPRS Radio Resource Management

Datentransfer auf der Luftschnittstelle

Wie in Abbildung 2.5 dargestellt wurde, kann ein Timeslot bei GPRS mehreren Teilnehmern gleichzeitig zugeordnet sein. Daten der unterschiedlichen Teilnehmer werden dann abwechselnd übertragen. Einem Teilnehmer können andererseits aber auch zur Steigerung seiner Übertragungsgeschwindigkeit mehrere Timeslots gleichzeitig zugeordnet sein. Die kleinste GPRS Übertragungseinheit ist dabei ein Block, der aus 4 Bursts eines Timeslots besteht.

RLC/MAC Header

Jeder Datenblock auf dem PDTCH oder PACCH besteht aus einem RLC/MAC (Radio Link Control/Medium Access Control) Header und einem Nutzdatenfeld.

Temporary Block Flow (TBF) im Downlink

Möchte das Netzwerk Daten an ein Endgerät senden, muss zuvor eine virtuelle Verbindung in Form eines Temporary Block Flow (TBF) zwischen Netzwerk und Endgerät aufgebaut werden. Dies geschieht durch Zuweisung eines Temporary Flow Identifier (TFI) in einer Packet Downlink Assignment Nachricht. Alle Datenblocks im Downlink, die für diesen Teilnehmer bestimmt sind, enthalten in ihrem RLC/MAC Header dann diesen TFI Wert. Abbildung 2.20 zeigt, wie mehrere Datenblocks nacheinander auf dem gleichen PDTCH übertragen werden. Datenblock 1 und 3 mit TFI=1 sind für das dargestellte Endgerät bestimmt. Datenblock zwei mit TFI=3 im RLC/MAC Header ist für ein anderes Endgerät bestimmt. Zwar empfängt das dargestellte Endgerät

auch diesen Datenblock, ignoriert diesen aber aufgrund des anderen TFI Wertes.

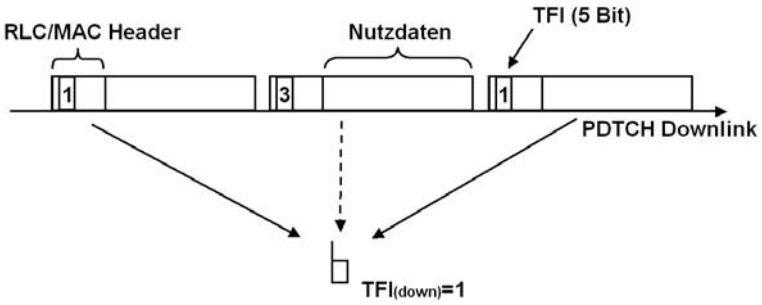

Abb. 2.20: Auswertung des TFI im Endgerät

Kontrollblocks für Downlink Daten

Die Bestätigung der Downlinkdatenblocks erfolgt über den Packet Associated Control Channel (PACCH) Uplink. Damit das Endgerät weiß, wann eine Bestätigung im Uplink gesendet werden darf, enthält ein Downlinkdatenblock des Teilnehmers im RLC/MAC Header die Information, in welchen Uplinkblocks die Bestätigungsmeldungen gesendet werden dürfen. Somit ist es möglich, Downlinkblocks zu bestätigen, ohne einen Uplink TBF zuzuteilen.

Final Block Indicator

Nachdem die PCU alle Daten eines Teilnehmers aus ihrer Sendequeue übertragen hat, wird der Downlink TBF beendet. Dazu wird im letzten Downlinkblock das Final Block Indicator Bit gesetzt. Nach Empfang des letzten Datenblocks beendet das Endgerät seine Empfangsbereitschaft und überprüft im Ready Zustand fortan nur noch den Access Grant Channel (AGCH) auf Zuteilung einer neuen Downlink Ressource.

TBF im Uplink

Auch in Uplinkrichtung muss für die Datenübertragung zuerst eine virtuelle Verbindung in Form eines Temporary Block Flows aufgebaut werden. Dem Endgerät wird wiederum wie in Downlinkrichtung ein TFI Wert zugewiesen. Dies geschieht über eine Packet Uplink Assignment Nachricht.

Uplink State Flag (USF)

Die Zuweisung eines TFI ist jedoch noch keine Sendeerlaubnis. Im Unterschied zu anderen Technologien wie z.B. Ethernet, darf ein GPRS Endgerät nur Daten senden, wenn es zuvor die Erlaubnis vom Netzwerk erhalten hat. In den Standards gibt es mehrere Möglichkeiten, wie diese Zuteilung (Allocation) erfolgen kann. Die heute gebräuchlichste Art ist die Dynamic Allocation. Dazu wird dem Endgerät in einer Packet Uplink Assignment

Nachricht neben den zugeteilten Timeslotnummern und seinem TFI Wert auch ein Uplink State Flag (USF) Wert übergeben. Das Endgerät überprüft fortan alle Downlinkdatenblocks in allen zugeteilten (Uplink-) Timeslosts, ob im RLC/MAC Header sein USF Wert enthalten ist. Findet das Endgerät seinen USF Wert, darf es im nächsten Uplinkblock Daten übertragen.

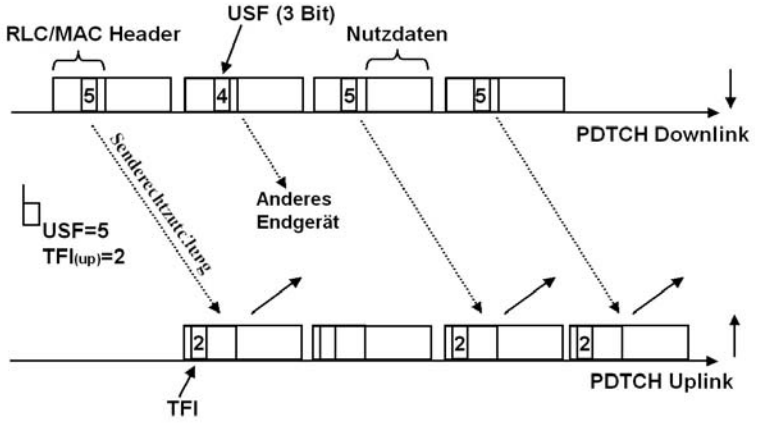

Abb. 2.21: Verwendung des Uplink State Flags.

Kontrollblocks für Uplink Daten

Während einem Endgerät ein Uplink TBF zugewiesen ist, muss das Netzwerk in Downlink Richtung die empfangen Datenblocks bestätigen. Dies geschieht über den Packet Associated Control Channel (PACCH) Downlink. Da der PACCH und PDTCH auf den gleichen Timeslots übertragen werden, dient das Payload Type Feld im RLC/MAC Header des Datenblocks der Unterscheidung dieser zwei logischen Kanäle. Da das Endgerät in den zugeteilten Timeslots wegen des Uplink State Flags sowieso die Datenblocks im Downlink mitlesen muss, können auch diese Kontrollnachrichten ohne zusätzlichen Aufwand empfangen werden.

Countdown Prozedur

Nachdem das Endgerät seinen Sendepuffer geleert hat, muss es dem Netzwerk signalisieren, dass keine weiteren Uplinkressourcen notwendig sind. Dies geschieht mit der Countdown Prozedur. Im RLC/MAC Header jedes Uplink Blocks befindet sich dazu ein 4 Bit Countdown Zähler, der bei der Übertragung jedes Blocks am Ende des Datentransfers vom Endgerät um 1 reduziert wird. Ist der Zähler bei 0 angekommen, vergibt die PCU keine Uplink Blocks mehr an den Teilnehmer und der Temporary Flow Identifier und das Uplink State Flag werden ungültig.

Extended Uplink TBF

Zwar ist die beschriebene Handhabung eines Uplink TBF sehr effizient, in der Praxis verursacht dieses Verfahren jedoch eine große Verzögerungszeit, wenn nur sporadisch Datenpakete gesendet werden. Dies wirkt sich z.B. bei der Übertragung von Webseiten in zweierlei Weise negativ aus: Zum einen werden die TCP Acknowledgement Pakete mit großer Verzögerung gesendet und verlangsamen so den Aufbau und Start einer TCP Verbindung. Da für eine Webseite üblicherweise mehrere TCP Verbindungen geöffnet werden, um paralell mehrere Elemente wie Bilder etc. zu laden, vervielfacht sich der Effekt. Aus diesem Grund wurde der GPRS Standard nachträglich um das sogenannte Extended Uplink TBF Verfahren erweitert. Unterstützen sowohl Netzwerk wie auch Endgerät das Verfahren, wird der TBF am Ende der Countdown Prozedur nicht automatisch geschlossen, sondern kann vom Netzwerk weiter offen gehalten werden. Dies ermöglicht dem Endgerät, neue Daten im Uplink ohne neue Ressoruceanforderung, also ohne Verzögerung zu senden. Tatsächlich kann man in der Praxis einen deutlichen Unterschied beim Aufbau von Webseiten gegenüber dem bisherigen Verfahren feststellen. Erste Endgeräte und Netzwerke, die das Extended Uplink TBF Verfahren unterstützen, wurden 2005 in der Praxis eingeführt.

```
[...]
          RLC/MAC PACKET TIMESLOT RECONFIGURE
000111--  Message Type : 7 = packet timeslot reconfigure
------00  Page Mode : 0 = normal paging
          Global TFI:
--01111-      Uplink Temporary Flow Identifier : 15
00------  Channel Coding Command : Use CS-1 in Uplink
          Global Packet Timing Advance:
----0001      Uplink TA Index : 1
101-----      Uplink TA Timeslot Number : 5
----0001      Downlink TA Index : 1
101-----      Downlink TA Timeslot Number : 5
---0----  Downlink RLC Mode : RLC acknowledged mode
----0---  CTRL ACK : 0 = downlink TBF already established
xxxxxxxx  Downlink Temporary Flow ID: 11
xxxxxxxx  Uplink Temporary Flow ID: 15
          Downlink Timeslot Allocation:
-0------      Timeslot Number 0 : 0
--0-----      Timeslot Number 1 : 0
---0----      Timeslot Number 2 : 0
----0---      Timeslot Number 3 : 0
-----1--      Timeslot Number 4 : 1 = assigned
------1-      Timeslot Number 5 : 1 = assigned
-------1      Timeslot Number 6 : 1 = assigned
0-------      Timeslot Number 7 : 0
          Frequency Parameters:
--000---      Training Sequence Code : 0
xxxxxxxx      ARFCN : 067
[...]
```

Abb. 2.22: Packet Timeslot Reconfiguration Nachricht

Abbildung 2.22 zeigt den Inhalt einer Timeslot Reconfiguration Nachricht, die für die Konfigurationsänderung eines bestehenden TBFs verwendet wird. Die gezeigte Nachricht teilt einem Endgerät 3 Timeslots in Downlink Richtung zu. Außerdem enthält sie neben den TFIs für Uplink und Downlinkrichtung weitere Informationen wie den zu verwendenden Timing Advance Wert und den Coding Scheme, den das Endgerät für Datenpakete in Uplinkrichtung verwenden soll.

2.7 GPRS Schnittstellen und Protokolle

Wie bereits in der Übersicht in Abbildung 2.16 dargestellt, werden die GPRS Netzwerkelemente über standardisierte und somit offene Schnittstellen miteinander verbunden. Mit Ausnahme der PCUs, die vom gleichen Hersteller wie die BSCs in einem Netzwerk sein müssen, können alle anderen Netzwerkkomponenten frei gewählt werden. Eine PCU von Nokia kann z.B. an einen SGSN von Nortel Networks angeschlossen werden, der wiederum mit einem GGSN von Cisco verbunden sein könnte. Natürlich können auch alle Komponenten auch vom gleichen Netzwerkhersteller sein, da die meisten Hersteller alle Komponenten eines GPRS Netzwerkes anbieten.

Abis Interface

Das Abis Interface verbindet die BTS mit dem BSC. Auf allen Timeslots, in denen im Radionetzwerk GPRS PDTCHs konfiguriert sind, kommt der Protokollstack wie in Abbildung 2.23 gezeigt, zum Einsatz. Üblicherweise werden die Daten transparent auf das nicht standardisierte Interface zwischen BSC und PCU weitergegeben. Auf den unteren Layern des Protokollstacks wird das RLC/MAC Protokoll für das Radio Ressource Management verwendet. Eine Protokollschicht höher sorgt das Logical Link Control Protocol (LLC) für das Framing der Nutzdatenpakete und Signalisierungsnachrichten (Mobility Management/Session Management). Optional sorgt das LLC Protokoll auch für eine gesicherte Verbindung zwischen Endgerät und SGSN durch einen Bestätigungsmechanismus für korrekt empfangene Blocks (Acknowledged Mode). Eine Stufe höher verpackt das Subnetwork Dependant Convergence Protocol (SNDCP) die IP Nutzdatenpakete für den korrekten Versand über das Radionetzwerk. Optional führt SNDCP auch eine Kompression der IP Header der Nutzdaten oder eine Kompression der kompletten Nutzdatenpakete durch. Diese elegante Art der Geschwindigkeitssteigerung wird leider nur von wenigen Endgeräten unterstützt. Der LLC Layer und alle höheren Schichten sind für die PCU, BSC und BTS

transparent, da sie für eine Ende zu Ende Verbindung im Radionetzwerk sorgen.

Gb Interface

Das Gb Interface verbindet den SGSN mit der PCU. Auf Layer 1 werden für dieses Interface hauptsächlich 2 MBit/s E-1 Verbindungen verwendet. Ein SGSN verwaltet in der Praxis mehrere PCUs, die jeweils mit mehreren 2 MBit/s Leitungen an den SGSN angeschlossen sind. Auf Layer 2 und 3 des Protokollstacks wird das Frame Relay Protokoll verwendet, das in der Telekommunikationswelt seit vielen Jahren zum Einsatz kommt und für den Versand von Paketdaten über E-1 Leitungen bestens geeignet ist. Nachteil ist jedoch, dass die Nutzdaten für den Versand über das Gb Interface in Frame Relay Pakete eingepackt werden müssen.

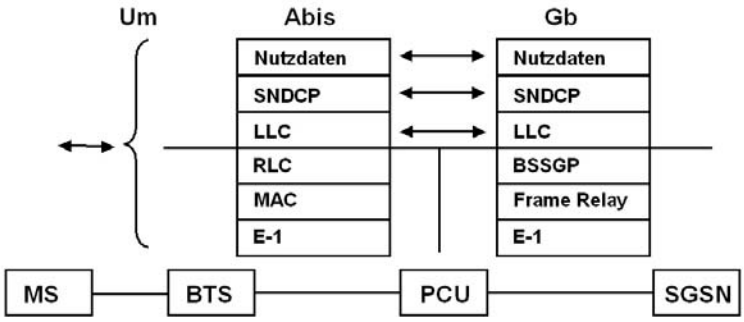

Abb. 2.23: GPRS Protokollstacks im Radionetzwerk

Gn Interface

Das Gn Interface verbindet SGSNs mit GGSNs innerhalb eines GPRS Netzwerkes und wird in 3GPP TS 29.060 spezifiziert. Je nach Größe des Netzwerkes besteht ein GPRS Netzwerk aus einem oder mehreren SGSNs. Auch die Anzahl der GGSNs, die üblicherweise aber geringer als die Anzahl der SGSNs ist, wird maßgeblich von der Anzahl der Nutzer des Netzwerks bestimmt.

Lastverteilung, Aufgabenteilung und Redundanz

Weiterhin ist es möglich, unterschiedliche GGSNs für unterschiedliche Anwendungen zu verwenden. Während ein oder mehrere GGSNs z.B. für Vertragskunden zuständig sein könnten, sind andere speziell auf die Bereitstellung des GPRS Dienstes für Prepaid Subscriber spezialisiert. Es spricht aber auch nichts dagegen, für alle Teilnehmer den gleichen GGSN zu verwenden. Oft werden auch aus Redundanzgründen mehrere GGSN im Netzwerk eingesetzt, die dann in unterschiedlichen Städten untergebracht sind. Beim Ausfall eines Standorts können neue Verbindungen automatisch umgelenkt werden.

IP als Grundlage für das Gn Interface

Auf Layer 3 des OSI Protokollstacks (Network Layer), wird auf dem Gn Interface das IP Protokoll für das Routing alle Nutzdatenpakete der Teilnehmer sowie für Signalisierungsnachrichten zwischen SGSNs und GGSNs verwendet. Werden SGSN und GGSN physikalisch nebeneinander aufgestellt, kommt auf den unteren Layern oft eine oder mehrere 100 Mbit/s Ethernet Verbindungen zum Einsatz. Für große Entfernungen wird von den Netzbetreiben jedoch ATM über STM Verbindungen (z.B. STM-1 mit 155 MBit/s) bevorzugt. Aus Redundanz und Kapazitätsgründen werden oft mehrere Leitungen parallel verwendet.

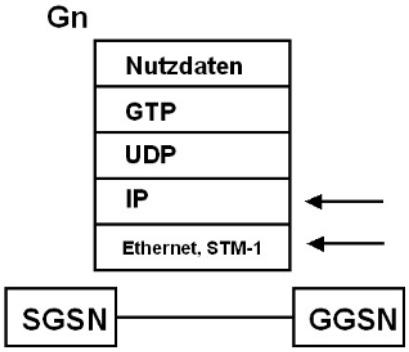

Abb. 2.24: Der Gn Protokoll Stack

GTP

Nutzdatenpakete der Teilnehmer werden auf dem Gn Interface nicht direkt, sondern in GPRS Tunneling Protocol (GTP) Paketen verpackt übertragen. Dies erzeugt zwar zusätzlichen Overhead im GPRS Kernnetz, ist aber aus folgenden Gründen notwendig:

Statisches Routing im Internet

Jeder Router im Internet zwischen GGSN und Ziel entscheidet anhand der IP Zieladresse des Datenpaketes und einer Routing Tabelle, wohin das Datenpaket weitergeleitet werden soll. Da sich die Position eines Teilnehmers im Internet nicht ändert, ist dieses Verfahren sehr effizient. Im GPRS Netzwerk kann dieses Verfahren jedoch nicht angewandt werden, da die Teilnehmer jederzeit ihren Standort wechseln können. Somit kann sich wie schon in Abbildung 2.19 gezeigt, die Route für die Datenpakete durch das GPRS Netzwerk jederzeit ändern. Da zwischen GGSN und SGSN beliebig viele IP Router geschaltet sein können, müsste in jedem Router im GPRS Netzwerk bei einer Positionsänderung des Teilnehmers das Routing für seine IP Adresse geändert werden. Um dies zu vermeiden, wird innerhalb des GPRS Netzwerkes nicht mit der Quell- und Ziel IP Adresse des Nutzdaten-

Dynamisches Routing im GPRS Netzwerk mit GTP

paketes geroutet, sondern es werden die IP Adressen von SGSN und GGSN verwendet. Das eigentliche Nutzdatenpaket wird zwischen dem SGSN und GGSN in ein GTP Paket eingepackt und läuft somit transparent durch das GPRS Netzwerk. Ändert sich später die Position des Teilnehmers, muss dem GGSN nur die IP Adresse des neuen SGSNs mitgeteilt werden. Der große Vorteil dieses Verfahrens ist somit, dass die Router zwischen SGSN und GGSN ihre Routing Tabellen nicht ändern müssen.

Abbildung 2.25 zeigt die wichtigsten Parameter der Protokollschichten eines Pakets auf dem Gn Interface. Die IP Adressen auf Layer 3 stammen vom SGSN und GGSN, während die IP Adressen des Nutzdatenpaketes, das in einem GTP Paket eingepackt ist, die IP Adressen des Teilnehmers und des angesprochenen Servers im Internet enthält. Dies bedeutet paradoxerweise, dass in einem GTP Datenpaket zwei IP Header vorhanden sind. Erhält der GGSN ein GTP Paket von einem SGSN, entfernt dieser alle Header inklusive des GTP Headers. Danach wird das vom Teilnehmer ursprünglich gesendete IP Paket auf dem Gi Interface zum Internet weitergesendet.

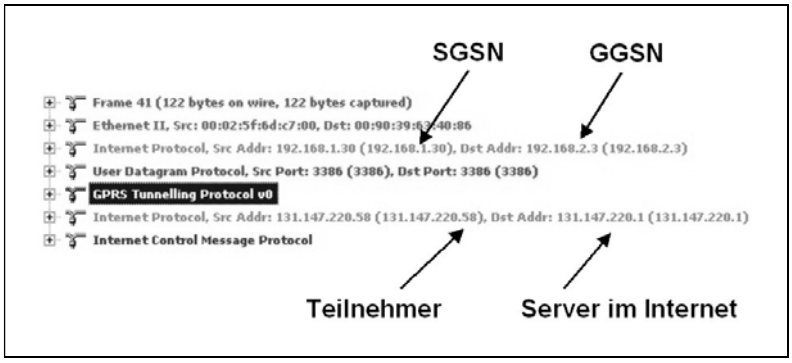

Abb 2.25: GTP Paket auf dem Gn Interface.

Gi Interface

Das Gi Interface verbindet das GPRS Netzwerk über den GGSN mit einem externen Netzwerk. Aus Sicht des externen Netzwerkes verhält sich der GGSN wie ein ganz normaler IP Router. Während die Nutzdaten der Teilnehmer innerhalb des GPRS Netzwerkes in GTP Pakete eingepackt werden, sind die Nutzdatenpakete auf dem Gi Interface wieder in ihrer originalen Form als IP Pakete auf Layer 3 präsent. Auf Layer 1 und 2 können je nach Anwendungsfall wieder Ethernet oder ATM über STM Verbindungen verwendet werden. Aus Redundanzgründen oder um

die verfügbare Bandbreite zu erhöhen, kann auch dieses Interface gleichzeitig über mehrere Verbindungen an den oder die nächsten Router im Internet oder dem Firmennetzwerk angeschlossen sein.

Gr Interface

Über das Gr Interface kommuniziert der SGSN mit dem HLR. Diese Verbindung ist nötig, da das HLR für jeden Teilnehmer dessen Berechtigungen für GPRS speichert. Dazu gehört unter anderem:

- Ob ein Teilnehmer den GPRS Dienst nutzen darf
- Welche Dienste von einem Teilnehmer verwendet werden dürfen (Access Point Names, APN)
- Internationales GPRS Roaming und Beschränkungen

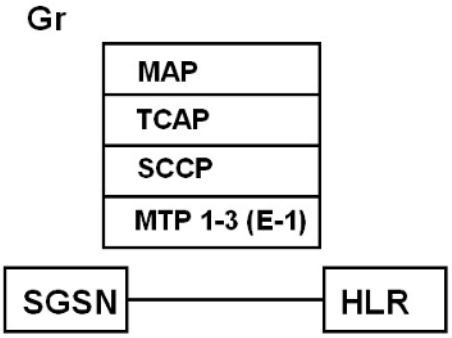

Abb. 2.26: Der Gr Protokoll Stack

Wie in Kapitel 1 gezeigt wurde, ist das HLR ein SS-7 Signalling Control Point (SCP). Aus diesem Grund ist das Gr Interface auf E-1 Trunks und dem SS-7 Protokol aufgebaut. Für die Signalisierungsnachrichten kommt das Mobile Application Part (MAP) Protokoll zur Anwendung, das auch die MSC für die Kommunikation mit dem HLR verwendet. Nachfolgend einige Beispiele für Nachrichten zwischen SGSN und HLR:

- Send Authentication Information: Diese Nachricht wird vom SGSN zum HLR geschickt, wenn sich ein Teilnehmer am Netzwerk anmeldet, um dessen Authentifizierungsdaten zu erhalten.

- Update Location: Mit dieser Nachricht informiert der SGSN das HLR, dass sich ein Teilnehmer in seinem Versorgungsgebiet angemeldet hat und erfolgreich identifiziert wurde.
- Insert Subscriber Data: Als Antwort auf die Update Location Nachricht liefert das HLR dem SGSN Informationen zurück, welche Dienste der Teilnehmer im GPRS Netzwerk verwenden darf.

Gp Interface

Das Gp Interface wird verwendet, um GPRS Netzwerke unterschiedlicher Länder miteinander zu verbinden und somit GPRS International Roaming zu ermöglichen. Das Gp Interface kann auch verwendet werden, um zwei nationale GPRS Netzwerke miteinander zu verbinden, falls zwei oder mehr Netzwerkbetreiber eines Landes Teile ihrer Netzwerkressourcen gemeinsam nutzen. Die Nutzdaten der Teilnehmer werden über das Gp Interface zwischen dem SGSN im besuchten Netzwerk und dem GGSN im Heimatnetzwerk in gleicher Weise wie über das netzwerkinterne Gn Interface übertragen.

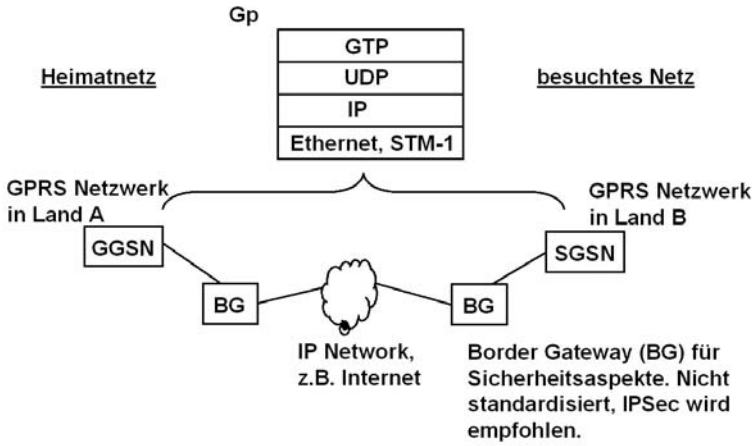

Abb. 2.27: Gp Interface für internationales Roaming

Einfaches Roaming mit GPRS

Befindet sich ein deutscher Teilnehmer z.B. in Spanien und nutzt GPRS für die Datenübertragung, werden seine Daten vom SGSN in Spanien an den GGSN im deutschen Heimatnetz übertragen. Von dort aus werden seine Datenpakete dann ins Internet weitergeleitet. Zunächst scheint dies wenig sinnvoll, da für die Daten des Teilnehmers theoretisch nicht nur der SGSN, sondern

auch der GGSN in Spanien genutzt werden könnte. Der große Vorteil der Verwendung des Gp Interfaces und des GGSN im Heimatnetzwerk des Teilnehmers ist jedoch, dass keine Einstellungen im Endgerät für das Roaming geändert werden müssen.

Die einfache Interneteinwahl im Ausland ohne jegliche Änderung der Konfiguration erweist sich in der Praxis als unschätzbarer Vorteil gegenüber bisherigen Vorgehensweisen. So scheitern Modemverbindungen im Ausland oft schon daran, dass entweder überhaupt kein Festnetzanschluss verfügbar ist, oder die entsprechenden Telefonkabel und Stecker nicht international kompatibel sind. Ist ein entsprechender Adapter vorhanden oder möchte der Reisende eine leitungsvermittelte GSM Datenverbindung verwenden, stellt sich als nächstes die Frage, über welchen Serviceprovider die Internetverbindung aufgebaut werden kann. Ein ausländischer Serviceprovider kommt in den meisten Fällen nicht in Betracht, da hier meist eine Anmeldung nötig ist. Bleibt der eigene Internetprovider im Heimatland, der aber nur zu teueren Roamingpreisen aus dem Ausland erreichbar ist. Oft ist auch das nicht möglich, da die nationalen Einwahlnummern mit spezieller Vorwahl aus dem Ausland nicht angerufen werden können.

SS-7 Verbindung für GPRS Roaming

Über das Gp Interface werden nur IP Nutz- und Signalisierungsdaten zwischen SGSNs und GGSNs unterschiedlicher GPRS Netzwerke ausgetauscht. Um GPRS Roaming zu ermöglichen, muss ein SGSN noch zusätlich über das Gr Interface auch Zugriff auf das HLR im Heimatnetzwerk des Teilnehmers haben.

Gs Interface

Das Gs Interface ist ein optionales Interface und verbindet die SGSNs des paketvermittelnden GPRS Teilnetzwerks mit den MSCs des leitungsvermittelnden GSM Netzwerkes. Die Vorteile, die sich durch Verwendung dieses Interfaces ergeben, wurden bereits in Kapitel 2.2.5 (Network Operation Mode 1) beschrieben.

2.8 GPRS Mobility und Session Management (GMM/SM)

Neben der Weiterleitung der Nutzdaten zwischen den Teilnehmern und dem Internet sind zwei weitere wesentliche Aufgaben des GPRS Netzwerkes die Mobilitätsverwaltung der Teilnehmer (Mobility Management) sowie die Kontrolle der Nutzdatenverbindungen (Session Management). Zu diesem Zweck wurden in den GPRS Standards auf den unterschiedlichen Interfaces Signalisierungsnachrichten und Signalisierungsabläufe definiert. Diese

Abläufe werden unter dem Begriff GPRS Mobility Management and Session Management, kurz GMM/SM zusammengefasst.

2.8.1 Mobility Management Aufgaben

GPRS Attach

Bevor über ein Endgerät eine Verbindung zu einem externen Netzwerk wie dem Internet aufgebaut werden kann, muss sich das Endgerät zunächst am GPRS Netzwerk anmelden. Dieser Anmeldevorgang wird GPRS Attach genannt und ist Abbildung 2.28 dargestellt. Das Endgerät beginnt diese Prozedur mit einer Attach Request Nachricht, die entweder seine IMSI oder die Packet Temporary Mobile Subscriber Identitiy (P-TMSI) enthält, die beim letzten Anmeldevorgang oder Routing Area Update vergeben wurde. Die P-TMSI wird auch Temporary Logical Link ID (TLLI) genannt. Somit wird die IMSI nur selten verwendet und die wahre Identität des Teilnehmers ist so nur dem Netzwerk bekannt.

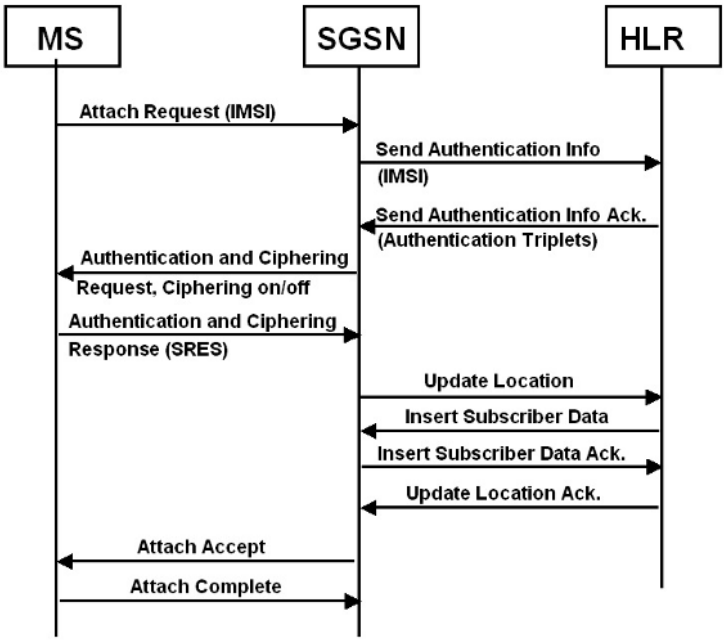

Abb. 2.28: GPRS Attach Message Flow

Sicherheit

Beim ersten Attach an einem SGSN mit der IMSI kennt der SGSN den Teilnehmer nicht. Deshalb fordert der SGSN daraufhin wie

in Abbildung 2.28 gezeigt, die Authentifizierungsdaten mit einer Send Authentication Information Nachricht beim HLR/Authentication Center (AC) an. Das HLR/AC liefert als Antwort ein oder mehrere Authentication Triplets, deren Erzeugung bereits in Kapitel 1.6.4 beschreiben wurde. Die zurückgegebene Zufallszahl RAND wird danach vom SGSN in einer „Authentication and Ciphering Request" Nachricht dem Endgerät übergeben. Das Endgerät berechnet dann in der SIM Karte die Antwort (SRES) und antwortet mit einer Authentication and Ciphering Response Nachricht. Im SGSN wird daraufhin die von Endgerät erhaltene Antwort mit der SRES des HLR/Authentication Centers verglichen. Stimmt sie überein, ist der Teilnehmer erfolgreich authentifiziert.

Während bei GSM die Verschlüsselung mit einer weiteren Nachricht aktiviert wird, enthält in GPRS schon die Authentication and Ciphering Request Nachricht diesen Befehl. Wird die Verschlüsselung also gleichzeitig mit der Authentifizierung aktiviert (optional), werden alle nachfolgenden Signalisierungs- und Nutzdatenpakete verschlüsselt von und zum SGSN übertragen.

Update Location und Insert Subscriber Data

Im nächsten Schritt informiert der SGSN das HLR über den Aufenthaltsort des Teilnehmers mit einer Update Location Nachricht. Das HLR sendet daraufhin die Daten des Teilnehmers mit einer Insert Subscriber Data Nachricht zum SGSN. Danach wird dem Endgerät die erfolgreiche Anmeldung mit einer Attach Accept Nachricht bestätigt und das Endgerät beendet den Dialog mit einem Attach Complete.

Abbildung 2.29 zeigt Auszüge aus dem Inhalt einer GPRS Attach Nachricht, die auf dem Gb Interface aufgezeichnet wurde. Die Nachricht enthält unter anderem die beim letzten Location Update oder Attach vergebene TMSI und Informationen über die letzte Position (MCC, MNC, LAC und RAC) des Teilnehmers. Außerdem enthält die Nachricht Informationen über die technischen Fähigkeiten des Endgeräts wie z.B. die Multislot Klasse, welche Frequenzbänder unterstützt werden (900 MHz, 1800 MHz,…), etc. Somit ist es möglich, mit der Zeit die GPRS Fähigkeiten neuer Endgeräte zu erweitern (z.B. bessere Multislot Klasse) und netzwerkseitig nur Funktionalitäten zu nutzen, die ein Endgerät auch unterstützt.

```
[...]
          Mobility Management: ATTACH REQUEST
            MS Network Capability:
1-------      GPRS encryption algorithm GEA/1: 1 = available
[..]
-----001    Attach Type : 001bin = GPRS attach
-100----    GPRS Ciphering Key Sequence Number : 100bin
            DRX Parameter
01000000      Split PG cycle code : 64 = 64
-----011      Non-DRX timer: max. 4 sec non-DRX mode after transfer state
----0---      SPLIT on CCCH: not supported
            Mobile Identity
-----100      Type of identity: TMSI
----0---      Parity: 0 = even
xxxxxxxx      TMSI: D4CC3EC4h
            Old Routing Area Identification
xxxxxxxx      Mobile Country Code: 232
xxxxxxxx      Mobile Network Code: 03
xxxxxxxx      Location area code: 6F32h
00000001      Routing area code: 0Fh
            MS Radio Access Capability
0001----      Access technology type: 1 = GSM E (900 MHz Band)
            Access capabilities
---100--        RF power capability: 4h
                A5 bits
-------1          A5/1: 1 = Encryption algorithm available
1-------          A5/2: 1 = Encryption algorithm available
-0------          A5/3: 0 = Encryption algorithm not available
[...]
------1-        ES IND : 1h = early Classmark Sending is implemented
[...]
                Multislot capability
xxxxxxxx          GPRS multi slot class: 4 (3 downlink + 1 uplink)
--0-----          GPRS extended dynamic allocation: not implemented
----1101          Switch-measure-switch value: 0
1000----          Switch-measure value: 8
xxxxxxxx      Access technology type: 3 = GSM 1800
xxxxxxxx      Access capabilities
001-----        RF power capability: 1
----1---        ES IND: 1 = early Classmark Sending is implemented
[...]
```

Abb. 2.29: Auszüge aus einer GPRS Attach Request Nachricht nach 3GPP TS 04.08, 9.4.1

Cancel Location

War der Teilnehmer zuvor bei einem anderen SGSN registriert, ist die Prozedur noch etwas umfangreicher. Vor Abschluss der Prozedur muss dann das HLR mit einer Cancel Location Nachricht zuerst die Daten im bisherigen SGSN löschen. Erst danach übergibt das HLR die Teilnehmerdaten an den neuen SGSN.

Gleichzeitiger GSM und GPRS Attach

Ist das Gs Interface zwischen MSC und SGSN im Netzwerk vorhanden (NOM 1), kann der GSM Attach und der GPRS Attach in einem Vorgang durchgeführt werden Dies beschleunigt den Vorgang für das Endgerät und reduziert den Signalisierungsaufwand im Radionetzwerk. Über das Gs Interface gibt der SGSN die Attach Nachricht auch an die für die Location Area des Teilnehmers zuständige MSC weiter.

Routing Area Update (RAU)

Die zweite wichtige Mobility Management Aufgabe ist der Routing Area Update (RAU). Ähnlich dem GSM Location Update muss dieser immer dann durchgeführt werden, wenn das Endgerät zu einer Zelle wechselt (Cell Update), die zu einer anderen Routing Area gehört. Eine Routing Area ist ein Teilbereich einer GSM Location Area oder kann mit ihr identisch sein. Die Durchführung des Routing Area Updates ist dem GSM Location Update sehr ähnlich (siehe Kapitel 1.8.1). Falls das Gs Interface zwischen MSC und SGSN vorhanden ist, kann der GSM Location Area Update und der GPRS Routing Area Update vom Endgerät gleichzeitig durchgeführt werden. Der SGSN gibt dann die entsprechenden Informationen an die zuständige MSC weiter.

Inter SGSN Routing Area Update (IRAU)

Wechselt ein Endgerät in eine Zelle, die in einer Routing Area eines neuen SGSNs liegt, findet aus Endgerätesicht ein ganz normaler Routing Area Update statt. Der neue SGSN kennt jedoch den Teilnehmer nicht und muss sich erst dessen Authentifizierungs- und Teilnehmerdaten besorgen. Da die Routing Area Update Nachricht Informationen über die vorherige Routing Area enthält, kann der neue SGSN danach beim alten SGSN diese Informationen anfordern. Dies dient auch gleichzeitig dazu, dass der bisherige SGSN bis auf weiteres alle vom GGSN eingehenden Nutzdatenpakete an den neuen SGSN weiterleitet, um möglichst keine Nutzdaten zu verlieren. Damit der GGSN in Zukunft seine Nutzdaten direkt an den neuen SGSN schickt, informiert der neue SGSN als nächstes den GGSN über den neuen Aufenthaltsort des Teilnehmers. Zum Schluss wird auch das HLR vom neuen Standort des Teilnehmers informiert und die Teilnehmerdaten im alten SGSN gelöscht. Details dieser Prozedur sind in 3GPP TS 23.060 in Kapitel 6.9.1.2.2 beschrieben.

2.8.2 GPRS Session Management

PDP Context Activation

Nachdem sich das Endgerät über die Attach Prozedur am Netzwerk angemeldet hat, kann nun für die Kommunikation mit dem Internet oder Firmenintranet ein sogenannter Packet Data Protocol (PDP) Kontext beim Netzwerk beantragt werden. Aus Sicht des Benutzers ist diese Prozedur nötig, um eine IP Adresse zu erhalten.

Packet Call

Eine paketvermittelnde Verbindung wird in Anlehnung an einen „Voice Call“ auch als „Packet Call“ bezeichnet, da im GPRS Netz die Paketverbindung ähnlich einer leitungsvermittelten Telefonverbindung explizit auf- und abgebaut wird. Großer Unterschied ist jedoch, dass bei einem Packet Call nur Ressourcen verwendet

werden, wenn tatsächlich Daten übertragen werden. Somit ist der PDP Kontext eines Packet Calls nur eine logische Verbindung, die nur physikalische Ressourcen benötigt, wenn auch tatsächlich Daten übertragen werden. Auch wenn keine Daten übertragen werden, kann der PDP Kontext über Minuten, Stunden oder sogar Tage aktiv bleiben. Dies wird auch als „Always On“ Funktionalität bezeichnet.

Access Point Name (APN)

Abbildung 2.30 zeigt den Ablauf einer PDP Context Activation Prozedur. Diese wird durch eine PDP Context Activation Request Nachricht vom Endgerät an den SGSN gestartet. Wichtigster Parameter ist der sogenannte Access Point Name (APN). Der APN dient dem SGSN dazu, den richtigen GGSN (Access Point) für den Übergang ins Internet für den Teilnehmer zu finden. Ein Netzbetreiber hat somit die Möglichkeit, viele unterschiedliche Dienste anzubieten. Dazu gehörten zum Beispiel:

- Eine direkte Verbindung mit dem Internet
- Eine direkte Verbindung mit dem Internet für Prepaid Kunden
- Eine IP Verbindung zu einem WAP Gateway
- Eine IP Verbindung zu einem WAP Gateway für Prepaid Kunden
- Eine direkte IP Verbindung zu einem Firmennetzwerk

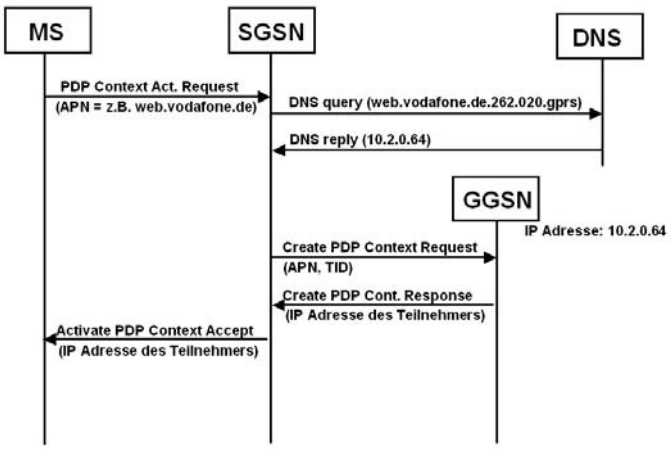

Abb. 2.30: Aufbau eines PDP Kontext

APN und das Domain Name System (DNS)

Der SGSN ermittelt mit dem übergebenen APN die IP Adresse des zu diesem APN gehörenden GGSNs. Für die Namensauflösung in eine IP Adresse verwendet das GPRS Netzwerk das Domain Name System (DNS). DNS Server werden auch im Internet verwendet, um z.B. beim Webbrowsen den Namen einer Website wie z.B. www.spiegel.de in die IP Adresse des Webservers der Spiegelredaktion umzuwandeln. Um die Adresse des GGSNs zu finden, geht der SGSN in genau gleicher Weise mit einem APN vor. Aus diesem Grund muss sich der Netzbetreiber bei der Vergabe von Namen für APNs auch an die Regeln der DNS Namensgebung halten. Um den APN international eindeutig zu machen, fügt der SGSN an das Ende des APN automatisch den Mobile Country Code (MCC) und den Mobile Network Code (MNC) aus der IMSI des Teilnehmers, sowie die Top Level Domain .gprs hinzu. Übergibt der Teilnehmer z.B. als APN den String „web.vodafone.de“ an das GPRS Netzwerk, ermittelt der SGSN über eine DNS Anfrage und den erweiterten APN „web.vodafone.de.262.020.gprs“ die IP Adresse des zuständigen GGSNs.

GPRS Roaming

Da der APN durch Anfügen des MCC und MNC weltweit eindeutig ist, kann ein Teilnehmer ohne Änderungen seiner GPRS Einstellungen auch in einem ausländischen Netz roamen. Damit die internationale APN Namensauflösung erfolgreich ist, müssen alle Domain Name Server der zusammengeschalteten GPRS Netzwerke verbunden und kaskadiert sein. Weiterhin muss für das GPRS Roaming auch eine SS-7 Signalisierungsverbindung mit dem HLR im Heimatnetzwerk für die Attach Prozedur vorhanden sein (Gr Interface), sowie eine IP Verbindung für die Nutzdaten und Signalisierungsdaten zwischen SGSN und GGSN (Gp Interface).

Tunnel ID (TID)

Nachdem die IP Adresse des für den APN zuständigen GGSNs bekannt ist, leitet der SGSN die PDP Context Activation Anforderung an den GGSN weiter. Teil dieser Nachricht ist der vom Teilnehmer gewünschte APN, sowie seine IMSI. Um später die Nutzdatenpakete des Teilnehmers transparent durch das GPRS Netzwerk leiten zu können (tunneln), vergibt der SGSN eine sogenannte Tunnel ID (TID) für diesen PDP Kontext. Diese ist ebenfalls Teil der Nachricht an den GGSN. Die TID wird dabei aus der IMSI des Teilnehmers und einem zwei Stellen langen Network Subsystem Access Point Identifier (NSAPI) zusammengesetzt. Der NSAPI ist notwendig, da ein Teilnehmer theoretisch

mehrere PDP Kontexte gleichzeitig aufgebaut haben kann. In der Praxis wird dies aber bisher nicht eingesetzt.

Zuteilung einer IP Adresse

Anhand der APN überprüft der GGSN, mit welchem Netzwerk der Teilnehmer verbunden werden soll. Optional gibt es noch die Möglichkeit, einen Benutzernamen und ein Passwort zwischen Teilnehmer und GGSN in der PDP Context Activation Nachricht auszutauschen. Dies wird in der Praxis von manchen Netzwerkbetreibern verwendet, was die Konfiguration des Endgeräts unnötig kompliziert. Stimmt auch der GGSN dem Verbindungswunsch zu, vergibt er für den PDP Kontext eine IP Adresse und schickt diese in einer PDP Context Activation Response Nachricht an den SGSN zurück. Außerdem speichert der GGSN für diese Verbindung folgende Informationen:

- TID des Teilnehmers
- IP Adresse des SGSN für den Austausch von Nutzdaten
- IP Adresse des SGSN für den Austausch von GPRS Signalisierungsdaten
- Die für den Teilnehmer vergebene IP Adresse

Nach Erhalt der PDP Context Activation Response Nachricht speichert der SGSN die IP Adresse des GGSNs in seinem Eintrag für den neuen PDP Kontext, da fortan alle Datenpakete des Teilnehmers an diese IP Adresse weitergeleitet werden. Im letzten Schritt schickt der SGSN eine PDP Context Activation Accept Nachricht an das Endgerät zurück und übergibt darin die vom GGSN zugewiesene IP Adresse.

Zusammenhang zwischen TFI, P-TMSI, TID und IP-Adresse

In den verschiedenen Netzwerkabschnitten werden die Datenpakete eines Teilnehmers aufgrund der unterschiedlichen Netzwerkprotokolle und Paketgrößen auch unterschiedlich identifiziert. Auf der Luftschnittstelle mit seinen kleinen Datenpaketen von 456 Bit = 57 Bytes abzüglich Fehlerkorrektur, wird der Teilnehmer mit dem 3 Bit Temporary Flow Identifier (TFI) adressiert. Im Radio Netzwerk wird der Teilnehmer mit der P-TMSI/TLLI identifiziert und im Kernnetzwerk mit der GPRS Tunnel ID (TID). Nur im externen Netzwerk wie dem Internet wird die zugeteilte IP Adresse des Teilnehmers für das Routing der Datenpakete verwendet. Abbildung 2.31 zeigt diese unterschiedliche Teilnehmeridentifizierung im Überblick.

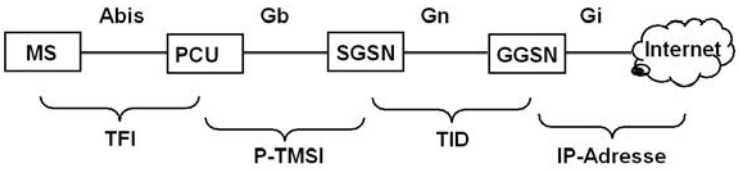

Abb. 2.31: Identifikation der Teilnehmerpakete im GPRS Netzwerk

2.9 Session Management aus Anwendersicht

Aus Anwendersicht wird ein PDP Kontext in zwei Fällen aufgebaut:

Interne Anwendung

Ein im Mobiltelefon eingebauter Client wie z.B. ein WAP Browser wird für das Abrufen von Informationen aus dem Internet verwendet. Alle relevanten Einstellungen für diese GPRS Verbindung müssen dazu im Endgerät konfiguriert werden. In vielen Fällen werden Mobiltelefone schon bei Auslieferung vorkonfiguriert und können sofort verwendet werden.

Externe Anwendung

Ein Teilnehmer verwendet ein Datenendgerät wie z.B. einen Notebook oder einen PDA, um über das Mobiltelefon mit dem Internet Verbindung aufzunehmen. Das Mobiltelefon dient in diesem Fall nur als externe Schnittstelle zum Internet. Für eine solche Verbindung sind die GPRS Einstellungen nicht im Mobiltelefon, sondern im Datenendgerät vorzunehmen.

Verwendung des DFÜ-Netzwerkes

Wird das Mobiltelefon als externe Schnittstelle zum Internet von einem Datenendgerät verwendet, kann der in allen Betriebssystemen vorhandene Modemstack, in Microsoft Windows auch DFÜ-Netzwerk genannt, zum Aufbau einer Internetverbindung verwendet werden. Der nächste Abschnitt zeigt deshalb zunächst, wie der Modemstack normalerweise verwendet wird, um eine Internetverbindung über ein Festnetzmodem oder eine leitungsvermittelte GSM Verbindung aufzubauen. Im nächsten Schritt wird dann gezeigt, wie sich eine Modemverbindung von einer GPRS Verbindung unterscheidet und welche zusätzlichen Einstellungen für GPRS deshalb auf dem Datenendgerät, also dem Notebook oder dem PDA notwendig sind.

2.9.1 Leitungsvermittelter Verbindungsaufbau

AT-Kommandos

Ein Modem bietet für die Verbindungsaufnahme mit einer Gegenstelle eine textbasierte Kommandoschnittstelle an, die AT-

Interface genannt wird. Um zum Beispiel eine Telefonnummer zu wählen, wird dem Modem das Kommando ATD zusammen mit der Telefonnummer (z.B. ATD 0899011782) übergeben. Das Modem wählt daraufhin diese Nummer und stellt eine Datenverbindung mit dem Dial In Server Modem des Internet Service Providers (ISP) her. War der Verbindungsaufbau erfolgreich, sendet das Modem eine CONNECT Nachricht mit der ausgehandelten Übertragungsgeschwindigkeit an das Datenendgerät zurück (z.B. CONNECT 38400). Daraufhin wechselt das Modem aus dem Kommandomodus in den Übertragungsmodus und leitet alle Daten von nun an transparent weiter.

PPP Verbindung

Um Datenpakete über diese transparente serielle Verbindung zu übertragen, verwendet das DFÜ-Netzwerk das Point to Point Protocol (PPP). Der PPP Client ist dabei das Endgerät, der PPP Server der Dial In Server des Internet Service Providers.

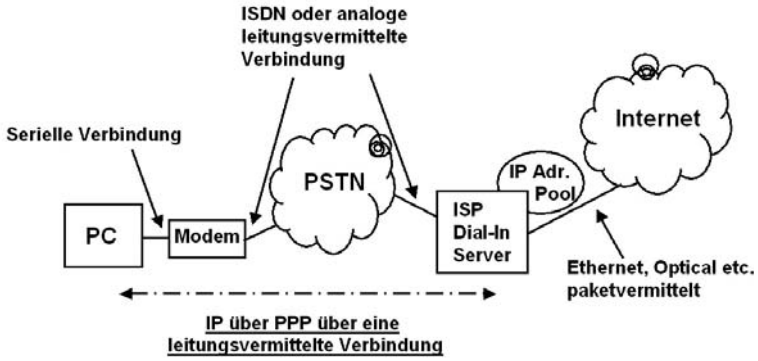

Abb. 2.32: Internetverbindung per Modem und PPP

Nach dem Verbindungsaufbau wird mit dem PPP Protokoll zunächst der Teilnehmer authentifiziert. Nach erfolgreicher Authentifizierung übermittelt der PPP Server dann dem Teilnehmer alle für die nachfolgende IP Übertragung nötigen Parameter. Dazu gehört insbesondere die IP Adresse für das Endgerät, sowie die IP Adresse des DNS Servers für die Namensauflösung. In der danach beginnenden Datenübertragungsphase ist es die Aufgabe des PPP Protokolls, IP Pakete über die transparente Verbindung zu übertragen. Um den Anfang und das Ende jedes Paketes auf der anderen Seite auch korrekt erkennen zu können, fügt das PPP Protokoll eine Start- und Endekennung, sowie einen Header an die vom IP Layer erhaltenen Pakete an.

2.9.2 GPRS Verbindungsaufbau

GPRS unterscheidet sich von einer leitungsvermittelten Verbindung in folgenden Punkten:

- GPRS ist bereits eine paketvermittelte Verbindung zum Internet, es gibt keine leitungsvermittelte Verbindung mehr zum ISP Dial In Server.
- Es gibt keine Telefonnummer die beim Verbindungsaufbau gewählt werden müsste.
- Es gibt keinen PPP Server, zu dem sich ein Client verbinden könnte. Im GPRS Netzwerk vergibt der GGSN die IP Adressen der Teilnehmer während der PDP Context Activation Prozedur.

GPRS mit dem DFÜ-Netzwerk

Aus diesen Gründen ist die für eine leitungsvermittelte Verbindung vorgestellte Prozedur für die Kontaktaufnahme mit dem Internet eigentlich wenig geeignet. Um aber keine spezielle Software für die Interneteinwahl per GPRS für Datenendgeräte entwickeln zu müssen, wurde das Verfahren wie folgt für GPRS Verbindungen angepasst:

PPP Server im Mobiltelefon

Um den PPP Client des DFÜ-Netzwerkes weiterverwenden zu können, wird auch für eine GPRS Verbindung ein PPP Server benötigt. Die Software für den PPP Server wurde dazu direkt in das Mobiltelefon integriert und bildet aus Sicht des Datenendgeräts die Schnittstelle zum Internet. Statt also eine PPP Verbindung zum Internet Service Provider herzustellen, endet die PPP Verbindung nun bereits im Mobiltelefon. Abbildung 2.33 zeigt diese Konfiguration.

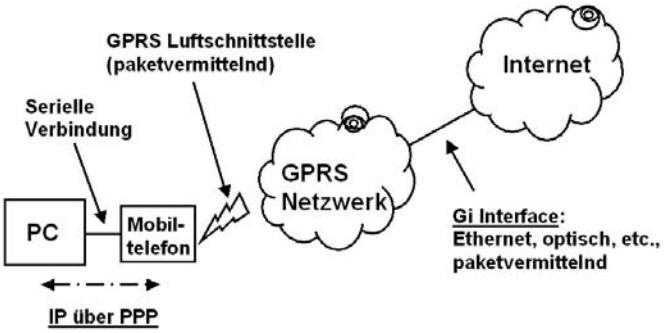

Abb. 2.33: Internetverbindung per GPRS und PPP

Der PPP Server im Mobiltelefon übersetzt die PPP Verbindungsaufnahme in eine Activate PDP Context Request Nachricht und sendet diese an das GPRS Netzwerk. Die IP Adresse wird dann wie zuvor in Abbildung 2.30 gezeigt zugeteilt.

Nach erfolgreicher Verbindungsaufnahme schickt der GGSN über die Activate PDP Context Accept Nachricht eine IP Adresse an das Mobiltelefon zurück. Von dort wird die IP Adresse dem Datenendgerät per PPP zurückgegeben und der Verbindungsaufbau ist abgeschlossen.

Während der Verbindung (dem Packet Call) werden im Mobiltelefon die über das PPP Protokoll eingehenden IP Pakete in kleine GPRS Datenpakete aufgeteilt und zum Netzwerk gesendet. In der umgekehrten Richtung werden die vom Netzwerk eingehenden kleinen GPRS Datenpakete vom Mobiltelefon wieder in komplette IP Pakete zusammengesetzt und danach über die serielle PPP Verbindung zum Datenendgerät weitergegeben.

Modemtreiber für GPRS

Um dieser geänderten Konfiguration Rechnung zu tragen, sind zusätzliche Einstellungen im DFÜ-Netzwerk notwendig. Aus Sicht des Endgeräts stellt das Mobiltelefon ein Modem dar. Deshalb muss zunächst ein Standardmodemtreiber für die Schnittstelle konfiguriert werden, über die das Mobiltelefon angesprochen werden kann. Da der benötigte Standardmodemtreiber bei den unterschiedlichen Betriebssystemen mitgeliefert wird, ist der Anwender nicht auf einen speziellen Treiber des Mobiltelefonherstellers angewiesen.

Senden der APN an das Mobiltelefon

Vor dem Aufbau der Verbindung muss dem Mobiltelefon der APN mitgeteilt werden, über die eine GPRS Internetverbindung aufgebaut werden soll. Damit im DFÜ Netzwerk des Datenendgeräts keine Softwareänderungen nötig sind, entschied man sich bei der Standardisierung dazu, den APN vor dem eigentlichen Verbindungsaufbau mit einem zusätzlichen AT Kommando zu übergeben. Dies geschieht mit dem AT+CGDCONT Kommando. Um zum Beispiel eine IP Verbindung über das GPRS Netzwerk mit dem APN „internet.t-d1.de“ aufzubauen, ist folgendes AT Kommando notwendig: ‘AT+CGDCONT=1,"IP","internet.t-d1.de"’. Dieses Kommando wird wie in Abbildung 2.34 gezeigt in den “Erweiterten Einstellungen” der Modemkonfiguration eingetragen.

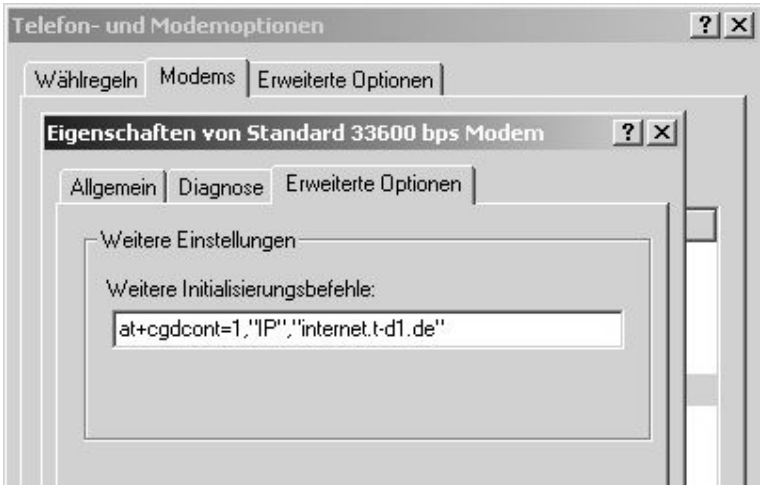

Abb. 2.34: APN als erweiterte Optionen bei der Modemkonfiguration

GPRS Verbindung statt Telefonnummer

Ein weiterer Unterschied zwischen einer leitungsvermittelten Internetverbindung und einer GPRS Internetverbindung ist die Tatsache, dass für GPRS keine Telefonnummer gewählt werden muss. Stattdessen muss dem DFÜ Netzwerk jedoch mitgeteilt werden, dass eine GPRS Verbindung mit dem zuvor eingestellten APN hergestellt werden soll. Dazu wird statt der Telefonnummer der String ‚*99***1#' in der entsprechenden Dialogbox des DFÜ-Netzwerkes eingetragen. Dieser String wird dann vom DFÜ-Netzwerk über das ATD Kommando zum Mobiltelefon übergeben (ATD *99***1#). Nach Erhalt dieses Kommandos startet das Mobiltelefon daraufhin den PPP Server und verwendet den im AT+CGDCONT übergebenen APN für die PDP Context Activation Prozedur. War die PDP Context Activation erfolgreich, liefert der PPP Server die in der PDP Context Activation Accept Nachricht enthaltene IP Adresse an das Datenendgerät zurück und die Verbindung zum Internet ist hergestellt.

Manuelle DNS Konfiguration

Zur Umwandlung eines Hostnamens wie z.B. www.vieweg.de in eine IP Adresse (Namensauflösung) wird im Internet das Domain Name System (DNS) verwendet. Dem Datenendgerät wird dazu bei der Verbindungsaufnahme über das PPP Protokoll die IP Adresse eines DNS-Servers mitgeteilt. Dies ist auch bei GPRS möglich, da dieser Parameter in der PDP Context Activation Accept Nachricht an das Datenendgerät übergeben werden kann. Da jedoch nicht alle Netzbetreiber von dieser Funktionalität gebrauch machen, ist es unter Umständen notwendig, die DNS-

Server IP Adresse manuell in den IP Einstellungen des DFÜ-Netzwerks anzugeben. Da jeder GPRS Netzbetreiber seinen eigenen DNS Server betreibt, wird die DNS IP Adresse normalerweise zusammen mit der APN bekannt gegeben.

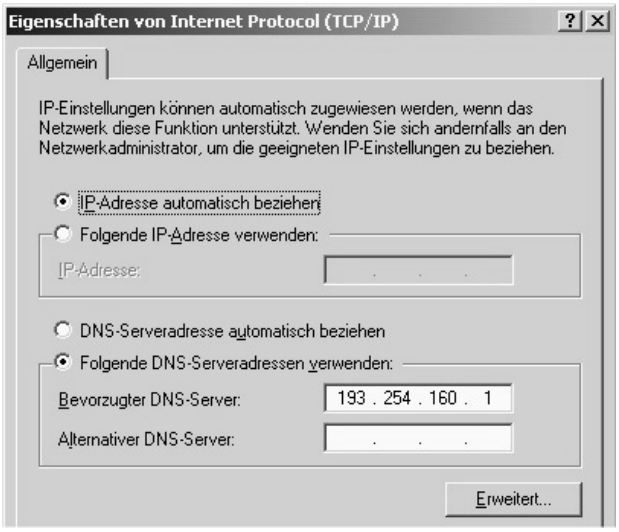

Abb. 2.35: Manuelle DNS Konfiguration für GPRS

Software der Endgerätehersteller

Viele Anwender dürften mit der aufwändigen Konfiguration des APN, des DNS-Servers und des Wählstrings nur schwer zurechtkommen. Aus diesem Grund liefern viele Mobiltelefonhersteller eigene Konfigurationsprogramme, die diese Einstellungen automatisch erledigen. Diese sind aber meistens nur für Windows Betriebssysteme erhältlich, MAC, Linux oder PDA Benutzer werden nicht berücksichtigt.

2.10 Der Multimedia Messaging Service (MMS) über GPRS

Eine weitere mobile Datenanwendung die sich zunehmender Beliebtheit erfreut, ist der Multimedia Messaging Service, kurz MMS genannt. MMS wird von den Mobilfunkbetreibern als multimedialer Nachfolger des textbasierten Kurznachrichtendienstes SMS beworben und kann neben Text auch Bilder, Musik- und Videodateien übertragen.

MMS nutzt IP für die Übertragung

Die Architektur der SMS und MMS Systeme unterscheiden sich jedoch grundlegend. Das SMS System verwendet die SS-7 Signalisierungskanäle des Mobilfunknetzes und ist somit komplett im GSM Netzwerk integriert. MMS basiert dagegen auf dem Internet

Protokoll (IP) und ist im Aufbau einer eMail sehr ähnlich. Das Mobilfunknetzwerk wird lediglich als transparenter IP Übertragungskanal genutzt. GPRS dient somit MMS nur als Transportmedium und könnte gegen ein beliebiges anderes IP Übertragungsmedium ausgetauscht werden.

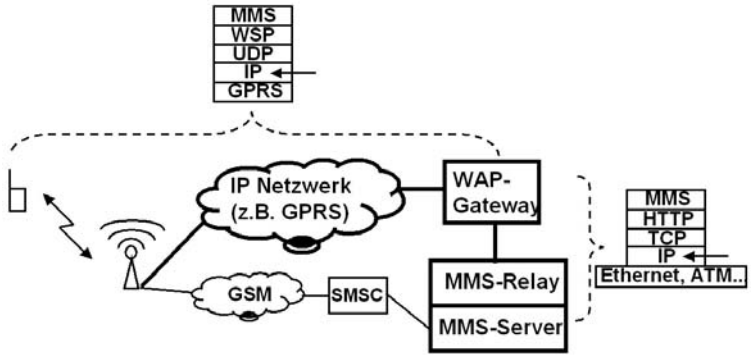

Abb. 2.36: MMS Architektur im Überblick nach 3GPP TS 23.140

Senden einer MMS

Beim Senden einer MMS wird vom Mobiltelefon eine IP Verbindung über das GPRS Netzwerk zum MMS Server aufgebaut. Die dazu nötige PDP Context Activation Prozedur wurde im letzten Abschnitt beschrieben. Statt jedoch den gleichen APN wie für eine direkte Internetverbindung zu verwenden, gibt es für MMS meist eine eigene APN. Somit ist es für den Netzbetreiber möglich, MMS Nachrichten nach einem extra Tarif abzurechnen. Wie in Abbildung 2.36 gezeigt wird, befindet sich zwischen MMS-Server und Endgerät ein WAP Gateway. Ursprünglich wurde das WAP Gateway entwickelt, um die Übertragung von WAP Seiten per GPRS zu optimieren. Durch Zwischenschalten des WAP Gateways kann diese Optimierung auch für MMS Nachrichten verwendet werden. Dies ist auch der Grund für die zwei unterschiedlichen Protokollstapel, die ebenfalls in Abbildung 2.36 gezeigt werden. Mit der Einführung von WAP 2.0 wurden jedoch die Protokollstapel auf beiden Seiten des WAP Gateways harmonisiert und neuere Endgeräte verwenden nun HTTP und TCP.

Zustellung einer MMS zu einem mobilen Endgerät

Wird als Empfänger der MMS eine Mobiltelefonnummer (MSISDN) verwendet, muss der MMS Server dessen Endgerät als nächstes über den Eingang der MMS benachrichtigen. Dies geschieht durch Senden einer SMS. Gehört die MSISDN zu einem nicht MMS fähigen Endgerät, enthält die SMS einen Nachrichtentext mit der Information, wie die MMS über eine Web Seite im Internet abgerufen werden kann. Hat der Teilnehmer sein End-

gerät als MMS fähiges Endgerät beim MMS Server angemeldet (z.B. automatisch durch erstmaliges Absenden einer MMS), enthält die SMS einen speziell formatierten Text. Dieser Text wird von einem MMS fähigen Endgerät automatisch erkannt und die SMS wird dem Nutzer nicht angezeigt. Je nach Benutzereinstellung kann das Endgerät nach Erhalt dieser SMS unterschiedlich reagieren: Wurde das Endgerät auf manuellen MMS Empfang eingestellt, informiert das Endgerät den Teilnehmer über die neue MMS und lädt diese erst nach Bestätigung des Teilnehmers vom MMS Server. Ist das Endgerät auf automatischen MMS Empfang eingestellt, wird die MMS ohne Benachrichtigung des Teilnehmers vom MMS Server angefordert und der Benutzer erst informiert, nachdem die MMS komplett in den Speicher des Endgerätes geladen wurde.

Zustellung einer MMS an eine eMail-Adresse

Im MMS Standard wurde von Beginn an vorgesehen, eine MMS auch direkt an eine beliebige eMail-Adresse senden zu können. Wie wir später noch sehen werden, ist dies aufgrund der großen Ähnlichkeit des MMS Formats zum eMail-Format auch sehr einfach möglich. In diesem Fall kann jedoch die Benachrichtigung des Empfängers per SMS entfallen und die MMS kann leicht modifiziert direkt an die Mailbox des Empfängers zugestellt werden.

MMS Konfiguration im Endgerät

Um MMS Nachrichten senden und empfangen zu können, sind eine Reihe Einstellungen im Endgerät nötig. Erster Schritt für das Senden oder Empfangen einer MMS per GPRS ist der Aufbau eines PDP Kontextes. Deshalb muss im Endgerät für den MMS Dienst einen APN, und optional ein Login Namen und Passwort für diesen APN eingetragen werden. Da der MMS Dienst den WAP Server für die Datenkomprimierung verwendet, muss in den MMS Einstellungen auch die IP Adresse des WAP Gateways eingetragen sein. Schließlich muss das Endgerät noch die Adresse des MMS Server kennen, die in Form einer URL (Universal Ressource Locater) angegeben wird. In nachfolgender Tabelle werden diese Einstellungen beispielhaft für das E-Plus Netz in Deutschland gezeigt:

APN	mms.eplus.de
Username	mms
Passwort	Eplus
IP Adresse WAP Gateway	212.23.97.153
MMS Server URL	http://mms/eplus

Aufbau einer MMS Nachricht

Ähnlich einer eMail kann eine MMS nicht nur Text, sondern auch Anhänge wie Bilder, Tondateien und Videosequenzen enthalten. Im Unterschied zu einer eMail kann ein Anwender jedoch beim Erstellen der MMS Nachricht entscheiden, in welcher Reihenfolge, an welcher Position und für welche Zeitdauer Bilder, Texte, Ton- und Videos auf dem Display angezeigt oder abgespielt werden.

SMIL

Das Endgerät erzeugt aus den Eingaben des Benutzers eine Ablaufbeschreibung mit der Synchronized Multimedia Integration Language (SMIL). Diese Beschreibungssprache wurde vom World Wide Web Consortium (http://www.w3c.org) standardisiert. SMIL hat große Ähnlichkeit mit der Hypertext Markup Language (HTML), in der Internet Webseiten erstellt werden. Abbildung 2.37 zeigt eine solche SMIL Datei. Sie enthält Informationen über das generelle Layout, Anzahl der Seiten sowie deren Inhalt. Die eigentlichen Informationen wie Texte, Bilder, Sound, Video, etc. sind nicht Bestandteil der SMIL Beschreibung. Diese werden über die ‚src=' Tags referenziert und im Anschluss an die SMIL Datei übertragen.

```
<smil>
  <head>
    <layout>
      <root-layout height="80" width="101"/>
        <region id="Image" fit="meet" height="40"
                left="0" top="0" width="101"/>
        <region id="Text" fit="meet" height="40"
                left="0" top="40" width="101"/>
    </layout>
  </head>

  <body>
    <par dur="10000ms">
      <img region="Image" src="cid:AA"/>
      <text region="Text" src="cid:AC"/>
    </par>

    <par dur="10000ms">
       <text region="Text" src="cid:AD"/>
    </par>

  </body>
</smil>
```

Layout der Seiten

Erste Seite mit Bild und Text

Zweite Seite, nur Text

Abb. 2.37: Beschreibung des Inhalts einer MMS Datei mit SMIL

MIME

In gleicher Weise wie bei einer eMail werden die einzelnen Teile einer MMS wie z.B. die SMIL Beschreibung, Texte, Bilder etc., nicht getrennt voneinander, sondern zusammen übertragen. Um die einzelnen Teile voneinander unterscheiden zu können, verwendet der MMS Standard das Multipart Internet Mail Extension

Protokoll (MIME), das auch bei der Übertragung von eMails verwendet wird. Im MIME Header befindet sich wie in Abbildung 2.38 gezeigt, eine generelle Beschreibung der zu übertragenden Informationen. Danach wird die SMIL Beschreibung der MMS, die Texte, Bilder, etc. übertragen. Um die einzelnen Teile voneinander unterscheiden zu können, werden diese durch eine „Boundary“ Markierung getrennt.

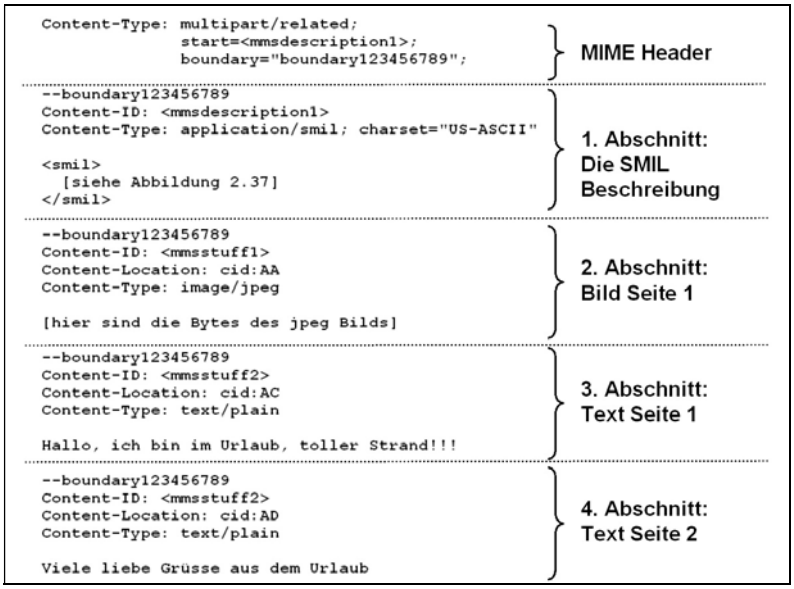

Abb 2.38: Versenden aller Teile einer MMS per MIME

Teil der Boundary Markierung sind Referenzen, die zuvor in der SMIL Datei gemacht wurden, sowie eine Beschreibung des Formats (Content Type). Für MMS Nachrichten wurden bisher unter anderen folgende Formate spezifiziert:

- Bilder: JPEG, GIF, WBMP, maximal garantierte Auflösung ist 160x120 Pixel. Dies entspricht der Auflösung eines kleinen Mobiltelefondisplays. Werden Bilder mit höherer Auflösung gesendet, müssen diese eventuell dann beim Empfänger auf diese Größe reduziert werden.
- Text: ASCII 8-Bit, UTF-8 oder UTF-16
- Audio: AMR (Adaptive Multi Rate)
- Video: MPEG 4, H.263, Quicktime

MMS Header

Um die fertig zusammengestellte MMS Nachricht versenden zu können, ist noch ein Header notwendig, der Informationen wie Absender und Empfänger enthält. Auch hier verwendet MMS einen Standard eMail Header. Diesem wurden lediglich einige zusätzliche MMS spezifische Felder angefügt, die jeweils mit „X-MMS“ beginnen. Ausserdem werden die Felder nicht im Klartext übertragen, sondern als IDs mit einer Länge von einem Byte. Dies senkt den Overhead und somit auch die Übertragungszeit. Da MMS Nachrichten neben eMail-Adressen hauptsächlich an Mobilfunkteilnehmer, also an Telefonnummern geschickt werden, definiert der MMS Standard außerdem die Kennzeichnung von Telefonnummern durch den Anhang „/TYPE=PLMN“. PLMN steht dabei für Public Land Mobile Network, dem Fachbegriff für Mobilfunknetzwerk.

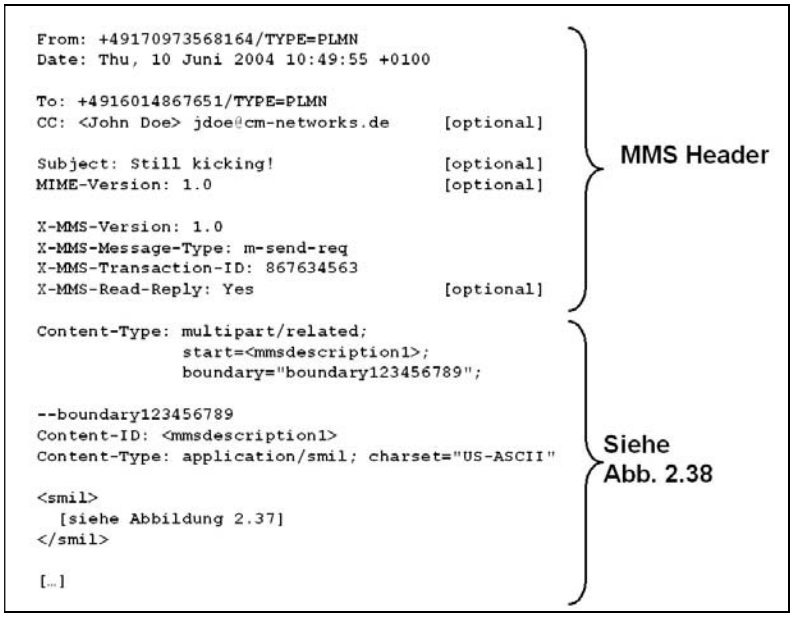

Abb. 2.39: MMS Header (nichtkomprimierte Darstellung)

MMS Versand mit HTTP POST

MMS und eMail verwenden für die Übertragung zum eMail bzw. MMS Server unterschiedliche Protokolle. Während eMail Nachrichten mit dem Simple Mail Transfer Protocol (SMTP) übertragen werden, entschied man sich für die Übertragung von MMS Nachrichten für das Hypertext Transfer Protocol (HTTP) POST Verfahren. Dieses Protokoll wurde ursprünglich entworfen, damit Web

Browser einen vom Benutzer eingegebenen Text in Eingabefeldern einer Web Page an einen Web Server senden können. Vorteil gegenüber SMTP für die MMS Übertragung ist, dass bei Beginn der Verbindung kein Login Vorgang notwendig ist und somit die MMS schneller übertragen wird.

Empfang einer MMS mit HTTP GET

Wie schon in der Einleitung zu diesem Kapitel erwähnt, verwendet der MMS Server eine SMS Nachricht, um den Empfänger über eine eingegangene Nachricht zu informieren. Die SMS enthält dabei einen Universal Ressource Locator (URL), der die abzuholende MMS identifiziert. Um dem Overhead des POP3 Protokolls zu entgehen, das für den Empfang von eMails spezifiziert wurde, werden MMS Nachrichten über das HTTP GET Protokoll vom MMS Server abgerufen. Das HTTP GET Protokoll wurde ursprünglich konzipiert, um mit einem Browser Webseiten von einem Webserver anzufordern. Um die Daten einer MMS bei der Übertragung durch das GPRS Netzwerk zu komprimieren, kommt wiederum das WSP Protokoll zum Einsatz.

MMS an einen eMail-Empfänger

Aufgrund der vielen Gemeinsamkeiten zwischen MMS und eMail ist auch der Versand einer MMS an einen eMail-Empfänger recht einfach. Der MMS Server konvertiert die MMS in eine eMail durch Entfernen der SMIL Beschreibung. Texte, Bilder, etc. werden als Anlagen an die eMail angehängt.

MMS über andere IP Netzwerke

Da MMS eine reine IP Applikation ist und nur offene Internet Standards verwendet, spielt das Übertragungsmedium keine Rolle. Theoretisch könnte eine MMS also auch von einem PC an einen PC im Internet übertragen werden. Praktisch macht dies jedoch wenig Sinn, da hier für die Kommunikation eine eMail besser geeignet ist. Während in Europa MMS also sowohl in GSM, als auch in UMTS verwendet werden kann, ermöglicht die Verwendung von IP und offenen Standards auch, MMS in anderen Mobilfunkstandards wie z.B. dem amerikanischen CDMA Standard ohne Änderungen zu verwenden. Somit wird es möglich, MMS auch zwischen Teilnehmern unterschiedlicher Mobilfunknetzwerke in Ländern wie z.B. den USA auszutauschen, in denen unterschiedliche Mobilfunkstandards wie UMTS, GSM, CDMA, etc. gleichzeitig betrieben werden.

2.11 Fragen und Aufgaben

1. Welche Unterschiede gibt es zwischen leitungsvermittelter Datenübertragung und paketorientierter Datenübertragung.
2. Welche Vorteile bietet die GPRS Datenübertragung gegenüber der bisherigen GSM Datenübertragung?
3. Warum gibt es unterschiedliche Coding Schemes?
4. Wie unterscheidet sich der GPRS Ready State vom GPRS Standby State?
5. Führt das Netzwerk bei GPRS einen Handover durch, wenn während eines Zellwechsels Daten übertragen werden?
6. Welche neuen Netzwerkelemente wurden mit GPRS eingeführt und welche grundsätzlichen Aufgaben haben diese?
7. Was ist ein Temporary Block Flow?
8. Welche Vorgänge finden bei einem Inter-SGSN Routing Area Update (IRAU) statt?
9. Warum kommt das IP Protokoll auf dem Gn Interface zweimal im Protokollstack vor?
10. Wie wird erreicht, dass beim internationalen Roaming für GPRS im Ausland keine Einstellungen im Endgerät geändert werden müssen?
11. Was ist der Unterschied zwischen einem GPRS Attach und einer PDP Context Activation?
12. Welche Rolle spielt der Access Point Name (APN) bei der PDP Context Activation Prozedur?
13. Wie werden MMS Nachrichten per GPRS gesendet und empfangen?
14. Wie ist eine MMS Nachricht aufgebaut?

Lösungen sind auf der Website zum Buch unter http://www.cm-networks.de zu finden.

3 UMTS und HSPA

UMTS ist nach GSM und GPRS der nächste Schritt in der Evolution mobiler Telekommunikationsnetzwerke. Seit GSM in den achtziger Jahren standardisiert wurde, gab es in vielen Bereichen enorme Fortschritte. Dies erlaubte es Systemdesignern, weit über die Grenzen von damals hinaus zu gehen. UMTS vereinigt die Eigenschaften eines leitungsvermittelnden Sprachnetzwerkes mit denen eines paketvermittelnden Datennetzwerkes und bietet im Vergleich zu bisherigen Technologien eine Vielzahl neuer Möglichkeiten. Da UMTS auch viel von GSM und GPRS übernimmt, gibt dieses Kapitel zunächst einen Überblick über die Vorteile und Weiterentwicklungen von UMTS. Nach einem Ende zu Ende Netzwerküberblick liegt dann der Schwerpunkt des Kapitels auf der Funktionsweise des UMTS Radio Access Netzwerks. Neue Konzepte wie Radio Ressource Control, sowie Änderungen im Mobility-, Call und Session Management werden ebenfalls im Detail beschrieben.

3.1 Überblick, Historie und Zukunft

Die Entwicklung im Mobilfunk verläuft mit einer zeitlichen Verschiebung von etwa 5 Jahren ähnlich wie im Festnetz. Dort ist seit dem Erscheinen der ersten Modems, die dem Internet zum Durchbruch als Massenmedium verhalfen, eine ständige Geschwindigkeitssteigerung zu beobachten. Während erste Modems Mitte der 90er Jahre noch mit Geschwindigkeiten von 14.4 kbit/s aufwarteten, bringt es die neueste Generation auf über 50 kbit/s. Einen Quantensprung vollzog das drahtgebundene Internet vor einigen Jahren mit der Massentauglichkeit von Technologien wie Kabelmodems oder ADSL. Übertragungsgeschwindigkeiten von mehreren Megabits pro Sekunde sind damit möglich. Im Mobilfunk ist die Einführung von GPRS (vgl. Kapitel 2) mit seinen paketorientierten Eigenschaften der erste Schritt hin zum mobilen Internet. Mit Datenraten im realen Betrieb von etwa 50 kbit/s erreicht diese Technologie annähernd die Geschwindigkeit von Festnetzmodems. Aufgrund der Eigenschaften der verschiedenen Schnittstellen, die bei der Entwicklung des GSM Netzwerkes

definiert wurden, ist diese Grenze mit dieser Technik nicht mehr beliebig nach oben verschiebbar. Neue Modulationsverfahren für die Luftschnittstelle wie EDGE (Enhanced Data Rates for GSM Evolution) werden zwar noch für eine Geschwindigkeitssteigerung sorgen, können aber andere Nachteile des aktuellen GSM Netzwerkes bei der Datenübertragung nicht überwinden. Dazu zählt insbesondere die Zeitschlitzorientierung und die Zugriffsverfahren des GSM Netzwerkes auf die Luftschnittstelle. Dies führt bei der paketorientierten Übertragung zu längeren Verzögerungszeiten, als man dies aus dem Festnetz gewohnt ist.

Auch seit der Inbetriebnahme der ersten GSM Netzwerke Anfang der 90er Jahre hat die ständige Steigerung der Rechen- und Speicherkapazität nicht haltgemacht. Mit einer Verdoppelung der Anzahl der Transistoren pro Fläche nach dem Moore´schen Gesetz alle 18 Monate, stehen heute Prozessoren auch für den Mobilfunk mit einer vielfachen Leistung zur Verfügung, als zu den Anfängen der GSM Entwicklung. Dies ermöglicht wiederum, Übertragungsverfahren auf der Luftschnittstelle zu verwenden, die wesentlich schneller sind als Verfahren, die in GSM verwendet werden. Diese sind aber auch wesentlich komplizierter und somit rechenintensiver.

Für UMTS, dem Universal Mobile Telecommunication System, wurden diese Weiterentwicklungen konsequent genutzt. Während bei GSM die Sprachkommunikation im Vordergrund stand, wurden bei der Spezifikation von UMTS von Beginn an auch Datendienste berücksichtigt und auf die Konvergenz von Sprach- und Datendiensten hingearbeitet.

Wie in den folgenden Abschnitten gezeigt wird, ist UMTS sowohl eine Evolution, wie auch eine Revolution. Viele Komponenten im Kernnetz benötigten lediglich ein Softwareupdate für UMTS. Eine Migration zu neuen Verfahren ist dort erst in den nächsten Jahren zu erwarten. Das Zugangsnetz auf der Basis der CDMA Technik für die Luftschnittstelle ist jedoch eine komplette Neuentwicklung.

3.1.1 Release 99: Neues Radionetzwerk

UMTS Releases

Die Schritte hin zu UMTS wurden vom Standardisierungsgremium 3GPP (3rd Generation Partnership Project) in aufeinander folgende Versionen eingeteilt, die jeweils als Release bezeichnet werden. Dabei wurde die Namensgebung während des Prozesses umgestellt, was für reichlich Verwirrung sorgte. Während am Anfang die Jahreszahl zur Identifizierung der unterschiedlichen

Releases verwendet wurde, änderte man zwischenzeitlich dieses Konzept. Somit trägt die erste Release von UMTS den Namen Release 99, während die nächsten Evolutionsschritte in Release 4, Release 5, Release 6 usw. spezifiziert sind.

Neue Technologien im Radionetzwerk

Release 99 enthält die Spezifikationen für die erste Stufe von UMTS. Die wesentliche Neuerung bei UMTS gegenüber GSM im ersten Schritt ist das komplett neu entwickelte Zugangsnetzwerk, auch UMTS Terrestrial Radio Network (UTRAN) genannt. Das bisher verwendete Verfahren von Zeit- und Frequenzmultiplex, das bei GSM aus heutiger Sicht nur für sehr niedrige Übertragungsgeschwindigkeiten konzipiert wurde, wird durch Wideband Code Division Multiple Access (W-CDMA) ersetzt. Bei diesem Verfahren werden weder Frequenz- noch Zeitmultiplex verwendet, die einzelnen Benutzer werden stattdessen über individuelle Codes unterschieden. Außerdem wurde auch die Bandbreite auf der Luftschnittstelle wesentlich erweitert. Somit steht nun auch mobil ein schneller Zugang ins Internet oder Intranet einer Firma zur Verfügung. UMTS Release 99 unterstützt Datenraten pro Benutzer von bis zu 384 kbit/s im Downlink (von Netzwerk zu Endgerät), sowie 64 – 128 kbit/s im Uplink. Unter guten Übertragungsbedinungen unterstützen neuere Versionen des Standards auch eine Datenübertragungsrate von bis zu 384 kbit/s im Uplink.

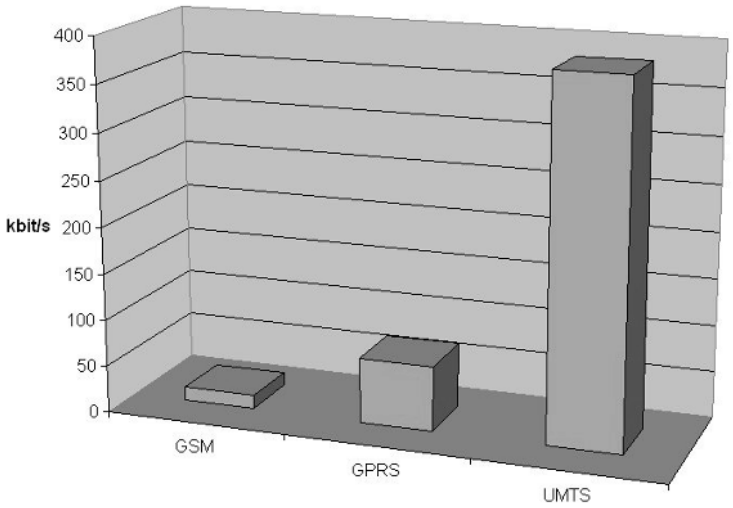

Abb. 3.1: Geschwindigkeitsvergleich GSM, GPRS und UMTS (Release 99)

Von GSM übernommen wurde das Konzept der Basisstationen und übergeordneten Controllern. Diese werden bei UMTS nicht mehr BTS und BSC genannt, sondern Node-B und Radio Network Controller (RNC). Außerdem wurde das Mobiltelefon von Mobile Station (MS) in User Equipment (UE) umbenannt.

Im Frequenzbereich belegt UMTS in Europa im Uplink zwölf Blöcke zu je 5 MHz im Bereich von 1920 – 1980 MHz und ist somit knapp oberhalb des Frequenzbereiches von DECT (Schnurlostelefone) angesiedelt. Im Downlink, also vom Netzwerk zum Anwender, sind für UMTS ebenfalls 12 Blöcke zu je 5 MHz im Bereich von 2110 – 2170 MHz reserviert.

Softwareupdate im Kernnetz

Das leitungsvermittelnde Core Network ist zwar schon seit vielen Jahren in Betrieb, bildet aber eine leistungsfähige und stabile Grundlage auch für UMTS. Deshalb wurde beschlossen, hier in der ersten Phase von UMTS mit Ausnahme von Softwareerweiterungen keine wesentlichen Änderungen vorzunehmen. Die Weiterentwicklung der Sprachdienste wird in den UMTS Releases 4 und 5 spezifiziert, die jedoch erst später implementiert werden. Die Softwareerweiterungen für Release 99 beschränken sich dabei im wesentlichen auf das neue Interface Iu(cs) zum Zugangsnetzwerk, das dem GSM A-Interface sehr ähnlich ist. Außerdem wurde die Software des HLR und des Authentication Centers erweitert, um UMTS spezifische Dienste zu unterstützen.

Im paketvermittelnden Kernnetz, das die Verbindung für mobile Teilnehmer zum Internet oder in ein Intranet einer Firma ermöglicht, wurde ebenfalls so verfahren. Das vorhandene GPRS Netzwerk wurde jedoch erst wenige Jahre vor dem Beginn der UMTS Standardisierung entwickelt und entspricht noch weitgehend dem Stand der Technik. Änderungen sind auch hier hauptsächlich an der Schnittstelle zum UTRAN erfolgt, das Iu(ps) Interface löst das von GPRS bekannte Gb Interface ab (vgl. Kapitel 2). Wesentliche Änderung bei dieser neuen Schnittstelle ist die Verwendung von ATM statt Frame Relay auf den unteren Protokollschichten. Außerdem werden die GTP Nutzdatenpakete nun direkt in das Zugangsnetzwerk weitergereicht, statt diese wie bisher im SGSN zu verarbeiten und für den Transport über das Gb Interface in einen neuen Protokollstapel zu verpacken.

Da es in den Kernnetzen für Release 99 keine grundlegenden Änderungen gibt, kann UMTS zusammen mit einem bereits in Betrieb befindlichen GSM und GPRS Kernnetzwerk betrieben werden. Das UMTS Zugangsnetzwerk wird dabei über die neu definierten Schnittstellen Iu(cs) und Iu(ps) an vorhandene MSCs

und SGSNs angeschlossen. Diese können mit angepasster Software Daten- und Sprachverbindungen mit GSM und UMTS Zugangsnetzwerken herstellen. Vor allem Mobilfunkbetreiber, die schon ein GSM/GPRS Netzwerk unterhalten, haben hiervon enorme Vorteile.

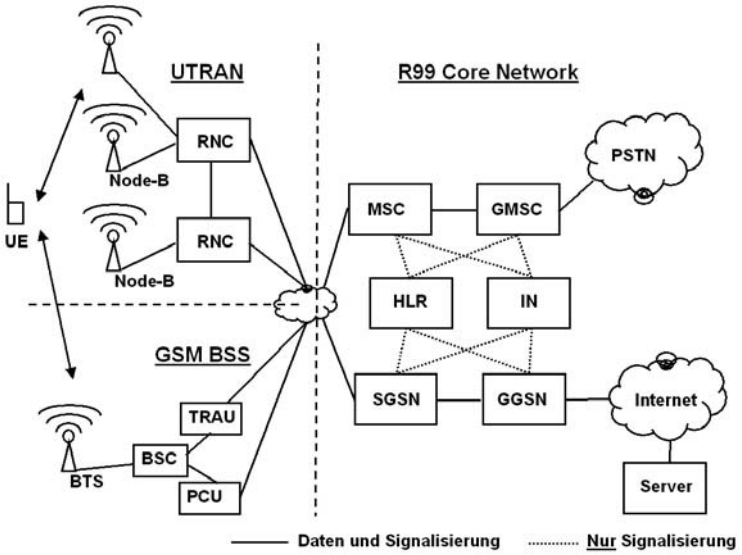

Abb. 3.2: Gemeinsames GSM/UMTS Netzwerk, Release 99

Außerdem ermöglicht ein gemeinsames Kernnetz auch einen einfachen Übergang zwischen GSM und UMTS für den Benutzer. Dies ist vor allem in den Anfangsjahren von UMTS sehr wichtig, in denen die meisten Netzwerke nur Ballungsräume abdecken. Während eine geringe Flächenabdeckung in den Anfängen von GSM mangels großer Teilnehmerzahlen des analogen Vorläufers kein großes Problem für Netzbetreiber war, ist eine flächendeckende Versorgung für UMTS auch in den Anfangsjahren unabdingbar. Kunden, die bereits ein flächendeckendes Netz gewohnt sind, werden eine neue Mobilfunktechnologie aber erst verwenden, wenn diese auch wie GSM in gewohnter Weise nahezu überall zur Verfügung steht. Somit werden für einige Jahre so genannte Dual Mode Endgeräte, die sowohl GSM, als auch UMTS beherrschen, sehr wichtig sein. Gespräche am Rande des UMTS Versorgungsbereiches können mit diesen Endgeräten automatisch im GSM Netzwerk weitergeführt werden, ohne dass der Benutzer dies merkt. Für Datenverbindungen geschieht das

gleiche. Aufgrund der geringeren Geschwindigkeit des Datendienstes in GSM/GPRS wird der Benutzer dies jedoch sehr wohl bemerken.

Hauptziel von UMTS Release 99 ist neben der Sprachtelefonie jedoch hauptsächlich die Einführung von schnellen Paketdatendiensten für zahlreiche neue Anwendungen. Seit das erste UMTS Netzwerk 2002 in Betrieb genommen wurde, sind Netzwerbetreiber somit in der Lage, Geschäfts- und Privatkunden einen Internetnetzugang anzubieten, der jederzeit und überall genutzt werden kann. UMTS Release 99 ermöglicht es Netzbetreibern weiterhin, neue integrierte Dienste anzubieten wie z.B. MMS Nachrichten mit breitbandigen Audio und Video Inhalten, mobiles Fernsehen oder Java Spiele zum Download auf das Endgerät. Ein weiterer interessanter UMTS Dienst ist der Download von Musik. Mit einer Dateigröße von 1.5 MByte pro Musiktitel und 200 – 500 kByte pro Spiel ist UMTS schnell genug, einen Musiktitel in weniger als 40 Sekunden zu übertragen und ein Spiel in weniger als 10 Sekunden. Bei der richtigen Preisgestaltung sind solche Dienste sehr interessant, da Musik und Spiele auch über das DSL- oder Kabelmodem nicht gratis bezogen werden können.

3.1.2 UMTS Release 4: Bearer Independent Core Network

Release 4: Bearer Independent Core Network (BICN)

Eine große Erweiterung für den leitungsvermittelnden Sprach- und Datendienst erfolgt mit UMTS Release 4. Bis Release 99 werden leitungsvermittelte Verbindungen über E1 Verbindungen als 64 kbit/s Zeitschlitze im Core Netzwerk weitervermittelt. In UMTS Release 4 wird als wichtigste Neuerung das Bearer Independent Core Network (BICN) eingeführt. Leitungsvermittelte Dienste werden im Kernnetzwerk nun nicht mehr über 64 kbit/s Zeitschlitze, sondern in ATM oder IP Paketen übertragen. Die MSC wird hierfür in einen MSC Server für die Signalisierung und in ein Media Gateway (MGW) für die Nutzdatenverbindung aufgeteilt. Der MSC Server ist weiterhin für die Call Control- und Mobility Management Protokolle verantwortlich (vgl. Kapitel 1), während das Media Gateway sich um die Weiterleitung der Nutzdaten kümmert. Media Gateways sind auch für die Umkodierung der Nutzdaten zwischen verschiedenen Übertragungsarten zuständig. Auf diese Weise können z.B. Sprachverbindungen auf dem GSM A-Interface über E-1 Zeitschlitze zum Media Gateway transportiert werden und von dort aus weiter über eine ATM

Verbindung zu einem Media Gateway eines anderen MSC-Server. Von dort aus erfolgt dann wiederum eine Umkodierung z.B. für das UMTS Radio Access Network oder zurück in E-1 Zeitschlitze für die Weiterleitung in das öffentliche Festnetz.

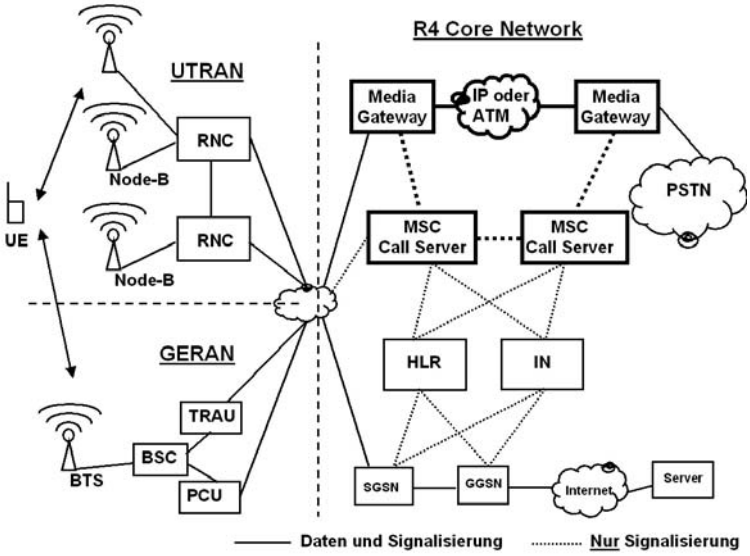

Abb. 3.3: UMTS Release 4 (Bearer Independent Core Network)

Der Grund für die Einführung einer solchen Architektur ist der Wunsch vieler Netzbetreiber, das leitungsvermittelnde und paketvermittelnde Kernnetz zusammenzuführen. Während früher hauptsächlich leitungsvermittelnde Sprachverbindungen im Kernnetzwerk transportiert wurden, nimmt der Anteil der paketorientierten Datenverbindungen ständig zu. Von der Übertragung von Sprach- und Datendiensten über eine gemeinsame Netzwerkarchitektur erhofft man sich deutliche Kostenvorteile auf der Weitverkehrsebene.

3.1.3 UMTS Release 5: Einführung des IP Multimedia Subsystems

Release 5 und 6: All IP Network

Während BICN in Release 4 ein erster Schritt hin zu einem gemeinsamen Sprach- und Datennetzwerk ist, wird mit UMTS Release 5 ein weiterer großer Schritt in Richtung All-IP Netzwerk gemacht. Mit Release 5 können Sprachverbindungen nicht mehr nur im Kernnetz über IP transportiert werden, sondern auch von Ende zu Ende, also von Endgerät zu Endgerät. Die leitungsvermittelnde MSC und die Iu(cs) Schnittstelle werden für eine Release 5 Verbindung nicht mehr benötigt. An Stelle des MSC tritt

das IP Multimedia Subsystem (IMS), mit dem ein Endgerät, wie in Abbildung 3.5 gezeigt, über den SGSN und GGSN kommuniziert. Kern des IMS ist die Call Session Control Function (CSCF), die Signalisierungsinformationen (z.B. für den Rufaufbau) zwischen den Teilnehmern vermittelt. Die eigentlichen Datenpakete für IMS Dienste wie z.B. Sprach- und Videotelefonie, Push to Talk Gruppenrufe und Messaging werden nach der Vermittlung durch die CSCF dann aber direkt zwischen den Teilnehmern ausgetauscht. Die CSCF ist grundsätzlich eine SIP (Session Initiation Protocol) Architektur die ursprünglich aus der Festnetzwelt stammt und dort schon heute für Voice over IP Telefonie sehr verbreitet ist. Mit der CSCF wurde dieser Standard konsequent weiterentwickelt und neue Funktionalitäten hinzugefügt, die für ein Mobilfunknetzwerk notwendig sind. Auf diese Weise ermöglicht die Release 5 Architektur, Sprachanrufe nicht nur im Kernnetz per IP zu transportieren, sondern erstmals auch von Ende zu Ende, d.h. zwischen zwei Mobiltelefonen. Die Media Gateway Control Function (MGCF) ist dabei nur dann nötig, wenn eine Verbindung in ein leitungsvermittelndes Netz, wie z.B. das Festnetz hergestellt werden soll.

Mit dem UMTS Radionetzwerk rückt eine gänzlich auf IP basierte mobile Sprach- und Videotelefoniearchitektur zum ersten Mal in greifbare Nähe. Bisher wurde bei GPRS die Mobilität der paketvermittelten Datenübertragung, also der Wechsel von einer Funkzelle zur nächsten, vom Mobiltelefon gesteuert. Dadurch entsteht beim Zellwechsel eine Unterbrechung der Datenübertragung von etwa zwei bis drei Sekunden. Dies ist für eine Sprach- oder Videoverbindung völlig inakzeptabel. Bei UMTS werden nun auch paketvermittelte Verbindungen auf der Luftschnittstelle vom Netzwerk kontrolliert. Dies sorgt für eine unterbrechungsfreie Datenübertragung auch während eines Zellwechsels. Ein Problem für die Sprachübertragung über IP ist weiterhin das Datenvolumen. Dies ist über IP sehr viel höher, als bei der klassischen Leitungsvermittlung. Da die Verzögerung möglichst gering sein muss, befinden sich pro IP Paket nur sehr wenige Nutzdaten in einem Datenpaket. Dies wiederum bedeutet, dass der Overhead pro IP Paket für den IP Header über 50 % beträgt. Leitungsvermittelte Verbindungen hingegen kommen gänzlich ohne Header Information aus und werden auch auf der UMTS Luftschnittstelle sehr effizient übertragen. Ein solcher Overhead spielt in drahtgebundenen Netzen zwar eine nicht zu vernachlässigende, aber aufgrund der möglichen Kapazitäten dennoch nicht entscheidende Rolle. Auf der Luftschnittstelle ist jedoch

eine Verdoppelung der benötigten Bandbreite für eine Sprachverbindung ganz und gar nicht vernachlässigbar. Da die gesamte Bandbreite auf der Luftschnittstelle auch bei UMTS weiterhin sehr begrenzt ist, bedeutet dies de facto eine Halbierung der möglichen Gespräche pro Zelle.

Leitungsvermittelte- und paketvermittelte Videotelefonie

Für Videotelefonie fällt der zusätzliche Bandbreitenbedarf für eine Ende zu Ende IP Verbindung etwas moderater aus. Aufgrund des sowieso erhöhten Bandbreitenbedarfs für das Videobild zusätzlich zum Sprachkanal, kann bei geschickter Übertragung der Anteil der Headerdaten am gesamten Übertragungsvolumen reduziert werden. Eine Anmerkung an dieser Stelle: Videotelefonie, die seit dem Start von UMTS in Release 99 Netzen angeboten wird, basiert nicht auf IP, sondern auf einem 64 kbit/s leitungsvermittelten Kanal, der über die MSC zwischen zwei Endgeräten geschaltet wird. Dieser Dienst ist erstmals mit UMTS möglich, da im klassischen GSM Netzwerk für eine Sprach- oder Datenverbindung im Radio Netzwerk nur 9.6 oder 14.4 kbit/s Kanäle zur Verfügung stehen.

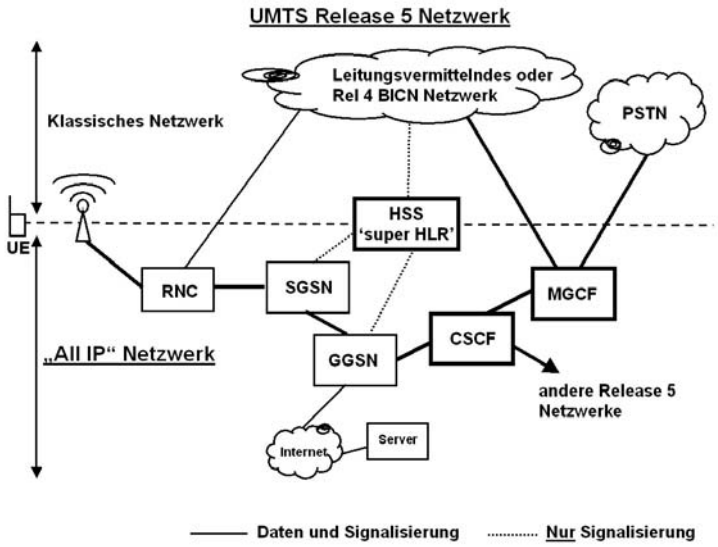

Abb 3.4: UMTS Release 5 Architektur

Unterschiedliche Sprachtelefonievarianten sind kompatibel

Trotz Evolution der Sprachtelefonie muss sichergestellt werden, dass jeder Teilnehmer mit jedem anderen Teilnehmer unabhängig von der verwendeten Evolutionsstufe kommunizieren kann. Dies wird durch Media Gateways, wie in Abbildung 3.4 und 3.5

gezeigt, erreicht. Diese konvertieren jeweils die unterschiedlichen Formate. Ein Netzwerk kann also nach und nach bestehende MSCs durch MSC-Server und Media Gateways ersetzen oder gleich zu einem Release 5 Netzwerk mit IMS Architektur übergehen. Aufgrund des radikal neuen Ansatzes der IMS Architektur ist anzunehmen, dass in der Praxis in den meisten Netzwerken über viele Jahre hinweg eine Mischform aus klasischen MSCs, Call Servern und Release 5 IMS Systemen verwendet werden wird.

Da das IMS als universelle Kommunikationsplatzform konzipiert wurde, ermöglicht das System neben Sprach- und Videotelefonie noch eine große Anzahl an weiteren Diensten. Aufgrund der bereits erwähnten Herausforderungen für IP basiere Telefonie in Mobilfunknetzwerken ist zu erwarten, dass bei der Einführung des IMS in 2006 zunächst andere Anwendungen dominieren werden. Push to Talk (PTT) für Walkie-Talkie ähnliche Gruppenkommunikation ist sicher eine dieser Anwendungen. Durch Verwendung einer standardisierten Platform für diesen Dienst ist es möglich, dass sich eine Gruppe aus Teilnehmern aus unterschiedlichen Mobilfunknetzwerken zusammensetzen kann, da standardisierte PTT Systeme untereinander kompatibel sind. Andere interessante IMS Dienste sind wie schon erwähnt Mobile Messaging und Mobile Presence wie sie heute schon von Yahoo oder dem Microsoft Messenger im Festnetz angeboten werden. Ausserdem ist es mit dem IMS System möglich, Videoinhalte oder mobiles Fernsehen auf einer standardisierten Platform und somit kostengünstiger als mit proprietären Lösungen anzubieten. Weiterhin erwähnenswert ist IMS als Kommunikations- und Signalisierungsplatform für verteilte Anwendungen wie z.B. Multi-Player Spiele.

3.1.4 UMTS Release 5: High Speed Downlink Packet Access (HSDPA)

Release 5 und 6: HSDPA im Radionetzwerk

Mit UMTS Release 5 und 6 wurde im Radio Netzwerk ein neues Übertragungsverfahren namens High Speed Downlink Packet Access (HSDPA) eingeführt. Während die maximale Übertragungsgeschwindigkeit von Release 99 bei maximal 384 kbit/s liegt, ermöglicht HSDPA eine theoretische Datenrate von bis zu 14 MBit/s pro Teilnehmer. In der Praxis werden heute mit aktuellen Endgeräten etwa 2 - 3 Mbit/s bei guten Übertragungsbedingungen und nur wenigen Nutzern pro Zelle erreicht. Selbst bei nicht optimalen Empfangsbedingungen am Ort des Teilnehmers und vielen gleichzeitigen Nutzern pro Zelle können noch immer Geschwindigkeiten von 800 kbit/s pro Nutzer erreicht werden.

Mobilfunkbetreiber können somit Anwendern einen noch schnelleren Internetzugang bieten und treten somit in direkte Konkurrenz zu anderen Technologien wie DSL, Kabelmodems und WiMAX. Manche Netzwerkanbieter gehen nun auch dazu über, Ihren Kunden einen schnellen mobilen Internetzugang für unterwegs kombiniert mit einem DSL oder Kabelzugang für zuhause anzubieten und erschließen sich somit neue Kundengruppen. Viele Netzbetreiber berichten, dass mit der Einführung von HSDPA und interessanten Preisstrukturen für den Endkunden das Datenaufkommen im Mobilfunketzwerk rasant steigt. Die Anzahl der benötigten Basisstationen ändert sich jedoch zur Zeit nur unwesentlich, da noch genug Kapazität auf der Luftschnittstelle vorhanden ist. Somit besteht die Hauptinvestition im Ausbau der Kapazität der Verbindungen zu den Basisstationen. Die meisten 3G Netzbetreiber zeigten großes Interesse an dieser Technik and haben HSDPA schon kurz nach Erscheinen in ihre Netze integriert. Somit gibt es heute nur noch wenige 3G Netze ohne HSDPA Erweiterung.

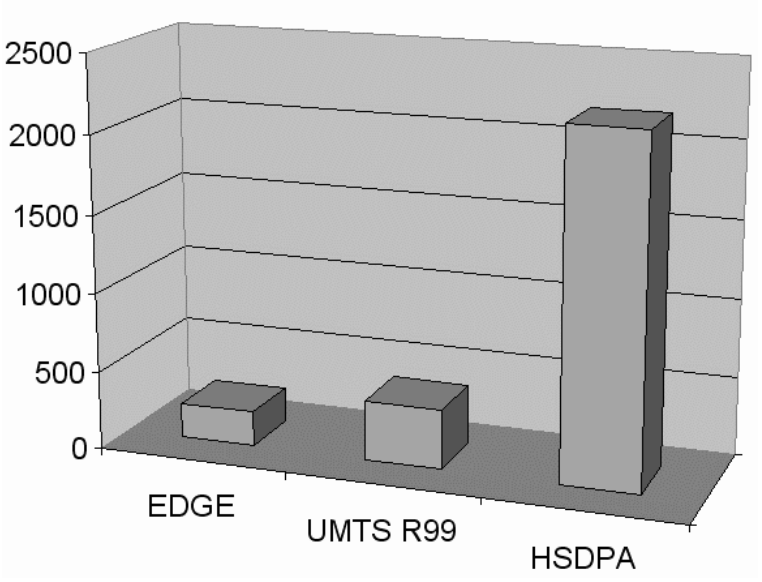

Abbildung 3.5: Geschwindigkeitsvergleich EDGE, UMTS (Release 99) und HSDPA in der Praxis in kbit/s

3.1.5 UMTS Release 6: High Speed Uplink Packet Access (HSUPA)

Auch mit HSDPA bleiben die maximal möglichen Datenraten im Uplink, also vom Endgerät zum Netzwerk auf 384 kbit/s begrenzt, in manchen Netzen oder bei schlechten Übertragungsbedinungen auch nur auf 64 oder 128 kbit/s. Mit Einführung von HSUPA, dem High Speed Packet Uplink Access mit Release 6 und 7 erfährt auch dieser Teil des Systems eine deutliche Geschwindigkeitssteigerung. Geplante Datenraten im Uplink erreichen dann Werte von 480 kbit/s bis zu fast 6 MBit/s, wobei auch hier die Obergrenze ein recht theoretischer Wert ist.

3.2 Wichtige neue Konzepte in UMTS Release 99

Wie im vorhergehenden Abschnitt beschrieben, bringt das UMTS Netzwerk einerseits viele Neuerungen im Vergleich zum bestehenden GSM und GPRS Netzwerk. Anderseits werden aber auch viele Eigenschaften, Verfahren und Methoden von GSM und GPRS beibehalten, die in den vorhergehenden Kapiteln beschrieben wurden. Aus diesem Grund werden nachfolgend im Wesentlichen nur die Neuerungen und Änderungen von UMTS zu seinen Vorgängern beschrieben. Um dabei jedoch auch den Ende zu Ende Überblick zu behalten, erfolgt bei Abläufen und Verfahren, die in UMTS beibehalten wurden, jeweils ein Verweis zu den entsprechenden Abschnitten in Kapitel 1 und 2.

3.2.1 Der Radio Access Bearer (RAB)

Ein wichtiges Konzept in UMTS ist der Radio Access Bearer (RAB, Radioübertragungskanal). Dieser wird eingeteilt in den Radio Bearer auf der Luftschnittstelle und den Iu Bearer im Radionetzwerk (UTRAN). Bevor Daten von oder zu einem Teilnehmer übertragen werden können, ist es notwendig, einen RAB aufzubauen. Über diesen Kanal werden dann die Nutz- und Signalisierungsdaten übertragen. Aufgebaut wird ein RAB im UTRAN auf Anforderung der MSC, bzw. des SGSN. Im Unterschied zur bisherigen Sichtweise in GSM werden aber keine genauen Angaben zur Beschaffenheit des RABs gemacht, sondern es werden nur die gewünschten Eigenschaften des RABs beschrieben. Wie diese Eigenschaften dann in eine physikalische Verbindung umgesetzt werden, bleibt dem UTRAN überlassen. Gewünschte Eigenschaften die dem UTRAN für einen RAB übergeben werden sind zum Beispiel:

- Service Klasse (Service Class Conversational, Streaming, Interactive oder Background)
- Maximale Geschwindigkeit (Maximum Speed)
- Zugesicherte Geschwindigkeit (Guaranteed Speed)
- Verzögerung (Delay)
- Fehlerwahrscheinlichkeit (Error Probability)

Das UTRAN ist dann dafür zuständig, für die gewählte Kombination dieser Eigenschaften einen entsprechenden Radioübertragungskanal (RAB) bereitzustellen. Dabei spielt nicht nur die Bandbreite des Kanals eine Rolle. Ebenso wichtig ist auch das Kodierungsverfahren, Auswahl eines logischen und physikalischen Übertragungskanals, sowie auch das Verhalten bei Auftreten von fehlerhaften Datenpaketen auf den einzelnen physikalischen Schichten des Protokollstapels. Bei der Wahl dieser Eigenschaften ist das UTRAN frei, die Standards geben hierzu nur Beispiele. Für eine Sprachübertragung (Service Class „Conversational“) ist es zum Beispiel wenig sinnvoll, falsch übertragene Datenblöcke zu einem späteren Zeitpunkt zu wiederholen. Im Falle der Service Class „Interactive“, die zum Beispiel für die Übertragung von Web Seiten verwendet wird, ist dies jedoch im Gegenteil sehr wünschenswert.

3.2.2 Aufteilung in Access Stratum und Non-Access Stratum

In UMTS wird in den Standards eine klare Unterscheidung zwischen Funktionalitäten in der Access Stratum (AS) und der Non-Access Stratum (NAS) gemacht:

Access Stratum

Die Access Stratum beinhaltet alle Funktionalitäten, die direkt mit dem Radio Netzwerk und der Kontrolle einer aktiven Verbindung eines Teilnehmers mit dem Radio Netzwerk zusammenhängen. So ist z.B. die Handoverkontrolle, die im UTRAN durch den RNC durchgeführt wird, ein Teil der Access Stratum.

Non Access Stratum

Zur Non Access Stratum (NAS) werden alle Funktionalitäten und Protokolle gezählt, die direkt zwischen dem mobilen Endgerät (User Equipment, UE) und dem Kernnetz ausgetauscht werden. Diese haben keinen direkten Einfluss auf die Eigenschaften eines bestehenden Übertragungskanals und dessen Aufrechterhaltung. Hierzu zählen insbesondere die Call Control, Mobility Management, Session Management und Supplementary Services Protokolle (z.B. SMS) von MSC und SGSN.

Service Access Points

Die Protokolle der Non Access Stratum (NAS) haben keinen direkten Einfluss auf einen bestehenden Übertragungskanal. Um einen RAB aufzubauen, abzubauen oder zu modifizieren, ist es jedoch nötig, dass Protokolle der NAS mit der Access Stratum kommunizieren. Dies ist z.B. beim Call Control Protokoll der Fall, das den Auf- oder Abbau eines physikalischen RABs von der Access Stratum anfordert. Diese Art von Operationen erfolgt durch einen der drei definierten logischen Service Access Points (SAPs):

- Notification SAP (Nt, z.B. Paging)
- Dedicated Control SAP (DC, z.B. RAB Setup)
- General Control SAP (GC, Modification of Broadcast Messages, optional)

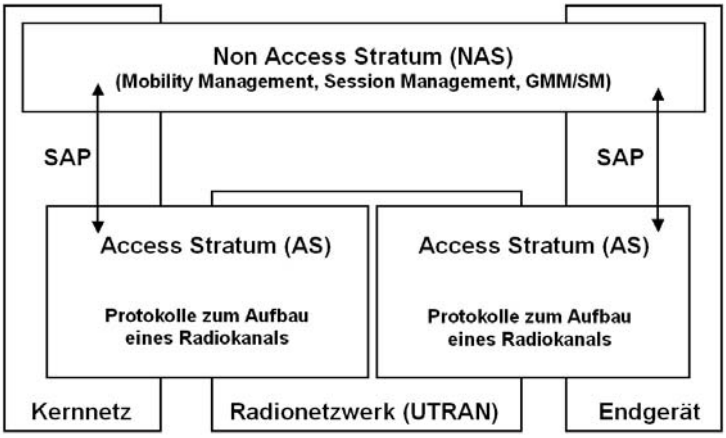

Abb. 3.6: Aufteilung der Protokolle zwischen Kernnetz und Radionetzwerk in Access Stratum (AS) und Non-Access Stratum (NAS)

3.2.3 Gemeinsames Übertragungsprotokoll für CS und PS

In GSM werden auf Grund der Historie Daten über drei unterschiedliche Protokolle über die Luftschnittstelle übertragen. Eine der wichtigsten Aufgaben dieser Protokolle ist, die Daten in kleinere Datenpakete aufzuteilen, die dann übertragen werden. Diese Protokolle sind in Kapitel 1 (GSM) und 2 (GPRS) beschrieben. Hier noch einmal ein kurzer Überblick:

- Leitungsvermittelte Sprachdaten (circuit switched, cs): Die TRAU wandelt die PCM kodierten Sprachdaten für das Zugangsnetz in Full Rate, Enhanced Full Rate oder Half Rate um und sendet diese transparent durch das Zugangsnetz. Die BTS fügt lediglich noch die Kanalkodierung hinzu.
- Signalisierungsdaten (leitungsvermittelnd, sowie teilweise GPRS Channel Requests und Paging): Diese werden per LAPD übertragen, das schon aus der ISDN Welt bekannt ist und für GSM modifiziert wurde.
- Paketvermittelte Userdaten (packet switched, ps) und Signalisierung für GPRS: Die bei der Leitungsvermittlung noch getrennte Übertragung dieser zwei Datentypen wurde bei GPRS in das RLC/MAC Protokoll konvergiert.

In UMTS werden all diese Aufgaben im Radio Link Control / Medium Access Control (RLC/MAC) Protokoll zusammengefasst. Die Namensgleichheit zum entsprechenden GPRS Protokoll kommt nicht von ungefähr. Beide Protokolle arbeiten sehr ähnlich im Bereich der Aufteilung von großen Datenblöcken in kleinere, die dann über die Luftschnittstelle übertragen werden. Aufgrund der anderen Übertragungsweise der Daten über die UMTS Luftschnittstelle gibt es aber auch große Unterschiede, wie der nächste Abschnitt zeigt.

3.3 Code Division Multiple Access (CDMA)

Um die Vorteile des neuen UMTS Zugangsnetzes gegenüber seinen Vorgängern besser einschätzen zu können, folgt hier nochmals ein kurzer Überblick über die Funktionsweise des GSM/GPRS Zugangsnetzwerkes und seinen Einschränkungen: Bei GSM werden Daten für unterschiedliche Teilnehmer, wie in Kapitel 1 beschrieben, in einem Mix aus Frequenz- und Zeitmultiplex übertragen. Ein Teilnehmer erhält dabei einen von 8 Zeitschlitzen auf einer bestimmten Frequenz. Um die Anzahl der Teilnehmer, die über eine Basisstation kommunizieren können zu erhöhen, können mehrere Frequenzen verwenden werden. Diese dürfen nicht von Nachbarstationen verwendet werden, da die Signale sich sonst gegenseitig stören. Um die Übergeschwindigkeit für GPRS zu erhöhen, können mehrere Zeitschlitze pro Teilnehmer verwendet werden.

Dieses System ist zwar für die Datenübertragung geeignet, hat aber auch auf Grund der ursprünglichen Ausrichtung für Sprach-

übertragung folgende Grenzen, die mit UMTS überwunden werden sollen:

GPRS Zeitschlitzbündelung nur begrenzt möglich

Es können nur Zeitschlitze auf einer Frequenz gebündelt werden. Somit ist es theoretisch maximal möglich, bis zu 8 Zeitschlitze zu bündeln. Tatsächlich werden aber selten mehr als 4 Zeitschlitze genutzt, da natürlich weiterhin der Sprachverkehr über diese Basisstation abgewickelt wird. Auf der Endgeräteseite sind auch GSM Mobiltelefone nur für die Bündelung von bis zu 4 Zeitschlitzen im Downlink ausgelegt. Bündelung von mehr Zeitschlitzen erfordert weit komplexere Endgeräte.

Geringe Bandbreite einer GSM Basisstation

Eine GSM Basisstation wurde für den Sprachverkehr ausgelegt, der nur eine geringe Übertragungskapazität benötigt. Deshalb sind GSM Basisstationen nur mit einer 2 MBit/s E-1 Verbindung an den Base Station Controller angeschlossen. Je nachdem, wie viele Trägerfrequenzen verwendet werden, nutzt eine Basisstation nur einen Bruchteil der vorhandenen Leitungskapazität. Die restlichen 64 kbit/s Timeslots einer E-1 Verbindung werden dann für weitere Basisstationen verwendet. Auch die Rechenkapazität der Basisstationen ist nur für solche Kapazitäten ausgelegt.

Lange Verzögerungszeiten bei GPRS

Bei GPRS werden einem Teilnehmer nur Ressourcen, sprich Zeitschlitze in Uplink Richtung zugeteilt, wenn diese auch tatsächlich benötigt werden. Die Mobilstation muss dazu im Netzwerk Ressourcen anfordern. Dadurch kommt es zu unerwünschten Verzögerungen beim Senden von Daten und der darauf folgenden Antwort von 500 – 700 ms.

Bei GPRS werden einem Teilnehmer nur Ressourcen in Downlink Richtung zugeteilt, wenn Daten aus dem Kernnetz für den Teilnehmer zur Übertragung bereitstehen. Auch hier findet wieder eine Zuweisung statt, die nochmals 200 ms in Anspruch nimmt.

Diese Verzögerungszeiten, die in Abbildung 3.7 im Verhältnis zu Verzögerungszeiten von anderen Systemen dargestellt sind, fallen bei der Übertragung von größeren und zusammenhängenden Datenblöcken nicht so sehr ins Gewicht. Bei kurzen, burstartigen Übertragungen, wie z.B. dem Websurfen, sind diese Verzögerungen jedoch deutlich spürbar.

UMTS löst diese Probleme wie folgt:

Breiterer Übertragungskanal

Um die Datenübertragungskapazität pro Frequenz zu steigern, wurde bei UMTS die Bandbreite pro Trägerfrequenz von 200 kHz auf 5 MHz vergrößert. Da Endgeräte nur auf einer Trägerfrequenz senden bzw. empfangen können, steigert dies die mög-

lichen Übertragungsgeschwindigkeiten pro Benutzer enorm. Außerdem können somit wesentlich mehr Benutzer auf der gleichen Frequenz kommunizieren, als bei GSM.

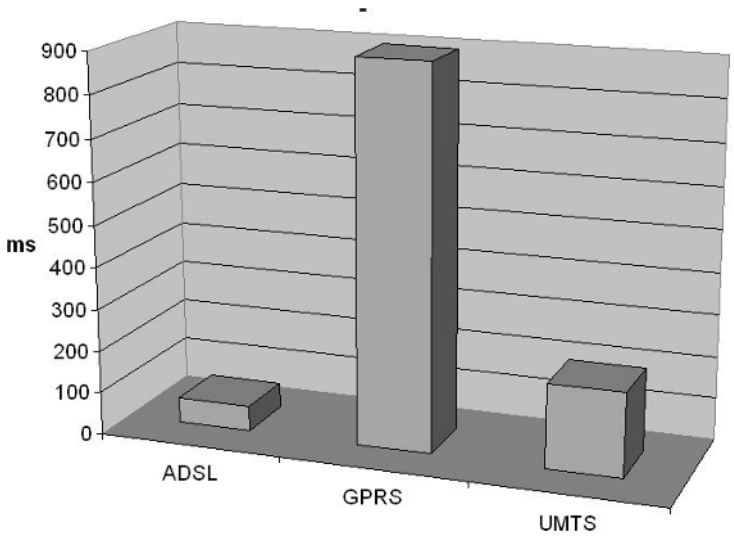

Abb. 3.7: Verzögerungszeiten (Round Trip Delay Time)

UMTS verwendet Codemultiplex

Die entscheidende Neuerung von UMTS ist jedoch die Verwendung eines neuen Zugriffsverfahrens auf der Luftschnittstelle. Statt Frequenz- und Zeitmultiplex wie bei GSM, verwendet UMTS ein Codemultiplex Verfahren, um über eine Basisstation mit mehreren Benutzern gleichzeitig zu kommunizieren. Dieses Verfahren wird Code Division Multiple Access (CDMA) genannt.

Im Unterschied zum Zeit- und Frequenzmultiplex von GSM senden hier alle Teilnehmer auf der gleichen Frequenz und zur gleichen Zeit. Die Daten jedes Teilnehmers werden dabei mit einem Code multipliziert, der möglichst große Unterschiede zu Codes aufweist, die von anderen Teilnehmern zur gleichen Zeit verwendet werden. Da alle Teilnehmer gleichzeitig senden, addieren sich alle Signale auf dem Übertragungsweg zur Basisstation. Die Basisstation kann jedoch die Daten der einzelnen Teilnehmer wieder aus dem empfangenen Signal herausrechnen, da ihr die Sendecodes der Teilnehmer bekannt sind. Dieses Prinzip

kann in gewissen Grenzen auch durch folgende Analogie beschrieben werden:

- Kommunikation während einer Vorlesung: Üblicherweise spricht nur eine Person, viele hören zu. Die Bandbreite ist hoch, da der Übertragungskanal, sprich die Luft, nur von einer Person verwendet wird. Das Flüstern der Studenten erzeugt jedoch ein kleines „Hintergrundrauschen", dessen Lautstärke jedoch wesentlich geringer als die Lautstärke des Vortragenden ist.
- Kommunikation während einer Party: In einem Raum sind viele Menschen, die sich unterhalten. Obwohl sich alle Gespräche in der Luft überlagern, ist das menschliche Gehör trotzdem in der Lage, die einzelnen Gespräche voneinander zu trennen und sich auf ein bestimmtes Gespräch zu konzentrieren. Die anderen Gespräche werden als Hintergrundrauschen herausgefiltert. Je mehr Menschen auf gleichem Raum kommunizieren, desto höher wird das Hintergrundrauschen für den Einzelnen. Die Konversation muss entsprechend deutlicher werden. Die Sprechgeschwindigkeit sinkt, da Worte genauer ausgesprochen werden müssen. Eventuell muss auch lauter gesprochen werden, um das Hintergrundrauschen zu überwinden. Dies bedeutet jedoch für alle Anderen ein größeres Hintergrundrauschen.
- Kommunikation in einer Disco: Hier ist das Hintergrundrauschen, sprich die Musik, so laut, das keine Kommunikation zwischen einzelnen Personen möglich ist.

Andere Teilnehmer werden als Hintergrundrauschen wahrgenommen.

Auf die Datenübertragung bei UMTS abgebildet, sehen diese Szenarien wie folgt aus: Kommunizieren nur wenige Teilnehmer gleichzeitig mit einer Basisstation, gibt es aus der Sichtweise jedes einzelnen Teilnehmers nur sehr wenige Störungen auf dem Übertragungskanal. Es genügt eine geringe Sendeleistung des Teilnehmers, um sein Signal deutlich vom Rauschen, also von den Signalen der anderen Teilnehmer, zu unterscheiden. Die zur Verfügung stehende Bandbreite pro Teilnehmer ist hoch und kann bei Bedarf auch entsprechend genutzt werden, um die Übertragungsgeschwindigkeit für Daten eines Teilnehmers zu erhöhen. Um Daten schneller zu übertragen, muss aber mehr Sendeleistung aufgewandt werden, da ein größerer Signal/Rauschabstand nötig ist. Dies ist jedoch in diesem Fall kein Problem, da es nur wenige andere Teilnehmer gibt, die sich auf

das für sie erhöhte Rauschniveau entsprechend einstellen können.

Kommunizieren viele Teilnehmer gleichzeitig mit einer Basisstation, dann erzeugen aus Sicht eines Teilnehmers viele andere Teilnehmer zusammen ein hohes Hintergrundrauschen. Somit muss jeder Teilnehmer mit mehr Leistung senden, um das Hintergrundrauschen zu überwinden. Da dies bei allen Teilnehmern möglich ist, bleibt das System stabil. Die zur Verfügung stehende maximale Übertragungsgeschwindigkeit ist nun nicht nur durch die 5 MHz Bandbreite begrenzt, sondern für jeden einzelnen auch noch durch das erhöhte Rauschen. Daten können jetzt unter Umständen für einen Teilnehmer nicht mehr so schnell übertragen werden, wie noch in der vorherigen Situation, da der Signal/Rauschabstand für weiter entfernte Teilnehmer nicht mehr erreicht werden kann.

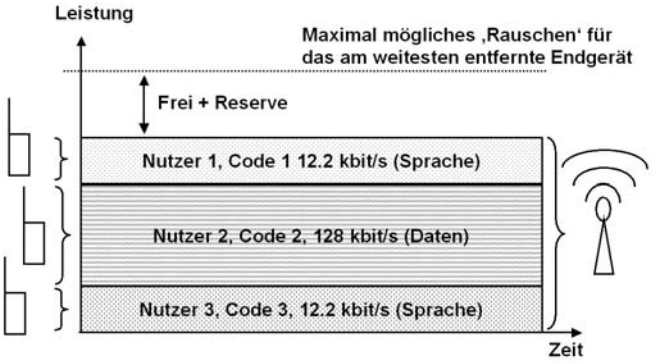

Abb. 3.7a: Gleichzeitige Kommunikation mehrerer Teilnehmer mit einer Basisstation in Uplink Richtung. (Achsen nicht maßstäblich, Anzahl der Nutzer pro Basisstation in Praxis wesentlich größer)

Sendeleistung ist begrenzt

Die Sendeleistung kann aber nicht beliebig erhöht werden, da diese für UMTS Endgeräte in Europa auf 0.250 Watt begrenzt ist. Würde das Zugangsnetz die Sendeleistung der Teilnehmer nicht aktiv regeln, könnte es zu Situationen kommen, in denen zu viele Teilnehmer vorhanden sind. Da die Signale aller anderen Teilnehmer als Rauschen gesehen werden, ist es auch mit der maximalen Sendeleistung eines Mobiltelefons nicht mehr möglich, einen akzeptablen Signal/Rauschabstand zu erzeugen. Schlimmer noch: Sendet das Mobiltelefon trotzdem, wird auch das Rauschen für alle anderen Teilnehmer weiter erhöht und somit werden auch die Verbindungen anderer Teilnehmer gestört.

Aus mathematischer Sicht löst das Code Division Multiple Access (CDMA) Verfahren den gleichzeitigen Medienzugriff wie folgt:

Umwandlung von Bits in Chips

Nutzdatenbits werden nicht direkt über die Luftschnittstelle übertragen, sondern zuerst mit einem Vektor multipliziert, der z.B. eine Länge von 128 hat. Das Ergebnis dieser Multiplikation ist wieder ein Vektor, ebenfalls mit der Länge 128. Die Elemente dieses Ergebnisvektors werden „Chips" genannt. Ein Vektor mit Länge 128 hat also 128 Chips. Statt also ein Bit über die Luftschnittstelle zu übertragen, werden 128 Chips übertragen. Dieses Verfahren wird „Spreizen" (Spreading) genannt, da 128 mal mehr Informationen übertragen werden, als beim bloßen übertragen des Bits. Auf der Gegenseite kann diese Multiplikation wieder rückgängig gemacht werden und aus den 128 Chips kann wieder auf das gesendete Bit zurückgerechnet werden.

Abbildung 3.8 zeigt die dazugehörigen mathematischen Operationen mit 2 Sendern (also Mobiltelefone), die gleichzeitig Daten zu einem Empfänger (Basisstation) senden.

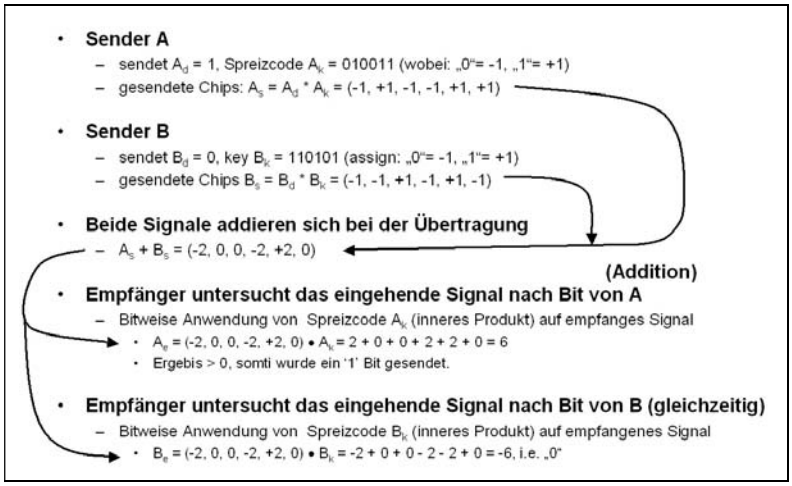

Abb. 3.8: Gleichzeitige Kommunikation von zwei Teilnehmern mit einer Basisstation durch Spreizen des Signals.

Dem Nachteil, dass statt einem Bit nun 128 Chips übertragen werden, stehen zwei wesentliche Vorteile gegenüber: Fehler, die sich während der Übertragung von 128 Chips über die Luftschnittstelle einschleichen, können erkannt und korrigiert werden. Selbst wenn einige Chips durch Übertragungsfehler verändert werden, ist die Wahrscheinlichkeit sehr groß, dass das in den 128 Chips kodierte Bit trotzdem richtig erkannt wird. Für die

Umrechung des Bits in die Chips wird jedem Teilnehmer ein eigener Vektor zugeteilt, der auch „Code“ genannt wird. Der Empfänger kann die Sender voneinander trennen, da die Codes im mathematischen Sinne orthogonal zu einander sind.

3.3.1 Spreizfaktor, Chiprate und Prozessgewinn

Die Kodierung eines Bits in mehrere Chips wird als Spreizen (Spreading) bezeichnet. Der Spreizfaktor (Spreading Factor) gibt dabei an, wie viele Chips pro Bit verwendet werden. Die Geschwindigkeit, mit der Chips bei UMTS über die Luftschnittstelle übertragen werden (Chip Rate), ist unabhängig vom Spreizfaktor konstant 3.84 MChips/s.

Vor- und Nachteile eines großen Spreizfaktors

Ein größerer Speizfaktor bedeutet bei konstanter Chip Rate, dass die Datenrate für den Benutzer sinkt. Dies hat neben der größeren Robustheit gegen Übertragungsfehler auch noch weitere Vorteile: Je länger der Code, desto mehr Codes gibt es, die orthogonal zueinander sind. Das bedeutet, dass mehr Benutzer gleichzeitig den Übertragungskanal nutzen können, als bei kürzeren Codes. Da mehr Chips pro Bit verwendet werden, kann außerdem der Signal/Rauschabstand reduziert werden. Dies erzeugt zwar mehr Chipfehler, durch die größere Anzahl der Chips pro Bit kann das übertragene Bit aber trotzdem korrekt berechnet werden. Da durch den geringeren Signal/Rauschabstand die Sendeleistung verringert werden kann, wird auch von einer Erhöhung des Prozessgewinns (Processing Gain) gesprochen.

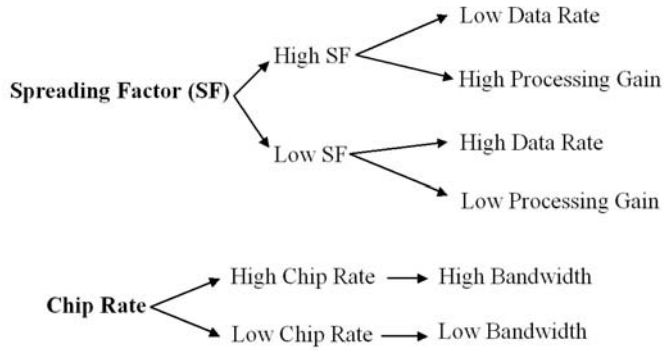

Abb. 3.9: Zusammenhang zwischen Spreizfaktor, Chiprate, Prozessgewinn und verfügbare Bandbreite für einen Teilnehmer.

Vor- und Nachteile eines kleinen Spreizfaktors

Bei kurzen Codes, sprich bei weniger Chips pro Bit, erhöht sich die Übertragungsgeschwindigkeit für einen einzelnen Benutzer. Dies hat jedoch auch zwei Nachteile: Aufgrund der kürzeren Codes können weniger Benutzer gleichzeitig mit einer Basisstation kommunizieren. Bei einer Codelänge von 8, das einer Nutzdatenrate von 384 kbit/s im Downlink entspricht, können nur maximal 8 Teilnehmer gleichzeitig in dieser Geschwindigkeit Daten von einer Basisstation erhalten. Wäre die Codelänge z.B. 256, könnten bis zu 256 Teilnehmer gleichzeitig mit der Basisstation kommunizieren, wenn auch wesentlich langsamer. Außerdem wird bei einem kleineren Spreizfaktor der Prozessgewinn geringer. Das bedeutet für den einzelnen Teilnehmer, dass er mit größerer Leistung senden muss, um Anzahl der Übertragungsfehler zu verringern. Gleichzeitig steigt dadurch natürlich auch das Rauschen für die anderen Teilnehmer.

3.3.2 Der OVSF Codebaum

Auf der UMTS Luftschnittstelle ist die Chiprate fest mit 3.84 MChips/s vorgegeben. Wäre auch der Spreizfaktor fest vorgegeben, würde dies bedeuten, dass alle Teilnehmer einer Zelle mit der gleichen Geschwindigkeit senden und empfangen müssten. Dies ist jedoch nicht erwünscht, da in einer Zelle sowohl Dienste mit niedriger Übertragungsgeschwindigkeit, wie z.B. Sprachtelefonie und Dienste mit hoher Übertragungsgeschwindigkeit, wie z.B. Web Surfen oder Video Streaming möglich sein sollen.

Variable Spreizfaktorlängen mit OVSF

Die Lösung dieses Problems heißt Orthogonal Variable Spreading Factors, kurz OVSF. Während bei der vorhergehenden mathematischen Betrachtung davon ausgegangen wurde, dass die Spreading Codes aller Teilnehmer die gleiche Länge, also den gleichen Spreizfaktor besitzen, bietet das OVSF Prinzip die Möglichkeit, unterschiedlich lange Codes gleichzeitig zu verwenden.

Damit unterschiedlich lange Codes trotzdem orthogonal zueinander sind, gilt folgende Bedingung, die in Abbildung 3.10 grafisch dargestellt wird: Im einfachsten Fall (C1,1) ist der Vektor eindimensional. Auf der nächsten Ebene gibt es im binären Raum 4 Vektoren und zwei, die zueinander orthogonal sind (C2,1 und C2,2). Auf der dritten Ebene gibt es 16 Vektoren und 4, die zueinander orthogonal sind (C4,1 bis C4,4), usw. Auf diese Weise entsteht ein Baum von Vektoren, die auf ihrer Ebene jeweils orthogonal zueinander sind. Je größer der Spreizfaktor, desto mehr Teilnehmer können gleichzeitig kommunizieren, der Baum wird breiter.

Verwendet nun ein Teilnehmer z.B. ein Spreizfaktor von 8, so bedeutet dies, dass alle Codes auf allen weiteren Hierarchieebenen dieses Zweiges nicht mehr verwendet werden dürfen. Diese sind nicht mehr orthogonal mit dem verwendeten Code mit Spreizfaktor 8 auf der höheren Baumebene. Da es aber auf der Stufe mit SF 8 noch sieben andere Teilbäume gibt, können andere Teilnehmer durchaus mit größeren Spreizfaktoren kommunizieren. Es bleibt dabei dem Netzwerk überlassen, wie viele Codes mit welchen Spreizfaktoren verwendet werden. Somit hat das Netzwerk die Möglichkeit, auf unterschiedliche Nutzungssituationen zu reagieren.

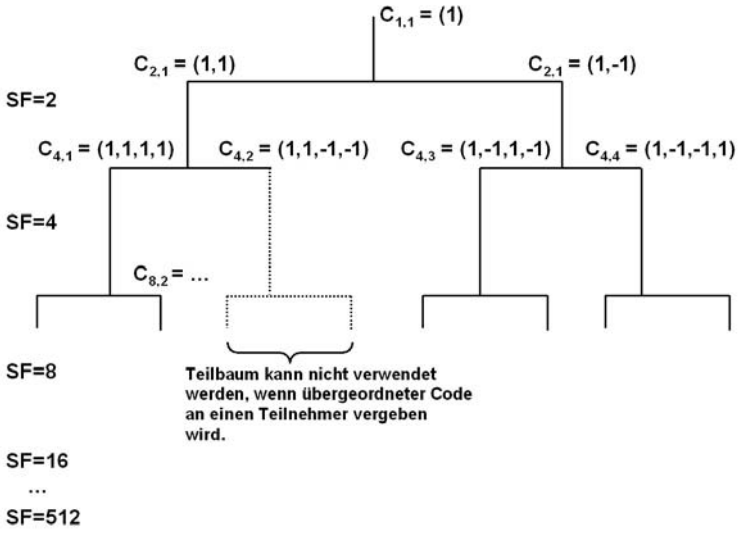

Abb. 3.10: Der OVSF Codebaum

Unterschiedliche Spreizfaktoren für verschiedene Anwendungen

Nachfolgende Tabelle stellt einige Spreizfaktoren im Downlink, also von Node-B zum Endgerät, mit der Brutto- und Nettodatenrate gegenüber. Die Bruttodatenrate ist dabei die Anzahl der übertragenen Bits pro Sekunde. Die Nettodatenrate entsteht aus der Bruttodatenrate abzüglich Channel Coding wie z.B. Fehlererkennung, Fehlerkorrektur, Signalisierungsdaten, Kanalregelung etc.

Spreizfaktor (Downlink)	Brutto Datenrate (kbit/s)	Netto Datenrate (kbit/s)	Anwendung
8	960	**384**	Packet Data
16	480	**128**	Packet Data
32	240	**64**	Packet Data und Videotelefonie
64	120	**32**	Packet Data
128	60	**12.2** **8**	Sprache Packet Data
256	30	**5.15**	Sprache
512	15	**1.7**	Signalisierung, SMS, Location Update…

3.3.3 Scrambling in Uplink- und Downlink Richtung

Über OVSF Codes kann die Datenrate jedes Teilnehmers individuell angepasst werden und unterschiedliche Datenströme können voneinander unterschieden werden. Da manche Codes jedoch keine Zufallsmuster aufweisen (z.B. C(256,1), der nur aus '1' Chips besteht), gäbe es bei direkt anschließender Modulation keine gleichmäßig spektrale Verteilung.

Scrambling

Um dies zu vermeiden, wird nach dem Spreizen noch ein weiterer Verarbeitungsschritt benötigt, das Scrambling. Der aus den Bits entstandene Chipstream wird, wie in Abbildung 3.11 gezeigt, in diesem Schritt mit einem Pseudo Zufallscode (Scrambling Code) multipliziert. Die Chiprate von 3.84 MChips/s ändert sich dadurch aber nicht.

Scrambling im Downlink

In Downlink Richtung wird der Scrambling Code außerdem verwendet, um unterschiedliche Basisstationen voneinander zu

unterscheiden. Dies ist notwendig, da alle Basisstationen auf der gleichen Frequenz senden. Außerdem ist dies notwendig, damit eine Basisstation den kompletten Codebaum verwenden kann und sich diesen nicht mit den Nachbarstationen teilen muss. In Downlink Richtung wird die maximale Übertragungskapazität somit für alle Teilnehmer hauptsächlich durch die Anzahl der Codes aus dem Codebaum bestimmt, sowie der Interferenz von anderen Basisstationen relativ von jedem Teilnehmer aus gesehen.

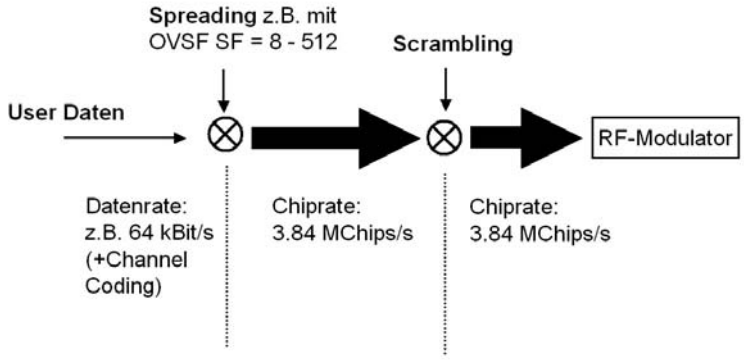

Abb. 3.11: Spreading und Scrambling

Scrambling im Uplink

In Uplink Richtung hingegen bekommt jeder Teilnehmer seinen eigenen Scrambling Code. Somit stehen jedem mobilen Teilnehmer alle Codes des Codebaums zur Verfügung. In der Uplink Richtung ist das System also nicht durch die Anzahl der Codes, sondern durch die maximale Sendeleistung des Endgeräts begrenzt, sowie der Interferenz, die andere Teilnehmer in der Umgebung erzeugen.

Timing Advance durch Scrambling nicht nötig

Ein weiterer Grund für den individuellen Scrambling Code per Teilnehmer im Uplink sind die auftretenden Signallaufzeiten. Da sich Teilnehmer in unterschiedlichen Abständen zu einer Basisstation befinden, erreichen deren Signale die Basisstation zu unterschiedlichen Zeiten. Bei GSM wurde dies durch die Timing Advance Regelung (siehe Kapitel 1.7.4) ausgeglichen. Bei UMTS ist eine solche Regelung aber nicht möglich, da im Soft Handover Zustand (siehe Kapitel 3.7.1) ein Teilnehmer gleichzeitig mit mehreren Basisstationen kommuniziert und das Timing aufgrund unterschiedlicher Abstände nicht für mehrere Basisstationen

gleichzeitig regeln kann. Würde kein individueller Scrambling Code verwendet werden, würde die am Anfang des Kapitels beschriebene Mathematik nicht mehr funktionieren. Einzelne Bits würden zueinander vorschoben eintreffen, und das Ergebnis würde sich somit ändern.

	Downlink	**Uplink**
Spreading	• Adressierung unterschiedlicher Nutzer. • Individuelle Datenrate für jeden Nutzer.	• Steuerung der Datenrate
Scrambling	• Gleichmäßige spektrale Verteilung. • Unterscheidung der Basisstationen.	• Gleichmäßige spektrale Verteilung. • Unterscheidung der Teilnehmer. • Durch Scrambling kein Timing Advance notwendig, um Orthogonalität zu gewährleisten.

3.3.4 Frequenz- und Zellplanung in UMTS

Da in UMTS alle Zellen die gleiche Frequenz verwenden, ist die Frequenzplanung gegenüber GSM stark vereinfacht. Während es bei GSM absolut vermieden werden musste, bei benachbarten Zellen die gleiche Frequenz zu verwenden, wird genau dies bei UMTS gemacht. Dies ist auf Grund der vorgestellten Eigenschaften von CDMA möglich. Während bei GSM eine Frequenzplanung unabdingbar war, die zudem durch neue Zellen zur Kapazitätserhöhung immer wieder geändert werden muss, ist dies bei UMTS nicht mehr notwendig. Wird hier eine neue Zelle in Betrieb genommen, muss jedoch die Sendeleistung der benachbarten Zellen verringert werden, da diese dann nur noch kleinere geographische Gebiete abdecken müssen. Aus einer Frequenz-

Interfrerenzplanung

planung in GSM ist eine Interferenzplanung bei UMTS geworden, die jedoch nicht weniger kompliziert ist.

Wichtig sind auch bei UMTS in gleicher Weise wie bei GSM die Nachbarschaftsbeziehungen zwischen den einzelnen Zellen im Zugangsnetz. Nur bei korrekter Definition können Handover (vgl. Kapitel 3.7.1) und Cell Reselections (vgl. Kapitel 3.7.2) richtig funktionieren. Je besser der Zellwechsel funktioniert, je weniger Interferenzen treten im System auf, und umso höher ist die nutzbare Übertragungskapazität über alle Zellen gesehen.

3.3.5 Near-Far Effekt und Zellatmung

Da alle Teilnehmer auf der gleichen Frequenz senden, ist Interferenz der hauptsächlich limitierende Faktor in einem UMTS Netzwerk. In Zusammenhang damit stehen folgende zwei CDMA spezifische Phänomene:

Near-Far Effect

Um Interferenzen gering zu halten, ist eine sehr präzise und schnelle Leistungsregelung erforderlich. Weiter entfernte Teilnehmer müssen dabei mit mehr Leistung senden, als näher an der Basisstation befindliche Teilnehmer, da sich das Signal auf dem weiteren Weg stärker abschwächt. Dieser Effekt wird Near-Far Effect genannt. Auch kleine Positionsänderungen wie z.B. ein Schritt hinter eine Hauswand relativ zur Basisstation gesehen, hat schon große Auswirkungen auf die nötige Sendeleistung. Wie wichtig die Leistungsregelung ist, zeigt die Tatsache, dass bei UMTS die Leistungsregelung 1500 mal in der Sekunde für jeden Teilnehmer erfolgt. Einen angenehmen Nebeneffekt für die Teilnehmer ist dabei, dass bei guter Verbindung nur wenig Sendeleistung verwendet werden muss und somit die Laufzeit einer Akkuladung erhöht wird.

Anmerkung: Auch in GSM gibt es eine Leistungsregelung. Die Regelgeschwindigkeit liegt dort jedoch nur im Sekundenbereich, da die Interferenz hier eine wesentlich weniger wichtige Rolle spielt. Leistungsregelung wird hier hauptsächlich verwendet, um die Lebensdauer des Akkus zu erhöhen.

Zellatmung

Die Abhängigkeit der UMTS Teilnehmer von der Interferenz hat auch noch einen weiteren unerwünschten Nebeneffekt. Nehmen wir folgendes an:

1. Es befindet sich schon eine größere Anzahl von Teilnehmern mit unterschiedlichen Abständen im Versorgungsbereich der Basisstation.

2. Aufgrund der Interferenzen ist der am weitesten entfernte Teilnehmer gezwungen, mit seiner maximalen Leistung zu senden.
3. Nun versucht noch ein weiterer Teilnehmer, der sich in mittlerem Abstand zum Zentrum der Zelle befindet, eine Verbindung zum Netzwerk aufzubauen.

In dieser Situation kann nun folgendes passieren: Akzeptiert das Netzwerk die zusätzliche Verbindung, erhöht sich für alle Teilnehmer der Zelle die Interferenz. Die Teilnehmer sind deshalb gezwungen, ihre Sendeleistung entsprechend zu erhöhen. Der Teilnehmer am Rand der Zelle sendet jedoch schon mit seiner maximalen Leistung und kann deshalb seine Sendeleistung nicht weiter erhöhen. Somit kann er von der Basisstation nicht mehr korrekt empfangen werden und die Kommunikationsverbindung bricht für ihn ab. Von außen betracht, ändert sich somit die maximal mögliche geographische Versorgungsfläche einer Zelle, da der am weitesten entfernte Teilnehmer nun nicht mehr kommunizieren kann. Dieses Verhalten wird Zellatmung (Cell Breathing) genannt, da das Verhalten ähnlich einer Lunge ist, die ihr Volumen während des Atmens vergrößert und verkleinert.

Um diesen Effekt zu vermeiden, kontrolliert das Netzwerk ständig den Signal/Rauschabstand jedes Teilnehmers. Durch aktive Leistungsregelung jedes Teilnehmers weis das Netzwerk, dass durch einen weiteren Teilnehmer eine bereits bestehende Kommunikationsverbindung abreißen würde. Das Netzwerk kann somit z.B. die Entscheidung treffen, den zusätzlichen Teilnehmer abzuweisen.

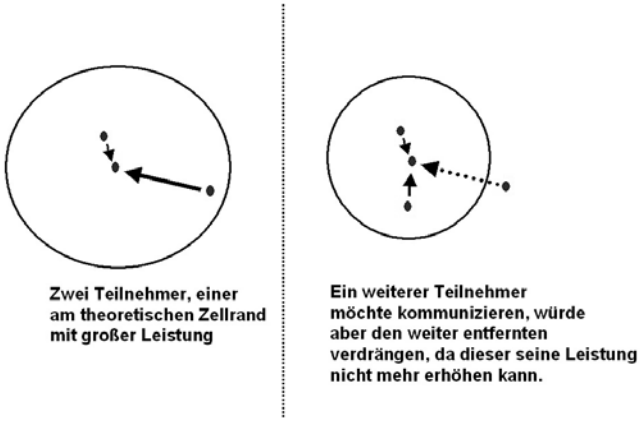

Abb. 3.12: Zellatmung

Um alle bestehenden Verbindungen beizubehalten und zusätzlich auch dem neuen Teilnehmer die Kommunikation zu ermöglichen, kann das Radionetzwerk auch eine andere Strategie anwenden: Ziel dieser Strategie ist es, das Interferenzniveau soweit zu senken, dass alle Teilnehmer kommunizieren können. Dies kann durch unterschiedlichste Verfahrensweisen erreicht werden. Eine Möglichkeit ist, den aktiven Teilnehmern längere Spreizcodes zuzuweisen. Wie in Kapitel 3.3.2 gezeigt wurde, kommen Teilnehmer mit einem längeren Spreizcode mit einer kleineren Sendeleistung aus. Dies wiederum senkt die Interferenz für alle anderen. Nachteil für Teilnehmer, deren Spreizfaktor geändert wurde, ist jedoch, dass ihre Datenübertragungsgeschwindigkeit sinkt. Bei welchen Teilnehmern der Spreizfaktor geändert wird, kann auf die unterschiedlichsten Weisen vom System entschieden werden. UMTS Teilnehmer können z.B. in unterschiedliche Nutzerklassen eingeteilt werden. Die Neuzuteilung der Spreizcodes kann dann z.B. zuerst bei Teilnehmern erfolgen, die eine einfache Nutzerklasse haben, dafür aber z.B. weniger bezahlen. Auch ist es denkbar, schon vor der maximalen Lastgrenze die Zuteilung von kürzeren Spreizcodes ganz oder nur auf bestimmtes Nutzerklassen zu begrenzen.

Übertragungsgeschwindigkeit und Distanz zur Basisstation

Neben der Zellatmung gibt es noch eine Reihe anderer Interferenzszenarien. Wie bereits erwähnt, muss bei kleineren Spreizfaktoren die Sendeleistung erhöht werden, um eine korrekte Übertragung zu gewährleisten. Somit hängt die maximal mögliche Entfernung eines Teilnehmers zur Basisstation auch vom verwendeten Spreizfaktor ab. Bewegt sich ein Benutzer zwischen zwei Zellen, ist es bei einem zu großen Zellabstand oder zu großem Interferenzlevel möglich, dass der aktuell verwendete Spreizfaktor keine Übertragung mehr erlaubt, während ein größerer Spreizfaktor durchaus noch eine Kommunikation bei gleicher Leistung ermöglicht.

Wie dieses und ähnliche Szenarien an Zellgrenzen letztendlich gelöst werden, hängt von der Implementierung des jeweiligen Netzwerklieferanten ab. Wie auch in anderen Bereichen in UMTS schreiben die Standards keine Lösungsmöglichkeit vor. Somit bietet sich für Netzwerkhersteller die Möglichkeit, sich mit guten Lösungen einen Wettbewerbsvorteil zu schaffen und somit am Markt erfolgreich zu sein.

3.3.6 Vorteile des UMTS Radionetzwerkes gegenüber GSM

Nachdem in den vorangegangenen Abschnitten die grundsätzlichen Eigenschaften und Verfahren von W-CDMA bei UMTS vorgestellt wurden, zeigt der folgende Abschnitt, wie die Limitationen von GSM/GPRS mit UMTS gelöst wurden:

Kürzere Verzögerungszeit

Die Hauptursache der langen Verzögerungszeiten bei GPRS ist die ständige Neuzuweisung von Ressourcen, vor allem bei burstartigen Datenübertragungen. Dies ist bei UMTS nicht mehr nötig, da auch für die paketvermittelte Übertragung ein dedizierter Kanal zwischen Teilnehmer und Netzwerk in Form eines Codes verwendet werden kann. Dieser Kanal wird nicht sofort wieder abgebaut, wenn für einige Sekunden keine Daten mehr übertragen werden, sondern steht dem Teilnehmer weiterhin zur Verfügung. In der Downlink Richtung werden während einer inaktiven Phase des Nutzers (fast) keine Daten übertragen. Der Code steht zwar für andere Teilnehmer nicht zur Verfügung, da jedoch bis auf Kontrollnachrichten keine Daten übertragen werden, sinkt der Interferenzlevel für alle anderen Teilnehmer und es geht nur sehr wenig Kapazität durch Aufrechterhaltung des Kanals verloren. Erst wenn für eine längere Zeit keine Daten übertragen werden, wird der Übertragungskanal modifiziert, um auch den Code freizugeben. Das System kann dazu zum Beispiel einen Code mit höherem Spreizfaktor vergeben, von denen weit mehr zur Verfügung stehen, als von Codes mit kürzeren Spreizfaktoren. Wird die Datenübertragung wieder aufgenommen, entsteht keine Verzögerungszeit, da ja immer noch ein dedizierter Kanal zur Verfügung steht. Dessen Kapazität kann auch schnell wieder erhöht werden, indem das Netzwerk wieder einen Code mit kleinerem Spreizfaktor vergibt. Bei noch längerer Inaktivität ist es auch möglich, dem Teilnehmer alle Ressourcen auf der Luftschnittstelle zu entziehen, ohne die logische Verbindung zu beenden. Dies spart weitere Ressourcen und auch Batteriekapazität im Endgerät des Teilnehmers, bringt aber eine längere Reaktionszeit mit sich, wenn die Datenübertragung wieder aufgenommen wird. Im Uplink finden prinzipiell die gleichen Methoden Anwendung. Jedoch ist zu berücksichtigen, dass während dem Teilnehmer einen Code zugeteilt ist, sich die Mobilstation ständig im Sendebetrieb befindet. Zwar ist die Sendeleistung während einer Pause der Nutzdatenübertragung geringer, jedoch werden weiterhin Kontrollinformationen mit dem Netzwerk ausgetauscht. Deshalb ist es sehr sinnvoll, bei längerer Inaktivität in den Cell-FACH Zustand zu wechseln. In diesem

Zustand werden keine ständigen Kontrollinformationen mehr vom Endgerät an das Netzwerk übertragen, und dem Endgerät ist auch kein Spreizcode mehr zugeteilt. Mehr dazu im Kapitel 3.5.4.

Keine Unterbrechung bei Zellwechseln

Die Vergabe eines dedizierten Kanals nicht nur für die leitungsvermittelte-, sondern auch für paketvermittelte Datenübertragung, bringt auch beim Zellwechsel gegenüber GPRS wesentliche Vorteile. Bei GPRS wird der Zellwechsel von der Mobilstation selbständig durchgeführt. Danach muss das Endgerät zuerst den Broadcast Kanal abhören, bevor die Verbindung mit dem Netzwerk wiederhergestellt werden kann. Dies bedeutet in der Praxis eine Unterbrechung der Übertragung von 1-3 Sekunden. Ein Handover, der vom Netzwerk kontrolliert wird und somit keine oder nur geringe Unterbrechungen beim Zellwechsel mit sich bringt, ist für GPRS nicht vorgesehen. Vor allem während Datenübertragungen aus Autos oder Zügen macht sich dies störend bemerkbar. Bei UMTS hingegen gibt es keine Unterbrechung beim Zellwechsel, da der Zellwechsel hier per Soft Handover vom Netzwerk kontrolliert wird. Somit werden Datenübertragungen aus fahrenden Objekten wesentlich effizienter als bisher. Außerdem sind so Anwendungen wie Telefonie über IP (VoIP) oder Videotelefonie über IP während Zug- oder Autofahrten erst möglich.

Größere Bandbreite

Ein weiteres Problem bei GSM ist die historisch bedingte Auslegung auf schmalbandige Sprachtelefonie. Dies konnte mit GPRS zwar per Timeslotbündelung überwunden werden, die maximale Datenrate bleibt aber weiterhin aufgrund einer Bandbreite von nur 200 kHz pro Trägers sehr begrenzt. Bei UMTS wurde jedoch von vorneherein darauf Wert gelegt, dass auch breitbandigere Datendienste möglich sind. So ist bei einem Spreizfaktor von 8 im Downlink eine Übertragungsgeschwindigkeit von 384 kbit/s möglich. Auch im Uplink ist eine Übertragungsgeschwindigkeit von 384 kbit/s möglich, allerdings nur bei sehr gutem Empfang. Aufgrund der schwächeren Sendeleistung und einer omnidirektionalen Antenne werden im Uplink ansonsten Geschwindigkeiten von 64 und 128 kbit/s erreicht. Diese Übertragungsgeschwindigkeiten eignen sich sowohl für schnelles Websurfen, wie auch für Applikationen wie VoIP oder Videotelefonie, die mit GPRS aufgrund der schmalbandigen Auslegung, langen Verzögerungszeiten und der Übertragungsunterbrechung bei Zellwechsel nicht möglich sind.

Videotelefonie mit 64 kbit/s Verbindungen

Mit UMTS sind auch leitungsvermittelte 64 kbit/s Datenverbindungen in Up- und Downlink möglich. Dies entspricht der Ge-

schwindigkeit einer ISDN Verbindung und wird hauptsächlich für Videotelefonie zwischen UMTS Teilnehmern verwendet.

Flexible Codeänderung

Das UMTS Netz kann auch sehr flexibel auf die aktuelle Signalqualität des Teilnehmers reagieren. Entfernt dieser sich vom Zellmittelpunkt, kann sein Spreizfaktor erhöht werden. Zwar wird seine Datenrate sinken, sein Übertragungskanal kann aber weiterhin aufrechterhalten werden.

Auch auf unterschiedliche Lastzustände kann das UMTS Netzwerk sehr flexibel reagieren. Wird die Interferenz zu hoch, oder werden die zur Verfügung stehenden Codes des Codebaumes knapp, kann neuen oder schon kommunizierenden Teilnehmern ein größerer Spreizfaktor zugewiesen werden.

Weitere Vorteile des CDMA Ansatzes ist der Soft Handover, der in Kapitel 3.7.1 beschrieben wird. Durch Verwendung verschiedener Sprachcodecs ist es auch möglich, verschiedene Spreizfaktoren für Sprachverbindungen zu verwenden und diesen auch während eines laufenden Gesprächs zu ändern. Näheres dazu siehe Kapitel 3.5.3. Somit kann auch hier wiederum auf verschiedene Situationen des Benutzers und der allgemeinen Last der Zelle reagiert werden. Welche Verfahren in welchen Situationen angewandt werden, wird vom Standard nicht vorgeschrieben und kann somit vom Netzwerkhersteller und Netzwerkbetreiber selbst festgelegt werden.

3.4 UMTS Kanalstruktur auf der Luftschnittstelle

3.4.1 User Plane und Control Plane

Grundsätzlich werden bei UMTS, wie auch bei GSM und allen modernen drahtgebundenen Kommunikationsnetzen, zwei unterschiedliche Arten von Daten unterschieden. Diese sind bei UMTS und GSM in zwei so genannte Planes unterteilt: Daten in der User Plane sind Nutzdaten, wie z.B. Sprachtelefoniedaten oder IP Pakete. Die Control Plane hingegen ist für alle Signalisierungsdaten zuständig, die zwischen Benutzer und dem Netzwerk ausgetauscht werden. Über die Control Plane werden z.B. Signalisierungsdaten für den Verbindungsauf- und Abbau gesendet, oder Nachrichten wie z.B. ein Location Update, um das Netzwerk über seinen aktuellen Standort zu informieren. Abbildung 3.13 zeigt die Unterteilung in User- und Control Plane, sowie einige Beispiele für Protokolle, die in den einzelnen Planes verwendet werden.

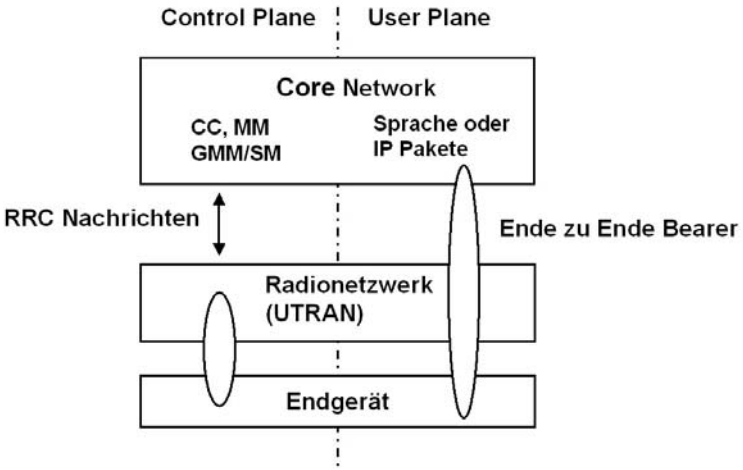

Abb. 3.13: User und Control Plane

3.4.2 Common und Dedicated Kanäle

Sowohl User Plane Daten als auch Control Plane Daten werden bei UMTS über die Luftschnittstelle in Channels (Kanälen) übertragen. Dabei unterscheidet man grundsätzlich drei Kanalarten:

Dedicated Channels

Dedicated Channels: Diese Kanäle übertragen Daten für einen einzelnen Benutzer. Ein Dedicated Channel überträgt also zum Beispiel eine Sprachverbindung, IP Pakete von und zu einem Teilnehmer, oder eine Location Update Nachricht.

Common Channels

Das Gegenstück sind Common Channels, deren übertragene Daten von allen Endgeräten einer Zelle empfangen werden. Ein Beispiel für einen solchen Kanal ist der Broadcast Channel. Dieser überträgt für alle Teilnehmer allgemeine Informationen über die Zelle und das Netzwerk. Common Channels können auch für die Nutzdatenübertragung für mehrere Endgeräte verwendet werden. Jedes Endgerät filtert dabei seine eigenen Pakete aus dem Datenstrom heraus und leitet nur diese an höhere Protokollschichten weiter.

Shared Channels

Den Common Channels sehr ähnlich sind Shared Channels: Diese Kanäle werden nicht von allen Endgeräten abgehört, sondern nur von solchen, die vom Netzwerk dazu aufgefordert wurden. Ein Beispiel hierfür ist der Downlink Shared Channel.

Die paketvermittelte Nutzdatenübertragung ist jedoch nicht auf den Downlink Shared Channel beschränkt. Dieser Kanal kann optional mit einem Dedicated Channel verwendet werden, um

z.B. IP Pakete zu übertragen. Da dieser Kanal optional ist, ist davon auszugehen, dass die Netzwerkausrüster und Endgerätehersteller zuerst die paketvermittelnde Datenübertragung über Dedicated Channels und den FACH implementieren und erst später über den Downlink Shared Channel.

HSDPA

Die Weiterentwicklung des Downlink Shared Channel Konzepts ist der High Speed Downlink Packet Access (HSDPA) in UMTS Release 5. Dieser führt neben der Codebündelung im Downlink auch ein neues Modulationsverfahren auf der Luftschnittstelle ein, um Daten bei guten Empfangsbedingungen eines Endgeräts schneller übertragen zu können.

3.4.3 Logische, Transport- und Physikalische Kanäle

Um die logische Datenübertragung von den physikalischen Eigenschaften der Luftschnittstelle zu entkoppeln, wurden bei UMTS drei unterschiedliche Kanalschichten spezifiziert. In Abbildung 3.14 werden die nachfolgend beschriebenen Downlinkkanäle dargestellt, in Abbildung 3.15 die Uplinkkanäle.

Logische Kanäle

Die oberste Kanalschicht bilden die Logical Channels (logische Kanäle). Mit logischen Kanälen werden die unterschiedlichen Arten von Daten unterschieden, die über die Luftschnittstelle übertragen werden. Sie enthalten keinerlei Informationen, wie diese später physikalisch über die Luftschnittstelle übertragen werden. Zu den logischen Kanälen gehören:

BCCH

Der BCCH (Broadcast Control Channel): Dieser Kanal wird von allen Teilnehmern im Idle Zustand abgehört, um Systeminformationen zu erhalten. Dazu gehören Information, wie auf das Netzwerk zugegriffen werden kann, welche Nachbarzellen mit welchen Codes senden und vieles mehr. Diese Informationen werden in so genannten System Information Blocks (SIBs) übertragen. Eine genaue Beschreibung der SIBs ist im 3GPP Standard 25.331, Kapitel 10.2.48.8 zu finden.

PCCH

Der PCCH (Paging Control Channel): Auf diesem Kanal werden Teilnehmer über eingehende Telefonanrufe oder SMS Nachrichten informiert. Auch für die paketvermittelte Datenübertragung wird eine Paging Nachricht für den Fall gesendet, dass das Netzwerk nach langer Inaktivität dem Teilnehmer alle für ihn reservierten Ressourcen auf der Luftschnittstelle entzogen hat (z.B. RRC Idle Mode) und plötzlich neue Datenpakete aus dem Kernnetz für die Übertragung zum Teilnehmer eintreffen. In diesem Fall muss sich das Endgerät erst wieder beim Netzwerk

melden, damit eine logische RRC Verbindung aufgebaut werden kann. Erst danach können wieder Nutzdaten zum Endgerät übertragen werden.

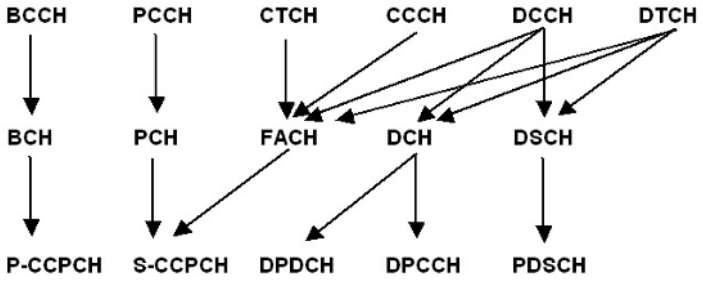

Abb. 3.14: Logische-, Transport- und Physikalische Kanäle im Downlink

CCCH

Der CCCH (Common Control Channel): Dieser Kanal wird für alle Nachrichten von und zu Teilnehmern verwendet (bidirektional), die eine Verbindung zum Netzwerk aufbauen wollen. Dies ist z.B. nötig, wenn der Benutzer z.B. einen Telefonanruf machen möchte, eine SMS versendet oder eine paketvermittelnde Datenverbindung aufbaut.

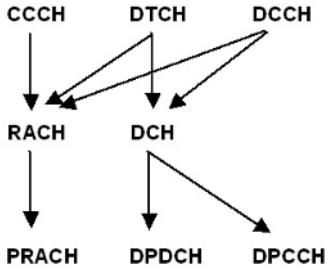

Abb 3.15: Logische-, Transport- und Physikalische Kanäle im Uplink

DCCH

Der DCCH (Dedicated Control Channel): Während die drei zuvor beschriebenen Kanäle Common Channels sind, ist ein DCCH immer nur für jeweils einen Benutzer gedacht. In diesem Kanal werden Nachrichten für die Protokolle Mobility Management (MM) und Call Control (CC) für leitungsvermittelnde Dienste, sowie Packet Mobility Management (PMM) und Session Management (SM) Nachrichten für paketvermittelnde Dienste von und zu Kernnetzwerkkomponenten wie MSC und SGSN übertragen. Diese Protokolle sind in Kapitel 3.6 und 3.7 näher beschrieben.

DTCH

Der DTCH (Dedicated Traffic Channel): Auch dieser Kanal ist wie der DCCH nur für einen einzelnen Benutzer gedacht und dient zur Übertragung der eigentlichen Nutzdaten. Nutzdaten können z.B. ein leitungsvermitteltes Telefongespräch oder paketvermittelte IP Daten sein. Während für ein Telefongespräch zwingend auch ein physikalischer Dedicated Channel verwendet werden muss, ist dies für IP Pakete aber nicht unbedingt erforderlich. Wie in Abbildung 3.14 dargestellt, kann der DTCH deshalb nicht nur auf Dedicated Transport- und Physical Channels abgebildet werden, sondern auch auf Common/Shared Channels.

Anmerkung: In der Praxis werden auch IP Pakete meistens über einen Dedicated Physical Channel übertragen. Common/Shared Physical Channels (z.B. der nachfolgend vorgestellte FACH) werden nur verwendet, wenn ein Teilnehmer lange Zeit inaktiv war und nur von Zeit zu Zeit kleine Datenmengen sendet bzw. empfängt. Shared Channels können im umgekehrten Fall aber auch verwendet werden, um die Übertragungsgeschwindigkeit eines Teilnehmers zu steigern. Dazu wird einem Teilnehmer zusätzlich zu einem Dedicated Physical Channel ein Downlink Shared Channel oder ein Highspeed Downlink Shared Channel (HSDPA) zugewiesen.

CTCH

Der CTCH (Common Traffic Channel): Über diesen Kanal können Cell Broadcast Informationen versandt werden. In GSM wird der gleiche Mechanismus z.B. von Vodafone-D2 verwendet, um den Anwender über die Festnetzvorwahlen zu informieren, die am aktuellen Ort des Teilnehmers zu einem niedrigeren Tarif zu erreichen sind.

Transport Kanäle

Transportkanäle (Transport Channels) bereiten in der Senderichtung Daten für die Übertragung über die Luftschnittstelle vor. Die Daten aus logischen Kanälen werden dazu durch das RLC/MAC Protokoll in kleine Datenpakete aufgeteilt, die für die Übertragung über die Luftschnittstelle geeignet sind. In der Empfangsrichtung arbeiten die Transport Channels entsprechend umgekehrt. Jedem Datenblock geht ein Header voraus, der die Übertragungsparameter der Luftschnittstelle beschreibt. Beispiele hierfür sind:.

- Größe der Datenpakete (10,20,40 oder 80 ms).
- Art der Datensicherung (CRC Checksumme).
- Format der Kanalcodierung für die Fehlererkennung und Korrektur.

- Rate Matching (Datenratenanpassung), falls die Geschwindigkeit des physikalischen Kanals und des Datenkanals nicht übereinstimmen.
- Kontrolle der Discontinuous Transmission (DTX), falls keine Daten zu senden sind.

All diese Eigenschaften werden in einem so genannten Transportformat zusammengefasst. Die eigentliche Kanalkodierung wird jedoch erst in den physikalischen Kanälen auf dem Node-B durchgeführt. Dies ist sehr wichtig, da vor allem die Kanalcodierung zur Fehlererkennung und Korrektor einen großen Overhead mit sich bringt. Im Kapitel über GSM wurde bereits der Half Rate Convolutional Decoder für die Kanalcodierung beschrieben, der die Datenrate praktisch verdoppelt. Auch bei UMTS wird dieser Kanalkodierer verwendet, hier sind jedoch für diverse Anwendungsfälle auch noch andere Kanalkodierer spezifiziert. Würde die Kanalcodierung bereits auf dem RNC erfolgen, würde sich auch die Datenrate zwischen dem RNC und den angeschlossenen Node-Bs verdoppeln, was aufgrund hoher Leitungskosten mit großen operationellen Kosten verbunden wäre.

Logische Kanäle werden in einem weiteren Verarbeitungsschritt auf folgende Transportkanäle abgebildet:

BCH Der BCH (Broadcast Channel): Transportkanal Variante des logischen BCCH.

DCH Der DCH (Dedicated Channel): Dieser nimmt die Daten aus zwei logischen Kanälen auf, dem logischen Dedicated Traffic Channel (DTCH) und dem logischen Dedicated Control Channel (DCCH). Da Daten in beide Richtungen gesendet werden können, existiert dieser Kanal in Uplink- und Downlink Richtung.

PCH Der PCH (Paging Channel): Transportkanal Variante des logischen PCCH.

RACH Der RACH (Random Access Channel): Der bidirektionale logische Common Control Channel (CCCH) heißt auf der Transportkanalebene in Uplink Richtung RACH. Dieser dient dem Teilnehmer zum Senden von RRC Connection Request Nachrichten, wenn eine Verbindungsaufnahme mit dem Netz gewünscht wird, sowie zum Senden von Paketdaten (im Cell_FACH State), falls kein Dedicated Channel zwischen Teilnehmer und Netzwerk existiert.

FACH Der FACH (Forward Access Channel): Über diesen Kanal sendet das Netzwerk RRC Connection Setup Nachrichten an Teilnehmer, die zuvor über den RACH einen Verbindungswunsch gemeldet

haben. Die Nachricht enthält Informationen darüber, wie der Teilnehmer auf das Netzwerk zugreifen soll. Im Falle der Zuweisung eines Dedicated Channels, enthält die Nachricht z.B. die zu verwendenden Spreadingcodes für Uplink und Downlink Richtung. Auf dem FACH können aber auch Userdaten gesendet werden. Dies ist nur für paketvermittelte Daten sinnvoll, wenn nur kleine Datenmengen zu übertragen sind. Der Teilnehmer ist bei dieser Übertragungsart nicht im Cell_DCH Zustand (siehe Kapitel 3.5.4), sondern im Cell_FACH Zustand. Daten in der Uplink Richtung werden dann statt auf einem Dedicated Channel auf dem RACH übertragen.

DSCH

Der DSCH (Downlink Shared Channel): Wie in Kapitel 3.4.2 erläutert, ist dies ein optionaler Kanal und dient zur Übertragung von Userdaten für mehrere Teilnehmer in der Downlink Richtung. Wie in Abbildung 3.14 gezeigt, erhält er seine Daten aus logischen Dedicated Channels verschiedener Teilnehmer.

Physikalische Kanäle

Physikalische Kanäle (Physical Channels) sind schließlich dafür zuständig, ein physikalisches Transportmedium einem oder mehreren Transportkanälen zur Verfügung zu stellen. Außerdem erfolgt auf dieser Stufe die Kanalcodierung, also das Hinzufügen von Redundanz und Fehlererkennung.

Das Zwischenprodukt zwischen Transportkanälen und physikalischen Kanälen wird Composite Coded Transport Channel (CCTrCh) genannt und ist die Zusammenfassung mehrerer Transportkanäle, die dann anschließend über einen oder mehrere physikalische Kanäle übertragen werden. Dies trägt der Tatsache Rechnung, dass nicht nur mehrere Transportkanäle auf einen physikalischen Kanal gemappt werden können, (z.B. der PCH und FACH auf den S-CCPCH), sondern umgekehrt auch mehrere physikalische Kanäle auf einen einzelnen Transportkanal (z.B. der DPDCH und DPCCH auf den DCH).

Die physikalischen Kanäle im Einzelnen:

P-CCPCH

Der P-CCPCH (Primary Common Control Physical Channel): Dieser Kanal dient für die Ausstrahlung der Broadcast Informationen.

S-CCPCH

Der S-CCPCH (Secondary Common Control Physical Channel): Auf diesem Kanal werden die Transportkanäle PCH und FACH ausgestrahlt. Der Spreadingfaktor für diesen Kanal ist in den Standards dynamisch festgelegt worden. Die möglichen Datenraten reichen von einigen 10 kbit/s bis zu einigen 100 kbit/s. Dies wurde so festgelegt, da der PCH und FACH neben Nachrichten

für den ersten Netzwerkzugriff auch Userdaten transportieren können (vgl. Cell_FACH state). Da diese Verkehrslast nicht von vorneherein bekannt ist, kann der Spreadingfaktor vom Netzbetreiber entsprechend der Verkehrssituation angepasst werden.

PRACH Der PRACH (Physical Random Access Channel): Die physikalische Implementierung der Random Access Channels.

AICH Der AICH (Acquisition Indication Channel): Dieser Kanal ist nicht in den Kanalübersichtsbildern enthalten, da es für diesen physikalischen Kanal kein Mapping zu einem Transportkanal gibt. Dieser Kanal wird ausschließlich zusammen mit dem PRACH für die Verbindungsaufnahme eines Teilnehmers mit dem Netzwerk verwendet. Näheres dazu in Kapitel 3.4.5.

DPDCH Der DPDCH (Dedicated Physical Data Channel): Dieser Kanal ist die physikalische Implementierung eines dedizierten Kanals zu einem Endgerät. Hier werden nicht nur Userdaten, sondern auch Signalisierungsdaten wie Mobility Management und Call Control übertragen.

DPCCH Der DPCCH (Dedicated Physical Control Channel): Dieser wird jeweils im Uplink und Downlink zusätzlich zu einem DPDCH verwendet. Er enthält ausschließlich Layer 1 Informationen wie z.B. die Transmit Power Control (TPC) Bits zur Regelung der Sendeleistung. Außerdem werden in diesem Kanal so genannte Pilot Bits übertragen. Da die Pilot Bits immer den gleichen Wert haben, kann der Empfänger mit diesen eine Kanalschätzung für die Dekodierung des restlichen DPCCH und des dazugehörenden DPDCHs durchführen. Standardisiert ist der DPCCH in 3GPP 25.211, 5.2.1.

PDSCH Der PDSCH (Physical Downlink Shared Channel): Dieser optionale Kanal kann verwendet werden, um paketvermittelte Daten an mehrere Teilnehmer zu versenden. Zwar müssen sich alle Teilnehmer, die Daten auf diesem Kanal empfangen, die Kanalkapazität teilen, das Netzwerk kann aber auf diese Weise Codes aus dem Codebaum sparen, da diese nur begrenzt zur Verfügung stehen.

Zusammenfassung Während die Einteilung bei GSM in logische und physikalische Kanäle noch recht einfach zu verstehen ist, fällt dies bei der Dreiteilung in UMTS in logische-, transport- und physikalische Kanäle schon schwieriger. Deshalb hier eine Zusammenfassung der Kanalarten und ihre wichtigsten Aufgaben:

- **Logische Kanäle**: Beschreiben unterschiedliche Informationsflüsse wie User- und Signalisierungsdaten. Logi-

sche Kanäle enthalten keine Information über die Charakteristiken des Übertragungskanals.

- **Transport Kanäle**: Bereiten die Datenpakete von logischen Kanälen für die Übertragung über die Luftschnittstelle vor. Außerdem wird hier festgelegt, welche Kanalkodierungsverfahren (z.B. Fehlerkorrekturverfahren) in der physikalischen Schicht anzuwenden sind.
- **Physikalische Kanäle**: Beschreiben, wie Daten aus Transportkanälen tatsächlich physikalisch übertragen werden und führen die Kanalkodierung bzw. Dekodierung durch.

Um einen Eindruck zu bekommen, in welcher Weise unterschiedliche Kanäle verwendet werden, folgen nun zwei Beispiele:

3.4.4 Beispiel: Netzwerksuche

Nach dem Einschalten eines Endgeräts erfolgt zuerst die Suche nach einem vorhandenen und geeigneten UMTS Netzwerk. Danach meldet sich das Endgerät beim Netzwerk an und ist ab diesem Zeitpunkt für eingehende Telefonanrufe, Kurznachrichten usw. erreichbar. Beim Ausschalten schreibt das Endgerät die aktuellen Informationen über das Netzwerk (z.B. den von der aktuellen Zelle verwendeten primären Scrambling Code) auf die SIM Karte. Damit kann nach erneutem Einschalten des Endgeräts ein Großteil der nötigen Prozeduren für die Netzwerksuche entfallen. In diesem Beispiel wird jedoch davon ausgegangen, dass bisher keine oder nur ungültige Netzwerkinformationen auf der SIM Karte gespeichert sind. Dies ist z.B. der Fall, wenn die SIM Karte das erste Mal verwendet wird, oder wenn beim Einschalten die auf der SIM Karte beschriebene Zelle nicht mehr gefunden wird. Dies kann z.B. dann vorkommen, wenn der Benutzer ein Endgerät im ausgeschalteten Zustand an einen anderen Ort gebracht hat.

Slot Synchronisation

Wie bei allen Kommunikationsverbindungen, müssen auch bei UMTS Netzwerk und Endgeräte synchronisiert sein. Ohne eine korrekte Synchronisierung ist es z.B. nicht möglich, zum richtigen Zeitpunkt eine RRC Connection Request Nachricht zu senden, oder den Anfang eines Datenframes zu erkennen, der vom Netzwerk gesendet wird. Die erste Aufgabe für das Endgerät nach dem Einschalten ist deshalb, sich mit dem Netzwerk zu synchronisieren. Dazu sucht das Endgerät auf den für UMTS

vergebenen Frequenzen nach dem Primary Synchronization Channel (P-SCH). Wie in Abbildung 3.16 gezeigt, besteht ein UMTS Datenframe aus 15 Slots, die normalerweise jeweils 2560 Chips transportieren. Auf dem P-SCH werden jedoch nur die ersten 256 Chips pro Slot verwendet und alle Basisstationen senden mit dem gleichen Code. Werden mehrere Signale (z.B. von unterschiedlichen Basisstationen) zeitlich verschoben empfangen, synchronisiert sich das Endgerät auf das Timing der Bursts mit der besten Signalqualität.

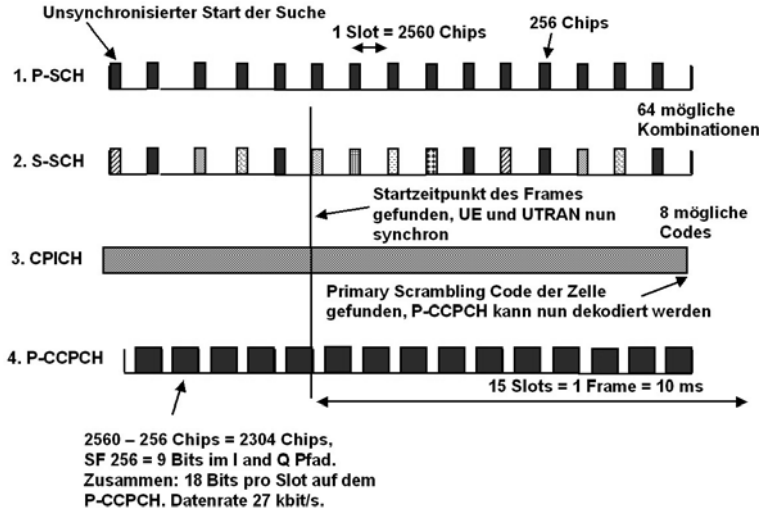

Abb. 3.16: Zellsuche nach Einschalten des Mobiltelefons

Frame Synchronisation

Wurde der P-SCH und somit der Anfang eines Slots gefunden, wird im nächsten Schritt der Anfang eines Frames gesucht. Dazu sucht das Endgerät den Secondary Synchronization Channel (S-SCH). Auch auf diesem Kanal werden in jedem Slot wiederum nur die ersten 256 Chips gesendet, jedoch wird in jedem Slot ein anderes Chipmuster verwendet. Da die Chipmuster und die Reihenfolge bekannt sind, kann das Endgerät somit herausfinden, welcher Slot der erste eines Frames ist. Somit ist nun auch der Beginn eines Frames bekannt.

Suche nach dem Primary Scrambling Code der Zelle

Da alle Basisstationen eines Netzbetreibers auf der gleichen Frequenz senden, unterscheiden sich diese im Downlink nur durch die Verwendung von unterschiedlichen Scrambling Codes. Mit dem Scrambling Code werden alle Downlink Kanäle der Zelle inklusive des P-CCPCH kodiert, der die System Broadcast Infor-

mationen ausstrahlt. Ziel des nächsten Schrittes ist es deshalb, den Primary Scrambling Code der ausgewählten Zelle zu ermitteln. Der erste Teil dieses Prozesses wurde schon mit der korrekten Identifizierung des S-SCH und des gesendeten Chipmusters eingeleitet. Insgesamt gibt es auf dem S-SCH 64 unterschiedliche Chipmuster, die fest vom Standard vorgegeben sind. Somit können an einem Ort theoretisch bis zu 64 unterschiedliche Zellen betrieben werden. Auf einem weiteren Kanal, dem Common Pilot Channel (CPICH), wird zur Ermittlung des Primary Scrambling Codes wiederum ein festes und somit bekanntes Chipmuster ausgestrahlt. In Abhängigkeit der 64 unterschiedlichen S-SCH Chipmuster gibt es 8 mögliche Scrambling Codes. Nur mit einem dieser 8 kann der CPICH korrekt dekodiert werden.

Lesen der Systeminformationen

Nachdem über den CPICH nun auch der Primary Scrambling Code der Zelle bekannt ist, kann das Endgerät im nächsten Schritt den P-CCPCH und die darin enthaltenen Systeminformationen lesen. Der P-CCPCH wird dabei immer mit dem Spreading Code $C_{256,1}$ übertragen und kann so vom Endgerät einfach gefunden werden. Erst danach weis das Endgerät, zu welchem Netzwerk die Zelle gehört. Informationen, die auf dem Broadcast Channel / P-CCPCH ausgestrahlt werden, sind z.B.:

- Netzwerk Identität (MCC/MNC), Location Area (LAC) und Cell-ID.
- Cell Access Restrictions, d.h. welche Teilnehmergruppen mit der Zelle kommunizieren dürfen.
- Primary Scrambling Codes und Frequenzen der Nachbarzellen. Diese Informationen werden für Nachbarzellenmessung und Cell Reselection benötigt.
- Frequenzinformationen von benachbarten GSM Zellen, die verwendet werden, wenn keine geeignete UTRAN Zelle für ein Zellwechsel zur Verfügung steht.
- Parameter, die den Cell Reselection Algorithmus beeinflussen können.
- Maximale Sendeleistung, mit der das Endgerät auf den RACH zugreifen darf.
- Informationen über die Konfiguration des PRACH und S-CCPCH (also des PCH und FACH).

Das Endgerät hat nun im nächsten Schritt die Möglichkeit, sich am Netzwerk über ein Location Update oder GPRS Attach anzu-

melden. Diese Prozeduren verwenden auf den oberen Protokollschichten die Mobility Management bzw. Packet Mobility Management Protokolle, die auch bei GSM und GPRS verwendet werden. Für UMTS wurden diese nur leicht angepasst. Für weitere Information hierzu siehe Kapitel 1.8.1 und 2.7.1.

3.4.5 Beispiel: Der erste Netzwerkzugriff

Die Initial Network Access Prozedur wird immer dann durchgeführt, wenn das Endgerät mit dem Netzwerk Verbindung aufnehmen möchte. Dies kann ganz unterschiedliche Ursachen haben, wie z.B. ein Location Update, ein abgehendes Telefonat, eine erhaltene Paging Nachricht, oder auch der Beginn einer paketvermittelten Datenübertragung (PDP Context Activation). In allen Fällen muss das Endgerät vom Radio Netzwerk einen Übertragungskanal anfordern.

Zu Beginn der Initial Network Access Prozedur sendet das Endgerät eine oder mehrere 4096 Chip lange Sequenzen, die Präambel genannt werden. Die Übertragungsdauer einer 4096 Chip langen Präambel ist genau eine Millisekunde. Erhält das Endgerät keine Antwort, wird erneut eine Präambel gesendet, jedoch mit einer etwas höheren Sendeleistung. Dieser Vorgang wird wiederholt, bis das Netzwerk reagiert. Diese allmähliche Leistungssteigerung ist notwenig, da das Endgerät bei der ersten Verbindungsaufnahme noch nicht wissen kann, welche Sendeleistung genügt, um mit dem Netzwerk zu kommunizieren. Deshalb erfolgt die Verbindungsaufnahme erst mit einer kleinen Sendeleistung, die wenig Interferenzen hervorruft, aber auch nicht unbedingt Erfolg garantiert. Um dem Netzwerk Gelegenheit zur Antwort zu geben, sind die Sequenzen jeweils 3 Slots voneinander getrennt. Hat das Netzwerk die Präambel eines Teilnehmers empfangen, sendet es diesem auf dem Acquisition Indication Channel (AICH) eine Nachricht zurück. Somit kennt das Endgerät die zu verwendende Sendeleistung und sendet auf dem PRACH einen 10 oder 20 Millisekunden langen Frame, der eine RRC Connection Request Nachricht enthält. Da der Spreizfaktor des PRACHs variabel sein kann, kann diese Nachricht 9 bis 75 Octets enthalten.

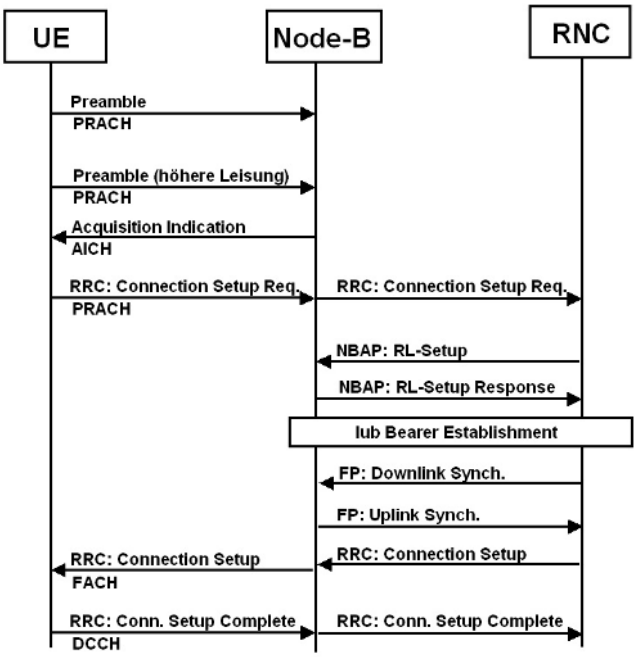

Abb. 3.17: Verbindungsaufnahme mit dem Netzwerk (RRC Connection Setup) (siehe auch 3GPP TS 25.931, 7.3.1)

Um Kollisionen auf dem PRACH von unterschiedlichen Endgeräten zu vermeiden, wird der PRACH in 15 Slots eingeteilt. Außerdem gibt es 16 unterschiedliche Codes für die Präambel. Somit ist es sehr unwahrscheinlich, dass zwei Endgeräte zur selben Zeit den gleichen Code verwenden. Geschieht dies doch, wird die Verbindungsaufnahme dieser Geräte scheitern, und die Prozedur muss wiederholt werden. Nachdem der RNC die RRC Connection Request Nachricht erhalten hat, kann er die nötigen Übertragungskanäle im Radionetzwerk und auf der Luftschnittstelle reservieren. Der RNC hat dabei zwei Möglichkeiten:

- Der RNC kann einen Dedicated Channel für die Kommunikation verwenden, das Mobiltelefon wechselt dann in den RRC State Cell-DCH (vgl. Kapitel 3.5.4). Ein solcher Kanal wird gewählt, wenn aus der Connection Request Nachricht ersichtlich ist, dass das Endgerät eine Nutzdatenverbindung aufbauen möchte. Diese Möglichkeit ist in Abbildung 3.17 dargestellt.

- Der RNC kann sich aber auch entscheiden, die Kommunikation weiterhin über den RACH und den FACH fortzuführen. Das Mobiltelefon wechselt in diesem Fall in den RRC State Cell-FACH (vgl. Kapitel 3.5.4). Ein solcher „Shared" Channel kann als Übertragungskanal vom RNC ausgewählt werden, wenn aus der Connection Request Nachricht ersichtlich ist, dass ein Endgerät nur eine Signalisierungsverbindung z.B. für einen Location Update aufbauen möchte. Ein solcher Kanal kann auch verwendet werden, wenn das Endgerät eine paketvermittelte Datenverbindung aufbauen will, die keine hohe Bandbreite oder schnelle Antwortzeit benötigt.

Nach Auswahl und Reservierung der Kanäle schickt der RNC eine RRC Connection Setup Nachricht über den FACH an das Endgerät zurück. Das Endgerät antwortet daraufhin auf dem zugeteilten Kanal mit einer RRC Connection Setup Complete Nachricht.

Nach dieser allgemeinen Prozedur folgen jetzt die spezifischen Prozeduren zwischen dem Kernnetz und dem Endgerät, wie der Aufbau eines Telefongesprächs oder die Aktivierung eines PDP Contexts. Einige dieser Szenarien werden in Kapitel 3.7 gezeigt.

3.4.6 Der Uu Protokoll Stack

Wie im vorhergehenden Abschnitt gezeigt, werden in UMTS Daten auf der Luftschnittstelle in Kanälen übertragen. Wie auf jeder anderen Schnittstelle auch, werden die Daten in diesen Kanälen über mehrere Protokollebenen für die Übertragung vorbereitet. Für die meisten Kanäle werden im Radionetzwerk alle Teile des Protokollstacks, mit Ausnahme des Physical Layers, im RNC bearbeitet. Nur für Kanäle wie z.B. dem BCCH, der großteils statische Informationen enthält, ist der Protokollstack auf dem Node-B implementiert.

Wie in Abb. 3.18 dargestellt, werden am oberen Ende des Protokollstacks so genannte Higher Layer PDUs (Datenpakete) an den RNC übergeben. Dies können z.B. Userdaten wie IP Pakete oder Sprachdaten sein, sowie Control Plane Nachrichten der MM, CC, PMM und SM Subsysteme.

PDCP Layer Headerkomprimierung nach RFC 2507

Handelt es sich bei einem eingehenden Paket um IP Daten, komprimiert das PDCP (Packet Data Convergence Protocol) Protokoll im nächsten Schritt den IP Header. Der verwendete Algorithmus wird in RFC 2507 beschrieben. Dies steigert die Daten-

übertragungsrate, da der IP Header je nach Paketgröße einen nicht zu vernachlässigenden Anteil am Datenaufkommen hat. Da die meisten Werte in einem IP Header statisch sind, ist eine Komprimierung leicht möglich.

RLC Layer (3GPP 25.322)

Der RLC (Radio Link Control) Layer kennt die physikalischen Eigenschaften der Luftschnittstelle und teilt die aus den oberen Schichten angelieferten Datenpakete für die Übertragung über die Luftschnittstelle auf (Segmentation). Dies ist notwendig, da PDCP Pakete, also z.B. komprimierte IP Pakete unterschiedliche Längen haben und durchaus über 1000 Bytes lang sein können. Pakete, die über die Luftschnittstelle übertragen werden, sind jedoch wesentlich kleiner und haben stets eine feste Länge. Die Größe der Nutzdaten in diesen Paketen wird im Wesentlichen durch den Spreizfaktor, das Übertragungszeitintervall (10 - 80 Millisekunden = Transmit Time Interval, TTI) und den verwendeten Fehlerkorrekturmechanismen bestimmt.

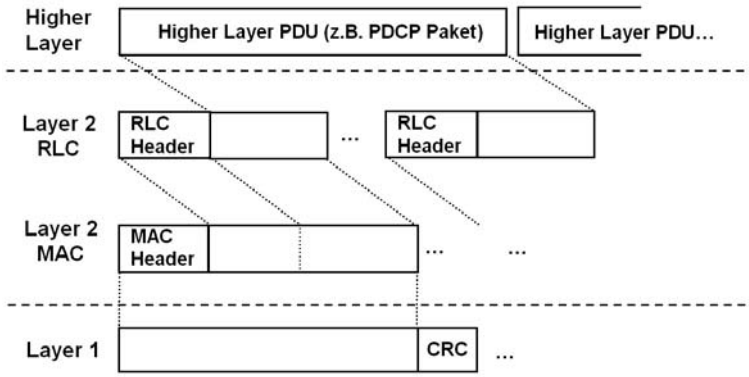

Abb. 3.18: Aufbereitung der Daten für die Übertragung über die Luftschnittstelle (Uu)

Wie bei GSM, werden auch bei UMTS möglichst kleine Datenpakete über die Luftschnittstelle übertragen. Dies hat den Vorteil, dass im Fehlerfall nur wenige Daten erneut zu übertragen sind. Einige Beispiele: Wurde einem Endgerät z.B. ein Kanal mit einer Datenrate von 384 kbit/s und einem TTI von 10 Millisekunden zugeteilt, kann jedes Datenpaket 480 Bytes Nutzdaten enthalten. Bei einer Datenrate von 64 kbit/s und einem Übertragungsintervall von 20 Millisekunden sind es 160 Bytes. Bei einer Sprach-

übertragung mit 12,2 kbit/s und TTI von 20 Millisekunden werden pro Paket schließlich nur noch 30 Bytes übertragen.

Im umgekehrten Fall ist es auch möglich, mehrere RLC Pakete pro TTI zu übertragen (concatenation), falls die Datenpakete aus höheren Schichten kleiner als die Paketgröße im Zeitintervall sind.

Sollten alle gerade vorhandenen Datenpakete aus höheren Schichten kein komplettes Paket für die Luftschnittstelle ausfüllen können, füllt der RLC Layer die restlichen Bits des Pakets auf, da die Paketgröße über die Luftschnittstelle konstant ist. Dieser Vorgang wird Padding genannt. Statt dem Padding können die ungenutzten Bits auch für RLC Kontrollnachrichten verwendet werden.

Je nach Art der zu übertragenden Daten gibt es drei unterschiedliche RLC Modi:

RLC Transparent Mode

Der RLC Transparent Mode wird hauptsächlich für die Übertragung von leitungsvermittelten Sprachkanälen verwendet, sowie für den BCCH und den PCCH. Im Falle der Sprachpakete ist keine Segmentierung oder Padding notwendig, da die Pakete schon in einem festen Frame Format (alle 20 Millisekunden ein Sprachpaket mit fester Länge) geliefert werden und somit ohne weitere Modifikationen übertragen werden können.

RLC Non Acknowledged Mode

Auch der RLC Non Acknowledged Mode bietet das oben beschriebene Segmentation und Concatenation für Daten aus höheren Schichten an. Darüber hinaus ist es in diesem Mode möglich, über ein oder mehrere Längenangaben im RLC Header den Beginn und das Ende von Layer-3-Nutzdatenpaketen zu markieren. Somit ist es möglich, unabhängig von der Größe der Pakete aus höheren Schichten die RLC Pakete immer komplett zu füllen.

Werden Pakete fehlerhaft übertragen oder gehen verloren, gibt es im Non Acknowledged RLC Mode keine Möglichkeit, dies zu erkennen und die Pakete nochmals zu übertragen. Somit muss diese Aufgabe, falls gewünscht, auf höheren Protokollschichten (z.B. im IP und TCP Layer) durchgeführt werden.

RLC Acknowledged Mode

Dritter Modus ist der RLC Acknowledged Mode. Zusätzlich zu den Diensten des Non Acknowledged Modes bietet diese Übertragungsart noch zusätzlich Flusskontrolle und erneute Übertragung von fehlerhaften oder verlorenen Datenblöcken an. Ähnlich wie bei TCP wird ein ‚Fensterverfahren' für die Bestätigung korrekter Blocks verwendet. Dies bedeutet, dass nicht nach jeder Übertragung eines Blocks auf eine Bestätigung gewartet werden

muss. Stattdessen können weitere Blöcke bis zur maximalen Fenstergröße übertragen werden. Während dieser Zeit hat die Gegenstelle die Möglichkeit, Blöcke innerhalb des Fensters zu bestätigen und somit das Fenster weiter nach vorne zu schieben. Ging ein Block verloren, bleibt eine Bestätigung für diesen aus, und der fehlende oder fehlerhafte Block wird automatisch neu übertragen. Dieses Verfahren hat den Vorteil, dass bei korrekter Übertragung keine Verzögerung durch das Warten auf eine Bestätigung entsteht. Die Fenstergröße kann bei UMTS von 1 bis 2^{12} Datenblöcken zwischen UE und RNC ausgehandelt werden. Diese Flexibilität ist das Resultat aus den Erfahrungen, die bei GPRS gemacht wurden. Dort ist die Fenstergröße fest mit 64 Blöcken vorgegeben. Dies führt vor allem bei Verwendung von CS-3 und 4 und steigender Fehlerrate (Block Error Rate, BLER) zu Unterbrechungen bei der Übertragung, da Datenblöcke nicht schnell genug gemeldet und erneut übertragen werden können.

Der MAC Layer

Nachdem der RLC Layer die Datenpakete für die Übertragung über die Luftschnittstelle segmentiert und evtl. mit Kontrollinformationen versehen hat, führt der MAC (Medium Access Control) Layer folgende Operationen aus:

Auswahl eines geeigneten Transportkanals: Wie in Abbildung 3.14 gezeigt wurde, können logische Kanäle auf unterschiedliche Transportkanäle abgebildet werden. Nutzdaten des Dedicated Traffic Channel (DTCH) können z.B. auf einem Dedicated Channel (DCH), auf dem Forward Access Channel (FACH), oder auf einem Shared Channel übertragen werden. Welche Art Transportkanal für eine Verbindung verwendet wird, wurde vom Netzwerk beim Aufbau der Verbindung festgelegt. Diese Zuordnung kann jedoch vom Netzwerk auch jederzeit geändert werden.

Eine weitere Aufgabe des MAC Layers ist das Multiplexing von Daten auf Common und Shared Channels. Der FACH kann, wie bereits beschrieben, nicht nur für den Transport von RRC Nachrichten für unterschiedliche Benutzer verwendet werden, sondern kann auch Nutzdatenpakete befördern. Der MAC Layer ist dafür zuständig, die logischen Kanäle auf gemeinsamen Transportkanälen zu multiplexen und jeweils einen MAC Header voranzustellen. Dieser beschreibt unter anderem, für welchen Teilnehmer das Datenpaket bestimmt ist. Dieser Teil des MAC Layer wird MAC c/sh (common/shared) genannt.

Auch für Dedicated Channels ist der MAC Layer für das Multiplexing unterschiedlicher Datenströme zuständig. Wie ebenfalls in

Abbildung 3.14 zu sehen ist, werden der logische Nutzdatenkanal (DTCH) und der logische Signalisierungskanal (DCCH) eines Nutzers auf einen gemeinsamen Transport Dedicated Channel (DCH) gemultiplext. Somit ist es möglich, dass der Benutzer über einen Transportkanal nicht nur Nutzdaten empfängt, sondern auch gleichzeitig Signalisierungsnachrichten der MM (Mobility Management), PMM (Packet Mobility Management), CC (Call Control) und SM (Session Management) Subsystems. Dieser Teil des MAC Layers wird MAC-d (dedicated) genannt.

Bevor die so zusammengesetzten Datenpakete an die physikalische Schicht weitergegeben werden, fügt die MAC Schicht noch Informationen in den MAC Header ein, die dem physikalischen Layer im nächsten Schritt Aufschluss darüber geben, in welchem Transport Format die Daten übertragen werden sollen. Dieses so genannte Transport Format Set (TFS) beschreibt die Kombination aus Datenübertragungsrate, dem Transmit Time Interval (TTI) des Paketes, der Art der Kanalkodierung, sowie den anzuwendenden Mechanismus für die Fehlerkorrektur.

Der Physikalische Layer

Für die meisten Kanäle sind alle bisher beschriebenen Protokollschichten im RNC implementiert. Der unterste Layer, der Physical Layer, ist jedoch in der Basistation (Node-B) implementiert. Der Physical Layer im Node-B hat folgende Aufgaben:

Um den für die Fehlererkennung und Fehlerkorrektur auf der Luftschnittstelle nötigen Overhead nicht auf der Iub Schnittstelle übertragen zu müssen, wird die Kanalkodierung erst im Node-B durchgeführt. Dies ist möglich, da im Header jedes Datenpakets das Transport Format Set (TFS) Feld angibt, welcher Kanalkodierer anzuwenden ist. Bei UMTS gibt es neben dem schon von GSM bekannten ½ Rate Convolutional Coder auch noch einen 1/3 Rate Coder, sowie den Turbocode Codierer. Durch Hinzufügen von Fehlererkennung und Fehlerkorrekturbits zum Datenstrom verdoppelt sich der Datensttrom beim ½ Rate Coder und wird durch den 1/3 Rate Coder sogar verdreifacht.

Danach findet auf dem physikalischen Layer die Spreizung des Orginaldatenstroms statt, aus den Bits werden Chips, die dann über die Luftschnittstelle übertragen werden.

Schließlich werden die zu übertragenden Daten im Modulator in ein analoges Signal umgewandelt und anschließend über die Luftschnittstelle übertragen. Als Modulationsverfahren kommt das Quadrature Phase Shift Keying (QPSK) Verfahren zum Einsatz, mit dem pro Übertragungsschritt 2 Chips übertragen werden können.

Downlink

Im Node-B wird dabei im Downlink, wie in Abbildung 3.19 dargestellt, ein Bit über die komplexe I Ebene übertragen, und ein weiteres Bit gleichzeitig über die Q Ebene. Da in jeder Ebene die Datenrate mit 3.84 MChips/s fest vorgegeben ist, ergibt sich eine „Gesamtdatenrate" von 2 * 3.84 MChips/s. Der Dedicated Physical Data Channel (DPDCH) und der Dedicated Physical Control Channel (DPCCH), der vor allem bei niedrigen Spreizfaktoren nur einen kleinen Teil der Datenmenge ausmacht, werden im Downlink im Zeitmultiplex übertragen.

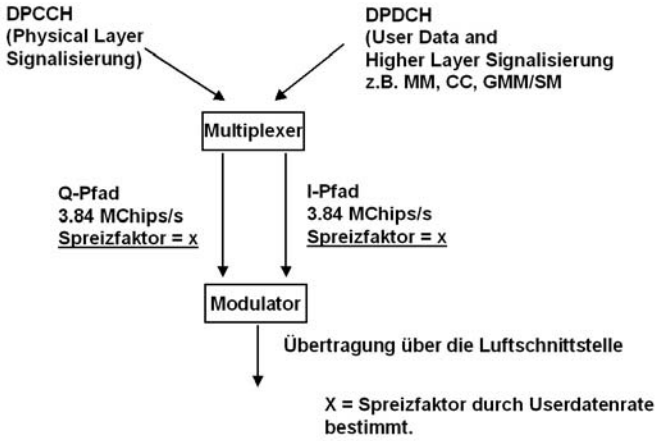

Abb. 3.19: Datenübertragung im Downlink Richtung über den I und Q Pfad

Uplink

Im Uplink, also vom Endgerät zum Netz, wurde für die Übertragung ein etwas anderes Verfahren gewählt: Wie im Downlink wird ebenfalls das QPSK Modulationsverfahren verwendet. Statt jedoch auf dem I und Q Pfad Nutzdaten zu übertragen, werden diese im Uplink nur auf dem I-Pfad gesendet. Der Q Pfad wird ausschließlich zur Übertragung des Dedicated Physical Control Channels (DPCCH) verwendet, der Layer 1 Nachrichten z.B. für die Leistungsregelung (Power Control) überträgt (vgl. 3GPP 25.211, 5.2.1). Somit wird im Uplink nur ein Pfad für die eigentliche Nutzdatenübertragung verwendet. Wenn im Uplink und Downlink die Datenraten gleich sind (z.B. für Sprachübertragung) ist somit der Spreizfaktor in Uplink Richtung nur halb so lang wie der Spreizfaktor im Downlink.

Anmerkung: Der Dedicated Physical Control Channel (DPCCH) übertragt nur Layer 1 Kontrollnachrichten (z.B. für die Leistungs-

regelung). Kontroll- und Signalisierungsnachrichten der MM, PMM, CC und SM Subsysteme zwischen Endgerät und MSC bzw. SGSN, werden nicht über den DPCCH, sondern über den logischen DCCH übertragen. Dieser wird zusammen mit dem logischen DTCH (Nutzdaten) im DPDCH Transportkanal übertragen (vgl. Abbildung 3.14, 3.19 und 3.20).

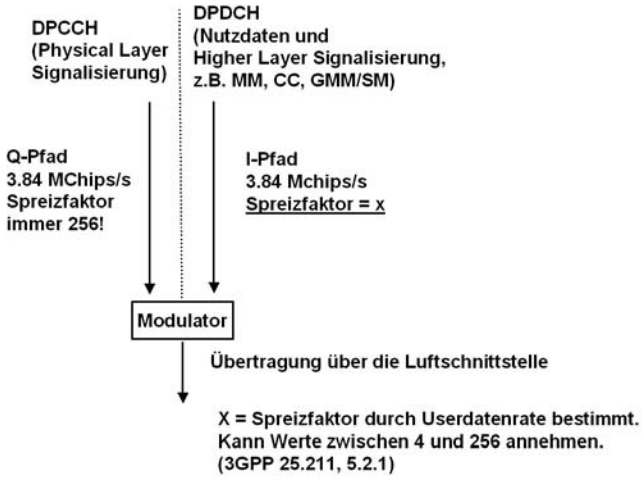

Abb. 3.20: Datenübertragung in Uplink Richtung verwendet nur die I-Ebene mit DPCCH in Q-Ebene

Keine komplette Abschaltung im Uplink bei DTX

Dieses Verfahren wurde aus folgendem Grund gewählt: In vielen Fällen müssen in der Uplink Richtung keine Daten übertragen werden. Dies ist z.B. bei Sprachverbindungen der Fall, wenn gerade nicht gesprochen wird, sowie bei paketvermittelter Datenübertragung, wenn keine Daten für die Übertragung vorhanden sind. Sendet während dieser Phase die Mobilstation keine Pakete (Discontinous Transmission, DTX), kann Batteriekapazität eingespart werden und das Interferenzniveau für andere Teilnehmer gesenkt werden. Der Nachteil einer kompletten Leistungsabschaltung ist jedoch, dass das An- und Abschalten der Leistung über nahe gelegene Radioempfänger zu hören ist. Dies ist z.B. bei GSM Endgeräten der Fall und kann dort auch deutlich gehört werden. Bei UMTS wird im Uplink jedoch nur die Übertragung auf dem I-Pfad zeitweise eingestellt, der DPCCH im Q-Pfad wird weiterhin gesendet. Die Sendeleistung wird somit nicht ganz abgeschaltet, aber dennoch deutlich reduziert. Das typische GSM Brummen in nahe gelegenen Radioempfängern ist somit nicht mehr zu hören.

3.5 Das UMTS Terrestrial Radio Access Network (UTRAN)

3.5.1 Node-B, Iub Interface, NBAP und FP

Die Basisstation, bei UMTS Node-B genannt, übernimmt alle Funktionen für das Senden und Empfangen von Daten über die Luftschnittstelle. Dies umfasst, wie in Kapitel 3.4 beschrieben, im Wesentlichen die Kanalkodierung, das Spreading bzw. De-Spreading der Daten, sowie die Modulation. Außerdem ist der Node-B auch für die Leistungsregelung der einzelnen Verbindungen zuständig. Der Node-B erhält hierzu lediglich Vorgaben vom RNC.

Seketorisierte Node-B Konfiguration

Größe und Kapazität eines Node-Bs sind variabel. Für Regionen mit großem Daten- und Sprachaufkommen werden bevorzugt sektorisierte Konfigurationen eingesetzt. Das bedeutet, dass der Node-B seinen Versorgungsbereich mit mehreren, voneinander unabhängigen Zellen abdeckt. Jede Zelle hat dabei ihre eigene Cell ID, Scrambling Code, sowie ihren eigenen Codebaum. Jede Zelle hat außerdem eine oder mehrere eigene Antennen. Diese decken z.B. 180 Grad (2 Sektor Konfiguration), 120 Grad (3 Sektoren) oder sogar nur 90 Grad (4 Sektoren) ab, wenn sehr hohes Datenaufkommen erwartet wird. Je nach Anzahl der Sektoren und Datenaufkommen muss der Node-B dann auch mit entsprechender Kapazität über die Iub Schnittstelle an seinen RNC angeschlossen sein. Nur wenige 64 kbit/s Timeslots wie bei GSM reichen für einen Node-B nicht mehr aus, da die Datenrate der Luftschnittstelle bei UMTS wesentlich größer ist. Um hohe Datenraten für möglichst viele Teilnehmer zu garantieren, ist ein Node-B deshalb je nach Ausstattung üblicherweise mit einer oder mehreren E-1 Verbindungen (je 2.048 MBit/s) an seinen RNC angeschlossen.

Omnidirektionale Node-B Konfiguration

Für Regionen mit geringem Daten- und Sprachaufkommen wird üblicherweise nur ein Node-B mit einer Zelle verwendet. Mit einer entsprechend hohen Sendeleistung kann dieser dann einen großen omnidirektionalen geographischen Bereich abdecken. Von außen ist eine solche Konfiguration nicht ohne weiteres zu erkennen, da durchaus eine sektorisierte Antennenanordnung verwendet werden kann. Dies wird vor allem deshalb gemacht, um die Empfangseigenschaften des Node-Bs zu verbessern. Im Downlink wird in einer solchen Konfiguration das gleiche Signal über alle Antennen ausgestrahlt, die Kapazität ist mit einer omnidirektionalen Konfiguration identisch. Im Uplink jedoch kann die Signalenergie eines Teilnehmers mit einer sektorisierten Anten-

nenkonfiguration wesentlich besser empfangen werden, als mit einer einzigen omnidirektionalen Antenne (Antennengewinn).

Microzellen

Für Gebiete mit sehr hohem Datenaufkommen, z.B. Straßenzüge in Innenstädten, werden Node-Bs in einer Microzellenkonfiguration verwendet. Auch diese haben nur eine Antenne, decken dann aber meistens nur ein wenige hundert Meter einer Straße ab. Für solche Anwendungen haben Netzwerkanbieter Node-Bs mit kompakten Abmessungen im Programm. Die Kapazität eines solchen Node-Bs ist jedoch meist auf einen Sektor begrenzt und auch die Sendeleistung ist geringer als bei Node-Bs mit größeren Abmessungen.

NBAP (3GPP 25.433)

Für den Austausch von Kontroll- und Konfigurationsinformationen wird auf der Iub Schnittstelle zwischen RNC und Node-B das Node-B Application Part (NBAP) Protokoll verwendet. Es hat unter anderen folgende Aufgaben:

- Zellkonfiguration
- Common Channel Management
- Dedicated Channel Management, wie z.B. den Aufbau einer neuen Verbindung zu einem Teilnehmer.
- Übertragung von Signal- und Interferenzmesswerten von Common und Dedicated Channels.
- Kontrolle des Compressed Mode (vgl. Kapitel 3.7.1 Intersystem Handover).

Das Frame Protocol (FP)

Nutzdaten werden zwischen RNC und Node-B über das Frame Protocol (FP) übertragen, das für Dedicated Channels im 3GPP Standard 25.427 beschrieben ist. Dies ist für das korrekte Senden und den korrekten Empfang von Nutzdaten über die Iub Schnittstelle zuständig. Es transportiert die Daten in einem Format, das vom Node-B direkt in einen Uu Frame umgewandelt werden kann. Für diese Umwandlung verwendet der Node-B den Traffic Format Identifier (TFI), der Teil jedes FP Pakets ist. Dieser gibt unter anderem die Framelänge vor, sowie den zu verwendenden Channel Coder.

Synchronisation des Datenstroms

Das Frame Protocol wird außerdem zur Synchronisation der Nutzdatenverbindung zwischen RNC und Node-B verwendet. Dies ist besonders für den Datentransfer im Downlink wichtig, da der Node-B alle 10, 20, 40 oder 80 Millisekunden ein Frame zum Endgerät sendet. Um kurze Verzögerungszeiten zu gewährleisten ist es notwendig, dass die vom RNC gesendeten Datenpakete rechtzeitig für den nächsten Uu Frame beim Node-B einge-

hen. Geschähe dies nicht, müsste das Datenpaket bis zum nächsten Uu Frame gepuffert werden. Um dies zu gewährleisten, werden Synchronisationsnachrichten beim ersten Einrichten des Kanals (Bearers) zwischen Node-B und RNC ausgetauscht, sowie auch dann, wenn die Synchronisierung einmal verloren gehen sollte.

Schließlich werden in FP Frames auch Quality Estimates vom Node-B zum RNC übertragen. Diese helfen dem RNC bei einem Soft Handover (vgl. Kapitel 3.7.1), den besten Datenblock eines Teilnehmers von unterschiedlichen Node-Bs auszuwählen.

3.5.2 Der RNC, Iu, Iub und Iur Schnittstelle, RANAP und RNSAP

Das Herz des UMTS Radionetzwerkes ist der Radio Network Controller, kurz RNC genannt. Wie in Abbildung 3.21 und 3.22 gezeigt, laufen hier alle Schnittstellen des Radionetzwerkes zusammen.

Die Iub Schnittstelle

In Richtung des mobilen Teilnehmers sind über die Iub Schnittstelle normalerweise mehrere dutzend Node-Bs an einen RNC angeschlossen. In der UMTS Anfangsphase sind die meisten Node-Bs über eine oder mehrere 2 MBit/s E-1 Strecken drahtgebunden oder per Richtfunk an den RNC angeschlossen. Wie viele Verbindungen pro Node-B verwendet werden, hängt hauptsächlich von der Anzahl der Sektoren des Node-Bs ab, sowie der Anzahl der verwendeten Frequenzen. Da anzunehmen ist, dass das Datenaufkommen pro Node-B in Zukunft steigen wird, ist zu erwarten, dass Node-Bs in Zukunft auch über STM-1 (155 MBit/s) angeschlossen werden. Da ein Node-B diese Kapazität alleine nicht benötigt, können sich mehrere Node-Bs eine STM-1 Verbindung über eine Reihenschaltung teilen. Auf der physikalischen Schicht hat ein Netzbetreiber die Wahl, diese Verbindung elektrisch, optisch oder per Richtfunk herzustellen. Welche Übertragungsart gewählt wird, hängt hauptsächlich von der Datenrate ab, die der Node-B unterstützen soll, sowie von den monatlichen Kosten, die eine solche Verbindung verursacht. Je größer die Übertragungskapazität, desto höher auch die monatlichen Kosten. Diese sind bei UMTS gegenüber GSM höher, da UMTS wesentlich höhere Datenraten bietet und somit ein Node-B mit einer größeren Bandbreite an das Radionetzwerk angeschlossen werden muss.

Iub Bandbreite pro Node-B

ATM und IP als Transportprotokoll

Auf höheren Schichten spielt es keine Rolle, welches Übertragungsverfahren zum Einsatz kommt, da unabhängig davon grundsätzlich ATM als Transportprotokoll verwendet wird. Für

die Zukunft ist im Standard auch vorgesehen, alternativ statt ATM das IP Protokoll als Layer 3 Transportprotokoll auf allen Schnittstellen des UTRAN zu verwenden. Dies bereitet jedoch zusätzlichen Aufwand, da Datenströme zwischen Node-B und RNC synchron ausgetauscht werden müssen. Dies kann mit IP als Transportprotokoll nicht ohne zusätzliche neue Mechanismen gewährleistet werden. Um UMTS jedoch möglichst schnell einführen zu können, wurde daher zuerst auf ATM mit seinen ausgezeichneten und über Jahre bewährten Eigenschaften als Echtzeitübertragungsprotokoll zurückgegriffen.

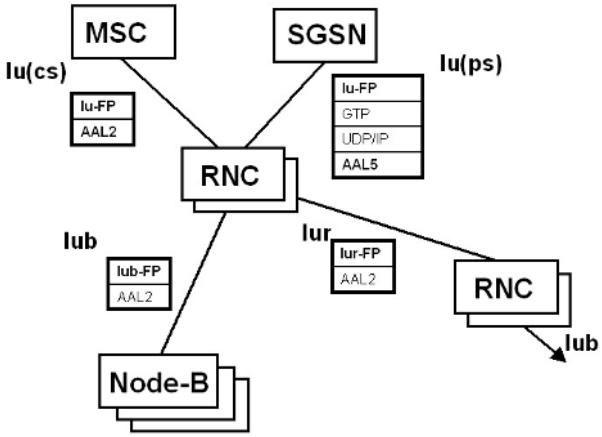

Abb 3.21: RNC Protokolle und Interfaces für User Daten (User Plane)

In Richtung des Kernnetzwerks ist der RNC über die Iu Schnittstelle verbunden. In Release 99 gibt es weiterhin, wie in Abbildung 3.3 in der Einleitung des Kapitels gezeigt wurde, zwei voneinander weitgehend unabhängige Kernnetzwerke:

Iu(cs) für Sprach- und Videotelefonie

Die Iu(cs) Schnittstelle: Für die Sprach- und Videotelefonie wird weiterhin auf die bereits bestehende leitungsvermittelnde GSM Core Netzwerk Technologie zurückgegriffen. Das Mobile Switching Center (MSC) stellt also weiterhin die Brücke zwischen Core- und Zugangsnetz dar. Um den Neuerungen von UMTS Rechnung zu tragen, wurden jedoch folgende Modifikationen vorgenommen: Bei UMTS wurde die Transcoding and Rate Adaptation Unit (TRAU) logisch dem Core Netzwerk zugeordnet und neu implementiert. Dies ist ein Unterschied zu GSM, wo die

TRAU logisch dem Zugangsnetz zugeordnet ist. In der Praxis wird die TRAU jedoch bei GSM und UMTS in den allermeisten Fällen zusammen mit der MSC aufgestellt. Durch die Umwandlung des Sprachcodecs von 64 kbit/s im Core Netzwerk zu z.B. 12.2 kbit/s im Zugangsnetzwerk kann einiges an Übertragungskapazität und somit an Kosten eingespart werden. Eine MSC wird somit nicht, wie in den meisten Bildern gezeigt, direkt an einen RNC angeschlossen, sondern immer über eine TRAU. Die Schnittstelle zwischen MSC, TRAU und RNC wurde Iu(cs) genannt, wobei ‚cs' für circuit switched steht. Die Iu(cs) Schnittstelle entspricht somit der A-Schnittstelle bei GSM und ist dieser auf höheren Protokollschichten auch sehr ähnlich. Weitere Informationen zur Funktionalität einer TRAU sind in Kapitel 1.7.5 zu finden, sowie anschließend im Kapitel 3.5.3 zum Thema AMR.

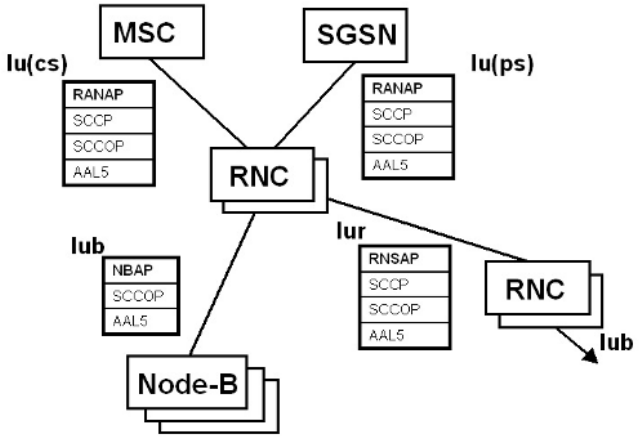

Abb. 3.22: RNC Protokolle und Interfaces für Signalisierung (Control Plane)

RANAP

Das von GSM bekannte BSSMAP Protokoll wurde für UMTS etwas erweitert und modifiziert und in Radio Access Network Application Part (RANAP) umbenannt. In den Standards ist RANAP in 3GPP TS 25.413 zu finden. RANAP bildet die Grundlage für die Mobility Management, Call Control und Session Management Protokolle. Außerdem können MSC und SGSN über RANAP auch den Auf- und Abbau von Radiokanälen (RABs) zu Teilnehmern vom RNC anfordern.

Um RANAP mit einer schon vorhandenen GSM MSC zu unterstützen, ist eine Software Erweiterung nötig. Da das bisherige A-Interface weiterhin Teil der MSC ist, kann diese gleichzeitig ein

UMTS Zugangsnetzwerk über RANAP und Iu(cs), sowie ein GSM Zugangsnetzwerk über BSSMAP und dem A-Interface unterstützen.

Bei GSM und dem A-Interface war die MSC in Richtung Zugangsnetzwerk auf Sprachverbindungen mit 12.2 kbit/s und leitungsvermittelnde Datenverbindungen mit 9.6 kbit/s und 14.4 kbit/s beschränkt. Mit UMTS und dem Iu(cs) Interface sind nun auch 64 kbit/s Verbindungen zum RNC möglich, was der Geschwindigkeit eines ISDN B-Kanals im Festnetz entspricht. Diese neue und schnellere Verbindungsart wird hauptsächlich für Videotelefonie verwendet. Durch optimierte Video- und Sprachkompressionsverfahren stellt dieser leitungsvermittelnde Übertragungskanal in punkto Verzögerungszeit und garantierte Bandbreite ein optimales Medium dar. In der weiteren Evolution des UMTS Netzwerkes und der Endgeräte ist für die Zukunft zu erwarten, dass Videotelefonie auch über paketvermittelnde Verbindungen eingeführt wird.

Auch die Iu(cs) Schnittstelle basiert auf ATM und ist somit, wie schon bei der Iub Schnittstelle erläutert, weitgehend vom physikalischen Übertragungsmedium unabhängig.

Iu(ps) für paketvermittelte Daten

Alle paketvermittelten Dienste, in den meisten Fällen also Internetverbindungen, werden bei UMTS über die Iu(ps) Schnittstelle von und zum Core Netzwerk geführt. Diese Schnittstelle entspricht der Funktionalität der Gb Schnittstelle des GSM/GPRS Netzwerkes, die in Kapitel 2.6 beschrieben ist. Da das paketvermittelnde Core Netzwerk von GPRS und UMTS gemeinsam genutzt werden kann, können nicht nur GSM BSCs an einen Serving GPRS Support Node (SGSN) angeschlossen werden, sondern auch UMTS RNCs. Die Schnittstellenarchitektur selber hat jedoch wesentliche Änderungen erfahren. Statt Frame Relay wird, wie auch auf allen anderen UTRAN Schnittstellen, ATM als Layer 3 Protokoll genutzt.

Nutzdaten in UMTS für SGSN transparent

Für den SGSN ändert sich bei UMTS neben dem neuen Layer 3 Übertragungsprotokoll auch noch die Verarbeitung der Nutzerdaten grundlegend. Bei GSM/GPRS war der SGSN noch dafür zuständig, die vom GGSN eingetroffenen GTP Pakete zu verarbeiten und in einem BSSGP Paket und Frame Relay über die PCU and die richtige Zelle zu schicken. Bei UMTS hat der SGSN nun nur noch die Aufgabe, die GTP Pakte an den für den Anwender zuständigen RNC weiterzureichen. Der UMTS SGSN weis also im Unterschied zum GSM SGSN nicht mehr genau, in welcher Zelle

sich ein Teilnehmer befindet. Diese Änderung hat vor allem zwei Gründe:

- Der SGSN ist bei UMTS nun logisch vom Radio Netzwerk und der Zellarchitektur losgelöst. Er gibt das Paket lediglich zum RNC weiter. Erst dieser entscheidet, wie er die Pakete weiterleitet. Vor allem beim Soft Handover, der in Kapitel 3.7.1 detaillierter beschrieben wird, kann das Paket gleichzeitig über mehrere Node-Bs an den Teilnehmer gesendet werden. Diese Komplexität bleibt dem SGSN jedoch verborgen. Er kennt nur den momentanen Serving RNC (S-RNC) des Endgeräts.
- Durch Verwenden des GTP und IP Protokolls, sowie ATM in der Transportschicht, ergibt sich eine wesentliche Vereinfachung und eine Reduktion der verwendeten Protokollstapel im gesamten Netzwerk. Wie in Abbildung 3.21 zu sehen ist, wird der ATM Adaptation Layer (AAL) 5 verwendet, um die IP Datenpakete über ATM zu transportieren.

Packet Switched Mobility Management und Resource Anforderung

Nach wie vor ist der SGSN jedoch auch bei UMTS für das Mobility- und Session Management (GMM/SM) zuständig, das in Kapitel 2.7 beschrieben wurde. Für UMTS gibt es hier nur wenige Änderungen. Eine der wenigen ist die Anforderung eines Radio Beares beim RNC am Anfang einer Datenübertragung (PDP Context Activation). Dieses Konzept ist beim GSM/GPRS Netzwerk nicht bekannt, da hier ein Teilnehmer keine reservierten Ressourcen für sich auf der Luftschnittstelle hatte. Wie in Kapitel 2.5 beschrieben, bekommt der Nutzer dort nur für kurze Zeit einen oder mehrere Zeitschlitze für die Datenübertragung zugeteilt. Diese werden nach dem Beenden der aktuellen Übertragung, wie zum Beispiel nach der Übertragung einer Web Seite sofort wieder einem anderen Nutzer zugeteilt. Bei UMTS wurde dieses Prinzip geändert, und es gibt jetzt grundsätzlich drei Möglichkeiten, Paketdaten über die Luftschnittstelle zu übertragen:

Dedizierter Radiokanal (DCH) für die Paketdatenübertragung

Erste Möglichkeit: Der RNC vergibt einen Dedicated Channel (DCH) für die Paketdatenübertragung. Hier wird dem Nutzer in gleicher Weise wie für die leitungsvermittelte Sprachübertragung vom RNC ein dedizierter Kanal (RAB) zur Verfügung gestellt. Dies bedeutet auf der physikalischen Schicht, dass der Benutzer einen eigenen PDTCH und PDCCH für die Paketdatenverbinung zugeteilt bekommt. Die Bandbreite des Kanals steht für den Teilnehmer immer zur Verfügung, auch wenn keine Daten übertragen werden. In einem solchen Fall findet jedoch das in Kapitel

3.5.4 beschriebene Discontinuous Transmission (DTX) Verfahren Anwendung. Dies senkt die Interferenz in der Zelle und spart Energie im Endgerät. Der RNC kann beim Verbindungsaufbau zwischen unterschiedlichen Spreizfaktoren wählen und so dem Anwender eine Bandbreite von z.B. 8, 32, 64, 128 und 384 kbit/s garantieren.

Gleichzeitige Übertragung von Sprache und Daten

Ausserdem ist es möglich, über einen RAB paketvermittelte Daten und leitungsvermittelte Daten, wie z.B. Telefongespräche, gleichzeitig zu übertragen. Eine große Einschränkung, die noch bei GSM/GPRS in der Praxis existierte, wird somit elegant gelöst. Um dies zu ermöglichen, kann ein RAB auch nach dem Aufbau vom RNC jederzeit modifiziert werden. Kommt zu einer paketvermittelten Übertragung später noch ein leitungsvermitteltes Telefongespräch hinzu, modifiziert der RNC den RAB, um beide Verbindungen zur gleichen Zeit zu ermöglichen. Auch die Modifikation in umgekehrter Reihenfolge ist möglich. Einschränkend gilt aber, dass zusätzlich zu einer leitungsvermittelten Verbindung nur paketvermittelte Geschwindigkeiten von 64 oder 128 kbit/s möglich sind.

Ein Dedicated Channel bietet weiterhin noch folgende Vorteile:

Zellwechsel vom Netzwerk kontrolliert

Der Zellwechsel kann vom Netzwerk kontrolliert werden. Es entstehen somit keine Unterbrechungen beim Zellwechsel mehr, wie dies noch bei GPRS der Fall war. Zusammen mit den wesentlich höheren Geschwindigkeiten werden mit UMTS somit auch Dienste wie Videostreaming oder IP Videotelefonie möglich, bei denen eine Unterbrechung bei Zellwechsel sehr unerwünscht ist.

Schneller Zugriff auf den Übertragungskanal

Für das Senden von Daten in Up- und Downlink Richtung müssen bei Zuteilung eines dedizierten Kanals keine Ressourcen vom Netzwerk mehr angefordert werden, die Datenübertragung kann sofort beginnen. Dies machte sich bei GPRS vor allem beim Web surfen sehr störend bemerkbar. Hier werden pro Seite meist viele Objekte wie z.B. Bilder geladen. Diese erzeugen jeweils eine eigene Anfrage und Antwort vom Netz, für die in vielen Fällen die Ressourcen erst zugeteilt werden müssen.

Verwendet der Benutzer seinen dedizierten Kanal für einen längeren Zeitraum nicht, so gibt es mehrere Möglichkeiten den Radio Bearer zu modifizieren: So ist es z.B. möglich, einen anderen Spreizfaktor zu wählen. Dies senkt die maximale Geschwindigkeit für den Benutzer, gibt aber dem Netzwerk die Möglichkeit, den kürzeren Code für einen anderen Teilnehmer zu verwenden.

Common Channel für die Paketdatenübertragung

Zweite Möglichkeit der paketvermittelten Datenübertragung: Hat der Benutzer nur selten Daten zu übertragen, oder eine bereits zugewiesene dedizierte Verbindung wurde längere Zeit nicht benutzt, kann der RNC auch Daten über den Forward Access Channel (FACH) an ein Endgerät senden. Für Daten in Uplink Richtung verwendet das Endgerät in diesem Fall den Random Access Channel (RACH). Diese Kanäle stehen jedoch einem Benutzer nicht exklusiv zur Verfügung, er muss sich diese mit vielen anderen teilen. Interessant ist hierbei, dass der FACH und RACH nicht mehr nur für Signalisierungsdaten verwendet werden, sondern auch für Userdaten. Besonders in Uplink Richtung ergibt sich jedoch hier wieder ein ähnliches Verzögerungsproblem wie bei GPRS. Daten können hier nicht unmittelbar gesendet werden, da zuvor erst vom Netzwerk eine Zugriffserlaubnis eingeholt werden muss. Aufgrund der höheren Geschwindigkeiten von UMTS ist diese Verzögerungszeit aber geringer. Neben der nicht garantierten Bandbreite für einzelne Nutzer ist ein weiterer Nachteil des Common Channels, dass Endgeräte nicht vom Soft Handover profitieren können, der in Kapitel 3.7.1 beschrieben wird.

Shared Channel für die Paketdatenübertragung

Dritte Möglichkeit der paketvermittelten Datenübertragung: Optional kann für die Datenübertragung auch ein Downlink Shared Channel (DSCH) verwendet werden, sofern dieser von Netzwerk und Terminal unterstützt wird. Da der Downlink Shared Channel im Unterschied zum FACH nur für die Paketdatenübertragung verwendet wird, kann die Anzahl und Länge der Spreading Codes dynamisch an die aktuelle Verkehrslast einer Zelle angepasst werden. Somit sind Datenraten von 15 bis 960 kbit/s auf dem DSCH möglich. Außerdem ist einem DSCH auch ein Control Channel für die Leistungsregelung zugeordnet. Dies erhöht die Kapazität der Zelle und spart Energie in den Endgeräten. Durch den für die aktive Leistungsregelung notwendigen Dedicated Control Channel ist ein Endgerät, das Daten auf dem DSCH empfängt, im Cell-DCH State (vgl. Kapitel 3.5.4). Großer Nachteil des DSCH ist jedoch, dass ein Endgerät nicht vom Soft Handover profitieren kann.

Ab UMTS Release 5 wird zusätzlich zum DSCH ein High Speed DSCH eingeführt. Diese Technik wird High Speed Downlink Packet Access genannt und ermöglicht Datenraten von bis zu 2 MBit/s.

Quality of Service

Ob nun ein Dedicated-, Common oder Shared Channel auf Anforderung des SGSNs bei der PDP Context Activation zugewiesen

wird und mit welcher Geschwindigkeit die Daten dann übertragen werden, hängt von einer Vielzahl von Faktoren ab. Wesentliche Faktoren sind dabei z.B. die momentane Auslastung der Zelle und die Empfangsbedingungen am Ort des Teilnehmers. Ist z.B. das Interferenzverhältnis bereits sehr hoch, sind die Spreading Codes knapp, oder hat der Anwender einen großen Abstand zum Node-B, kann unter Umständen bei der Vergabe eines Dedicated Channels nur ein langer Spreading Code für kleine Datenraten vergeben werden.

QoS beim Aktivieren eines PDP Kontexts

Auch der Benutzer kann beim Aufbau des PDP Kontextes Einfluss auf die Zuteilung der Radio Ressourcen nehmen. Über optionale Parameter des at+cgdcont Befehls (vgl. Kapitel 2.8) kann der Benutzer verschiedene QoS Parameter wie minimale Datenrate, maximale Verzögerungszeit, etc. anfordern. Es ist auch möglich, über unterschiedliche Access Point Names unterschiedliche Quality of Service Klassen zu definieren. Im HLR ist dazu für jeden APN auch ein entsprechendes Quality of Service Profil gespeichert.

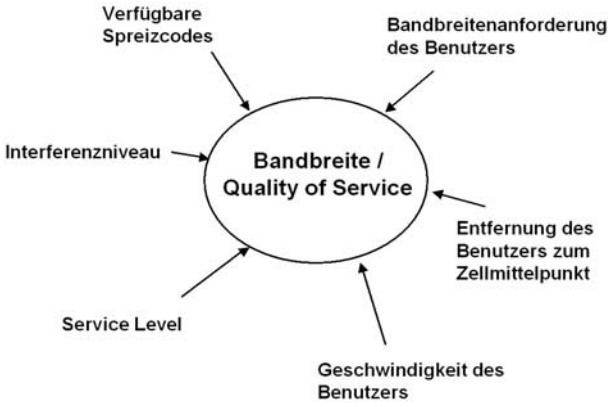

Abb. 3.23: Faktoren für die Beeinflussung der maximalen Bandbreite und des Quality of Service Level.

Service Level

Die Vergabe von Ressourcen auf dem Air Interface kann auch durch den Service Level des Nutzers beeinflusst werden. Dazu bietet UMTS die Möglichkeit, Nutzern unterschiedliche Service Levels zuzuteilen. Somit besteht für den Netzbetreiber die Möglichkeit, schnellere Datenübertragungsraten für Benutzer zu reservieren, die dafür eine extra Gebühr bezahlen. Auch ist es über

dieses Model möglich, bei hoher Last einer Zelle zuerst Kanäle von Benutzern auf geringere Geschwindigkeiten zu reduzieren, die weniger bezahlen.

Die Iur Schnittstelle und RNSAP

Aus Gründen der Vollständigkeit sollte an dieser Stelle auch noch kurz die Iur Schnittselle erwähnt werden, die RNCs untereinander verbinden kann. Diese Schnittstelle unterstützt das in Kapitel 3.7.1 beschriebene Soft Handover Verfahren über RNC Grenzen hinweg. Außerdem werden über die Iur Schnittsetlle die in Kapitel 3.5.4 beschrieben RRC Zustände Cell-FACH, Cell-PCH und URA-PCH über Zellgrenzen hinweg ermöglicht. Das dazu nötige Protokoll wird Radio Network Subsystem Application Part (RNSAP) genannt.

3.5.3 Adaptive Multi Rate (AMR) für Sprachübertragung

Auch mit dem Einsatz unterschiedlicher Sprachcodecs geht UMTS über seinen Vorgänger GSM hinaus. In GSM werden heute, wie in Kapitel 1.7.5 beschrieben, der Full Rate (FR) und Enhanced Full Rate Codec (EFR) verwendet, um 64 kbit/s Sprachkanäle des Kernnetzes auf ca. 12 kbit/s zu komprimieren. Dies ist nötig, da die Bandbreite auf der Luftschnittstelle sehr begrenzt ist. Der zu verwendende Codec wird dabei beim Aufbau der Verbindung zwischen Teilnehmer und Netzwerk ausgehandelt und ändert sich während der Verbindung nicht mehr. Die BTS fügt noch Fehlererkennungsbits und Fehlerkorrekturbits zum Datenstrom hinzu und erzeugt somit eine Datenrate von etwa 22 kbits/s. Auch bei UMTS wird der Enhanced Full Rate Codec verwendet. Da jedoch in der Zwischenzeit noch wesentlich effizientere Codecs entwickelt wurden, bietet UMTS auch die Möglichkeit, andere Codecs mit geringeren Bitraten einzusetzen. Der verwendete Sprachcodec ist bei UTMS auch nicht fest, sondern kann alle 20 Millisekunden geändert werden. Diese Eigenschaft wird Adaptive Multi Rate (AMR) genannt und bietet eine Anzahl von Vorteilen für Netzwerkbetreiber und Anwender:

AMR

Anpassung des Codecs an Übertragungsbedingungen

Wird die Verbindungsqualität schlechter, kann ein Sprachcodec mit geringerem Bandbreitenbedarf gewählt werden. Wird der Spreizfaktor nicht geändert, können die frei werdenden Bits für die Fehlererkennung und Fehlerkorrektur verwendet werden. Einerseits bietet ein Sprachcodec mit geringerer Bandbreite zunächst eine qualitativ schlechtere Sprachqualität. Dies ist aber einer höheren Fehlerrate und der daraus resultierenden schlechten Sprachqualität vorzuziehen. Wird die Verbindungsqualität

wieder besser, kann auch wieder ein besserer Sprachcodec verwendet werden.

Befinden sich viele Teilnehmer in einer Zelle, kann das Netzwerk für neue oder bestehende Sprachverbindungen einen Codec mit geringerem Bandbreitenbedarf wählen und den Spreizfaktor erhöhen. Somit sinkt zwar die Sprachqualität für diese Teilnehmer, es können aber mehr Teilnehmer über die Zelle kommunizieren.

Nachfolgende Tabelle gibt einen Überblick über die verschiedenen AMR Codecs, die in UMTS in 3GPP TS 26.071 standardisiert wurden. Während das Endgerät alle Codecs unterstützen muss, ist es dem Netzwerk freigestellt, welche es verwendet.

Codec Mode	Datenrate
AMR_12.20	12.20 kbit/s (GSM EFR)
AMR_10.20	10.20 kbit/s
AMR_7.95	7.95 kbit/s
AMR_7.40	7.40 kbit/s (IS-641)
AMR_6.70	6.70 kbit/s (PDC-EFR)
AMR_5.90	5.90 kbit/s
AMR_5.15	5.15 kbit/s
AMR_4.75	4.75 kbit/s

AMR auch für GSM

Das AMR Verfahren wurde im Nachhinein auch in den GSM Standard übernommen und alle größeren Netzwerkhersteller bieten in Ihren Radionetzwerkprodukten heute auch AMR für GSM an. Die Verwendung von AMR ist bei GSM aber optional und muss natürlich auch vom Endgerät unterstützt werden.

3.5.4 Radio Resource Control (RRC) Zustände

Die Aktivität eines Teilnehmers bestimmt, wie häufig und in welcher Art Daten auf der Luftschnittstelle zwischen Endgerät und Netzwerk ausgetauscht werden. In UMTS kann sich ein Endgerät in einem der folgenden fünf Radio Resource Control States (Zustände) befinden:

Idle State

Im Idle Zustand ist ein Endgerät zwar am Netzwerk angemeldet (vgl. Attach Prozedur), es besteht aber weder eine logische noch

eine physikalische Verbindung mit dem Netzwerk. Praktisch bedeutet dies, dass der Teilnehmer momentan weder ein Telefongespräch führt, noch Daten überträgt. Unter Umständen kann der Teilnehmer jedoch einen aktiven PDP Kontext besitzen, was gleichbedeutend mit einer zugewiesenen IP Adresse ist. Aufgrund einer langen Inaktivität wurde jedoch der Radio Bearer des Teilnehmers vom Netzwerk abgebaut. Möchte ein Endgerät Daten senden, muss zunächst erneuet eine Verbindung aufgebaut werden und das Endgerät wechselt in den Cell-DCH oder Cell-FACH Zustand.

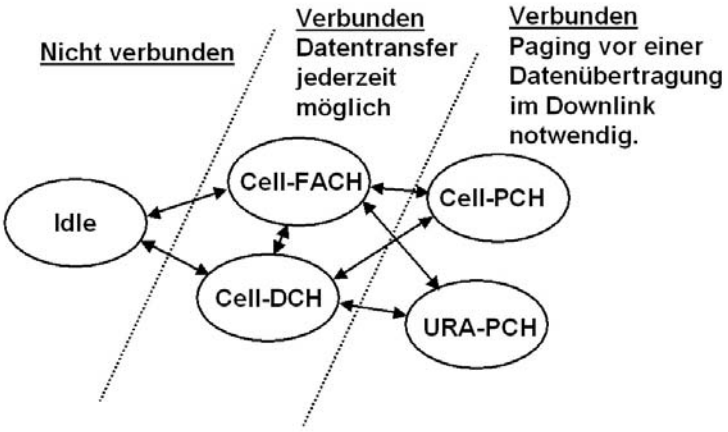

Abb. 3.24: Radio Ressource Control Zustände

Cell-DCH State

Der Cell-DCH RRC Zustand wird ähnlich dem GSM-Dedicated Mode für leitungsvermittelte Sprachverbindungen verwendet. In diesem Zustand besteht eine ständige physikalische Verbindung zwischen Teilnehmer und Netzwerk. Dies bedeutet bei UMTS, dass das Netzwerk dem Teilnehmer im Downlink einen eigenen Spreading Code und im Uplink eigene Spreading und Scrambling Codes zuteilt.

Der Cell-DCH Zustand wird bei UMTS auch für paketvermittelte Verbindungen verwendet. Dies widerspricht im ersten Moment dem paketvermittelten Ansatz. Dessen Vorteil ist normalerweise, dass nur Ressourcen während der Datenübertragung benötigt werden. Im Cell-DCH Zustand wird aber die Ressource, also der dedizierte Kanal, nicht freigegeben, wenn keine Daten mehr übertragen werden. Der CDMA Ansatz von UMTS bietet jedoch eine elegante Lösung dieses Problems. Empfängt oder sendet der

Teilnehmer keine Daten, wird auf dem Kanal außer Kontrolldaten auch nichts gesendet. Während der Sendepausen sinkt somit der Interferenzlevel für alle anderen Teilnehmer. Statt des dedizierten Kanals wird die Ressource in Form einer geringeren Interferenz freigegeben, und steht sofort für andere Teilnehmer zur Verfügung. Sind wieder Daten auf der Luftschnittstelle von oder zu einem Teilnehmer zu senden, müssen keine neuen Ressourcen angefordert werden, da der dedizierte Kanal in Form eines Spreading- oder Scrambling Codes nicht abgebaut wurde. Während des erneuten Sendens erhöht sich die Interferenz natürlich für die anderen Teilnehmer wieder. Diese Vorgehensweise wirkt sich speziell bei burstartigen Übertragungen wie dem Web Surfen sehr positiv aus. Bei einer solchen Anwendung sind die Zugriffe der einzelnen Teilnehmer auf die Luftschnittstelle im mittel statistisch gleichmäßig verteilt. Die Gesamtkapazität der Luftschnittstelle wird weiter optimal ausgenutzt, ohne den noch bei GSM/GPRS vorhanden Nachteil der zeitaufwändigen Anforderungen für Ressourcen.

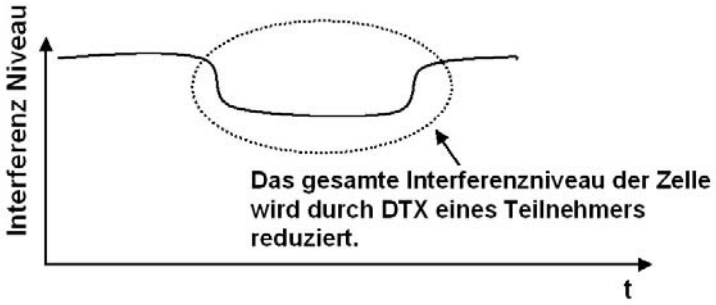

Abb. 3.25: Discontinuous Transmission (DTX) auf einem Dedicated Channel senkt Interferenz für andere Teilnehmer.

Mit Hilfe von Signalstärkemessungen des Endgerätes und des Node-Bs regeln der Node-B und der RNC die Sendeleistung des Kanals in Uplink und Downlink. Über den PDCCH hat das Netzwerk die Möglichkeit, die Sendeleistung des Teilnehmers 1500-mal pro Sekunde den aktuellen Bedingungen anzupassen. Diese sehr schnelle Leistungsregelung ist bei UMTS besonders wichtig, da die Interferenz die maximale Bandbreite einer Zelle limitiert.

Handover im Cell-DCH State

Auch im Cell-DCH Zustand misst das Endgerät ständig die Empfangsqualität aller Nachbarzellen und teilt das Ergebnis dem Netzwerk mit. Der RNC kann dann aufgrund dieser Messungen einen Zellwechsel (Handover) veranlassen (vgl. Kapitel 3.7.1).

Während das Reportintervall bei GSM eine fest vorgegebene Periode hat, wurde dies bei UMTS wesentlich flexibler gestaltet. Zum einen gibt es weiterhin das periodische Reporting, dessen Periode nun aber vom Netz zwischen 250 Millisekunden und 64 Sekunden flexibel konfigurierbar ist. Zum anderen ist es für ein UMTS Endgerät auch möglich, nur Messergebnisse an den RNC zu senden, wenn diese vom RNC vorgegebene Bedingungen erfüllen. So ist es zum Beispiel möglich, nur Messergebnisse von Nachbarzellen zu senden, die einen vom RNC festgelegten Grenzwert überschreiten. Die eingesparte Bandbreite kann somit in vielen Fällen statt für die Übertragung von Signalisierungsdaten für Nutzdaten verwendet werden. Ein weiterer Vorteil dieser Methode für den RNC ist außerdem, dass weniger Rechenleistung pro Verbindung benötigt wird, als bei periodisch eintreffenden Messergebnissen.

Ein Dedicated Channel kann je nach den Anforderungen an die zu übertragenden Daten ganz unterschiedliche Eigenschaften besitzen. Eine dieser Eigenschaften ist zum Beispiel die Länge des Spreading Codes. Dieser bestimmt, mit welcher maximalen Geschwindigkeit die Nutzdaten übertragen werden können. In Abhängigkeit des Spreading Codes können somit Datenraten von wenigen Kilobits bis mehrere hundert Kilobits pro Sekunde erreicht werden (vgl. auch Kapitel 3.3.2).

Cell-FACH State

Während der Idle und Cell-DCH RRC State in jedem Fall im Netzwerk implementiert sein müssen, sind der Cell-FACH, sowie der Cell-PCH und URA-PCH State nicht zwingend vom Standard vorgeschrieben. Der Cell-FACH State wird vor allem für die Übertragung von paketvermittelten Daten verwendet. Ein Teilnehmer bekommt in diesem Zustand keinen eigenen Kanal zugeteilt, sondern empfängt seine Daten auf dem Forward Access Channel (FACH). Wie in Kapitel 3.4.5 beschrieben, ist die primäre Aufgabe des FACH eigentlich die Übertragung von RRC Connection Setup Nachrichten an Teilnehmer, die über den Random Access Channel Verbindung mit dem Netz aufgenommen haben. Ist der Cell-FACH State im Netzwerk implementiert, kann dieser Kanal nun aber auch verwendet, um Nutzdatenpakete oder Signalisierungsnachrichten von MSC und SGSN an Endgeräte zu senden. Der FACH ist ein „Common“ Channel, da auf ihm Pakete unterschiedlicher Nutzer transportiert werden. Alle Endgeräte, die sich in diesem Zustand befinden, müssen den FACH abhören. Im MAC Header jedes Pakets befindet sich die Adresse des Teilnehmers, für den das Paket bestimmt ist. Nur Pakete für den eigenen Benutzer werden von den unteren Protokollschichten

eines Endgeräts an höhere Protokollschichten weitergegeben. Somit entspricht dieser RRC Zustand in etwa dem Ethernet Model. Auch hier gibt es ein gemeinsames Medium und jede Station empfängt alle Pakete. Außerdem entspricht der Cell-FACH Zustand auch in etwa dem GSM/GPRS Verfahren für die paketvermittelte Datenübertragung. Sind Daten in Downlink Richtung zwischen Netzwerk und Endgerät zu übertragen, müssen keine Ressourcen zugewiesen werden und die Übertragung kann je nach aktueller Netzwerklast und Teilnehmerpriorität sehr schnell erfolgen.

Cell-FACH bei geringer Nutzeraktivität

Da sich mehrere Teilnehmer den Kanal teilen, kann jedoch keine Datenrate und konstante Verzögerungszeit garantiert werden. Während die Mobilität im Cell-DCH Zustand vom Netzwerk kontrolliert wird, ist dies im Cell-FACH Zustand Aufgabe des Endgeräts. Statt eines Handovers wird in diesem Zustand ein Cell Update vom Endgerät autonom durchgeführt, und es entsteht eine kurze Unterbrechung der Verbindung. Für Echtzeitanwendungen oder Streamingapplikationen ist dieser RRC Zustand also nicht geeignet. Besser geeignet ist er jedoch für sehr burstartige Applikationen wie z.B. dem WAP browsen. Da Endgerätedisplays sehr klein sind, sind die zu übertragenen Datenmengen beim WAP browsen in vielen Fällen nur sehr klein. Somit wird nicht unbedingt ein dedizierter Übertragungskanal benötigt.

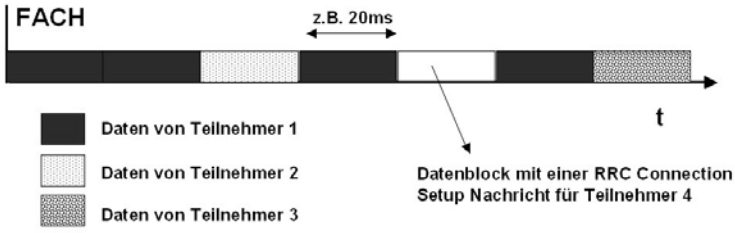

Abb. 3.26: Daten unterschiedlicher Teilnehmer auf dem FACH

Cell-FACH für Mobility Management Operationen

Der Cell-FACH Zustand eignet sich auch für die Übertragung von Mobility Management und Packet Mobility Management Signalisierungsnachrichten zwischen Endgerät und MSC bzw. SGSN. Da das Endgerät schon in der RRC Connection Setup Nachricht den Grund der Verbindung angibt, kann das Netzwerk dynamisch entscheiden, ob ein dedizierter Kanal für die Verbindung nötig ist, oder nicht. Ist der Cell-FACH Zustand im Netzwerk integriert,

braucht z.B. kein dedizierter Kanal für eine Location Update Prozedur zugeteilt werden.

RACH für Uplinkdaten

Im Uplink übertragen die Teilnehmer im Cell-FACH Zustand ihre Daten über den Random Access Channel (RACH), dessen Hauptaufgabe eigentlich die Übertragung von RRC Connection Setup Request Nachrichten ist. Wie in Kapitel 3.4.5 gezeigt wurde, ist der Zugriff auf den RACH ein zeitaufwändiger Prozess, der für eine Verzögerung sorgt, bevor die Daten tatsächlich gesendet werden können. Auch aus diesem Grund ist der Cell-FACH Zustand nicht für Echtzeitapplikationen geeignet.

Für ein Endgerät gibt es zwei Möglichkeiten, in den Cell-FACH Zustand zu wechseln. Wie bereits erwähnt, kann sich das Netzwerk während des RRC Connection Setups entscheiden, den Teilnehmer für eine MM/PMM Signalisierung oder für die paketvermittelte Datenübertragung in den Cell-FACH zu setzen. Außerdem ist es möglich, vom Cell-DCH Zustand in den Cell-FACH Zustand zu wechseln. Der RNC kann dies z.B. veranlassen, wenn für längere Zeit keine Daten von oder zu einem Endgerät übertragen wurden. Der dadurch frei werdende Spreizcode kann danach sofort an einen anderen Teilnehmer vergeben werden. Außerdem reduziert der Cell-FACH Zustand die Leistungsaufnahme des Endgerätes. Solange der Teilnehmer nun nur kleine Datenmengen überträgt, wird der Cell-FACH Zustand beibehalten. Überträgt der Teilnehmer wieder mehr Daten, ist natürlich wieder ein Zustandswechsel in den Cell-DCH Zustand möglich.

Cell-PCH, URA-PCH

Der optionale Cell-PCH (Cell-Paging Channel) RRC Zustand und der URA-PCH (UTRAN Registration Area–Paging Channel) RRC Zustand reduzieren in Phasen längerer Inaktivität die Leistungsaufnahme des Endgerätes weiter. Ähnlich dem Idle Zustand ist einem Endgerät in diesen Zuständen kein Übertragungskanal zugewiesen, der in Downlink Richtung überwacht werden müsste. Sollen erneut Daten in Downlink Richtung übertragen werden, muss der RNC den Teilnehmer zuvor pagen. Das Endgerät antwortet daraufhin mit einer RRC Connection Request Nachricht, die es dem RNC ermöglicht, einen neuen Übertragungskanal zum Endgerät aufzubauen. Auch für den Fall, dass zuerst das Endgerät neue Datenpakete zum Netzwerk senden möchte, muss zuvor ein neuer Übertragungskanal aufgebaut werden. In beiden Fällen wechselt das Endgerät durch den Aufbau des Übertragungskanals automatisch wieder in den Cell-FACH oder Cell-DCH Zustand. In welchen Zustand gewechselt wird, entscheidet der RNC.

Wie der Name Cell-PCH andeutet, wird ein Teilnehmer vom Netzwerk im Falle von neu eintreffenden Paketen nur in einer Zelle gesucht. Dies bedeutet, dass das Endgerät bei einem Zellwechsel eine Cell Update Nachricht zum RNC senden muss. Im URA-PCH Zustand wird der Teilnehmer hingegen in einer ganzen UTRAN Registration Area gepaged, die vom RNC verwaltet wird (vgl. Kapitel 3.7.3).

Im Unterschied zum Idle Zustand gibt es in diesen Zuständen jedoch weiterhin eine logische RRC Verbindung zwischen Endgerät und SGSN. Da die RRC Zustände auf dem RNC verwaltet werden, hat jedoch der SGSN als Kernnetzkomponente keine Informationen darüber, in welchem RRC Zustand sich ein Teilnehmer befindet. Somit sendet er die Pakete weiterhin ohne Verzögerungen zum Serving-RNC des Teilnehmers. Befindet sich das Endgerät im Cell-PCH oder URA-PCH Zustand, muss der RNC, wie gerade beschrieben, vor der Weiterleitung der Pakete erneut einen physikalischen Übertragungskanal aufbauen. Die logische Trennung von einer Verbindung zwischen Endgerät und Core Netzwerk (SGSN und MSC) einerseits und einer Verbindung zwischen Endgerät und dem Radionetzwerk (RNC) andererseits wurde in UMTS ganz bewusst eingeführt. Dies hat den großen Vorteil, dass der MSC und der SGSN komplett von den Eigenschaften des Radionetzwerkes abgekoppelt sind. Auf diese Weise ist es möglich, dass sich Radionetzwerk und Kernnetz unabhängig voneinander weiterentwickeln können.

Der Unterschied zwischen Idle-, Cell-PCH und URA-PCH State ist in der Praxis sehr gering. Sowohl bei der Leistungsaufnahme im Endgerät, als auch bei der Dauer für die Wiederaufnahme einer Datenübertragung unterscheiden sich die Zustände nur unwesentlich. Deshalb ist fraglich, ob alle RRC Zustände von den Netzwerkherstellern implementiert werden.

Wie in Kapitel 2 beschrieben, werden bei GSM die GPRS RRC Zustände nur im Endgerät und im SGSN verwaltet. Der SGSN weis in diesem System also zu jeder Zeit, ob sich ein Teilnehmer im Idle, Ready oder Standby State befindet. Somit musste dieser als Kernnetzkomponente auch Aufgaben des Radio Netzwerkes wie z.B. Cell Updates übernehmen. Dies hat einerseits den Vorteil, dass der SGSN für Teilnehmer im Ready State die genaue Zelle des Teilnehmers kennt. Vorteil der Lösung in UMTS ist jedoch das Verteilen dieser Aufgaben auf mehrere RNCs und somit eine Reduktion der Signalisierungslast des SGSNs.

	RNC State	SGSN State
Idle	Nicht verbunden	Nicht verbunden
Cell–DCH	Verbunden, Daten werden sofort über den DCH, DSCH oder HS-DSCH geschickt.	Verbunden
Cell-FACH	Verbunden, Daten werden sofort über den FACH (Common Channel) geschickt.	Verbunden
Cell-PCH	Verbunden, Teilnehmer muss jedoch vor der Datenübertragung gesucht werden (paging). Nach der Antwort auf das Paging wird der Teilnehmer in den Cell-FACH oder Cell-DCH gesetzt. Bei Zellwechsel muss das Netzwerk benachrichtigt werden.	Verbunden
URA-PCH	Wie Cell-PCH, jedoch muss das Netzwerk nur dann von einem Zellwechsel benachrichtigt werden, wenn der Teilnehmer in eine Zelle wechselt, die sich in einer anderen UTRAN Registration Area befindet.	Verbunden

3.6 Mobility Management aus Sicht des Kernnetzes

Aus Sicht des MSCs und des SGSNs kann sich ein Endgerät in den Mobility Management (MM) bzw. Packet Mobility Management (PMM) Zuständen Detached, Idle und Connected befinden.

Für die MSC haben diese Zustände folgende Bedeutung:

MM Detached MM Detached: Das Endgerät ist ausgeschaltet, und der Aufenthaltsort des Teilnehmers ist nicht bekannt. Eingehende Anrufe für den Teilnehmer können vom Netzwerk nicht zum Teilnehmer durchgestellt werden.

MM Idle MM Idle: Das Endgerät ist eingeschaltet und hat sich erfolgreich bei der MSC angemeldet (vgl. Attach Prozedur). Ein Teilnehmer kann nun jederzeit ein Gespräch beginnen. Bei eingehenden Anrufen wird der Anrufer von der MSC in seiner aktuellen Location Area gesucht (paging).

MM Connected MM Connected: Das Endgerät und die MSC haben eine aktive Signalisierungs- und Kommunikationsverbindung. Dies kann zum Beispiel ein Telefongespräch, ein Datenruf oder ein Videocall sein. In diesem Zustand hat das Radionetzwerk dem Teilnehmer immer einen DCH zugeteilt. Der Teilnehmer befindet sich somit aus der Sicht des RNCs im Cell-DCH RRC Zustand.

Für den SGSN gibt es folgende Packet Mobility Management Zustände:

PMM Detached PMM Detached: Das Endgerät ist ausgeschaltet, und der Aufenthaltsort des Teilnehmers ist dem SGSN somit nicht bekannt. Ein Endgerät kann in diesem Zustand auch keinen aktiven PDP Kontext haben, es hat also auch keine aktuelle IP Adresse.

PMM Connected PMM Connected: Das Endgerät und der SGSN haben eine aktive Signalisierungs- und Kommunikationsverbindung. Der PMM Connected Zustand kann nur beibehalten werden, wenn der Teilnehmer einen PDP Kontext aktiviert hat, sprich über eine vom GGSN zugeteilte IP Adresse verfügt. In diesem Zustand sendet der SGSN alle vom Netzwerk eingehenden Datenpakete an den Serving-RNC weiter. Im Unterschied zu GSM/GPRS ist dem SGSN nur der Serving-RNC des Teilnehmers bekannt, nicht jedoch die Zelle. Dies ist aufgrund des in Kapitel 3.7 vorgestellten Soft Handovers auch nicht mehr möglich. Wie zuvor beschrieben, ist dem SGSN auch nicht bekannt, in welchem RRC Zustand sich das Endgerät befindet. In Abhängigkeit des Quality of Service Profils, der Netzwerklast und der eigenen Aktivität kann sich ein Endgerät im PMM-Connected Zustand in den RRC Zuständen Cell-DCH, Cell-FACH, CELL-PCH oder auch URA-PCH befinden.

PMM Idle PMM Idle: Hat sich ein Endgerät am Netzwerk erfolgreich angemeldet, und existiert momentan keine logische Signalisierungsverbindung zum SGSN, befindet es sich im PMM Idle Zustand.

Dies ist zum Beispiel der Fall, wenn der Teilnehmer keinen PDP Kontext aktiviert hat.

Außerdem hat der RNC die Möglichkeit, die RRC Ressourcen für eine bestehende paketvermittelte Verbindung jederzeit zu modifizieren. Dies kann bedeuten, dass sich der RNC bei langer Inaktivität eines Teilnehmers entscheidet, das Endgerät in den RRC Idle Zustand zu versetzen. Da der RNC die Mobilität des Teilnehmers dann nicht mehr überwacht, fordert er den SGSN auf, den Teilnehmer vom PMM Connected Zustand in den PMM Idle Zustand zu setzten. Obwohl der Teilnehmer nun aus RRC Sicht und aus PMM Sicht im Idle Zustand ist, bleibt der PDP Kontext weiter aktiv, der Teilnehmer muss seine IP Adresse nicht abgeben. Für den SGSN bedeutet dies, dass bei neuen Daten aus dem Netzwerk der Teilnehmer erst gesucht und danach eine neue Verbindung für Signalisierungs- und Nutzdaten aufgebaut werden muss.

3.7 Mobility Management aus Sicht des Radionetzwerkes

Je nach Mobility Management Zustand des Kernnetzwerkes kann sich das Radionetzwerk in einer Reihe unterschiedlicher RRC Zustände befinden. Wie das Mobility Management im Radionetzwerk gehandhabt wird, hängt vom jeweiligen Zustand ab. Die nachfolgende Tabelle gibt einen Überblick über MM und PMM Zustände im Kernnetz und die jeweils dafür möglichen RRC Zustände im Radionetzwerk.

MM States und mögliche RRC States	MM Idle	MM connected	PMM Idle	PMM connected
Idle	x		x	
Cell-DCH		x		x
Cell-FACH				x
Cell-PCH				x
URA-PCH				x

3.7.1 Mobility Management im Cell-DCH Zustand

Vom Netzwerk kontrollierte Mobilität im Cell-DCH State

Für Applikationen wie Sprach- oder Videoübertragungen ist es sehr wichtig, dass bei einem Zellwechsel keine, oder nur eine möglichst kurze Unterbrechung der Datenübertragung entsteht. Für diese und andere Anwendungen befindet sich deshalb das Endgerät im Cell-DCH State. Das Netzwerk kontrolliert in diesem Zustand ständig die Qualität der Verbindung und kann das Gespräch auf andere Zellen umleiten, wenn sich der Teilnehmer bewegt. Dieser Zellwechselvorgang, der vom Netzwerk kontrolliert wird, wird Handover oder Handoff genannt. Bei UMTS gibt es eine ganze Reihe unterschiedlicher Handover Varianten:

Hard Handover

Hard Handover: Diese Art des Handovers ist einem GSM Handover sehr ähnlich. Aufgrund von Signalstärkemessungen der aktuellen und benachbarten Zellen kann der RNC erkennen, wenn sich eine Nachbarzelle für die Weiterführung einer Verbindung besser eignet. Um die Verbindung in eine andere Zelle umleiten zu können, wird die neue Zelle vom RNC für den Handover vorbereitet. Dies bedeutet, dass alle nötigen Ressourcen auf der Iub Schnittstelle, und wenn nötig, auch auf der Iur Schnittstelle in ähnlicher Weise wie bei einem neuen Verbindungsaufbau eingerichtet werden.

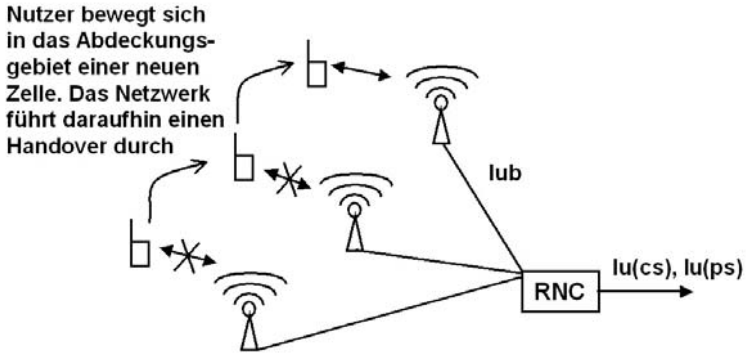

Abb. 3.27: UMTS Hard Handover

Danach wird das Endgerät über die noch aktive Verbindung aufgefordert, in die neue Zelle zu wechseln. Dieses Handover Kommando enthält unter anderem die neue Frequenz, sowie die Scrambling und Channelisation Codes der neue Zelle. Das Endgerät beendet dann die Verbindung zur aktuellen Zelle und versucht, eine neue Verbindung mit der neuen Zelle herzustellen.

Dies dauert normalerweise weniger als 100 Millisekunden, da das Netzwerk auf diesen Zellwechsel schon vorbereitet ist. Die Nutzdatenübertragung kann nach dem Zellwechsel sofort wieder aufgenommen werden. Diese Art Handover wurde UMTS Hard Handover genannt, da die Kommunikationsverbindung, wenn auch nur kurz, beim Zellwechsel unterbrochen wird.

Soft Handover

Soft Handover: Bei dieser Art des Handovers wird die Nutzdatenübertragung zwischen Endgerät und UTRAN zu keiner Zeit unterbrochen. Aufgrund von Signalstärkemessungen der aktuellen Zelle und der Nachbarzellen kann der RNC das Endgerät in den Soft Handover Zustand setzten. Alle Daten von und zum Endgerät werden dann nicht nur über einen Node-B, sondern über zwei oder mehr Node-Bs gesendet oder empfangen. Die an der Kommunikation beteiligten Node-Bs werden im so genannten Active Set der Verbindung geführt. Wird die Radioverbindung zu einem Node-B im Active Set zu schlecht, kann dieser aus der Kommunikationsverbindung entfernt werden. Auf diese Weise ist gewährleistet, dass trotz des Zellwechsels ein Teilnehmer zu keinem Zeitpunkt den Kontakt zum Netzwerk verliert. Ein Active Set kann dabei bis zu 6 Node-Bs umfassen. Abbildung 3.28 zeigt einen Soft Handover, an dem 3 Zellen beteiligt sind.

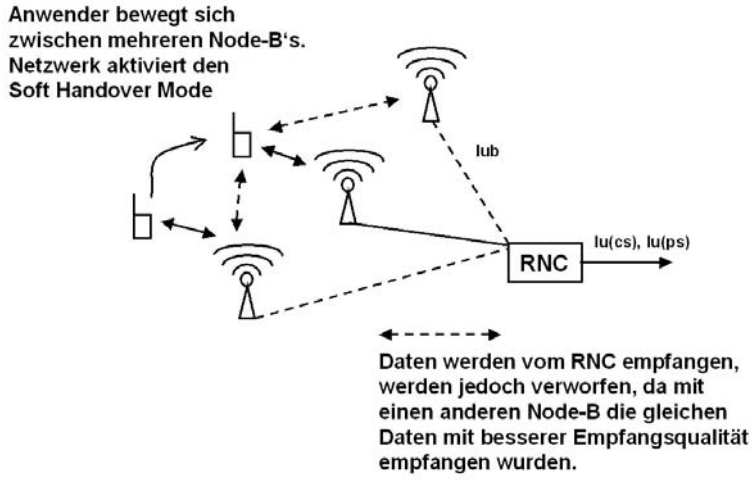

Abb. 3.28: Ein Teilnehmer während eines Soft Handovers mit 3 Node-Bs

Der Soft Handover hat gegenüber dem Hard Handover eine Reihe von Vorteilen: Durch den komplett unterbrechungsfreien Übergang zwischen den Zellen erhöht sich die Verbindungsqualität für den Teilnehmer. Da der Soft Handover schon begonnen

werden kann, wenn die Signalqualität der aktuellen Zelle noch akzeptabel ist, wird die Wahrscheinlichkeit eines Verbindungsabbruchs bei einer plötzlich eintretenden Signalverschlechterung deutlich reduziert.

Auch die Sendeleistung und somit der Stromverbrauch kann in einem Endgerät durch den Soft Handover Zustand in manchen Situationen verringert werden. Abbildung 3.29 zeigt ein solches Szenario. Ein Teilnehmer befindet sich in einem Bereich, der gut von Zelle 1 versorgt wird. Da er sich bewegt, verdecken von Zeit zu Zeit Gebäude den optimalen Übertragungsweg zu Zelle 1. Der Teilnehmer muss als Konsequenz seine Sendeleistung erhöhen. Im Soft Handover Fall kommuniziert der Teilnehmer aber auch gleichzeitig mit Zelle 2. Während die Verbindung zu Zelle 1 schlechter wird, bleibt die Verbindung zu Zelle 2 weiterhin gut, oder wird sogar besser. Die Sendeleistung des Endgeräts muss somit nicht erhöht werden, da die Daten vom Netzwerk über Zelle 2 weiterhin gut empfangen werden können. Dies bedeutet jedoch nicht, dass die Verbindung zu Zelle 1 in dieser Zeit abgebaut wird.

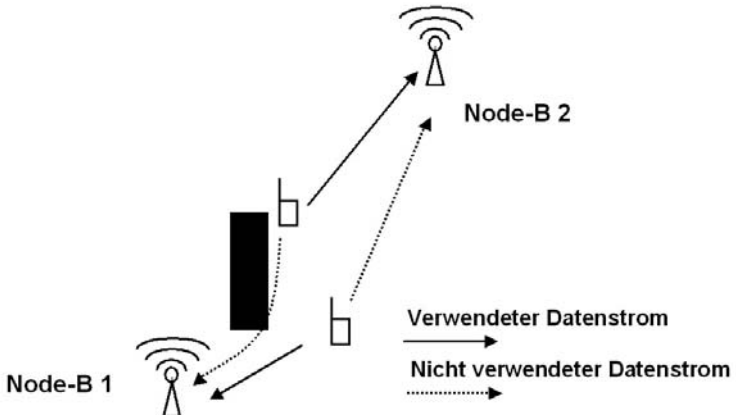

Abb. 3.29: Soft Handover reduziert die Sendeleistung des Endgeräts

In Uplink Richtung empfängt Zelle 1 weiterhin das gleiche Signal des Teilnehmers wie Zelle 2, wenn auch in schlechterer Qualität. Der RNC kann durch Auswertung der Signalqualität entscheiden, das aktuelle Datenpaket von Zelle 1 zu verwerfen und stattdessen das Paket von Zelle 2 ins Kernnetz weiterzuleiten. Diese

Entscheidung wird für jedes Paket, also alle 20,40 oder 80 Millisekunden neu getroffen.

Auch in Downlink Richtung empfängt der Teilnehmer weiterhin die Daten von Zelle 1 und Zelle 2. Da die Zellen unterschiedliche Channelisation und Scrambling Codes haben, werden diese vom Endgerät auch als zwei separate Datenströme auf der physikalischen Schicht behandelt. Dies bedeutet, dass der Downlink zweimal dekodiert werden muss, was natürlich mehr Rechenleistung in Anspruch nimmt.

Auch für das Netzwerk hat dieses Szenario Vorteile. Da das Endgerät immer nur mit der minimal nötigen Leistung sendet, um einen Node-B des Active Sets zu erreichen, reduziert sich die Interferenz in Uplink Richtung deutlich. Dies wiederum steigert die Kapazität des gesamten Systems, es können mehr Teilnehmer versorgt werden.

Der Soft Handover hat für das Netzwerk aber nicht nur Vorteile. In Downlink Richtung muss der RNC an jeden Node-B des Active Sets eine Kopie der Daten schicken. In der umgekehrten Richtung erhält der RNC von jedem Node-B eine Kopie der Daten im Uplink. Es wird somit wesentlich mehr Kapazität auf den Iub Schnittstellen für einen Teilnehmer im Soft Handover Zustand verwendet, als für einen Teilnehmer, der nur mit einem Node-B kommuniziert. Deshalb wird schon bei der Netzwerkplanung versucht, keine Bereiche zu schaffen, in denen mehr als 3 Node-Bs gut empfangen werden können.

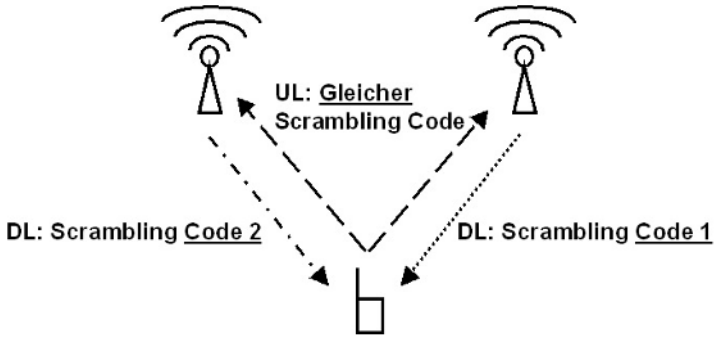

Abb. 3.30: Verwendung von Scrambling Codes beim Soft Handover

Soft Handover über Iur

Noch aufwändiger wird das Szenario, wenn am Soft Handover Node-Bs beteiligt sind, die nicht vom aktuellen S-RNC kontrolliert werden. In diesem Fall ist ein Soft Handover nur möglich, wenn der S-RNC mit dem oder den RNCs der zusätzlichen Node-Bs kommunizieren kann. Diese RNCs werden Drift RNCs oder D-RNCs genannt. Abbildung 3.31 zeigt ein Szenario mit einem S-RNC und einem D-RNC. Soll ein fremder Node-B in das Active Set eines Teilnehmers aufgenommen werden, muss der S-RNC über die Iur Schnittstelle mit dem zuständigen D-RNC Verbindung aufnehmen. Der D-RNC reserviert daraufhin die benötigten Übertragungsressourcen auf seinem Node-B und bestätigt die Anforderung des S-RNCs. Dieser informiert dann den Teilnehmer über eine „Update Active Set" Nachricht. Von nun an sendet der S-RNC alle Nutzdaten des Teilnehmers auch an den oder die zusätzlichen D-RNCs, die diese wiederum an ihre Node-Bs weitergeben. In umgekehrter Richtung leiten D-RNCs alle eingehenden Datenpakete des Endgerätes an den S-RNC weiter. Dieser kann dann entscheiden, ob Datenpakete von einem seiner eigenen Node-Bs oder von einem Node-B eines D-RNCs mit der besten Signalqualität empfangen wurden und leitet diese dann entsprechend an das Kernnetz weiter.

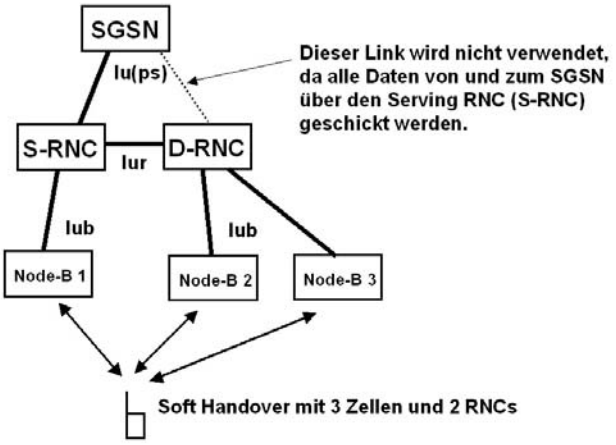

Abb. 3.31: Soft Handover mit S-RNC und D-RNC

Softer Handover

Als Softer Handover wird ein Szenario bezeichnet, bei dem zwei oder mehr Zellen des gleichen Node-Bs im Active Set eines Endgeräts enthalten sind. Für das Netzwerk bietet der Softer Handover den Vorteil, dass auf dem Iub Interface keine zusätzlichen Ressourcen für diesen Handover bereitgestellt werden müssen. Der Node-B übernimmt dabei die Aufgabe, die Datenströme in

Downlink Richtung auf seine Zellen zu verteilen und in Uplink Richtung die Daten zusammenzuführen. Der S-RNC erhält von einem solchen Node-B nur einen Datenstrom, selbst wenn z.B. drei unabhängige Zellen am Softer Handover beteiligt sind.

Kein Timing Advance in UMTS

Einer der wichtigsten Parameter auf der Luftschnittstelle bei GSM ist der Timing Advance. Mobilstationen, die weiter von der Basisstation entfernt sind, müssen aufgrund der Signallaufzeit ihre Daten früher in ihrem Zeitfenster senden, als Endgeräte, die näher an der Basisstation sind. Diese Sendezeitregelung wird Timing Advance genannt. In UMTS ist eine solche Regelung nicht möglich. Während sich ein Endgerät im Soft Handover Zustand befindet, empfangen alle Node-Bs im Active Set das gleiche Signal eines Endgerätes. Die Node-Bs befinden sich aber alle in einem unterschiedlichen Abstand zum Teilnehmer und empfangen somit die Signale zu etwas unterschiedlichen Zeiten. Für das Endgerät ist es nicht möglich, dies durch verschieben des Sendezeitpunktes auszugleichen, da es ja nur ein Signal in Uplink Richtung sendet. Eine Timing Advance Regelung ist aber auch aus folgenden Gründen nicht notwendig:

Alle Teilnehmer senden zur gleichen Zeit. Da keine Zeitschlitze verwendet werden, kann es auch keine Kollisionen zwischen verschiedenen Teilnehmern geben.

Um die Orthogonalität der Channelisation Codes zu gewährleisten, müssten alle Teilnehmer im Uplink am Node-B eigentlich gleichzeitig empfangen werden. Durch die zusätzliche Verwendung von Scrambling Codes werden die Teilnehmer aber voneinander entkoppelt. Eine zeitliche Verschiebung der unterschiedlichen Signale ist somit kein Problem.

Die Zeitverschiebung des Signals eines Teilnehmers an unterschiedlichen Node-Bs ist gemessen an der Übertragungsdauer eines kompletten Pakets immer noch sehr gering. Während die Übertragungsdauer eines Pakets 20,40 oder 80 Millisekunden beträgt, ist die Paketverzögerung auch bei einem Distanzunterschied von 30 Kilometer zwischen unterschiedlichen Node-Bs nur 0,1 Millisekunden. Diese Zeitdifferenz ist somit auf der Iub Schnittstelle vernachlässigbar.

SRNS Relocation

Entfernt sich ein Teilnehmer mit der Zeit immer weiter von seinem S-RNC, so kann der Fall eintreten, dass kein Node-B mehr an der Verbindung beteiligt ist, der direkt am S-RNC angeschlossen ist. Abbildung 3.32 zeigt dieses Szenario. Aus Gründen der Radionetzwerkoptimierung kann der S-RNC dann beim MSC und/oder SGSN eine Änderung des Routings auf dem

Iu(cs)/Iu(ps) Interface beantragen. Dies geschieht mit einer Serving Radio Network Subsystem (SRNS) Relocation Request Nachricht. Aus dem aktuellen D-RNC wird dann der neue S-RNC. Nach dem SRNS Relocation Request ist dann nur noch ein RNC an der Verbindung beteiligt und auch die Ressourcen auf der Iur Schnittstelle werden nicht mehr benötigt.

Ein SRNS Relocation ist auch dann notwendig, wenn zwischen zwei RNCs keine Iur Verbindung besteht und ein Handover notwendig ist. Hier steht nicht die Verbindungsoptimierung im Radionetzwerk im Vordergrund, sondern die Aufrechterhaltung der Verbindung. In diesem Fall ist neben dem SRNS Relocation auch ein Hard Handover zur neuen Zelle notwendig, da aufgrund der fehlenden Iur Verbindung kein Soft Handover möglich ist.

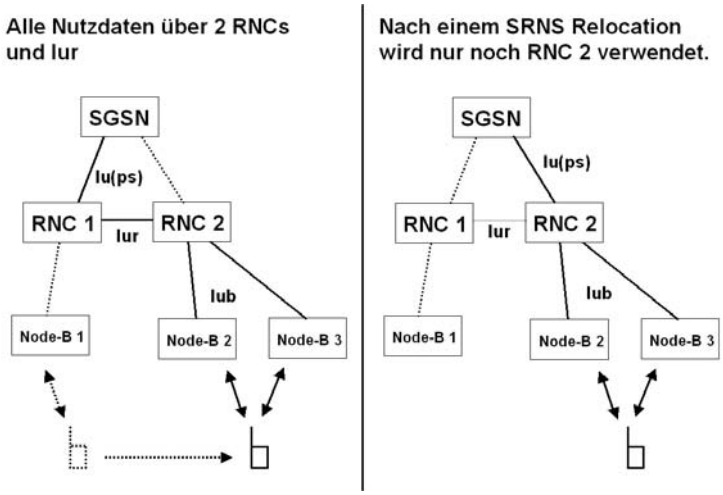

Abb. 3.32: SRNS Relocation

Intersystem Handover

Als die ersten GSM Mobilfunknetzwerke Anfang der neunziger Jahre aufgebaut wurden, gab es zwar schon flächendeckende Vorgängernetzwerke, deren Kundenzahl war jedoch gering. Somit war es nicht unbedingt notwendig, auch mit dem neuen GSM Netz sofort eine flächendeckende Netzversorgung zu gewährleisten.

Beim Start von UMTS hat sich die Situation jedoch völlig geändert. Durch den enormen Erfolg von GSM besitzt heute die Mehrzahl der Bewohner in Europa ein GSM Mobiltelefon. Da beim Start des UMTS Netzes noch keine flächendeckende Versorgung gewährleistet werden kann, ist ein fließender Übergang

zwischen GSM und UMTS Netzwerken notwendig. Dies bedeutet für den Mobiltelefonmarkt in der Praxis, dass UMTS Telefone auch GSM und GPRS unterstützen müssen. Während sich ein Teilnehmer in einer Region aufhält, die bereits per UMTS versorgt wird, werden sowohl Sprach- als auch Datenübertragung über das UMTS Netzwerk abgewickelt. Bewegt sich ein Teilnehmer aus einem von UMTS versorgten Gebiet hinaus, wechselt das Mobiltelefon automatisch in ein GSM Netzwerk und nutzt für die Datenübertragung GPRS. Dies soll auch während eines laufenden Telefongesprächs oder einer laufenden Datenübertragung möglich sein. Dieser Übergang wird als Intersystem Handover bezeichnet.

In UMTS gibt es eine Anzahl unterschiedlicher Möglichkeiten, einen solchen Intersystem Handover durchzuführen:

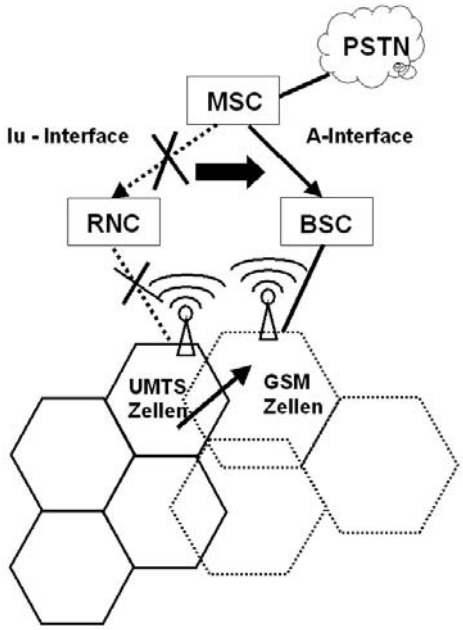

Abb. 3.33: 3G nach 2G Handover

Blind Intersystem Handover

Beim Blind Intersystem Handover weiß der RNC, ob für eine aktive UMTS Zelle eines Teilnehmers nur eine GSM Nachbarzelle existiert. Bewegt sich der Teilnehmer aus dem Versorgungsbereich der UMTS Zelle hinaus, leitet der RNC den Handover ein. Dieser Handover Vorgang wird „blind“ genannt, da bei der Handover Entscheidung keine Messergebnisse über die Empfangsstärke der GSM Zelle verwendet werden.

Vorteil dieses Verfahrens ist sicherlich die einfache Implementierung im Netzwerk und in den Endgeräten. Diesem stehen jedoch eine Reihe Nachteile gegenüber:

- Das Netzwerk hat keine Informationen, ob die Zielzelle vom Endgerät überhaupt empfangen werden kann.
- Das Endgerät ist mit der Zielzelle nicht synchronisiert. Dies verlängert die Zeit erheblich, die das Endgerät benötigt, mit der Zielzelle Kontakt aufzunehmen. Für den Anwender macht sich dies zum Beispiel bei der Sprachübertragung durch eine kurze Unterbrechung bemerkbar.
- Hat eine UMTS Zelle, wie in Abbildung 3.34 dargestellt, mehrere GSM Nachbarzellen, so kann der RNC nicht wissen, in welche GSM Zelle er den Teilnehmer übergeben soll. Ein solches Szenario sollte beim Blind Handover vermieden werden. Dies ist aber in der Praxis oftmals schwer.

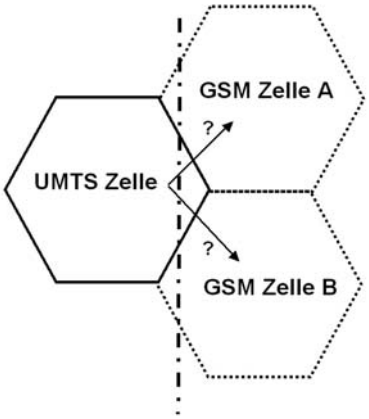

Abb. 3.34: UMTS Zelle mit mehreren GSM Nachbarzellen, die beim Blind Handover nicht unterschieden werden können.

Handover mit GSM Messungen

Neben dem Blind Intersystem Handover gibt es auch einen gesteuerten Intersystem Handover. Dazu informieren UMTS Zellen am Rande des UMTS Versorgungsgebietes Endgeräte im Idle und Dedicated Mode nicht nur über UMTS Nachbarschaftszellen, sondern auch über GSM Zellen. Ein Endgerät im Dedicated Mode kann somit während einer aktiven Kommunikation die Signalstärke und Qualität von UMTS und GSM Nachbarzellen messen. Wie bereits zu Beginn des Kapitels beschrieben, werden die Ergebnisse dieser Messungen an den RNC geschickt. Dieser

kann dann aufgrund der sich verschlechternden UMTS Signalqualität einen Intersystem Handover in das GSM Netzwerk veranlassen. Hier wird natürlich die Mithilfe des MSCs benötigt, da der RNC keine GSM Zellen kontrolliert.

Compressed Mode

Nachbarzellenmessungen sind bei UMTS recht einfach, wenn es sich um UMTS Nachbarzellen handelt, die auf der gleichen Frequenz senden. Das Endgerät muss dann lediglich die Primary Codes der Nachbarzellen auf das empfangene Signal anwenden, um das Signal dieser Zellen zu dekodieren. Dies bedeutet für das Endgerät nur einen zusätzlichen Rechenaufwand. Bei GSM Nachbarzellen kann dieses Verfahren nicht angewandt werden, da diese auf einer anderen Frequenz senden. Somit können diese nicht gleichzeitig zu den Zellen im Active Set empfangen werden. Auch UMTS Zellen, die auf einer anderen Frequenz senden, können mit diesem Verfahren nicht empfangen werden. Solche Zellen können aber z.B. verwendet werden, um die Gesamtkapazität des Systems zu erhöhen. Somit bleibt dem Endgerät nichts anderes übrig, als Sende- und Empfangspausen einzulegen, um diese Nachbarzellenmessungen vorzunehmen. Dies wird bei UMTS als Compressed Mode bezeichnet. Bei Bedarf wird dieser Modus, vom RNC gesteuert, in allen Node-Bs des Active Sets und dem Endgerät aktiviert und wieder deaktiviert. Der UMTS Standard definiert drei Möglichkeiten, wie der Compressed Mode realisiert werden kann. Die Systemhersteller können wählen, welche dieser Möglichkeiten sie implementieren:

- Reduktion des Spreizfaktors: Hier wird der Spreizfaktor für manche Pakete reduziert. Somit können in diesen Paketen mehr Daten übertragen werden. Diese kurzfristige Geschwindigkeitssteigerung kann danach für eine Übertragungspause verwendet werden. Während dieser Pause können dann die Messungen vorgenommen werden. Da sich der Spreizfaktor ändert, muss auch die Sendeleistung in dieser Zeit erhöht werden, um eine sichere Übertragung zu gewährleisten.
- Punktierung: Nachdem der Kanalkodierer dem Originaldatenstrom Fehlererkennungs- und Fehlerkorrekturbits hinzugefügt hat, werden ein Teil dieser Bits wieder entfernt, um Zeit für die Messungen zu schaffen. Auch hier muss wiederum die Sendeleistung erhöht werden, um die Anzahl der Fehler zu minimieren.

- Verwenden eines Rahmenformates mit weniger Datenbits: Da hier schon bei der Übertragung weniger Bits verwendet werden, muss die Sendeleistung nicht erhöht werden, um einen weiterhin guten Empfang zu gewährleisten. Der Nachteil zu den zwei anderen Verfahren ist jedoch die geringere Datenrate, während der Compressed Mode aktiviert ist.

Ziel aller Verfahren ist es, den Frequency Correction Channel (FCCH) und den Synch Channel (SCH) einer GSM Zelle zu finden (vgl. Kapitel 1.7.3).

Intersystem Handover von 3G nach 2G im Kernnetz

Abbildung 3.35 zeigt den Ablauf eines Intersystem Handovers von UMTS nach GSM. Dieser beginnt auf der UTRAN Seite, wie bei einem normalen Inter-MSC Handover, mit einem SRNS Relocation Request. Da in GSM der SRNS Relocation Vorgang nicht bekannt ist, verwendet die 3G MSC die schon von GSM bekannte 2G Prepare Handover Nachricht. Für die 2G MSC sieht dieser Handover wie ein normaler GSM-GSM Handover aus (Rückwärtskompatibilität) und wird entsprechend bearbeitet.

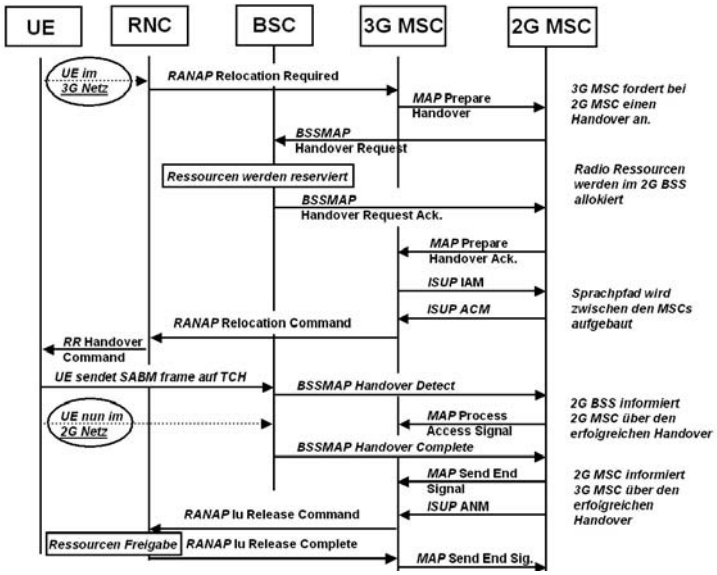

Abb. 3.35: 3G – 2G Intersystem Hard Handover Message Flow

3.7.2 Mobility Management im Idle Zustand

Im Idle Zustand verhält sich ein Endgerät passiv, d.h. es kann keine Daten senden oder empfangen. Trotzdem ist das Endgerät periodisch aktiv und führt folgende Aufgaben durch:

Überwachen des Paging Kanals

Um auf eingehende Sprachrufe, Kurznachrichten, etc. reagieren zu können, wird ständig der Paging Kanal (PCH) der aktuellen Zelle überwacht. Wird dort eine Paging Nachricht mit der eigenen IMSI oder TMSI entdeckt, nimmt das Endgerät Kontakt mit dem Netzwerk auf. Da auch das Abhören des Paging Kanals Energie benötigt, wird ein Verfahren verwendet, das die Teilnehmer anhand ihrer IMSI in unterschiedliche Gruppen einteilt (Paging Group). Paging Nachrichten für Teilnehmer einer Gruppe werden nur zu ganz bestimmten Zeiten ausgestrahlt. Somit muss das Endgerät nur zu diesen Zeiten den Paging Kanal abhören. In der restlichen Zeit kann der Empfänger abgeschaltet werden und somit Energie gespart werden. Dem gegenüber steht der kleine Nachteil, dass die Pagingprozedur etwas länger dauert.

Hat der Teilnehmer im Idle Zustand einen aktiven PDP Kontext, so kann das Netzwerk dem Endgerät ebenfalls eine Paging Nachricht senden, sobald ein IP Paket vom Netzwerk an den Nutzer gesendet wird. Ein solches IP Paket könnte z.B. durch eine Messaging Applikation geschickt werden. Auch in diesem Fall muss sich das Endgerät erst wieder beim Netzwerk melden. Danach wird wieder ein Radio Bearer aufgebaut, und das IP Paket kann zugestellt werden.

Cell Reselection

Im Idle State ist nicht das Netzwerk, sondern das Endgerät selber für den Zellwechsel zuständig. Dieser Vorgang wird nicht Handover, sondern Cell Reselection genannt.

Im Idle Zustand existiert zwischen Endgerät und Netzwerk keine physikalische oder logische Verbindung. Sollen Daten zwischen dem Endgerät und dem Netzwerk ausgetauscht werden, muss zuvor wieder eine physikalische Verbindung über die Luftschnittstelle aufgebaut werden. Für den leitungsvermittelnden Teil des UMTS Netzwerkes bedeutet der Idle State also, dass keine Sprachverbindung über die MSC aufgebaut ist. Über den SGSN kann jedoch auch im Idle Zustand ein PDP Kontext aktiv sein. In diesem Zustand können jedoch keine Daten übertragen werden. Ein Endgerät befindet sich also trotz aktivem PDP Kontext nur im Idle Zustand, wenn sehr lange keine Daten mehr übertragen wurden. Um die Datenübertragung erneut aufzuneh-

men, muss zuerst wieder eine logische und physikalische Verbindung aufgebaut werden und das Endgerät in den Cell-DCH oder Cell-FACH Zustand gesetzt werden.

Location Update mit dem MSC

Im Idle State kennt das Kernnetzwerk den genauen Aufenthaltsort eines Teilnehmers nicht. Dem MSC ist lediglich bekannt, in welcher Location Area sich ein Teilnehmer befindet. Eine Location Area besteht dabei aus einer Anzahl von Zellen. Bei einem ankommenden Anruf muss somit der Teilnehmer zuerst ausfindig gemacht werden. Dies geschieht mit einer Paging Nachricht, die über den Paging Kanal aller Zellen in einer Location Area ausgestrahlt wird. Dieses Konzept wurde ohne große Änderungen von GSM übernommen und ist in Kapitel 1.8.1 genauer beschrieben.

Routing Area Update mit dem SGSN

Aus Sicht des SGSNs wird für ein Datenpaket, das an ein Endgerät im Idle Zustand zugestellt werden soll, in ähnlicher Weise verfahren. Für den paketvermittlenden Teil des Netzwerkes sind die Zellen in Routing Areas eingeteilt. Eine Routing Area entspricht dabei einer Location Area oder einem Teilstück einer Location Area. Auch dieses Konzept wurde großteils unverändert von GPRS übernommen und ist in Kapitel 2.7.1 genauer beschrieben.

Wechselt ein Endgerät durch ein Cell Reselection die Location Area bzw. die Routing Area, muss es ein Location Update bzw. ein Routing Area Update durchführen. Dafür baut das Endgerät eine Signalisierungsverbindung mit dem Netzwerk auf und wird vom RNC in den Cell-DCH oder Cell-FACH RRC Zustand gesetzt. Danach kann der Location Area Update mit dem MSC, bzw. der Routing Area Update mit dem SGSN durchgeführt werden. Nach erfolgreichem Update kehrt das Endgerät wieder in den Idle Zustand zurück.

3.7.3 Mobility Management in anderen Zuständen

Auch in den Cell-FACH, Cell-PCH und URA-PCH Zuständen ist das Endgerät für den Zellwechsel zuständig. Der große Unterschied zum Idle Zustand ist jedoch, dass in diesen Zuständen eine logische Verbindung zwischen Endgerät und Netzwerk besteht. Sind diese Zustände im Radionetzwerk implementiert, so werden sie für Verbindungen mit geringem Datenübertragungsaufkommen verwendet. Die Vorteile dieser Zustände wurden bereits in Kapitel 3.5.4 beschrieben. Je nach Zustand ändern sich die Mobility Management Aufgaben, die vom Endgerät nach einem Zellwechsel durchgeführt werden müssen:

Cell-FACH Zustand

Im Cell-FACH Zustand kann das Endgerät mit dem Netzwerk Nutzdaten austauschen. Führt das Endgerät einen Zellwechsel durch, so muss dies sofort dem Netzwerk durch eine Cell Update Nachricht mitgeteilt werden. Alle Daten werden dann zukünftig über die neue Zelle übertragen. Befindet sich die neue Zelle im Bereich eines anderen RNCs, sendet dieser die Cell Update Nachricht über die Iur Schnittstelle an den Serving RNC (S-RNC) des Teilnehmers. Auch wenn sich die neue Zelle in einer neuen Location oder Routing Area befindet, wird kein Location Area bzw. Routing Area Update durchgeführt. Dies bedeutet, dass das Kernnetzwerk nicht informiert wird, dass sich der Teilnehmer in einer neuen Location- bzw. Routing Area befindet. Dies ist aber auch nicht notwendig, da der S-RNC die Daten über die Iur Schnittstelle an den Teilnehmer weiterleitet. Zwar tritt während des Zellwechsels eine kurze Übertragungsunterbrechung auf, diese wird jedoch durch dieses Verfahren so kurz wie möglich gehalten.

Ist die neue Serving Cell an einem neuen RNC angeschlossen, der keine Iur Schnittstelle zum bisherigen RNC hat, wird ein Cell Update fehlschlagen. Da der neue RNC den bisherigen RNC nicht über den neuen Aufenthaltsort informieren kann, setzt er das Endgerät während der Cell Update Prozedur vom Cell-FACH, Cell-PCH oder URA-PCH Zustand zurück in den Idle Zustand. Danach führt das Endgerät automatisch einen Location Update mit der MSC und dem SGSN durch.

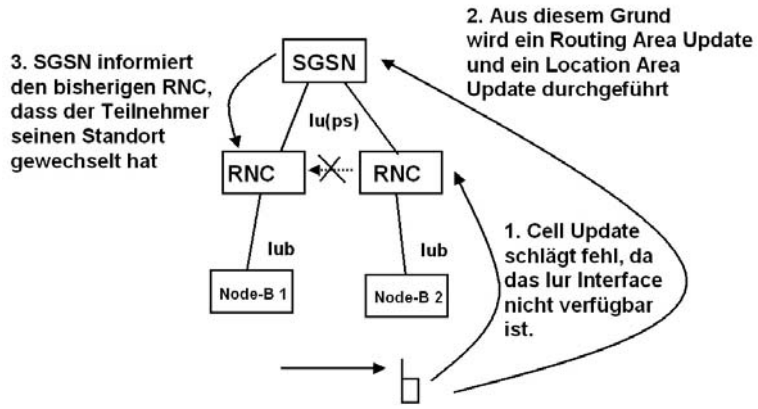

Abb. 3.36: Zellwechsel im PMM Connected Zustand in eine Zelle, über die der S-RNC nicht mehr erreichbar ist.

Da der SGSN beim Location Update erkennt, dass noch eine weitere Signalisierungsverbinung zum bisherigen RNC besteht, kann er diesen über den Wechsel des Teilnehmers zu einem neuen RNC informieren. So wird sichergestellt, dass auf dem bisherigen RNC alle Ressourcen freigegeben werden. Abbildung 3.36 zeigt einen solchen Zellwechsel.

Cell-PCH

Aus Mobility Management Sicht entspricht der Cell-PCH Zustand dem Cell-FACH Zustand. Im Cell-PCH Zustand kann das Endgerät jedoch keine Daten übertragen. Werden in diesem Zustand Daten für den Teilnehmer aus dem Kernnetzwerk zum RNC geliefert, muss dieser den Teilnehmer erst wieder in den Cell-FACH oder Cell-DCH Zustand setzen. Möchte der Teilnehmer von sich aus in diesem Zustand Daten übertragen, muss das Endgerät dies dem RNC zunächst signalisieren. Dieser setzt dann das Endgerät wieder in den Cell-DCH oder Cell-FACH Zustand, und der Datentransfer kann beginnen.

URA-PCH

Bei noch längerer Inaktivität kann das Radionetzwerk einen Teilnehmer mit aktivem PDP Kontext auch in den URA-PCH Zustand setzen. Eine Cell Update Nachricht muss in diesem Zustand nur an das Netzwerk gesendet werden, wenn der Teilnehmer in eine neue UTRAN Registration Area (URA) wechselt. Eine UTRAN Registration Area ist ein neues Konzept, das mit UMTS eingeführt wurde. Es verfeinert, wie in Abb. 3.37 gezeigt, eine Location Area, bzw. eine Routing Area.

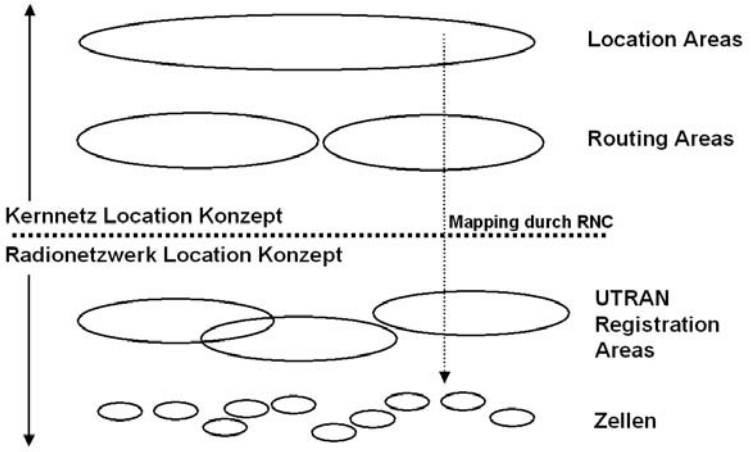

Abb. 3.37: Location Konzepte von Radio- und Kernnetz

UMTS Registration Areas sind dem Kernnetzwerk nicht bekannt. Auch die einzelnen Zellen wurden für das Kernnetzwerk in so genannte Service Areas abstrahiert. Bei GSM kannte eine MSC oder ein SGSN noch die Location Area und die genaue Cell ID jeder Zelle. Bei UMTS wurde dies nun durch die Location Area und die abstrakte Service Area ersetzt. Es ist jedoch möglich, pro Service Area nur eine Zelle zu konfigurieren. Auf diese Weise gibt es eine klare Trennung zwischen dem Location Prinzip des Kernnetzwerkes, das Location Areas, Routing Areas und Service Areas kennt und dem Location Prinzip des Radio Netzwerkes, das UTRAN Registration Areas und einzelne Zellen kennt. Kernnetz und Radionetz sind also auch hier logisch voneinander entkoppelt worden. Das Mapping zwischen dem Location Prinzip im Kernnetzwerk und dem Location Prinzip im Radionetzwerk wird im RNC durchgeführt.

3.8 UMTS CS und PS Verbindungsaufbau

Um eine leitungsvermittelte oder paketvermittelte Verbindung aufzubauen, muss das Endgerät mit dem Netzwerk Verbindung aufnehmen und seinen Verbindungswunsch mitteilen. Der Aufbau der eigentlichen Nutzdatenverbindung verläuft dann in mehreren Phasen:

Aufbau eines leitungsvermittelnden Kanals

Um aus dem Idle Mode heraus eine erste Signalisierungsverbindung zum Radionetzwerk aufzunehmen, verwendet das Endgerät, wie in Abbildung 3.37a gezeigt, die RRC Connection Setup Prozedur. Diese wurde in Kapitel 3.4.5 und Abbildung 3.17 vorgestellt. Ziel des RRC Connection Setup ist es, einen temporären Radiokanal für eine Signalisierungsverbindung zwischen Endgerät und RNC aufzubauen. Der RNC hat für die Signalisierungsverbindung die Wahl, einen Dedicated Channel zu vergeben (Cell-DCH State), oder die Signalisierung über den FACH Channel durchzuführen (Cell-FACH State).

Falls, wie in Abbildung 3.37a dargestellt, eine leitungsvermittelte Verbindung aufgebaut werden soll, schickt das Endgerät danach über die eingerichtete Signalisierungsverbindung eine CM Service Request Nachricht über den RNC an die MSC. DTAP Nachrichten werden zwischen RNC und dem MSC über das SCCP Protokoll ausgetauscht (vgl. Kapitel 1.4), das verbindungsorientiert ist. Aus diesem Grund muss zuerst eine neue logische SCCP Verbindung zwischen RNC und MSC hergestellt werden, bevor der RNC die Nachricht an das MSC weitergeben kann.

Nachdem das MSC die CM Service Request Nachricht erhalten hat, überprüft sie mit der darin enthaltenen Teilnehmer Identität (TMSI oder IMSI) zunächst die Authentizität des Teilnehmers. Dies geschieht mit einem Challenge Response Verfahren ähnlich wie bei GSM. Große Neuerung ist bei UMTS jedoch, dass sich auch das Netzwerk gegenüber dem Teilnehmer authentifiziert. Nach erfolgreicher Authentifizierung wird danach die Verschlüsselung des Radiokanals durch die Security Mode Command Nachrichten aktiviert. Optional erfolgt nun die Vergabe einer neuen temporären Identität (TMSI) an den Teilnehmer. Dies ist im Nachrichtenfluss zur besseren Übersicht jedoch nicht dargestellt.

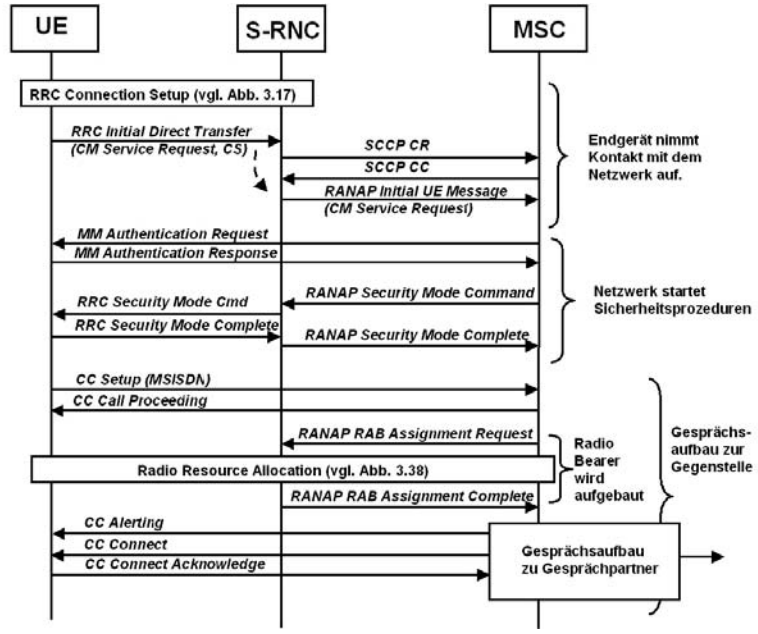

Abb. 3.37a: Mobile Originated Voice Call (MOC)

Nach erfolgreicher Authentifizierung und Aktivierung der Verschlüsselung teilt das Endgerät im nächsten Schritt die genauen Einzelheiten des Verbindungswunsches mit. In einer Call Control (CC) Setup Nachricht wird dem Netzwerk dazu unter anderem die Telefonnummer für den Verbindungswunsch mitgeteilt. Die MSC quittiert diese Nachricht dem Endgerät mit einer Call Proceeding Nachricht und startet daraufhin zwei Vorgänge:

Bisher ist zwischen Teilnehmer und Radionetzwerk nur eine Signalisierungsverbindung aufgebaut, über die keine Sprachverbindung geführt werden kann. Aus diesem Grund fordert die MSC deshalb vom RNC mit einer RAB Assignment Request Nachricht den Aufbau einer Verbindung für die Übertragung der Sprachdaten an. Der RNC baut daraufhin auf dem Iub Interface einen für eine Sprachverbindung geeigneten Kanal auf und weist den Node-B an, einen entsprechenden Radiokanal auf der Luftschnittstelle zum Teilnehmer aufzubauen. Außerdem baut der RNC auch eine Verbindung für die Sprachdaten über die Iu(cs) Schnittstelle zur MSC auf. Diese Radio Ressource Allocation Prozedur ist zur besseren Übersicht in Abbildung 3.38 separat dargestellt. Da in unserem Beispiel schon ein Dedicated Channel für die Signalisierungsverbindung zum RNC besteht, wird dieser durch die Radio Ressource Allocation Prozedur nur neu konfiguriert (Radio Link Reconfiguration). Die Neukonfigurierung umfasst dabei z.B. die Änderung des Spreading Codes, da eine leitungsvermittelte Verbindung mehr Bandbreite als die bisherige Signalisierungsverbindung benötigt. Hätte der RNC die Signalisierung zuvor über den FACH durchgeführt (Cell-FACH State), müsste an dieser Stelle ein neuer Dedicated Channel aufgebaut werden.

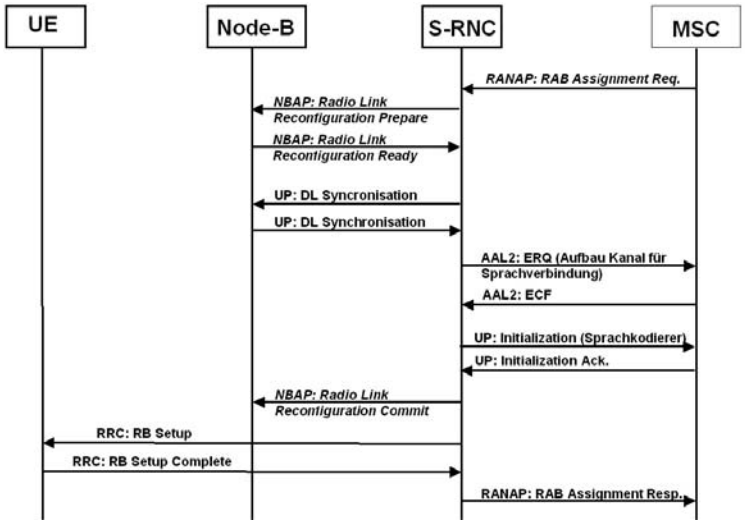

Abb. 3.38: Radio Ressource Allocation für den Sprachkanal

Gleichzeitig zum Aufbau der Ressourcen für die Sprachverbindung im Radionetzwerk versucht die MSC, die gewünschte Ver-

bindung für den Teilnehmer über das Kernnetzwerk aufzubauen. Dies geschieht über die schon bekannte ISUP Signalisierung, die in Kapitel 1.4 beschrieben ist. Konnte die Gegenstelle erreicht werden, sendet das MSC die entsprechenden Call Control Nachrichten an das Endgerät.

Aufbau eines Kanals für die Paketdatenübertragung (PDP Context Activation)

Der Aufbau einer paketvermittelten Verbindung wird auch Packet Data Protocol (PDP) Context Activation genannt. Aus Anwendersicht bedeutet die Aktivierung eines PDP Kontextes die Verbindungsaufnahme mit dem Internet und die Zuweisung einer IP Adresse. Weitere Informationen zu diesem Thema sind in Kapitel 2.8 und 2.7.2 zu finden. Auch der Aufbau einer paketvermittelten Verbindung erfolgt, wie in Abbildung 3.39 gezeigt, im ersten Schritt mit einer RRC Connection Setup Prozedur.

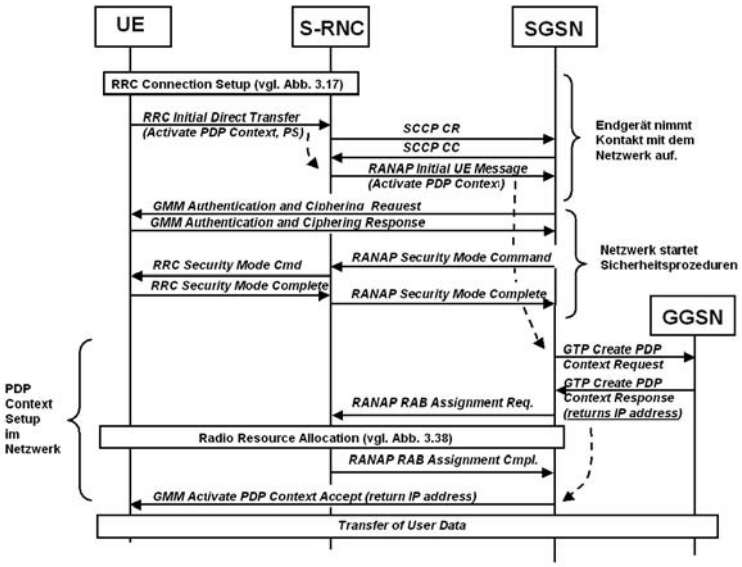

Abb. 3.39: PDP Context Activation

Nach erfolgreichem Aufbau der Signalisierungsverbindung sendet das Endgerät dann eine Activate PDP Context Request Nachricht über den RNC an den SGSN. Danach erfolgen, wie im vorigen Beispiel auch, die Authentifizierung des Teilnehmers und die Aktivierung der Verschlüsselung. Im weiteren Verlauf des Verbindunsaufbaus vergibt der GGSN eine IP Adresse für den Teilnehmer und der SGSN fordert vom RNC den Aufbau einer Verbindung für die Nutzdatenübertragung zum Teilnehmer an. Der SGSN übergibt dafür dem RNC die Quality of Service Parameter

(z.B. die gewünschte Bandbreite) für die neue Verbindung. Diese wurden am Anfang der Verbindungsaufnahme vom Endgerät in der PDP Context Activation Request Nachricht an den SGSN übermittelt, können aber vom SGSN oder GGSN für den RAB Assignment Request noch modifiziert werden. Der Aufbau des paketvermittelten Kanals erfolgt dabei in gleicher Weise wie in Abbildung 3.38 für einen leitungsvermittelten Kanal. Lediglich die Parameter der einzelnen Nachrichten enthalten Werte für andere Eigenschaften des einzurichtenden Datenkanals. Ausserdem entfallen die Nachrichten für die Einrichtung des Sprachkanals.

3.9 High Speed Downlink Packet Access

Wie schon in Kapitel 3.1.4 im Überblick dargestellt, wird die UMTS Spezifikation ständig den neuen Möglichkeiten der Technik und den Anforderungen des Marktes angepasst. Mit HSDPA in Release 5 der 3GPP Spezifikation wurde der UMTS Standard um einen wichtigen Baustein erweitert. Dieser ermöglicht im Downlink im Vergleich zu einem Release 99 UMTS Netzwerk wesentlich höhere Datenraten pro Zelle und User. Mit Datenraten zwischen 500 kbit/s und 3.6 Mbit/s pro Nutzer ermöglicht es HSDPA den UMTS Netzbetreibern, in direkte Konkurrenz zu DSL und anderen Internetzugangstechnologien zu treten.

Wichtige Dokumente im Standard zu HSDPA sind die Overall Description Stage 2 in 3GPP TS 25.308, die Physical Layer Description in TS 25.858, Physical Layer Procedures in TS 25.214, HSDPA auf dem Iub und Iur Interface in TS 25.877, RRC Erweiterungen in TS 25.331 und Beispiele zu Signaling Procedures in TS 25.931.

3.9.1 HSDPA Kanäle

Kombination von Dedicated und Shared Channels

Wie in Abbildung 3.40 und 3.41 gezeigt wird, kombiniert HSDPA die Konzepte von Dedicated und Shared Channels. Für die Übertragung der Nutzdaten im Downlink werden ein oder mehrere High Speed Physical Downlink Shared Channels (HS-PDSCH) verwendet, die sich mehrere Nutzer teilen. Somit ist es möglich, Daten gleichzeitig an unterschiedliche Teilnehmer zu senden oder durch Bündelung mehrerer HS-PDSCH, die jeweils einen anderen Code verwenden, die Übertragungsrate für einen einzelnen Teilnehmer zu erhöhen.

Jeder HS-PDSCH verwendet einen Spreizfaktor von 16, womit theoretisch bis zu 15 gleichzeitige HS-DSCH Kanäle in einer Zelle konfiguriert sein können. In der Praxis werden jedoch meist nur

5-10 HS-PDSCH pro Zelle verwendet werden, da die Zelle neben HSDPA auch noch andere Dienste wie Telefonie und Paketdatenübertragung für Release 99 Endgeräte anbietet. Außerdem ist es für Dienste wie z.B. Videostreaming weiterhin von Vorteil, einen Release 99 Dedicated Channel zu verwenden, da hier dem Teilnehmer die Bandbreite während der gesamten Verbindung garantiert werden kann. Dies ist bei HSDPA nicht so einfach möglich, da hier je nach Anzahl der Teilnehmer pro Zelle und aktueller Signalqualität die Übertragungsrate sehr dynamisch ist. HSDPA opfert somit das Konzept des dedizierten Kanals mit garantierter Bandbreite für eine wesentlich schnellere Datenübertragung, bei der jedoch eine konstante Bandbreite nicht garantiert werden kann. Für viele Applikationen wie z.B. dem Websurfen oder der Übertragung von großen Dateien oder eMails mit Anhängen ist dies jedoch sehr vorteilhaft.

High Speed Shared Control Channel (HS-SCCH)

Die Zuteilung der Timeslots auf den HS-DSCH Kanälen an einzelne Benutzer erfolgt über mehrere gleichzeitig ausgestrahlte High Speed Shared Control Channels (HS-SCCH) mit einem SF=128. Ein Endgerät muss in der Lage sein, mindestens vier dieser Kanäle gleichzeitig empfangen und dekodieren zu können. Auf diese Weise ist es möglich, viele Teilnehmer gleichzeitig zu informieren, auf welchen HS-PDSCH Kanälen im nächsten Timeslot Daten für sie übertragen werden.

Neben den Shared Channels werden während einer HSDPA Verbindung auch noch eine Anzahl Dedicated Channels pro Teilnehmer verwendet:

- Ein Dedicated Physical Control Channel (DPCCH) im Uplink mit SF=256 für HSDPA Kontrollinformationen wie Acknowledgements bzw. Neuanforderung von nicht korrekt empfangenen Datenpaketen sowie die Übertragung der zuletzt ermittelten Signalqualität. Dieser Kanal wird nicht im Zeit- oder IQ-Multiplex mit den anderen Kanälen übertragen, sondern mit einem eigenen Channelization Code.
- Ein Dedicated Control Channel (DCCH) für RRC Nachrichten im Up- und Downlink zwischen RNC und Endgerät, die z.B. für Aufgaben wie das Mobility Management, sprich für Zellwechsel benötigt werden.
- Ein Dedicated Traffic Channel (DTCH) für IP Nutzdatenpakete im Uplink, da HSDPA nur einen Shared Channel für den Downlink vorsieht. Dieser hat eine Bandbreite von 64 – 384 kbit/s.

- Optional ein zusätzlicher Dedicated Traffic Channel (DTCH) in Up- und Downlinkrichtung, falls während der HSDPA Verbindung auch telefoniert wird.

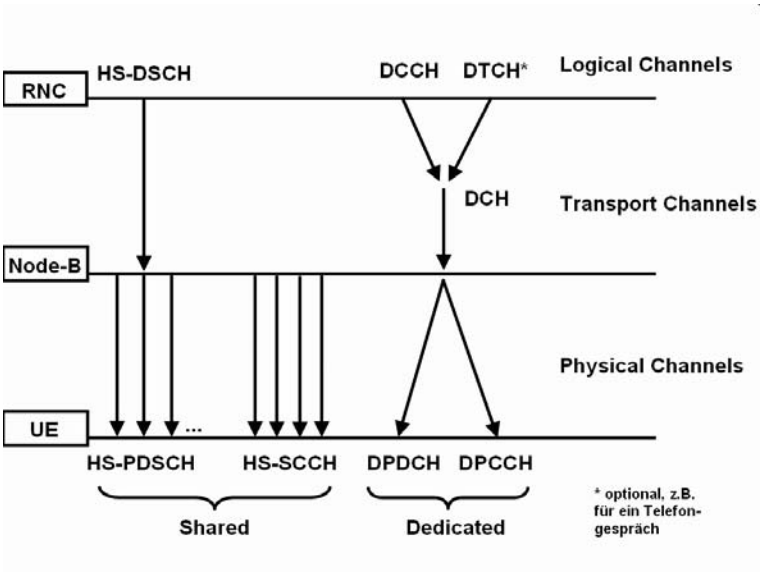

Abb. 3.40: Vereinfachte HSDPA Kanaldarstellung im Downlink

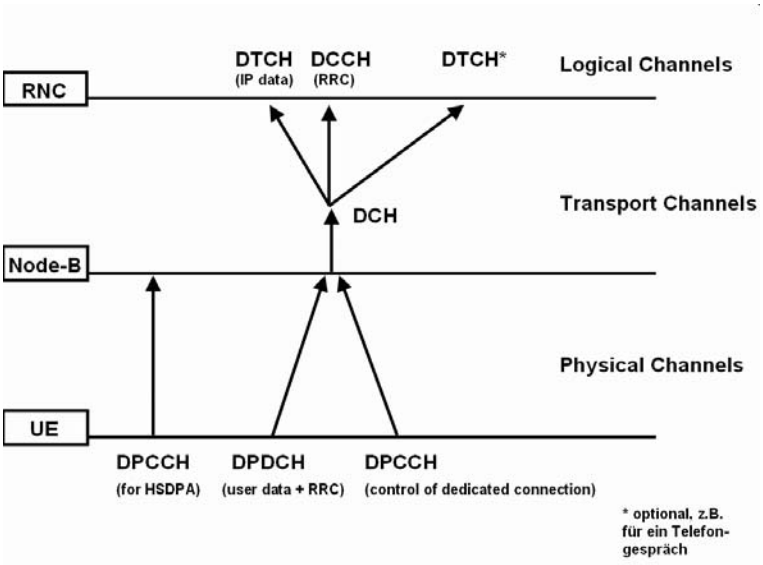

Abb. 3.41: Vereinfachte HSDPA Kanaldarstellung im Uplink

3.9.2 Kleinere Delay- Zeiten und Hybrid ARQ (HARQ)

Neben schnelleren Geschwindigkeiten ist ein weiteres Ziel von HSDPA eine Reduzierung der Round Trip Delay (RTD) Zeit sowohl für den stationären, als auch für den mobilen Betrieb. Mit Release 99 Dedicated Channels beträgt die RTD Zeit etwa 160 – 200 ms, mit HSDPA etwa 70 ms. Dies ist z.B. bei Applikationen wie dem Webbrowsing von großer Bedeutung, da beim Laden einer Web Seite neben einer DNS-Abfrage zur Auflösung des Webseitennamens auch noch mehrere TCP Verbindungen geöffnet werden und sich die Round Trip Delay Zeit somit mehrfach auf die Zeit auswirkt, bis erste Teile der Seite angezeigt werden können. Um dies zu erreichen, wurde die Blockgröße auf 2 ms reduziert. Bei den Release 99 Dedicated Channels beträgt die Blockgröße hingegen mindestens 10 ms.

HARQ

Aufgrund der sich ständig ändernden Übertragungsbedingungen im mobilen Betrieb z.B. im Auto, im Zug oder auch während des Gehens, lassen sich Übertragungsfehler nicht immer vermeiden. In der Praxis tritt zwar kein Paketverlust auf, da falsche oder verlorene Pakete vom Radionetzwerk erneut übertragen werden, der Delay der erneut übertragenen Pakete ist jedoch größer. Höhere Protokolle wie z.B. TCP reagieren jedoch sehr empfindlich auf plötzlich schwankende Delay Zeiten und deuten dies irrtümlich als Übertragungsfehler. Um diesen Effekt zu minimieren, wird neben der Fehlerkorrektur und Neuübertragung auf dem RLC Layer mit HSDPA auch noch eine Fehlerkorrektur auf der MAC Ebene eingeführt. Dieser Mechanismus ist direkt im Node-B implementiert und wird Hybrid ARQ (HARQ) genannt. Zusammen mit einer Blockgröße von 2 ms statt wie bisher mindestens 10 ms für einen Dedicated Channel kann ein als fehlerhaft gemeldeter MAC Datenblock vom Node-B innerhalb von 10 ms erneut übertragen werden. Dies ist ein großer Vorschritt gegenüber Release 99 Dedicated Channels. Hier findet nur eine Fehlerkorrektur auf dem RLC Layer statt, die mindestens 80-100 ms für die Erkennung und erneute Übertragung eines fehlerhaften Frames benötigt.

Gegenüber anderen Fehlererkennungs- und Korrekturverfahren wird wie z.B. bei TCP wird bei HARQ kein Fensterverfahren verwendet, sondern es erfolgt eine gezielte Rückmeldung für jeden Frame. Dieses Verfahren wird Stop and Wait (SAW) genannt. Abbildung 3.42 zeigt, wie ein Datenframe im Downlink übertragen, fehlerhaft empfangen und daraufhin neu übertragen wird. Vor der eigentlichen Übertragung des Frames kündigt das

Netzwerk dem Benutzer über den Shared Control Channel die Übertragung an. Jeder HS-SCCH Frame enthält dazu folgende Informationen:

- ID des Endgeräts, für den in einem oder mehreren HS-PDSCH Kanälen im nächsten Frame Daten übertragen werden.
- Die Channelization Codes der HS-PDSCH Kanäle, die dem Endgerät im nächsten Frame zugeordnet sind
- Kodierungsinformation in Form von Transport Format und Ressource Indicator
- Modulationsart (QPSK or 16QAM)
- HARQ Prozessnummer (s.u.)
- ob es sich um eine erneute Übertragung handelt (Retransmit) und welche Redundancy Version (RV) verwendet wird (s.u.)

Jeder Frame ist dazu in drei Slots unterteilt. Bereits nach der Übermittlung von zwei der drei Slots des Frames hat das Endgerät alle nötigen Informationen, die zum Empfang des Nutzdatenframes notwendig sind. Deshalb wartet das Netzwerk das Ende des Control Frames gar nicht ab, sondern sendet die Nutzdaten sofort. Das bedeutet, dass der Shared Control Channel und der Downlink Shared Channel um einen Slot versetzt übertragen werden. Nach Empfang des Datenframes hat das Endgerät genau 5 ms Zeit, den Frame zu dekodieren und zu überprüfen, ob die Übertragung korrekt war. Falls das Paket korrekt übertragen wurde wird daraufhin auf dem Dedicated Physical Control Channel (DPCCH) im Uplink eine Bestätigung (Acknowledgement) geschickt, im Fehlerfall ein NACK (Not Acknowledge). Um auch hier Zeit zu sparen, wird der Control Channel im Uplink wiederrum leicht versetzt zum Downlink Shared Channel gesendet. Dies ermöglicht es dem Netzwerk, beim Empfang eines NACK den fehlerhaften Frame sofort erneut zu übertragen.

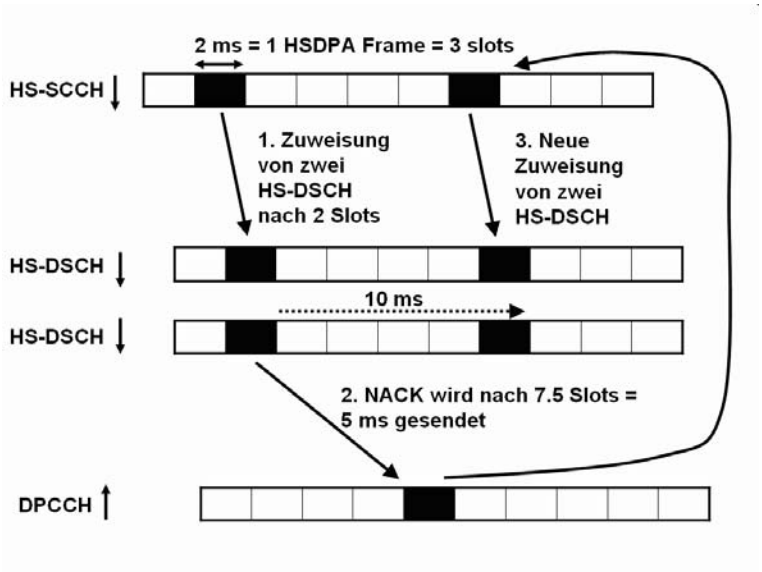

Abb 3.42: Erkennung und erneute Übertragung eines fehlerhaften Frames innerhalb von 10 ms

Bis zu 8 gleichzeitige HARQ Prozesse

Da mit HARQ nur nach einer positiven Bestätigung der nächste Frame des Datenstroms übertragen werden kann, muss ein Endgerät in der Lage sein, bis zu acht gleichzeitige HARQ Prozesse zu kontrollieren. Auf diese Weise wird gewährleistet, dass der Datenfluss auf der MAC Ebene nicht ins Stocken gerät, wenn ein Frame falsch übertragen wurde. Für höhere Ebenen kann der Datenstrom jedoch erst dann weitergegeben werden, wenn das fehlerhafte Paket bei der nächsten Übertragung korrekt empfangen wurde, da höhere Schichten die Daten in der richtigen Reihenfolge benötigen.

Incremental Redundancy

Für das Netzwerk gibt es zwei unterschiedliche Möglichkeiten, ein Paket erneut zu übertragen: Beim Incremental Redundancy Verfahren nutzt das Netzwerk die Tatsache, das ein Teil der Fehlererkennung und Fehlerkorrekturbits vor der Übertragung wieder entfernt werden. Dieses so genannte Puncturing wird auch bei UMTS, GPRS und EDGE verwendet, um den Datenstrom der Bandbreite des Übertragungskanals anzupassen. Weitere Informationen zum Thema Puncturing finden sich z.B. in Kapitel 2.2.3 zum Puncturing bei GPRS. Bei einer erneuten Übertragung eines Frames werden statt des ursprünglichen Datenstroms ein Datenstrom mit Fehlererkennungs- und Korrekturbits gesendet, die bei

der Übertragung zuvor punktiert wurden. Man spricht hier auch von einer anderen Redundany Version des Frames. Durch Kombination der beiden Pakete wird somit erreicht, dass der Datenstrom eine höhere Redundanz aufweist, womit sich die Chance auf eine korrekte Dekodierung erhöht. Sollte der Frame auch dann noch nicht richtig dekodiert werden können, kann der Frame in weiteren Redundancy Version geschickt werden und die Dekodierungschancen weiter zu erhöhen.

Chase Combining

Mit dem zweiten Verfahren, dem Chase Combining, wird hingegen der Frame mit der gleichen Redundancy Version wie zuvor übertragen. Statt auf der MAC Ebene wird mit diesem Verfahren die Signalenergie der zwei übertragenen Frames auf der physikalischen Ebene addiert und dann eine weitere Dekodierung versucht. Ob Incremental Redundancy oder Chase Combining verwendet wird, wird vom Netzwerk bestimmt, hängt aber auch von den Fähigkeiten des Endgerätes ab.

3.9.3 Scheduling im Node-B

Die HS-DSCH Channels stehen einem User meist nicht exklusiv zur Verfügung stehen, sondern werden vom Netzwerk für mehrere Benutzer gleichzeitig verwendet. Das Netzwerk bestimmt dann für jeden Frame, welchem Benutzer dieser zugeteilt werden soll und teilt diese Entscheidung den Endgeräten dann über die HS-SCCH Kanäle mit. Diese Aufgabe wird als Scheduling bezeichnet. Um schnell auf sich ändernde Übertragungsbedingungen einzelner Teilnehmer reagieren zu können, wurde das Scheduling für die HS-DSCHs nicht wie bisher üblich im RNC implementiert, sondern direkt im Node-B. Dies ist auch in Abbildung 3.40 zu sehen, da die High Speed Shared Control Channels (HS-SCCH) direkt vom Node-B ausgehen. Für HSDPA werden also dem Node-B eine weitere Aufgabe übertragen, die für Dedicated Channels bisher und weiterhin vom RNC erledigt werden. Auf diese Weise ist es möglich, dass der Scheduler z.B. bei sich temporär verschlechternden Übertragungsbedingungen (Fading) eines Nutzers sofort reagieren kann. Statt Pakete zu senden, die während des Fadings mit hoher Wahrscheinlichkeit nicht korrekt empfangen werden können, kann der Scheduler mehr Frames anderen Endgeräten zuteilen. Auf diese Weise kann der Gesamtdurchsatz der Zelle gesteigert werden, da weniger Frames für das erneute Senden von nicht korrekt empfangenen Daten verwendet werden müssen. Neben der Signalqualität pro User bestimmen auch andere Faktoren wie z.B. die Priorität eines Users über

die Zuteilung von Ressourcen. Da es wiederum wie bei vielen anderen Funktionalitäten den Netzwerkherstellern überlassen bleibt, welche Faktoren, deren Gewichtung usw. der Scheduler für seine Entscheidung verwendet, können gute Implementierungen zu einem Wettbewerbsvorteil führen.

Da der RNC keinen direkten Einfluss mehr auf die Ressourcezuteilung pro Teilnehmer hat, kann dieser auch nicht mehr wissen, wie schnell die Daten tatsächlich übertragen werden können. Deshalb gibt es für HSDPA zwischen RNC und den Node-Bs einen Flow Control Mechanismus. Dazu wird im Node-B für jede Prioritätsstufe ein Datenpuffer angelegt, aus denen dann der Scheduler die zu übertragenen Daten ausliest und über die Luftschnittstelle versendet. Wie viel Platz in den einzelnen Puffern noch für weitere Daten vorhanden ist, kann der RNC über eine Capacity Request Nachricht ermitteln, die vom Node-B mit einer Capacity Allocation Nachricht beantwortet wird. Ein Node-B verwaltet somit nicht für jeden Teilnehmer einen Datenpuffer, sondern nur pro Prioritätsstufe.

3.9.4 Adaptive Modulation, Codierung und Geschwindigkeit

16QAM

Um bei guten Übertragungsbedingungen eine möglichst große Übertragungsgeschwindigkeit zu erreichen, wird bei HSDPA ein neues Modulationsverfahren verwendet. Dadurch ist es möglich, 4 Bits pro Übertragungsschritt zu übertragen. Da in 4 Bits 16 Werte kodiert werden können (2^4) wird diese Modulation 16QAM genannt. Im besten Fall kann somit die Gesamtkapazität einer Zelle bei einer Beibehaltung der bisherigen Kanalbandbreite von 5 MHz verdoppelt werden. Bei mittleren bis schlechten Übertragungsbedingungen wird jedoch auf die schon von UTMS Release 99 bekannte QPSK Modulation umgeschaltet, die zwei Bits pro Übertragungsschritt kodieren kann.

Channel Quality Index

Neben dem Umschalten zwischen unterschiedlichen Modulationsarten kann das Netzwerk auch den Coding Scheme jedes Frames und die Anzahl der gleichzeitig genutzten HS-DSCH Kanäle für den Benutzer an den zuletzt vom Endgerät gemeldeten Channel Quality Index (CQI) anpassen. Der CQI kann Werte von 1 (sehr schlecht) bis 31 (sehr gut) annehmen und teilt dem Netzwerk mit, wie viele Redundanzbits benötigt werden, um die Block Error Rate (BLER) unter 10% zu halten. In der Praxis bedeutet dies also, dass bei schlechter werdenden Bedingungen mehr Bits pro Frame für die Fehlererkennung und Fehlerkorrektur verwendet werden. Die Übertragungsgeschwindigkeit sinkt

dadurch zwar, auf diese Weise kann jedoch eine stabile Datenübertragung aufrechterhalten werden. Da Modulation und Codierung eines Frames pro Teilnehmer individuell geregelt wird, hat eine schlechte Empfangssituation eines Teilnehmers keine Auswirkungen auf die Übertragungsgeschwindigkeit für einen anderen Teilnehmer, dessen Daten das Netzwerk auf dem gleichen HS-DSCH sendet.

Adaptive Modulation and Coding Schemes

Durch Anpassung der Modulation und des Coding Schemes kann die Sendleistung, die in der Zelle für die HSDPA Kanäle reserviert ist, konstant gehalten werden. Die Strategie von HSDPA, mit konstanter Sendeleistung, z.B. 40% der gesamten Sendeleistung einer Zelle und variablen Teilnehmergeschwindigkeiten unterscheidet sich somit deutlich von der Strategie der Release 99 Dedicated Channel. Bei diesen wird durch schnelle Regelung der Sendeleistung eine bestimmte Bandbreite für den Teilnehmer gewährleistet. Erst wenn die Leistung nicht weiter erhöht werden kann, bzw. wenn der Nutzer über längere Zeit die angebotene Bandbreite nicht nutzt, kann der Spreizfaktor der Verbindung erhöht und somit die maximal mögliche Geschwindigkeit reduziert werden.

Auch die Fähigkeiten des Endgerätes haben einen Einfluss auf die maximale Datenrate. Der Standard definiert dazu eine Anzahl unterschiedlicher Geräteklassen, die in 3GPP TS 25.306 aufgelistet werden. Nachfolgende Tabelle zeigt einige Beispielkategorien und deren Eigenschaften:

HS-DSCH Category	Max. Anzahl gleichzeitiger HS-PDSCH	Minimum TTI Interval	Maximum Anzahl an Transport Block Bits per TTI
6	5	1	7298 (mit 16QAM)
11	5	2	3630 (nur QPSK)
12	5	1	3630 (nur QPSK)

Mit einem Category 6 Endgerät, das neben QPSK auch 16QAM unterstützt ist folgende maximale Übertragungsgeschwindigkeit möglich: 7298 Bits pro TTI (die verteilt über 5 HS-PDSCH Kanäle übertragen werden) alle 2 ms = (1/0.002)*7298 = 3.6 MBit/s. Das entspricht einer Geschwindigkeit von 720 kbit/s pro Kanal bei einem Spreizfaktor von 16. Verglichen mit einem Release 99

384 kbit/s Dedicateded Channel mit Spreizfaktor von 8, ergibt sich wegen des unterschiedlichen Spreizfaktors und Modulation eine Geschwindigkeitssteigerung um den Faktor 4. Während die Modulation wie am Anfang dieses Unterkapitels beschrieben die Übertragungsgeschwindigkeit um den Faktor 2 steigert, sorgt die geringere Anzahl von Fehlerkorrekturbits bei guten Übertragungsbedingungen für eine weitere Beschleunigung um den Faktor zwei. Eine HSDPA Zelle kann somit theoretisch den vierfachen Durchsatz gegenüber einer Release 99 Zelle erreichen. In der Praxis kann dieser Wert jedoch nicht erreicht werden, da sich nicht alle Endgeräte in unmittelbarer Nähe zu einer Zelle befinden werden und somit QPSK und mehr Fehlerkorrekturbits verwendet werden müssen.

Mit einem Category 11 Endgerät hingegen, dass nur QPSK beherrscht und nur in jedem zweiten Frame Daten empfangen kann ist die maximale Geschwindigkeit auf 3630 Bits alle 4 ms = (1/0.004)*3630 = 900 kBit/s.

Es sind auch Endgeräte vorstellbar, die mehr als 5 HS-DSCH Kanäle gleichzeitig empfangen können und theoretisch eine maximale Empfangsgeschwindigkeit bis zu 14.4 MBit/s erreichen können. Dies würde jedoch alle Ressourcen der Zelle benötigen und natürlich optimale Empfangsbedingungen voraussetzen.

Somit zeigt sich, dass viele Faktoren einen Einfluss darauf haben, wie schnell Daten zu einem Endgerät übertragen werden können. Hier nochmals eine Auflistung der wesentlichen Faktoren:

- Empfangsbedinungen
- Anzahl der gleichzeitigen HSDPA Nutzer in der Zelle
- Anzahl der Nutzer von Dedicated Channels für Sprach- und Videotelefonie.
- Anzahl der Nutzer in der Zelle, die einen Dedicated Channel für die Datenübertragung nutzen.
- Endgerätekategorie
- Bandbreite der Anbindung der Zelle an das Netzwerk
- Interferenz der Nachbarzellen
- Erreichbarer Durchsatz in anderen Teilen des Netzwerkes, da bei solch hohen Geschwindigkeiten nicht immer gewährleistet ist, dass z.B. ein Web Server Daten schnell genug liefern kann um die maximale Geschwindigkeit auch auszunutzen.

An dieser Stelle sei noch kurz erwähnt, dass die mit HSDPA möglichen Geschwindigkeiten auch Auswirkungen auf andere Teile des Endgeräts haben. Neben einer höheren Prozessorleistung ergeben sich auch neue Anforderungen an das Interface zwischen Terminal und Endgerät wie z.B. einem Notebook. Die maximale Übertragungsrate von etwa 700 kbit/s der ersten Version von Bluetooth (siehe Kapitel 5), reichen für HSDPA nicht mehr aus. Somit sollten HSDPA Endgeräte auch die Bluetooth Enhanced Data Rates unterstützen, um nicht die drahtlose Verbindung zwischen Endgerät und Notebook zum Nadelöhr werden zu lassen.

3.9.5 Auf- und Abbau einer HSDPA Verbindung

Um eine HSDPA Verbindung zwischen Netzwerk und Endgerät aufzubauen, muss bereits eine dedizierte Verbindung (DCH) vorhanden sein. Dies ist notwendig, da wie in Kapitel 3.9.1 gezeigt, neben dem High Speed Shared Channel auch noch Dedicated Channels für die Verbindung benötigt werden. Erkennt das Netzwerk beim Aufbau der dedizierten Verbindung, dass das Endgerät auch HSDPA unterstützt, können im nächsten Schritt dann die notwendigen Ressourcen aufgebaut werden. Abbildung 3.43 zeigt diesen Ablauf.

Für den Aufbau der HSDPA Verbindung informiert der S-RNC zunächst den Node-B, damit dieser die HS-PDSCH Kanäle entsprechend konfigurieren kann. Im nächsten Schritt werden dann die nötigen Ressourcen für die Datenübertragung zwischen RNC und Node-B allokiert. Ist auch dies erledigt, ist das Netzwerk für die Datenübertragung bereit und kann das Endgerät über eine RRC Radio Bearer Reconfiguration Nachricht dazu auffordern, ab sofort auch Daten über den HS-DSCH zu empfangen und die dazu benötigten Dedicated Channels einzurichten, bzw. zu modifizieren. Sobald der SGSN nun Datenpakete für den Nutzer zum RNC weiterleitet, tauschen RNC und Node-B wie in Kapitel 3.9.3 beschreiben, Flow Control Informationen aus. Damit wird verhindert, dass der Datenpuffer im Node-B überläuft, denn der RNC kann nicht wissen, wie schnell die Daten über die Luftschnittstelle weitergegeben werden können. Nachdem der RNC weis, wie viel Platz aktuell noch im Puffer des Node-B vorhanden ist, beginnt dieser die Userdaten an den Node-B weiterzugeben. Danach ist es die Aufgabe des HSDPA Schedulers auf dem Node-B, Ressourcen auf dem Air Interface für den Teilneh-

mer einzuplanen und dies dem Endgerät über den Shared Control Channel mitzuteilen.

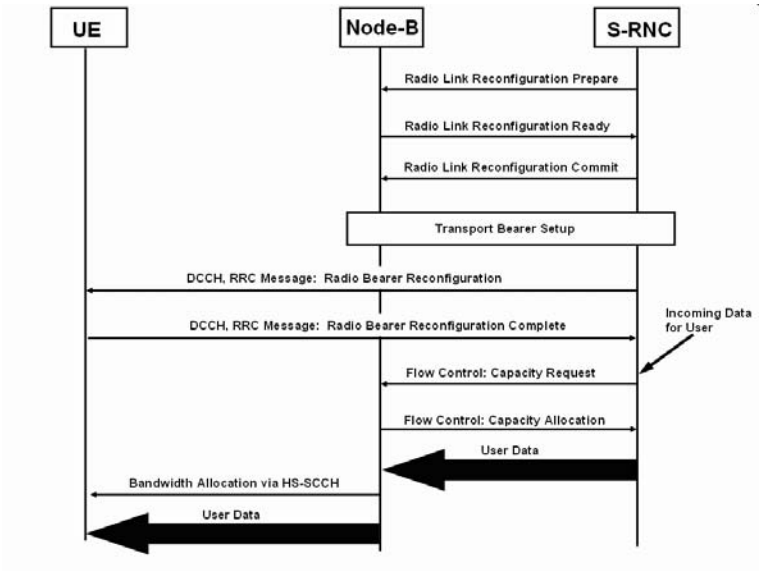

Abb. 3.43: Aufbau einer HSDPA Verbindung zu einem Endgerät

Fallback in den Cell-FACH State bei Inaktivität

Während sich das Endgerät im HSDPA Empfangsmodus befindet, muss es ständig die zugeteilten HS-SCCH Kanäle abhören und auch die notwendigen Dedicated Channels aufrechterhalten. Dies geht natürlich mit einem höheren Stromverbrauch einher, der nicht sehr ins Gewicht fällt, solange Daten übertragen werden. Werden jedoch für längere Zeit keine Daten übertragen, ist dieser Zustand natürlich sehr ungünstig, da das Terminal weiter einen erhöhten Stromverbrauch hat und somit die Laufzeit eines Batterie betriebenen Geräts verkürzt wird. Auch für das Netzwerk ist dieser Zustand ungünstig, da auch auf dieser Seite Ressourcen in Form von Rechenkapazität für die Aufrechterhaltung der Verbindung benötigt werden. Aus diesem Grund kann sich das Netzwerk entscheiden, die HSDPA Verbindung nach einiger Zeit der Inaktivität zu beenden und den Teilnehmer z.B. in den Cell-FACH State zu setzten (vgl. hierzu auch Kapitel 3.5.4). In diesem Zustand kann das Endgerät weiterhin mit einer sehr begrenzten Bandbreite Nutzdaten senden und empfangen, ohne dass dazu Dedicated Channel nötig wäre. Bei Bedarf kann auch aus diesem Zustand heraus schnell wieder eine neue HSDPA Verbindung aufgebaut werden.

3.9.6 HSDPA Mobility Management

Auch bei HSDPA ist es wichtig, die Verbindung aufrechtzuerhalten, während sich der User bewegt. Dazu unterhält das Endgerät wie schon in Kapitel 3.7.1 für den Soft Handover beschrieben, ein so genanntes Active Set für die Dedicated Channels der HSDPA Verbindung. Im Unterschied zu den Dedicated Channels und dem Soft Handover empfängt das Endgerät seine Daten auf den HS-PDSCH Kanälen jedoch nur über einen einzelnen Node-B. Basierend auf Vorgaben des Netzwerkes meldet dann das Terminal, wenn eine Zelle des Active bzw. Candidate Sets einen besseren Empfang gewährleisten würde. Der RNC kann daraufhin entscheiden, das Endgerät über diese Zelle zu versorgen. Bei HSDPA wird deshalb auch nicht von einem Handover gesprochen, sondern von einem Cell Change.

Im Vergleich zum Cell Update Verfahren von GPRS/EDGE wird der Cell Change Vorgang bei HSDPA vom Netzwerk gesteuert und nicht vom Endgerät. Da das Endgerät auch schon mit der neuen Zelle synchronisiert ist, führt der Zellwechsel nur zu einer sehr kurzen Unterbrechung der Datenübertragung auf den HS-PDSCH.

Je nachdem in welchem Verhältnis alte und neue Zelle zueinander stehen, gibt es mehrere Arten von Cell Changes:

- Intra Node-B Cell Change: Alte und neue Zelle sind Teil des gleichen Node-Bs. Dies ist die einfachste Variante, da der gleiche Node-B auch für die alte und neue Verbindung zuständig ist und somit die Datenpakete des Users, die ggf. noch im Puffer des Node-B sind, einfach über die neue Zelle geschickt werden können
- Inter Node-B Cell Change: Alte und neue Zelle gehören zu unterschiedlichen Node-Bs. Hier muss der RNC einen neuen Node-B anweisen, Ressourcen für die Übertragung von Nutzdaten über HSDPA bereitzustellen. Dies funktioniert im Netzwerk ähnlich wie ein komplett neuer Aufbau einer HSDPA Verbindung, der in Abbildung 3.43 gezeigt wurde. Nutzdaten, die noch für den Teilnehmer im Puffer des alten Node-B gespeichert sind gehen verloren und müssen von höheren Schichten neu übertragen werden.
- Cell Change mit Iur Interface: Befinden sich die alte und neue Zelle unter der Kontrolle von unterschiedlichen

RNCs, muss die HSDPA Verbindung über das Iur Interface aufgebaut werden.

- Cell Change ohne Iur Interface: Befinden sich alte und neue Zelle unter der Kontrolle von unterschiedlichen RNCs, die jedoch nicht über das Iur Interface verbunden sind, muss ein SRNS Relocation durchgeführt werden, an dem auch das Core Netzwerk (SGSN und ggf. MSC) beteiligt sind.
- Alte und neue Zelle senden auf unterschiedlichen Frequenzen (Inter Frequency Cell Change). Hier ist zusätzlicher Aufwand nötig, um Zellen auf anderen Frequenzen zu finden und dann in diese zu wechseln.
- Neue Zelle unterstützt kein HSDPA: Für diesen Fall kann des Netzwerk in der neuen Zelle einen dedicated Channel allokieren und dem Endgerät zuteilen. Dieser bietet zwar nicht die gleiche Geschwindigkeit wie HSDPA, die Verbindung bricht jedoch nicht ab.
- Inter-RAT Cell Change: Falls der Teilnehmer sich aus dem Versorgungsbereich des UMTS Netzwerkes hinausbewegt, ist auch ein Handover von UMTS/HSDPA zu GSM spezifiziert. Dazu gibt es einen HSDPA Compressed Mode, der es ähnlich dem Compressed Mode für Dedicated Channels erlaubt, nach GSM Zellen zu suchen, während noch eine Verbindung zum UMTS Netzwerk beseht.

Bei allen Varianten ist es natürlich möglich, dass parallel zur Datenverbindung auch noch eine Sprach- oder Videotelefonieverbindung aufgebaut ist. Dies erschwert den Cell Change / Handover natürlich noch zusätzlich, da diese Verbindung natürlich simultan zur Datenverbindung aufrechterhalten, bzw. in die neue Zelle übergeben werden muss.

3.10 UMTS Release 6: High Speed Uplink Packet Access (HSUPA)

Durch das Aufkommen von Peer-to-Peer Anwendungen wie Multimediatelefonie mit Videoübertragungen, Upload von großen Dateien, Podcasts und Bildern ist zu erwarten, dass der Bedarf an Uplink-Kapazität im Netzwerk wachsen wird. Auch für andere Anwendungen wie eMails mit großen Dateianhängen und MMS mit großen Bilddateien ist eine höhere Uplinkgeschwindigkeit

von großem Nutzen. Seit der Einführung von UMTS Release 99 wurde jedoch hauptsächlich an einer Geschwindigkeitssteigerung im Downlink gearbeitet. Somit sind bis einschließlich UTMS Release 5 nur Datenraten bis 128 kbit/s im Uplink möglich, in manchen Netzwerken auch bis zu 384 kbit/s.

HSDPA+HSUPA = HSPA

Mit Release 6 wurde dann ein neues Verfahren für eine Erhöhung der Uploadbandbreite ausgearbeitet, das High Speed Uplink Packet Access (HSUPA) genannt wird. Für die Kombination aus HSDPA und HSUPA wird auch die Abkürzung HSPA (High Speed Packet Access) verwendet. HSUPA erhöht die mögliche Uplink Datentransfergeschwindigkeit auf theoretische 5.8 MBit/s. Unter realistischen Umgebungsbedingungen, mehreren simultanen Nutzern, und unter Berücksichtigung der Leistungsfähigkeit des Endgeräts können in der Praxis aber immer noch Geschwindigkeiten von 800 kbit/s und mehr erreicht werden.

Auch aus Netzwerksicht hat HSUPA eine Reihe von Vorteilen. Für HSDPA (vgl. Kapitel 3.9) wird für jedes aktive Endgerät ein Dedicated Channel (DCH) im Uplink benötigt, um TCP Acknowledgements und andere Nutzdaten zu übertragen. HSUPA führt dieses Konzept durch Weiterentwicklung des Dedicated Channel Konzepts im Uplink zum Enhanced Dedicated Channel (E-DCH) fort. Dieser enthält eine Reihe von Verbesserungen, um die Nachteile eines dedizierten Kanals, wie nachfolgend beschrieben, für burstartige Übertragungen zu reduzieren. Um die Geschwindigkeit sowohl im Uplink, als auch im Downlink zu erhöhen, werden HSUPA und HSDPA üblicherweise gemeinsam verwendet.

Vergleich zwischen DCH und E-DCH

Während ein Release 99 Dedicated Channel (DCH) eine konstante Bandbreite und konstante Verzögerungszeit für Datenpakte garantiert, tauscht der E-DCH diese Vorteile gegen höhere Datenraten ein. Für viele Anwendungen ist dies akzeptabel und erhöht die Anzahl an Nutzern, die gleichzeitig mit hohen Geschwindigkeiten Daten übertragen können. Dies ist möglich, da das Netzwerk das Rauschen in einer sehr viel effizienteren Weise durch dynamische Bandbreitenregelung individueller Teilnehmer kontrollieren kann, als dies bisher mit einem DCH und fester Bandbreitenzuweisung möglich war.

Das E-DCH Konzept stellt zudem sicher, dass nach wie vor auch nicht stationäre Teilnehmer mit hohen Datenraten kommunizieren können. Die neuen Algorithmen für die dynamische Bandbreitenregelung sind jedoch für stationäre oder sich nur langsam bewegende Teilnehmer optimiert.

Quality of Service

Der neue E-DCH unterstützt die schon bekannten Traffic Klassen Streaming (z.B. Mobile TV), Interactive (z.B. Webbrowsing) und Background Service (z.B. FTP). Um auch Echtzeitanwendungen (Real Time) wie Voice- oder Video over IP mit IMS zu unterstützen, enthält das E-DCH Konzept eine Reihe von optionalen Erweiterungen. Mit diesen ist es möglich, eine minimale Bandbreite während der Übertragung zu garantieren. Da diese Erweiterungen optional sind, ist zu erwarten, dass erste E-DCH Implementieren im Netzwerk ihren Focus zunächst auf die wichtigsten E-DCH Konzepte legen und weitere Funktionen erst mit zukünftigen Softwareupdates im Netzwerk und auch in den Endgeräten verfügbar werden. Trotzdem können auch heute schon IP basierte Sprach- und Videoübertragungen über nicht optimierte E-DCH Kanäle übertragen werden, solange genügend Bandbreite in einer Zelle vorhanden ist. An dieser Stelle sei angemerkt, dass die zuvor genannten Traffic-Klassen zwar schon seit den Anfängen von UMTS spezifiziert sind, bisher aber so gut wie nicht genutzt werden. Einzig die Limitierung auf eine maximale Geschwindigkeit wird von manchen Netzwerkbetreibern für die Preisgestaltung verwendet.

Da die Bandbreite in Uplinkrichtung steigt, reduziert der E-DCH auch zusätzlich die Round Trip Verzögerungszeit. Dies wirkt sich vor allem beim Websurfen und bei interaktiven Spielen positiv aus.

Wie andere Erweiterungen des Standards auch ist das E-DCH Konzept rückwärtskompatibel. Somit können in einer Zelle sowohl Release 99 Endgeräte kommunizieren, die nur DCH Kanäle unterstützen, HSDPA kompatible Geräte und eben auch Endgeräte, die sowohl HSDPA als auch HSUPA unterstützen.

Standarddokumente

Da E-DCH eine Weiterentwicklung des existierenden Standards ist, wurden eine Anzahl neuer Standarddokumente erstellt und mehrere bereits existierende Dokumente erweitert. In der 3GPP Technical Recommendation (TR) 25.896 wurden zunächst unterschiedliche Optionen für HSUPA diskutiert. Nachdem sich die Mitglieder im Standardgremium geeinigt hatten, welche der Optionen in den Standard einfließen sollten, wurde zunächst die 3GPP Technical Specification (TS) 25.309 erstellt, die einen Überblick über das neue E-DCH Konzept gibt. Unter den Standarddokumenten, die für E-DCH erweitert wurden, sind die Beschreibung der physikalischen Kanäle in TS 25.211, und die Beschreibung von Spreading und Modulation für E-DCH in TS 25.231.

3.10.1 E-DCH Kanalstruktur

Für das E-DCH Konzept wurden eine Reihe neuer Kanäle im Uplink und Downlink definiert, die in den Abbildungen 3.44 und 3.45 gezeigt werden. Zusätzlich werden für eine E-DCH Verbindung auch Release 99 und HSDPA Kanäle benötigt, die in Kapitel 3.4.3 und 3.9.1 bereits beschrieben wurden. Diese Kanäle sind ebenfalls in den Abbildungen gezeigt.

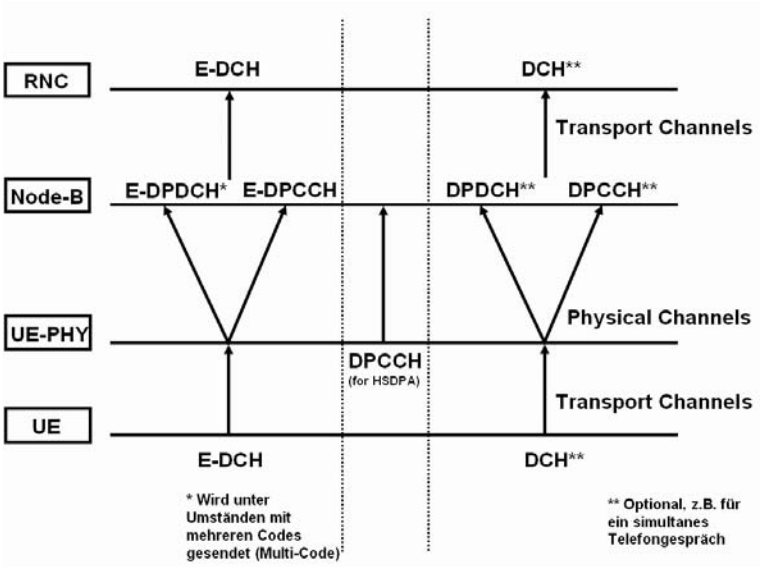

Abb. 3.44: Transportkanäle und physikalische Kanäle, die im HSUPA Betrieb verwendet werden.

Wie auf der linken Seite in Abbildung 3.44 gezeigt, führt HSUPA einen neuen Transportkanal ein, den Enhanced-DCH (E-DCH). Wie der Name des Kanals andeutet, verwendet HSUPA im Unterschied zu HSDPA keinen Shared Channel, der von mehreren Teilnehmern verwendet werden kann, sondern verwendet wie bisher auch einen dedizierten Kanal pro Endgerät. Trotzdem werden eine Reihe von Funktionalitäten, die bereits mit HSDPA eingeführt wurden, auch für den E-DCH verwendet. Da diese bereits in Kapitel 3.9 beschrieben sind, folgt an dieser Stelle nur eine kurze Auflistung:

- Node-B Scheduling: Während bisherige dedizierte Kanäle vom RNC kontrolliert wurden, ist der Node-B für E-DCH Kanäle zuständig. Dies ermöglicht eine schnellere Reaktion beim auftreten von Übertragungsfehlern. Außerdem kann der Node-B schneller auf sich verändernde Signalpegel reagieren, sowie auf die sehr variable Nutzung des Übertragungskanals durch die Teilnehmer. Zusammen bedeutet dies, dass die vorhandene Bandbreite auf der Luftschnittstelle effizienter genutzt wird.
- HARQ: Auch der E-DCH verwendet nun das Hybrid Automatic Retransmission Request (HARQ) Verfahren für die Fehlerkorrektur, statt wie bisher nur die RLC Schicht für diese Aufgabe zu nutzen. Auf diese Weise können Übertragungsfehler von Node-B schon im MAC-Layer erkannt werden. Für weitere Details hierzu siehe Kapitel 3.9.2.
- Chase Combining und Incremental Redundancy werden in ähnlicher Weise für den E-DCH verwendet wie in Kapitel 3.9.2 für HSDPA gezeigt, um die vom HARQ Mechanismus als fehlerhaft erkannten MAC-Frames erneut zu übertragen.

Auf der physikalischen Schicht ist der E-DCH in zwei Kanäle geteilt. Der Enhanced Dedicated Physical Data Channel (E-DPDCH) ist der Haupttransportkanal und wird für Nutzdaten (IP Pakete über RLC/MAC Frames) und Schicht 3 RRC Signalisierung zwischen Endgerät und RNC verwendet. Wie weiter unten noch genauer gezeigt, ist der Spreizfaktor für diesen Kanal variabel und kann dynamisch von 64 bis 2 geregelt werden, je nach aktuellen Übertragungsbedingungen und der gerade vom Endgerät benötigten Bandbreite. Um die Übertragungsgeschwindigkeit zu steigern, werden mehrere Channelisation Codes gleichzeitig verwendet. Dieses Konzept wird Multi-Code Kanal genannt und ist vergleichbar mit dem HSDPA Konzept, mehrere Downlink Shared Kanäle einem einzelnen Endgerät zuzuordnen. Die Anzahl an gleichzeitigen Kanälen pro Endgerät wurde auf maximal vier begrenzt, von denen jeweils zwei mit SF=2 und die anderen zwei mit SF=4 betrieben werden. E-DPDCH Frames können eine Länge von 2 oder 10 Millisekunden haben. 10 ms Frames müssen von allen Endgeräten unterstützt werden, 2 ms Frames sind hingegen optional.

Der Enhanced Dedicated Physical Control Channel (E-DPCCH) wird für Physical Layer Steuerungsinformationen verwendet. Für jeden Frame, der auf dem E-DPDCH zum Node-B übertragen wird, gibt es einen Kontrollframe auf dem E-DPDCCH. Wichtigster Parameter ist die 7 Bit lange Traffic Format Combination ID (TFCI). Nur nach Dekodierung dieses Parameters ist der Node-B in der Lage, den MAC Frame im E-DPDCH zu dekodieren, da das Endgerät selbständig einen Spreizfaktor und eine geeignete Kodierung aus einem vom Node-B vorgegebenen Set auswählen kann. Welcher Spreizfaktor und welche Kodierung gewählt werden, hängt von der aktuellen Signalqualität ab und der Menge an Daten, die sich momentan im Sendepuffer des Endgeräts befinden. Ein E-DPCCH Frame enthält auch eine 2 Bit lange Retransmission Sequence Nummer (RSN) für die Steuerung der HARQ Prozesse (vgl. Kapitel 3.9.2). Schließlich enthält der Frame noch ein so genanntes „Happy" Bit. Mit diesem kann dem Netzwerk mitgeteilt werden, ob die aktuelle maximale Datenrate ausreichend ist, um den Sendepuffer nicht überlaufen zu lassen. Während der Spreizfaktor für die Nutzdaten variabel ist, verwendet der E-DPCCH immer einen Spreizfaktor von 256.

Abbildung 3.44 zeigt in der Mitte und rechts eine Reihe von UMTS Release 99 und Release 5 bekannten Kanälen, die zusammen mit einem E-DCH verwendet werden. Normalerweise wird ein E-DCH zusammen mit High Speed Downlink Shared Kanälen verwendet, die einen separaten Dedicated Physical Control Channel (DPCCH) benötigen, um Kontrollinformationen für Downlink HARQ Prozesse zu übertragen. Für Applikationen wie leitungsvermittelte Sprach- oder Videoübertragungen während einer E-DCH Sitzung müssen zusätzlich auch Release 99 Dedicated Data- und Control Kanäle im Uplink übertragen werden. Dies ist notwendig, da diese Anwendungen einen eigenen Kanal mit einer Bandbreite von 12.2 oder 64 kbit/s benötigen. Insgesamt muss ein E-DCH fähiges Endgerät somit mindestens fünf simultane Uplink Kanäle unterstützen. Werden während einer E-DCH Übertragung mehrere Kanäle verwendet (Multi-Code) müssen sogar bis zu 8 Code Kanäle in Uplinkrichtung gleichzeitig gesendet werden.

In Downlinkrichtung führt HSUPA drei neue zusätzliche Kanäle ein, von denen einer optional ist. Abbildung 3.45 zeigt alle Kanäle, die ein Endgerät in Downlink Richtung zu dekodieren hat, während ein E-DCH verwendet wird.

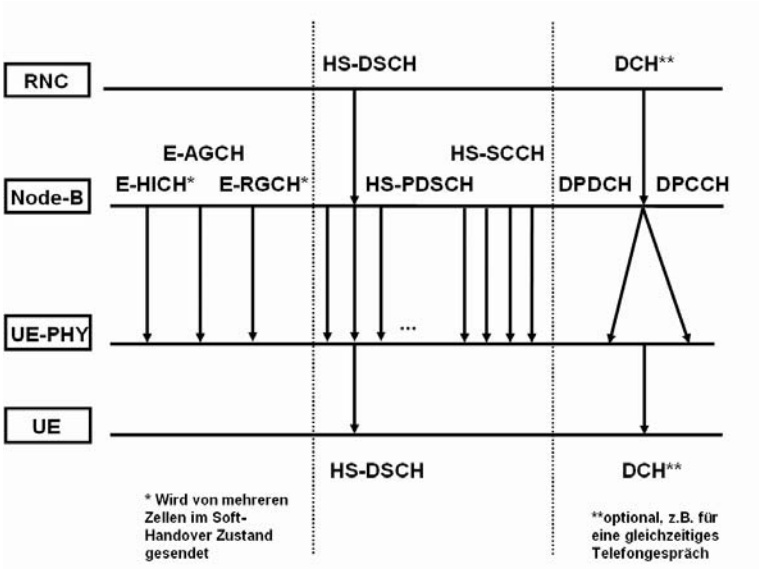

Abb. 3.45: Kanäle, die im Downlink während einer HSDPA / HSUPA Sitzung dekodiert werden müssen.

Auch wenn HSUPA nur Daten im Uplink transportiert, sind trotzdem eine Anzahl Kontrollkanäle im Downlink notwendig. Für die Bestätigung von Datenpaketen die im Uplink vom Endgerät zum Netzwerk übertragen werden, gibt es den Enhanced HARQ Information Channel (E-HICH). Der E-HICH ist ein dedizierter Kanal, d.h. das Netzwerk verwaltet pro aktivem Endgerät einen E-HICH.

Für eine schnelle und dynamische Geschwindigkeitsregelung jedes aktiven Endgerätes gibt es den Enhanced Access Grant Channel (E-AGCH), der von allen aktiven E-DCH Endgeräten einer Zelle überwacht werden muss. Dieser hat einen festen Spreizfaktor von 256. Mehr zum Thema Bandbreitenmanagement in Kapitel 3.10.3.

Zusätzlich kann das Netzwerk die maximale Geschwindigkeit jedes Endgeräts, die ursprünglich auf dem E-AGCH zugeteilt wurde, über den Enhanced Relative Grant Channel (E-RGCH) vergrößern oder verkleinern. Der E-RGCH ist ein dedizierter Kanal, jedem aktiven E-DCH Endgerät wird also ein eigener E-RGCH zugeteilt. Der E-RGCH ist jedoch optional und muss somit nicht zwingend von allen Netwerkherstellern verwendet werden.

An dieser Stelle sei noch erwähnt, dass die meisten hier vorgestellten Kanäle zwar als „Enhanced“ (verbessert) bezeichnet werden, jedoch keine Release 99 Vorgänger haben. Einzige Ausnahme ist der E-DCH.

Zusätzlich zu diesen drei Kontrollkanälen muss ein E-DCH Endgerät noch eine Anzahl weiterer Downlink Kanäle dekodieren. Da HSUPA normalerweise zusammen mit HSDPA verwendet wird, sind zusätzlich alle zugeteilten High Speed Downlink Shared Kanäle (HS-DSCH) zu dekodieren, sowie die High Speed Shared Control Channels (HS-SCCH). Ist noch zusätzlich ein Sprach- oder Videoanruf aufgebaut, öffnet das Netzwerk noch zwei weitere Kanäle im Downlink wie in Abbildung 3.45 auf der rechten Seite gezeigt. Insgesamt muss ein E-DCH Endgerät somit 10 bis 15 Downlink Kanäle gleichzeitig dekodieren können. Falls das Endgerät zusätzlich im Soft Handover State ist (vgl. Kapitel 3.7.1) steigt die Anzahl der Kanäle noch weiter, da manche Kanäle dann von mehreren Zellen ausgestrahlt werden.

3.10.2 Der E-DCH Protokoll Stack

Um die Komplexität für höhere Schichten zu verringern und die neu hinzugekommenen Aufgaben zwischen Node-B und RNC verteilen zu können, führt das E-DCH Konzept zwei neue Protokollschichten ein, die MAC-e und MAC-es genannt werden. Beide Schichten befinden sich unterhalb der MAC-d Schicht, die auch für Release 99 Kanäle verwendet wird. Höhere Protokollschichten mussten somit für E-DCH nicht modifiziert werden.

Während in Engeräten die MAC-e und MAC-es Schichten kombiniert wurden, sind deren Funktionalitäten auf der Netzwerkseite zwischen Node-B und RNC verteilt. Die Funktionalitäten der unteren MAC-e Schicht sind im Node-B implementiert, da dieser für das Scheduling der Datenpakete und die HARQ Fehlerkorrektur verantwortlich ist. Details hierzu werden weiter unten beschrieben. Die MAC-es Schicht ist im RNC angesiedelt und übernimmt die Kombination von Frames, die von unterschiedlichen Node-Bs empfangen werden, während eine E-DCH Verbindung im Soft-Handover Zustand ist.

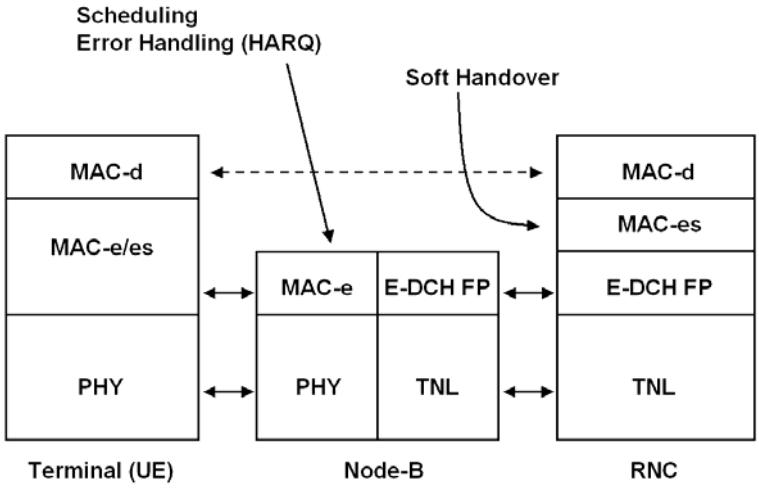

Abb. 3.46: Der E-DCH Protokoll Stack

Des Weiteren ist der RNC für den Aufbau einer E-DCH Verbindung mit dem Endgerät zuständig. Dies ist nicht Teil der MAC-es Schicht, sondern des Radio Ressource Control (RRC) Algorithmus, der für HSUPA erweitert wurde. Da der RRC Algorithmus im RNC einen E-DCH Kanal wie einen normalen dedizierten Kanal behandelt, ist ein Endgerät während einer HSUPA Verbindung im Cell-DCH Zustand. Die generelle Administration der E-DCH Kanäle verbleibt also beim RNC, während das Scheduling der Nutzerdaten nun Aufgabe des Node-Bs ist. Der RNC kann deshalb weiterhin als übergeordnete Instanz entscheiden, wann ein Endgerät bei Inaktivität den E-DCH Kanal abgeben muss und in den Cell-FACH Zustand zurückfällt. Somit wird eine HSUPA Verbindung Teil des Cell-DCH Zustands und Teil des allgemeinen Radio Ressource Management, das in Kapitel 3.5.4 beschrieben wurde.

Da HSUPA im Uplink einen Dedicated Channel verwendet, kann für Zellwechsel oder bei schlechter Signalstärke ein Soft-Handover mit mehreren Zellen aktiviert werden. Dies ist mit Shared Channels, wie sie bei HSDPA verwendet werden, nicht möglich, da die Zellen synchronisiert sein müssten, um ein Datenpaket an einen Teilnehmer genau zur gleichen Zeit über Shared Channels zu übertragen. In der Praxis würde dies einen sehr hohen Signalisierungsaufwand im Netzwerk bedeuten. Durch die Verwendung von Dedicated Channels ist außerdem ein unter-

schiedliches Timing verschiedener Endgeräte nicht kritisch, da diese zur selben Zeit aber mit unterschiedlichen Scrambling Codes senden können, ohne miteinander synchronisiert zu sein. Der einzige daraus entstehende Nachteil ist ein erhöhtes Rauschen (Noise) in der Zelle. Dies kann jedoch von Nachbarzellen reguliert werden, indem sie Endgeräte im Soft -Handover Zustand über den Relative Grant Channel (E-RGCH) auffordern können, ihre Sendeleistung zu reduzieren. In der Praxis ist der Soft-Handover für Uplink Übertragungen sehr hilfreich, da Endgeräte im Vergleich zu einer Basisstation nur eine sehr begrenzte Sendeleistung haben. Außerdem erhöht der Soft- Handover die Chance, dass das Netzwerk ein Datenpaket korrekt empfängt. Das Endgerät muss somit ein Datenpaket nur dann erneut übertragen, wenn alle Zellen des Active Sets ein negatives Acknowledgement (NAK) für ein Paket zurücksenden. Dies wiederum bedeutet, dass ein Endgerät seine Sendeleistung reduzieren kann, was sich wiederum positiv auf die zur Verfügung stehende Gesamtbandbreite im Netzwerk auswirkt. Die Nutzung des Soft-Handovers für E-DCH wurde im Standard jedoch als optional deklariert. Deshalb ist anzunehmen, dass erste E-DCH Implementierungen noch keinen Gebrauch davon machen werden.

Ein weiterer Vorteil eines dedizierten Kanals ist, dass Endgeräte in einer Zelle nicht untereinander synchronisiert sein müssen und somit keine Wartezeit anfällt, bis ein Datenpaket gesendet werden kann. Alle Endgeräte senden wie bei Release 99 Verbindungen zu jeder Zeit, was sich positiv auf Round Trip Verzögerungszeiten auswirkt.

3.10.3 E-DCH Scheduling

Möchte der RNC ein Endgerät z.B. auf Grund eines Verbindungsaufbaus oder erneuter Aktivität in den Cell-DCH Zustand setzen, kann ein E-DCH Kanal an Stelle eines DCH gewählt werden, wenn folgende Kriterien erfüllt sind:

- Das Endgerät unterstützt E-DCH.
- Die aktuelle Zelle unterstützt E-DCH.
- Die Quality of Service (QoS) Anforderungen der Verbindung (des PDP Kontexts) erlauben die Verwendung eines E-DCH. Manche E-DCH Implementationen können z.B. vorschreiben, dass ein DCH statt eines E-DCH verwendet wird, wenn die Verbindung ursprünglich für

Echtzeitanwendungen wie VoIP oder Videoübertragungen aufgebaut wurde. Fortgeschrittene E-DCH Implementierungen hingegen können auch diese Dienste unterstützen, da es durchaus möglich ist, auch über einen E-DCH eine minimale Bandbreite und eine konstante Verzögerungszeit zu gewährleisten. Dies kann z.B. durch Non-Scheduled Grants geschehen, die nachfolgend beschrieben werden.

Steuerung der Datenrate

Der Aufbau einer E-DCH Verbindung ist dem einer DCH Verbindung sehr ähnlich. Wie auch für einen DCH teilt der RNC dem Endgerät während dieser Prozedur mit, welches Transport Format Combination Set (TFCS) für den E-DCH Kanal verwendet werden kann. Ein TFCS ist eine Liste (ein Set) von verschiedenen Kombinationen aus Codierschema, Spreizfaktoren und Punktierungsverfahren, die unterschiedliche Übertragungsgeschwindigkeiten ermöglichen. Somit kann das Endgerät später eine geeignete Transport Format Combination (TFC) für jeden Frame in Abhängigkeit der aktuellen Signalstärke und Füllstand des Sendepuffers wählen. Über die TFCS Liste hat der RNC somit die Möglichkeit, die Geschwindigkeit eines Endgeräts zu limitieren. Während des E-DCH Verbindungsaufbaus erfährt das Endgerät auch, welche Zelle des Active Sets die Serving E-DCH Zelle wird. Über die Serving Cell kontrolliert das Netzwerk dann die Bandbreitenzuteilungen.

In der Praxis werden mindestens zwei Kanäle über einen gemeinsamen physikalischen E-DPDCH Kanal übertragen. Dies sind ein Dedicated Transport Channel (DTCH) für Nutzdaten und ein Dedicated Control Channel (DCCH) für RRC Nachrichten. Die Übertragung beider Kanäle erfolgt in gleicher Weise wie bei einen normalen DCH.

Nach erfolgreichem Aufsetzen eines E-DCH sendet das Endgerät eine Bandbreitenanforderung an den Node-B. Dies geschieht mit einer Nachricht die über den E-DCH gesendet wird, obwohl zu diesem Zeitpunkt noch keine Bandbreite für diesen Kanal zugeteilt wurde. Die Bandbreitenanforderung enthält folgende Informationen für den Node-B:

- Eine Schätzung des Endgerätes über die zur Verfügung stehende Sendeleistung nach Abzug der Leistung, die für

andere schon aktive Kanäle wie den DPCCH verwendet wird.

- Priorität des wichtigsten Kanals der übertragen werden soll.
- Sendepufferstatus des Kanals mit der höchsten Priorität
- Zusammenfassung des Status aller anderen Sendepuffer

Nachdem der Node-B die Bandbreitenanforderung erhalten hat, erteilt er eine absolute Bandbreitenzuweisung (Absolute Grant) unter Berücksichtigung des aktuellen Rauschlevels, des Bandbreitenbedarfs anderer Endgeräte und der Verbindungspriorität, die dem Node-B vom RNC während des Aufbaus der E-DCH Verbindung mitgeteilt wurde. Der Absolut Grant, auch Scheduling Grant genannt, enthält dann Informationen über das höchste Sendeleistungsverhältnis, das ein Endgerät zwischen E-DPDCH und E-DPCCH verwenden darf. Da dem Endgerät bekannt ist, mit welcher Sendeleistung der E-DPCCH gesendet werden muss, um vom Node-B noch korrekt empfangen werden zu können, wird über dieses Verhältnis auch implizit die Sendeleistung begrenzt, die für die Nutzdatenübertragung über den E-DPDCH verwendet werden darf. Dies limitiert die Anzahl an möglichen Transport Format Combinations (TFCs), die das Endgerät aus der ursprünglich zugewiesenen TFCS Liste auswählen kann, da schnellere TFCs unter Umständen mit mehr Leistung gesendet werden müssten, als vom Netzwerk zu einem Zeitpunkt zugeteilt ist.

Ein Absolute Grant kann an ein einzelnes Endgerät oder auch an mehrere Endgeräte gleichzeitig adressiert sein. Wenn das Netzwerk mehrere Endgeräte gleichzeitig erreichen will, erteilt es die gleiche Enhanced Radio Network Temporary ID (E-RNTI) an alle Endgeräte, die zu einer Gruppe zusammengefasst werden sollen. Auf diese Weise kann der Signalisierungsaufwand reduziert werden.

Eine andere Möglichkeit eine Bandbreitenzuweisung (Grant) für ein einzelnes Endgerät oder ein Gruppe zu erhöhen bzw. zu verringern ist ein relativer Grant, der über den optionalen Relative Grant Channel (E-RGCH) erteilt wird. Mit relativen Zuweisungen wird die Sendeleistung Schritt für Schritt in einem Intervall von einem Transmit Time Intervall (TTI) geändert. Auf diese Weise kann das Netzwerk somit ebenfalls recht schnell (alle 2 oder 10 Millisekunden) die Sendeleistung ändern, was sich im-

plizit wieder auf die maximal zur Verfügung stehende Bandbreite auswirkt. Relative Grants können von allen Zellen im Active Set eines Endgerätes gesendet werden. Auf diese Weise können Zellen das Rauschen von E-DCH Verbindungen steuern, die aktuell von anderen Zellen kontrolliert werden. Dies ist unter Umständen nötig, um sich selber vor einem zu hohen Rauschlevel zu schützen. In der Praxis muss also ein Endgerät in der Lage sein muss, von jeder Zelle des Active Sets den E-RGCH separat zu dekodieren.

Wie in Abbildung 3.47 gezeigt kann jede Zelle des Active Sets einer Verbindung eine von drei Rollen übernehmen:

- Eine der Zellen im Active Set ist die Serving E-DCH Zelle. Über diese erhält das Endgerät über den E-AGCH Anweisungen, seine Sendeleistung zu erhöhen, zu verringern oder zu halten. Außerdem kann die Serving E-DCH Zelle die Sendeleistung des Endgeräts auch über den E-RGCH Kanal anpassen.
- Die Serving E-DCH Zelle und alle anderen Zellen dieses Node-Bs, die Teil des Active Sets einer Verbindung sind (Zelle 3 und 4 in Abbildung 3.47), sind Teil des Serving Radio Link Set. Die Kommandos, die über den E-RGCH dieser Zellen gesendet werden sind identisch und das Endgerät kann somit diese Kanäle für die Dekodierung bündeln.
- Alle anderen Zellen im Active Set gehören zum Non-Serving Radio Link Set (Zellen 1,2 und 5 in Abbildung 3.47). Endgeräte müssen die E-RGCHs dieser Zellen jeweils einzeln dekodieren. Zellen im Non-Serving RLS können nur Hold oder Down Anweisungen schicken.

Wird ein „Up“ Kommando vom Serving RLS empfangen, darf das Endgerät seine Sendeleistung erhöhen, wenn nicht zur gleichen Zeit auch ein „Down“ Kommando von einer oder mehreren Zellen des Non-Serving RLS empfangen wird. Das „Down“ Kommando einer einzigen Zelle überstimmt somit alle „Up“ oder „Hold“ Kommandos aus anderen Zellen. Bei Erhalt eines „Down“ Kommandos muss das Endgerät dann sofort seine Sendeleistung reduzieren.

In der Praxis ist es unwahrscheinlich, dass fünf Zellen gleichzeitig Teil des Active Sets einer Verbindung sind, wie dies in Abbildung 3.47 gezeigt wird. Der Vorteil des Soft-Handover Mecha-

nismus für die Kapazität auf der Luftschnittstelle würde bei einer solch hohen Anzahl an Zellen zunichte gemacht werden. Unter realen Bedingungen wird normalerweise durch gutes Radio Engineering beim Netzaufbau gewährleistet, dass maximal zwei oder drei Zellen während eines Soft Handovers eine gute Verbindung gewährleisten können.

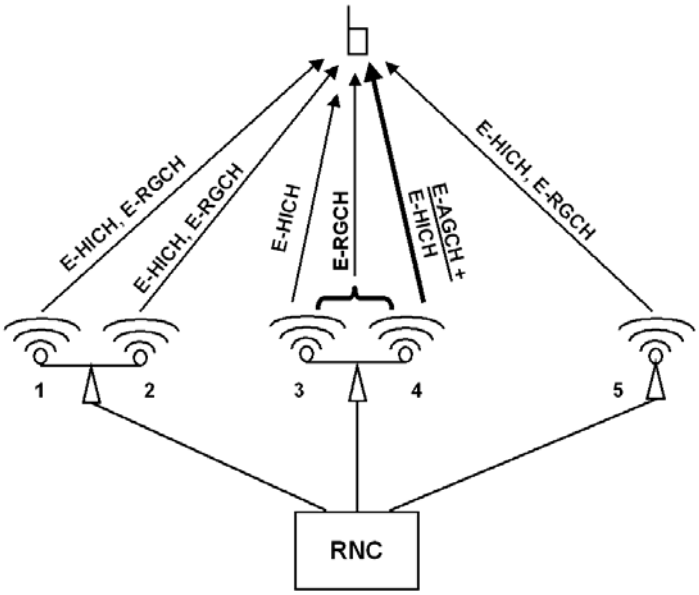

Abb. 3.47: Die Serving E-DCH Zelle, das Serving RLS und das Non-Serving RLS

Wie in diesem Kapitel gezeigt, hat der Node-B eine große Anazahl an Parametern um entscheiden zu können, welche maximale Sendeleistung welches Endgerät zu welcher Zeit verwenden darf. Der Standard legt jedoch nicht fest, welche Parameter für diese Scheduling Entscheidungen verwendet werden müssen. Netzwerkhersteller können somit ihre eigenen Algorithmen implementieren.

Um einen E-DCH auch für Echtzeitanwendungen wie Voice- oder Video over IP verwenden zu können, sieht der Standard Non-Scheduled Grants vor. Entscheidet der RNC, dass eine konstante Bandbreite und eine konstante Verzögerungszeit für eine Verbindung notwendig sind, kann es den Node-B anweisen, die dafür notwendige Sendeleistung zu garantieren. Das Endgerät kann dann seine Daten ohne vorherige Bandbreitenanforderung

an den Node-B schicken. Wird dieser Mechanismus verwendet, muss der Node-B sicherstellen, dass auch in Spitzenzeiten für Übertragungen mit Non-Scheduled Grants genügend freie Bandbreite zur Verfügung steht.

3.10.4 E-DCH Mobility

Die höchsten Datenraten können mit einem E-DCH erreicht werden, wenn das Endgerät stationär betrieben wird, oder sich der Nutzer nur langsam bewegt. In diesen Fällen können kleine Spreizfaktoren verwendet werden und die Anzahl der Redundanzbits auf ein Minimum reduziert werden. HSUPA wurde jedoch so spezifiziert, dass auch sich schnell bewegende Teilnehmer mit höheren Datenraten im Vergleich zu Release 99 Kanälen rechnen können.

Erste E-DCH Implementierungen verwenden unter Umständen nur eine einzige Serving Cell, d.h. es gibt keine Macro Diversity (Soft-Handover). Für die Mobilität bedeutet dies, dass die erreichbaren Datenraten zwischen zwei Zellen nicht ideal sind, da das Endgerät nicht genug Sendeleistung hat, um einen niedrigen Spreizfaktor und gute Kodierraten wählen zu können. Entscheidet sich der RNC aufgrund von Signalstärkemessungen des Node-B und des Endgerätes, eine andere Zelle für die E-DCH Verbindung zu wählen, gibt es eine kurze Unterbrechung, da das Endgerät nach dem Handover zunächst den E-DCH in der neuen Zelle wiederherstellen muss.

Bessere Implementierungen werden, wie in Abbildung 3.47 gezeigt, die Soft-Handover Funktionalität verwenden. Im Uplink wird dann der Datenstrom eines Endgerätes von mehreren Zellen empfangen, die ihre Kopie des Datenstroms an den RNC weiterleiten. Jede Zelle teilt außerdem dem Endgerät mit, ob sie ein Paket korrekt empfangen hat. Hat zumindest eine Zelle im Active Set ein Datenpaket korrekt empfangen, muss das Datenpaket nicht erneut gesendet werden. Dies ist vor allem bei mobilen Datenübertragungen von Vorteil, da sich hier wie in Abbildung 3.30 gezeigt, die Empfangsbedingungen bedingt durch auftauchende Hindernisse im Übertragungspfad und Fadingeffekte sehr schnell ändern. Außerdem ermöglicht ein Soft-Handover im Uplink eine unterbrechungsfreie Übertragung, während sich der Anwender mit seinem Endgerät durch das Netzwerk bewegt.

Inter-frequency und Inter-RAT (Radio Access Technology) Handover Prozesse wurden ebenfalls für HSUPA erweitert, um die

Verbindung zwischen Endgerät und Netzwerk auch in folgenden Fällen zu gewährleisten:

- Der Nutzer bewegt sich mit seinem Endgerät in eine Zelle die nur Release 99 DCH Kanäle unterstützt. In diesem Fall instruiert das Netzwerk das Endgerät einen Handover in die neue Zelle durchzuführen und dort einen DCH statt eines E-DCH aufzubauen.
- Aus Kapazitätsgründen kann ein Netzwerkbetreiber mehrere 5 MHz Carrier in einer Zelle verwenden. Ein Carrier wird dann z.B. für Telefongespräche und Release 99 Dedicated Channels verwendet, während der zweite Carrier für HSDPA und HSUPA Verbindungen reserviert ist. Muss dann das Endgerät in eine Zelle wechseln, in der nur ein Carrier verwendet wird, bekommt es vom Netzwerk einen Befehl, den Carrier zu wechseln. Dieser Vorgang wird auch als Inter-Frequency Hard Handover bezeichnet.
- Im ungünstigsten Fall verlässt ein Anwender die UMTS Abdeckung. Falls jedoch noch ein GSM Netzwerk vorhanden ist, kann eine aktive Verbindung auch dorthin übergeben werden. Dies wird als Inter-RAT Handover bezeichnet.

3.10.5 E-DCH Endgeräte

Neue E-DCH Endgeräte müssen eine höhere Verarbeitungsgeschwindigkeit und Speicher aufweisen als Release 99 DCH oder HSDPA Geräte, um hohe Datenraten sowohl im Downlink (HSDPA) als auch im Uplink (HSUPA) verarbeiten zu können. Um von der ständigen Weiterentwicklung der Endgerätehardware zu profitieren, definiert der Standard sechs Terminalkategorien. Diese Kategorien unterscheiden sich durch die Anzahl an gleichzeitig unterstützen E-DCH Spreading Codes, deren maximale Code Länge und durch die Unterstützung von Paketlängen von 2 oder 10 ms. Je mehr und je kleinere Spreading Codes unterstützt werden, desto schneller die Datenübertragung. Die nachfolgende Tabelle zeigt die definierten E-DCH Terminalkategorien und die dazugehörende maximale Datenrate unter idealen Übertragungsbedingungen. Für die beste Endgerätekategorie sind vier simultane Codes definiert, zwei mit einem Spreizfaktor von zwei und zwei mit einem Spreizfaktor von vier. Die maximale Datenrate auf Anwendungsebene ist etwas geringer als für

Schicht zwei in der nachfolgenden Tabelle angegeben, da der Overhead der Protokollschichten darunter noch abzuziehen ist.

Kategorie	**Spreizfaktor und Anzahl gleichzeitiger Codes**	**Größte Transport-blockgröße für ein 10 ms / 2 ms TTI**	**Maximale Übertragungs-geschwindigkeit für ein 10 ms / 2ms**
1	1x SF-4	7.296 bits	729 kbit/s
2	2x SF-4	14.592 bits / 2.919 bits	1.4592 MBit/s / 1.4595 MBit/s
3	2x SF-4	14.592	1.4592 Mbit/s
4	2x SF-2	20.000 bits / 5.837 bits	2.000 MBit/s / 2.9185 Mbit/s
5	2x SF-2	20.000 bits	2.000 MBit/s
6	2x SF-2 + 2x SF4	20.000 bits / 11.520 bits	2.000 MBit/s 5.76 Mbit/s

Wie in der Tabelle gezeigt, können Geschwindigkeiten über 2 MBit/s nur mit 2 Millisekunden Frames erreicht werden. Dies wurde so festgelegt, da bei höheren Geschwindigkeiten die Verwendung von 10 ms Frames aufgrund der daraus resultierenden Blockgrößen nicht mehr sinnvoll ist. Bei 2 MBit/s beispielsweise passen in einen 10 Millisekunden Block schon etwa 2500 Bytes.

Unter weniger optimalen Bedingungen hat das Endgerät oft nicht genügend Sendeleistung, um die maximale Anzahl an Codes für eine Übertragung verwenden zu können. Außerdem ist es in vielen Fällen nötig, auch die Anzahl der Fehlerkorrekturbits zu erhöhen, d.h. die Anzahl der pro Transportblock übertragenen Nutzdatenbits sinkt. Außerdem kann auch der Node-B die Sendeleistung des Endgeräts begrenzen, um die vorhandene Kapazität der Luftschnittstelle unter allen aktiven Endgeräten der Zelle aufzuteilen.

3.11 Fragen und Aufgaben

1. Welche wesentlichen Unterschiede gibt es zwischen dem GSM und dem UMTS Radionetzwerk?
2. Welche Vorteile bietet das UMTS Radionetzwerk gegenüber bisherigen Technologien für Benutzer und Netzbetreiber?
3. Welche Datenraten sind mit einem Release 99 UMTS Netzwerk möglich?
4. Was bedeutet der Begriff OVSF?
5. Warum wird zusätzlich zum Spreading Code noch ein Scrambling Code verwendet?
6. Was bedeutet der Begriff Cell Breathing?
7. Welche Unterschiede gibt es zwischen dem Cell-DCH und dem Cell-FACH RRC Zustand?
8. In welchen RRC Zuständen kann sich ein Endgerät im PMM Connected Zustand befinden?
9. Wie funktioniert das UMTS Soft Handover Verfahren und welche Vor- und Nachteile hat es?
10. Was ist ein SRNS Relocation?
11. Wie funktioniert das Mobility Management im Cell-FACH Zustand?
12. Wofür wird der Compressed Mode benötigt?

Lösungen sind auf der Website zum Buch unter http://www.cm-networks.de zu finden.

4 Wireless LAN IEEE 802.11

Mitte der neunziger Jahre fristete eine neue Technologie namens Wireless LAN noch ein Schattendasein. Dies änderte sich sehr schnell Anfang dieses Jahrzehnts, nachdem die benötigte Hardware deutlich billiger wurde. Wireless LAN wurde so schnell das optimale Medium, um Computer drahtlos untereinander und mit dem Internet zu verbinden. Kapitel 4 dieses Buches beschäftigt sich ausführlich mit diesem System, das vom IEEE (Institute of Electrical and Electronics Engineers) unter der Bezeichnung 802.11 standardisiert wurde. Der erste Teil des Kapitels beschreibt zunächst die technischen Grundlagen dieses Systems. Neben der Heimvernetzung und Hotspots kommen auch Themen wie Roaming und Wireless Bridging nicht zu kurz. Mit der Verbreitung dieses Systems wurde schnell entdeckt, dass Datensicherheit und Verschlüsselung einige gravierende Schwachstellen aufwiesen. Deshalb wird in diesem Kapitel auch gezeigt, wie diese beseitigt wurden und wie heute ein Wireless LAN sicher betrieben werden kann. Wireless LAN und UMTS werden oft miteinander verglichen, denn sie haben viele Gemeinsamkeiten. Da es aber auch viele Unterschiede gibt, stellt das Kapitel am Ende beide Systeme gegenüber und zeigt, für welche Anwendungen welches System am besten geeignet ist.

4.1 Wireless LAN Überblick

Wireless LAN (Local Area Network) trägt seinen Namen zu Recht, denn es basiert im Wesentlichen auf LAN Standards, die ursprünglich vom IEEE für die drahtgebundene Vernetzung von Computern in den 802.X Standards beschrieben sind. Diese LAN Standards werden im täglichen Sprachgebrauch auch oft als „Ethernet“ bezeichnet. Die drahtlose Variante, also das Wireless LAN (WLAN), wurde in den 802.11 Standards spezifiziert. Wie in Abbildung 4.1 zu sehen ist, dient WLAN heute hauptsächlich dazu, auf Schicht 3 des OSI Modells IP Pakete zu transportieren. Schicht 2, der Data Link Layer, wurde mit wenigen Änderungen aus der drahtgebundenen „Ethernetwelt“ übernommen. Um der drahtlosen Natur des Netzwerkes Rechnung zu tragen, wurden zusätzlich für Layer 2 einige Management Operationen definiert,

die in Kapitel 4.2 beschrieben werden. Lediglich Schicht 1, der Physical Layer, wurde komplett neu entwickelt, da bei WLAN kein Kabel, sondern Funkwellen für die Übertragung der Datenpakete verwendet werden.

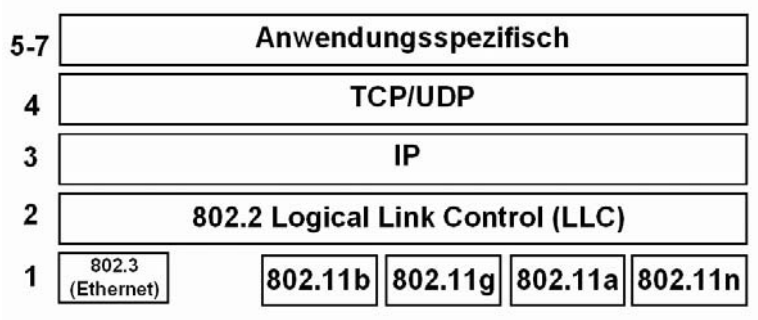

Abb. 4.1: WLAN Protokollstack

4.2 Geschwindigkeiten und Standards

Seit Bestehen der 802.11 Standards gab es zahlreiche Weiterentwicklungen bei der Funkübertragung. Aus diesem Grund gibt es mehrere Physical Layer, die in den Spezifikationen abgekürzt PHY genannt werden.

Standard	**Frequenzband (landesabhängig)**	**Geschwindigkeit**
802.11b	2.4 GHz, (2.401-2.483 GHz)	1-11 MBit/s
802.11g	2.4 GHz (2.401-2.483 GHz)	6-54 MBit/s
802.11a	5 GHz (5.150-5.350 GHz und 5.470-5725 GHz)	6-54 Mbit/s
802.11n	2.4 GHz (wie oben) 5 GHz (wie oben)	6-600 MBit/s

802.11b

Der große Durchbruch für WLAN erfolgte mit dem 802.11b Standard, mit dem Datenraten von 1-11 MBit/s möglich sind. Die Übertragungsrate richtet sich dabei hauptsächlich nach der Entfernung zwischen Sender und Empfänger, sowie nach der Anzahl der Hindernisse wie Wände oder Decken. 11 MBit/s sind dabei in Gebäuden nur über kurze Entfernungen in Größenordnungen von 10-20 Metern möglich. Die Redundanz in den Datenpaketen wird je nach Übertragungsqualität automatisch angepasst und reduziert so die Geschwindigkeit bei sehr schlechten Bedingungen auf bis zu 1 MBit/s. Die von vielen Herstellern angepriesene Reichweite von bis zu 300m wird bestenfalls bei 1 MBit/s nur im Freien erreicht, wenn keine Hindernisse zwischen Sender und Empfänger die Übertragung stören. Der 802.11b Standard sendet im 2.4 GHz ISM (Industrial, Scientific and Medical) Band, der in den meisten Ländern lizenzfrei verwendet werden darf. Wichtigste Bedingung für die Verwendung dieses Bandes ist die Beschränkung der maximalen Sendeleistung auf 100 mW. Das ISM Band ist ein öffentliches Frequenzband, neben WLAN senden hier auch noch andere Funksysteme wie z.B. Bluetooth.

802.11g

Im 802.11g Standard wurde ein im Vergleich zum 802.11b Standard weit komplexerer PHY spezifiziert, der Datenraten je nach Qualität des Übertragungsmediums von bis zu 54 MBit/s erlaubt. Auch dieser Standard sendet auf dem 2.4 GHz ISM Band und wurde so gestaltet, dass die Verfahren rückwärtskompatibel zu 802.11b sind. Somit ist sichergestellt, dass 802.11b Geräte auch mit 802.11g Geräten kommunizieren können. Mehr dazu in Kapitel 4.6 über die einzelnen PHYs.

802.11a

Zusätzlich zum 2.4 GHz ISM Band wurde auch im 5 GHz Frequenzbereich ein Band für WLAN freigegeben, für das zunächst der 802.11a Standard spezifiziert wurde. Wie beim 802.11g Standard sind auch hier Datenraten von 6-54 Mbit/s möglich. 802.11a Endgeräte wurden jedoch aufgrund der nötigen Rückwärtskompatibilität zu 802.11b/g nie besonders erfolgreich, da die Unterstützung von zwei Frequenzbereichen zusätzliche Kosten verursachte. In der Praxis standen dem bisher jedoch keine nennenswerten Vorteile gegenüber.

802.11n

Aufgrund der steigenden Datenraten bei lokalen Netzwerken und auch bei Internetzugängen per Kabel oder ADSL wurde bald klar, dass auch bei Wireless LANs weitere Geschwindigkeitssteigerungen notwendig waren. Nach einigen Jahren Standardisierungsarbeit einigten sich schließlich die beteiligten Firmen auf ein gemeinsames neues Verfahren, dass im IEEE 802.11n Stan-

dard definiert ist. Durch doppelte Kanalbreiten und zahlreichen weiteren Neuerungen, die im Laufe dieses Kapitels näher beschrieben werden, erreicht dieser Standard theoretische Spitzengeschwindigkeiten von bis zu 600 Mbit/s. Außerdem unterstützt der Standard sowohl das 2.4 GHz Band als auch das 5 GHz Band. Dies wurde notwendig, da das 2.4 GHz Band bereits sehr stark genutzt wird und in vielen Fällen nur im 5 GHz Band freie Kanäle zur Verfügung stehen. In vielen Fällen wird es in Zukunft nur dort möglich sein, hohe Datenraten zu erzielen, die für Anwendungen wie Video Streaming notwendig sind.

Proprietäre Systeme

Neben diesen Geschwindigkeitsstandards bieten manche Hersteller auch eigene, proprietäre oder in 802.11g als optional deklarierte Zusätze an, um so die Übertragungsgeschwindigkeit zu steigern. Der Geschwindigkeitsvorteil kann aber nur dann genutzt werden, wenn Sender und Empfänger vom gleichen Hersteller sind. Viele dieser proprietären Erweiterungen sind während der Standardisierung in 802.11n eingeflossen um in Zukunft ein Wildwuchs vermieden werden kann.

Weitere 802.11 Standards

Weitere 802.11 Standards, die in der nachfolgenden Tabelle aufgelistet sind, spezifizieren diverse zusätzliche optionale Wireless LAN Funktionalitäten:

Standard	Beschreibung
802.11e	Wichtigste neue Funktionalität des Standards sind Methoden, um für eine Übertragung eine bestimmte Quality of Service (QoS) zu gewährleisten. Damit ist es möglich, Bandbreite und schnellen Medienzugriff für Echtzeitanwendungen wie z.B. Voice over IP (VoIP) auch in stark ausgelasteten Netzen zu gewährleisten. Außerdem spezifiziert der Standard das Direct Link Protocol (DLP), mit dem zwei WLAN Endgeräte auch direkt unter Umgehung des Access Points Daten austauschen können. Dies steigert die Übertragungsgeschwindigkeit zwischen zwei drahtlosen Endgeräten wesentlich.
802.11f	Spezifikation für den Datenaustausch zwischen Access Points. Mehr dazu in Kapitel 4.3.1 über Extended Service Sets (ESS).

802.11h	Ergänzung für Standards im 5 GHz Bereich für Leistungsregelung und dynamische Frequenzwahl. In Europa sind ab einer gewissen Sendeleistung nur 802.11a Systeme zugelassen, die sich an diese Erweiterungen halten.
802.11i	Standardisiert erweiterte Authentifizierungs- und Verschlüsselungsalgorithmen für WLAN. Wichtiger Bestandteil von 802.11i ist 802.1x. Mehr hierzu in Kapitel 4.7 zum Thema WLAN Sicherheit.

4.3 WLAN Konfigurationen: Von Ad-hoc bis Wireless Bridging

Alle Stationen, die auf dem gleichen Übertragungskanal Daten austauschen, werden im 802.11 Standard unter dem Begriff Basic Service Set (BSS) zusammengefasst. Die Definition des BSS umfasst auch den geographischen Bereich, in dem sich die Teilnehmer des BSS aufhalten können. Ein BSS kann in folgenden unterschiedlichen Modi betrieben werden:

4.3.1 Ad-hoc, BSS, ESS und Wireless Bridging

Ad-hoc Mode (IBSS)

Im Ad-hoc Mode, auch Independent BSS (IBSS) genannt, kommunizieren zwei oder mehr WLAN Endgeräte direkt miteinander. Jede Station ist gleichberechtigt und Daten werden direkt von Endgerät zu Endgerät gesendet. Der Ad-hoc Mode entspricht also im Wesentlichen einem drahtgebundenen Ethernet, in dem ebenfalls alle Stationen gleichberechtigt sind und Datenpakete ebenfalls direkt zwischen zwei Teilnehmern ausgetauscht werden. Die gesendeten Daten werden zwar auch von allen anderen Teilnehmern des Netzwerks empfangen, von diesen aber ignoriert, weil die Zieladresse des Pakets nicht mit ihrer eigenen Adresse übereinstimmt. Alle Teilnehmer des Ad-hoc Netzes müssen sich zu Beginn auf die Werte für einige Parameter einigen und diese dann in ihren Endgeräten entsprechend konfigurieren. Wichtigster Parameter ist die Service Set ID (SSID), die als Namen für das Netzwerk dient. Weiterhin müssen alle Teilnehmer des Netzwerkes die gleiche Kanalnummer einstellen und auch der Verschlüsselungskey muss bei allen Teilnehmern gleich konfiguriert werden. Zwar kann das Ad-hoc Netzwerk auch ohne Verschlüsselung betrieben werden, aus Sicherheitsgründen ist hiervon jedoch abzuraten. Schließlich müssen sich die Teilnehmer noch auf die zu verwendenden IP Adressen einigen und auch diese

entsprechend in ihren Endgeräten eintragen. Die komplizierte Konfiguration ist einer der Gründe, warum der Ad-hoc Modus in der Praxis selten verwendet wird.

Infrastructure BSS

Eine der Hauptanwendungen eines WLAN Netzwerkes ist der Zugang zu einem Firmen- oder Heimnetzwerk, sowie dem Internet. Für diesen Zweck eignet sich der Infrastructure BSS Mode des WLAN Standards am besten. Im Unterschied zum Ad-hoc Mode gibt es hier einen so genannten Access Point, der eine zentrale Rolle übernimmt.

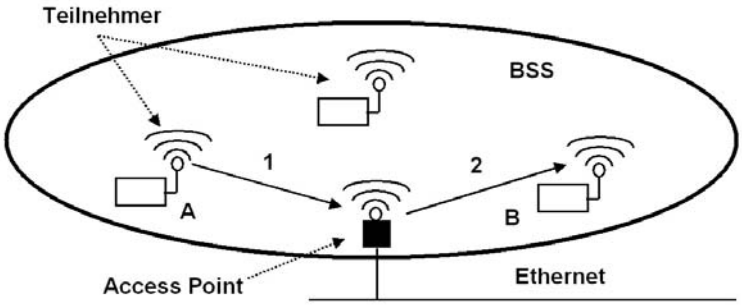

Abb. 4.2: Infrastructure BSS

Der Access Point bildet wie in Abbildung 4.2 gezeigt, den Übergang zwischen dem drahtlosen und drahtgebundenen Netzwerk für alle Endgeräte im BSS. Außerdem kommunizieren Endgeräte in einem Infrastructure BSS nicht direkt miteinander, sondern immer über den Access Point. Möchte Endgerät A an Endgerät B ein Datenpaket schicken, sendet es dies zunächst an den Access Point. Der Access Point analysiert die Zieladresse und stellt das Paket danach an Teilnehmer B zu. Auf diese Weise ist es möglich, Endgeräte im drahtlosen und im drahtgebundenen Netzwerk zu erreichen, ohne dass Teilnehmer wissen müssen, um welche Sorte Endgerät es sich handelt. Der zweite Vorteil dieses Verfahrens liegt darin, dass auch drahtlose Endgeräte über den Access Point miteinander kommunizieren können, die sich für eine direkte Kommunikation zu weit auseinander befinden. Dies kann z.B. der Fall sein, wenn sich wie in Abbildung 4.2 gezeigt, der Access Point zwischen Endgerät A und B befindet. Die Sendeleistung jedes Endgeräts reicht zwar aus, den Access Point zu erreichen, nicht jedoch das jeweils andere Gerät. Großer Nachteil dieses Verfahrens ist jedoch, das bei Kommunikation zwischen zwei drahtlosen Teilnehmern das Datenpaket zweimal über die Luftschnittstelle übertragen wird und somit die maximale Bandbreite des BSS halbiert wird. Aus diesem Grund wurde als Teil

des 802.11e Standards das optionale Direct Link Protocol (DLP) eingeführt, das eine direkte Kommunikation zwischen zwei Endgeräten erlaubt. In der Praxis implementieren jedoch heute erst wenige Endgeräte diese Erweiterung. Weitere Informationen hierzu in Kapitel 4.8.

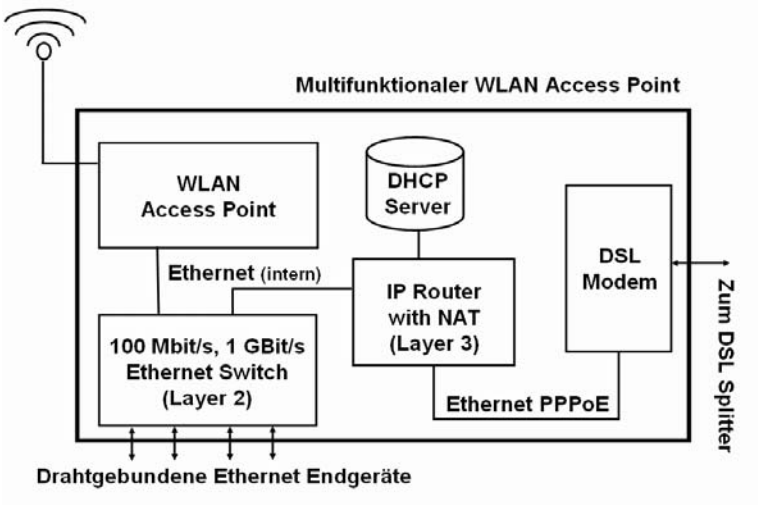

Abb. 4.3: Access Point, IP Router und DSL Modem in einem Gerät

Oft ist ein WLAN Access Point mit weiteren Funktionen ausgestattet:

- 100 MBit/s oder 1 GBit/s Anschlüsse für den Anschluss drahtgebundener Ethernet Endgeräte mit Layer 2 Switching Funktionalität.
- Oft dient ein WLAN Access Point im Heimbereich auch gleichzeitig als IP Router zum Internet und kann per Ethernet mit einem DSL oder Kabelmodem verbunden werden.
- Um Endgeräte automatisch für das Netzwerk zu konfigurieren, ist üblicherweise auch ein DHCP (Dynamic Host Configuration Protocol) Server in einem Access Point integriert. Dieser übergibt allen drahtlosen und drahtgebundenen Endgeräten die benötigen Netzwerkeinstellungen wie individuelle IP Adressen, sowie die Adresse des DNS Servers für die Namensauflösung und die IP Adresse des Internet Gateways.

- Schließlich kann auch das Kabelmodem oder das DSL Modem im Wireless LAN Access Point integriert sein. Dies ist sehr praktisch, da weniger Geräte verkabelt werden müssen und nur noch ein Netzteil für die Stromversorgung benötigt wird. Ein solcher voll integrierter Access Point ist in Abbildung 4.3 gezeigt.

Extended Service Set (ESS)

Da ein WLAN Access Point (AP) aufgrund seiner geringen Sendeleistung nur eine begrenzte Reichweite hat, sind in manchen Fällen mehrere APs notwenig, um ein bestimmtes Gebiet zu versorgen. Ändert ein mobiler Teilnehmer seinen Aufenthaltsort und kann dadurch von einem anderen AP besser versorgt werden, meldet sich die Netzwerkkarte automatisch beim neuen AP an. Eine solche Anordnung wird Extended Service Set (ESS) genannt und ist in Abbildung 4.4 dargestellt. Meldet sich ein Endgerät an einem anderen Access Point des ESS an, tauschen der neue und bisherige AP über die Ethernet Verbindung, die in den WLAN Standards auch Distribution System genannt wird, Teilnehmerinformationen aus. Zukünftig werden dann Pakete, die über das Distribution System für den Teilnehmer eingehen, über den neuen AP an den Teilnehmer zugestellt, der alte Access Point ignoriert fortan diese Pakete. Für höhere Schichten des Protokollstacks ist der Wechsel des Access Points in einem ESS nicht sichtbar, die IP Adresse kann deshalb beibehalten werden.

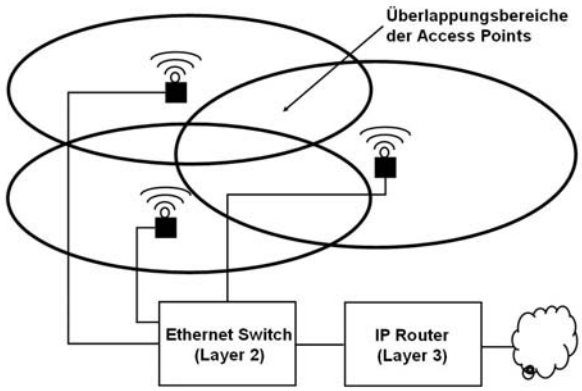

Abb. 4.4: Extended Service Set (ESS) mit 3 Access Points

Folgende Bedingungen müssen erfüllt sein, um den reibungslosen Übergang eines Teilnehmers zu einem anderen Access Point (AP) in einem ESS zu gewährleisten:

- Alle APs eines ESS müssen sich im gleichen IP Subnetz befinden, es dürfen also keine IP Router zwischen den APs liegen. Ethernetswitches, die auf OSI Layer 2 arbeiten, sind jedoch erlaubt. Dies limitiert das Ausbreitungsgebiet eines ESS beträchtlich, da IP Subnetze oft nicht sehr groß sind (z.B. ein Gebäude oder ein Stockwerk).
- Alle APs müssen die gleiche BSS Service ID, oft auch mit „SSID“ abgekürzt, besitzen. Mehr zur SSID in Kapitel 4.3.2.
- APs müssen auf unterschiedlichen Frequenzen senden und sich bei der Frequenzwahl an ein Muster halten, das in Abbildung 4.5 gezeigt wird.
- Viele APs verwenden für den Austausch der Teilnehmerinformationen bei einem AP Wechsel ein proprietäres Protokoll. Aus diesem Grund sollten alle APs eines ESS vom gleichen Hersteller stammen. Um ein ESS mit APs unterschiedlicher Hersteller zu ermöglichen, wurde vom IEEE Anfang 2003 der Standard 802.11f (Recommended Practice for Multi-Vendor Access Point Interoperability) verabschiedet, der aber nicht verpflichtend für Hersteller ist.
- Zwischen den Abdeckungsbereichen der einzelnen Access Points muss es eine Überlappung geben, damit Endgeräte auch in den Randgebieten die Netzabdeckung nicht verlieren. Da die APs mit unterschiedlichen Frequenzen senden, stellt diese Überlappung aber kein Problem dar.

Wireless Bridging

Eine weitere WLAN Variante ist das Wireless Bridging. In dieser Betriebsart wird das drahtgebundene Ethernet Distribution System zwischen zwei oder mehr APs eines ESS durch eine Funkstrecke ersetzt.

4.3.2 SSID und Frequenzwahl

Bei Inbetriebnahme eines Access Points gibt es zwei grundsätzliche Parameter, die individuell vergeben werden müssen:

SSID

Der erste Parameter ist die Basic Service Set ID, kurz SSID genannt. Die SSID wird vom Access Point über Beacon Frames, die in Kapitel 4.4 besprochen werden, in regelmäßigen Abständen über die Luftschnittstelle bekannt gegeben (Broadcast). Das Wort „Frame“ wird bei WLAN synonym zu „Paket“ verwendet. Die

SSID identifiziert einen Access Point eindeutig und ermöglicht es, mehrere unterschiedliche Access Points, die Zugriff auf unterschiedliche Netzwerke gewähren, am gleichen Ort zu betrieben. Eine Konfiguration von unabhängigen APs sollte nicht mit einem ESS verwechselt werden, das für alle APs die gleiche SSID verwendet. Üblicherweise wird für die SSID ein Textstring gewählt, da dieser bei der Konfiguration der Endgeräte später in einer Dialogbox dem User zur Auswahl des Access Points angeboten wird. Oft wird die SSID in Konfigurationsprogrammen auch als „Netzwerkname“ (Network Name) bezeichnet.

Kanäle im 2.4 GHz Bereich

Zweiter wichtiger Parameter, der bei Vorhandensein mehrerer APs sorgfältig gewählt werden sollte, ist die Sendefrequenz. Das ISM Band im 2.4 GHz Bereich von 2.410 MHz bis 2.483 MHz ist je nach Land in bis zu 13 Kanäle von jeweils 5 MHz Bandbreite unterteilt. Da ein WLAN Kanal eine Bandbreite von 25 MHz benötigt, sollten unterschiedliche WLAN Netze, die sich überlappen oder die gleiche Fläche abdecken, mindestens 5 ISM Kanäle Abstand zueinander halten. Wie in Abb. 4.5 dargestellt, können auf diese Weise 3 unabhängige BSS oder ein ESS mit sich überlappenden Grenzen von 3 Access Points betrieben werden. Bei 3 unabhängigen BSS ist diese Überlappung nicht unbedingt gewünscht, lässt sich in der Praxis jedoch oft nicht vermeiden. Bei 3 Access Points, die zusammen ein ESS bilden, ist diese Überlappung jedoch notwendig, um einen nahtlosen Wechsel von einem AP zum anderen zu ermöglichen. Um mindestens 5 Kanäle Abstand einzuhalten, müssen in den Access Points jeweils Kanal 1, 6 und 11 eingestellt werden.

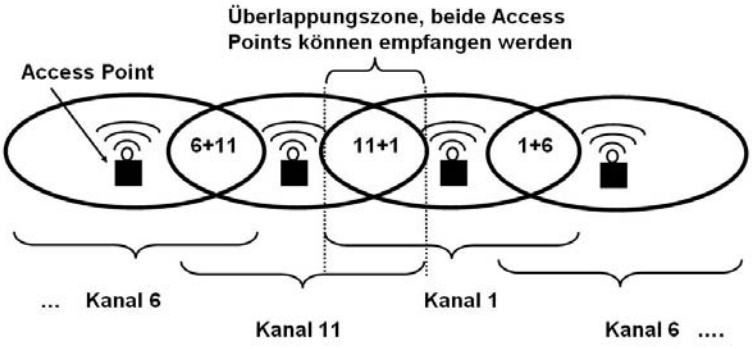

Abb. 4.5: Überlappende Abdeckung von Access Points

Kanäle 12 und 13 nur in Europa

Da die Kanäle 12 und 13 nur in Europa zugelassen sind, wird bei der Installation der meisten WLAN-Karten das Land abgefragt. Manche Produkte sparen sich jedoch diese Abfrage und blockieren Kanal 12 und 13 permanent. Steht deshalb beim Aufbau eines Access Points nicht fest, mit welchen Netzwerkkarten später auf das Netzwerk zugegriffen wird, sollten Kanal 12 und 13 nicht verwendet werden.

Kanäle im 5 GHz Bereich

802.11a und 802.11n Systeme senden im 5 GHz Bereich in Europa von 5.150 – 5.350 GHz und von 5.470 – 5.725 GHz. Zusammen sind dies 455 MHz, in denen 18 unabhängige WLAN Netzwerke Platz finden. Gegenüber den 3 unabhängigen Netzen im 2.4 GHz Band ist dies ein enormer Fortschritt. Da für diesen Frequenzbereich eine automatische Frequenzwahl vorgeschrieben ist, suchen sich Access Points automatisch einen freien Kanal.

Client Konfiguration von SSID und Frequenz

Auf Endgeräteseite ist die Grundkonfiguration des Wireless LANs für ein BSS und ESS einfacher. Das Endgerät sucht bei der Konfiguration alle Frequenzen nach vorhandenen Access Points ab und zeigt dann die gefundenen SSIDs an. Der Benutzer hat daraufhin die Möglichkeit, eine SSID auszuwählen. Dies ist in Abbildung 4.6 gezeigt. Der Sendekanal hingegen muss nicht ausgewählt werden, da das Endgerät beim Einschalten immer alle Kanäle nach einem Access Point mit der ausgewählten SSID durchsucht. Werden mehrere Access Points auf unterschiedlichen Frequenzen mit der gleichen SSID gefunden, handelt es sich um ein ESS. Das Endgerät wählt dann den Kanal, auf dem die Beacon Frames (vgl. nächster Abschnitt) am besten empfangen werden.

Die meisten WLAN Konfigurationsprogramme können heute unterschiedliche Konfigurationen zu speichern. Findet beim Systemstart die Software dann eine bekannte SSID, wird automatisch das dazugehörige Profil geladen. Somit ist es möglich, unterschiedliche Konfiguration für zuhause, für den Arbeitsplatz und für öffentliche Hotspots einmal anzulegen, die dann bei Bedarf automatisch aktiviert werden.

Sicherheit

Neben SSID und Sendekanal ist die Konfiguration der Verschlüsselung für Heim- und Firmennetzwerke ebenfalls sehr wichtig. Viele Produkte haben diese noch immer standardmäßig bei Auslieferung deaktiviert. Dies stellt ein großes Sicherheitsrisiko dar, da Funkwellen nicht an der Wohnungs- oder Bürotür halt machen. Mehr zu diesem wichtigen Thema in Kapitel 4.7.

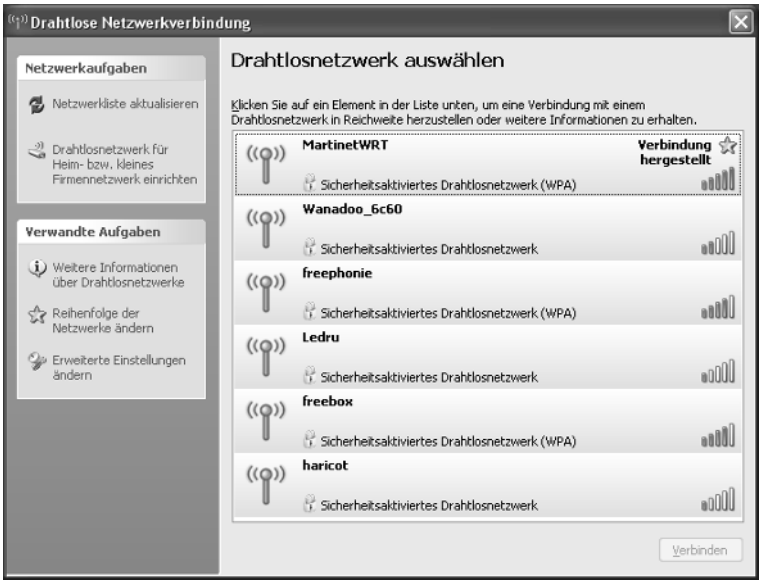

Abb. 4.6: Endgerätekonfiguration für ein BSS oder ESS.

4.4 Management Operationen

Im drahtgebundenen Ethernet genügt es, ein Endgerät mit einem Kabel am nächsten Hub oder Switch anzuschließen, um dem Endgerät Zugriff auf das Netzwerk zu gewähren. Ein solches physikalisches „Einstecken“ ist bei einem WLAN Endgerät nicht möglich. Zusätzlich verfügt ein WLAN Endgerät über Funktionen wie automatisches Roaming zu anderen Access Points eines ESS, oder die Verschlüsselung der Datenpakete auf Layer 2, die mit dem Netzwerk koordiniert werden müssen. Aus diesem Grund definiert der 802.11 Standard eine Reihe von Management Operationen und Nachrichten auf Layer 2, sowie zusätzliche Informationen im MAC Header von Datenpaketen, die im drahtgebundenen Ethernet nicht notwendig sind.

Scanning und Beacon Frames

In einem BSS nimmt der Access Point (AP) eine zentrale Rolle ein und stellt gleichzeitig den Übergang zum drahtgebundenen Ethernet her. Alle Datenpakete im WLAN werden immer an den AP geschickt, der dann die Weiterleitung an mobile und drahtgebundene Endgeräte übernimmt. Damit ein WLAN Endgerät beim Einschalten einen aktiven AP erkennen kann, sendet dieser in regelmäßigen Abständen (typisch sind 100 ms) Beacon Frames aus. Wie in Abbildung 4.7 auszugsweise gezeigt, enthalten Beacon Frames neben der SSID des Access Points noch eine Menge

weiterer Informationen, die einem Endgerät Aufschluss über Funktionen und Optionen des Access Points liefern. Jedes Bit des 2 Byte langen Capability Information Element (Capability IE) gibt Auskunft über eine bestimmte Eigenschaft. So ist zum Beispiel in Abbildung 4.7 zu sehen, dass der Access Point keine Verschlüsselung aktiviert hat (Privacy Disabled). Für umfangreichere Informationen wie z.B. die unterstützten Übertragungsraten, die mehr als ein Bit benötigen, werden eigene Information Elements (IE) im Beacon Frame verwendet. Jedes Information Element hat seine eigene ID wie z.B. 0 für das IE, das die SSID enthält, oder 1 für das IE „Supported (Data-) Rates“. Da IEs unter Umständen variable Längen haben (z.B. das SSID IE), folgt auf die ID eine Längenangabe. Somit ist es für das Endgerät möglich, optionale und evtl. unbekannte IEs, die Information für neuere Geräte enthalten, bei der Dekodierung der Nachricht zu überspringen.

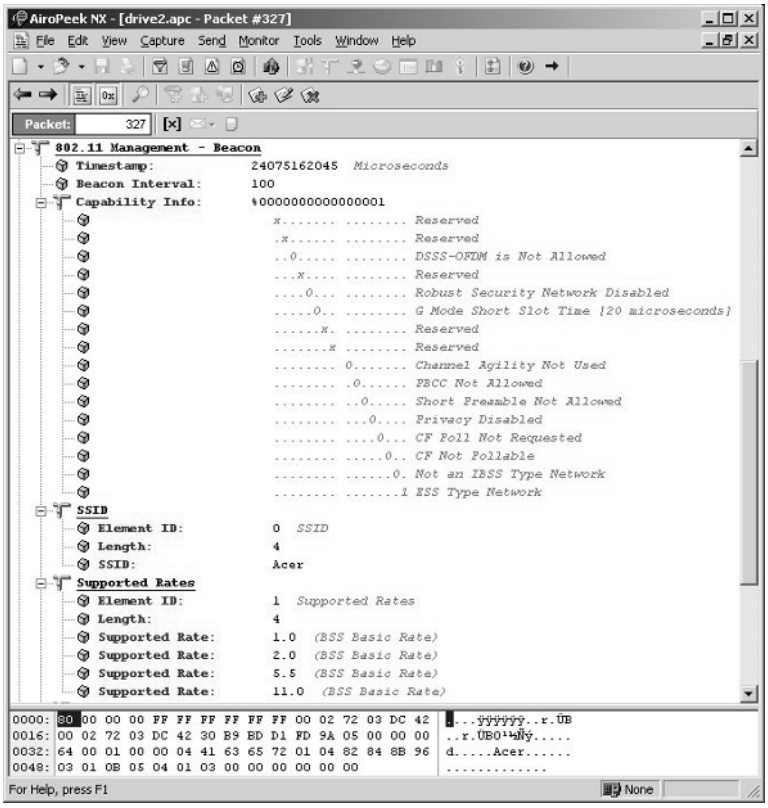

Abb. 4.7: Ausschnitt aus einem Beacon Frame

Ein Endgerät hat die Möglichkeit, bei der Netzsuche entweder nur passiv alle Kanäle nach Beacon Frames zu durchsuchen, oder aktiv mit Probe Request Frames einen Access Point zu suchen. In der Praxis verwenden die meisten Endgeräte beide Methoden. Empfängt ein Access Point einen Probe Request Frame, antwortet er mit einem Probe Response Frame, der die gleichen Informationen wie ein Beacon Frame enthält.

Nachdem ein Endgerät einen geeigneten Access Point gefunden hat, folgt im nächsten Schritt die Authentifizierung. Der Standard definiert dazu zwei Verfahren:

Open System Authentication

Die Open System Authentication trägt ihren Namen zu Unrecht, denn bei diesem Verfahren findet keine Authentifizierung statt. Das Endgerät sendet hier einen Authentication Frame mit einer Authentifizierungsanforderung an den Access Point (Authentication Request), der als Authentifizierungsalgorithmus Open System fordert. Weitere Authentifizierungsinformationen sind nicht nötig. Lässt der Access Point eine solche „Authentifizierung" zu, antwortet er mit einem positiven Statuscode und das Endgerät ist „authentifiziert".

Shared Key Authentication

Für die zweite Authentifizierungsart, der Shared Key Authentication, wird ein gemeinsamer Schlüssel benötigt, der dem Access Point und allen Endgeräten bekannt sein muss (shared). Bei einer solchen Authentifizierungsanforderung sendet der Access Point einen zufällig gewählten Text an das Endgerät zurück, der dann mit dem bekannten Key verschlüsselt wird (Challenge). Der so verschlüsselte Text wird dem Access Point zurückgeschickt (Response) und dort mit dem eigenen verschlüsselten Text verglichen. Stimmen beide Resultate überein, ist der Teilnehmer erfolgreich authentifiziert. Die Verwendung eines Schlüssels für alle Teilnehmer birgt jedoch Tücken und Sicherheitsrisiken. Weitere Informationen hierzu in Kapitel 4.7.

Association

Nach erfolgreicher Authentifizierung sendet ein Endgerät im nächsten Schritt einen Association Request (Zuordnungsanforderung) an den Access Point. Der Access Point antwortet daraufhin mit einer positiven Association Response Nachricht, in der die wichtigsten Systeminformationen wie das Capability Information Elemente noch einmal wiederholt werden. Außerdem wird dem Endgerät eine Association ID übergeben, die später für den Power Save Mode benötigt wird. Eine Trennung zwischen Authentication und Association wurde eingeführt, um einem Endgerät

den schnellen Wechsel zwischen Access Points des gleichen ESS zu ermöglichen.

Abbildung 4.8 zeigt die zwei für die Verbindungsaufnahme mit dem Netzwerk nötigen Prozeduren Authentication und Association. Acknowledgement Frames, die in Kapitel 4.5 eingeführt werden, wurden zur besseren Übersicht weggelassen.

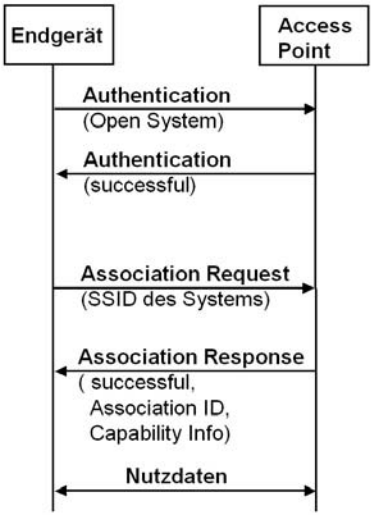

Abb. 4.8: Authentication und Association (ohne Acknowledgment Frames)

WEP Verschlüsselung der Datenpakete

Nach erfolgreicher Association des Endgeräts mit einem Access Point können bei offenen oder mit WEP geschützten Netzwerken sofort Nutzdatenpakete übertragen werden. Wurde im Access Point die WEP (Wired Equivalent Privacy) Datenverschlüsselung aktiviert, wird dies über das Capability Information Element bekannt gegeben. Alle Datenpakete werden dann vom Access Point und auch vom Endgerät vor der Übertragung mit dem gemeinsamen geheimen Schlüssel chiffriert. Da der ursprüngliche WEP Standard einige Sicherheitslücken aufweist, wurden mittlerweile weitere Verfahren wie WPA und WPA2 spezifiziert. Diese erfordern nach der Association Prozedur noch eine weitere Management Prozedur. Die Management Prozedur wird in Kapitel 4.7 näher beschrieben.

Verschlüsselung ohne Authentifizierung

Authentifizierung und Verschlüsselung sind unabhängig voneinander. So ist es heute bei den meisten Endgeräten und Access Points üblich, eine Open System „Authentication“ durchzuführen

und danach mit dem gemeinsamen geheimen Schlüssel den Datenverkehr per WEP, WPA oder WPA2 zu verschlüsseln. Endgeräte, die den geheimen Schlüssel nicht kennen oder einen falschen verwenden, können sich so zwar erfolgreich am Netzwerk anmelden, danach aber keine Daten korrekt senden oder empfangen. Manche Access Points bieten die Option, die Shared Authentication explizit einzuschalten. Dies bringt aber in der Praxis keine erhöhte Sicherheit. Darüber hinaus wird durch das Aktivieren der Shared Authentication die Konfiguration der Endgeräte erschwert, da neben der WEP Verschlüsselung noch zusätzlich manuell die Authentifizierung aktiviert werden muss.

Reassociation und Roaming

Befindet sich ein Endgerät in einem ESS mit mehreren Access Points (vgl. Abb. 4.4), kann es jederzeit zu einem anderen Access Point mit besserem Empfang für den aktuellen Aufenthaltsort wechseln. Die dazugehörende Prozedur wird Reassociation genannt und ist in Abbildung 4.9 dargestellt. Um dies zu ermöglichen, scannt ein Endgerät in Sende- und Empfangspausen alle Frequenzkanäle und kann so die Beacon Frames aller in der Nähe befindlichen APs empfangen. Anhand der SSID erkennt das Endgerät, welche APs zum aktuellen ESS gehören. Um zu einem neuen Access Point zu wechseln, ändert das Endgerät die Sende- und Empfangsfrequenz und sendet auf der neuen Frequenz einen Reassociation Request Frame. Dieser entspricht im Wesentlichen einem Association Request Frame mit der Ausnahme, dass zusätzlich noch die ID des vorherigen Access Points übergeben wird. Der neue Access Point sucht daraufhin über das drahtgebundene Ethernet (Distribution System) mit der übergebenen ID den bisherigen Access Point des Teilnehmers und informiert diesen über den Wechsel. Der bisherige Access Point sendet dem neuen Access Point dann eventuell zwischengepufferte Datenpakete des Endgeräts und löscht dessen Hardwareadresse und Association ID dann aus seiner Teilnehmerliste. Zukünftig eingehende Datenpakete über das drahtgebundene Distribution System, die immer von allen APs eines ESS empfangen werden, werden fortan nur vom neuen AP zum Teilnehmer übertragen und vom bisherigen AP ignoriert. Abgeschlossen wird die Reassociation Prozedur durch Senden einer positiven Reassociation Response Nachricht an das Endgerät.

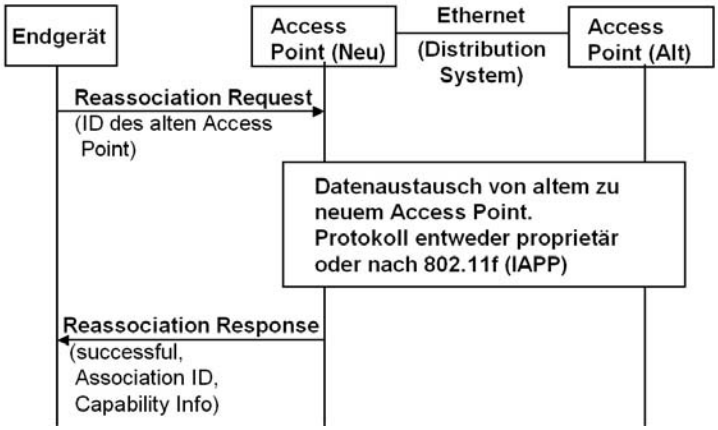

Abb. 4.9: Reassociation (ohne Acknowledgement Frames)

Nur die Signalisierung zwischen Endgerät und neuem Access Point der Reassociation Prozedur ist standardisiert. Für die drahtgebundene Kommunikation zwischen den Access Points gab es lange Zeit keinen Standard, so dass diese Prozedur von den Herstellern mit proprietären Protokollen gelöst wurde. Aus diesem Grund können in den meisten Fällen nur Access Points des gleichen Herstellers miteinander im gleichen ESS reibungslos eingesetzt werden. Mit Verabschiedung der 802.11f Empfehlung und des Inter Access Point Protocol (IAPP) könnte sich dies in Zukunft ändern.

Stromsparmodus (Power-Saving Mode)

Um die Laufzeit batteriebetriebener Geräte zu erhöhen, gibt es in den 802.11 Standards auch einen Stromsparmodus (Power-Saving Mode, PS). Dieser bremst die Datenübertragung in bestimmten Situationen etwas, reduziert aber die Leistungsaufnahme wesentlich.

Ist der Sendepuffer eines Endgeräts leer und wurden seit einiger Zeit auch keine Daten vom Access Point empfangen, kann ein Endgerät den PS Mode aktivieren. Dazu sendet das Endgerät einen leeren Frame an den Access Point, in dessen MAC-Header das PS Bit gesetzt ist. Der Access Point puffert danach alle für das Endgerät eingehenden Frames und das Endgerät kann somit die Stromzufuhr zu seinem Sender und Empfänger abschalten. Die Zeit zwischen letztem Datenpaket und dem Einschalten des PS Mode kann vom Endgerätehersteller selbst bestimmt werden. In der Praxis werden hier Werte z.B. von batteriebetriebenen Ge-

räten wie Mobiltelefonen mit Wifi Funktionalität von 0.5 Sekunden gewählt.

Möchte ein Endgerät wieder Daten senden, schaltet es seine Sende- und Empfangsstufe wieder ein und sendet einen leeren Frame mit deaktiviertem PS Bit. Danach können die neuen Frames mit Nutzdaten sofort gesendet werden.

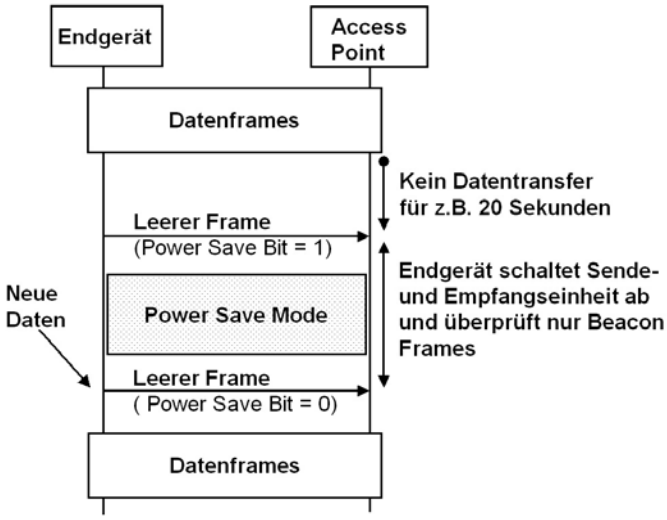

Abb. 4.10: Ein- und Ausschalten des Stromsparmodus (ohne Acknowledge Frames)

Traffic Indication Map (TIM)

Bei den meisten Anwendungen auf mobilen Endgeräten, wie z.B. dem webbrowsen, treffen nur in Ausnahmefällen nach dem Einschalten des PS Mode weitere Daten ein. Damit diese nicht verloren gehen, werden die Frames im Access Point zwischengespeichert. Aus diesem Grund muss das Endgerät auch im PS Modus periodisch seinen Empfänger aktivieren, um diese Pakete gegebenenfalls abholen zu können. Um ein Endgerät über gepufferte Frames zu informieren, gibt es in Beacon Frames das Traffic Indication Map (TIM) Information Element. Für jedes Endgerät ist in der TIM ein Bit vorhanden, das anzeigt, ob gepufferte Daten vorliegen. Das Endgerät identifiziert sein Bit in der TIM über seine Association ID (AID), die ihm bei der Association Prozedur übergeben wurde. Über die AID können bis zu 2007 Endgeräte angesprochen werden, die TIM ist also maximal 2007 Bits lang. Um die Beacon Frames möglichst klein zu halten, wird

mit Hilfe eines Offsets und einer Längenangabe nur ein Teil der TIM im Beacon Frame übertragen. Dies ist auch sinnvoll, da meist nur wenige Endgeräte an einem Access Point gleichzeitig betrieben werden.

Damit ein Endgerät nicht für jeden Beacon Frame seinen Empfänger einschalten muss, übergibt das Endgerät bei der Association Prozedur ein Listen Intervall an den Access Point, das vorgibt, in welchen Abständen die Beacon Frames überprüft werden. Akzeptiert der Access Point dieses Intervall, muss er eingehende Daten mindestens für diesen Zeitraum puffern. In der Praxis wird für das Listen Intervall zum Beispiel ein Wert von 3 verwendet. Dies bedeutet, dass das Endgerät nur jeden dritten Beacon Frame empfängt und somit seinen Empfänger für 300 ms abschalten kann. Ist das TIM Bit für das Endgerät nicht gesetzt, kann es nach Empfang des Beacon Frames seinen Empfänger wieder für die nächsten 300 Millisekunden deaktivieren.

Polling

Ist das TIM Bit für ein Endgerät gesetzt, aktiviert es neben seinem Empfänger auch seine Sendeeinheit und ruft die gepufferten Datenpakete über PS-Poll Frames beim Access Point ab. Als Antwort auf einen PS-Poll Frame erhält das Endgerät dann einen gepufferten Frame. Ist im MAC-Header des Frames das More Bit gesetzt, sind noch weitere Frames im Access Point gepuffert, die dann jeweils durch einen weiteren PS-Poll Frame angefordert werden müssen.

Gepufferte Broadcast und Multicast Frames nach DTIM

Auch Broadcast und Multicast Frames, die an mehrere oder alle Endgeräte gerichtet sind, müssen für Endgeräte im Power-Save Mode gepuffert werden. Statt jedoch diese Frames für jedes Endgerät einzeln zu puffern, gibt stattdessen das erste Bit in der TIM an (AID 0), ob Broadcastdaten gepuffert wurden. Diese Frames werden dann automatisch nach einem Beacon Frame gesendet, der statt einer TIM periodisch eine Delivery TIM (DTIM) enthält. In welchen Abständen statt der TIM eine DTIM gesendet wird, wird über eine Periode und einen Count Down Zähler in der TIM den Endgeräten mitgeteilt.

4.5 Die MAC Schicht

Das Medium Access Control Protocol (MAC, Layer 2) hat bei WLAN ähnlich wie im drahtgebundenen Ethernet unter anderem folgende Aufgaben:

- Es regelt den Zugriff der Endgeräte auf das Übertragungsmedium.

- Jedem Datenpaket wird ein MAC Header vorangestellt, der unter anderem die Adresse des Senders und Empfängers (MAC Adressen) enthält.

4.5.1 Zugriffssteuerung auf das Übertragungsmedium

Acknowledgement Frames

Aufgrund der höheren Fehleranfälligkeit der Datenübertragung über die Luftschnittstelle werden bei WLAN alle Datenpakete von der Gegenstelle nach korrektem Empfang durch ein Acknowledgement (ACK) Frame bestätigt. Dies ist ein großer Unterschied zum drahtgebundenen Ethernet, in dem Pakete nicht bestätigt werden. In allen bisherigen Abbildungen dieses Kapitels wurden diese Frames zur Übersichtlichkeit weggelassen. Abbildung 4.11 zeigt den Austausch von Frames zwischen Access Point und einem Endgerät zum ersten Mal mit ACK Frames. Jeder Frame, der entweder Nutzdaten oder Management Daten (Authentication, Association, etc.) enthält, muss von der Gegenseite durch ein ACK Frame bestätigt werden. Erst danach darf der nächste Nutzdatenframe vom gleichen oder einem anderen Endgerät gesendet werden. Bleibt der ACK Frame aus, muss das Datenpaket wiederholt werden.

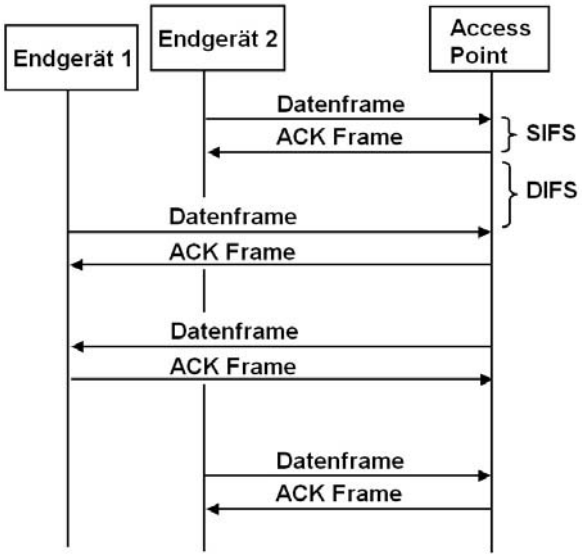

Abb. 4.11: Bestätigung (Acknowledgement) für jeden Frame

SIFS und DIFS

Durch einen sehr kurzen Sendeabstand zwischen Datenframe und ACK Frame, der Short Interframe Space (SIFS) genannt wird, ist sichergestellt, dass kein anderes Endgerät einen Frame dazwischen senden kann. Für normale Frames wird deshalb ein längerer Sendeabstand zum letzten Paket eingehalten, der DCF Interframe Space (Distributed Coordination Function Interframe Space, abgekürzt DIFS) genannt wird. Somit kann der ACK Frame auf jeden Fall gesendet werden, bevor eine andere Station den Kanal für einen normalen Frame verwenden darf. Mehr zum Thema DCF im nächsten Abschnitt.

Hidden Station RTS/CTS

Optional gibt es für ein Endgerät die Möglichkeit, die Luftschnittstelle für die Übertragung eines Frames im Vorhinein zu reservieren. Dies ist in Fällen sinnvoll, in denen Teilnehmer eines BSS zu weit voneinander entfernt sind, um die Datenpakete des jeweils anderen zu sehen. In diesen Fällen kann es passieren, dass beide Stationen gleichzeitig einen Frame an den Access Point senden und sich die Frames am Access Point gegenseitig stören. Dieses Szenario wird auch „Hidden Station“ Problem genannt. Um dieses Problem zu umgehen, sendet ein Endgerät wie in Abbildung 4.12 gezeigt vor dem Datenframe zuerst einen kurzen RTS (Ready to Send) Frame an den Access Point. Der Access Point antwortet daraufhin mit einem kurzen CTS (Clear to Send) Frame, und die Luftschnittstelle ist für den Teilnehmer reserviert. Während der RTS Frame vom zweiten Endgerät aufgrund des zu großen Abstands nicht gesehen wird, sieht es aber auf jeden Fall den CTS Frame, da dieser vom näheren Access Point gesendet wird. Damit das zweite Endgerät weis, wie lange es nicht senden darf, enthalten RTS und CTS Frames die Information, wie lange die Luftschnittstelle reserviert ist. Abgeschlossen wird die Übertragung des Frames wieder durch ein ACK Frame. Ob ein Endgerät ein Frame mit oder ohne RTS/CTS Sequenz überträgt, ist in den meisten Endgeräten in Abhängigkeit der Framegröße konfigurierbar. Dies ist sinnvoll, da der zusätzliche Zeitaufwand des RTS/CTS Mechanismus nur bei großen Paketen sinnvoll ist. Meist ist diese Option jedoch per Default deaktiviert und muss manuell konfiguriert werden.

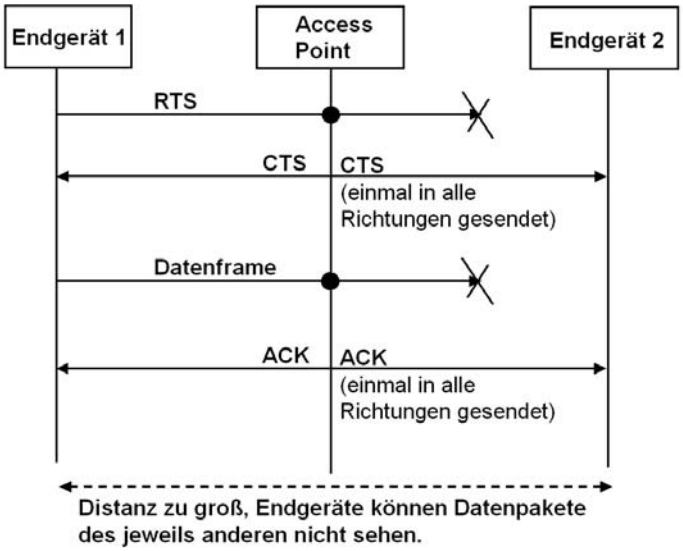

Abb. 4.12: Reservierung der Luftschnittstelle mit RTS/CTS

Distributed Coordination Function (DCF)

Bei Wireless LAN gibt es keine zentrale Steuerung, welcher Teilnehmer zu welchem Zeitpunkt auf das Übertragungsmedium (Luftschnittstelle) zugreifen darf. Jeder Teilnehmer trifft für sich die Entscheidung, wann ein anstehendes Datenpaket übertragen wird. Da aber möglichst keine Kollisionen mit anderen Teilnehmern auftreten sollen, koordinieren sich die Teilnehmer mit einem Verfahren, das Distributed Coordination Function (DCF) genannt wird. Dieser Ansatz unterscheidet sich grundlegend vom zentral gesteuerten Medienzugriff aller anderen Systeme, die in diesem Buch vorgestellt werden. Diese haben alle eine verwaltende Instanz, die genau vorgibt, welcher Teilnehmer zu welchem Zeitpunkt und für wie lange senden darf. Vorteil des DCF Verfahrens ist die einfache Implementierung in Endgeräten. Großer Nachteil des Verfahrens ist jedoch, dass keine Bandbreite reserviert oder garantiert werden kann. Besonders für Echtzeitanwendungen wie Sprach- oder Videotelefonie ist dies ein Problem, wenn das Medium von anderen Teilnehmern stark ausgelastet wird. Aus diesem Grund wurde im 802.11e Standard für Geräte und Anwendungen, die eine hohe Anforderung bezüglich konstanter Bandbreite und Medienzugriffszeit haben, eine DCF Erweiterung spezifiziert, die in Kapitel 4.8 beschrieben wird.

Wichtigster Teil der DCF ist das Medienzugriffsverfahren, das Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA) genannt wird. CSMA/CA ist CSMA/CD (CSMA/Collision Detect) sehr ähnlich, das im drahtgebundenen Ethernet verwendet wird, bietet aber einige zusätzliche Möglichkeiten, Kollisionen zu vermeiden.

Backoff

Möchte ein Endgerät ein Datenpaket versenden, und es wird keine Aktivität auf der Luftschnittstelle festgestellt, kann das Datenpaket ohne Verzögerung gesendet werden. Wird jedoch zu diesem Zeitpunkt gerade ein Datenpaket eines anderen Teilnehmers übertragen, muss das Endgerät zunächst warten, bis diese Übertragung abgeschlossen ist. Danach wartet das Endgerät noch das Ende der DIFS Periode ab. Um zu vermeiden, dass mehrere sendebereite Endgeräte danach gleichzeitig ihre Pakete absenden, wird zusätzlich noch eine per Zufallsgenerator in jedem Endgerät ermittelte Backoff-Zeit gewartet. Da mit großer Wahrscheinlichkeit jeder Teilnehmer eine andere Backoff-Zeit ermittelt hat, sendet somit nur ein Endgerät. Alle anderen sendebereiten Endgeräte sehen das Datenpaket, brechen ihre Backoff-Wartezeit ab und starten ihre Zugriffsprozedur erneut von vorn. Sollten trotz dieser Prozedur einmal zwei Endgeräte gleichzeitig senden, stören sich die Pakete gegenseitig und der Acknowledgement Frame bleibt aus. Beide Stationen müssen dann erneut versuchen, ihr Datenpaket zu senden. Bei einem Übertragungsfehler vergrößert sich jedoch die Zeitspanne für die mögliche Backoff-Zeit für das Endgerät. Somit wird erreicht, dass bei hoher Auslastung die Anzahl der Kollisionen gering bleibt.

Die Backoff-Zeit wird in Slots zu 20 Mikrosekunden eingeteilt. Beim ersten Sendeversuch gibt es bei 802.11b und g 31 Slots, von denen einer per Zufallsgenerator ausgewählt wird. Schlägt die Übertragung fehl, vergrößert sich das Fenster auf 63 Slots, danach auf 127 Slots usw., bis maximal 1023 Slots, was maximal 20 Millisekunden entspricht. Bei 802.11n wurde das erste Backoff Fenster auf 15 Slots verkleinert, was 0.3 Millisekunden entspricht.

Network Allocation Vector (NAV)

Zusätzlich zur Erkennung einer laufenden Datenübertragung und anschließender Backoff-Zeit enthält jedes Datenpaket auch eine Zeitspanne, wie lange die Übertragung des Datenpakets und anschließendem ACK Frame dauert. Diese Zeitspanne wird Network Allocation Vector (NAV) genannt. Diese zusätzliche Funktion ist vor allem dann sinnvoll, wenn wie in Abbildung 4.12 gezeigt, die Luftschnittstelle mit RTS und CTS Frames reserviert wird. Das RTS Frame enthält die Information, wie viel Zeit für

die Übertragung des CTS, des Datenpakets und das anschließende ACK Frame benötigt wird. Das anschließende CTS Paket der Gegenseite enthält dann einen etwas kleineren NAV, der nur noch die Zeitspanne für das anschließende Datenpaket und den ACK Frame enthält.

4.5.2 Der MAC Header

Wichtigste Aufgabe des MAC Headers auf Layer 2 ist die Adressierung der Endgeräte im lokalen Netzwerk. Zu diesem Zweck enthält der MAC Header eines WLAN Frames in gleicher Weise wie ein Frame im drahtgebundenen Ethernet die 48 Bit langen MAC Adressen von Sender (Source) und Empfänger (Destination). In einem Basic Service Set (BSS) wird ein Datenframe jedoch nicht direkt vom Sender zum Empfänger geschickt, sondern immer zuerst zum Access Point. Aus diesem Grund enthält der MAC Header eines Frames, wie in Abbildung 4.13 gezeigt, nicht zwei, sondern drei MAC Adressen. Die dritte MAC Adresse ist dabei die Adresse des Access Points. Dieser empfängt das Paket und überprüft, ob die MAC Adresse des Empfängers zu einem drahtlosen oder einem drahtgebundenen Endgerät gehört und leitet den Frame entsprechend weiter. Somit spielt es für das Endgerät keine Rolle, ob der Empfänger des Frames ein WLAN oder Ethernet Endgerät ist.

MAC Adressen

Frame Type

Weitere wichtige Elemente im MAC Header sind der Frame Type und Subtype. Das Frame Type Element gibt an, ob es sich beim aktuellen Frame um einen Nutzdatenframe, Management Frame (z.B. Association Request) oder Control Frames (z.B. ACK) handelt. Je nach Frame Type enthält das Subtype Element dann weitere Informationen. Bei Management Frames gibt das Subtype Feld an, um welche Management Operation es sich handelt (z.B. Authentication, Association, Beacon, etc.).

Control Flags

In den Frame Control Flags werden in jedem Frame zusätzliche Informationen zwischen zwei Teilnehmern ausgetauscht. Dort ist unter anderem angegeben, ob die Nutzdaten des Frames verschlüsselt sind (WEP enabled Bit), ob das Endgerät in den Stromsparmodus wechseln wird (Power Management Bit) und ob der Frame für einen Access Point bestimmt ist (To Distribution System Bit).

LLC Header

Bei Nutzdatenframes folgt auf den MAC Header, in gleicher Weise wie im drahtgebundenen Ethernet, der Logical Link Control Header (LLC Header, Layer 2). Dessen wichtigste Aufgabe ist es, das Layer 3 Protokoll zu identifizieren, das anschließend folgt.

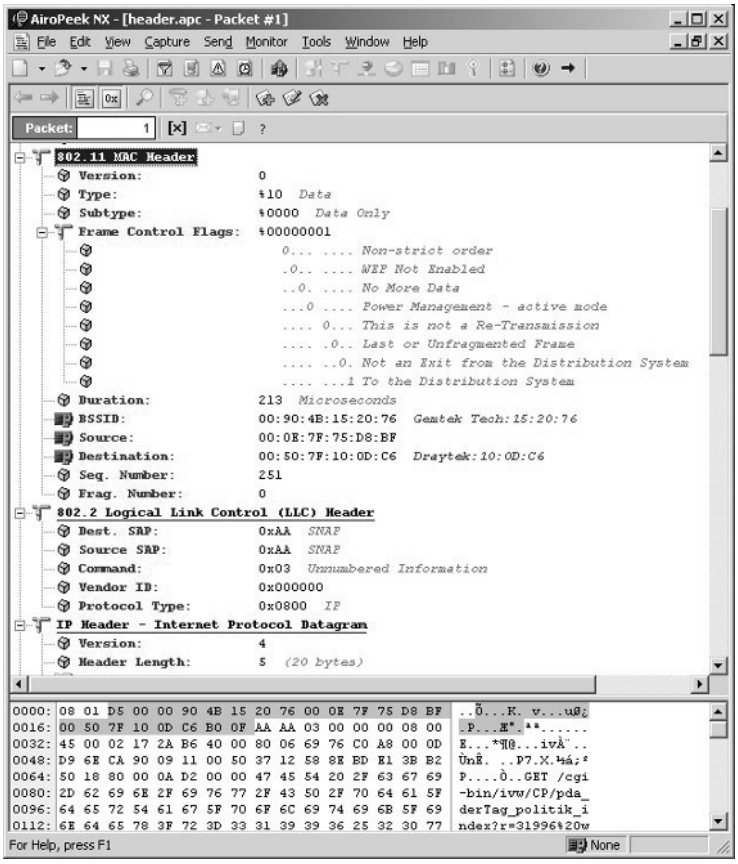

Abb. 4.13: MAC und LLC Header eines WLAN Frames

4.6 Physical Layer und MAC-Erweiterungen

Auf Layer 1, dem Physical Layer, gibt es wie in Kapitel 4.2 gezeigt, unterschiedliche Varianten mit unterschiedlichen Geschwindigkeiten, die in den Standards IEEE 802.11b, g, a und n beschrieben sind.

4.6.1 IEEE 802.11b mit bis zu 11 MBit/s

Mit einer maximalen Geschwindigkeit von bis zu 11 MBit/s erfolgte mit dem 802.11b Standard der Durchbruch von WLAN im Massenmarkt. Mit neueren Physical Layern wie 802.11g oder 802.11a sind mit der gleichen Bandbreitennutzung von etwa 22 MHz noch weit höhere Geschwindigkeiten möglich. Mehr dazu

im nächsten Abschnitt. Um ein Gefühl für ein 802.11 System im Vergleich zu anderen Technologien zu bekommen, sind folgende Daten hilfreich:

802.11b Eckdaten

- Maximale Leistung auf 0.1 Watt begrenzt.
- 22 MHz Bandbreite pro Kanal. Somit können im ISM Band drei Netze am gleichen Ort überlappend betrieben werden.
- Framegröße: 4-4095 Bytes, IP Frames sind jedoch meist nicht größer als etwa 1500 Bytes. Interessant ist hier der Vergleich zu anderen Technologien: In einem GPRS Paket, das wie in Kapitel 2.2.3 gezeigt, aus 4 Bursts zu je 114 Bits besteht, können nur 456 Bits übertragen werden. Bei Coding Scheme 2 bleiben hier nach Abzug der Fehlerkorrekturbits nur 240 Bits, also 30 Bytes. Während ein IP Paket über WLAN komplett in einem Paket übertragen wird, wird dieses in GPRS über mehrere Pakete aufgeteilt.
- Übertragungszeit eines großen Pakets: Dies ist zum einen von der Größe des Pakets und zum anderen von der Übertragungsrate abhängig. Wird ein großes Paket mit z.B. 1500 Bytes mit einer Übertragungsgeschwindigkeit von 1 MBit/s übertragen, dauert die Übertragung 12 Millisekunden. Bei gutem Empfang und einer Übertragungsgeschwindigkeit von 11 MBit/s dauert die Übertragung hingegen nur etwa 1.1 Millisekunden. Hinzu kommt noch die Übertragungszeit für den ACK Frame, sowie die Sendepause zwischen den Frames.
- Zeit zwischen Datenframe und ACK Frame (SIFS): 10 Mikrosekunden, oder 0.01 Millisekunden.
- Tritt ein Übertragungsfehler auf, wird das im letzten Absatz beschriebene Backoff-Verfahren angewandt. Ein Backoff Slot, von denen es bei der ersten Wiederholung 63 gibt, hat eine Länge von 20 Mikrosekunden oder 0.02 Millisekunden.
- Zu Beginn jedes Frames wird eine Präambel gesendet, die anderen Endgeräten die Übertragung ankündigt. Dies ist notwendig, damit sich alle anderen Endgeräte auf den Frame synchronisieren können. Die Präambel hat eine Länge von 144 Mikrosekunden, oder 0.144 Millisekunden.

PLCP Header und Übertragungsrate

Die Präambel ist Teil des Physical Layer Convergence Procedure (PLCP) Header, der vor jedem Frame gesendet wird. Der PLCP Header enthält auch die Information, mit welcher Übertragungsrate der nachfolgende MAC Frame gesendet wird. Bei 802.11 kann ein MAC Frame mit 1 MBit/s, 2, 5.5 und 11 MBit/s gesendet werden. Diese Flexibilität ist nötig, da Endgeräte mit schlechtem Empfang mit geringer Geschwindigkeit senden können, um somit die Redundanz zu erhöhen. Üblicherweise entscheidet das Endgerät automatisch anhand der Übertragungsbedingungen, mit welcher Geschwindigkeit ein Frame gesendet werden soll. Manche Endgeräte bieten aber auch die Möglichkeit, die maximale Datenrate fest einzustellen (z.B. auf 5.5 MBit/s). Dies hilft vor allem dann weiter, wenn die Automatik nur schlecht funktioniert. Bei manchen Access Points ist in der Praxis zu beobachten, dass Nutzdatenpakete zu einem Endgerät mit der zuletzt vom Endgerät gewählten Geschwindigkeit gesendet werden. Beacon Frames hingegen werden beispielsweise von manchen Access Points immer mit 1 oder 2 MBit/s übertragen. Auf diese Weise können auch weiter entfernte Geräte die Beacon Frames noch korrekt empfangen. Dies ist aber nicht vorgeschrieben und so senden manche Access Points die Beacon Frames mit 11 MBit/s. Dies erhöht zwar den Durchsatz des Netzwerkes geringfügig, weit entfernte Stationen werden aber Probleme haben, die Beacon Frames korrekt zu empfangen.

DSSS für 1 und 2 MBit/s

Für die Codierung der Daten eines Frames für die Übertragung mit 1 oder 2 MBit/s wird das Direct Sequence Spread Spectrum Verfahren (DSSS) verwendet. Ein Bit wird dabei nicht direkt übertragen, stattdessen werden 11 Chips übertragen. Für ein Bit mit dem Wert 1 wird die Chipsequenz „0,1,0,0,1,0,0,0,1,1,1“ übertragen, für ein Bit mit dem Wert 0 die Sequenz „1,0,1,1,0,1,1,1,0,0,0“. Diese Sequenzen werden auch Barker Code genannt. Da statt einem Wert nun 11 Werte pro Bit übertragen werden, erhöht sich die Redundanz ganz erheblich. Somit ist es möglich, auch bei einigen nicht korrekt empfangenen Chips das übertragene Bit dennoch korrekt zu erkennen.

Auch UMTS macht sich dieses Verfahrens, das „spreizen“ genannt wird, für die Erhöhung der Redundanz zunutze. Während bei WLAN jedoch nur ein Endgerät zu einer Zeit sendet (Time Division Multiple Access), ermöglicht das Spreizen bei UMTS zusätzlich die gleichzeitige Datenübertragung von mehrere Endgeräten (Code Division Multiple Access). Bei UMTS werden jedoch,

wie in Kapitel 3 gezeigt wurde, keine festen Sequenzen, sondern variable orthogonale Codes verwendet.

Modulation

Die Barker Chip Sequenz wird anschließend mit dem Differential Binary Phase Shift Keying (DBPSK) Verfahren mit einer Übertragungsgeschwindigkeit von 11 MChips/s übertragen. Dies ergibt somit eine Bitrate von 1 MBit/s. Beim DBPSK Verfahren ändert sich bei jeder Übertragung eines Chips mit dem Wert 1 die Phasenlage des Sinussignals um 180 Grad. Bei einem Chip mit dem Wert 0 hingegen ändert sich die Phasenlage nicht.

Für eine Übertragungsgeschwindigkeit von 2 MBit/s wird statt DBPSK das Differential Quadrature Phase Shift Keying (DQPSK) Verfahren angewandt. Statt einem Chip pro Übertragungsschritt werden hier 2 Chips übertragen. Die 4 (quadrature) möglichen unterschiedlichen Werte (00, 01, 10 oder 11) der 2 Chips werden in diesem Verfahren mit 90 Grad Phasenwechseln pro Übertragungsschritt kodiert.

HR/DSSS für 5.5 und 11 MBit/s mit CCK

Um bei gleicher Bandbreitennutzung noch schnellere Datenraten zu ermöglichen, wurde mit dem 802.11b Standard das Complementary Code Keying (CCK) Verfahren unter dem Namen High Rate DSSS (HR/DSSS) eingeführt. Statt ein Bit statisch in einer 11 Chip Barker Sequenz zu kodieren, werden die Bits beim CCK Verfahren wie folgt übertragen:

Um eine Datenrate von 11 MBit/s zu erhalten, werden die Bits eines Frames wie in Abbildung 4.14 gezeigt, zunächst in 8 Bit Blöcke eingeteilt. Die ersten zwei Bits werden wie beim vorhergehenden Verfahren auch per DQPSK in eine Änderung der Phasenlage in 90 Grad Schritten übertragen.

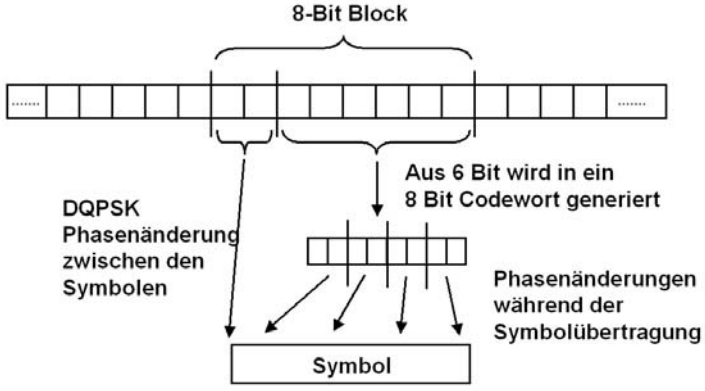

Abb. 4.14: Complementary Code Keying für 11 MBit/s

Aus den restlichen 6 Bits wird danach ein 8 Chip Codewort gebildet. Dieses 8 Chip Codewort wird auch Symbol genannt. Da 6 Bit in einem 8 Bit Symbol kodiert werden, ist auch hier noch eine gewisse Redundanz enthalten. Das so erhaltene Symbol wird wiederum in 4 Teile zu 2 Bits unterteilt und danach in Phasenänderungen kodiert übertragen.

Da die Taktgeschwindigkeit zum 1 bzw. 2 MBit/s Verfahren nicht geändert wurde, können auf diese Weise 11 MBit/s übertragen werden. Nachteil ist jedoch, dass in den übertragenen Informationen wesentlich weniger Redundanz vorhanden ist.

Header immer mit 1 MBit/s

Damit auch Endgeräte mit schlechten Empfangsbedingungen keine Kollisionen erzeugen, muss zumindest der Beginn eines Frames korrekt empfangen werden können. Um dies zu gewährleisten, wird der PLCP Header immer mit einer Geschwindigkeit von 1 MBit/s übertragen, auch wenn der anschließende MAC Frame mit 11 MBit/s übertragen wird. Da auch die Übertragungszeit für den anschließenden MAC Frame im PLCP Header enthalten ist, weis ein empfangendes Endgerät genau, wie lange das Medium besetzt ist, auch wenn die nachfolgenden „schnellen" Bits nicht korrekt empfangen werden können.

Geschwindigkeitsvergleich 802.11b und 10 MBit/s Ethernet

Vergleicht man die tatsächliche Geschwindigkeit eines 11 MBit/s Wireless LANs mit einem 10 MBit/s drahtgebundenen Ethernet, ist ein deutlicher Unterschied sichtbar. Ein 10 MBit/s Ethernet ermöglicht unter idealen Bedingungen einen maximalen Durchsatz von etwa 700-800 kByte/s. Bei WLAN beträgt die maximale Geschwindigkeit beim Datenaustausch zwischen zwei mobilen Endgeräten hingegen ‚nur' 300 kByte/s. Dies liegt an folgenden WLAN Eigenschaften, die in diesem Abschnitt beschrieben wurden:

- Der PLCP Header jedes WLAN Frames wird mit 1 MBit/s gesendet.
- Auf jeden Frame muss der Empfänger mit einem ACK Frame antworten. Auch dies kostet zusätzliche Zeit.
- Während bei Ethernet ein Frame direkt zum Empfänger geschickt wird, muss ein Frame in einem WLAN BSS zuerst an den Access Point geschickt werden. Dieser sendet das Paket dann an den Empfänger. Die Luftschnittstelle wird somit durch das Paket zweimal belegt. Die maximale Datenrate reduziert sich somit um die Hälfte.

4.6.2 IEEE 802.11g mit bis zu 54 MBit/s

Um die Übertragungsgeschwindigkeit weiter zu erhöhen, wurde für die 802.11g Standarderweiterung ein neues Modulationsverfahren mit der Bezeichnung Orthogonal Frequency Division Multiplexing (OFDM), gewählt. Mit dieser Modulation sind bei etwa gleicher Bandbreitennutzung wie bei 802.11b Geschwindigkeiten von bis zu 54 MBit/s möglich. Im Standard wird dieser Physical Layer als Extended-Rate (ERP) PHY bezeichnet.

OFDM

Das OFDM Modulationsverfahren unterscheidet sich grundlegend von den in 802.11b verwendeten Techniken. Wie Abbildung 4.15 vereinfacht zeigt, teilt OFDM den Übertragungskanal von etwa 20 MHz in 52 Unterkanäle (Sub-Channels) auf, über die unabhängig voneinander Daten übertragen werden können.

Die Unterkanäle werden als Orthogonal bezeichnet, weil die Amplituden der Nachbarkanäle an der Mittenfrequenz eines anderen Kanals genau Null sind. Somit haben sie keinen Einfluss auf die Amplitude eines anderen Kanals. Um Daten auf die Unterkanäle aufzumodulieren, wird beim OFDM Verfahren keine Phasenverschiebung wie in den bisherigen Verfahren verwendet, stattdessen werden die Informationen über die Höhe der Amplitude kodiert. Je nach Empfangsqualität des Signals wir die Amplitude in eine unterschiedliche Anzahl von Stufen aufgeteilt.

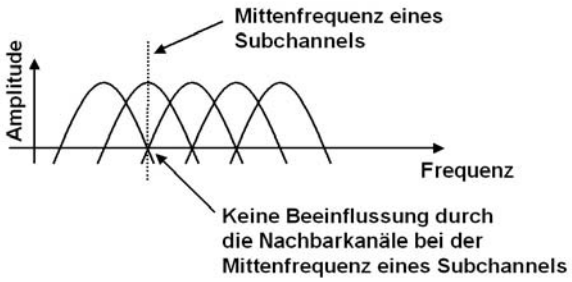

Abb. 4.15: Vereinfachte Darstellung des OFDM Modulationsverfahren

Um das Signal zu demodulieren, wird im Empfänger für jeden Übertragungsschritt eine FFT (Fast Fourier Transformation) Analyse durchgeführt. Mit diesem Verfahren ist es möglich, die Signalenergie (Amplitude) über das Frequenzband zu berechnen. Das Ergebnis einer FFT ist vereinfacht in Abbildung 4.15 gezeigt. Das Frequenzband ist dabei auf der der x-Achse aufgezeichnet

(statt wie bei anderen Verfahren die Zeit), die Amplitude auf der y-Achse.

Die folgende Tabelle zeigt die bei 802.11g möglichen Geschwindigkeiten:

Geschwindigkeit (MBit/s)	Modulation und Coding	Kodierte Bits pro Kanal	Kodierte Bits in 48 Kanälen	Datenbits pro Schritt
6	BPSK, R=1/2	1	48	24
9	BPSK, R=3/4	1	48	36
12	QPSK, R=1/2	2	96	48
18	QPSK, R=3/4	2	96	72
24	16-QAM, R=1/2	4	192	96
36	16-QAM, R=3/4	4	192	144
48	64-QAM, R=2/3	6	288	192
54	64-QAM, R=3/4	6	288	216

Bei günstigen Übertragungsbedingungen kann z.B. das 64 Quadrature Amplitude Modulation (64QAM) Verfahren verwendet werden. Zusammen mit einem ¾ Convolutional Coder (3 Datenbits pro 4 übertragenen Bits) und einer Schrittgeschwindigkeit (Symbol Speed) von 250.000 Symbolen/s wird dadurch eine Geschwindigkeit von 54 MBit/s erreicht (216 Bits pro Schritt * 250.000 Symbole/s = 54 MBit/s). Der Convolutional Coder, auch Faltungskodierer genannt, dient zur Erhöhung der Redundanz und wird auch bei GSM und UMTS verwendet (vgl. Kapitel 1.7.5 und Abb. 1.35).

802.11g ist kompatibel zu 802.11b

802.11g Endgeräte und Access Points sind abwärtskompatibel zu langsameren 802.11b Geräten. Das bedeutet, dass ein 802.11g Access Point auch 802.11b Endgeräte unterstützt, die mit maximal 11 MBit/s senden können. Im umgekehrten Fall können auch 802.11g Endgeräte mit 802.11b Access Points kommunizieren, wobei dann die Datenrate natürlich auf 11 MBit/s begrenzt ist.

Da langsame 802.11b Endgeräte die neue OFDM Modulationsart nicht erkennen können, müssen 802.11g Geräte Schutzmassnahmen ergreifen, sobald sich ein älteres 802.11b Gerät am Netzwerk anmeldet. Während mindestens ein solches Gerät am Access Point anmeldet ist, informiert dieser über einen Parameter in den Beacon Frames alle Teilnehmer des Netzwerkes. 802.11g Geräte senden dann vor dem eigentlichen Datenpaket ein Clear To Send (CTS) Paket. Dieses kann auch von 802.11b Endgeräten

dekodiert werden und enthält die Zeitdauer, die die Luftschnittstelle danach belegt ist. Somit ist sichergestellt, dass 802.11b Endgeräte nicht gleichzeitig mit 802.11g Geräten senden. Außerdem muss der PLCP Header jedes Frames mit 1 MBit/s gesendet werden, um von allen Geräten korrekt erkannt zu werden. Zusammen bringt dies in der Praxis jedoch aufgrund des zusätzlichen Overheads einen Geschwindigkeitsverlust von bis zu 40% mit sich. Aus diesem Grund kann in den meisten Access Points auch ein „G-Only“ Mode eingeschaltet werden, der diesen zusätzlichen Overhead vermeidet, ältere 802.11b Geräte jedoch ausschließt. Dieser Modus ist vor allem für private WLANs sinnvoll, in denen alle Endgeräte zu 802.11g kompatibel sind.

802.11g Geschwindigkeitsvergleich

Unter optimalen Übertragungsbedingungen sind in der Praxis Übertragungsgeschwindigkeiten von etwa 2.500 kByte pro Sekunde möglich. Kommunizieren zwei drahtlose Endgeräte miteinander, reduziert sich die maximale Geschwindigkeit auf etwa 1.200 kByte pro Sekunde, da alle Frames zuerst zum Access Point übertragen werden und erst von dort zum Empfänger weitergeschickt werden. Abhilfe wird hier der 802.11e Standard verschaffen, der am Anfang des Kapitels erwähnt wurde. Im Vergleich zu einem 802.11b Netz mit 600 bzw. 300 kByte/s zwischen zwei mobilen Endgeräten stellt der 802.11g Standard einen beachtlichen Fortschritt dar. Jedoch bleibt der Standard noch weit hinter einem 100 MBit/s drahtgebundenen Ethernet zurück, das mit einer Datenrate von etwa 7.000 kByte/s immer noch etwa um den Faktor 3 schneller ist.

4.6.3 IEEE 802.11a mit bis zu 54 MBit/s

Der 802.11a Standard ist im Wesentlichen mit dem zuvor beschriebenen 802.11g Standard identisch. Dieser Standard sendet jedoch im 5 GHz Bereich und ist somit nicht mit 802.11b Netzen kompatibel. Dies hat jedoch auch den Vorteil, dass die bei 802.11g verwendeten Verfahren für die Rückwärtskompatibilität hier nicht angewandt werden müssen und der PLCP Header statt mit 1 MBit/s mit 6 MBit/s gesendet werden kann. Reine 802.11a Netze sind somit deutlich schneller als gemischte 802.11b/g Netze und haben auch gegenüber reinen 802.11g Netzen einen kleinen Geschwindigkeitsvorteil durch den schnelleren PLCP Header.

4.6.4 IEEE 802.11n mit bis zu 600 MBit/s

Wie in Kapitel 4.6.2 gezeigt, sind mit dem 802.11g Standard Übertragungsgeschwindigkeiten unter günstigen Bedingungen von 20 – 25 MBit/s auf Applikationsebene zu erreichen. Für aktuelle ADSL oder Kabelanschlüsse ist diese Geschwindigkeit ausreichend. Zunehmend sind jedoch auch ADSL2+, VDSL und neue Kabelanschlüsse verfügbar, die höhere Geschwindigkeiten bieten und für die somit ein 802.11g Netzwerk nicht mehr ausreichend ist. Auch für die Anbindung von Endgeräten an zentrale Datei- oder Medienserver im Büro oder im Heimbereich, sowie für neue Anwendungen wie High Definition Video Streaming wird das Wireless LAN Netzwerk schnell zum Nadelöhr. Aus diesen Gründen entschlossen sich eine große Anzahl von Firmen in der 802.11n Arbeitsgruppe den Standard weiterzuentwickeln. Hauptziel für viele Firmen war die Erhöhung der Datenrate. Weitere Ziele waren die Erhöhung der Reichweite und die Einführung von Quality of Service (QoS) Mechanismen, um Applikationen wie Sprachtelefonie über IP (VoIP) oder Videostreaming auch in stark genutzten Drahtlosnetzwerken oder größeren Entfernungen mit guter Qualität zu ermöglichen. Aufgrund der großen Anzahl an Firmen, die sich an der Standardisierung beteiligten, wurde die 802.11n Erweiterung des Wireless LAN Standards sehr umfangreich und enthält zahlreiche optionale Funktionalitäten, die in der Praxis nur von höherwertigen Geräten genutzt werden. Im Folgenden werden deshalb zunächst jene neuen Funktionen des High Througput (HT) Physical Layers (PHY), sowie jene MAC Layer Erweiterungen beschrieben, die im Standard fest vorgeschrieben sind, sowie jene Optionen, die auch im Consumer Segment weite Verbreitung finden.

20 MHz und 40 MHz Kanäle

Einfachstes Mittel um die Geschwindigkeit zu steigern ist die Verbreiterung des Übertragungskanals. Zusätzlich zu 20 MHz Kanälen erlaubt der Standard nun auch die Verwendung von 40 MHz Kanälen. In der Praxis wurde dies schon von vielen Herstellen mit 802.11g proprietär implementiert, Endgeräte unterschiedlicher Hersteller waren jedoch nicht untereinander kompatibel.

Mehr Subkanäle

Für die Datenübertragung werden bei 802.11n statt 52 OFDM Subkanäle wie bei 802.11g nun 56 OFDM Subkanäle in einem 20 MHz Kanal verwendet. Die Bandbreite pro Subkanal ist bei beiden Varianten 312.5 kHz. Dies wurde erreicht, indem jeweils rechts und links im Frequenzband zwei weitere Subkanäle verwendet werden, die bei 802.11g noch nicht genutzt wurden. Die Anzahl der Pilotkanäle, die dem Empfänger das Ausmessen des

Kanals ermöglichen und keine Nutzdaten übertragen, bleibt in beiden Varianten bei vier. In einem 40 MHz Kanal werden insgesamt 114 Subkanäle verwendet, von denen 6 als Pilot verwendet werden.

	20 MHz non-HT (wie 802.11g)	**20 MHz HT**	**40 MHz HT**
Anzahl Carrier	48	52	108 (2* 54)
Anzahl Pilots	4	4	6
Gesamte Anzahl an Carriern	52	56	114 (2 * 57)
Nicht benutzte Carrier in der Mitte	1	1	3

Frame Aggregation

Der ursprüngliche Wireless LAN Standard verlangte nach jeder Übertragung eines Pakets eine Empfangsbestätigung der Gegenstelle durch ein Acknowledgement (ACK) Frame wie zuvor in Abbildung 4.11 gezeigt. Dies ist bei einem unzuverlässigen Übertragungsmedium wichtig, um Übertragungsfehler schnell korrigieren zu können, hat jedoch den Nachteil, dass die Luftschnittstelle nicht sehr effizient genutzt wird. Erst mit 802.11e wurden effizientere Verfahren standardisiert, die in Kapitel 4.8 und Abbildung 4.28 näher beschrieben werden. Um den Overhead weiter zu reduzieren, wurde im 802.11n Standard auf dem MAC Layer ein weiteres Verfahren eingeführt, um Pakete gebündelt übertragen zu können. Dieses Verfahren wird Frame Aggregation genannt. Statt jedes Paket einzeln zu übertragen und danach auf eine Bestätigung zu warten, kann der Sender jetzt Pakete auf dem MAC Layer bis zu einer Gesamtgröße von 65535 Byte bündeln und gemeinsam übertragen. Der Empfänger bestätigt dann das gesamte Bündel mit nur einem ACK Paket. Der Overhead wird dadurch vor allem dann stark minimiert, wenn ein Endgerät große Datenmengen überträgt und somit den Sendepuffer der Netzwerkkarte ständig gefüllt hält. Ein großer Nachteil ist jedoch,

dass bei einem Übertragungsfehler das komplette Paket erneut übertragen werden muss.

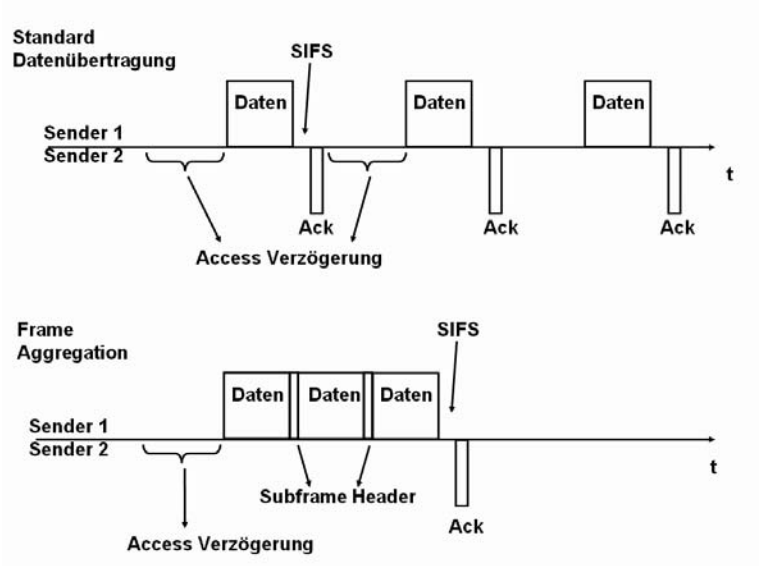

Abb. 4.16: Normale Datenübertragung im Vergleich mit Frame Aggregation

Verkürztes Guard Interval

Ein weiterer Parameter für die Optimierung der Luftschnittstelle ist das OFDM Guard Intervall. Dieses ist bei OFDM Übertragungen notwendig, um die Interferenz zwischen aufeinander folgenden Symbolen abklingen zu lassen. In der Praxis zeigte sich, dass für die meisten Umgebungen ein Guard Intervall von 400 ns pro Symbol statt bisher 800 ns ausreicht. Die Übertragungszeit eines OFDM Symbols verringert sich dadurch deutlich von 4 auf 3.6 Mikrosekunden, d.h. es können im gleichen Zeitraum mehr Symbole, also mehr Daten übertragen werden.

Weniger Fehlerkorrekturbits

Eine weitere Möglichkeit die Geschwindigkeit leicht zu steigern ist die Anzahl der Fehlerkorrekturbits weiter zu senken. Die niedrigste Codierrate in 802.11g Netzwerken ist 3/4, d.h. in 4 Bits sind drei Nutzdatenbits und ein Fehlerkorrekturbit enthalten. Bei 802.11n ist jetzt bei sehr guten Übertragungsbedingungen auch ein 5/6 Codierverfahren erlaubt, das für 5 Nutzdatenbits nur ein Fehlerkorrekturbit enthält.

Alle bisherigen Maßnahmen zusammen steigern die Geschwindigkeit um etwa das 2.5-fache verglichen mit 802.11g auf bis zu 150 MBit/s. Wie bei früheren Standards auch, bleibt auf Grund

der Acknowledgement Frames und anderen Eigenschaften der Luftschnittstelle für Applikationen in etwa die Hälfte dieser Geschwindigkeit übrig.

Verwenden des 2.4 GHz und 5 GHz Bands

Wie am Anfang des Kapitels in Abbildung 4.5 gezeigt, finden im 2.4 GHz ISM Band nur drei unabhängige Netzwerke mit einer Bandbreite von 20 MHz Platz. Besonders in Städten teilen sich jedoch weit mehr Netze das ISM Band. In einer solchen Situation schreibt der Standard vor, dass ein Access Point bei Empfang von Frames anderer Netzwerke in einem der zwei für den 40 MHz Doppelkanal verwendeten Bänder sofort in den 20 MHz Kanalmodus zurückschalten muss und erst 30 Minuten nach dem letzten Auffinden eines Frames eines anderen Netzwerkes den breiteren Kanal wieder aktivieren darf. In der Praxis kann somit der 40 MHz Kanalmodus im 2.4 GHz Band nur in den wenigsten Fällen verwendet werden. Zwar kann der Access Point in einem solchen Fall die Frequenz wechseln und dies den Endgeräten über Channel Switch Announcement Management Frames mitteilen, dies wird jedoch im überfüllten 2.4 GHz Band nur in den seltensten Fällen helfen. Der Standard erlaubt jedoch auch die Verwendung des 5 GHz Bandes, in dem bis zu neun 40 MHz oder achtzehn 20 MHz Netzwerke Platz finden. Da dieser Frequenzbereich bisher nur selten genutzt wird, ist es hier meist ohne Probleme möglich, einen breiteren Kanal zu betreiben. In der Praxis bieten jedoch erst wenige Access Point- und Endgerätehersteller 802.11n Geräte für den 5 GHz Bereich an. Apple ist mit manchen Notebookmodellen und dem Airport Express Access Point eine der wenigen Ausnahmen.

MIMO Spatial Multiplexing

Um die Geschwindigkeit und Reichweite weiter zu steigern, wurden im Standard sowohl für 20 MHz wie auch für 40 MHz Kanäle diverse Multiple Input – Multiple Output (MIMO) Verfahren spezifiziert. Die meisten Endgeräte werden zunächst MIMO Spatial Multiplexing bieten. Dieser MIMO Mode nutzt den Umstand, dass bei der Funkübertragung zwischen einem Sender und einem Empfänger ein Signal an Objekten reflektiert und der Empfänger somit nicht nur ein Signal, sondern mehrere identische sieht, die jedoch aus unterschiedlichen Richtungen kommen. Bei MIMO Spatial Multiplexing haben nun sowohl Sender wie auch Empfänger mehrere Antennen und auch mehrere Sende- bzw. Empfangsstufen. Der Sender sendet nun auf jeder Antenne auf der gleichen Frequenz einen anderen Datenstrom, die dann am Empfänger wieder von getrennten Empfangsstufen empfangen werden. Dies ist in Abbildung 4.17 gezeigt.

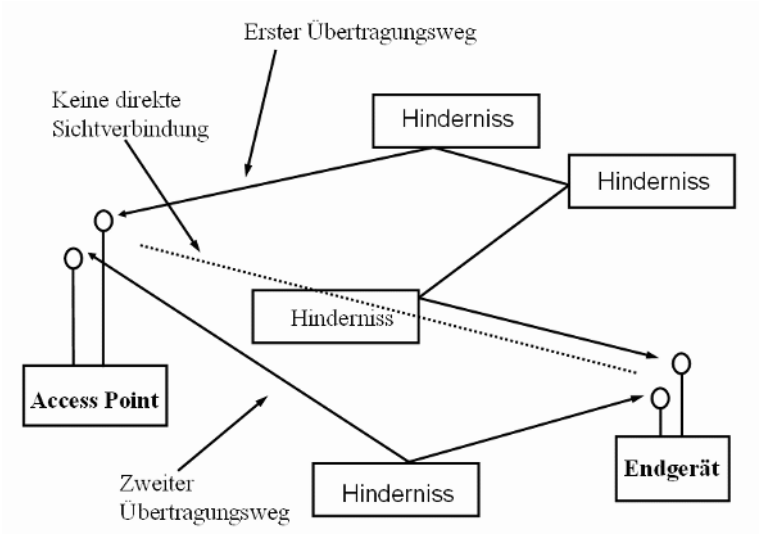

Abb. 4.17: 2x2 MIMO

Im Standard sind bis zu 4 MIMO Kanäle vorgesehen. Access Points müssen mindestens 2 MIMO Kanäle unterstützen, andere 802.11n Endgeräte, also Notebooks, USB Wifi Stecker und Einsteckkarten, sowie kleine Endgeräte wie PDA's, Mobiltelefone, etc., dürfen auch mit nur einen MIMO Pfad ausgestattet sein. Diese Regelung ist sinnvoll, da Access Points meistens nur wenige Restriktionen für Baugröße und Stromaufnahme haben. Kleine batteriebetriebene Geräte jedoch können mit nur einem MIMO Zweig kleiner und stromsparender sein. Zudem werden solche Endgeräte in der Praxis kaum die höheren Geschwindigkeiten benötigen. Da Endgeräte während der Association Prozedur dem Access Point ihre Fähigkeiten mitteilen könne, kann dieser dann z.B. einen 20 MHz Kanal ohne MIMO für ein VoIP Telefon verwenden und für das nächste Paket einen 40 MHz Kanal mit zwei MIMO Zweigen.

In der Praxis gibt es zur Zeit Geräte mit zwei Sende/Empfangseinheiten, was im günstigsten Fall die Datenrate gegenüber einem Single Input / Single Output (SISO) Endgerät verdoppelt. An dieser Stelle sei angemerkt, dass auch manche 802.11g Access Points über zwei Antennen verfügen. Diese haben jedoch nur eine Sende/Empfangseinheit und entscheiden auf Grund der Empfangslage, welche der beiden Antennen verwendet werden soll.

Insgesamt gibt es auf Grund der zahlreichen Variablen wie Anzahl der MIMO Kanäle, langer oder kurzer Guard Time, Modulation und Kodierung nun 77 mögliche Kombinationen, die zu unterschiedlichen Übertragungsgeschwindigkeiten führen. Die nachfolgende Tabelle zeigt exemplarisch einige Möglichkeiten.

	20 MHz, kein MIMO	20 MHz, 2 MIMO Streams	40 MHz 2 MIMO Streams
802.11b	1, 2, 5.5, 11 MBit/s		
802.11g	1, 2, 6, 9, 12, 18, 24, 36, 48, 54 MBit/s		
802.11n, GI 800ns	6.5, 13, 19.5, 26, 39, 52, 58.5, 65 MBit/s	13, 26, 39, 52, 78, 104, 117, 130 MBit/s	27, 54, 81, 108, 162, 216, 243, 270 MBit/s
802.11n, GI 400ns	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2 MBit/s	14.4, 28.9, 43.3, 57.8, 86.7, 115.6, 130, 144.4 MBit/s	30, 60, 90, 120, 180, 240, 270, 300 MBit/s

Die Tabelle zeigt auch anschaulich den Einfluss der Kanalbündelung und des kürzeren Guard Intervalls (GI). Durch die Kanalbündelung wird die Geschwindigkeit etwas mehr als verdoppelt, da zwischen den zwei Kanälen keine ungenutzten Subkanäle liegen und weniger Pilotkanäle verwendet werden. Der Einfluss des kürzeren Guard Intervalls zeigt sich vor allem bei einem 40 MHz Kanal mit zwei MIMO Streams. Durch das kürzere Guard Intervall kann die maximale Geschwindigkeit von 270 MBit/s auf 300 MBit/s gesteigert werden.

Geschwindigkeit in der Praxis

Zusammen mit den zuvor beschriebenen Verfahren, ergibt sich mit 2x2 MIMO (2 Senderantennen, 2 Empfängerantennen) eine maximale Geschwindigkeitssteigerung gegenüber 802.11g von Faktor 5 auf etwa 300 MBit/s auf der Luftschnittstelle. In einem 4x4 MIMO System, das 4 Antennen sowohl beim Sender als auch beim Empfänger benötigt, ist eine theoretische Maximalgeschwindigkeit von bis zu 600 MBit/s möglich.

In der Praxis erreichen derzeit erhältliche 2x2 MIMO Systeme auf dem Applikationslayer eine maximale Geschwindigkeit zwischen 80 und 110 MBit/s. Dies kann aber nur unter günstigen Bedin-

gungen, also auf kurzer Distanz von wenigen Metern, keine dicken Mauern zwischen den Geräten und im Greenfield Mode erreicht werden. Außerdem muss der Access Point unbedingt Gigabit Ethernet Ports unterstützen, um Datenraten über 100 MBit/s auch tatsächlich weiterleiten zu können. Unter weniger optimalen Bedingungen wählen die Endgeräte automatisch statt einer 64-QAM Modulation eine robustere Modulation (16-QAM, QPSK oder BPSK) und statt einer 5/6 Fehlerkorrektur Kodierung nur 3/4, 2/3 oder 1/2.

QoS

Eine weitere wichtige Eigenschaft von 802.11n zertifizierten Endgeräten ist die vorgeschriebene Implementierung der in 802.11e spezifizierten Quality of Service (QoS) Erweiterungen für die Luftschnittstelle. Mit dieser Erweiterung ist es möglich, dass Applikationen wie Voice over IP bevorzugt behandelt werden. Somit können Telefoniepakete oder Daten von anderen Applikationen, die eine konstante Bandbreite benötigen auch in Perioden mit hoher Netzwerklast (Streaming oder Übertragung von großen Dateien) deterministisch und zur richtigen Zeit übertragen werden. Da QoS in Zukunft eine wichtige Rolle spielen wird, geht Kapitel 4.8 näher auf dieses Thema ein.

HT Capabilities in Beacon und Management Frames

Beacon Frames von 802.11n Access Points enthalten eine Anzahl neuer Parameter. Der erste nennt sich „HT Capabilities“ (Element ID 45) und beschreibt, welche High Througput Funktionen der Access Point unterstützt. Die folgende Liste gibt einen Überblick über die wichtigsten Funktionen:

- Unterstützung des 40 MHz Modus (ja/nein).
- Anzahl der gleichzeitig unterstützten MIMO Streams und mögliche Modulations- und Kodiermodi (MCS).
- Unterstützung der auf 400ns verkürzten Guard Time .
- Ob der optionale MCS Feedback Modus unterstützt wird. Mit diesem kann der Empfänger dem Sender eine Rückmeldung über die zu verwendende Modulation geben und somit die Datenrate optimal an die Übertragungsbedingungen anpassen.
- STBC Diversity Support (siehe unten).
- Power Save Multipoll Support (PSMP), eine verbesserte Stromsparoption.
- Zahlreiche Parameter für das optionale MIMO Beamforming (siehe unten).

- Zahlreiche Parameter für die optionale Unterstützung diverser dynamischer Antennenauswahlverfahren. (siehe unten).

Der zweite neue Parameter in Beacon Frames ist der ‚HT Information' Parameter (Element ID 61). In diesem teilt der Access Point den Endgeräten mit, welche HT Funktionalitäten aktuell verwendet werden dürfen, und welche nicht. In der nachfolgenden Liste sind die wichtigsten Informationen zusammengefasst.

- Ob aktuell ein 40 MHz Kanal verwendet werden darf oder ob Übertragungen auf den 20 MHz Primärkanal limitiert sind.
- Operating Mode: Greenfield, HT-Mixed, Non-Member Protection Mode (Endgeräte, die mit anderen Access Points kommunizieren, senden im gleichen Band).
- Ob es Endgeräte im Netzwerk gibt, die nicht Greenfield Mode kompatibel sind.
- Overlapping BSS Protection: Entdeckt der Access Point Beacon Frames von anderen Access Points im gleichen Frequenzband, die nicht HT fähig sind oder im Mixed Mode arbeiten, kann mit diesem Bit Endgeräten signalisiert werden, ebenfalls den HT-mixed Mode zu aktivieren. Benachbarte Access Points, die dieses Bit sehen, selber jedoch keine nicht-HT Endgeräte beobachten können, müssen keine Sicherungsmaßnahmen treffen. Auf diese Weise wird erreicht, dass HT Netzwerke auf nicht kompatible Netzwerke in der Nähe Rücksicht nehmen, sich dies aber nicht über deren Grenzen hinaus fortsetzt.
- Secondary Beacon: Gibt an, ob dieses Beacon Paket im primären 20 MHz Kanal eines 40 MHz Kanals gesendet wurde, oder im zweiten 20 MHz Kanal.

Zusätzlich zu den Beacon Frames werden die HT Capability und HT Information Parameter von Access Points auch in Association-, Reassociation- und Probe Response Frames gesendet. Endgeräte erhalten somit auch während der Anmeldung und beim Wechsel des Access Points noch einmal zusätzlich alle unterstützten Parameter und die aktuelle Konfiguration.

Außer HT Parameter müssen 802.11n kompatible Access Points auch Informationen für das in der 802.11e Erweiterung spezifi-

zierte Quality of Service Handling in den Beacon Frames übertragen. Weitere Details hierzu in Kapitel 4.8.

Damit der Access Point auch über die Fähigkeiten jedes einzelnen Endgerätes im Netzwerk bescheid weiß, sendet auch ein Endgerät während der Association Prozedur seine „HT Information" an den Access Point. Somit ist es dann möglich, dass der Access Point für ein Endgerät Daten in einem 40 MHz Kanal mit kurzen Guard Intervall und zwei MIMO Streams überträgt, während Daten für ein Gerät mit weniger Fähigkeiten automatisch im 20 MHz Kanal, mit 800ns Guard Intervall und ohne MIMO geschickt werden.

Rückwärtskompatibilität zu 802.11b, g und a

Aufgrund der nötigen Rückwärtskompatibilität zu 802.11b, g und a, sowie den vielen Optionen der 802.11n Erweiterung muss ein Endgerät vor der Übertragung eines Datenpakets aus zahlreichen Optionen wählen. Wird ein Datenpaket an ein 802.11b Endgerät geschickt, kommt die HR/DSSS Modulation zum Einsatz. In Abhängigkeit des Übertragungskanals muss dann noch eine entsprechende Coderate gewählt werden. Für 802.11g Endgeräte wird für die Übertragung eine OFDM Modulation mit weniger Subkanälen (Non-HT Format) als für 802.11n Endgeräte verwendet, sowie ein 802.11g PLCP Header. Bei Übertragungen zwischen zwei 802.11n Geräten kommt ebenfalls die OFDM Modulation zum Einsatz, der PLCP Header ist jedoch kürzer und enthält HT spezifische Informationen (HT Greenfield Mode). Sind im Netzwerk 802.11n und 802.11g Geräte angemeldet (HT-Mixed Mode), wird, wie in Abbildung 4.18 gezeigt, ein entsprechend rückwärtskompatibler PLCP Header gesendet. Dieser kann auch von 802.11g Endgeräten dekodiert werden, umfasst jedoch einige Bytes mehr. Außerdem werden weniger OFDM Subkanäle verwendet. Falls auch 802.11b Endgeräte vorhanden sind, muss zudem noch ein CTS Paket in HR/DSSS Modulation der eigentlichen Übertragung vorangehen. Des Weiteren muss ein 802.11n Endgerät wissen, welche 802.11n Funktionalitäten die Gegenstelle unterstützt. Dies ist notwendig, um die OFDM Modulation entsprechend zu steuern (z.B. kurzes Guard Intervall), die Wahl zwischen einem 20 oder 40 MHz Kanal zu treffen, sowie die Anzahl der MIMO Kanäle und die Codierrate in Abhängigkeit der Kanalqualität zu bestimmen.

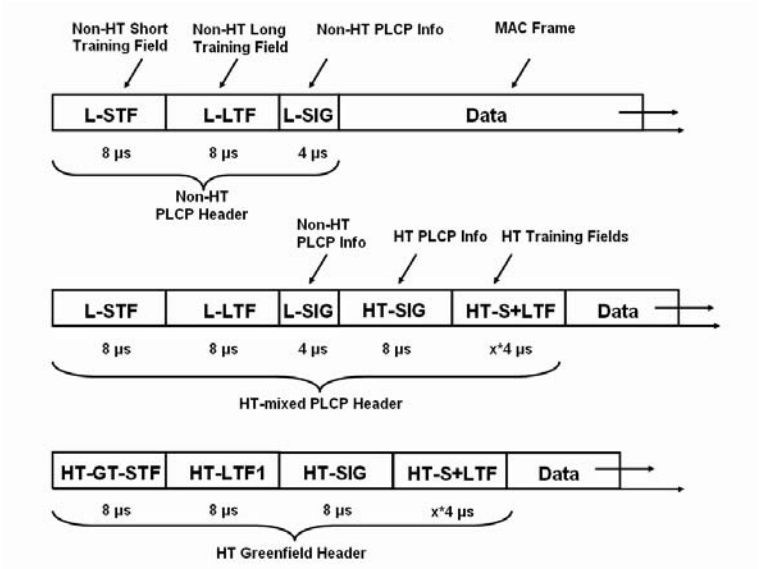

Abb. 4.18: PLCP Headervarianten

Selbst diese umfangreiche Liste berücksichtigt noch nicht zahlreiche weitere optionale 802.11n Funktionen, die nachfolgend beschrieben werden. Da diese Funktionen zum Teil recht komplex sind, ist davon auszugehen, dass die meisten davon anfangs nur in wenigen Endgeräten und Access Points implementiert sind.

Neuer Stromsparmodus: PSMP

Für batteriebetriebene Endgeräte ist es sehr wichtig, dass der Wireless LAN Chip in Zeiten, in denen keine Daten übertragen werden, nur minimale Energie benötigt. Für diesen Zweck gibt es den in Kapitel 4.4 vorgestellten Power Save (PS) Mode, der heute auch von vielen Endgeräten verwendet wird. Dieser Power Save Mode kann aber nicht aktiviert werden, wenn Multimedia Anwendungen wie Voice over IP z.B. alle 20 Millisekunden ein kleines Datenpaket von wenigen Mikrosekunden übertragen und dann für den Rest des Intervalls keine Daten übertragen. Auch wenn keine Daten übertragen werden, benötigt der WLAN Chip trotzdem Energie, da der Funkkanal weiterhin abgehört werden muss. Für solche Anwendungen wurde im 802.11n Standard optional ein zusätzlicher Stromsparmechanismus eingeführt, der Power Save Multi Poll (PSMP) genannt wird. Bei diesem Verfahren beantragt ein Endgerät beim Access Point periodisch Datenpakete einer bestimmten Größe senden und empfangen zu dür-

fen. Der Access Point setzt daraufhin ein PSMP Fenster auf und teilt dem Endgerät mit, zu welchen Zeiten dieses Fenster genutzt werden kann. Das Endgerät schaltet seinen Transciever dann nur während dieses Fensters ein und empfängt seine Datenpakete. Nach dem Downlink Fenster folgt automatisch ein Uplink Fenster, in dem ein Endgerät ohne vorherige Reservierung des Mediums seine Daten schicken kann. Während der restlichen Zeit kann das Endgerät dann seinen Transciever komplett abschalten und somit die Batterielaufzeit erhöhen.

Datenpakete in beide Richtungen enthalten im PSMP Modus nicht nur Nutzdaten, sondern auch Acknowledgement Informationen für die jeweils zuletzt empfangenen Datenpakete. Während eines PSMP Fensters kann ein Endgerät mehrere Datenpakete senden bzw. empfangen. Werden diese einzeln verschickt, muss zwischen den Datenpaketen eine SIFS Pause eingelegt werden oder optional eine kürzere Sendepause, die RIFS (Reduced Inter Frame Space) genannt wird. Datenpakete können auch mit dem weiter oben beschriebenen Frame Aggregation Verfahren in einem Physical Frame gebündelt werden.

Wie in Abbildung 4.19 gezeigt, kann ein PSMP Fenster auch von mehreren Endgeräten geteilt werden. Ein PSMP Frame am Anfang des Intervalls enthält Informationen für alle Endgeräte zu welchen Zeiten jedes einzelne Endgerät im PSMP Fenster Daten empfangen und senden darf. Der Standard gibt vor, dass PSMP Fenster alle 5 bis 40 Millisekunden eingelegt werden sollen, mit einer Granularität von 5 Millisekunden. Für Voice over IP ist z.B. ein Intervall von 20 Millisekunden interessant, da Sprachcodecs üblicherweise Sprachinformationen über diesen Zeitraum komprimieren und dann in einem kleinen Paket übertragen (vgl. Abbildung 1.34).

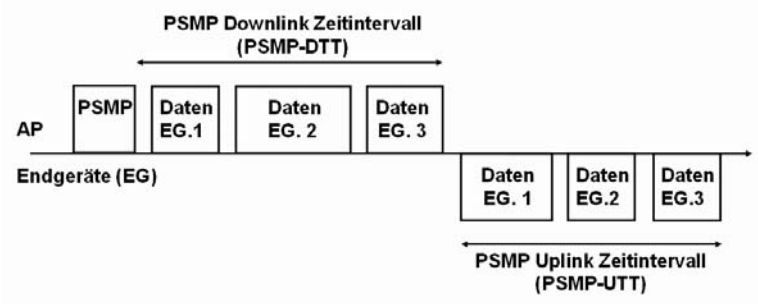

Abb. 4.19: Ein Power Save Multi Poll Fenster (PSMP), in dem mehrere Endgeräte senden und empfangen

Die PSMP Fenster und die für jedes Endgerät vorhandenen Übertragungszeiten sind für eine kontinuierliche und gleich bleibende Übertragung gedacht und so optimiert, dass bei konstanter Nutzung möglichst wenig Bandbreite ungenutzt bleibt. Nun kann es jedoch sein, dass ein Endgerät kurzzeitig mehr Bandbreite benötigt oder ein Paket aufgrund eines Übertragungsfehlers erneut übertragen werden muss. Dies kann dann nicht im normalen Zeitfenster geschehen, da für solche zusätzlichen Übertragungen kein Platz vorhanden ist. Für zusätzliche Uplink Kapazität kann das Endgerät deshalb dem Access Point über ein Flag im MAC Header mitteilen, dass zusätzliche Bandbreite benötigt wird. Dies ist ähnlich der Funktion des ‚Happy' Bit bei HSUPA (vgl. Kapitel 3.11.1). Der Access Point hat dann die Möglichkeit, an das nächste PSMP Fenster ein weiteres PSMP Fenster direkt anzuhängen und teilt dies im PSMP Frame, das jedem PSMP Fenster voransteht, den Endgeräten entsprechend mit. Tritt ein Übertragungsfehler in Uplink Richtung auf, signalisiert dies der Access Point dem Endgerät durch ein negatives Acknowledgement im nächsten PSMP Downlink Abschnitt und fügt ebenfalls ein PSMP Fenster an.

Weitere Funktionalitäten, die im Zusammenhang mit PSMP interessant sind, ist das Versenden eines Datenpakets ohne anschließendes Acknowledgement. Dies ist z.B. bei VoIP sinnvoll, da es evtl. besser ist ein Datenpaket zu verwerfen, anstatt einen großen Jitter Buffer vorzuhalten. Außerdem hat der Access Point die Möglichkeit, Endgeräten zu signalisieren, dass in diesem Netzwerk nur PSMP taugliche Geräte zugelassen sind. Damit können mehrere Access Points z.B. in einem Büro verteilt werden, von denen dann einer exklusiv spezielle Endgeräte wie z.B. VoIP Telefone bedient, während andere Access Points sich um Notebooks und andere Endgeräte kümmern.

MIMO Power Save Modi

Eine weitere Stromsparfunktion wurde im 802.11n Standard für MIMO Spatial Multiplexing (SM) fähige Endgeräte eingeführt. Auch wenn keine Daten übertragen werden, müssen diese im Standardmodus ständig mehrere Empfänger bereithalten, da der Access Point ihnen ja zu jeder Zeit ein Paket schicken kann. Um die Stromaufnahme für batteriebetriebene Geräte zu reduzieren, wurden zwei optionale MIMO SM Power Save Modi spezifiziert. Im statischen Modus signalisiert ein Endgerät einem Access Point über eine „SM Power Save Management Action Frame" Nachricht, wenn es den SM Power Save Modus an- oder abschaltet. Zusätz-

lich gibt es auch SM Power Save Bits im HT Capabilities Parameter, die ein Endgerät während der Association Prozedur verwenden kann, um dem Access Point mitzuteilen, dass es aktuell nur Single Stream Übertragungen zulässt. Des Weiteren gibt es auch einen dynamischen SM Power Save Modus. Hier schaltet das Endgerät alle zusätzlichen Empfänger ab und arbeitet im Single Stream Modus. Das Endgerät aktiviert seinen MIMO Modus wieder automatisch, sobald der Access Point das Endgerät mit einem Paket wie z.B. eine RTS/CTS Sequenz im Single Stream Modus adressiert. Alle nachfolgenden Frames schickt der Access Point ohne weitere Vereinbarung dann mit mehreren MIMO Streams.

MIMO Spatial Multiplexing steigert zwar die Datenrate, nicht jedoch die Reichweite eines Netzwerkes. Deshalb gibt es im Standard optional weitere Möglichkeiten, die zusätzlichen Sende- und Empfangseinheiten (Transciever) statt für erhöhten Durchsatz für eine bessere Reicherweite zu nutzen.

MIMO Beamforming

Eines dieser Verfahren ist das MIMO Beamforming. Hier wird über alle Transciever der gleiche Datenstrom gesendet. Durch geschickte Kombination der Sendeleistung und zeitlichen Versatz der Datenströme kann jedoch eine Richtwirkung erzeugt werden. Somit wird die gesamte Übertragungsleistung nicht gleichmäßig im Raum verteilt, sondern gezielt in der Umgebung des Empfängers konzentriert. Damit Beamforming funktioniert, benötigt der Sender Rückmeldungen vom Empfänger, um den Strahl (Beam) in die richtige Richtung zu dirigieren. Somit müssen sowohl der Sender als auch der Empfänger MIMO Beamforming unterstützten.

MIMO Diversity: Space Time Block Code (STBC)

Statt Beamforming kann die Reichweite eines Netzwerkes auch mit einem Verfahren gesteigert werden, das ein mathematisches Verfahren namens Space Time Block Code (STBC) nutzt. Unterstützen Sender und Empfänger diesen Modus, wird z.B. in einer 2x2 MIMO Konfiguration auch hier ein einzelner Datenstrom getrennt über zwei Pfade übertragen. STBC kodiert jedoch den Datenstrom für jeden Transmitter unterschiedlich und in einer Weise, dass diese zueinander orthogonal sind. Auf der Empfängerseite erhöht dies den Signal- zu Rauschabstand, was wiederum dabei hilft, die Signalstärke und damit den Durchsatz bei weiter entfernten Endgeräten zu steigern.

Antenna Selection und MRC

Unterstützt eine Gegenstelle keine der optionalen MIMO Funktionalitäten, gibt es für einen Empfänger noch andere optionale Möglichkeiten, die Signalqualität zu steigern. Hat das Endgerät mehrere Antennen, kann es untersuchen, mit welcher Antenne

Daten am besten empfangen werden und verwendet dann diese. In der Praxis kann dies durchaus eine deutliche Signalverbesserung für weiter entfernte Endgeräte bedeuten. Dies lässt sich anschaulich bei Endgeräten mit nur einer Antenne und schlechten Empfangsbedingungen nachvollziehen. Hier reicht bei schlechten Empfangsbedingungen oft schon das manuelle Versetzen der Antenne um wenige Zentimeter um den Empfang zu verbessern. Diese Funktionalität ist nicht 802.11n spezifisch sondern wird auch schon bei 802.11g Access Points eingesetzt, die mehrere Antennen haben. Ein etwas aufwändigeres Verfahren ist das Maximum Ratio Combining (MRC). Hier untersucht der Empfänger den eingehenden Datenstrom auf mehreren Receivern und kombiniert die zwei getrennt empfangenen Signale, um so den Signal zu Rauschabstand zu verbessern.

Welche MIMO Art für welchen Zweck

Für Endgeräte die sich näher am Access Point befinden, ist natürlich das zuerst beschriebene MIMO Spatial Multiplexing das Mittel der Wahl, um die Übertragungsgeschwindigkeit zu steigern. Die Transciever werden dann genutzt, um mehrere Datenströme parallel zu übertragen. Bei weniger günstigen Übertragungsbedingungen sind Beamforming und STBC das bessere Mittel, so sie denn von Sender und Empfänger unterstützt werden. Die damit erreichbaren Datenraten sind natürlich geringer als mit MIMO Spatial Multiplexing, da nur ein Datenstrom verwendet wird. Welches der Verfahren für eine Übertragung angewandt wird, muss der Sender selbständig anhand der Übertragungssituation entscheiden, sowie mit dem Wissen, welche MIMO Arten die Gegenstelle unterstützt. Bei mehreren Endgeräten im Netzwerk können alle Verfahren nebeneinander koexistieren. Ein Gerät mit guten Empfangsbedingungen wird dann vom Access Point mit Spatial Multiplexing bedient, während das nächste Paket an ein weiter entferntes Gerät mit STBC kodiert wird.

An dieser Stelle sei angemerkt, dass in Zukunft auch andere Technologien wie 802.16e WIMAX, HSPA+ und 3GPP LTE alle beschriebenen MIMO Arten unterstützen.

MCS Feedback

Eine weitere optionale Funktionalität, die in der 802.11n Arbeitsgruppe definiert wurde, ist das Modulation and Coding Scheme (MCS) Feedback. Ohne dieses Verfahren müssen Sender anhand der Signalstärke des zuletzt vom Empfänger erhaltenen Paketes oder dessen verwendeten MCS entscheiden, welche Modulation und Kodierung sie für die Übertragung des eigenen Paketes verwenden. Dies ist in der Praxis nicht optimal und führt dazu, dass unter Umständen ein MCS verwendet wird, der die Emp-

fangsbedingungen nicht optimal ausnutzt, sprich die Daten zu langsam überträgt. Mit MCS Feedback wurde eine Möglichkeit geschaffen, dass ein Sender von einem Empfänger Feedback über seine Empfangseigenschaften anfordern kann. Der Empfänger liefert dann Informationen im MAC Header in darauf folgenden Übertragungen implizit zurück.

Klassifizierung in der Praxis

In der Praxis wird es in Zukunft aufgrund der vielen möglichen Optionen schwierig werden, allein anhand der Bezeichnung ‚802.11n' die Leistungsfähigkeit und Effizienz eines Endgerätes zu beurteilen. Es bleibt deshalb abzuwarten, ob die Industrie darauf entsprechend reagiert und für Anwender klare Vergleichskategorien schaffen wird, um sich bei der Anschaffung gezielt für ein Gerät mit bestimmten Eigenschaften entscheiden zu können.

4.7 Wireless LAN Sicherheit

Sicherheit ist bei Wireless LAN vor allem deswegen ein sehr heftig diskutiertes Thema, da die normalen Sicherheitseinstellungen und Verfahren den Anwender nur ungenügend schützen. Im Auslieferungszustand ist die Verschlüsselung in so gut wie jedem Access Point deaktiviert. Wird die Verschlüsselung nicht explizit konfiguriert, kann jedes WLAN fähige Endgerät diesen Access Point ohne vorherige Erlaubnis des Besitzers verwenden. Diese Konfiguration eignet sich vor allem für öffentliche Hotspots, da hier stets wechselnde Teilnehmer einen Hotspot verwenden. Da die Daten aber unverschlüsselt übertragen werden, können diese sehr leicht von anderen abgehört werden. Noch bedenklicher ist diese Konfiguration für private Heimnetzwerke, die über den Access Point einen Zugang zum Internet herstellen. Wurde die Verschlüsselung nicht explizit konfiguriert, können Nachbarn ohne Wissen des Besitzers seine Internetverbindung nutzen. Außerdem ist es anderen möglich, den Datenverkehr abzuhören und so z.B. Passwörter etc. auszuspähen. Da auf alle Rechner des Netzwerks Zugriff besteht, können Angreifer auch direkt Schwachstellen der Betriebssysteme ausnutzen, um Daten auf den Rechnern ausspähen. Wie real diese Möglichkeit ist, zeigte eine Testfahrt. Von zwölf innerhalb von wenigen Minuten gefundenen Access Points wurden fünf ohne Verschlüsselung betrieben.

4.7.1 Wired Equivalent Privacy (WEP)

WEP Verschlüsselung und dessen Schwächen

Um WLAN Netzwerke vor unbefugter Nutzung und die Datenübertragung vor dem Abhören zu schützen, ist die Wired Equivalent Privacy (WEP) Verschlüsselung Teil des 802.11b, g und a Standards. Sie basiert ähnlich wie bei GSM und UMTS auf einem Stream Ciphering Algorithmus (vgl. Abb. 1.37), mit dem die Originaldaten mit einer Ciphersequenz verschlüsselt werden. Die Ciphersequenz wird für jedes Paket mit Hilfe eines Keys und eines Initial Vectors (IV) berechnet. Der Initial Vector ändert sich für jeden Frame und erzeugt somit wechselnde Ciphering Keys. WEP verwendet jedoch im Unterschied zu GSM oder UMTS nur einen Key für alle Anwender. Dies ist das erste große Problem vor allem bei der Verwendung von WLAN Netzwerken in Firmen. Da jeder Anwender den gleichen Schlüssel verwendet und diesen manuell in seinem Endgerät konfigurieren muss, kann dieser nicht geheim gehalten werden. Bei GSM oder UTMS hingegen ist ein individueller Schlüssel in der SIM Karte jedes Teilnehmers gespeichert und kann von dort nicht ausgelesen werden.

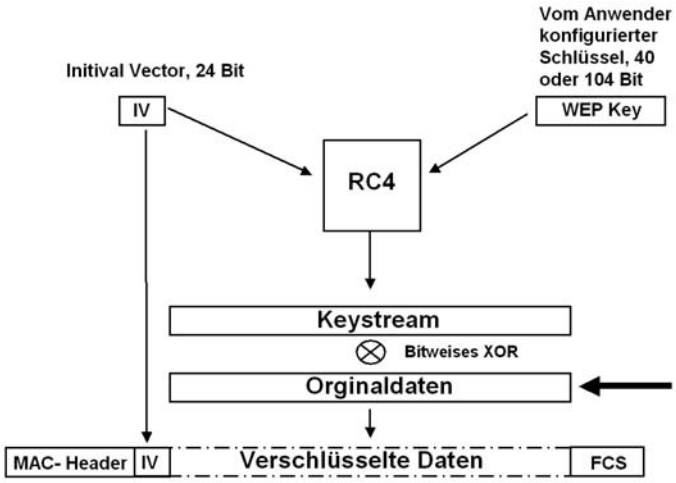

Abb. 4.20: WEP Verschlüsselung

Ein noch schwerwiegenderes Problem ist jedoch, dass der Beginn des verschlüsselten Frames immer die gleiche und somit bekannte Bytefolge des LLC Headers enthält. In Kombination mit bestimmten, im Klartext übertragenen IVs ist es für einen Angreifer möglich, den Schlüssel durch Analyse von etwa 5-6 Millionen

Datenpaketen zu berechnen. Die Länge des WEP Schlüssels spielt dabei nur eine untergeordnete Rolle. Tools, die dies automatisch erledigen, sind im Internet frei erhältlich, der Angreifer muss sich also lediglich in Reichweite des Netzwerkes aufhalten. Die Zahl der benötigten Pakete hört sich zunächst sehr groß an. Nimmt man für eine grobe Abschätzung jedoch an, dass jedes dieser 5 Millionen Datenpakete 300 Bytes an Nutzdaten enthält, so kann der Schlüssel durch Abhören von 5.000.000 Pakete * 0.3 kByte = 1.5 GByte an Daten ermittelt werden. Je nach Last des Netzwerkes lies sich somit der Schlüssel mit ersten Programmen in einem Zeitraum von mehreren Wochen bis hin zu wenigen Stunden errechnen. Im Laufe er Zeit wurden die automatisierten Tools zum Errechnen des Schlüssels immer ausgefeilter. Mittlerweile können diese in bestimmten Fällen durch erneutes Senden von Paketen, die zuvor abgehört wurden, Antwortpakete erzeugen. Somit sind diese Tools nicht mehr auf passives Abhören angewiesen, sondern erzeugen die Datenpakete unter Mithilfe des Netzwerkes für ihre Auswertung quasi selber. Somit ist es möglich, unabhängig von der Verkehrslast die Verschlüsselung in sehr kurzer Zeit zu überwinden.

Hide SSID und MAC-Adressen Filterung

Um die Sicherheit eines WLAN Netzwerkes zu erhöhen, bieten heute viele Access Points zwei weitere Sicherheitsmerkmale an: Durch Aktivieren der „Hide SSID“ Funktion sendet der Access Point Beacon Frames mit leerem SSID Feld. Dadurch ist der Access Point nur für Anwender sichtbar, die bei der manuellen Konfiguration ihres Endgeräts die korrekte SSID angeben. Per MAC-Adressen Filter lässt sich bei vielen Access Points außerdem festlegen, welche Endgeräte sich anmelden dürfen. Für Angreifer, die wie oben beschrieben, über das Wissen und die Möglichkeiten verfügen, den WEP Schlüssel zu errechnen, stellen diese Funktionalitäten aber keine großen Hürden da. Zwar wird die SSID durch die „Hide SSID“ Funktion aus den Beacon Frames entfernt, bei der Association Prozedur wird die SSID aber weiterhin unverschlüsselt übertragen. Auch die MAC-Adresse einer WLAN Karte kann von einem Angreifer ohne viel Mühe auf einen Wert geändert werden, die zuvor im Netzwerk beobachtet wurde.

4.7.2 WPA und WPA2 Personal Mode Authentifizierung

Aufgrund der oben beschriebenen Sicherheitsprobleme wurde von der IEEE 802.11i Arbeitsgruppe der 802.1x Standard erarbeitet. Dieser Standard bietet eine Lösung für sämtliche bisher be-

kannt gewordenen Sicherheitsprobleme. Da sich jedoch die Verabschiedung des Standards beträchtlich hinauszögerte, wurde die Industrie ihrerseits selbst aktiv und entwickelte in der Wifi Alliance die Wireless Protected Access (WPA) Spezifikation. WPA enthält alle wichtigen Funktionalitäten von 802.11i und wurde so spezifiziert, dass die neuen Funktionen auch mit Hardware funktionieren, die ursprünglich nur für WEP Verschlüsselung entwickelt wurde.

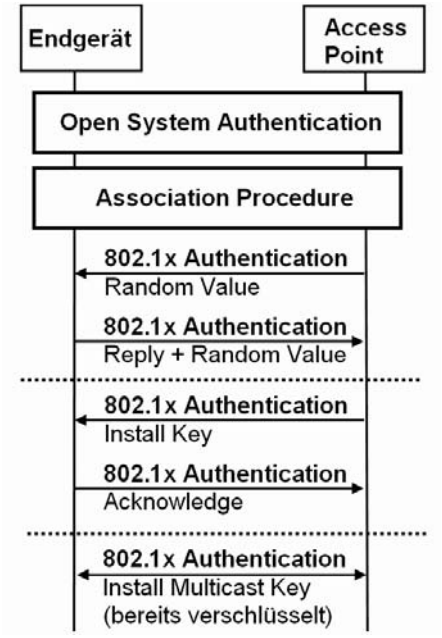

Abb. 4.21: WPA-PSK Authentifizierung und Schlüsselaustausch

Die Schwächen von WEP werden von WPA durch verbesserte Authentifizierung während der Verbindungsaufnahme und eine neue Verschlüsselung gelöst. Wie in Abbildung 4.8 gezeigt, meldet sich ein Teilnehmer bei einem Netzwerk durch eine Pseudo-Authentifizierung und eine Association Prozedur am Netzwerk an. Bei WPA folgt darauf eine weitere Authentifizierung und danach eine sichere Schlüsselübergabe für die Chiffrierung der Nutzdaten. Die erste Authentifizierung ist damit überflüssig, wurde aber dennoch aus Kompatibilitätsgründen beibehalten. Um Endgeräten mitzuteilen, dass ein Netzwerk WPA statt WEP unterstützt, enthalten Beacon Frames einen zusätzlichen WPA Parame-

ter. Dieser informiert Endgeräte, dass ein zusätzlicher Authentifizierungsschritt und Schlüsselaustauch nach der Association Prozedur notewendig ist. Der WPA Parameter enthält auch zusätzliche Informationen über den für die Authentifizierung und Verschlüsselung zu verwendenden Algorithmus. Erste WPA Endgeräte verwendeten zunächst nur TKIP (Temporal Key Integrity Protocol) für die Verschlüsselung. Neuere Endgeräte unterstützen auch AES (Advanced Encryption Standard), welcher bei WPA2 fest vorgeschrieben ist. Weitere Details dazu folgen im Laufe dieses Kapitels.

Abbildung 4.21 zeigt die vier neu hinzugekommenen Schritte für die WPA Pre-Shared Key (PSK) Methode um Endgeräte gegenüber dem Access Point zu authentifizieren und umgekehrt. Pre-Shared Key bedeutet in diesem Zusammenhang, dass im Access Point und im Endgerät das gleiche Passwort hinterlegt wurde. Außerdem einigen sich Endgeräte und Access Point während dieses Prozesses auf ein gemeinsames Schlüsselpaar für die Chiffrierung der Nutzdaten, die Session Keys. In der ersten Nachricht sendet der Access Point eine Zufallszahl an das Endgerät. Dieses verwendet dann die Zufallszahl und das gemeinsame Passwort (Pre-Shared Key), um eine Antwort zu generieren. Das Passwort hat eine Länge von 8 bis 64 Zeichen. Die Antwort wird dann zusammen mit einer weiteren Zufallszahl zurück an den Access Point geschickt. Der Access Point vergleicht im nächsten Schritt die Antwort mit der zuvor selber berechneten Antwort. Diese können nur identisch sein, wenn beide Seiten für die Berechnung der Antwort das gleiche Passwort verwendet haben. Stimmen die Antworten überein, ist das Endgerät authentifiziert. Im nächsten Schritt generiert der Access Point einen Sitzungsschlüssel (Session Key), welcher mit dem gemeinsamen Passwort verschlüsselt wird und zum Endgerät geschickt wird. Das Endgerät entschlüsselt den Sitzungsschlüssel mit dem gemeinsamen Passwort und bestätigt dem Access Point den korrekten Empfang der Nachricht. Diese Bestätigung aktiviert auch implizit die Verschlüsselung in beiden Richtungen. In einem letzten Schritt teilt dann der Access Point dem Endgerät noch den Schlüssel für die Dechiffrierung von Broadcast Frames mit. Diese Nachricht ist bereits verschlüsselt. Während der Sitzungsschlüssel für jedes einzelne Endgerät individuell ist, ist der Broadcast Schlüssel für alle Endgeräte gleich, da ein Broadcast Paket von allen Endgeräten gleichzeitig entschlüsselt werden muss.

Der Vorteil der Verwendung von individuell generierten Sitzungsschlüsseln gegenüber der direkten Verwendung des Pass-

worts für die Verschlüsselung ist, dass dieser während einer laufenden Verbindung geändert werden kann. Dies verhindert so genannte „Brute Force Attacken“, die versuchen, den Schlüssel durch ausprobieren zu erraten. Ein typischer Wert für das Austauschen des Sitzungsschlüssels ist eine Stunde.

4.7.3 WPA und WPA2 Enterprise Mode Authentifizierung

Zusätzlich zur WPA-PSK Authentifizierung, für die ein gemeinsamer Schlüssel (Pre-Shared Key) im Access Point und in den Endgeräten gespeichert werden muss, gibt es bei WPA und WPA2 auch einen Enterprise Mode für Firmen. Hier werden die Passwörter in einem zentralen Authentifizierungsserver, wie in Abbildung 4.22 gezeigt, gespeichert. Dies ermöglicht es Firmen, mehrere Access Points zu betreiben, ohne die Authentifizierungsinformationen in jedem einzelnen Access Point separat vorrätig zu halten. Außerdem ermöglicht diese Methode, Nutzer individuell zu authentifizieren. Somit kann für jeden Benutzer individuell eine Zugangsberechtigung erteilt und auch wieder entzogen werden. Die zwei wichtigsten Authentifizierungsserver sind RADIUS (Remote Authentical Dial In User Service), das normalerweise auf einem Unix Server läuft, oder der Microsoft Authentication Service auf einem Windows Server.

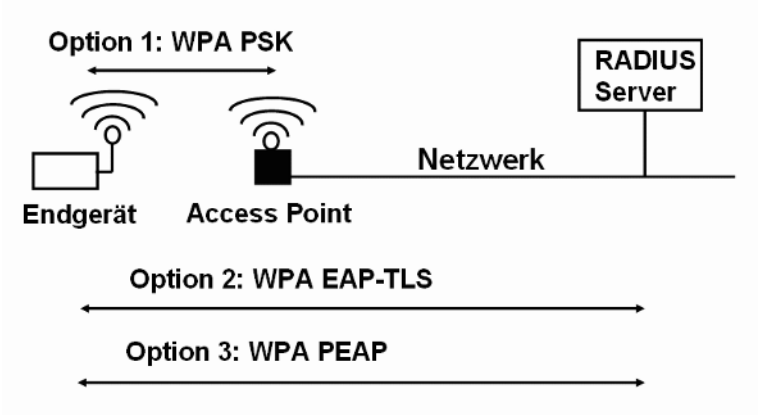

Abb. 4.22: Drei WPA Authentifizierungsmethoden

Aufgrund der verschiedenen Authentifizierungsserver kennt WPA mehrere Authentifizierungsprotokolle. Diese werden Extensible

Authentication Protocols (EAP) genannt. Ein sehr häufig genutztes EAP Protocol ist EAP Transport Layer Security (EAP-TLS) von Haverinen and Salovei, das in RFC 4186 beschrieben ist. Dieses Protokoll verwendet Zertifikate, die im Endgerät und Authentifizierungsserver gespeichert werden. Der wichtigste Teil des Zertifikats sind die öffentlichen Schlüssel (Public Keys) des Endgeräts und des Authentifizierungsservers. Diese Schlüssel werden verwendet, um die Sitzungsschlüssel (Session Keys) zu chiffrieren, die zwischen Endgerät und Netzwerk ausgetauscht werden. Wie zuvor beschrieben, werden dann die Sitzungsschlüssel verwendet, um die Nutzdaten zwischen Access Point und Endgerät zu verschlüsseln.

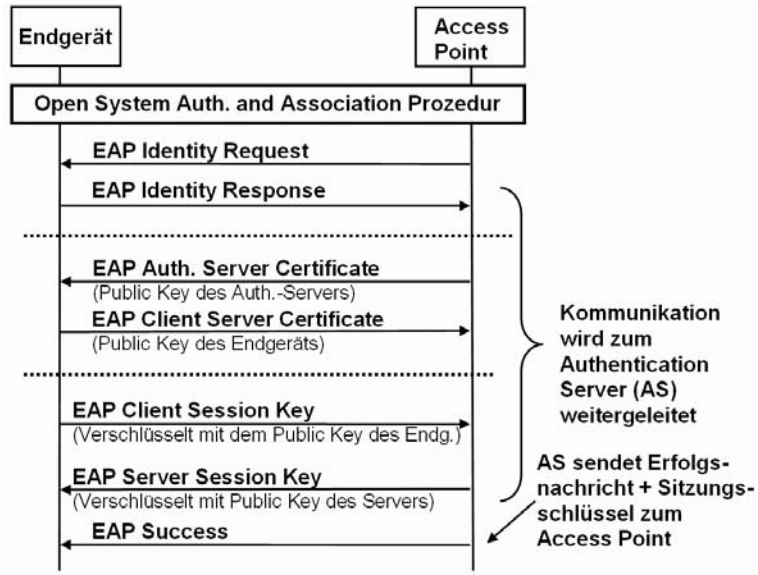

Abb. 4.23: EAP-TLS Authentifizierung

Nachdem der Sitzungsschlüssel mit dem öffentlichen Schlüssel chiffriert wurde, kann dieser nur mit dem privaten Schlüssel (Private Key) der Gegenstelle wieder dechiffriert werden. Dieser Vorgang wird in Abbildung 4.23 gezeigt. Da die privaten Schlüssel niemals zwischen Endgerät und Netzwerk ausgetauscht werden, kann durch Abhören der Verbindung der Session Key nicht kompromitiert werden. Somit kann auch die Übertragung der Nutzdaten später nicht von einem Angreifer dechiffriert werden. Einziger Nachteil der Nutzung von Zertifikaten ist der Umstand,

dass diese einmalig auf dem Endgerät installiert werden müssen. Dies ist etwas komplizierter als einfach ein Passwort zu vergeben, jedoch wesentlich sicherer, wenn die Zertifikate korrekt verteilt und installiert werden. Nicht gezeigt wird in Abbildung 4.23 die Übertragung des Sitzungsschlüssels für Broadcast Pakete, die unmittelbar nach der erfolgreichen Authentifizierung übertragen werden.

In Abbildung 4.23 ist außerdem zu sehen, dass der Access Point in der Authentifizierungsphase nur den Datenaustausch mit dem Authenticationserver zulässt. Erst nachdem die Authentifizierung erfolgreich abgeschlossen wurde, und nachdem der Server dem Access Point die Freigabe erteilt hat, erlaubt der Access Point dem Endgerät freien Zugriff auf das Netzwerk. Die Nutzdaten sind dann über die Luftschnittstelle schon verschlüsselt. Üblicherweise ist das erste Nutzdatenpaket eine DHCP (Dynamic Host Configuraiton Protocol) Anforderung, um eine IP Adresse zu erhalten.

Des Weiteren sei angemerkt, dass die EAP-TLS Authentifizierung große Ähnlichkeit zu TLS und SSL (Secure Socket Layer) hat. Diese Protokolle werden von HTTPS (Secure HTTP) für die Authentifizierung und Generierung von Sitzungsschlüsseln für eine sichere Verbindung zwischen einem Web Server und einem Webbrowser verwendet. Der Hauptunterschied zwischen EAP-TLS und der HTTP TLS Authentifizierungsprozedur ist, dass bei EAP-TLS eine gegenseitige Authentifizierung stattfindet, während sich bei HTTPS TLS nur der Web Server gegenüber dem Webbrowser authentifizieren muss. Aus diesem Grund benötigt der Webbrowser auch kein Zertifikat für den Aufbau einer verschlüsselten Verbindung.

Eine mögliche Alternative zu EAP-TLS ist Protected EAP (PEAP). Während dieses Protokoll seltener verwendet wird, hat PEAP jedoch den Vorteil dass auf der Nutzerseite ein Passwort statt eines Zertifikates verwendet werden kann.

4.7.4 Authentifizierung mit EAP-SIM

Eine wachsende Anzahl von GSM und UMTS Endgeräten haben heute auch ein integriertes Wifi Modul. Dieses Modul kann dann sowohl im heimischen Wifi Netzwerk, im Büro, oder auch über Hotspots für einen schnellen und kostengünstigen Zugang ins Internet sorgen. Mobilfunkbetreiber, die auch ein Wifi Hotspot Netzwerk betreiben, stehen nun vor dem Problem, wie sie ihre Kunden auch in ihrem Wifi Netzwerk authentifizieren können.

Zwar gibt es hier heute auf dem Markt schon einige Lösungen, die jedoch alle eine Interaktion mit dem Nutzer vorsehen. Da dies umständlich und für viele Applikationen hinderlich ist, wurde das EAP-SIM Protokoll in RFC 4186 spezifiziert. Bei dieser Art der Authentifizierung ist wie bei GSM oder UMTS keine Interaktion mit dem Nutzer nötig, da alle Informationen von der SIM Karte abgefragt werden.

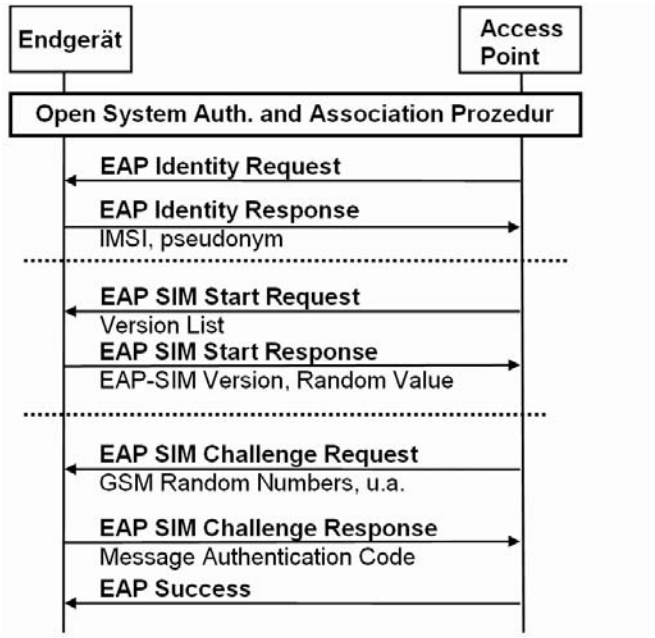

Abb. 4.24: EAP-SIM Authentifizierung

EAP-SIM verwendet die gleiche Authentifizierungsmethode wie bereits im Kapitel über WPA Personal und Enterprise Authentifizierung beschrieben. Abbildung 4.24 zeigt die Nachrichten, die während der Authentifizierung zwischen dem mobilen Endgerät und dem Authenifizierungsserver über einen EAP-SIM kompatiblen Access Point übertragen werden. Nach einer Wifi Open System Authentifizierung und der Association Prozedur startet das Netzwerk die EAP Prozedur durch Senden einer EAP Identiy Request Nachricht, auf die das mobile Endgerät mit einer EAP Identity Response Nachricht antworten muss. Die Identität die in dieser Nachricht zurückgegeben wird besteht aus einem Identity Type Identifier, der IMSI aus der SIM Karte und einem spezifi-

schen Postfix (Anhang) des Mobilfunkbetreibers. Alternativ kann das mobile Endgerät auch eine temporäre Identität (Pseudonym) an das Netzwerk schicken, das während einer früheren Authentifizierung ausgehandelt wurde. Das Pseudonym hat die gleiche Aufgabe wie die TMSI (Temporary Mobile Subscriber Identity) in GSM und UMTS Netzwerken, nämlich der Verschleierung der Identität gegenüber Abhörversuchen auf der Luftschnittstelle, hat jedoch ein anderes Format.

Im nächsten Schritt sendet dann das Netzwerk eine EAP-SIM Start Request Nachricht. Diese enthält Informationen über die unterstützten EAP-SIM Authentifizierungsalgorithmen. Das mobile Endgerät wählt dann einen dieser Algorithmen aus und antwortet mit einer EAP-SIM Start Response Nachricht. Diese enthält eine Zufallszahl, die später im Netzwerk zusammen mit dem geheimen GSM Schlüssel Kc für diverse Berechnungen verwendet wird. Da der geheime GSM Schlüssel Kc sowohl dem Netzwerk als auch der SIM Karte bekannt ist, kann sich auf diese Weise nicht nur das Endgerät gegenüber dem Netzwerk authentifizieren, sondern das Netzwerk auch gegenüber dem Endgerät.

An diesem Punkt verwendet der Authentifizierungsserver die IMSI des Teilnehmers, um vom Home Location Register (HLR) / Authentication Center (AuC) wie im Kapitel 1.6.4 beschrieben Authentication Triplets anzufordern. Das HLR/AuC antwortet auf diese Anfrage mit zwei oder drei Triplets, die jeweils eine Zufallszahl und Kc Chiffrierungsschlüssel enthalten. Diese werden dann verwendet, um die EAP-SIM Sitzungsschlüssel und andere Parameter für den Authentifizierungsprozess zu erzeugen. Diese werden dann in verschlüsselter Form zusammen mit den zwei oder drei GSM Zufallszahlen im Klartext zum mobilen Endgerät in der SIM Challenge Request Nachricht geschickt.

Das Endgerät schickt nach Empfang der Nachricht die GSM Zufallszahlen weiter zur SIM Karte. Die SIM Karte erzeugt mit diesen die GSM Signed Response (SRES) und die GSM Chiffrierschlüssel (Kc), die im folgenden verwendet werden, um die zuvor erhaltenen EAP-SIM Parameter zu entschlüsseln. Stimmt nach der Entschlüsselung die Signed Response vom Netzwerk mit der der SIM Karte überein, ist das Netzwerk authentifiziert und das Endgerät kann eine korrekte Antwort zurückschicken. Im Netzwerk wird diese Nachricht dann verifiziert und im Erfolgsfall eine EAP Success Nachricht an das Endgerät zurückgeschickt. Ab diesem Zeitpunkt hat das Endgerät dann Zugriff auf das Netzwerk.

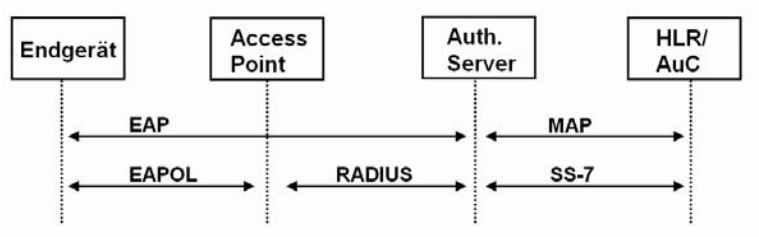

Abb. 4.25: An der EAP-SIM Authentifizierung beteiligte Komponenten

Abbildung 4.25 zeigt die bei der EAP-SIM Authentifizierung beteiligten Komponenten und Protokolle. Links ist das mobile Endgerät dargestellt, das seine EAP Nachrichten über das EAPOL Protokoll sendet. Für die Kommunikation zwischen Access Point und dem Authentifizierungsserver wird das RADIUS (Remote Authentication Dial In User Service) Protokoll verwendet. Der Authentifizierungsserver seinerseits kommuniziert mit dem HLR/AuC über das SS-7 Signalisierungsnetzwerk und dem MAP (Mobile Application Part) Protokoll.

4.7.5 Verschlüsselung mit WPA und WPA2

Um die Verschlüsselung gegenüber WEP zu verbessern, führt WPA das Temporal Key Integrity Protocol (TKIP) ein. Bei WEP wurde ein 24 Bit Initial Vector (IV), der WEP Schlüssel und der RC-4 Algorithmus verwendet, um eine Verschlüsselungssequenz für jedes Paket zu generieren (vgl. Abbildung 4.16). TKIP verwendet nun einen 48 Bit Initial Vector, einen Master Key und den RC-4 Algorithmus, um die Verschlüsselungssequenz für jedes Paket zu erzeugen. Dieses Verfahren ist wesentlich sicherer, da der Initial Vector verlängert wurde und der Master Key ständig (z.B. einmal pro Stunde) zwischen Endgerät und Access Point neu ausgehandelt wird.

Die von WPA verwendete Verschlüsselung entspricht nicht ganz den Anforderungen des 802.11i Standards, wird jedoch trotzdem als sicher angesehen. Vorteil des Verfahrens ist, dass TKIP mit Hardware kompatibel ist, die nur für den Einsatz mit WEP vorgesehen war.

Um Attacken zu verhindern, die eine Schwäche ausnützen, die beim Wiedereinspielen von zuvor abgehörten und leicht veränderten Paketen auftreten, wird der Initial Vector bei jedem Paket

um 1 erhört. WPA kompatible Gerät ignorieren Pakete mit schon verwendeten IV's und sind somit gegen diese Angriffsart immun.

In der Theorie können Access Points gleichzeitig WPA und WEP Endgeräte unterstützen. In der Praxis bieten dies jedoch nur wenige Access Points an. Dies ist auch sinnvoll, da dies die Sicherheit des Systems stark reduzieren würde.

Als zusätzliche Sicherheit führt TKIP auch einen Message Integrity Code (MIC) für jedes Datenpaket ein. Der Prozess für die Erzeugung des MIC wird manchmal auch als ‚Michael' bezeichnet. Im Unterschied zur CRC Prüfsumme, die weiterhin Teil jedes Datenpakets ist, ist wie folgt: Die CRC Prüfsumme wird aus dem Inhalt des Pakets mit einem öffentlich bekannten Algorithmus erzeugt. Der Empfänger kann somit prüfen, ob der Inhalt eines Pakets durch einen Übertragungsfehler geändert wurde. Da der Eingangsparameter und Algorithmus bekannt sind, ist die Prüfsumme jedoch nicht geeignet um zu überprüfen, ob das Paket gezielt durch einen Angreifer verändert wurde, da der Angreifer die Prüfsumme selber ändern könnte. Der MIC andererseits wird ebenfalls mit einem bekannten Algorithmus berechnet, hat jedoch als Eingangsparameter sowohl die Nutzdaten, als auch einen Message Integrity Key, der bei der TKIP Authentifizierung zusammen mit dem Sitzungsschlüssel erzeugt wurde. Einem Angreifer ist es somit nicht möglich, einen korrekten MIC zu berechnen und kann somit auch nicht den Inhalt des Pakets verändern. Bleibt anzumerken, dass sowohl der CRC als auch der MIC im verschlüsselten Teil des Datenpakets untergebracht sind. Um also die CRC Prüfsumme oder den MIC zu verändern, müsste ein Angreifer also zunächst einmal die RC-4 Verschlüsselung in Kombination mit den WPA Sicherheitsvorkehrungen überwinden.

Tritt während der Übertragung ein Fehler auf, sind beim Empfänger sowohl die MIC als auch die CRC Prüfsumme falsch. Der Empfänger eines Datenpaketes kann somit zwischen Übertragungsfehlern und Angriffen auf die Datenintegrität unterscheiden. WPA schreibt vor, dass Endgeräte die mehr als einen Frame pro Minute mit falschem MIC und korrektem CRC empfangen sich vom Netzwerk trennen müssen und danach eine Minute warten, bis sie sich wieder am Netzwerk anmelden. Auf diese Weise werden Attacken auf die Nutzdatenintegrität effektiv verhindert.

Nach der Verabschiedung des 802.11i Standards passte die Wifi Alliance den WPA Zertifizierungsprozess entsprechend an. WPA2

ist eine Implementierung des 802.11i Standards und ist Rückwärtskompatibel zu WPA. Das bedeutet, dass ein WPA2 zertifizierter Access Point auch ‚nur' WPA fähige Endgeräte unterstützt. WPA2 Access Points können auch ältere WEP Endgeräte unterstützen, wenn WPA/WPA2 deaktiviert wird. Zusätzlich zum TKIP Algorithmus, der mit WPA eingeführt wurde, unterstützt WPA2 nun auch die stärkere AES (Advanced Encryption Standard) Verschlüsselung. Wie bei WPA gibt es auch bei WPA2 in zwei Ausführungen: Ist ein Gerät für den „Personal Mode" zertifiziert, erlaubt es eine Authentifizierung mit einem Access Point per Pre-Shared Key (PSK) Verfahren. Für Firmen, in denen oftmals mehrere Access Points verwendet werden, sollte ein Access Point „WPA2 Enterprise Mode" zertifiziert sein. Zusätzlich zum PSK Verfahren unterstützen solche Access Points auch das 802.1x Authentifizierungsframework und können mit externen Authentifizierungsservern kommunizieren, wie dies weiter oben beschrieben wurde.

4.8 IEEE 802.11e und WMM – Quality of Service

Innerhalb von nur wenigen Jahren haben Wireless LANs die Kommunikation in Büros, Arbeits- und Wohnzimmer revolutioniert. Anfangs wurden Netzwerke hauptsächlich für Anwendungen wie Web Browsing und Zugriff auf Fileserver verwendet. Diese benötigen hohe Bandbreiten, stellen jedoch sonst nur geringe Anforderungen an das Übertragungsmedium in Punkto Verzögerungszeit und gleich bleibende Bandbreite. Mehr und mehr werden Wireless LANs heute jedoch auch von Anwendungen wie Voice over IP oder Videostreaming verwendet, die zusätzliche Anforderungen an ein Übertragungsmedium stellen. Videostreaming beispielsweise braucht neben einer hohen Bandbreite ebenso wie Voice over IP eine garantierte Mindestbandbreite und garantierte maximale Verzögerungszeiten beim Kanalzugriff, um Bild- und Tonaussetzer zu verhindern. Dies ist mit den bisher vorgestellten Wireless LAN Standards auch problemlos möglich, solange der Datenverkehr das Netzwerk nicht an seine Leistungsgrenzen bringt. Benötigt jedoch z.B. eine Multimediaübertragung schon einen Großteil der vorhandenen Bandbreite, können weitere Endgeräte, die gleichzeitig spontan Daten z.B. von einem Fileserver oder aus dem Internet abrufen, den Datenfluss der Multimedia Anwendung stören. Aus diesem Grund wurde mit IEEE 802.11e dem Wireless LAN Standard eine Quality of Service (QoS) Komponente hinzugefügt. Wie auch bei

anderen Erweiterungen gibt es Teile, die von einem Endgerät unterstützt werden müssen und andere, die nur optional sind.

WMM und 802.11e

Um die Markteinführung von 802.11e zu beschleunigen, wurde von der Wifi Alliance die Wifi Multi-Media (WMM) Spezifikation auf Basis von 802.11e entwickelt. Ist ein Access Point oder ein Endgerät WMM zertifiziert, enthält es alle von WMM vorgeschriebenen Funktionen und ist mit WMM zertifizierten Geräten anderer Hersteller kompatibel. Um sicherzustellen, dass QoS Erweiterungen in Zukunft in den meisten Geräten implementiert werden, schreibt sowohl der IEEE Standard als auch die 802.11n Zertifizierung der Wifi Alliance vor, dass die WMM QoS Erweiterungen bei 802.11n Endgeräten zum Funktionsumfang gehören müssen. Nachfolgend werden deshalb zunächst die von WMM verwendeten 802.11e Funktionalitäten beschrieben und danach optionale Komponenten, die zusätzlich unterstützt werden können.

DCF

Kern der Quality of Service Erweiterungen ist eine Erweiterung der Distributed Co-ordination Function (DCF), die den Zugriff von Endgeräten auf den Übertragungskanal regelt und in Kapitel 4.5.1 beschrieben ist. DCF schreibt vor, dass ein Endgerät vor der Übertragung eines Pakets eine variable Zeit warten muss, bevor es den Funkkanal belegt um somit Kollisionen von mehreren Endgeräten beim Kanalzugriff zu vermeiden. Die Wartezeit kann beim ersten Versuch bei 802.11b und g bis zu 31 Slots zu je 20 Mikrosekunden betragen. Ermittelt wird dieser Wert durch Erzeugen einer Zufallszahl zwischen 1 und 31. Sollte die Übertragung fehlschlagen, vergrößert sich sie Kanalzugriffswartezeit dann auf 63, 127, usw., bis maximal 1023 Slots, was 20 Millisekunden entspricht.

HCF

802.11e erweitert die DCF zur Hybrid Coordination Function (HCF). HCF umfasst zwei neue Kanalzugriffsverfahren, den Enhanced Distributed Channel Access (EDCA) und den HCF Controled Channel Access (HCCA). Außerdem ist HCF rückwärtskompatibel zu DCF, es können sich also gleichzeitig HCF und nicht HCF fähige Endgeräte im Netzwerk befinden. Im folgenden wird nun zunächst das EDCA Verfahren beschrieben, das Grundlage der WMM Spezifikation ist.

EDCA

Statt allen Endgeräten und allen Datenpaketen ein gleich langes Fenster für das Ermitteln der Zufallszahl zu geben, werden vier Quality of Service Klassen mit je einer Warteschlange eingeführt. Jeder QoS Warteschlange werden dann unterschiedliche Wartezeitfenster für Datenpakete beim Kanalzugriff zugeordnet. WMM

definiert je eine Warteschlange für Voice, Video, Background und Best Effort Daten. Jede Klasse hat folgende variablen Parameter:

- Anzahl der Slots die mindestens gewartet werden muss, bevor ein Datenpaket gesendet werden darf (Arbitration Interframe Space Number, AIFSN).
- Kleinstes Contention Window (CWMin), also die Anzahl der Slots, aus denen ein Zufallsgenerator eine Kanalzugriffswartezeit (Backoff) auswählen kann.
- Grösstes Contention Window (CWMax), die maximale Anzahl der Slots aus denen ein Zufallsgenerator eine Wartezeit nach fehlgeschlagenen Übertragungen auswählen kann.
- Transmit Opportunity (TXOP): Maximale Sendezeit. Granularität des Parameters ist 32 Mikrosekunden.
- Admission Control: Zeigt an, ob Endgeräte sich die Verwendung dieser Klasse genehmigen lassen müssen (siehe unten).

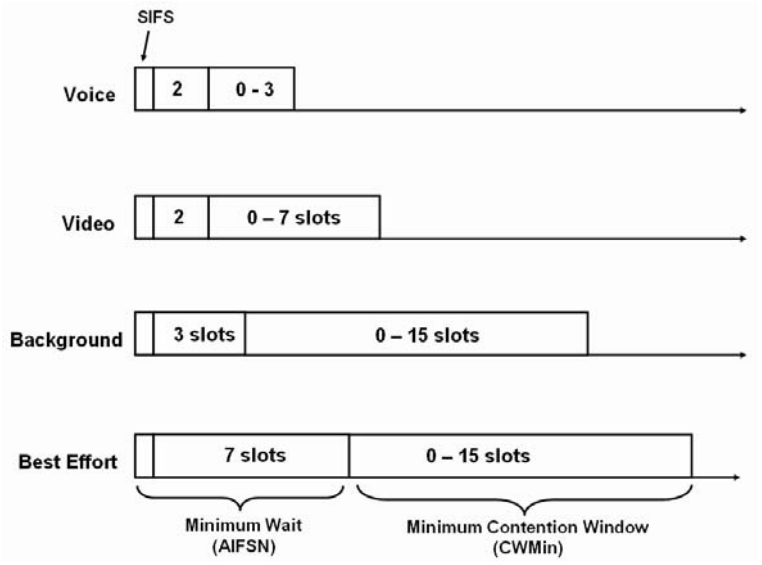

Abb. 4.26: WMM Prioritätsklassen mit beispielhaften Werten für CWMin, CWMax und TXOP

Abbildung 4.26 zeigt, wie diese Werte in der Praxis für die unterschiedlichen Prioritätsklassen gesetzt werden können. Sprachdaten haben sehr hohe Anforderungen an gleich bleibende Verzö-

gerungszeiten. Deshalb ist es in dieser QoS Kategorie wichtig, dass ein Datenpaket bei der Backoff Prozedur bevorzugt wird. Dies wird erreicht, in dem die kleinste Wartezeit (AIFSN) nur 2 Slots und das Contention Window nur maximal 3 Slots lang sind. Die maximale Wartezeit beträgt somit nur 5 Slots. Somit werden diese Datenpakete immer vor Best Effort Daten übertragen, da diese mindestens 7 Slots warten müssen, bevor das Contention Window überhaupt beginnt.

Da die Werte für CWMin, CWMax und TXOP variabel sind und in Access Points von diversen Herstellern auch manuell gesetzt werden können, werden diese über den WMM Parameter in Beacon Frames, sowie in Association- und Probe Response Frames den Endgeräten mitgeteilt.

Diffserv QoS auf Layer 3, QoS Control Field auf Layer 2

Wichtig bei Quality of Service Implementierungen ist auch, dass Applikationen ihre Daten möglichst einfach und von der Art der Netzwerkschnittstelle unabhängig einer QoS Klasse zuordnen können. Bei IP Datenpaketen geschieht dies beispielsweise über das Differentiated Services Feld (DSCP) im IP Header. Wenn von einer Applikation nicht speziell angefordert, ist dieses Feld auf „Default“ gesetzt. Abbildung 4.27 zeigt den IP Header eines Voice over IP Datenpakets, welches dieses Feld auf „Expedited Forwarding“ gesetzt hat. Der Netzwerktreiber der Wireless LAN Karte setzt dieses Feld dann entsprechend in den von 802.11e neu definierten QoS Parameter auf dem Wireless LAN MAC Layer um und stellt das Datenpaket in die Warteschlange für Voice Pakete.

Admission Control

Die Priorisierung von Datenpaketen auf der Luftschnittstelle wird in den meisten Netzwerkumgebungen die Quality of Service Anforderungen erfüllen. Befinden sich jedoch zu viele Anwendungen im Netzwerk die über EDCA eine höhere Priorität für ihre Datenpakete fordern, tritt erneut das schon von DCF bekannte Problem auf, dass die Anzahl der Paketkollisionen steigt. Somit steigt auch die Zugriffszeit auf das Netzwerk sprunghaft an und die Datenrate fällt. Dies kann nur verhindert werden, indem Endgeräte bzw. Anwendungen die Anforderungen eines neuen Datenstroms (z.B. erwartete Datenrate, Paketgröße, etc.) beim Access Point anmelden. Auf diese Weise kann der Access Point weiteren Teilnehmern den Zugang zu einer QoS Klasse verweigern, sobald die Netzwerklast dies nicht mehr zulässt. Diese Endgeräte oder Applikationen müssen dann eine schlechtere QoS Klasse verwenden. Im 802.11 Standard gibt es für diesen Zweck den optionalen Admission Control Mechanismus. In Bea-

con Frames wird dazu den Endgeräten mitgeteilt, ob für eine QoS Klasse eine Zugangskontrolle vom Access Point gefordert wird. Unterstützt ein Endgerät keine Admission Control, darf es eine QoS Klasse die der Access Point in Beacon Frames nur mit Admission Control zulässt, nicht verwenden.

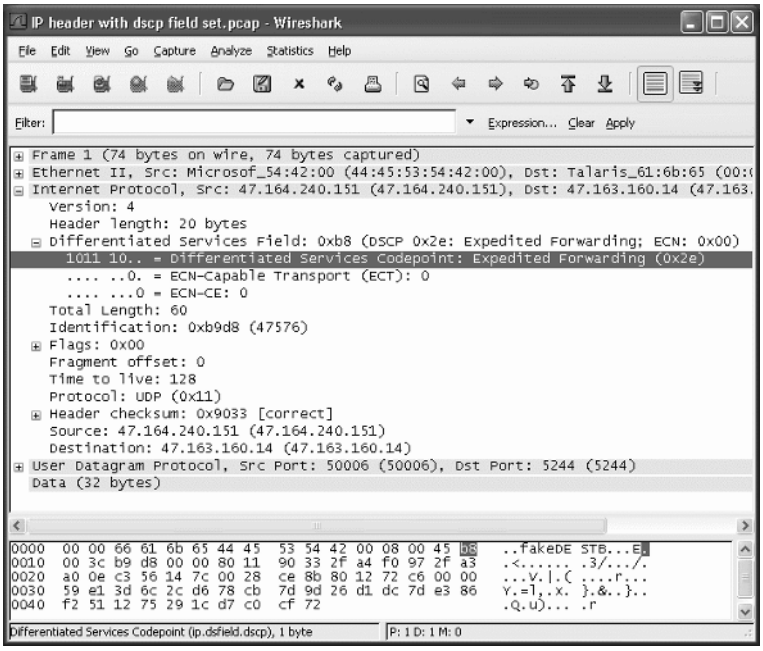

Abb. 4.27: QoS Markierung in einem IP Paket

Um einen neuen Datenstrom anzumelden, sendet ein Endgerät eine Traffic Specification (TSPEC) in einer ADDTS (Add Traffic Specification) Management Nachricht an den Access Point. Dieser überprüft daraufhin ob das Netzwerk den zusätzlichen Anforderungen gerecht werden kann und erteilt bzw. verweigert in einer Antwortnachricht eine Genehmigung. Wie der Access Point diese Prüfung durchführt ist vom Standard nicht definiert. In der Praxis fließen in eine solche Entscheidung viele zum Teil auch dynamische Parameter ein. Ein solch dynamischer Parameter ist z.B. die noch vorhandene Verkehrskapazität, die in einem Netzwerk momentan noch zur Verfügung steht. Dies hängt stark von den Empfangsbedingungen und Fähigkeiten der im Netzwerk befindlichen Endgeräte ab.

Packet Bursting und Block ACK

Neben Quality of Service Funktionalitäten führt die 802.11e Erweiterung auch eine Reihe von optionalen Funktionalitäten ein,

um die Kapazität der Luftschnittstelle besser zu nutzen. Wichtigste Funktionalität hierbei ist das Packet Bursting, das auch schon mit proprietären Erweiterungen des 802.11g Standards implementiert wurde und von 802.11e quasi legalisiert wird. Packet Bursting setzt voraus, dass im Sendepuffer eines Endgerätes mehrere Datenpakete auf die Übertragung warten. Statt nach dem Acknowledgement für ein Datenpaket den DCF Backoff Mechanismus zu verwenden, sendet das Endgerät nach einem Short Interfame Space (SIFS) sofort sein nächstes Datenpaket. Zusätzlich gibt es optional noch die Möglichkeit, zwischen Sender und Empfänger einen Block Acknowledgement Mode zu vereinbaren, falls beide Geräte dies unterstützen. Statt jedes Paket einzeln zu bestätigen, sendet der Empfänger wie in Abbildung 4.28 gezeigt, zuerst eine reihe Datenpakete und fordert dann ein Block Acknowledgement für alle Datenpakete an. Hat der Empfänger alle Datenpakete richtig empfangen, muss dieser nur eine einzige Bestätigung zurückschicken. Dies geschieht entweder sofort (Immediate Block ACK) oder erst etwas verzögert (Delayed Block ACK), um dem Empfänger mehr Zeit für die Analyse der empfangenen Daten zu geben.

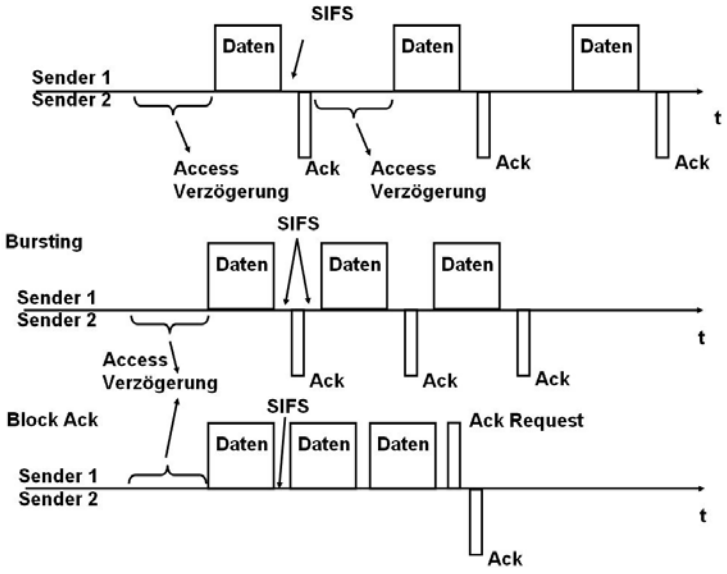

Abb. 4.28: Packet Bursing und Block Acknowledgements

Ob ein Access Point den Block ACK Mechanismus unterstützt, wird den Endgeräten über Beacon Frames im Capability Information Parameter mitgeteilt, während Endgeräte dem Access Point dies während der Association Prozedur mitteilen. Die in Abbildung 4.16 gezeigte Packet Aggregation, die mit 802.11n eingeführt wurde, kann zusätzlich zu Packet Bursting und Block ACK verwendet werden. Somit gibt es nun zahlreiche unterschiedliche Möglichkeiten, das Übertragungsmedium für die Übertragung von großen Datenmengen sehr effizient im Vergleich zum ursprünglichen Verfahren zu verwenden.

Automated Power-Save Delivery (APSD)

Zusätzlich zu dem in Kapitel 4.4 beschriebenen ursprünglichen Power Save (PS) Mode und dem in Kapitel 4.6.2 beschriebenen Power Save Multi Poll (PSMP) Mechanismus, der mit 802.11n spezifiziert wurde, führt der 802.11e Standard einen weiteren Power Save Mechanismums ein, das Automated Power-Save Delivery (APSD). Auch hier gibt es wieder mehrere Optionen. Beim Unscheduled-APSD (U-APSD), der von WMM optional unterstützt wird, vereinbaren Endgerät und Access Point, dass das Endgerät in den Schlafzustand überwechseln kann und dass in dieser Zeit eingehende Pakete im Access Point zwischengespeichert werden. Teil dieser Vereinbarung ist auch, Pakete welcher Prioritätsklasse mit diesem Algorithmus behandelt werden und welche Pakete weiterhin mit dem normalen PS Modus nach dem Aufwachen des Endgeräts zugestellt werden. Zusätzlich wird eine Service Periode (SP) vereinbart, in der das Endgerät nach dem Aufwachen aktiv ist, bevor es dann automatisch wieder in den Schlafzustand wechselt.

Bei U-APSD wird keine genaue Zeit vereinbart, nach der das Endgerät wieder aktiv sein muss. Stattdessen schickt das Endgerät einen Trigger Frame an den Access Point, sobald es wieder empfangsbereit ist. Datenpakete von QoS Klassen, für die U-APSD zuvor aktiviert wurde, werden dann automatisch innerhalb der Service Periode zugestellt. Am Ende der Service Periode wechselt das Endgerät wieder automatisch in den Schlafmodus. Pakete von QoS Klassen, für die kein U-APSD aktiviert wurden, müssen weiterhin mit den für das PS Verfahren nötigen Poll Frames einzeln angefordert werden. Ob ein Access Point U-APSD unterstützt, teilt dieser den Endgeräten im WMM Parameter in den Beacon Frames mit. Auf der Endgeräteseite wird der U-APSD Betrieb während der Association Prozedur über den QoS Capability Parameter vereinbart oder später während des Betriebs über eine Traffic Specification (TSPEC) Nachricht.

Zusätzlich spezifiziert der 802.11e Standard auch ein Scheduled-APSD (S-APSD) Betrieb, welcher allerdings bei WMM nicht vorgesehen ist. Statt eines Trigger Frames vereinbaren hier Endgerät und Access Point ein zyklisches Aktivitätsintervall.

Direct Link Specification (DLS), Direct Link Protocol

Während heute meist Endgeräte über den Access Point direkt mit dem Internet kommunizieren, gibt es mehr und mehr Anwendungen im Heimbereich, wie z.B. Video Streaming zwischen einem Notebook und einem Monitor oder Fernseher, die Daten zwischen zwei Endgeräten im gleichen Netzwerk übertragen. Daten können in einem solchen Fall bisher nicht direkt zwischen den Endgeräten ausgetauscht werden, sondern müssen zunächst zum Access Point geschickt werden und von dort dann weiter zum eigentlichen Empfänger. Da das Datenpaket in einem solchen Fall zweimal über die Luftschnittstelle übertragen werden muss, halbiert sich somit die maximal Bandbreite. Für solche Anwendungen wurde deshalb im 802.11e Standard das Direct Link Protokoll (DLP) spezifiziert. Möchten zwei Endgeräte direkt miteinander kommunizieren, richtet eines der beiden Endgeräte eine Anfrage an den Access Point. Dieser leitet die Anfrage an das andere Endgerät weiter. Befindet sich dieses in Reichweite des ersten Endgerätes und unterstützt ebenfalls das Direct Link Protocol, gibt es eine positive Antwort an den Access Point zurück, der diese wiederum an das anfragende Endgerät weiterleitet. Danach können die zwei Endgeräte dann direkt Verbindung aufnehmen und fortan unter Umgehung des Access Point Datenpakete austauschen.

HCCA

Der Vollständigkeit halber sei an dieser Stelle auch noch der optionale HCF Controlled Channel Access (HCCA) erwähnt. Dieser Scheduling Algorithmus kann statt EDCA verwendet werden, ist jedoch optional und nicht Teil der WMM Spezifikation. Somit ist es unwahrscheinlich, dass HCCA größere Verbreitung finden wird. HCCA ist im Unterschied zu EDCA ein zentraler Scheduling Algorithmus und ermöglicht dem Access Point den Kanalzugriff zu kontrollieren. Dazu sendet der Access Point Poll Frames an jedes Endgerät, dass danach die Möglichkeit hat, in einem vorgegebenen Zeitfenster seine Daten zu übertragen. Da der Access Point die Poll Frames schickt, bevor ein anderes Endgerät die Möglichkeit hat auf den Kanal zuzugreifen, wird auf diese Weise sichergestellt, dass nur Endgeräte die mit einer ADDTS Nachricht eine Traffic Specification TSPEC angefordert haben auch Daten übertragen können. HCCA unterstützt auch die zuvor erwähnten Quality of Service Klassen und kann somit wie EDCA, Paketen

mit bestimmten Quality of Service Anforderungen Priorität einräumen.

Wifi Analyse in der Praxis

Um ein Gefühl zu bekommen, welche der in diesem Kapitel vorgestellten Optionen in der Praxis verwendet werden, gibt es eine Anzahl von Netzwerkanalysetools, die sich für eigene Nachforschungen sehr gut eignen. Ein kostenloses und sehr leistungsfähiges Programm ist beispielsweise Wireshark, erhältlich unter http://www.wireshark.org. Unter Linux kann mit diesem Programm und diversen Wireless LAN Karten die Datenübertragung in einem Wifi Netzwerk aufgezeichnet und analysiert werden. Wireshark ist auch unter Windows erhältlich, für das Aufzeichnen von Wireless LAN Pakete ist jedoch ein spezieller Wireless LAN Adapter nötig. Außerdem bietet die Seite auch über das integrierte Wiki diverse Wifi Traces zum Download an, die ebenfalls einen guten Einblick in die Funktionsweise des Wireless LAN Standards bieten. Eine weitere interessante Alternative zum Aufzeichnen von Wifi Paketen ist die Anschaffung eines Linksys WRT54G Access Points, der sich mit einem freien Linux Betriebssystem namens OpenWRT und Kismet zu einem ausgezeichneten Paketmonitor und Aufzeichnungsgerät umfunktionieren lässt. Weitere Information hierzu finden sich im OpenWRT Wiki auf http://www.openwrt.org

4.9 Vergleich zwischen Wireless LAN und UMTS

Als vor einigen Jahren sowohl Wireless LAN als auch UMTS am Anfang ihrer Entwicklung standen, gab es zahlreiche Diskussion über einen Konkurrenzkampf der Systeme. Zwischenzeitlich sind beide Systeme herangewachsen und haben ihre Anwendungsgebiete gefunden.

Wireless LAN und 3.5G Netzwerke heute

Während Wireless LAN vor allem im Heim- und Bürobereich genutzt wird und in Form von Hotspots auch auf Flughäfen und in Hotels, hat sich UMTS insbesondere auch durch die Weiterentwicklungen wie HSDPA zum großflächigen Hotspot entwickelt, der fast überall verfügbar ist. Da HSDPA heute überall zusammen mit UMTS verfügbar ist, wird nachfolgend nur von UTMS gesprochen. Um vor allem die Konkurrenzsituation zwischen WLAN und UMTS zu untersuchen, widmet sich das letzte Unterkapitel dem Vergleich zwischen Wireless LAN und UMTS für Anwendungen außerhalb von Heim- und Büro.

Geschwindigkeit

Vergleicht man die maximal möglichen Geschwindigkeiten von WLAN und UMTS beim Einsatz außerhalb von Wohnung oder

Büro, ist zunächst ein großer Unterschied festzustellen. Während viele WLAN Hotspots heute noch den 802.11b Standard mit bis zu 11 MBit/s verwenden, werden im Zuge von Erweiterungen und durch Austausch alter Access Points auch 802.11g Geräte mit 54 MBit/s und in Zukunft auch 802.11n Access Points mit noch schnelleren Geschwindigkeiten und der WMM Quality of Service Erweiterung zum Einsatz kommen. Wie in diesem Kapitel gezeigt, können auf der Luftschnittstelle Datenraten von 5, 24 und 100 MBit/s erreicht werden. Demgegenüber stehen aktuelle 3.5G Datenraten von 3.6, 7.2 und 14.4 MBit/s, mit in der Praxis erreichbaren Datenrate von 2 bis 3 MBit/s. Zunächst scheinen deshalb WLAN Hotspots in punkto Geschwindigkeit einen Vorteil zu haben. Bei öffentlichen Hotspots ist jedoch nicht die Wireless LAN Geschwindigkeit der begrenzende Faktor, sondern die Geschwindigkeit der Anbindung des Access Points an das Internet. Vor allem bei kleinen Hotspots werden heute DSL Verbindungen mit einer Downlink Geschwindigkeit von wenigen MBit/s verwendet, die sich alle Anwender eines Hotspots teilen müssen. Die Kapazität des Wireless LANs kann also nicht vollständig ausgenutzt werden. Bei UMTS Netzwerken sind die genannten 2 – 3 MBit/s in der Praxis eine Geschwindigkeit, die sich ebenfalls die meisten Nutzer eines Sektors einer Basisstation teilen müssen. Eine UMTS Basisstation mit 3 Sektoren hat somit eine maximale Kapazität von etwa 9 MBit/s. Wird mehr Kapazität benötigt, können Netzwerkbetreiber auch von ihrem zweiten Frequenzband gebrauch machen und somit die Kapazität nochmals verdoppeln. Die Kapazität der Basisstation steigt somit auf 18 MBit/s an. Ein einzelner Teilnehmer ist jedoch weiterhin mit seiner Übertragungsrate auf einen Sektor und eine Frequenz begrenzt. Für heutige Anwendungen wie Web Browsing, Zugriff auf Unternehmensdaten und Dateiübertragungen reicht diese Bandbreite in den meisten Fällen aus und ermöglicht komfortables Arbeiten. Somit spürt ein Anwender in den meisten Fällen keinen großen Unterschied zwischen der Nutzung eines UMTS Netzwerks und eines WLAN Hotspots. Auch bei der Datenübertragung in Uplink Richtung, also vom Endgerät zu einem Server im Netzwerk liegen beide Netzwerktypen mit 200 kbit/s bis 1 MBit/s etwa gleich auf (ADSL Uplink Geschwindigkeit vs. HSUPA).

Es sollte aber nicht vergessen werden, dass eine Basisstation auch einen größeren geographischen Bereich als ein Wireless LAN Hotspot abdeckt. Zudem muss auch berücksichtigt werden, dass eine Basisstation auch für den Sprachverkehr in diesem Bereich verantwortlich ist und damit die Kapazität für den Daten-

verkehr verringert wird. Sollte deshalb ein Kapazitätsengpass in manchen Gebieten auftreten, können entweder weitere UMTS Basisstationen aufgestellt werden, oder kleine Gebiete mit so genannten Picozellen ausgeleuchtet werden. Diese sind in Größe und Form vergleichbar mit Wireless LAN Access Points.

Roaming und Verfügbarkeit

In den letzten Jahren war zu beobachten, dass Wireless LAN Access Points an vielen öffentlichen Plätzen wie z.B. Hotels, Flughäfen und Bahnhöfen installiert wurden. Auch in Zukunft ist zu erwarten, dass sich dieser Trend fortsetzt. Aufgrund der geringen Reichweite ist aber nicht gewährleistet, dass ein Hotspot immer am gewünschten Ort verfügbar ist. Dies ist z.B. in Hotels ärgerlich, wenn nur einzelne Etagen oder Bereiche mit Wireless LAN ausgestattet sind. Somit wird es weiterhin sorgfältiger Planung bedürfen oder einfach dem Zufall überlassen bleiben, ob am Zielort Wireless LAN zur Verfügung steht.

UMTS Netzwerke haben inzwischen eine große Flächendeckung in vielen Ländern erreicht. Selbst in ländlichen Gebieten ist bereits in vielen Fällen eine UMTS Abdeckung vorhanden, in jedem Fall sind jedoch zumindest GSM, GPRS und in vielen Fällen auch EDGE flächendeckend verfügbar. Durch Roaming Vereinbarungen ist außerdem sichergestellt, dass UMTS Netzwerke zusammen mit GSM in den meisten anderen Ländern der Welt verfügbar ist. Auch bei Wireless LAN Hotspot Betreibern ist zu beobachten, dass diese untereinander Roamingabkommen abschließen und sich z.B. ein französischer Kunde in Deutschland mit seinem Nutzeraccount aus Frankreich an vielen Hotspots anmelden kann. Ob dies jedoch an einem bestimmten Hotspot möglich ist, bleibt heute noch etwas dem Zufall überlassen.

Abrechnung

Da UMTS eine Weiterentwicklung von GSM und GPRS ist, bereitet auch die weltweite Abrechnung (Billing) keine Probleme. Diese Verfahren sind integraler Bestandteil des Netzwerkes. Manche Netzwerkbetreiber bieten seit einiger Zeit auch Tarife für Datenroaming an, so dass auch über UMTS Netzwerke im Ausland in vielen Fällen eine preisliche attraktive Internetnutzung möglich ist. Der Wireless LAN Standard hingegen beinhaltet keine standardisierte Abrechnung. Aufgrund eines fehlenden Standards und der vielen Anbieter gibt es heute zahlreiche Zahlungsmodelle. Diese reichen von Rubbelkarten, die z.B. an der Hotelrezeption gekauft werden können, über Kreditkartenzahlung, bis hin zur Abrechnung auf der GSM oder UMTS Mobilfunkrechnung eines Kunden. Letzteres ist nur möglich, wenn der WLAN Hotspot vom Mobilfunkbetreiber des Kunden betrieben

wird. In den meisten Fällen wird deshalb ein Kunde den Hotspot nicht sofort verwenden können, sondern muss sich erst um die Abrechnung kümmern.

Lawful Intercept

Bisher nicht vollständig geklärt ist die technische Umsetzung des Abhörens durch Behörden und Sicherheitsorganisationen (Lawful Intercept) von Nutzern eines Wireless LAN Hotspots. Für alle Telekommunikationsnetzwerke inklusive GSM, GPRS und UMTS gibt es in den meisten Ländern gesetzliche Bestimmungen und Verfahren, die das Abhören von Teilnehmern durch die Polizei und andere Organisationen regeln. Aufgrund des jungen Marktes ist dies bei Wireless LAN Hotspots bisher noch nicht der Fall und ist aufgrund der heutigen Architektur und Authentifizierung der Teilnehmer auch nicht so ohne weiteres möglich. Bei zunehmendem Erfolg von Wireless LAN ist jedoch anzunehmen, dass auch für Wireless LAN Regelungen eingeführt werden. Dies wird für viele Anbieter einen Umbau der Nutzeridentifizierung und Datenweiterleitung bedeuten.

Mobilität und Handover

Wireless LAN wurde für die Abdeckung von kleinen Flächen konzipiert. Diese kann durch Einsatz von mehreren Access Points, die zusammen ein Extended Service Set (ESS) bilden, begrenzt erweitert werden. Da sich alle Access Points im gleichen IP Subnet befinden müssen (vgl. Kapitel 4.4 und Abb. 4.9), ist somit die maximale Ausdehnung eines Netzes z.B. auf ein Gebäude begrenzt. Für die meisten Wireless LAN Anwendungen ist dies ausreichend, zumal auch ein automatischer Wechsel zwischen den einzelnen Access Points möglich ist. UMTS Netzwerke hingegen sind für die flächendeckende Versorgung konzipiert. Weiterhin legt der Standard, wie in Kapitel 3 gezeigt, besonderen Wert auf einen reibungslosen Handover, um Verbindungen auch über weite Distanzen, lange Zeiträume und hohen Geschwindigkeiten des Benutzers aufrechterhalten zu können. Nur so ist es möglich, mobil („on the move“) zu telefonieren oder mit einem PDA oder Notebook während einer Zugfahrt ständig Kontakt mit dem Internet oder einem Firmennetzwerk zu halten.

Zellgrößen

Auch bei der Zellgröße gibt es große Unterschiede zwischen Wireless LAN und UMTS. Wireless LAN ist aufgrund seiner maximalen Sendeleistung von 0.1 Watt auf eine Zellgröße von wenigen hundert Metern begrenzt. Innerhalb von Gebäuden sinkt die Rechweite aufgrund von Hindernissen wie z.B. Wänden auf wenige Zimmer. UMTS Zellen haben jedoch Reichweiten von mehreren Kilometern, können aber auch für die Versorgung von ein-

zelnen Gebäuden oder Stockwerken wie z.B. Einkaufszentren etc. verwendet werden (Picozellen).

Sicherheit

Wie in diesem Kapitel bereits diskutiert, wurde bei Wireless LAN an Sicherheit und Verschlüsselung erst nachträglich gedacht. Während es für Firmennetzwerke und private Hotspots heute mit WPA und WPA2 gute Sicherheitslösungen gibt, ist die Sicherheit bei öffentlichen Hotspots weiterhin ein Problem. Hier ist fraglich, ob sich WPA Verschlüsselung in Zukunft durchsetzten kann, da das Passwort für jeden Hotspot vom Nutzer manuell eingegeben werden müsste. Heutige Hotspots ohne WPA ermöglichen es Angreifern die sich ebenfalls im Hotspot befinden, mit einfachen Mitteln den Datenverkehr der Teilnehmer abzuhören und aufzuzeichnen. Da ohne zusätzliche Maßnahmen Datenpakete nicht verschlüsselt sind, können Passwörter und andere sensible Daten auf nicht verschlüsselten Webseiten oder Zugangsdaten bei nicht verschlüsselter Kommunikation mit einem eMail Server sehr einfach entwendet werden. Hotspotnutzer sollten deshalb drauf achten, dass sensible Daten nur auf geschützten Webseiten eingegeben werden (https) und für eMail nur verschlüsselte Verbindungen verwendet werden. Zusätzlich sollte grundsätzlich auch der gesamte Datenverkehr über einen verschlüsselten IPSec oder PPTP Tunnel geleitet werden. Dies erfordert jedoch einen nicht unerheblichen Aufwand und Know-How des Anwenders.

In UMTS Netzwerken ist Sicherheit Teil des Systemkonzepts. Nutzer müssen sich deshalb nicht selbst um die Verschlüsselung auf der Luftschnittstelle kümmern. Dies wird vom System automatisch ohne manuelle Eingabe eines Passworts ewährleistet, da der geheime Schlüssel auf der SIM Karte des Teilnehmers gespeichert ist.

Telefonie

Der leitungsvermittelnde Teil eines UMTS Netzwerkes ist speziell für Sprach- und Videotelefonie konzipiert. Diese Dienste sind zwei der wesentlichen Anwendungen von Mobilfunknetzwerken, die von Wireless LAN Hotspots heute nur unzureichend abgedeckt werden. Wie in diesem Kapitel gezeigt, geht der Trend auch bei Sprach- und Videoübertragung weg von der Leitungsvermittlung und hin zu Voice over IP. So ist es heute durchaus möglich, mit Notebooks und so genannten „Soft-Telefonie Clients“ über Wireless LAN zu telefonieren.

Darüber hinaus ist heute ein WLAN Chip schon in vielen Smartphones integriert und Voice over IP Programme ermöglichen das Telefonieren im Wireless LAN. Während dies zuhause oder im Büro meist keine Probleme mehr macht, gibt es in Wire-

less LAN Hotspots noch zwei Stolpersteine. Zum einen erfordern Hotspots normalerweise eine webbasierte Benutzerauthentifizierung. Vor dem Telefonieren muss ein Anwender deshalb zunächst mit dem integrierten Web Browser die Verbindung aktivieren. Ein zweites Problem tritt in Hotspots auf, die stark ausgelastet sind. Da die Distributed Coordination Function (vgl. Kapitel 4.5) nicht geeignet ist, die nötige Bandbreite und Verzögerungszeit für ein Telefongespräch zu garantieren, leidet die Qualität der Verbindung. Zwar sind hier schon Lösungsansätze wie z.B. der 802.11e Standard erkennbar, bis diese jedoch in der Mehrzahl der Wireless LAN Hotspots und Endgeräte verfügbar ist, werden sicher noch einige Jahre vergehen. Aber selbst dann wird Telefonie über Wireless LAN die Telefonie über UMTS oder GSM aufgrund der begrenzten Reichweite und fehlenden Handovers nur ergänzen, nicht jedoch ersetzten können.

Zusammenfassung der WLAN Eigenschaften

Zusammenfassend lässt sich feststellen, dass Wireless LAN eine Hotspottechnologie für Anwender ist, die in einem begrenzen Bereich für eine begrenzte Zeitdauer Zugriff auf das Internet benötigen. Aufgrund der im Vergleich zu UMTS einfachen Technologie sowie dem lizenzfreien Betrieb sind die Kosten für Installation und Betrieb weit geringer als für ein UMTS Netzwerk. Einen schnellen Zugang zum Internet vorausgesetzt, bieten WLAN Hotspots in diesem Umfeld mit seinen sehr schnellen Datenübertragungsraten viele Möglichkeiten. Endgeräte die in WLAN Hotspots verwendet werden sind hauptsächlich Notebooks, PDAs und zunehmend auch Smartphones, die UMTS und Wifi integrieren. An seine technischen Grenzen gelangt Wireless LAN bei mobilen Nutzern in Autos oder Zügen, sowie mit seinem maximalen Abdeckungsbereich in der Größenordnung eines Gebäudes. Im Zusammenhang mit Wireless LAN wird deshalb auch vom „**nomadischen Internet**“ gesprochen, da sich der mobile Nutzer während der Kommunikation in einem Hotspot aufhält und sich dort normalerweise nicht oder nur über kleine Distanzen bewegt.

Zusammenfassung der UMTS Eigenschaften

UMTS richtet sich an die Anforderungen mobiler Nutzer, die unterwegs kommunizieren möchten. Mit seinen schnellen Datentransferraten eignet sich UMTS ebenfalls gut für den Internetzugriff und viele Geschäftsreisende setzten heute auf UMTS Datenkarten um unabhängig vom nächsten WLAN Hotspot kommunizieren zu können. Die komplexe Technologie, die für die Mobilität des Teilnehmers und für Anwendungen wie Telefonie an jedem Ort unerlässlich ist, macht UMTS teurer als Wireless LAN. Dazu tragen auch die hohen Lizenzgebühren bei, die Mo-

bilfunkfirmen bereit waren, bei Frequenzversteigerungen in diversen Ländern zu bezahlen. Hauptanwendungsgebiete für UMTS sind somit neben mobiler Sprach- und Videotelefonie sowie einem Internetzugang für Notebooks auch typische Mobilfunkapplikationen für kleine Endgeräte wie WAP, MMS, eMail und Videostreaming, sowie Web 2.0 Anwendungen wie Podcasts, Einstellen von Bildern bei Diensten wie Flickr, Navigation mit online Kartenzugriff und nicht zu vergessen, Instant Messaging. Im Zusammenhang mit UMTS wird deshalb vom „**mobilen Internet**“ gesprochen, da Kommunikation immer und überall, selbst in Autos und Zügen möglich ist.

4.10 Fragen und Aufgaben

1. Welche Unterschiede gibt es zwischen der Ad-hoc und der BSS Betriebsart eines Wireless LAN?
2. Welche weiteren Funktionen werden oft zusätzlich in einem Wireless LAN Access Point eingebaut?
3. Was ist ein Extended Service Set (ESS)?
4. Welche Aufgabe hat die SSID und in welchen Frames wird diese verwendet?
5. Welche Stromsparmechanismen gibt es in den Wireless LAN Standards?
6. Warum werden in einem Wireless LAN Acknowledgement Frames verwendet?
7. Aus welchen zwei Gründen wird der RTS/CTS Mechanismus bei 802.11g verwendet?
8. Warum gibt es in einem BSS Szenario drei MAC-Adressen in einem Wireless LAN MAC Header?
9. Wie wird dem Empfänger die Datenrate des Nutzdatenpakets mitgeteilt?
10. Welche maximale Datenrate kann bei der Kommunikation zwischen zwei 802.11g Endgeräten in einem BSS erreicht werden?
11. Welche Nachteile hat das DCF Verfahren für Anwendungen wie Telefonie oder Video Streaming?

12. Welche Sicherheitslücken gibt es bei Wired Equivalent Privacy und wie werden diese durch WPA und WPA2 gelöst?
13. Mit welchen Verfahren steigert der 802.11n Standard die Übertragung im Vergleich zum bisherigen Standard?
14. Wie erreicht EDCA eine Priorisierung von Sprachdaten?

Lösungen sind auf der Website zum Buch unter http://www.cm-networks.de zu finden.

5 Bluetooth

Um Geräte wie Computer, Drucker, Mobiltelefone, PDAs oder Headsets miteinander zu verbinden, konnte man bisher zwischen einer Kabel- oder Infrarotverbindung wählen. Kabelverbindungen eigneten sich vor allem für große und stationäre Geräte, während Infrarotverbindungen vor allem für die Kommunikation zwischen kleinen und mobilen Geräten Vorteile hatten. In der Praxis ist jedoch die Handhabung einer Kabel- oder Infrarotverbindung vor allem mit mobilen Geräten oft umständlich und in vielen Situationen auch nicht sehr praktikabel. Die Bluetooth Funktechnologie bietet hier eine ideale Lösung. Um aufzuzeigen, welche Möglichkeiten Bluetooth bietet, gibt Kapitel 5 zunächst einen Überblick über die physikalischen Eigenschaften des Systems, sowie den Aufbau und die Funktionsweise des Protokollstacks. Im weiteren Verlauf führt das Kapitel dann in das Konzept der Bluetooth Profile ein und demonstriert deren praktische Funktionsweise und große Anwendungsvielfalt. Bluetooth und Wireless LAN sind zwei sehr unterschiedliche Systeme, haben aber auch Gemeinsamkeiten. Den Abschluss des Kapitels bildet deshalb ein Vergleich zwischen Bluetooth und Wireless LAN. Dieser zeigt auf, für welche Anwendungen sich welche Technologie am besten eignet.

5.1 Überblick und Anwendungen

Durch die fortschreitende Miniaturisierung finden heute zunehmend kleine elektronische Geräte Einzug in das tägliche Leben. Mit Bluetooth können diese Geräte drahtlos und ohne direkte Sichtverbindung miteinander kommunizieren. Hieraus ergeben sich eine Vielzahl neuer Möglichkeiten und Anwendungen, von denen nachfolgend einige kurz beschrieben werden.

Im Mittelpunkt vieler neuer Anwendungen steht das Mobiltelefon. Zusätzlich zur reinen Sprachtelefonie können Mobiltelefone heute auch für die mobile Datenübertragung genutzt werden. Neben dem eingebauten WAP Browser können auch externe Geräte wie Notebooks oder PDAs das Mobiltelefon als Schnittstelle zum Internet verwenden. Das Mobiltelefon muss sich dazu

nur in der Nähe des Geräts befinden und braucht nicht einmal aus der Tasche geholt zu werden. Das lästige und oft auch umständliche Einstecken von Kabeln oder positionieren der Geräte für eine Infrarotübertragung entfällt komplett. Dies ist vor allem in Zügen, in der U-Bahn oder im Auto von großem Vorteil, wenn nur wenig Platz zur Verfügung steht und die Bewegungsfreiheit eingeschränkt ist.

Ein im Mobiltelefon integriertes Bluetooth Modul eignet sich aber noch zu weit mehr. Termine und Adressen, die im Mobiltelefon gespeichert sind, können schnell und unkompliziert an andere Mobiltelefone, PDAs und Notebooks von Freunden geschickt werden, die sich in der Nähe aufhalten.

Viele Mobiltelefone besitzen heute auch eine eingebaute Fotokamera und ein Dateisystem, um Bilder zwischenzuspeichern. Über Bluetooth können diese Bilder wiederum an Mobiltelefone, PDAs, Notebooks und PCs in der näheren Umgebung schnell und kostenlos geschickt werden.

Das im Mobiltelefon eingebaute Dateisystem eignet sich nicht nur für Fotos, sondern generell für alle Arten von Dateien. Somit ist es auch möglich, Dateien von einem PC oder Notebook in den Speicher eines Mobiltelefons zu sichern und an einem anderen Ort mit einem anderen Endgerät wieder auszulesen. Das Mobiltelefon dient somit als mobiler Datenspeicher.

Auch die Sprachübertragung zwischen einem Mobiltelefon und einem Headset ist eine interessante Anwendung für Bluetooth. Bei einem eingehenden Anruf kann das Mobiltelefon in der Tasche bleiben, da das Gespräch über eine Taste am Headset angenommen werden kann. Bei abgehenden Gesprächen kann die heute bei den meisten Mobiltelefonen übliche Sprachwahl genutzt werden, um mit einem einzigen Knopfdruck eine Verbindung herzustellen.

Bluetooth ist jedoch nicht auf Mobiltelefone begrenzt. Da bei der Entwicklung großen Wert auf schnelle und einfache Konfiguration gelegt wurde, eignet sich Bluetooth auch hervorragend für die Datenübertragung zwischen PCs, Notebooks und PDAs. Ohne langwierige Konfiguration ist es möglich, Dateien, Termine und Notizen zwischen diesen Geräten auszutauschen oder komplette Kalender und Adressbücher zu synchronisieren.

Auch PCs und Peripheriegeräte können per Bluetooth drahtlos verbunden werden. So sind z.B. heute Drucker, Mäuse, Tastatu-

ren und Modems mit Bluetooth Funkmodulen erhältlich, um den „Kabelsalat“ am Schreibtisch zu reduzieren.

Ein weiteres Anwendungsfeld für Bluetooth sind mobile Spielekonsolen. Bei Multiplayer-Spielen kann Bluetooth verwendet werden, um die Spielekonsolen mehrerer Teilnehmer miteinander zu verbinden.

Versionen der Bluetooth Spezifikation

Da heute eine Vielzahl von unterschiedlichen Herstellern Bluetooth Geräte entwickeln, ist eine einwandfreie Interoperabilität grundlegende Voraussetzung für den Erfolg von Bluetooth. Dies wird durch den Bluetooth Standard und Interoperabilitätstests sichergestellt, die „Unplug Fests“ genannt werden. Nachfolgende Tabelle zeigt die bisher erschienenen Protokollversionen. Grundlegend gilt, dass jede neue Version zur alten Version abwärtskompatibel ist. Das bedeutet, dass ein Bluetooth 1.1 Gerät auch mit einem Bluetooth 1.2 Gerät einwandfrei zusammenarbeitet. Teilweise können jedoch Funktionalitäten, die mit einer neuen Version eingeführt wurden, nicht zusammen mit älteren Geräten genutzt werden.

Version	Erschienen	Kommentar
1.0B	Dez. 1999	Erste Bluetooth Version, die aber nur von den Geräten der ersten Generation verwendet wurde.
1.1	Feb. 2001	Diese Version korrigiert eine Reihe von Fehlern und Zweideutigkeiten der vorhergehenden Version des Standards (Errata List). Auf diese Weise wurde die Interoperabilität zwischen Geräten weiter verbessert.
1.2	Nov. 2003	Diese Version führt einige neue Funktionalitäten ein. Die wichtigsten sind: • Schnelleres Auffinden von Bluetooth Geräten im Empfangsbereich. Gefundene Geräte können jetzt auch nach der Empfangsqualität sortiert werden, siehe Kapitel 5.4.2. • Schnellere Verbindungsaufnahme, siehe Kapitel 5.4.2.

		• Adaptive Frequency Hopping (AFH), siehe Kapitel 5.3. • Verbesserte Sprachübertragung z.B. für Headsets (eSCO), siehe Kapitel 5.4.1 und 5.6.4. • Verbesserte Fehlererkennung und Flusskontrolle im L2CAP Protokoll. • Neue Sicherheitsfunktionalität: Anonyme Verbindungsaufnahme.
2.0	2004	Enhanced Data Rate (EDR): Erweitert die Bluetooth 1.2 Spezifikation um schnellere Datenraten. Siehe Kapitel 5.2 und 5.4.1.
2.1	2007	Sicherheits- und Detailverbesserungen. Die wichtigsten sind: • Secure Simple Paring: Verbesserung der Sicherheit und Vereinfachung des Paring Prozesses. Siehe Kapitel 5.5.2 • Sniff-Subrating: Weitere Energiesparoption für aktive Verbindungen mit geringem Datenaufkommen. Siehe Kapitel 5.4.2 • Erroneous Data Reporting für eSCO Pakete. Siehe Kapitel 5.4.1.

5.2 Physikalische Eigenschaften

Bevor die nächsten Abschnitte näher auf die Funktionsweise von Bluetooth eingehen, folgt hier nun zunächst ein Überblick über die wichtigsten technischen Daten:

Übertragungsgeschwindigkeiten

Die maximale Datenrate eines Bluetooth Kanals beträgt 780 kbit/s. Alle Endgeräte, die direkt miteinander kommunizieren, müssen sich diese Datenrate teilen. Die maximale Datenrate für einen einzelnen Teilnehmer ist deshalb von folgenden Faktoren abhängig:

- Anzahl der Teilnehmer, die untereinander gleichzeitig Daten austauschen

- Aktivität der anderen Teilnehmer

Die höchste Geschwindigkeit aus Sicht eines einzelnen Endgerätes kann erreicht werden, wenn nur zwei Geräte miteinander kommunizieren und nur eines der beiden Geräte eine große Datenmenge zu übertragen hat. In diesem Fall beträgt die maximal mögliche Datenrate 723 kbit/s. Nach Abzug des Overheads ergibt dies eine Datenrate von etwa 650 kbit/s. Dem anderen Endgerät bleibt dann jedoch nur eine Datenrate von etwa 57 kbit/s. Diese Situation gibt es in der Praxis z.B. beim Websurfen oder bei der Dateiübertragung recht oft. In beiden Fällen hat eines der beiden Endgeräte sehr viele Daten zu übertragen, während das andere nur Anfragen und Empfangsbestätigungen schickt. Abbildung 5.1 zeigt die möglichen Geschwindigkeiten für dieses Szenario im linken Teil der Grafik.

Möchten beide Teilnehmer möglichst schnell senden, liegt die maximal mögliche Geschwindigkeit für beide bei jeweils etwa 390 kbit/s. Abbildung 5.1 zeigt diese Situation in der Mitte der Grafik.

Kommunizieren mehr als zwei Teilnehmer untereinander, sinkt die maximale Datenrate pro Teilnehmer weiter, falls alle Teilnehmer gleichzeitig mit der maximalen Geschwindigkeit senden wollen. Abbildung 5.1 zeigt dies auf der rechten Seite.

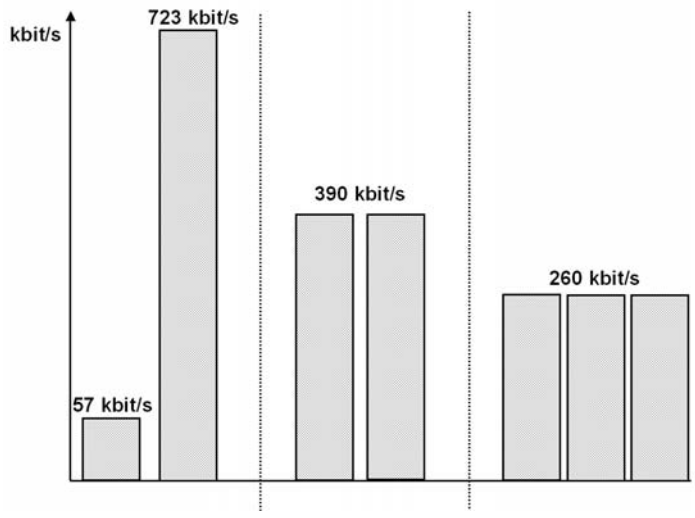

Abb 5.1: Drei Beispiele für die maximale Geschwindigkeit in Abhängigkeit der Anzahl der Teilnehmer und Teilnehmeraktivität

Der im Jahre 2004 erschienene Enhanced Data Rate (EDR) Draft erweitert den Bluetooth Standard mit zusätzlichen Modulationsverfahren und ermöglicht somit Datenraten von bis zu 2.178 MBit/s. Mehr hierzu in Kapitel 5.4.1.

Bandbreitenbedarf

Um diese Übertragungsraten zu erreichen, verwendet Bluetooth einen Kanal im 2.4 GHz ISM (Industrial Scientific and Medical) Band mit einer Bandbreite von 1 MHz. Als Modulationsverfahren wird für normale Pakete das Gaussian Frequency Shift Keying (GFSK) Verfahren verwendet, sowie DQPSK und 8PSK für Enhanced Data Rate Pakete. Die benötigte Bandbreite für eine Bluetooth Übertragung ist verglichen mit Wireless LAN, das für einen Kanal 22 MHz belegt, sehr gering.

Zeitschlitzarchitektur

Um eine bidirektionale Übertragung zu ermöglichen, wird ein Übertragungskanal in Zeitschlitze (Slots) mit einer Länge von je 625 Mikrosekunden unterteilt. Alle Teilnehmer, die untereinander Daten austauschen, verwenden diesen Kanal abwechselnd. Dies ist der Grund für die variablen Übertragungsgeschwindigkeiten in Abbildung 5.1. Hat ein Teilnehmer mehr zu senden, kann er bis zu 5 aufeinander folgende Zeitschlitze belegen, bevor das Senderecht an eine andere Station übergeht. Hat diese nur wenig zu senden, belegt sie den Übertragungskanal nur für einen Zeitschlitz. Auf diese Weise ist es möglich, die Datenrate in beiden Richtungen dynamisch dem Datenaufkommen anzupassen.

Frequency Hopping Spread Spectrum (FHSS)

Da sich Bluetooth das 2.4 GHz ISM Frequenzband mit anderen Funktechnologien wie z.B. Wireless LAN teilt, sendet Bluetooth nicht auf einer festen Frequenz, sondern wechselt nach jedem Paket die Frequenz. Ein Paket kann dabei eine Länge von einem, drei oder fünf Slots haben. Dieses Verfahren wird Frequency Hopping Spread Spectrum (FHSS) genannt. In den meisten Fällen können somit gegenseitige Störungen vermieden werden. Sollte die Übertragung in einem Zeitschlitz trotz allem einmal gestört sein, werden die Daten automatisch erneut übertragen. Bei Paketen mit einer Länge von einem Slot (625 Mikrosekunden) ist somit die Hopping-Frequenz 1600 Hz, werden 5 Slot Pakete verwendet, beträgt die Hopping-Frequenz 320 Hz.

Damit mehrere Bluetooth Verbindungen, die auch Piconetze genannt werden, an einem Ort gleichzeitig betrieben werden können, verwendet jedes Piconetz eine eigene Hopping-Sequenz. Für das Frequency Hopping stehen Bluetooth im ISM-Band 79 Kanäle zur Verfügung. Diese Anzahl genügt, um an einem Ort Wireless LAN Netzwerke und viele Bluetooth Netzwerke gleich-

zeitig und ohne wesentliche gegenseitige Beeinflussung zu betreiben.

Adaptive Frequency Hopping (AFH)

Die gegenseitige Beeinflussung von WLAN und Bluetooth in Form einer überlagerten Übertragung auf der gleichen Frequenz bleibt gering, solange Wireless LAN und Bluetooth nur wenig ausgelastet sind. Wie in Kapitel 4 gezeigt wurde, werden in einem Wireless LAN bei geringer Aktivität außer kurzen Beacon Frames fast keine Datenpakete gesendet. Ist jedoch ein Wireless LAN stark ausgelastet, wird auch ständig gesendet und eine Bandbreite von 25 MHz, also fast ein Drittel der Bluetooth Kanäle, dauerhaft belegt. In einem solchen Fall ist die Anzahl der gegenseitig zerstörten Pakete recht hoch. Aus diesem Grund wurde mit Bluetooth 1.2 das Adaptive Frequency Hopping (AFH) eingeführt. Sind alle Geräte die in einem Piconetz kommunizieren zu Bluetooth 1.2 kompatibel, führt das Piconetz Master-Gerät (vgl. Kapitel 5.3) für alle Kanäle eine Kanalabschätzung (Channel Assessment) durch. Der Link Manager (vgl. Kapitel 5.4.3) legt dazu eine Liste aller Kanäle an (Channel Bitmap), die für das Frequency Hopping nicht verwendet werden sollen. Diese wird dann an alle Endgeräte des Piconetzes weitergegeben. Wie die Kanalabschätzung gemacht werden soll, wird vom Standard nicht vorgeschrieben. Mögliche Verfahren sind z.B. das Received Signal Strength Indication (RSSI) Verfahren oder der Ausschluss eines Kanals aufgrund einer hohen Packet Error Rate (PER). Bei Endgeräten, die Bluetooth und WLAN Funk eingebaut haben, bietet der Bluetooth 1.2 Standard auch die Möglichkeit, dass das Endgerät dem Bluetooth Stack Informationen übergibt, welche Kanäle gemieden werden sollen. Dies ist möglich, da das Endgerät weiß, welcher WLAN Kanal aktuell konfiguriert ist und welche Frequenzen somit vom eingebauten Bluetooth Modul vermieden werden sollten.

Leistungsklassen und Reichweiten

Da Bluetooth speziell für kleine, mobile und batteriebetriebene Geräte konzipiert wurde, sind im Standard drei verschiedene Sendeleistungen spezifiziert. Endgeräte wie z.B. Mobiltelefone gehören meist zur Leistungsklasse (Power Class) 3 und senden mit einer Leistung von bis zu einem Milliwatt. Endgeräte der Klasse 2 senden mit bis zu 2.5 Milliwatt und Endgeräte der Klasse 1 mit bis zu 100 Milliwatt. Nur Endgeräte wie z.B. manche USB Sticks für Notebooks und PCs haben einen Sender der Leistungsklasse 1. Deren Energieverbrauch ist jedoch im Vergleich zu Leistungsklasse 3 sehr hoch und sollte deshalb nur von Geräten verwendet werden, bei denen der Energieverbrauch keine entscheidende Rolle spielt. Die Reichweiten der einzelnen Leis-

tungsklassen sind natürlich auch dementsprechend unterschiedlich. Während Klasse 3 Endgeräte eine maximale Distanz von 10 Metern überbrücken und maximal durch eine Wand senden können, schaffen Klasse 1 Endgeräte bis zu 100 Meter und können auch mehrere Wände durchdringen. Alle Endgeräte, gleich welcher Leistungsklasse, können miteinander kommunizieren. Da jede Kommunikationsverbindung bidirektional ist, bestimmt jedoch das Endgerät mit der geringeren Leistungsklasse die maximal mögliche Reichweite.

Sicherheit und Verschlüsselung

Sicherheitsmechanismen spielen bei Bluetooth eine wichtige Rolle. So wurden in den Standard starke Mechanismen für die Authentifizierung aufgenommen. Diese stellen sicher, dass nur vom Benutzer zugelassene Geräte untereinander kommunizieren können. Auch die Verschlüsselung ist Pflichtbestandteil des Standards und muss in jedem Endgerät integriert sein. Die Verschlüsselungssequenzen sind bei Bluetooth bis zu 128 Bit lang und bilden einen wirksamen Schutz gegen fremdes Abhören.

5.3 Piconetze und das Master Slave Konzept

Piconetze

Bei Bluetooth werden alle Geräte die momentan miteinander kommunizieren in einem so genannten Piconetz zusammengefasst. Die in Abbildung 5.2 beschriebene Frequency Hopping Sequenz des Piconetzes wird durch die Hardwareadresse des Endgerätes berechnet, das als erstes Kontakt zu einem anderen Endgerät aufnimmt und somit das Piconetz aufbaut. Auf diese Weise ist es möglich, viele Piconetze am gleichen Ort ohne gegenseitige Beeinflussung zu betrieben.

Master Slave Konzept

Ein Piconetz kann ein Master- und bis zu sieben Slave Endgeräte umfassen. Dies scheint auf den ersten Blick sehr wenig zu sein. Da die meisten Bluetooth Anwendungen, wie in Kapitel 5.1 gezeigt, nur Punkt zu Punkt Verbindungen sind, ist diese Zahl aber vollkommen ausreichend. Jedes Endgerät kann Master oder Slave eines Piconetzes sein. Per Definition ist immer jenes Endgerät der Master eines Piconetzes, welches dies ursprünglich aufgebaut hat. Folgendes Beispiel verdeutlicht dieses Konzept:

Ein Anwender hat ein Bluetooth fähiges Mobiltelefon und ein Headset. Nachdem diese zwei Geräte anfangs einmal miteinander gekoppelt wurden (Pairing, siehe Kapitel 5.5.1), können diese Geräte jederzeit miteinander Verbindung aufnehmen und somit für die Dauer eines Telefonats ein Piconetz bilden. Nach dem Ende des Telefonats wird die Bluetooth Verbindung zwischen Mobiltelefon und Headset wieder beendet und das Pico-

netz dadurch wieder abgebaut. Bei einem ankommenden Telefongespräch nimmt das Mobiltelefon mit dem Headset Kontakt auf und ist somit der Master der Verbindung. Möchte im umgekehrten Fall der Anwender ein abgehendes Telefonat führen, betätigt er eine Taste am Headset. Das Headset nimmt daraufhin Verbindung mit dem Mobiltelefon auf. In diesem Fall ist nicht das Mobiltelefon, sondern das Headset der Master des neu aufgebauten Piconetzes. Befindet sich ein anderer Anwender in unmittelbarer Nähe, der auch gerade per Bluetooth Headset telefoniert, führt dies nicht zu Problemen, da die Frequency Hopping Sequenzen der beiden Piconetze unterschiedlich sind. Durch die ursprüngliche Kopplung von Headset und Mobiltelefon ist auch sichergestellt, dass jedes Headset sein eigenes Mobiltelefon findet und auch nur mit diesem kommunizieren darf.

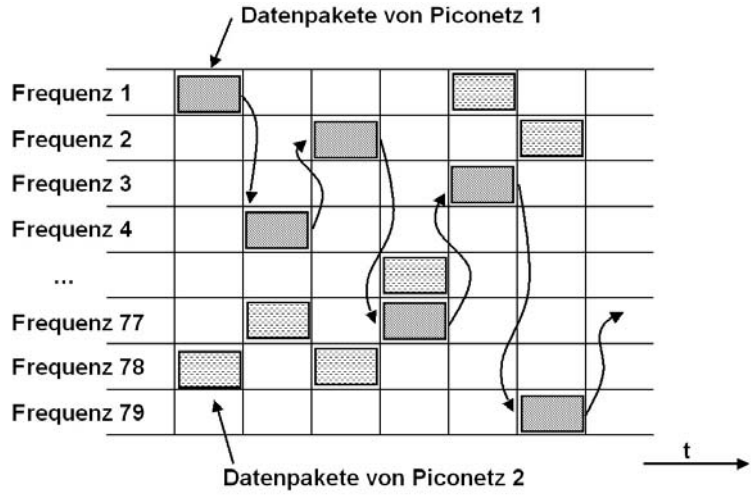

Abb. 5.2: Durch unterschiedliche Hop-Sequenzen können viele Piconetze am gleichen Ort betrieben werden.

Master kontrolliert das Piconetz

Der Master eines Piconetzes hat die Kontrolle, wer zu welchem Zeitpunkt Daten auf dem Kanal übertragen darf. Um einem Slave Endgerät das Senderecht zu erteilen, schickt ihm der Master ein Datenpaket. Das Slave Endgerät wird über eine 3-Bit Adresse im Header des Datenpakets identifiziert, die ihm bei der ersten Kontaktaufnahme zugewiesen wurde. Das Datenpaket des Masters kann je nach Datenaufkommen 1 – 5 Slots lang sein. Hat der Master keine Daten für den Slave, sendet er ein leeres Paket. Unabhängig, ob das Paket Nutzdaten enthält oder nicht, übergibt der Master dem Slave auf diese Weise implizit das Senderecht.

Der Slave kann dann in den nächsten 1 - 5 Slots ein Antwortpaket zurückschicken. Bei Bluetooth 1.1 antwortet der Slave auf der nächsten Frequenz in der Frequency Hopping Abfolge. Bei Bluetooth 1.2 wurde dieses Konzept leicht geändert, der Slave antwortet hier auf der zuvor vom Master verwendeten Frequenz. Hat der Slave keine Daten für den Master, antwortet er trotzdem mit einem leeren Paket als Empfangsbestätigung für das zuvor vom Master eingegangene Paket. Nach spätestens 5 Slots geht das Senderecht wieder automatisch an den Master über, auch wenn der Slave noch weitere Daten in seinem Sendepuffer hat. Danach kann der Master entscheiden, ob er wieder diesem, oder einem anderen Slave das Senderecht erteilt. Empfing der Master in den letzten Datenpaketen keine Nutzdaten und ist auch sein Sendepuffer leer, kann er eine Sendepause von bis zu 800 Slots einlegen, um damit Strom zu sparen. Da ein Slot eine Dauer von 625 Mikrosekunden hat, entsprechen 800 Slots einer Sendepause von 0.5 Sekunden.

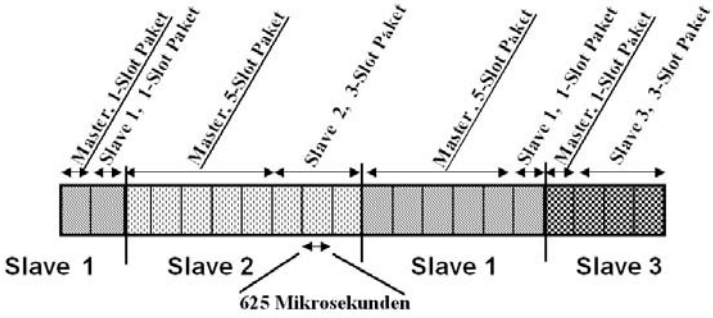

Abb. 5.3: Kommunikation zwischen einem Master und drei Slave Endgeräten.

Master-Slave Rollentausch

Da ein Slave nicht vorhersehen kann, zu welchem Zeitpunkt Datenpakete des Masters eingehen, kann er keine Verbindungen zu weiteren Geräten aufnehmen. In manchen Fällen ist es deshalb notwendig, dass Master und Slave ihre Rollen tauschen können. Diese Funktion ist z.B. notwendig, wenn ein PDA mit einem PC Kontakt aufgenommen hat, um mit ihm Daten zu synchronisieren. Da der PDA die Verbindung zum PC aufgebaut hat, ist er der Master des Piconetzes. Während die Verbindung besteht, möchte der Nutzer des PCs jedoch ein Bild von einem Mobiltelefon zu sich übertragen und muss deshalb zusätzlich eine Verbindung zum Mobiltelefon herstellen. Dies ist aber nur möglich, wenn PDA (Master) und PC (Slave) die Rollen im Piconetz tau-

schen. Diese Prozedur wird auch Master-Slave Role Switch genannt. Nach dem Rollentausch ist der PC der Master des Piconetzes zwischen ihm und dem PDA. So ist es ihm möglich, zusätzlich den Kontakt zum Mobiltelefon aufzubauen, während die Datenübertragung mit dem PDA noch läuft. Durch die Kontaktaufnahme mit dem Mobiltelefon und der Übertragung des Bildes verringert sich jedoch die Datenrate zwischen PC und PDA.

5.4 Der Bluetooth Protokoll Stack

Abbildung 5.4 zeigt die unterschiedlichen Schichten des Bluetooth Protokoll Stacks und dient den nachfolgenden Unterkapiteln als Referenz. Die einzelnen Bluetooth Protokollschichten halten sich nur lose an das 7 Schichten OSI Modell, da manche Bluetooth Layer Aufgaben aus unterschiedlichen OSI Schichten übernehmen.

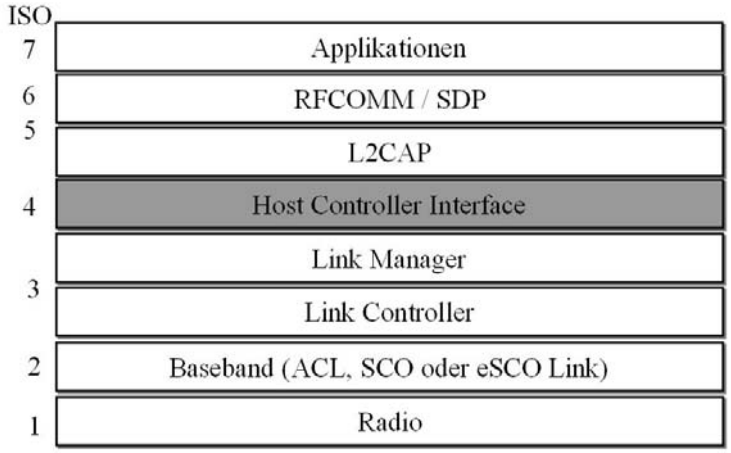

Abb. 5.4: Der Bluetooth Protokoll Stack

5.4.1 Der Baseband Layer

Die Eigenschaften der physikalischen Schicht, also der Radioübertragung, wurden im vorhergehenden Abschnitt schon beschrieben. Auf den Eigenschaften des physikalischen Kanals setzt dann der Baseband Layer auf, der typische Aufgaben eines Layer 2 Protokolls wie z.B. das Framing von Datenpaketen übernimmt. Für die Datenübertragung bietet der Baseband Layer drei unterschiedliche Frametypen:

ACL Pakete

Für die Paketdatenübertragung werden bei Bluetooth Asynchronous Connection-Less (ACL) Pakete verwendet. Wie in Abbil-

dung 5.5 gezeigt, besteht ein ACL Paket aus einem 68-72 Bit langen Access Code, einem 18 Bit Header und einem 0-2744 Bit langen Feld für die eigentlichen Nutzdaten (Payload).

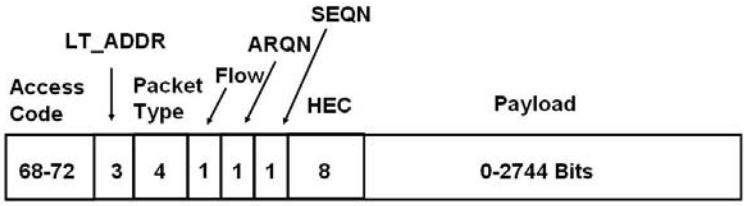

Abb. 5.5: ACL Paket

Vor der Übertragung werden die 18 Header-Bits noch durch einen Forward Error Correction Algorithmus in 54 Bits kodiert (1/3 FEC). Dies stellt sicher, dass Übertragungsfehler in den meisten Fällen korrigiert werden können. Je nach Größe des Nutzdatenfeldes benötigt ein ACL Paket 1, 3 oder 5 Slots zu je 625 Mikrosekunden Dauer.

Der Access Code am Anfang des Pakets dient in erster Linie zur Identifikation des Piconetzes, zu dem das aktuelle Paket gehört. Erzeugt wird der Access Code deshalb aus der Geräteadresse des Piconet Masters. Der eigentliche Header des ACL Pakets besteht aus einer Reihe von Bits, die folgende Funktionen haben: Die ersten drei Bits des Headers ist die Logical Transfer Address (LT_ADDR) eines Slaves, die der Master bei der Verbindungsaufnahme zuweist. Über die 3 Bit lassen sich insgesamt bis zu 7 Slaves adressieren.

Daran anschließend folgt der Pakettyp mit 4 Bits, der den Aufbau des restlichen Pakets näher beschreibt. Nachfolgende Tabelle zeigt die unterschiedlichen Möglichkeiten für ACL Pakete. Neben der Anzahl der Slots eines Paketes, unterscheiden sich die Pakettypen auch in der Anwendung einer Forward Error Correction (FEC) für den Nutzdatenteil. Diese ermöglicht es auf der Empfängerseite, Übertragungsfehler zu korrigieren. Nachteil ist jedoch, dass die Anzahl der Nutzdatenbits pro Paket reduziert wird. Mit einer 2/3 FEC wird für zwei Nutzdatenbits ein Bit für die Fehlerkorrektur hinzugefügt. Statt zwei Bits werden dann drei Bits übertragen (2/3). Außerdem wird bei ACL Paketen grundsätzlich eine CRC Checksumme berechnet, um Fehler erkennen zu können.

Paket-typ	Anzahl Slots	Linktyp	Payload (Bytes)	FEC	CRC
0100	1	DH1	0-27	Nein	Ja
1010	3	DM3	0-121	2/3	Ja
1011	3	DH3	0-183	Nein	Ja
1110	5	DM5	0-224	2/3	Ja
1111	5	DH5	0-339	Nein	Ja

Um einen Empfangspufferüberlauf zu vermeiden, kann ein Gerät über das Flow Bit seiner Gegenstelle signalisieren, für den Moment keine weiteren Daten zu senden.

Über das ARQN Bit teilt ein Endgerät seiner Gegenstelle mit, ob das zuvor gesendete Paket korrekt empfangen wurde. Ist dieses Bit nicht gesetzt, sendet die Gegenstelle das zuvor übertragene Paket erneut.

Um auch den kompletten Verlust eines Pakets erkennen zu können, folgt als nächstes Feld im ACL Header das Sequence (SEQN) Bit. Dieses wird bei jeder Übertragung eines neuen Pakets auf den jeweils anderen Bitwert gesetzt. Werden zwei aufeinander folgende Pakete mit identischem SEQN Bit empfangen, bedeutet dies für Endgerät-2, dass sein letztes Paket Endgerät-1 nicht erreicht hat und Endgerät-1 daraufhin sein Paket wiederholt hat. Endgerät-2 wiederholt daraufhin sein Paket mit Empfangsbestätigung zu Endgerät-1 und ignoriert alle Pakete, bis wieder ein Paket mit korrektem SEQN Bit von Endgerät-1 empfangen wird. Auf diese Weise wird sichergestellt, dass auch bei mehrfachem Paketverlust die Empfangsbestätigung trotzdem zugestellt werden kann.

Als letztes Header-Feld folgt der Header Error Check (HEC). Dieses Feld stellt sicher, dass bei falsch empfangenem Header das Paket beim Empfänger ignoriert wird.

Auf den ACL Header folgt das Payload-Feld. Dieses enthält am Anfang den Payload Header, der folgende Aufgaben erfüllt: Das erste Feld wird L_CH (Logical Channel) genannt. Es gibt an, ob das Payload Feld Nutzdaten (L2CAP Pakete, vgl. Kapitel 5.4.6) oder Signalisierungsdaten in Form einer LMP Nachricht enthält (vgl. Kapitel 5.4.3).

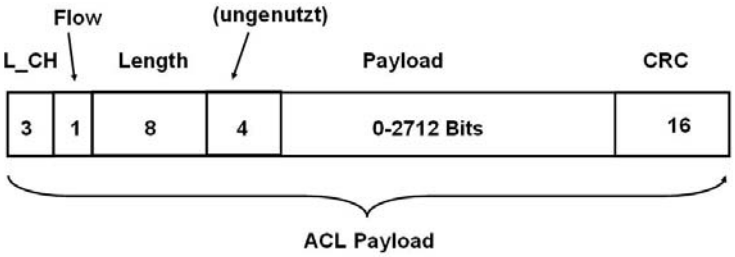

Abb. 5.6: Das ACL Payload-Feld mit Header

Mit dem Flow Bit kann ein voller Empfangspuffer auf der L2CAP Nutzdatenschicht gemeldet werden. Schließlich enthält der Payload Header noch ein Längenfeld. Abgeschlossen wird ein ACL Paket immer durch eine 16 Bit Checksumme.

SCO Pakete

Da bei der Übertragung von ACL Paketen keine Bandbreite garantiert werden kann, eignen sich diese nicht für die Übertragung von Echtzeitdaten wie z.B. Sprache. Für diese Anwendung gibt es auf dem Baseband Layer zusätzlich den Synchronous Connection Oriented (SCO) Pakettyp. Im Unterschied zu ACL Paketen werden SCO Pakete zwischen Master und Slave in fest vorgegebenen Intervallen übertragen. Das Intervall wurde dabei so gewählt, dass die resultierende Bandbreite genau 64 kbit/s beträgt.

Bei SCO Verbindungen ist das Slave Endgerät autonom, es sendet sein SCO Datenpaket auch dann, wenn es zuvor kein Paket vom Master erhalten hat. Dies ist bei einer SCO Verbindung problemlos möglich, da Pakete zu vordefinierten Intervallen gesendet und empfangen werden. Der Slave ist somit also nicht auf eine Sendeerlaubnis des Masters angewiesen und es ist implizit sichergestellt, dass zu dieser Zeit nur er Daten überträgt. Auf diese Weise wird erreicht, dass trotz eines nicht erhaltenen Pakets in Empfangsrichtung das eigene Sprachpaket trotzdem übertragen wird.

Der Header eines SCO Paketes entspricht dem eines ACL Paketes, die Flow, ARQN und SEQN Felder werden bei SCO Paketen jedoch nicht verwendet. Die Länge des Nutzdatenfeldes beträgt immer genau 30 Bytes. Je nach verwendetem Fehlerkorrekturverfahren entspricht dies 10, 20 oder 30 Nutzdatenbytes. Nachfolgende Tabelle gibt einen Überblick über die möglichen SCO Pakettypen.

Paket-typ	Anzahl Slots	Linktyp	Payload (Bytes)	FEC	CRC
0101	1	HV1	10	1/3	Nein
0110	1	HV2	20	2/3	Nein
0111	1	HV3	30	keine	Nein
1000	1	DV	10 (+0-9)	2/3	Ja

Die letzte Zeile der Tabelle zeigt einen Spezialpakettyp, der gleichzeitig SCO und ACL Daten enthält. Dieser Pakettyp wird verwendet, wenn neben den reinen Sprachdaten auch Steuerdaten zu übertragen sind. Wie später in Kapitel 5.6.4 im Zusammenhang mit dem Headset Profil gezeigt wird, werden zwischen einem Headset und einem Mobiltelefon nicht nur Sprachdaten, sondern auch in manchen Fällen Signalisierungsdaten (z.B. Lautstärkeregelung) übertragen. Die SCO Sprachdaten werden in einem solchen „DV“ Datenpaket dann in den ersten 10 Bytes übertragen, auf die 0 - 9 Bytes für den ACL Kanal folgen. Die in der Tabelle eingetragene Forward Error Correction und Checksumme wird nur für den ACL Teil verwendet. Der Standard schreibt die Verwendung eines DV Pakets nicht zwingend vor, falls Sprache und Daten gleichzeitig zwischen zwei Geräten zu übertragen sind. Eine weitere Möglichkeit ist, eigenständige ACL Pakete in den von der SCO Verbindung nicht verwendeten Slots zu senden. Dritte Möglichkeit ist, die Sprachdaten eines Slots zu verwerfen und statt des SCO Pakets ein ACL Paket zu schicken.

eSCO Pakete

Da bei SCO Paketen nicht festgestellt werden kann, ob die Nutzdaten des Pakets korrekt übertragen wurden, werden bei schlechten Übertragungsbedingungen fehlerhafte Pakete an höhere Protokollschichten weitergegeben. Diese erzeugen bei der Wiedergabe der Sprache hörbare Knackgeräusche. Außerdem limitiert die maximale Geschwindigkeit eines SCO Kanals von 64 kbit/s die Anwendungsmöglichkeiten eines SCO Kanals, da z.B. Musikdaten beim Audiostreaming meist höhere Datenraten benötigen. Um diese Nachteile zu beseitigen, wurde mit Bluetooth Version 1.2 der Enhanced-SCO (eSCO) Pakettyp eingeführt. Dieser bietet folgende Vorteile:

Die Datenrate eines eSCO Kanals kann beim Aufbau der Verbindung festgelegt werden. Auf diese Weise sind konstante Datenraten bis zu 288 kbit/s in beide Richtungen möglich.

eSCO Pakete besitzen für den Nutzdatenteil eine Checksumme. Beim Auftreten eines Übertragungsfehlers kann das Paket erneut übertragen werden, falls noch genügend Zeit vor der Übertragung des nächsten regulären Pakets bleibt. Abbildung 5.7 zeigt diese Situation. Bluetooth macht sich für dieses Verfahren den Umstand zunutze, dass z.B. bei einer 64 kbit/s eSCO Verbindung nur ein Bruchteil der gesamten Bandbreite des Kanals genutzt wird und somit genug Zeit für eine erneute Übertragung bleibt. Trotz der mehrfachen Übertragung eines Pakets bleibt dadurch die Datenrate konstant. Um der Gegenseite ein verlorenes oder fehlerhaftes Paket zu signalisieren, wird das von ACL Paketen bekannte Acknowledge Verfahren verwendet. Ist es bis zur Übertragung des nächsten regulären Paketes nicht möglich ein Paket korrekt auszuliefern, wird es verworfen. Somit ist gewährleistet, dass der Datenstrom nicht ins Stocken gerät. Ab Bluetooth V2.1 kann auch ein nicht korrekt empfangenes Paket an höhere Schichten zusammen mit einer Fehlerindikation weitergegeben werden (Erroneous Data Reporting). Dies macht Sinn, wenn ein Codec kleine Übertragungsfehler selber ausgleichen kann.

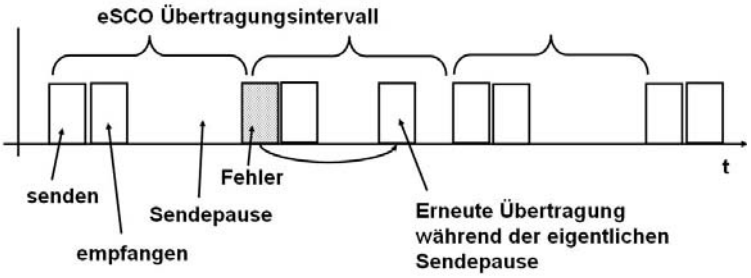

Abb. 5.7: Erneute Übertragung eines eSCO Pakets nach einem Übertragungsfehler

Enhanced Data Rate ACL und eSCO Pakete

Um die Übertragungsgeschwindigkeit von Bluetooth zu erhöhen, erschien 2004 die Bluetooth Version 2.0 + Enhanced Data Rate (EDR). Kern von EDR ist die Verwendung von neuen Modulationsverfahren für den Nutzdatenteil eines ACL oder eSCO Paketes. Während Header und Nutzdatenteil der zuvor beschriebenen Pakete per GFSK moduliert werden, wird der Nutzdatenteil von EDR ACL oder eSCO Paketen per DQPSK oder 8DPSK moduliert. Diese Verfahren erlauben pro Übertragungsschritt die Übertragung von mehr als einem Bit. Auf diese Weise kann unter Beibehaltung der Kanalbandbreite von 1 MHz und der Slotzeit von 625 Microsekunden die Übertragungsgeschwindigkeit gesteigert werden. Um rückwärtskompatibel zu sein, wird der Header jedes

Paketes weiterhin über GFSK moduliert. Somit kann der Header auch von einem Bluetooth Endgerät ohne EDR Funktionalität korrekt empfangen werden. Auch bei Wireless LAN wird dieses Verfahren verwendet, um die Kompatibilität zwischen der 802.11b und der schnelleren 802.11g Variante zu gewährleisten. Die Beibehaltung der bisherigen Headermodulation sorgt außerdem dafür, dass auch nicht-EDR Geräte bei der Übertragung von Multislotpaketen zwischen dem Master und einem anderen Gerät weiterhin ihren Empfänger abschalten und somit Strom sparen können.

Die nachfolgende Tabelle gibt einen Überblick über alle möglichen ACL Pakettypen und die maximale Datenrate im asymmetrischen Betrieb. Asymmetrisch bedeutet, dass 5 Slot Pakete in Vorwärtsrichtung verwendet werden und 1 Slot Pakete in der Gegenrichtung. Im ersten Teil der Tabelle sind alle ACL Pakettypen aufgelistet, die von allen Bluetooth Endgeräten beherrscht werden. Im zweiten und dritten Teil der Tabelle sind dann die EDR ACL Pakettypen aufgelistet. 2-DH1, 3 und 5 werden mit DQPSK moduliert, 3-DH1, 3, 5 mit 8DPSK. Die Zahl 1, 3 oder 5 am Ende des Namens gibt die Anzahl der Slots an, die das Paket belegt.

Typ	**Payload (Bytes)**	**Datenrate uplink (kbit/s)**	**Datenrate downlink (kbit/s)**
DM1	0-17	108.8	108.8
DH1	0-27	172.8	172.8
DM3	0-121	387.2	54.4
DH3	0-183	585.6	86.4
DM5	0-224	477.8	36.3
DH5	0-339	723.2	57.6
2-DH1	0-54	345.6	345.6
2-DH3	0-367	1174.4	172.8
2-DH5	0-679	1448.5	115.2
3-DH1	0-83	531.2	531.2
3-DH3	0-552	1766.4	265.6
3-DH5	0-1021	2178.1	177.1

Durch die neuen Pakettypen ist es nicht mehr möglich, alle Pakettypen eindeutig über das 4 Bit lange Paket Type Feld zu identifizieren (vgl. Abb. 5.5). Die Bluetooth Spezifikation behilft sich deswegen mit folgendem Umweg: Im Grundzustand ist EDR deaktiviert. Erkennen zwei Bluetooth Endgeräte beim Einrichten einer Verbindung, dass sie beide EDR beherrschen, können die Link Manager der beiden Geräte (vgl. Kapitel 5.4.3) diese Funktionalität aktivieren und die Bitkombinationen des Paket Type Felds werden den 2-DHx und 3-DHx Typen zugeordnet.

Während EDR die DQPSK Modulation als verbindlich vorschreibt, bleibt die 8DPSK Modulation für die 3-DHx Pakete optional. Ob ein Endgerät also eine maximale Datenrate von 1448.5 oder 2178.1 MBit/s unterstützt kann nicht von seiner EDR Fähigkeit abgeleitet werden.

Weitere Pakettypen

Neben ACL, SCO und eSCO Paketen für die eigentliche Datenübertragung gibt es noch eine Anzahl weiterer Pakettypen, die nur für den Aufbau oder den Erhalt einer Verbindung verwendet werden:

ID Pakete

ID Pakete werden vor dem Verbindungsaufbau von einem Gerät gesendet, um andere Geräte ausfindig zu machen. Da das Timing und die Hopping Sequenz der Gegenstelle zu diesem Zeitpunkt nicht bekannt sind, enthält ein solches Paket nur den Access Code.

FHS Pakete

Ein Frequency Hop Synchronization (FHS) Paket wird während eines Verbindungsaufbaus zwischen zwei Endgeräten in der Inquiry und Paging Phase gesendet. Inquiry und Paging werden im nächsten Unterkapitel genauer vorgestellt. Es enthält neben der 48 Bit Device Adresse des sendenden Geräts auch Timing Informationen, um die weitere Verbindungsaufnahme zu erleichtern.

NULL Pakete

NULL Pakete dienen der Empfangsbestätigung eines zuvor eingegangenen Pakets, enthalten aber keine Nutzdaten. NULL Pakete müssen nicht bestätigt werden. Somit bieten sie die Möglichkeit, den gegenseitigen Bestätigungskreislauf zu unterbrechen, wenn keine Daten mehr im Sendepuffer anstehen.

POLL Pakete

Ein weiteres Spezialpaket ist das POLL Paket. Mit diesem kann überprüft werden, ob Slaves bei längerer Übertragungspause noch im Piconetz angesprochen werden können. Wie das NULL Paket enthält es keine Nutzdaten.

5.4.2 Der Link Controller

Auf dem Baseband Layer baut die Link Controller Schicht auf. Wie der Name schon andeutet, ist der Link Controller für den Aufbau, den Erhalt und den korrekten Abbau von Verbindungen zuständig. Für die Verwaltung der Verbindungen wird auf dieser Schicht ein Zustandsmodell verwendet. Für ein Gerät, das eine Verbindung zu einem anderen Gerät aufbauen möchte, gibt es folgende Zustände:

Inquiry und Inquiry Scan

Möchte ein Endgerät bisher noch unbekannte Geräte in seiner Umgebung finden, wird der Link Controller von den höheren Protokollschichten angewiesen, in den Inquiry Zustand zu wechseln. In diesem Zustand sendet das Gerät in jedem Slot auf zwei unterschiedlichen Frequenzen ein ID Paket aus.

Alle Endgeräte, die eine Verbindungsaufnahme von unbekannten Geräten zulassen, müssen von Zeit zu Zeit in den Inquiry Scan Zustand wechseln und dort auf abwechselnden Frequenzen nach ID Paketen Ausschau halten. Die Empfangsfrequenz wird hier jedoch nur alle 1.28 Sekunden geändert. Um Strom zu sparen, oder die Verbindung mit anderen Endgeräten aufrecht zu erhalten, sucht ein Endgerät aber nicht im gesamten Intervall nach ID Paketen. Der Bluetooth Standard schlägt eine Scanzeit von 11.25 Millisekunden pro 1.28 Sekunden Intervall vor. Durch die Kombination aus schnellem Frequenzwechsel des suchenden Endgerätes und langsamem Frequenzwechsel des Ausschau haltenden Endgeräts, ergibt sich eine 90 % Wahrscheinlichkeit, dass sich die Geräte innerhalb von 10 Sekunden finden.

Um die Geschwindigkeit der Suche zu beschleunigen, wurde mit Bluetooth 1.2 der so genannte Interlaced Inquiry Scan eingeführt. Mit dieser Methode wird statt auf einer Frequenz pro Periode auf zwei Frequenzen pro Periode nach ID Paketen gesucht. Außerdem ist es seit dieser Bluetooth Version möglich, eine Empfangsstärkemessung (RSSI, Received Signal Strength Indication) für gefundene Geräte an höhere Schichten weiterzugeben. Somit ist es möglich, die Liste der gefundenen Geräte nach der Empfangsstärke zu sortieren. Dies ist vor allem dann sinnvoll, wenn z.B. während einer Messe sehr viele Bluetooth Endgeräte in der Nähe sind und ein Nutzer seine elektronische Visitenkarte an ein Endgerät senden möchte, das sich in unmittelbarer Nähe befindet. Da dieses Gerät besser als weiter entfernte Geräte empfangen wird, erscheint es auf diese Weise ganz oben in der Liste.

Empfängt ein Endgerät ein ID Paket, sendet es ein Frequency Hop Synchronization (FHS) Paket zurück, das neben seiner Device-Adresse auch Frequency Hopping und Synchronisationsinformationen enthält.

Das suchende Endgerät hat nach Empfang des FHS Paketes die Möglichkeit, die Inquiry Prozedur fortzusetzen, um weitere Endgeräte zu finden. Alternativ kann die Inquriy Prozedur auch beendet werden, um sofort über die nachfolgend beschriebene Paging Prozedur eine ACL Verbindung zu dem neu gefundenen Endgerät herzustellen.

Auch Master Endgeräte, die sich schon in einer aktiven Verbindung befinden, können von Zeit zu Zeit in den Inquiry Scan Zustand wechseln. Somit sind sie auch während einer bestehenden Verbindung weiterhin für unbekannte Endgeräte sichtbar. Manche Endgeräte wie z.B. Mobiltelefone unterstützen diese optionale Funktionalität jedoch nicht.

Möchte ein Anwender gar keinen Kontakt von unbekannten Geräten zulassen, kann die Inquiry Scan Funktion abgeschaltet werden. Somit können nur noch Geräte mit der nachfolgend beschriebenen Paging Prozedur Kontakt aufnehmen, denen die Device Adresse des Endgeräts bekannt ist. Diese Einstellung ist sinnvoll, nachdem der Anwender seine Bluetooth Geräte untereinander bekannt gemacht hat (Pairing, siehe Kapitel 5.5.1) und fortan nur noch mit diesen kommunizieren will.

Page und Page Scan

Um eine ACL Verbindung aufzubauen, müssen Endgeräte, denen die Device Adresse eines anderen Endgerätes schon bekannt ist, oder diese zuvor mit einer Inquiry Prozedur gefunden haben, eine Paging Prozedur durchführen. Das Paging funktioniert ähnlich dem Inquiry, ID Pakete werden in schneller Reihenfolge auf unterschiedlichen Frequenzen gesendet. Statt einer allgemeinen Adresse enthält das Paket jedoch die Geräteidentifikation der Gegenstelle, die zuvor über das FHS Paket ermittelt wurde, oder noch von der letzten Verbindung bekannt ist. Die Gegenstelle antwortet darauf ebenfalls mit einem ID Paket und gibt somit dem anfragenden Gerät die Möglichkeit, ein FHS Paket zurückzusenden, das seine Hopping Sequenz etc. enthält. Abbildung 5.8 zeigt den Ablauf der Paging Prozedur und Übergang in den Connected Zustand.

Führt ein Endgerät Inquiry und Page Scans durch, und bestehen keine aktiven Verbindungen zu anderen Geräten, ist der Stromverbrauch eines Bluetooth Chips sehr niedrig. Typisch ist dann ein Energieverbrauch von weit unter einem Milliwatt. Bei Akku-

kapazitäten von Mobiltelefonen im Bereich von 2000-3000 Milliwattstunden ist somit gewährleistet, dass die Bluetooth Funktionalität nur einen geringen Einfluss auf die Standby-Zeit des Geräts hat.

Connection-Active

Nach erfolgreichem Paging befinden sich beide Endgeräte im Connection Active Zustand und der Datenaustausch über die neue ACL Verbindung kann beginnen.

Bei der Verbindungsaufnahme kann es vorkommen, dass der Slave der neuen Verbindung auch gleichzeitig Master einer anderen Verbindung ist, die schon vorher bestanden hat. In solchen Fällen wird von den oberen Bluetooth Protokollschichten schon beim eingehenden Paging die Verbindung nur mit der Bedingung zugelassen, sofort nach der Verbindungsaufnahme automatisch einen Master-Slave Rollentausch durchzuführen. Nur so ist es möglich, dass das Endgerät gleichzeitig mit zwei anderen Endgeräten Daten austauschen kann.

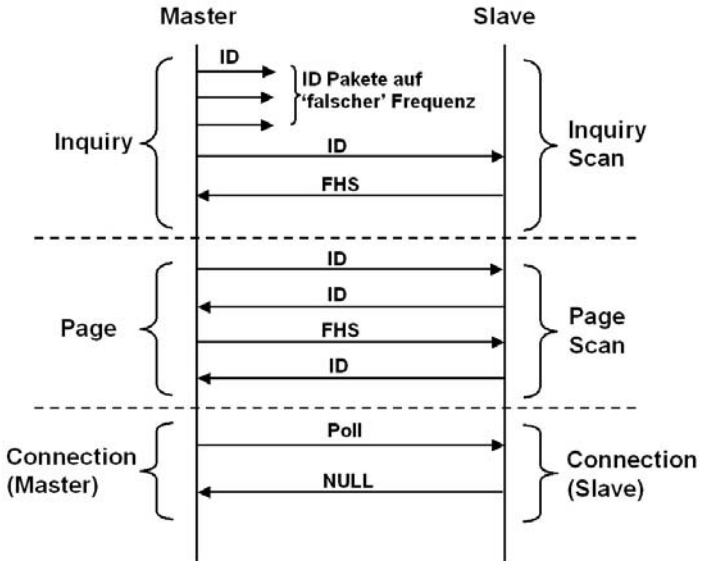

Abb. 5.8: Verbindungsaufbau zwischen zwei Bluetooth Geräten

Stromsparmodi

Der Stromverbrauch während einer aktiven Verbindung hängt im Wesentlichen von der Leistungsklasse des Endgeräts ab (vgl. Kapitel 5.2). Während einer aktiven Verbindung kann es jedoch auch vorkommen, dass für einige Zeit keine Daten zu übertragen sind. Gerade für Endgeräte wie Mobiltelefone oder PDAs ist es in dieser Zeit sehr wichtig, möglichst wenig Strom zu verbrauchten und somit die Laufzeit des Gerätes zu erhöhen. Für solche Fälle

definiert der Bluetooth Standard für den Connected Zustand drei Unterzustände:

Connection–Hold Der erste Unterzustand ist der Connection-Hold Zustand. Um in diesen Zustand zu wechseln, einigen sich Master und Slave über die Dauer des Hold Zustandes. Danach können Sender und Empfänger für diese Zeitdauer komplett abgeschaltet werden. Nach Ende der Hold Periode wechseln Master und Slave wieder automatisch in den Connection-Active Zustand.

Connection-Sniff Wesentlich flexibler ist der Connection-Sniff Zustand. Dieser Stromsparmodus ist ideal für Verbindungen mit wenig oder zeitweise keiner Aktivität geeignet. Master und Slave einigen sich beim Aktivieren des Sniff-Modus darauf, in welchen Intervallen und für wie lange pro Intervall ein Slave den Übertragungskanal abhören soll. In der Praxis ist zu beobachten, dass der Connection-Sniff Mode für folgende Anwendungen genutzt wird:

- Bei allen Profilen bei längerer Inaktivität (z.B. 15 Sekunden): Üblich sind dann Sniff Intervalle von z.B. 2 Sekunden. Bei erneuter Aktivität wird der Sniff-Modus wieder abgeschaltet, um eine möglichst hohe Übertragungsgeschwindigkeit zu erreichen.
- Bei Human Interface Device (HID) Profilen für Tastaturen und Mäuse: Da hier die benötigte Bandbreite gering ist, können sich Verbindungen für diese Profile ständig im Sniff-Modus befinden.

Im Sniff-Modus reduziert sich der Stromverbrauch des kompletten Bluetooth Chips auf weit unter 1 mW.. Vergleicht man den Stromverbrauch des Sniff-Modus mit dem Wireless LAN 802.11 Power Save Mode, ist ein großer Unterschied festzustellen. Dieser braucht durchschnittlich 200 - 500 mW. Im Vergleich zum Bluetooth Stromverbrauch im Sniff Modus von unter 1 mW wird deutlich, in welchem Maße bei der Bluetooth Architektur auf Stromspartechniken Wert gelegt wurde.

Sniff-Subrating Ab Bluetooth Version 2.1 gibt es zusätzlich den Sniff-Subrating Mode, um den Energieverbrauch vor allem für HID Geräte weiter zu verringern. Endgeräte im Sniff-Mode können mit diesem Mechanismus eine weitere Reduzierung des Sniff Intervalls nach einem gewünschten Timeout aushandeln. Nach Ablauf des Timers fällt die Verbindung automatisch in den Sniff-Subrating Modus. Wird dann ein Paket empfangen, fällt die Verbindung in den normalen Sniff-Modus zurück und der Timer startet von neuem.

Connection-Park

Um die Leistungsaufnahme noch weiter zu reduzieren, gibt es den Connection-Park Zustand. In diesem Zustand gibt der Slave seine Piconetadresse (LT_ADDR) auf und überprüft nur noch sehr selten, ob der Master die Verbindung reaktivieren möchte.

5.4.3 Der Link Manager

Die nächste Schicht des Protokoll Stacks (vgl. Abb. 5.4) ist die Link Manager Schicht. Während die zuvor besprochene Link Controller Schicht Datenpakete je nach Verbindungszustand sendet und empfängt, ist die Aufgabe des Link Managers die Einrichtung und Aufrechterhaltung von Verbindungen. Dies beinhaltet folgende Operationen:

- Aufbau einer ACL Verbindung zu einem Slave und Vergabe einer Linkadresse (LT_ADDR).
- Abbau von Verbindungen.
- Konfiguration einer Verbindung wie z.B. das Aushandeln der maximalen Anzahl von Slots von ACL oder eSCO Paketen.
- Einschalten der Enhanced Data Rate (EDR) Übertragung, falls beide Geräte diese Erweiterung unterstützen.
- Durchführung eines Master-Slave Rollentausches.
- Durchführen des in Kapitel 5.5.1 beschriebenen Pairings.
- Aktivierung und Kontrolle der Authentifizierung und Verschlüsselung, falls dies für die Verbindung von höheren Schichten gefordert wird.
- Kontrolle des mit Bluetooth 1.2 eingeführten Adaptive Frequency Hoppings (AFH).
- Management (Aktivierung/Deaktivierung) der Stromsparmodi Hold, Sniff und Park.
- Aufbau einer SCO oder eSCO Verbindung und Aushandeln der verwendeten Parameter wie z.B. die zu verwendenden Fehlerkorrekturmechanismen, Datenübertragungsraten (nur eSCO), etc.

Der Link Manager führt diese Operation entweder auf Befehl von höheren Schichten aus (vgl. nächstes Kapitel), oder aufgrund von Anfragen des Link Managers der Gegenstelle. Link Manager zweier Bluetooth Endgeräte kommunizieren, wie in Abb. 5.9 gezeigt, über ACL Verbindungen mit dem Link Manager Protocol (LMP). Ob es sich bei einem eingehenden ACL Paket um Nutzda-

ten oder um eine LMP Nachricht handelt, erkennt der Link Manager, wie in Abbildung 5.6 gezeigt, über das Logical Channel (L_CH) Feld des ACL Nutzdatenheaders.

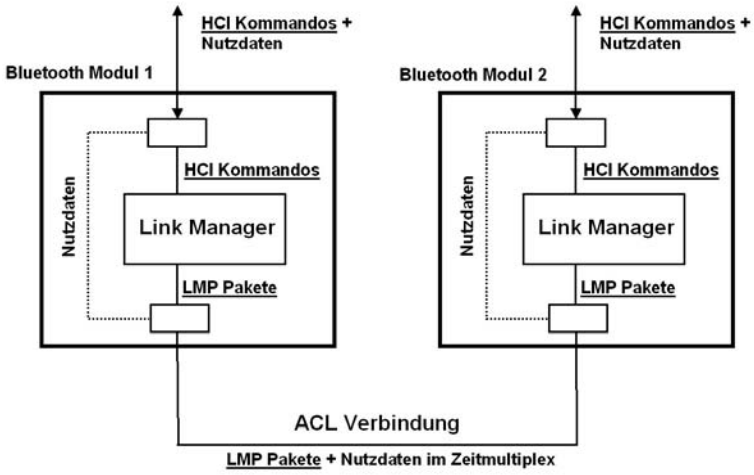

Abb 5.9: Kommunikation zwischen zwei Link Managern per LMP

Damit eine Verbindung zu höheren Schichten nach erfolgreichem Aufbau einer ACL Verbindung hergestellt werden kann, muss zunächst der Link Manager des Geräts, das die ACL Verbindung veranlasst hat (Master), mit dem Link Manager der Gegenseite Kontakt aufnehmen. Dies geschieht mit einer LMP_Host_Connection_Request Nachricht. Danach können optionale Konfigurationsnachrichten ausgetauscht werden. Beendet wird die LMP Verbindungsphase durch gegenseitiges Senden einer LMP_Setup_Complete Nachricht. Nach diesem Schritt ist es dann möglich, Nutzdatenpakete transparent zwischen den zwei Endgeräten auszutauschen. Es können jedoch auch jederzeit innerhalb des Nutzdatenstroms weitere LMP Nachrichten eingeschoben werden, die für die am Anfang des Abschnitts beschriebenen Operationen notwendig sind.

5.4.4 Das HCI Interface

Die nächste Ebene im Bluetooth Protokollstack ist das Host Controller Interface (HCI). Bei den meisten Bluetooth Implementierungen wird dieses Interface verwendet, um das Endgerät und den Bluetooth Chip physikalisch voneinander zu trennen. Ausnahmen sind z.B. Headsets, die aufgrund ihrer physikalischen

Größe und der Limitation auf Sprachübertragung alle Bluetooth Protokollschichten in einem Chip integrieren.

HCI Hardware Interface

Über die HCI Schnittstelle können zwischen Endgerät (Host) und Bluetooth Chip (Controller) Daten und Kommandos für den Link Manager in definierten Kommandos und Nachrichtenpaketen übertragen werden. Der Bluetooth Standard sieht für das HCI Interface zwei Schnittstellentypen vor:

Für Endgeräte wie z.B. Notebooks eignet sich die USB (Universal Serial Bus) Schnittstelle am besten. USB ist die vom PC bekannte universelle Schnittstelle, über die auch Drucker, Scanner und Mäuse an den PC angeschlossen werden. Der Bluetooth Standard definiert für dieses Hardware Interface, wie HCI Kommandos und Datenpakete über USB zu übertragen sind.

Für kompakte Endgeräte, wie z.B. Mobiltelefone oder PDAs kann auch ein serielles Interface verwendet werden, das UART (Universal Asynchronous Receiver and Transmitter) genannt wird. Von den verwendeten Spannungspegeln abgesehen, ist dieses Interface mit der von PCs bekannten seriellen RS-232 Schnittstelle kompatibel. Während die RS-232 Schnittstelle jedoch auf eine Geschwindigkeit von 115 kbit/s beschränkt ist, können Daten über die UART Schnittstelle bei manchen Bluetooth Chips mit bis zu 1.5 MBit/s übertragen werden. Dies ist auch notwendig, da die maximale Bluetooth Datenrate die Datenrate einer gewöhnlichen RS-232 Schnittstelle bei weitem übersteigt. Welche Geschwindigkeit auf der UART Schnittstelle verwendet wird, bleibt den Entwicklern des Host Endgerätes überlassen. So ist bei manchen Endgeräten festzustellen, dass diese nicht die volle Bluetooth Geschwindigkeit ausnutzen können. Dies liegt dann z.B. an der zu kleinen Rechenkapazität der Host Architektur und der dadurch reduzierten Geschwindigkeit auf der UART Schnittstelle.

HCI Pakettypen

Auf der HCI Schnittstelle können eine Reihe unterschiedlicher Pakettypen übertragen werden. Dies sind:

- Kommandopakete (Commands), die vom Host an den Link Manager im Bluetooth Chip übertragen werden.
- Antwortpakete auf Kommandos, die der Bluetooth Controller an den Host zurückschickt. Diese Pakete werden Events genannt. Events können auch ohne vorheriges Kommando an den Host geschickt werden, wenn z.B. ein anderes Bluetooth Gerät Kontakt aufnehmen möchte.
- Nutzdatenpakete von und zum Bluetooth Chip.

Auf der UART Schnittstelle werden die unterschiedlichen Pakettypen durch einen Header unterschieden. Das erste Byte eines Pakets gibt dabei an, um welchen Pakettyp es sich handelt. Wird USB als Übertragungsschnittstelle für das HCI Interface verwendet, werden die unterschiedlichen Pakettypen über unterschiedliche USB Endpunkte identifiziert. Eine USB Pollrate von einer Millisekunde sorgt dafür, dass Event Pakete und Nutzdatenpakete, die vom Bluetooth Chip an den Host zu übertragen sind, mit sehr kurzer Verzögerung erkannt und abgeholt werden.

HCI Spy

Bei manchen Bluetooth USB Adaptern, die den Bluetooth Stack der Firma Broadcom (vormals Widcomm) verwenden, befindet sich auf der Installations-CD in einem etwas versteckten Verzeichnis ein Programm namens „BtserverSpyLite.exe“. Dieses Programm eignet sich hervorragend, um HCI Pakete aufzuzeichnen und zu dekodieren.

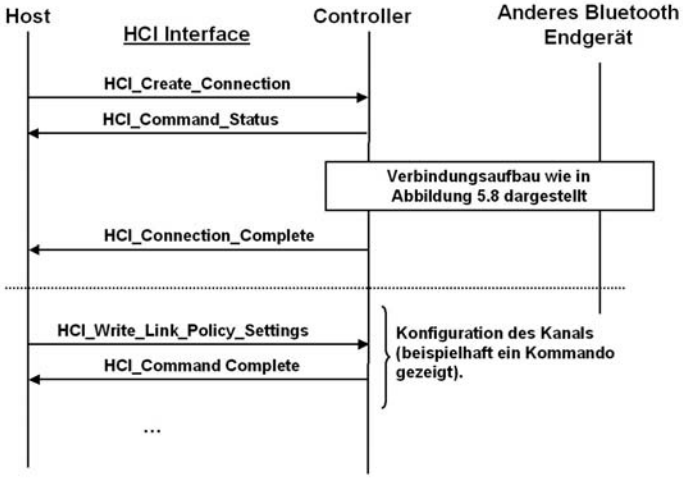

Abb. 5.10: Aufbau einer Verbindung per HCI Kommando

HCI Kommandos für einen Verbindungsaufbau

Abbildung 5.10 zeigt, wie ein Bluetooth Modul über das HCI Interface veranlasst wird, eine Verbindung zu einem anderen Bluetooth Endgerät aufzubauen. Über das HCI_Create_Connection Kommando werden dem Bluetooth Controller alle benötigten Informationen für den Verbindungsaufbau übergeben. Der wichtigste Parameter ist die Device-Adresse des anderen Bluetooth Gerätes. Nach Erhalt des Kommandos quittiert der Controller dieses mit einer HCI_Command_Status Event Nachricht und startet als nächstes die Suche nach dem anderen Endgerät. Der Ablauf dieser Suche ist in Abbildung 5.8 zu sehen, wobei für diesen Fall

jedoch die dort gezeigte Inquiry Phase entfällt, da die Bluetooth Device Adresse des anderen Gerätes schon bekannt ist. Konnte die Verbindung erfolgreich aufgebaut werden, sendet der Bluetooth Controller ein HCI_Connection_Complete Event zurück. Wichtigster Parameter ist ein Connection Handle, um Pakete von und zu unterschiedlichen Endgeräten unterscheiden zu können. Das Connection Handle steht über diese Zuweisung in direkter Beziehung zum L_CH Parameter eines ACL bzw. SCO Paketes.

Für die Kontrolle einer Verbindung und die Konfiguration des Bluetooth Controllers gibt es eine Vielzahl weiterer HCI Kommandos und Events. Nachfolgende Tabelle zeigt eine kleine Auswahl der Kommandos:

Kommando	**Aufgabe**
Setup_Synchronous_ Connection	Für die Sprachübertragung (z.B. mit einem Headset) baut dieses Kommando einen SCO oder eSCO Sprachkanal auf.
Accept_Connection_ Request	Bei einer ankommenden Bluetooth Verbindung signalisiert der lokale Link Manager dies den höheren Schichten über ein Connection_Request Event. Möchte der Host die Verbindung zulassen, antwortet er dem Link Manager im Controller Chip mit diesem Kommando.
Write_Link_Policy_ Settings	Über dieses Kommando kann der Host die möglichen Verbindungszustände wie Hold, Park und Sniff erlauben oder sperren.
Read_Remote_ Supported_Features	Mit diesem Kommando kann ein Host den Bluetooth Controller anweisen, bei einer Gegenstelle eine Liste aller verfügbaren Bluetooth Funktionalitäten anzufordern. So kann der Host z.B. ermitteln, welche Multislot Pakettypen das andere Endgerät unterstützt, welche Stromsparmechanismen möglich sind, ob Adaptive Frequency Hopping verwendet werden kann, usw.

Disconnect	Beenden einer Verbindung.
Write_Scan_Enable	Mit diesem Kommando kann der Host kontrollieren, ob das Bluetooth Modul periodische Inquiry- und oder Page Scans durchführen soll. Wird beides abgeschaltet, können nur abgehende Verbindungen aufgebaut werden, das Gerät ist für andere Bluetooth Geräte unsichtbar.
Write_Inquiry_Scan_ Activity	Übergibt dem Bluetooth Controller Werte für die Konfiguration des Inquiry Scans wie z.B. die Größe des Inquiry Scan Zeitfensters.
Write_Local_Name	Über dieses Kommando übergibt der Host einen „lesbaren“ Gerätenamen an das Bluetooth Modul. Dieser kann dann automatisch anderen Geräten übergeben werden, die nach Bluetooth Geräten suchen. So ist es möglich, dem Benutzer eine Liste mit Gerätenamen statt Bluetooth Device Adressen anzuzeigen.

5.4.5 Der L2CAP Layer

Im nächsten Schritt der Verbindungsaufnahme wird über eine bestehende ACL Verbindung eine L2CAP (Logical Link Control and Adaptation Protocol) Verbindung aufgebaut. Diese Protokollschicht befindet sich über dem HCI Layer und kann mehrere logische Verbindungen zu einem Gerät über eine physikalische ACL Verbindung multiplexen. Somit kann z.B. während dem bestehen einer Bluetooth Dial-Up Verbindung zwischen einem PC und einem Mobiltelefon noch eine weitere zusätzliche logische Verbindung für die Übertragung eines Adressbucheintrages zwischen den Geräten aufgebaut werden. Bestehen zu einem Zeitpunkt noch weitere ACL Verbindungen zu anderen Geräten, kann die L2CAP Schicht auch Daten von und zu unterschiedlichen Geräte multiplexen. Ein solches Szenario ist in Abbildung 5.11 dargestellt. Während einer Internet Dial-Up Verbindung über Slave 1 wird gleichzeitig noch eine Datei aus dem Speicher des Mobiltelefons zum Master übertragen, sowie ein MP-3 Datenstrom zwischen Master und Slave 2 übertragen.

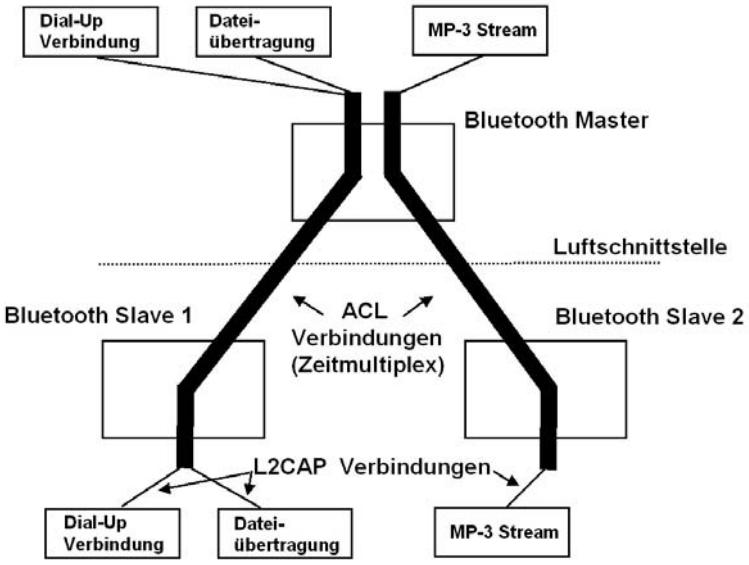

Abb. 5.11: Multiplexing verschiedener Datenströme

Der Protocol Service Multiplexer (PSM)

Der Aufbau einer L2CAP Verbindung erfolgt über eine L2CAP_Connection_Request Nachricht. Wichtigster Parameter ist der Protocol Service Multiplexer (PSM). Dieser gibt an, an welche höhere Schicht Pakete nach erfolgreichem L2CAP Verbindungsaufbau weitergereicht werden sollen. Für die meisten Bluetooth Anwendungen wird der PSM 0x0003 verwendet, mit dem eine Verbindung zur RFCOMM Schicht hergestellt wird. Die RFCOMM Schicht stellt für Anwendungen eine virtuelle serielle Verbindung zu einem entfernten Bluetooth Endgerät her und wird in Kapitel 5.4.8 genauer beschrieben. Außerdem enthält die L2CAP_-Connection_Request Nachricht eine Connection ID (CID), über die fortan alle L2CAP Pakete der Verbindung identifiziert werden. Die CID ist notwendig, da die RFCOMM Schicht von mehreren Diensten gleichzeitig verwendet werden kann und somit der PSM nur beim Verbindungsaufbau eindeutig ist. Nimmt die Gegenstelle die L2CAP Verbindung an, sendet sie ein L2CAP_Connection_-Response zurück und teilt ihrerseits eine Connection ID zu, über die L2CAP Pakete in der Gegenrichtung identifiziert werden. Danach ist die Verbindung eingerichtet und kann verwendet werden. Optional gibt es jetzt die Möglichkeit, weitere Parameter für die Verbindung über das L2CAP_Configuration_Request Kommando zu übertragen. Dazu zählen, z.B. die Anzahl der erneuten Sendeversuche bei Paketverlust und die maximale Paketlänge, die von einem Gerät unterstützt wird.

Segmentierung von Datenpaketen

Eine weitere wichtige Aufgabe der L2CAP Schicht ist die Segmentierung von Datenpaketen aus höheren Schichten. Dies ist notwendig, wenn Pakete aus höheren Schichten größer als ein ACL Paket sind. Ein 5 Slot ACL Paket hat beispielsweise eine maximale Größe von 339 Bytes. Werden von der Anwendungsschicht größere Pakete angeliefert, werden diese in kleinere Stücke aufgeteilt und in mehreren ACL Paketen versandt. Im Header jedes ACL Paketes wird außerdem vermerkt, ob es den Anfang eines L2CAP Paketes darstellt, oder ein nachfolgendes Teilstück ist. Auf der Gegenseite kann dann die L2CAP Schicht mit dieser Information aus mehreren ACL Paketen wieder ein einziges Paket zusammensetzen, das an die Anwenderschicht weitergereicht wird.

5.4.6 Das Service Discovery Protocol

Theoretisch könnte nach dem Aufbau einer ACL und L2CAP Verbindung der Datentransfer zwischen zwei Endgeräten sofort aufgenommen werden. Bluetooth eignet sich jedoch für eine Vielzahl unterschiedlicher Dienste, und die meisten Endgeräte bieten mehrere Dienste gleichzeitig an. Ein Mobiltelefon beherrscht beispielsweise Dienste wie Internet Verbindung (Dial-Up Network), Dateitransfer, den Austausch von Adressen und Terminen und vieles mehr. Damit ein Bluetooth Gerät in Erfahrung bringen kann, welche Dienste andere Bluetooth Endgeräte bieten und wie diese angesprochen werden können, muss vor dem Verbindungsaufbau zum eigentlichen Dienst eine Service Datenbank befragt werden. Die Service Datenbank wird über L2CAP PSM 0x0001 angesprochen und das Protokoll zur Kommunikation wird Service Discovery Protocol (SDP) genannt. Dieser Schritt kann entfallen, wenn das Endgerät genau weis, wie der Dienst angesprochen werden kann. Bluetooth ist jedoch sehr flexibel und erlaubt Diensten, ihre Verbindungsparameter zur Laufzeit zu ändern. Einer dieser Verbindungsparameter ist z.B. die zu verwendende RFCOMM-Kanalnummer. Mehr hierzu in Kapitel 5.4.8.

Dienste und Profile

Auf Anwenderebene werden Dienste auch Profile genannt. Der Headset Dienst / das Headset Profil stellt sicher, dass ein Headset mit allen gängigen Bluetooth Telefonen zusammenarbeitet, die ebenfalls das Headset Profil unterstützen. Mehr zu Bluetooth Profilen in Kapitel 5.5.

Parametersuche für einen Dienst

Jeder Bluetooth Dienst hat seine eigene universelle Identifikationsnummer (Universally Unique ID, UUID), über die er in der SDP Datenbank gefunden werden kann. Der Dial-Up Server Dienst hat z.B. die UUID 0x1103. Damit sich der Bluetooth Stack

eines PCs mit diesem Dienst z.B. auf einem Mobiltelefon verbinden kann, wird nach der ersten Verbindungsaufnahme zuerst die SDP Datenbank des Mobiltelefons nach den nötigen Einstellungen für diesen Dienst befragt. Dies geschieht über eine SDP_Service_Search_Attribute_Req Nachricht. Wichtigster Parameter, den der Client der SDP Datenbank des anderen Gerätes übergibt, ist die UUID des Dienstes. Die Datenbank liefert dann in einer SDP_Service_Search_Attribute_Response Nachricht die benötigten Parameter in Form von Records zurück. Im Falle des Dial-Up Server Dienstes liefert die Datenbank die Information zurück, dass für diesen Dienst die L2CAP Schicht, sowie die im nächsten Unterkapitel vorgestellte RFCOMM Schicht zu verwenden sind.

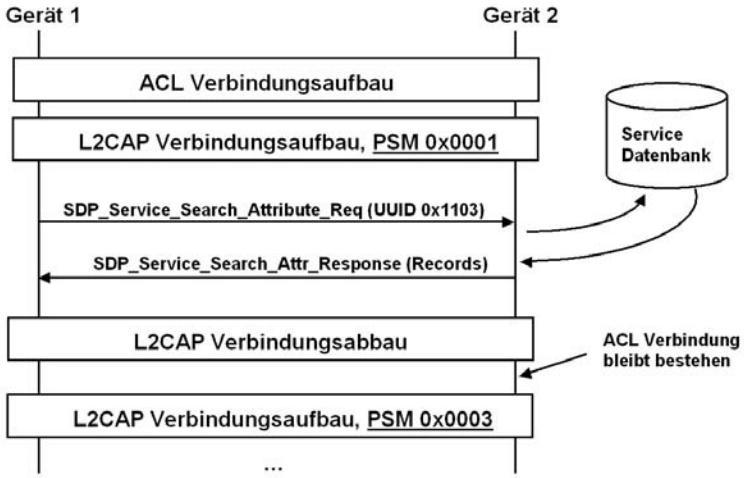

Abb. 5.12: Verbindungsaufbau zu einem Dienst mit vorheriger Datenbankabfrage

Allgemeine Dienstsuche

Die Service Datenbank eines Bluetooth Geräts bietet außerdem eine allgemeine Suchmöglichkeit. Diese wird von einem Endgerät verwendet, wenn es ein neues Bluetooth Gerät gefunden hat und der Benutzer wissen möchte, welche Dienste dieses Gerät anbietet. Die Nachricht für eine allgemeine Suche in der Datenbank lautet SDP_Service_Search_Request. Statt einer spezifischen UUID wie im Beispiel oben, wird die UUID der Public Browse Group (0x1002) übergeben. Die Datenbank liefert dann die UUIDs aller Dienste die es anbietet an das andere Endgerät. Die weiteren Parameter der einzelnen Dienste können nun mit

SDP_Service_Search_Attribute_Request Anfragen an die Datenbank ausgelesen werden. Bei einer Anfrage liefert die Datenbank auch einen frei wählbaren Namen des angeforderten Dienstes im Klartext zurück. Auf diese Weise ist eine flexible länder- und sprachspezifische Anzeige eines Dienstnames für den Anwender möglich. Der Name dient jedoch nur zur Benutzerinformation, der Bluetooth Stack selber identifiziert einen Dienst immer über die UUID und niemals über den Namen.

Oft werden die Informationen auch lokal auf der Anwenderschicht gespeichert, damit dem Anwender bei erneuter Nutzung eines Geräts die Liste der verfügbaren Dienste eines entfernten Geräts schneller angezeigt werden kann.

Beenden der Datenbankabfrage und Aktivierung eines Dienstes

Um die Datenbankabfrage zu beenden, löst das abfragende Gerät die L2CAP Verbindung durch Senden einer L2CAP_Disconnection_Request Nachricht auf. Möchte das Gerät anschließend sofort eine Verbindung zu einem Dienst herstellen, bleibt die ACL Verbindung bestehen, und es wird sofort wieder ein L2CAP_Connection_Request Nachricht geschickt. Diese Nachricht enthält jedoch nicht die PSM ID 0x0001 für die Service Datenbank, sondern die PSM ID für die nächst höhere Schicht, die der gewünschte Dienst verwendet. Abgesehen von Sprachdiensten verwenden die meisten anderen Dienste den RFCOMM Layer, der eine virtuelle serielle Schnittstelle bietet. Dieser wird über den PSM 0x0003 angesprochen.

5.4.7 Der RFCOMM Layer

Wie in Kapitel 5.4.6 gezeigt, wird der L2CAP Layer verwendet, um mehrere Datenströme über eine physikalische Verbindung zu multiplexen. Die Service Datenbank ist z.B. eine Anwendung, die über den L2CAP Protocol Service Multiplexer (PSM) 0x0001 angesprochen wird. Andere Dienste könnten auf gleiche Weise über andere PSM angesprochen werden. In der Praxis verwenden jedoch viele Dienste noch einen weiteren gemeinsamen Layer, der RFCOMM genannt wird und über PSM 0x0003 angesprochen wird. RFCOMM stellt den Diensten virtuelle serielle Schnittstellen zur Verfügung und vereinfacht diesen dadurch die Datenübertragung.

Virtuelle serielle Schnittstelle

Wie diese seriellen Schnittstellen verwendet werden, hängt von den übergeordneten Diensten ab. Mit dem „Serial Port“ Dienst beispielsweise wird über den RFCOMM Layer eine virtuelle serielle Schnittstelle für beliebige „nicht“ Bluetooth Anwendungen bereitgestellt. Diese unterscheidet sich aus Sicht einer Anwen-

dung nicht von anderen seriellen Schnittstellen. Meist bekommen virtuelle serielle Bluetooth Schnittstellen vom Betriebssystem die COM-Port Nummern 3,4,5,6,7 usw. zugeteilt. Welche genau, entscheidet sich bei der Installation des Bluetooth Protokoll Stacks auf einem PC. Diese seriellen Schnittsellen können z.B. bei der Einrichtung eines neuen Modemtreibers verwendet werden, bei dessen Einrichtung einfach die entsprechende COM-Port Nummer angegeben wird. Sobald eine Anwendung wie z.B. das DFÜ-Netzwerk diesen COM-Port öffnet, wird automatisch eine Bluetooth Verbindung zur Gegenseite hergestellt. Damit diese automatische Verbindungsaufnahme funktioniert, muss zuvor über die Bluetoothsoftware diese COM-Port Nummer einmalig mit der gewünschten Gegenstelle verbunden werden.

UART Simulation

Um Anwendungen eine komplette serielle Schnittstelle zu bieten, simuliert der RFCOMM Layer nicht nur die Sende- und Empfangsleitungen, sondern auch die Statusleitungen Request to Send (RTS), Clear to Send (CTS), Data Terminal Ready (DTR), Data Set Ready (DSR), Data Carrier Detect (CD), sowie die Ring Indicator (RI) Leitung. Bei einer physikalisch vorhandenen seriellen Schnittstelle werden diese Leitungen über einen UART (Universal Asynchronous Receiver and Transmitter) Baustein angesprochen. Aus diesem Grund simuliert die Bluetoothsoftware für den „Serial Port“ Dienst einen kompletten UART Baustein. Während ein UART Baustein die Befehle der Anwendungsschicht auf physikalische Leitungen umsetzt, sendet der virtuelle Bluetooth UART Baustein die erhaltenen Steuerkommandos und Daten in RFCOMM Paketen verpackt an den L2CAP Layer weiter.

RFCOMM für andere Dienste

Auch andere Dienste wie z.B. der Dateitransferdienst (OBEX) oder der Dial-Up Server Dienst (vgl. Kapitel 5.6.2 und 5.6.3) setzen die RFCOMM Schicht ein. Über unterschiedliche RFCOMM Kanalnummern ist es möglich, beim Verbindungsaufbau auszuwählen, welcher Dienst angesprochen werden soll. Die Kanalnummer ist Teil der Dienstbeschreibung in der Servicedatenbank. Fragt also ein anderes Gerät die Servicedatenbank eines Bluetooth Geräts nach dem Dial-Up Server Dienst, so erfährt es über die Antwort, dass dieser Dienst über die L2CAP Schicht zu erreichen ist und als nächst höhere Schicht RFCOMM benutzt. Hieraus kann das Endgerät zunächst schließen, dass der L2CAP PSM 0x0003 zu verwenden ist, um die Verbindung zum RFCOMM Layer herzustellen (L2CAP nach RFCOMM). Außerdem entnimmt das Endgerät der Dial-Up Server Dienstbeschreibung, mit welcher RFCOMM-Kanalnummer dieser angesprochen werden kann (RFCOMM zu Anwendung). Da die RFCOMM-Kanalnummer dy-

namisch einem Dienst zugeordnet werden kann, ist vor der Verbindungsaufnahme deswegen immer die Service Datenbank zu befragen, um die korrekte Kanalnummer zu erhalten.

Abbildung 5.13 zeigt, wie unterschiedliche Kanalschichten Datenströme multiplexen. Während der HCI Layer die Verbindung zu mehreren Geräten multiplext (Connection Handles), können über den L2CAP Layer unterschiedliche Dienste pro Gerät adressiert werden (PSM und CID). Dies wird in der Praxis verwendet, um zwischen der Service Datenbank (PSM 0x0001) und der RFCOMM-Schicht (PSM 0x0003) zu unterscheiden. Von der Service Datenbank abgesehen, verwenden die meisten Bluetooth Dienste die RFCOMM-Schicht und müssen deshalb noch zusätzlich durch unterschiedliche RFCOMM-Kanalnummern voneinander unterschieden werden.

RFCOMM multiplext mehrere serielle Datenströme

Die RFCOMM Kanalnummer ermöglicht es außerdem, bis zu 30 RFCOMM Dienste zwischen zwei Geräten gleichzeitig zu verwenden. Somit ist es möglich, während einer Dial-Up Verbindung auch gleichzeitig Dateien mit dem Object Exchange Dienst (OBEX) zu übertragen. Da beide Dienste unterschiedliche RFCOMM Kanalnummern verwenden, können die RFCOMM Datenpakete der beiden Dienste im Zeitmultiplex übertragen werden und am Empfänger wieder dem richtigen Dienst zugestellt werden.

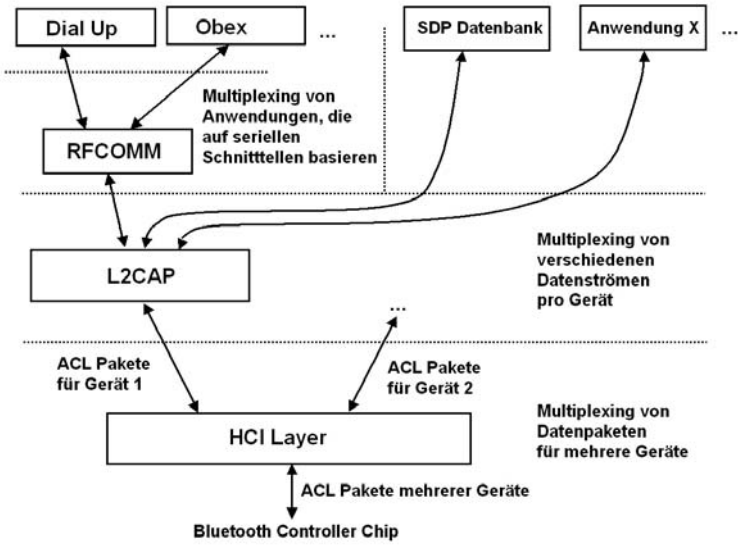

Abb. 5.13: Multiplexing auf den einzelnen Protokollschichten.

5.4.8 Aufbau einer Verbindung im Überblick

Abbildung 5.14 zeigt den Aufbau einer Bluetooth Verbindung durch die unterschiedlichen Schichten noch einmal im Überblick. Um Kontakt zu einer Anwendung auf einem entfernten Bluetooth Gerät aufzunehmen, baut ein Endgerät zunächst eine ACL Verbindung auf. Nach der Konfiguration des ACL Übertragungskanals wird dann über den Protocol Service Multiplexer (PSM) eine L2CAP Verbindung zur Bluetooth Service Datenbank aufgebaut, um den Service Record der Anwendung anzufordern. Dieser enthält alle Informationen für den weiteren Verbindungsaufbau, wie beispielsweise, welche Protokolle auf höheren Schichten zu verwenden sind und wie diese konfiguriert werden. Nach erfolgreicher Übertragung des Service Records wird die L2CAP Verbindung wieder abgebaut, die ACL Verbindung bleibt jedoch zwischen den zwei Geräten bestehen.

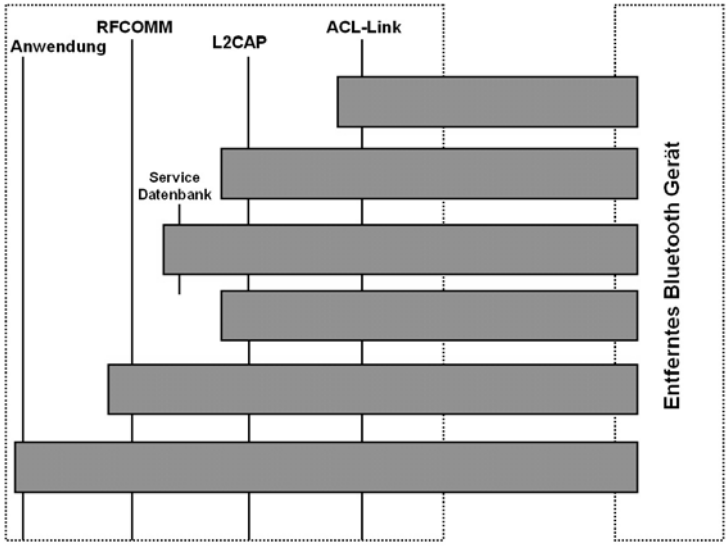

Abb. 5.14: Einzelne Stufen eines Bluetooth Verbindungsaufbaus

Über die ACL Verbindung wird jetzt Kontakt zur eigentlichen Anwendung aufgenommen. Dies geschieht im ersten Schritt durch Aufbau einer L2CAP Verbindung. Die meisten Anwendungen verwenden außerdem die RFCOMM Schicht, die serielle Schnittstellen bereitstellt. Aufgrund der beim RFCOMM Verbin-

dungsaufbau übergebenen Kanalnummer kann der Bluetooth Stack schließlich die Verbindung zwischen dem RFCOMM Layer und der eigentlichen Anwendung, wie z.B. einem Dial-Up Server, herstellen. Wie die Anwendungsschichten der zwei Bluetooth Geräte miteinander kommunizieren, ist Sache der jeweiligen Anwendung und für alle bisher beschriebenen Schichten inklusive des RFCOMM Layers transparent. Um die Interoperabilität auch auf der Anwendungsschicht zu gewährleisten, definiert Bluetooth so genannte Profile, die in Kapitel 5.6 beschrieben werden.

5.5 Bluetooth Sicherheit

Da Bluetooth Funkwellen nicht an der Wohnungstür halt machen, spezifiziert der Bluetooth Standard eine Reihe von Sicherheitsfunktionen. Alle Verfahren sind optional und müssen beim Verbindungsaufbau oder während einer laufenden Verbindung nicht unbedingt verwendet werden. Diese Entscheidung wurde bewusst getroffen, da manche Dienste keine Sicherheitsfunktionen benötigen. Welche Dienste dies sind, liegt im Ermessen des Herstellers und des Anwenders. So kann sich der Hersteller eines Mobiltelefons z.B. entscheiden, einen eingehenden Dateitransfer ohne Authentifizierung der Gegenstelle zuzulassen. Die eingehende Datei wird dann in einem Zwischenspeicher gehalten und der Benutzer kann dann auswählen, ob er die Datei speichern oder verwerfen möchte. Bei anderen Diensten, wie z.B. beim Dial-Up Server, ist es hingegen gerade umgekehrt. Hier sollte immer eine Authentifizierung beim Verbindungsaufbau erfolgen, da sonst ein fremdes Gerät z.B. eine Internetverbindung ohne Wissen des Gerätebesitzers aufbauen könnte.

Schwachstellen

Die bei Bluetooth verwendeten SAFER+ (Secure And Fast Encryption Routine) Verschlüsselungsmechanismen wurden an der ETH Zürich entwickelt und sind öffentlich verfügbar. Bis heute wurden keine Methoden bekannt, diese zu kompromittieren. In der Praxis wurden jedoch zwischenzeitlich Schwachstellen beim einmaligen Aushandeln der Schlüssel gefunden. Diese erlauben es Angreifern, beim Abhören des gleich nachfolgend beschriebenen Pairing, die Schlüssel zu berechnen und Verbindungen dann zukünftig abzuhören. Aus diesem Grund wurden mit Bluetooth 2.1 neue Pairing Mechanismen eingeführt, die in Kapitel 5.5.2 beschrieben werden.

5.5.1 Pairing bis Bluetooth 2.0

Erster Schritt der Sicherheitsvorkehrungen, der einmalig durchgeführt werden muss, ist das so genannte Pairing zweier Endgeräte. Aus Sicht des Anwenders bedeutet ein Pairing von zwei Endgeräten, dass auf beiden Endgeräten eine identische PIN Nummer eingegeben werden muss. Diese wird im Anschluss verwendet, um auf beiden Seiten einen Link Key zu generieren. Der Link Key wird in beiden Endgeräten gespeichert und kann in Zukunft für die Authentifizierung und Verschlüsselung verwendet werden. Das Pairing der zwei Endgeräte läuft, wie in Abbildung 5.15 gezeigt, in folgenden Schritten ab:

Um das Pairing zu starten, sendet das auslösende Endgerät eine LMP_IN_RAND Nachricht über eine neue aufgebaute ACL Verbindung an das andere Endgerät. Der Inhalt der Nachricht ist eine Zufallszahl. Mit dieser wird zusammen mit der PIN und der Geräteadresse ein Initialisierungskey generiert, der K_{init} genannt wird. Da die PIN nicht zwischen den Geräten ausgetauscht wird, kann K_{init} nicht von einem dritten Gerät berechnet werden.

Mit Hilfe von K_{init}, der auf beiden Seiten identisch ist, wird jetzt auf jeder Seite ein Teil eines Combination Keys erstellt. Dieser basiert auf K_{init}, der Geräteadresse eines der beiden Geräte und einer weiteren Zufallszahl, die aber nicht zwischen den zwei Geräten ausgetauscht wird. Im Anschluss werden die jeweils halben Combination Keys mit K_{init} noch XOR verknüpft und danach untereinander über LMP_COMB_KEY Nachrichten ausgetauscht. Die XOR Verknüpfung ist notwendig, um die zwei Combination Key Hälften nicht im Klartext über die Luftschnittstelle übertragen zu müssen.

Da K_{init} auf beiden Seiten bekannt ist, kann die XOR Verknüpfung wieder rückgängig gemacht werden und beide Seiten erhalten dann durch die Kombination der beiden Combination Key Hälften den endgültigen Link Key. Dieser ist zukünftig die Grundlage für die Authentifizierung und Verschlüsselung zwischen den zwei Geräten.

Da der mit dieser Methode generierte Link Key in beiden Endgeräten gespeichert wird, braucht das Pairing nur beim Aufbau der ersten Kommunikationsverbindung durchgeführt werden. Über die Endgeräteadresse der Gegenstelle kann bei der nächsten Verbindungsaufnahme der Link Key dann auf beiden Seiten aus der Link Key Datenbank entnommen werden. Die Authentifizierung erfolgt dann ohne zutun des Anwenders.

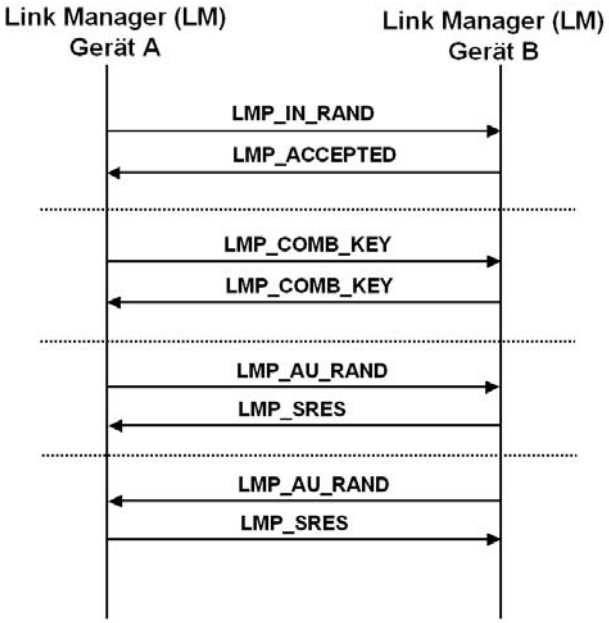

Abb. 5.15: Pairing zwischen zwei Bluetooth Geräten

Um zu überprüfen, ob der Link Key auf beiden Seiten richtig erzeugt wurde, findet im Anschluss an das Pairing eine gegenseitige Authentifizierung statt. Wie diese Abläuft, wird im nächsten Unterkapitel beschrieben. Wie in Abbildung 5.15 ebenfalls zu sehen ist, wird das komplette Pairing von der Link Manager Schicht in den Bluetooth Chips der beiden Endgeräte durchgeführt. Über das HCI Interface muss für die Pairing Prozedur lediglich die PIN Nummer übergeben werden.

5.5.2 Pairing ab Bluetooth 2.1 (Secure Simple Pairing)

In 2005 entdeckten Yaniv Shaked und Avishai Wool einige Schwachstellen die es ermöglichen, nach dem Abhören der Pairing Prozedur die PIN und die Link Keys zu berechnen. Dies war wohl ein wichtiger Grund, warum mit Bluetooth 2.1 der Pairing Mechanismus komplett geändert wurde. Der neue Mechanismus trägt den Namen Secure Simple Pairing und umfasst eine Reihe unterschiedlicher Paring Protokolle für unterschiedliche Sicherheitsanforderungen:

Numeric Comparison Protokoll

Das Numeric Comparison Protocol: Der wichtigste Unterschied dieses Pairing Verfahrens zum bisherigen Verfahren ist, dass statt einer PIN ein Public/Private Key Verfahren zusammen mit dem

Elliptic Curve Diffie-Hellmann Kryptoalgorithmus verwendet wird. Jedes Gerät hat dazu einen privaten und öffentlichen (public) Schlüssel. Beim Pairing schickten beide Endgeräte jeweils ihre öffentlichen Schlüssel zur Gegenstelle, die damit eine Zufallszahl verschlüsselt und zurückschickt. Nach Empfang der verschlüsselten Zufallszahl entschlüsseln die Endgeräte diese mit ihrem privaten Schlüssel und verwenden dann die Zufallszahlen um die Link Keys zu erzeugen. Die Ver- und Entschlüsselung funktioniert nur in eine Richtung, d.h. eine Nachricht, die mit dem öffentlichen Schlüssel chiffriert wurde, kann nur mit dem privaten Schlüssel wieder dechiffriert werden. Da die privaten Schlüssel niemals übertragen werden, kann somit kein anderes Gerät, welches das Pairing belauscht, die Nachrichten dekodieren und somit keine korrekten Link Keys erzeugen. Eine ähnliche Art der Authentifizierung findet sich auch bei Wireless LAN mit EAP-TLS im Enterprise Mode (vgl. Kapitel 4.3.7) sowie beim ersten Zugriff auf eine verschlüsselte Website mit Secure http (HTTPS, SSL/TLS).

Da sich die zwei Endgeräte bisher nicht kannten, könnte bei dieser Art des Pairing ein Angreifer ein Gerät zwischen A und B schalten und sich gegenüber A als B ausgeben und gegenüber B als A. Dies wird oft als Man in the Middle Attack (MITM) bezeichnet. Um diese Möglichkeit auszuschließen, geht das Numeric Comparison Protocol nach der Generierung der Link Keys noch einen Schritt weiter und beide Endgeräte errechnen eine 6-stellige Zahl, die dann dem Anwender gezeigt wird. Das Paring ist erst dann abgeschlossen, wenn der Anwender auf beiden Endgeräten die Zahl bestätigt. Die Berechnungsvorschrift für die 6-stellige Zahl ist so gestaltet, dass bei einer MITM Attacke das zwischengeschaltete Endgerät diese Zahl nicht für beide Geräte berechnen kann. Die Bluetooth SIG gibt an, dass auf diese Weise die Chance eines erfolgreichen MITM Angriffs bei 1:1.000.000 liegt.

Just Works Protokoll

Das Just Works Protocol: Dieses Protokoll ist identisch zum Numeric Comparison Protokoll, es wird jedoch am Ende der Pairing Prozedur keine 6-stellige Zahl berechnet, die der Anwender auf beiden Endgeräten bestätigen muss. Dies bietet zwar keinen Schutz vor einem MITM Angriff, manche Endgeräte wie z.B. Headsets haben jedoch kein Display, um die 6-stellige Zahl darzustellen. Aus diesem Grund sollte ein Pairing für solche Geräte nur durchgeführt werden, wenn hinreichend sicher ist, dass kein Angreifer die Pairing Prozedur abhören und verändern kann. Da diese Schwachstelle nur den Pairing Prozess betrifft, sind alle

später aufgebauten und verschlüsselten Verbindungen trotzdem sicher, und das Just Works Protocol bietet somit für die meisten Anwendungen ausreichend Sicherheit beim Paring. Sollte während des Pairings eine MITM Attacke erfolgreich gewesen sein, muss der Angreifer jedoch bei jeder zukünftigen Kommunikation dabei sein, da sonst der Verbindungsaufbau fehlschlägt.

Passkey Protokoll

Das Passkey Protokoll: Bei diesem Protokoll wird ein Passkey (PIN) für die Authentifizierung verwendet. Für den Anwender ist diese Art des Pairing identisch zum bisherigen Verfahren. Die PIN wird jedoch während des Pairings nicht wie in Kapitel 5.5.1 gezeigt verwendet, sondern es kommt wiederum zu einem Public/Private Key Austausch in Verbindung mit jeweils unabhängigen Zufallszahlen auf beiden Seiten. Für jedes einzelne Bit wird eine verschlüsselte Bestätigung, die Commitment genannt wird, auf beiden Seiten generiert. Eingangsparameter für den dazu verwendeten Algorithmus sind auf beiden Seiten beide öffentlichen Schlüssel, eine auf beiden Seiten unterschiedliche Zufallszahl und das aktuelle Bit der PIN. Im ersten Schritt tauschen beide Endgeräte das Commitment für ein Bit aus. Danach schickt Endgerät A die verwendete Zufallszahl, damit Endgerät B das Commitment über den Umkehralgorithmus überprüfen kann. War die Nachricht korrekt, schickt Endgerät B seine eigene Zufallszahl zurück, damit auch Gerät A überprüfen kann, ob das zuvor gesendete Comittment authentisch ist. Für das nächste Bit wird der Prozess in umgekehrter Richtung durchgeführt, d.h. Gerät B sendet als erstes sein Commitment. Ein Gerät in der Mitte kann bei diesem Prozess somit die Commitments nicht fälschen, da das PIN Bit erst aus dem Comittment zurückberechnet werden kann, nachdem im zweiten Schritt die Zufallszahlen ausgetauscht wurden. Da die Commitments alternierend sind, kann ein Angreifer also nur von jeder Seite ein Bit bekommen, bevor er selber zuerst ein Commitment schicken muss. Dies kann er jedoch nicht, da er nicht über das PIN Bit verfügt.

Out of Band Protokoll

Das Out of Band Protokoll: Schließlich wurde mit Bluetooth 2.1 auch noch ein Verfahren spezifiziert, um die Authentifizierung nicht über den Bluetooth Funkkanal, sondern teilweise oder ganz über andere Übertragungswege durchzuführen. In der Praxis wird diese Variante zusammen mit Near Field Communication (NFC) verwendet. Hierfür müssen sich die Geräte während des Pairings in unmittelbarer Nähe zueinander befinden, der Anwender hält die Geräte also in der Praxis zusammen. Dies schließt eine MITM Attacke aus, da ein eventueller Angreifer zwar potentiell den Nachrichtenaustausch abhören könnte, jedoch selber

keine Möglichkeit hat, sich zwischen die zwei Teilnehmer zu schalten und Nachrichten zu fälschen. Der Bluetooth Standard unterstützt sowohl aktive NFC Chips, die senden und empfangen können, sowie passive NFC Chips, die nur senden können, wenn ihnen über die Antenne eine Spannung induziert wird. Dies ist notwendig, da manche Endgeräte wie z.B. Headsets keinen Platz für eine zusätzliche NFC Antenne haben. In solchen Fällen wird ein passiver NFC Chip z.B. auf dem Benutzerhandbuch oder der Verpackung angebracht. Während des Pairing Prozesses wird dann ein Bluetooth Endgerät mit aktivem NFC Chip, der sowohl senden als auch empfangen kann, an den passiven NFC Chip gehalten. Der passive NFC Chip überträgt dann alle notwendigen Informationen um ein Pairing ohne weitere Benutzerinteraktion durchzuführen.

NFC eignet sich neben dem Pairing auch für Anwendungen, in denen bei Berührung von zwei Geräten eine Aktion durchgeführt werden soll. Ein praktisches Beispiel ist der automatische Ausdruck eines Fotos auf einem Fotodrucker, da mit einem Mobiltelefon oder einem anderen Gerät aufgenommen wurde. Der Nutzer wählt das Bild auf seinem Telefon aus und hält das Telefon dann an den Fotodrucker. Beide Geräte erkennen sich dann über ihre NFC Schnittstelle und beginnen automatisch mit der Übertragung des Bildes.

5.5.3 Authentifizierung

War das Pairing zweier Geräte erfolgreich, können sich diese fortan beim Verbindungsaufbau über den Link Key authentifizieren. Dieser Vorgang funktioniert nach dem allgemeinen Challenge/Response Verfahren, dass z.B. auch bei GSM, GRPS und UMTS verwendet wird. Für die Authentifizierung werden bei Bluetooth drei Parameter benötigt:

- Eine Zufallszahl
- Die Bluetooth Adresse des Geräts, das die Authentifizierung auslöst (BD_ADDR).
- Der 128 Bit Link Key, der beim Pairing der Geräte erzeugt wurde.

Wie in Abb. 5.16 gezeigt, schickt das auslösende Endgerät (Verifier) für die Authentifizierung die Zufallszahl an die Gegenstelle (Claimant). Der Link Manager des Claimant Endgeräts verwendet daraufhin die BD_ADDR des Verifier Endgeräts, um den Link

Key für diese Verbindung über das HCI Interface vom Host anzufordern.

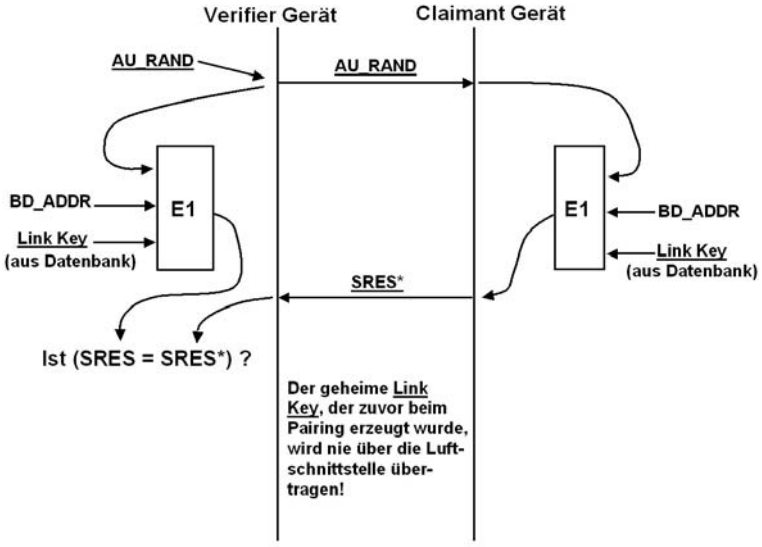

Abb 5.16: Authentifizierung eines Endgeräts

Mit der Zufallszahl, der BD_ADDR, sowie dem Link Key, berechnet der Link Manager des Claimant nun eine Antwort, die Signed Response* (SRES*) genannt wird. Die so berechnete SRES* schickt der Link Manager danach an das Verifier Endgerät zurück. Dieses hat die gleiche Operation ausgeführt und seine eigene SRES errechnet. Die beiden Ergebnisse können nur identisch sein, wenn der Link Key auf beiden Seiten identisch war. Da der Link Key niemals über die Luftschnittstelle übertragen wird, kann sich kein Gerät erfolgreich authentifizieren, mit dem zuvor kein Pairing durchgeführt wurde.

5.5.4 Verschlüsselung

Nach erfolgreicher Authentifizierung können beide Endgeräte jederzeit die Verschlüsselung aktivieren oder deaktivieren. Als Schlüssel wird jedoch nicht der beim Pairing erzeugte Link Key verwendet. Stattdessen wird ein auf beiden Seiten der Verbindung eigens bei der Aktivierung der Verschlüsselung generierter Ciphering Key benutzt. Wichtigster Parameter für die Erzeugung des Ciphering Keys ist neben dem Link Key der Verbindung eine Zufallszahl, die beim Start der Verschlüsselung zwischen den Link Managern ausgetauscht wird. Auf diese Weise ist gewähr-

leistet, dass bei jeder Aktivierung der Verschlüsselung ein neuer Ciphering Key verwendet wird.

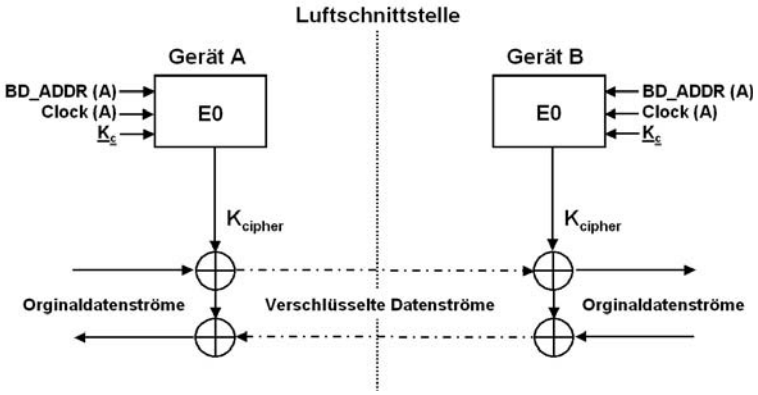

Abb. 5.16a: Bluetooth Verschlüsselung mit einer Ciphersequenz

Der Ciphering Key hat üblicherweise eine Länge von 128 Bit. Es können jedoch auch kürzere Ciphering Keys verwendet werden, wenn Bluetooth Chips für ein Land hergestellt werden, für das es Exportrestriktionen für starke Verschlüsselungskeys gibt.

Zusammen mit der Geräteadresse des Masters und den 26 untersten Bits der Master Echtzeituhr (Master Real Time Clock) dient der Ciphering Key als Eingangswert für den SAFER+ Algorithmus E0, der einen kontinuierlichen Bitstrom erzeugt. Da der aktuelle Wert der Master Real Time Clock auch dem Slave bekannt ist, kann auf beiden Seiten der Verbindung der gleiche Bitstrom generiert werden. Der Bitstrom wird dann über bitweise Modulo-2 Operationen mit dem zu verschlüsselnden Datenstrom kombiniert. Verschlüsselt wird der komplette Teil des ACL Nutzdatenpaketes inklusive der CRC Checksume vor dem optionalen Hinzufügen einer Forward Error Correction (FEC).

5.5.5 Autorisierung

Ein weiteres wichtiges Konzept der Bluetooth Sicherheit ist die Autorisierung des Nutzers für einen Dienst. Dieser weitere Schritt ist nötig, um manche Dienste nicht allen, sondern nur bestimmten Endgeräten zugänglich zu machen. So könnte man auf einem PC einem Nutzer eines anderen Bluetooth Geräts das Recht einräumen, auf ein freigegebenes Verzeichnis Dateien abzulegen oder von dort abzuholen. Der Dateitransfer Dienst (OBEX) ist also für diesen Nutzer aktiviert. Andere Dienste, wie z.B. den Di-

al-Up Netzwerk Dienst, soll der entfernte Anwender jedoch nicht verwenden dürfen.

Über die Autorisierung kann für jeden Dienst einzeln festgelegt werden, welche bekannten Bluetooth Endgeräte auf diesen zugreifen dürfen. Es bleibt dabei dem Hersteller eines Bluetooth Gerätes überlassen, wie diese Funktionalität genutzt wird. Manche Mobiltelefonhersteller beispielsweise erlauben jedem entfernten Endgerät, mit dem ein Pairing erfolgreich durchgeführt wurde, die Benutzung des Dial-Up Dienstes. Andere Mobiltelefonhersteller bauen jedoch noch eine zusätzliche Sicherung ein und fordern vom Nutzer des Mobiltelefons eine explizite Autorisierung des Verbindungswunsches. Dies geschieht über eine Nachricht auf dem Display des Mobiltelefons, die der Besitzer des Mobiltelefons bestätigen muss.

Bluetooth Stacks auf PCs bieten meist eine sehr flexible Autorisierungsfunktionalität an. Dienste können dort sehr flexibel konfiguriert werden:

- Dienst ohne Authentifizierung und Autorisierung nutzbar.
- Dienst darf von allen authentifizierten Geräten ohne weitere Autorisierung verwendet werden. Dies setzt ein einmaliges Pairing voraus.
- Dienst darf nach Authentifizierung und Autorisierung einmalig oder für eine bestimmte Zeitdauer verwendet werden.
- Dienst darf von einem bestimmten Endgerät nach Authentifizierung und einmaliger Autorisierung immer verwendet werden, eine nochmalige Autorisierung ist nicht erforderlich.

Zusätzlich bieten manche Bluetooth Stacks auf dem PC an, immer eine Information auf dem Bildschirm anzuzeigen, wenn ein Dienst von einem entfernten Gerät aufgerufen wird. Dies dient nur zur Information des Nutzers des PCs, der Zugriff wird automatisch gewährt.

5.5.6 Sicherheitsmodi

Zu welchen Zeitpunkten beim Verbindungsaufbau eine Authentifizierung, Verschlüsselung und Autorisierung durchgeführt werden, ist abhängig von der Implementation des Bluetooth Stacks

und der Konfiguration durch den Anwender. Der Bluetooth Standard gibt dazu drei mögliche Konfigurationen vor:

Security Mode 1 Im Sicherheitsmodus 1 (Security Mode 1) findet keine Authentifizierung statt und die Verbindung wird nicht verschlüsselt. Dieser Sicherheitsmodus eignet sich z.B. für die Adress- oder Terminübertragung zwischen zwei Endgeräten. Oft kennen sich die Teilnehmer nicht und es wäre zu umständlich, mit den Geräten vor dem Austausch einer elektronischen Visitenkarte ein Pairing durchzuführen. Die elektronische Visitenkarte wird dann meist von den Geräten in ein extra Verzeichnis kopiert und erst in den Adresskalender aufgenommen, wenn der Benutzer dies bestätigt.

Security Mode 2 Im Sicherheitsmodus 2 bestimmt der Anwender, ob für eine Verbindung eine Authentifizierung, Verschlüsselung und Autorisierung nötig ist. Viele Bluetooth PC Benutzeroberflächen erlauben diese Konfiguration individuell für jeden einzelnen Dienst. Sicherheitsmodus 1 entspricht Sicherheitsmodus 2 eines Dienstes, der weder Authentifizierung noch Verschlüsselung aktiviert hat.

Security Mode 3 Im Sicherheitsmodus 3 wird beim Aufbau jeder Verbindung automatisch eine Authentifizierung und Verschlüsselung vom Bluetooth Chip hergestellt. Dies geschieht schon während der ersten Link Manager Kommunikation, also noch vor dem Aufbau einer L2CAP Verbindung. Bei einer eingehenden Kommunikation fordert deshalb der Bluetooth Controller über die HCI Schnittstelle den Link Key für eine neue Verbindung an. Wurde mit dem entfernten Gerät bisher kein Pairing durchgeführt, kann der Bluetooth Host dem Controller keinen Link Key zurückgeben. In diesem Fall schlägt der Verbindungsaufbau fehl. Sicherheitsmodus 3 ist also vor allem für Geräte gedacht, die nur mit Geräten kommunizieren, mit denen zuvor ein Pairing durchgeführt wurde. Für Mobiltelefone, die auch nicht authentifizierte Verbindungen z.B. für die Übertragung von Adressdaten erlauben, ist dieser Modus nicht geeignet.

Security Mode 4 Sicherheitsmodus 4 ist dem Service Level Enforced Security Mode 2 sehr ähnlich, wurde jedoch für die neuen Pairingmechanismen für Bluetooth 2.1 spezifiziert (vgl. Kapitel 5.5.2). In diesem Modus wählt ein Dienst aus, welche Security Kategorie er für das Pairing verlangt:

- Es wird ein gesicherter Link Key verlangt (Numeric Comparsion, Out of Band oder Passkey Protokoll sind notwendig)

- Es wird nur ein nicht gesicherter Link Key benötigt (Just Works Protokoll)
- Der Dienst benötigt keine Sicherheit

5.6 Bluetooth Profile

Wie in der Einleitung dieses Kapitels gezeigt, ist Bluetooth für eine Vielzahl sehr unterschiedlicher Anwendungen geeignet. Diese Anwendungen haben immer eine Server- und eine Client Seite. Ein Client nimmt durch Aufbau einer Bluetooth Verbindung Kontakt zum Master auf und die Datenübertragung beginnt. Bei den meisten Bluetooth Anwendungen sind die Aufgaben der Masterseite und der Clientseite unterschiedlich. Bei der Übertragung eines Adressbucheintrags beispielsweise, nimmt der Client Kontakt mit dem Server auf. Der Client überträgt einen Termin, ist also eine Sendekomponente, der Server empfängt ihn, ist also eine Empfangskomponente. Um zu gewährleisten, dass der Client auch mit einem Server kommuniziert, der von einem anderen Hersteller programmiert wurde, spezifiziert der Bluetooth Standard so genannte Bluetooth Profile. Für jede Anwendung (Dial-Up, Terminübertragung, serielle Schnittstelle, etc.) gibt es ein Bluetooth Profil, das genau beschreibt, wie die Serverseite und die Clientseite miteinander kommunizieren. Unterstützen zwei Endgeräte das gleiche Bluetooth Profil, ist die Interoperabilität gewährleistet.

Anmerkung: Das Client/Server Prinzip der Bluetooth Profile darf nicht mit dem Master/Salve Konzept der unteren Bluetooth Protokollschichten verwechselt werden. Beim Master Slave Konzept geht es um die Kontrolle des Piconetzes, also wer zu welcher Zeit senden darf, während das Client/Server Prinzip einen Dienst und einen Nutzer des Dienstes beschreibt. Ob nun das Bluetooth Endgerät, auf dem der Server eines Dienstes läuft, der Master oder der Slave im Piconetz ist, spielt keine Rolle.

Nachfolgende Tabelle gibt einen Überblick über zahlreiche Bluetooth Profile für die verschiedensten Anwendungen. Einige davon sind in den nachfolgenden Unterkapiteln genauer beschrieben.

Profilname	**Anwendungsgebiet**
Dial Up Networking (DUN) Profile	Bluetooth Verbindung zwischen einem Modem oder einem Mobiltelefon und einem externen Gerät wie PDA, PC oder

	Notebook.
FAX Profile	Profil für FAX Übertragung.
Common ISDN Access Profile	Profil zur Verbindung eines ISDN Adapters mit einem externen Gerät wie PDA, PC oder Notebook.
LAN Access Profile	IP Verbindung zwischen PDA, PC oder Notebook zu einem Local Area Network (LAN) und dem Internet.
Personal Area Network (PAN) Profile	Wie LAN Access Profile, es wird jedoch eine Ethernet Netzwerkkarte auf dem PAN Gerät simuliert.
File Transfer Profile	Übertragung von Dateien zwischen Bluetooth Geräten.
Object Push Profile	Einfache Übertragung von Dateien zwischen Bluetooth Geräten für Ad-Hoc Datenaustausch.
Synchroization Profile	Synchronisation von Personal Information Manager (PIM) Anwendungen für Adressen, Termine, Notizen, etc.
Basic Imaging Profile	Übertragung von Bildern, für den Einsatz mit Digitalkameras gedacht.
Hard Copy Cable Replacement Profile	Kabelersatz zwischen Drucker und einem Endgerät (z.B. PC).
Basic Printing Profile	Drucken ohne Druckertreiber von mobilen Geräten wie PDAs oder Mobiltelefonen an beliebigen Druckern.
Advanced Audio Distribution Profile	Profil für die Übertragung von Audio Streaming Dateien (z.B. MP-3).
Headset Profile	Kabellose Headsets für Mobiltelefone.
Hands-Free Profile	Verbindung zwischen Freisprecheinrichtung und Mobiltelefon.

SIM-Access Profile	Zugriff einer Freisprecheinrichtung auf die SIM-Karte eines Mobiltelefons.
Human Interface Device (HID) Profile	Anbindung von Mäusen, Tastaturen und Joysticks an Endgeräte wie PCs, Notebooks und PDAs.
Unrestricted Digital Information Profile	Übertragung von breitbandigen leitungsvermittelten Verbindungen zwischen einem Endgerät und einem 3G Mobiltelefon.

5.6.1 Grundlegende Profile: GAP, SDP und Serial Profile

Generic Access Profile (GAP)

Bluetooth spezifiziert zwei Profile, die keine eigentlichen Anwendungen aus Sicht des Benutzers darstellen. Das Generic Access Profile (GAP) legt fest, wie zwei Geräte in unterschiedlichen Situationen Kontakt miteinander aufnehmen und wie sie sich dabei verhalten sollen. Das Profil beschreibt unter anderem:

- Die Präsentation von Bluetooth spezifischen Parametern wie der Geräteadresse (BD_ADDR) oder der PIN für den Anwender.
- Sicherheitsaspekte (Security Mode 1-3)
- Verhalten im Idle Mode (z.B. Inquiry, Device Discovery)
- Verbindungsaufbau

Durch das GAP Profil kann somit sichergestellt werden, dass sich die Benutzeroberflächen für die Konfiguration des Bluetooth Stacks von verschiedenen Endgeräten in den wichtigsten Punkten sehr ähnlich sind. Außerdem wird durch das GAP Profil erreicht, dass bei der Verbindungsaufnahme genau spezifiziert ist, welche Aktionen und Nachrichten in welcher Reihenfolge durchgeführt werden.

Service Discovery Profile (SDP)

Wie in Kapitel 5.4.7 gezeigt, besitzt ein Bluetooth Endgerät eine Service Datenbank, in der jeder Server-Dienst alle wichtigen Informationen für die Verbindungsaufnahme hinterlegen kann. Über das Service Discovery Profil (SDP) wird festgelegt, wie auf diese Datenbank zugegriffen werden kann, und wie und in welcher Struktur die nachfolgend vorgestellten Profile ihre Informationen in der Service Datenbank hinterlegen.

Serial Port Profile (SPP)

Das Serial Port Profile (SPP) ist ein grundlegendes Profil, auf dem zahlreiche nachfolgend vorgestellte Profile aufbauen. Wie der Name schon andeutet, stellt dieses Profil eine serielle Schnittstelle für beliebige Anwendungen zur Verfügung. Es verwendet dazu die in Kapitel 5.4.8 vorgestellte RFCOMM Schicht. Über das Serial Port Profile können beliebige Anwendungen, die Daten über eine serielle Schnittstelle übertragen, kommunizieren. Anpassungen der Anwendungen an Bluetooth sind nicht notwendig, da aus Ihrer Sicht auf eine ganz normale serielle Schnittstelle zugegriffen wird. Abbildung 5.17 zeigt den Protokollstack, den das Serial Port Profile verwendet.

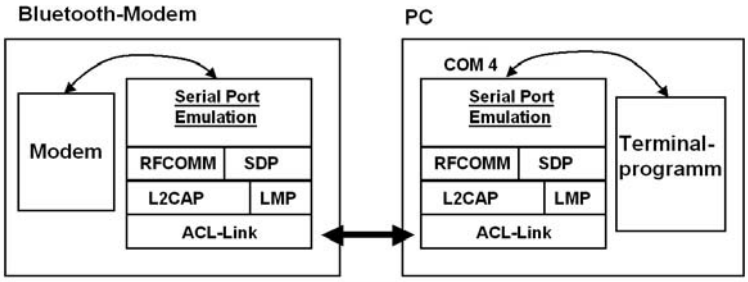

Abb. 5.17: das SPP stellt eine Serielle Schnittstelle zur Verfügung

Ein Anwendungsbeispiel: Das Serial Port Profile kann z.B. mit einem Terminalprogramm wie Hyperterm verwendet werden, um auf ein entferntes Modem zuzugreifen, das auch über eine Bluetooth Schnittstelle verfügt. Bevor die Bluetooth Verbindung benutzt werden kann, muss der PC mit dem Modem ein Pairing durchführen. Danach wird über die Bluetooth Konfigurationsoberfläche auf dem PC noch einmalig ein Bluetooth COM-Port (z.B. COM 4) diesem Endgerät zugeordnet. Jedes Mal, wenn danach das Terminalprogramm gestartet wird und auf die serielle Schnittstelle zugreift, baut der Bluetooth Stack automatisch und ohne zutun des Terminalprogramms eine Verbindung zum entfernten Modem auf.

5.6.2 Netzwerkprofile: DUN, LAP und PAN

Für den Zugriff auf ein Netzwerk spezifiziert der Bluetooth Standard drei unterschiedliche Profile:

Dial-Up Network Profile (DUN)

Das Dial-Up Network (DUN) Profil ersetzt eine Kabelverbindung zwischen einem Endgerät wie einem PC oder PDA und einem Modem. Wie in Kapitel 2.8 und Abbildung 2.33 gezeigt, kann z.B. die Modememulation in einem Mobiltelefon verwendet wer-

den, um über GPRS oder UMTS eine Verbindung ins Internet herzustellen. Das Mobiltelefon verhält sich über die serielle Schnittstelle dann wie ein Modem, das über AT-Kommandos gesteuert werden kann. Über im GSM/UMTS Standard spezifizierte AT-Kommandos ist es dann möglich, statt einer leitungsvermittelten Verbindung auch eine GPRS oder UMTS Verbindung aufzubauen. Gesteuert wird dieser Vorgang über das DFÜ-Netzwerk des Anwenderendgerätes. Das DFÜ-Netzwerk auf dem PC setzt dafür nur eine serielle Schnittstelle und ein Modem voraus. Genau dies bietet das Dial-Up Network Profil. Aus diesem Grund ist das DUN-Profil auch auf dem Serial Port Profile aufgebaut. Wichtigster Unterschied ist jedoch, dass statt einer transparenten Verbindung zwischen beiden Seiten ein Modem auf der Serverseite auf Kommandos der Clientseite wartet.

Wie in Abbildung 5.18 gezeigt, emuliert die DUN-Serverseite ein Modem. Damit das Modem von beliebigen Gegenstellen angesprochen werden kann, legt das DUN Profil auch fest, welche AT Kommandos unterstützt werden. Diese Modem Seite des Profils wird auch Gateway genannt. Da das für das DUN-Profil benötigte virtuelle Modem im Mobiltelefon bereits vorhanden ist, ist meist kein zusätzlicher Aufwand nötig, um neben dem Serial Port Profil auch das DUN-Profil zu unterstützen.

Auf der Client Seite (also auf dem PC oder PDA), im DUN-Profil auch Data Terminal genannt, stellt das Profil dem DFÜ-Netzwerk eine serielle Schnittstelle zur Verfügung.

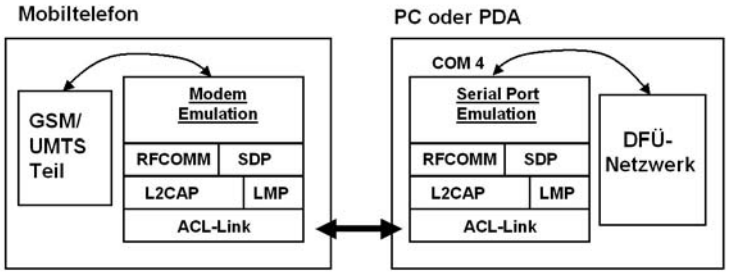

Abb. 5.18: Protokollschichten des Dial-Up Network Profils

Wurde die Verbindung mit dem Internet erfolgreich aufgebaut, starten der PC und das Mobiltelefon den PPP Stack und die Netzwerkverbindung ist aufgebaut (vgl. Kapitel 2.8). Dieser Teil des Internet Verbindungsaufbaus wird jedoch nicht vom DUN-Profil spezifiziert, da das DUN Netzwerk auch für eine allgemeine Modemverbindung verwendet werden kann. Dort ist nach

Aufbau der Wählverbindung nicht unbedingt gesagt, dass ein PPP Server gestartet wird.

LAN Access Profile (LAP)

Das zweite Bluetooth Netzwerk Profil nennt sich LAN Access Profile (LAP) und dient dem Zugang von Bluetooth Geräten zu einem Local Area Network (LAN) und somit potenziell auch dem Internet.

Das LAN Access Profile ist ähnlich wie das DUN-Profil aufgebaut. Auf der Serverseite des Profils befindet sich jedoch kein Modem als oberste Schicht im Protokollstack, sondern die LAN Access Point Komponente. Die LAN Access Point Komponente ist dabei der PPP Server, der eine IP Verbindung über eine serielle Schnittstelle herstellen kann.

Der LAN Access Point kann z.B. ein eigenständiges Gerät mit einer Ethernet Schnittstelle sein. Zwar konkurriert dieses Bluetooth Profil dann mit Wireless LAN, aufgrund der maximalen Datenrate des Übertragungskanals von 723 kbit/s, bzw. etwa 2 MBit/s mit EDR, bleibt die praktische Anwendung aber auf eine Internetverbindung beschränkt. Im Vergleich dazu sind Wireless LAN Access Points mit Geschwindigkeiten von bis zu 54 MBit/s auch für andere Zwecke, wie z.B. dem Austausch großer Datenmengen zwischen den Rechnern des Netzwerkes, geeignet.

Der Bluetooth LAN Access Point kann jedoch auch ein PC sein, der per Ethernet, DSL, ISDN, Modem, etc. mit dem LAN und Internet verbunden ist. Über die Bluetooth Verbindung und dem LAP Profil können dann z.B. mobile Geräte, wie z.B. ein PDA, kostengünstig an das LAN und die Internetverbindung angeschlossen werden.

Aus Sicht des Clients unterscheidet sich der Aufbau einer Internetverbindung über das LAP-Profil nur unwesentlich vom Aufbau einer GPRS oder UMTS Internetverbindung über das DUN-Profil, da auch hier das DFÜ Netzwerk und das PPP Protokoll verwendet werden. Ein Unterschied ist jedoch, dass keine Modemkommandos nötig sind, um den Zugang zum PPP Server herzustellen (vgl. Kapitel 2.8). Während mit dem DUN Profil über das Modem, das auf der Server Seite simuliert wird, auch eine leitungsvermittelte Verbindung hergestellt werden kann, dient das LAN Access Profil ausschließlich dem Aufbau einer IP Verbindung über PPP. Da keine Modemkommandos nötig sind, wählt man für das DFÜ-Netzwerk auf der Client Seite am besten ein “Nullmodem“ als Modemtreiber für die Verbindung auf.

Falls ein PC auf der Serverseite des Profils verwendet wird, implementiert der Bluetooth Stack meist einen PPP Server oder verwendet alternativ eine PPP Serverkomponente des Betriebssystems. Auf der Client Seite wird normalerweise der PPP Client des DFÜ-Netzwerks verwendet, die manuelle Konfiguration des Nullmodems und der DFÜ-Verbindung entfällt dann.

Personal Area Network Profile (PAN)

Vorteil des LAN Access Profils, vor allem bei der Entwicklung der ersten Bluetooth Produkte, war die einfache Implementierung, da der PPP-Server und Client des Betriebssystems verwendet werden konnten. Der Nachteil für Benutzer des LAP Profils ist jedoch die etwas umständliche Konfiguration. Abhilfe schafft das Personal Area Network (PAN) Profil. PAN setzt nicht auf einer seriellen Verbindung auf, sondern emuliert aus Sicht des Betriebssystems eine Ethernet Netzwerkkarte. Wie in Abbildung 5.19 gezeigt, werden deshalb im Bluetooth Protokollstack die RFCOMM und PPP Layer nicht mehr verwendet. Stattdessen wird ein neues Protokoll spezifiziert, das über den L2CAP PSM=15 angesprochen wird und Bluetooth Network Encapsulation Protocol (BNEP) genannt wird. Aufgabe dieses Protokolls ist die Übertragung von Ethernet Frames der virtuellen Netzwerkkarte über Bluetooth.

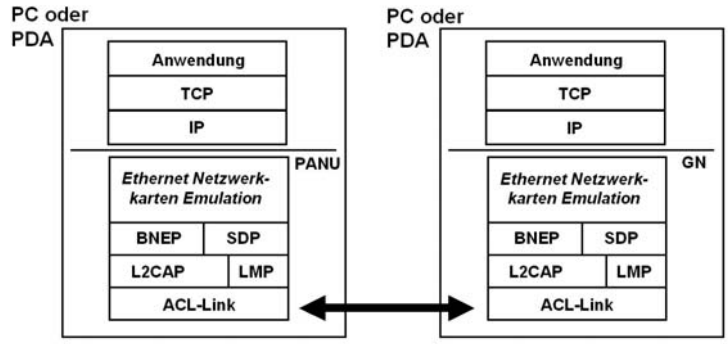

Abb. 5.19: Protokollstack des PAN Profils

Das PAN Profil spezifiziert drei unterschiedliche Rollen. Nutzer eines PAN Netzwerkes werden PAN-User (PANU) genannt. Diese verwenden einen Network Access Point (NAP), um untereinander oder mit einem Ethernet Endgerät, bzw. mit dem Internet zu kommunizieren. Ähnlich wie in einem Wireless LAN kommunizieren die Clients nicht direkt miteinander. Das Network Access Point (NAP) Gerät ist immer der Master des Piconetzes und kann somit die im BNEP Protokoll eingepackten Ethernet Frames zwi-

schen den bis zu 7 Bluetooth PAN-Usern vermitteln, sowie an drahtgebundene Ethernet Geräte weiterleiten (Bridging Funktion).

Wird statt einem dedizierten Network Access Point das Endgerät eines Nutzers verwendet, um als Brücke zwischen den Teilnehmern des PANs zu vermitteln, wird von einem Group Ad-hoc Netzwerk (GN) gesprochen. Der PC, der diese Aufgabe übernimmt, ist dann kein normales PAN-User Gerät, sondern wird als GN Gerät bezeichnet. GN Geräte erfüllen also die gleiche Aufgabe wie ein Network Access Point, können im Unterschied zu diesen aber keine Ethernet Frames zu drahtgebundenen Endgeräten weiterleiten (keine externe Bridging Funktionlität).

In der Praxis kann jedoch statt des Ethernet Bridgings auf Layer 2 auch ohne Probleme das IP Routing auf Layer 3 verwendet werden, um zwischen den Bluetooth PAN-Usern und drahtgebundenen Endgeräten bzw. dem Internet zu vermitteln. Diese Funktionalität ist aber nicht Teil des PAN Profils.

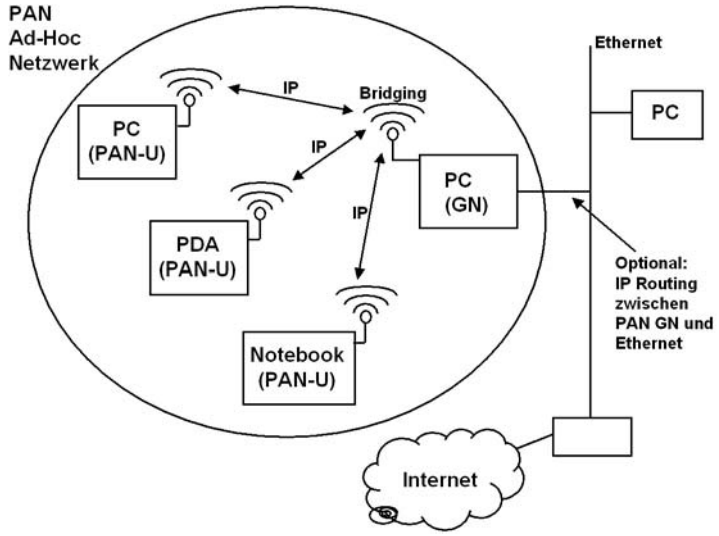

Abb. 5.20: Aufbau eines Personal Area Networks

Neben der Weiterleitung der Pakete stellen NAPs und GNs meist auch einen DHCP Server zur Verfügung, um den IP Stack der PAN-User nach der Verbindungsaufnahme automatisch zu konfigurieren. Dies reduziert die Verbindungsaufnahme aus der Sicht

eines Benutzers auf einen einfachen Doppelklick in der Bluetooth Benutzeroberfläche. Vergleicht man dies mit dem LAN Access Profil, bei dem vor der Verbindungsaufnahme ein Nullmodem und eine neue DFÜ Verbindung im DFÜ-Netzwerk konfiguriert werden muss, ist dies ein enormer Vorteil.

Das PAN Profil ist somit nicht nur geeignet, um mit PDAs eine IP Verbindung zum heimischen PC und über diesen zum Internet herzustellen, sondern auch für die schnelle Einrichtung eines Ad-hoc IP Netzwerkes.

Ein Bluetooth Ad-hoc IP Netzwerk mit dem PAN Profil hat deutliche Vorteile gegenüber einem Wireless LAN Ad-hoc IP Netzwerk (vgl. Kapitel 4.3.1). Während für ein Wireless LAN Ad-hoc IP Netwerk bei allen Teilnehmern eine Vielzahl von Konfigurationsschritten wie z.B. Selektion des Ad-hoc Profils, Konfiguration der Verschlüsselung, Auswahl des Kanals und einer Service Set ID, Konfiguration des IP Stacks, usw. nötig ist, genügt für den Aufbau eines Bluetooth Ad-hoc IP Netzwerkes mit fremden Geräten ein Pairing der Geräte und ein simpler Doppelklick auf das „Netzwerk Icon".

5.6.3 Object Exchange Profile: FTP, Object Push und Synchronize

Die zuvor vorgestellten Profile für den Aufbau von IP Verbindungen sind nicht geeignet, um möglichst schnell und unkompliziert Dateien, Visitenkarten, Termine, Adressbucheinträge oder generell Objekte zu übertragen. Für diese Aufgabe sind die nun vorgestellten Object Exchange Profile (OBEX) wesentlich besser geeignet.

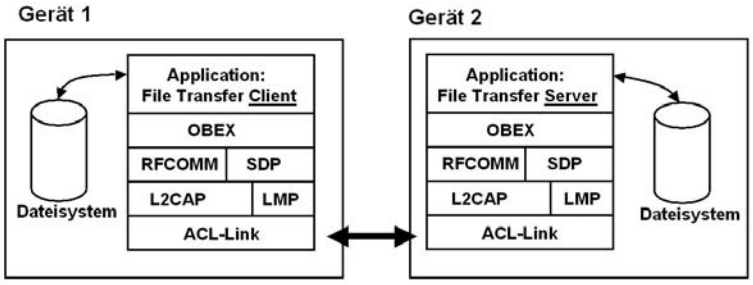

Abb. 5.21: OBEX mit File Transfer Profile als Anwendung

Die Verbindung zwischen zwei Geräten besteht bei diesen Profilen nur während der Übertragung eines oder mehrerer unmittelbar aufeinander folgender Objekte und wird danach sofort wieder abgebaut. Zu diesem Zweck definiert der Bluetooth Standard

als Grundlage für weitere Profile das General Object Exchange (OBEX) Profile (GOEP), das auf den L2CAP und RFCOMM Schichten aufsetzt. Drei weitere Object Exchange (OBEX) Profile verwenden dann dieses Profil für spezifische Dienste.

File Transfer Profile (FTP)

Für die Übertragung einer oder mehrerer Dateien, oder sogar eines ganzen Verzeichnisbaumes, wurde das File Transfer Profile (FTP) entwickelt. Dieses sollte nicht mit dem File Transfer Protocol aus der TCP/IP Welt verwechselt werden, das ebenfalls mit FTP abgekürzt wird.

Eingesetzt wird das OBEX FTP Protokoll hauptsächlich, um zwischen PCs, PDAs und Mobiltelefonen Dateien auszutauschen. Diese können sich an einem beliebigen Ort innerhalb eines Dateisystems befinden. Zu diesem Zweck definiert das allgemeine OBEX Profil (GOEP) die Kommandos CONNECT, DISCONNECT, PUT, GET, SETPATH und ABORT, die binär kodiert über eine aufgebaute RFCOMM Verbindung zur Gegenstelle übertragen werden. Manche PC Bluetooth Stacks klinken das Dateisystem einer Bluetooth Gegenstelle, ähnlich einer normalen Netzwerkverbindung, in den Verzeichnisbaum des lokalen Dateimanagers ein. Klickt der Benutzer das Bluetooth Gerät an, wird über das allgemeine OBEX GET Kommando das Root-Directory des entfernten Bluetooth Gerätes angefordert und dann im Dateimanager dargestellt. Der Anwender hat dann die Möglichkeit, eine oder mehrere Dateien auszuwählen und auf den lokalen PC zu übertragen. Auch diese Aktion wird in ein GOEP GET Kommando umgesetzt. Der Anwender kann auch eine Datei in ein Verzeichnis eines anderen Bluetooth Gerätes kopieren. Zu diesem Zweck wird das allgemeine OBEX PUT Kommando verwendet.

Wechselt der Anwender in ein Unterverzeichnis, wird in dieses über das OBEX SETPATH Kommando verzweigt und dessen Inhalt anschließend über das allgemeine OBEX GET Kommando angefordert. Wie das nachfolgende Beispiel in der Textbox zeigt, wird der Inhalt eines Verzeichnisses in lesbarer Form als XML Beschreibung übertragen.

Im OBEX Protokoll Layer werden CONNECT, DISCONNECT, PUT, GET, SETPATH und ABORT Kommandos und die entsprechenden Antworten darauf als Pakete behandelt. Der Wert des ersten Byte des Pakets beschreibt die Art des Kommandos. Nach einem zwei Byte Längenfeld folgen dann die Parameter des Kommandos. Ein Parameter kann z.B. ein Verzeichnisname, eine Verzeichnisauflistung oder eine angeforderte Datei sein. Diese Parameter werden im Standard etwas verwirrend als Header be-

zeichnet. Um die Art der Parameter auseinander halten zu können, hat jeder Parameter im ersten Byte eine Typinformation. Der Typ eines Parameters kann z.B. „Dateiname“ oder „Body“ (also die eigentliche Datei) sein.

```
<xml version="1.0">
<!DOCTYPE folder-listing SYSTEM „obex-folder listing.dtd">
<folder-listing-version="1.0">
   <folder name="Camera" modified="2004117T100840"
    user perm="RWD" group perm"W" />
   <folder name="other pics" modified="2004117T13321"
    user perm="RWD" group perm"W" />
</folder-listing>
```

Die maximale Paketgröße beträgt 64 kByte. Um größere Dateien (also Header vom Typ „Body“) zu übertragen, wird die Datei automatisch vom OBEX Layer in mehrere Pakete aufgeteilt.

Object Push Profile

Eine etwas einfachere Anwendung des General Object Exchange Profils ist das Object Push Profile. Dieses wird z.B. verwendet, wenn der Benutzer eines Mobiltelefons einen Kalendereintrag, einen Adressbucheintrag oder eine Datei über Bluetooth zu einem anderen Gerät übertragen möchte. Die Funktionsweise dieses Profils ist identisch zum File Transfer Profil, es verwendet ebenfalls die allgemeinen OBEX Kommandos wie PUT und GET. Das Object Push Profile unterstützt jedoch keine Verzeichnisoperationen und Löschen von Dateien. Auf diese Weise wird erreicht, dass der Benutzer beim Senden der Informationen möglichst wenige Entscheidungen treffen muss und der Vorgang somit schnell durchgeführt werden kann.

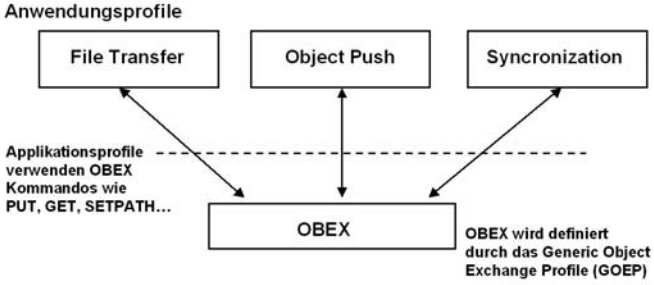

Abb 5.22: Zusammenhang zwischen OBEX, GOEP, FTP, Object Push und Synchronization Profile

Viele Endgeräte erlauben einen eingehenden Object Push Transfer ohne vorherige Authentifizierung und Verschlüsselung. Das empfangene Objekt wird dann nach Erhalt zunächst in einen Zwischenpuffer gelegt und erst nach Bestätigung des Benutzers in den Terminkalender, in das Adressbuch, oder, im Falle einer Datei, in ein Verzeichnis kopiert.

Für die Übertragung von Kalender- und Adressbucheinträgen schreibt das Object Push Profile das vCalendar, bzw. das vCard Format vor (www.imc.org). Dies ist Voraussetzung, um Adressbuch- und Kalendereinträge zwischen beliebigen Programmen und Endgeräten austauschen zu können. Bei anderen Objekten, wie z.B. Bildern, kann anhand der Endung des Dateinamens erkannt werden, um welche Art Datei es sich handelt.

Obwohl das Profil „Object Push" heißt, spezifiziert es auch optional eine Business Card Pull Funktion. Mit dieser Funktion kann man eine zuvor hinterlegte Standardvisitenkarte von einem Gerät anfordern. Die Business Card Exchange Funktion ergänzt diese Funktion, in dem nicht nur eine Visitenkarte angefordert wird, sondern auch die bei sich hinterlegte Visitenkarte automatisch dem anderen Gerät geschickt wird.

Synchronization Profile

Das dritte Profil, das auf GOEP aufsetzt, ist das Synchronization Profile. Es ermöglicht den automatischen Abgleich von Objekten wie Terminkalender- und Adressbucheinträgen, sowie Notizen zwischen zwei Geräten. Auch dafür werden wieder die allgemeinen OBEX Kommandos wie GET und PUT verwendet. Gegenüber dem Object Push Profil, über das vom Anwender nur ausgewählte Objekte, wie z.B. ein Adressbucheintrag, zu einem anderen Gerät übertragen werden können, spezifiziert das Synchronization Profile, wie der komplette Datenbestand einer Datenbank synchronisiert werden kann. Bei der ersten Synchronisation wird einmalig der komplette Datenbestand in beide Richtungen übertragen, bei allen folgenden Synchronisationen werden dann nur noch die geänderten Objekte übertragen. Zu diesem Zweck führen beide Geräte eine Protokolldatei über alle Änderungen. Damit Anwendungen unterschiedlicher Hersteller ihre Datenbankeinträge austauschen können, werden wie auch im Object Push Profil standardisierte Formate wie vCard oder vCalendar verwendet.

Der Bluetooth Standard definiert den Ablauf der Synchronisation nicht selbst, sondern verwendet dazu das Synchronisationssystem, das im IrMC Standard der Infrared Data Association (www.irda.org) definiert wurde.

5.6.4 Headset, Hands-Free und SIM-Access Profile

Headset Profile (HSP)

Drahtlose Headsets für Mobiltelefone waren die ersten Geräte, die mit Bluetooth Funktionalität auf den Markt kamen. Für die Sprachverbindung zwischen Mobiltelefon und Headset wird das Headset Profil verwendet. Dieses Profil ist eine Besonderheit, denn es verwendet als eines der wenigen Profile auch SCO oder eSCO Pakete (vgl. Kapitel 5.4.1). Mit diesen wird zwischen Mobiltelefon und Headset ein Sprachkanal mit 64 kbit/s aufgebaut. Sind Mobiltelefon und Headset kompatibel zu Bluetooth 1.2, werden automatisch eSCO Pakete verwendet, die Verbindung profitiert dann von automatischer Fehlerkorrektur und Adaptive Frequency Hopping (AFH). Diese in Bluetooth 1.2 eingeführten Funktionalitäten steigern die Sprachqualität vor allem dann wesentlich, wenn die Bluetooth Verbindung aufgrund eines großen Abstands, einer geringen Sendeleistung, oder durch Hindernisse nicht optimal ist. Ist das Headset oder das Mobiltelefon noch nicht zu Bluetooth 1.2 kompatibel, sorgt die Link Manager Schicht automatisch dafür, dass SCO Pakete verwendet werden und das AFH deaktiviert bleibt.

Um ein Headset mit einem Mobiltelefon verwenden zu können, müssen die zwei Geräte einmalig miteinander ein Pairing durchführen. Danach versucht das Mobiltelefon bei jedem eingehenden Anruf automatisch, eine Verbindung zum Headset herzustellen. Für die Signalisierung zwischen Headset und Mobiltelefon, das im Headset Profil als Audio Gateway (AG) bezeichnet wird, wird eine ACL Verbindung verwendet. Wie in Abbildung 5.23 zu sehen ist, wird für die Signalisierungsverbindung auf höheren Schichten L2CAP und RFCOMM verwendet.

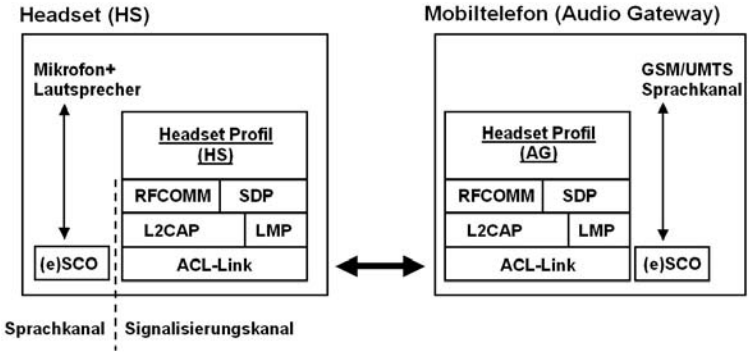

Abb. 5.23: Headset Protokollstack

Um Kommandos und die dazugehörigen Antworten zwischen Audio Gateway und Headset auszutauschen, wird das von Modems bekannte AT-Kommandoset verwendet. Das Headset Profil beschränkt sich jedoch auf nur wenige Kommandos. Wie in Abbildung 5.24 zu sehen ist, baut das Audio Gateway bei einem eingehenden Anruf zuerst eine Signalisierungsverbindung auf (ACL) und sendet über den Signalisierungskanal den String „RING“. Das Headset benachrichtigt daraufhin den Anwender über den eingehenden Anruf, in dem z.B. eine Melodie gespielt wird. Der Nutzer kann dann den Anruf durch Betätigen einer Taste am Headset annehmen. Das Betätigen der Taste bewirkt, dass das Headset das AT-Kommando at+ckpd=200 an das Audio Gateway zurückschickt. Dieses nimmt daraufhin das Gespräch an und stellt es zum Headset durch.

Um ein abgehendes Gespräch zu führen, kann umgekehrt auch das Headset eine Verbindung zum Audio Gateway herstellen. Zusammen mit einer im Audio Gateway (also im Mobiltelefon) vorhandenen Sprachwahlfunktion lassen sich somit abgehende Gespräche über das Headset starten, ohne das Mobiltelefon in die Hand zu nehmen.

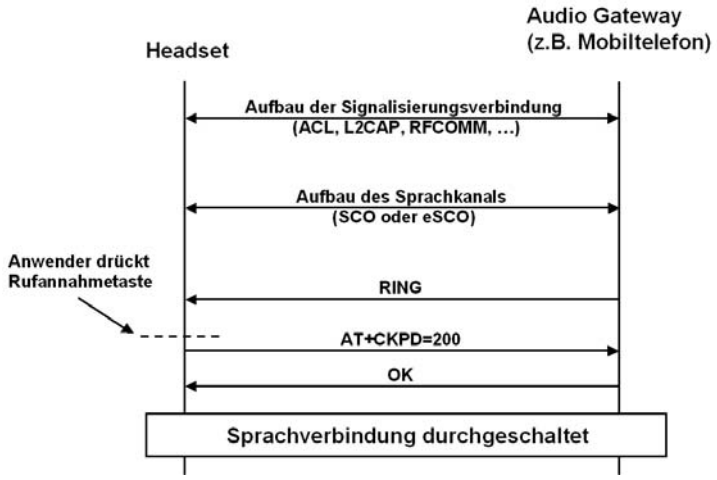

Abb. 5.24: Aufbau von Signalisierungs- und Sprachverbindung

Da die Bedienmöglichkeiten durch die Größe des Headsets begrenzt sind, bietet das Headset Profil außer der Gesprächsfunktionalität nur noch die Steuerung der Lautstärke. Dies geschieht über die Befehle +vgm für die Lautstärke des Mikrofons und mit +vgs für die Lautstärke des Lautsprechers. Mit diesen Befehlen

kann also vom Mobiltelefon aus die Lautstärke im Headset geändert werden.

Ein Headset kann auch mit einem PC gekoppelt werden, falls der Bluetooth Stack des PCs das Headset Profil unterstützt und die Rolle des Audio Gateways übernehmen kann. Auf diese Weise kann das Headset z.B. zusammen mit einer Voice over IP Software verwendet werden. Außerdem ist es durch die Umleitung der Soundkarten Ein- und Ausgänge auf das Headset theoretisch auch möglich, Musik, MP3 Streams, etc. über das Headset abzuspielen. Dies macht jedoch wenig Sinn, da der SCO Kanal auf 64 kbit/s begrenzt ist und nur für Sprachtelefonie ausgelegt ist. In der Praxis bedeutet dies, dass das Audiosignal nur mono übertragen wird und das Frequenzband auf 300-3400 Hz begrenzt ist.

Das Hands-Free Profil

Stark verwandt mit dem Headset Profil ist das Hands-Free Profil. Bei der Entwicklung dieses Profils standen jedoch nicht Headsets im Vordergrund, sondern KFZ-Freisprecheinrichtungen. Wichtigste Aufgabe des Hands-Free Profil ist das Ersetzen der Kabelverbindung zwischen Freisprecheinrichtung und Mobiltelefon. Auf diese Weise muss das Mobiltelefon bei Fahrtantritt nicht in einer Halterung festgemacht werden und kann sich während der Fahrt an einer beliebigen Stelle im Auto befinden. Diese Aufgabe könnte auch mit dem Headset Profil bewerkstelligt werden. Da Freisprecheinrichtungen aber heute weit mehr Funktionen bieten, als nur an- und abgehende Gespräche zu führen, wurde das Hands-Free Profil definiert.

Die grundsätzliche Funktionsweise des Hands-Free Profil ist mit dem Headset Profil identisch. Kommandos und entsprechende Antworten werden zwischen Freisprecheinrichtung (Hands-Free Unit) und dem Mobiltelefon (Audio Gateway) ebenfalls über AT-Kommandos ausgetauscht. Außerdem wird ebenso wie beim Headset Profil der Sprachkanal über eine SCO oder eSCO Verbindung geleitet. Zusätzlich zu den Funktionen des Headset Profils bietet das Hands-Free Profil auch folgende Möglichkeiten:

- Die Übertragung der Rufnummer des Anrufers an die Freisprecheinrichtung (CLIP Funktion).
- Abweisen von ankommenden Gesprächen von der Freisprecheinrichtung aus.
- Wählen einer Telefonnummer von der Freisprecheinrichtung.
- Gespräch halten sowie Dreierkonferenzsteuerung.

- Übertragung von Statusinformationen wie verbleibende Batteriekapazität und GSM/UMTS Empfangsstärke des Mobiltelefons.
- Roaminganzeige.
- Deaktivieren der optionalen Echounterdrückung im Endgerät, falls dies vom Endgerät unterstützt wird. Dies ist sinnvoll, wenn die Freisprecheinrichtung eine eigene Echounterdrückung besitzt.

Möchte ein Mobiltelefon Headsets und Freisprecheinrichtungen unterstützen, sollte es das Headset- und das Hands-Free Profil beherrschen. Manche Headsets verfügen zwar zusätzlich zum Headset-Profil auch über das Hands-Free Profil, dies ist aber beim Kauf oft nicht ersichtlich.

Leider ist in den Bluetooth Standards keine Interoperabilität zwischen den zwei Profilen definiert. Hat ein Anwender also sowohl ein Headset, um außerhalb des Autos zu telefonieren und zusätzlich eine Freisprecheinrichtung für Gespräche im Auto, ist nicht festgelegt, mit welchem Gerät das Mobiltelefon bei ankommenden Verbindungen kommunizieren soll. Einfache Implementierungen kommunizieren entweder nur mit dem Headset oder nur mit der Freisprecheinrichtung, in Abhängigkeit davon, mit welchem Gerät zuletzt ein Pairing durchgeführt wurde. Als Alternative wäre denkbar, dass der Anwender verschiedene Betriebsmodi im Mobiltelefon auswählen kann. Bei Beginn und Ende der Fahrt müsste der Anwender jedoch das Mobiltelefon immer entsprechend umstellen, was wiederum den Bedienkomfort einschränken würde. Eine Lösung dieses Problems wäre beispielsweise eine Bluetooth Freisprecheinrichtung mit abnehmbarem Bluetooth Headset. Befindet sich das Bluetooth Headset in der Freisprecheinrichtung, stellt es die Bluetooth Verbindung für die Freisprecheinrichtung zum Mobiltelefon dar. Verlässt der Anwender das Auto, nimmt er einfach das Headset mit.

Das SIM-Access Profile

Eine weitere Lösungsmöglichkeit für die gleichzeitige Verwendung eines Headsets und einer KFZ-Freisprecheinrichtung bietet das SIM-Access Profil. Im Unterschied zum Headset und Hands-Free Profil dient das Mobiltelefon beim SIM-Access Profil nicht als Audio Gateway, und somit als Brücke zum Mobilfunknetzwerk, sondern stellt nur die SIM Karte einem externen Gerät zur Verfügung. Abbildung 5.25 zeigt dieses Szenario. Das externe Gerät, in den meisten Fällen also eine KFZ-Freisprecheinrichtung, enthält ein eigenes GSM/UMTS Mobiltelefon, jedoch ohne SIM Karte. Wird die Freisprecheinrichtung bei Fahrtantritt

aktiviert, wird per Bluetooth Kontakt zum gekoppelten Mobiltelefon hergestellt. Durch die Aktivierung des SIM-Access Servers im Mobiltelefon wird automatisch der Mobilfunkteil deaktiviert. Dies ist notwendig, da die Mobiltelefoneinheit in der Freisprecheinrichtung fortan die Kommunikation mit dem Mobilfunknetzwerk übernimmt. Ein großer Vorteil dieser Methode ist weiterhin, dass die Freisprecheinrichtung auch an die KFZ-Spannungsversorgung und an eine Außenantenne angeschlossen ist. Dies können Headset und Hands-Free Profil nicht bieten.

Abbildung 5.25 zeigt außerdem den für das SIM-Access Profil verwendeten Protokollstack. Auf der L2CAP Verbindung wird der RFCOMM Layer für eine serielle Übertragung zwischen Freisprecheinrichtung (SIM-Access Client) und Mobiltelefon (SIM-Access Server) verwendet. Neben SIM-Access Profil Kommandos für die Aktivierung, Deaktivierung und den Reset der SIM-Karte werden über den Bluetooth Kanal auch SIM-Karten Kommandos und Antwortnachrichten ausgetauscht. Kommandos und Antwortnachrichten werden als Application Protocol Data Units (APDUs) übertragen. Diese wurden bereits in Kapitel 1.10 beschrieben und in den Abbildungen 1.49 und 1.50 dargestellt. Statt die APDUs also zwischen Mobilfunkteil und SIM Karte des Mobiltelefons über das elektrische Interface auszutauschen, werden mit dem SIM-Access Profil die APDUs über die Bluetooth Schnittstelle ausgetauscht. Für die Software der Freisprecheinrichtung, die auf dem SIM-Access Profile aufsetzt, ist es also völlig transparent, dass die SIM Karte nicht fest eingebaut ist, sondern über Bluetooth angesprochen wird.

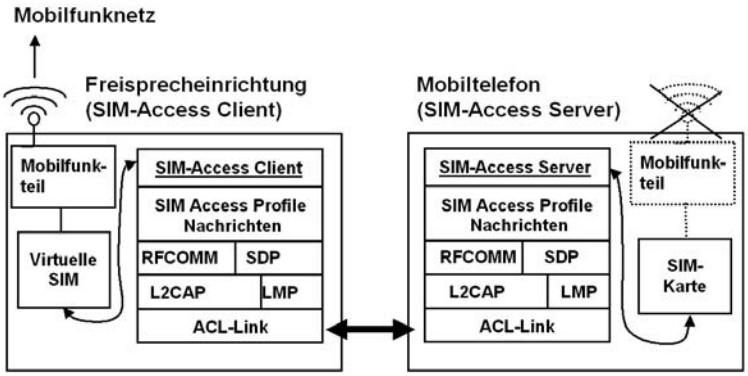

Abb. 5.25: Funktionsweise des SIM-Access Profils

Durch die Verwendung von APDUs können nicht nur die Dateien auf der SIM Karte gelesen und geschrieben werden, sondern es kann auch der Authentifizierungsalgorithmus der SIM-Karte angesprochen werden, der zu einer Zufallszahl (RAND) eine Signed Response (SRES) erzeugt (vgl. Kapitel 1.6.4). Außerdem kann auch das SIM Application Toolkit Protokoll über die Bluetooth Verbindung genutzt werden. Auch diese Nachrichten werden, wie ebenfalls in Kapitel 1.10 gezeigt, in APDUs verpackt.

5.6.5 High Quality Audio Streaming

Sowohl das Handset- als auch das Handsfree Profil wurden ursprünglich entwickelt, um Sprache in Telefonqualität und in mono zu übertragen. Für Hifi Audiostreaming reicht diese Qualität jedoch bei weitem nicht aus. Für diese Anwendung wurde deshalb das Advanced Audio Distribution Profil (A2DP) entwickelt, das Audiodaten mit Bandbreiten von 127 - 345 kbit/s überträgt. Da solche Datenraten nicht über SCO Verbindungen transportiert werden können, verwendet dieses Profil ACL Links zum Datentransport. Erste Versionen des Profils gibt es schon seit 2003, es dauerte jedoch einige Jahre, bis erste Geräte etwa 2006/07 auf den Markt kamen. Zu Geräten, die das A2DP Profil unterstützen sind Mobiltelefone mit eingebautem MP-3 Player und Kopfhörer. Kopfhörer unterstützen üblicherweise sowohl das A2DP und die Handsfree und Headset Profile. Mit einem eingebauten Mikrofon können diese dann sowohl für Musik als auch zum Telefonieren verwendet werden.

Rechtemanagement

Eines der großen Probleme bei der Übertragung von digitalen Audiosignalen ist das Rechtemanagement. Aus diesem Grund bietet das A2DP Profil Methoden, einen Audiodatenstrom verschlüsselt per Bluetooth zu übertragen. Somit wird das Abhören und Kopieren des Audiosignals auf dem Übertragungsweg unterbunden. Der Standard überlässt es jedoch den Herstellern, geeignete Schutzalgorithmen zu implementieren. Aus diesem Grund ist es fraglich, ob es hier Lösungen geben wird, die zwischen Herstellern kompatibel sind.

A2DP Protokollstack

Abbildung 5.26 zeigt den A2DP Protokollstack. Das Profil basiert auf GAP und erlaubt somit anderen Endgeräten, die unterstützten Funktionalitäten in der SDP Datenbank abzufragen. Oberhalb des L2CAP Layer wurde das Audio Video Distribution Transfer Protocol (AVDTP) für die Datenübertragung spezifiziert. Wie der Name des Protokolls schon andeutet, kann es sowohl für die Übertragung von Audiodaten, als auch für die Übertragung von

Videostreams verwendet werden. Das A2DP Profil verwendet das Protokoll jedoch lediglich für die Übertragung von Audiodaten. Neben der Übertragung des reinen Audiostreams werden auch Kontrollinformationen wie z.B. Codec Vereinbarungen und Austausch von Parametern wie der benötigten Bandbreite über das AVDTP Protokoll abgewickelt. Höhere Kontrollfunktionen wie z.B. das Springen zum nächsten Musikstück oder das Pausieren der Übertragung sind nicht Teil von AVDTP und werden über das Audio/Video Control Transport Protocol (AVCTP) übertragen, das nachfolgend beschrieben wird.

Der Bluetooth Standard erlaubt einem Endgerät, mehrere Verbindungen zu mehreren Geräten gleichzeitig geöffnet zu haben. Unterstützt ein Gerät dies, kann z.B. eine A2DP Verbindung zwischen einem Notebook und einem Kopfhörer aufgebaut sein, während gleichzeitig das Dial-Up Profil verwendet wird, um das Notebook über ein Mobiltelefon mit dem Internet zu verbinden. Eine A2DP Übertragung benötigt jedoch für einen Audiostream in guter Qualität schon einen großen Teil der über Bluetooth möglichen Bandbreite, so dass der Internet Zugang entsprechend langsam erscheint. Unterstützten alle Endgeräte im Piconet den Bluetooth 2.0 + EDR Standard, wird dies sicher weniger auffallen, da die Bandbreite dann etwa 2 MBit/s beträgt. Dies ist deutlich mehr als bei Version 1.2 mit einem Limit von 723 kbit/s, von denen dann mit dem besten Audio Codec 345 kbit/s für die Audioübertragung verwendet werden.

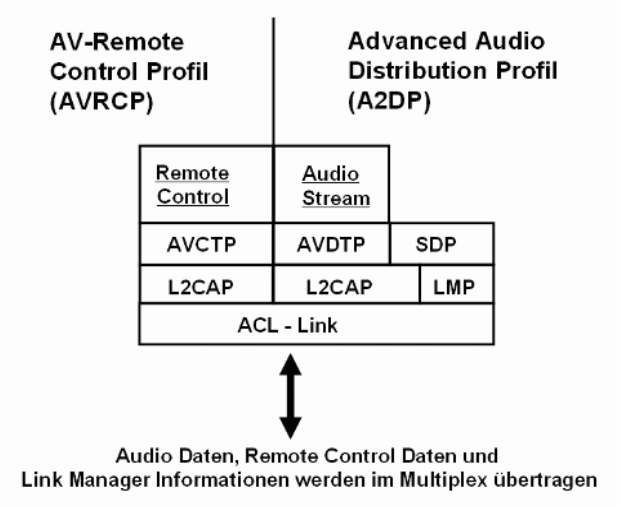

Abb. 5.26: Der A2DP Protokoll Stack inklusive Remote Control

Das A2DP Profil spezifiziert zwei Rollen für eine Verbindung. Die Audio Source Rolle wird von Geräten wie MP-3 Playern, Mobiltelefonen oder einem Mikrofon übernommen. Die andere Seite der Verbindung ist die Audio Senke (Audio Sink) Rolle, die üblicherweise von einem Headset oder einem Bluetooth Lautsprecherset übernommen wird.

Audio Codecs

Um mindestens einen gemeinsamen Audio Codec für eine A2DP Übertragung zwischen zwei Geräten zu gewährleisten, enthält die A2DP Spezifikation ein proprietäres Audioformat, das Subband Codec (SBC) genannt wird. Dieses muss von allen A2DP kompatiblen Endgeräten unterstützt werden und wird nachfolgend kurz beschrieben. Außerdem definiert der Standard die Übertragung anderer Codecs wie MPEG 1-2 Audio, MPEG-2,4, AAC und ATRAC über das Audio/Video Distribution Protocol (AVDTP). Diese Codecs sind optional. Der Standard erlaubt auch die Übertragung von weiteren Codecs über AVDTP. Um eine Interoperabilität zwischen Geräten unterschiedlicher Hersteller zu gewährleisten, muss ein Gerät jedoch immer in der Lage sein, einen Audiostream in SBC zu konvertieren, wenn ein anderes Gerät kein anderes optionales Format unterstützt.

Der SBC Codec

Grundsätzlich ist der SBC Codec wie folgt aufgebaut: Als Eingangssignal erwartet der SBC Codec ein PCM kodiertes Audiosignal mit einer Abtastfrequenz von 44.1 oder 48 kHz. Der Codec teilt im ersten Schritt dann das Frequenzband des Eingangssignals in mehrere Teilbereiche auf, die auch als Unterbänder (Sub-Bands) bezeichnet werden. Der Standard rät, das Signal entweder in vier oder in acht Unterbänder aufzuteilen. Danach wird ein Skalierungsfaktor für jeden Unterkanal berechnet, der die Lautstärke des Signals in diesem Unterband beschreibt. Die Skalierungsfaktoren werden dann miteinander verglichen, um dem Unterband mit der meisten Signalinformation auch die meisten Bits für die Kodierung zuzuordnen. Der Standard schlägt vor, mindestens 19 Bit für eine mittlere Audioqualität und einen Monokanal zu verwenden und bis zu 55 Bits für Stereokanäle mit hoher Qualität. Nach der Kodierung der Audioinformation der Unterkanäle werden die Datenströme komprimiert. Der Kompressionsfaktor ist variabel, und es besteht somit hier nochmals die Möglichkeit, eine Abwägung zwischen Datenrate und Audioqualität zu treffen. Wird für die Kompression der niedrigste Faktor verwendet und Stereokanäle mit höchster Qualität kodiert, erzeugt dies einen Datenstrom mit einer Geschwindigkeit von 345 kbit/s.

Gerätekategorien

Um Benutzeranweisungen vom Audio Sink Device (z.B. einem Kopfhörer) wie Lautstärkeregelung, nächster Track, Pause, etc., zurück zum Audio Source Gerät (z.B. einem MP-3 Player) zu übertragen, wird das Audio/Video Remote Control Profile verwendet. Wie in Abbildung 5.26 gezeigt, wird dazu das Audio/Video Control Transport Protocol verwendet. Auch diese Nachrichten sind standardisiert um sicherzustellen, dass Endgeräte verschiedener Hersteller zusammenarbeiten. Das Profil unterscheidet Controller und Target (Ziel) Geräte und gruppiert diese in folgende Kategorien:

- Kategorie 1: Abspiel- und Aufnahmegeräte
- Kategorie 2: Monitor/Verstärker
- Kategorie 3: Audio/Video Empfänger (z.B. Radio)
- Kategorie 4: Menu

Standardisierte Aktionen

Des Weiteren definiert der Standard eine Vielzahl von Kontrollkommandos (Operation IDs) und legt fest, welche Geräte in welchen Gerätekategorien diese Kommandos jeweils unterstützen müssen und welche optional sind. Standardisierte Kontrollkommandos sind z.B.: ‚select', ‚up', ‚right', ‚root menu', ‚setup menu', ‚channel up', ‚channel down', ‚volume up', ‚volume down', ‚play', ‚stop', ‚pause', ‚eject', ‚forward' und ‚backward'. Endgerätehersteller können auch selber Kommandos definieren, diese können jedoch nicht zwischen Geräten unterschiedlicher Hersteller verwendet werden.

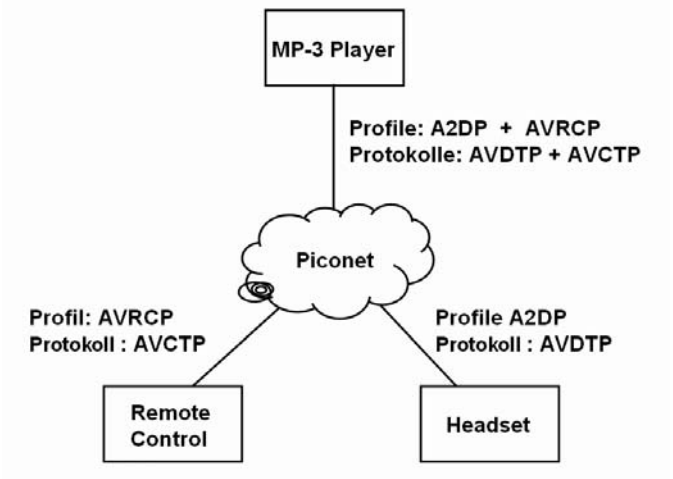

Abb. 5.27: Gleichzeitige Übertragung eines Audio Streams und Kontrollkommandos zwischen verschiedenen Geräten

Zwischen der Audio Streaming Session mit dem A2DP Profil und der Kontrollsession mit dem Remote Control Profil gibt es keine direkte Verbindung. Somit ist es möglich, in einem Piconet einen MP-3 Player für die Übertragung von Musik zu einem Kopfhörer zu verwenden, währen Lautstärkekommandos und andere Anweisungen von einem dritten Gerät, wie z.B. einer Fernbedienung, an den MP-3 Player gesendet werden können. Dieses Szenario ist in Abbildung 5.27 dargestellt.

5.7 Vergleich zwischen Bluetooth und Wireless LAN

Vor allem im letzten Abschnitt über die diversen Bluetooth Profile ist deutlich geworden, dass Wireless LAN und Bluetooth großteils keine konkurrierenden, sondern sich optimal ergänzende Technologien sind.

Die große Stärke von Wireless LAN liegt im Netzwerkbereich, denn es ersetzt ein Ethernet Kabel durch eine drahtlose Verbindung. Bei der voranschreitenden Entwicklung von Wireless LAN wird großen Wert auf möglichst hohe Geschwindigkeiten gelegt, die heute mit 802.11n im Bereich von bis zu 150 MBit/s auf Anwendungsebene liegen. Wireless LAN fügt sich somit optimal in den Netzwerkbereich ein, denn aus Sicht einer Netzwerkanwendung besteht kein Unterschied zwischen einem drahtgebundenen und drahtlosen Ethernet. Trotz Stromsparmechanismen ist der Stromverbrauch eines Wireless LAN Chips aber nicht zu vernachlässigen und führt bei kleinen batteriebetriebenen Geräten wie PDAs zu deutlich kürzen Akkulaufzeiten. Trotzdem werden heute zunehmend neben PCs und Notebooks auch PDAs und Smartphones mit Wireless LAN ausgestattet, da es heute in vielen privaten Haushalten, Firmen und öffentlichen Gebäuden wie Hotels oder Cafes WLAN Access Points für den Zugang zum Internet gibt.

Auch Bluetooth kann für die Vernetzung von Notebooks, PCs und PDAs genutzt werden. Die gegenüber Wireless LAN geringe Geschwindigkeit von 723 kbit/s (also 0.7 MBit/s) bzw. 2.178 MBit/s mit EDR macht dieses System dafür aber nur in Ausnahmefällen zur besseren Wahl. Wie im letzten Unterkapitel gezeigt, liegen die großen Stärken von Bluetooth außerhalb des Local Area Netzwerks. Von der schnellen und einfachen Übertragung von Dateien, Visitenkarten, Terminen und Adressbucheinträgen, über Kabelersatz für Internetverbindungen mit Mobiltelefonen, für Headsets und Freisprecheinrichtungen, bis hin zum Kabeler-

satz für den Schreibtisch zwischen PC, Drucker, Maus und Tastatur, eröffnen sich für Bluetooth eine Vielzahl von Anwendungsgebieten. Für die meisten dieser Anwendungen ist die mit Bluetooth mögliche Geschwindigkeit bei weitem ausreichend und die integrierten Stromspartechniken in vielen Fällen eine unverzichtbare Voraussetzung.

Aus diesen Gründen ist absehbar, dass in Zukunft vermehrt PCs, Notebooks, PDAs und Smartphones auf den Markt kommen werden, die sowohl über Bluetooth, als auch über Wireless LAN verfügen, um so von den Möglichkeiten beider Funksysteme zu profitieren.

5.8 Fragen und Aufgaben

1. Welche maximale Geschwindigkeit bietet Bluetooth und von welchen Faktoren hängt diese ab?
2. Was bedeutet der Begriff Frequency Hopping Spread Spectrum (FHSS) und welche erweiterten Möglichkeiten bietet der Bluetooth 1.2 Standard?
3. Was ist der Unterschied zwischen Inquiry und Paging?
4. Welche Stromsparmodi gibt es bei Bluetooth?
5. Welche Aufgaben hat der Link Manager?
6. Wie können über das L2CAP Protokoll unterschiedliche Datenströme für unterschiedliche Anwendungen im Zeitmultiplex übertragen werden?
7. Welche Aufgaben hat die Service Discovery Datenbank?
8. Wie können mehrere Dienste gleichzeitig die RFCOMM Schicht verwenden?
9. Was ist der Unterschied zwischen der Bluetooth Authentifizierung und Autorisierung?
10. Warum gibt es eine Vielzahl unterschiedlicher Bluetooth Profile?
11. Wie kann über das Dial-Up Netzwerk (DUN) Profil eine Internetverbindung über ein Mobiltelefon aufgebaut werden?
12. Welche Profile gibt es für die einfache und schnelle Übertragung von Dateien und Objekten zwischen zwei Bluetooth Endgeräten?

13. Wie unterscheidet sich das Hands-Free Profil vom SIM-Access Profil?
14. Warum gibt es Geräte, die über Wireless LAN und Bluetooth verfügen?

Literaturverzeichnis

Bücher

Bray, Jennifer und Sturman, Charles F.: Bluetooth – Connect Without Cables, 2. Auflage, Prentice Hall, 2002

Gast, Matthew S.: 802.11 Wireless Networks, 2nd Edition, O'Reilly, 2005

Heine, Gunnar: GSM-Signalisierung verstehen und praktisch anwenden, Franzis Verlag, 2001

Heine, Gunnar: GPRS - Gateway zu Mobilfunknetzen der 3. Generation, Franzis Verlag, 2001

Korhonen, Juha: Introduction to 3G Mobile Communications, 2. Auflage, Artech House, 2003

Lescuyer, Pierre: UMTS, Grundlagen, Architektur und Standard, DPunkt Verlag, 2002

Harri Holma und Antti Toskala, HSDPA/HSUPA for UMTS, John Wiley & Sons, 2006

Ralf Kreher und Torsten Rüdebusch: UMTS Signaling, John Wiley & Sons, 2005

Newton, Harry: Newton's Telecom Dictionary, 20. Auflage, Telecom Books, 2004

Internet

Website zu diesem Buch: http://www.cm-networks.de

GSM, GPRS und UMTS Standards: http://www.3gpp.org

Bluetooth Standards: http://www.bluetooth.org

Wireless LAN 802.11 Standards: http://www.ieee.org

Wireless LAN Zertifizierung und Artikel: http://www.wi-fi.org

GSM Association und Artikel zum Thema GSM, GPRS und UMTS: http://www.gsmworld.com

Technische Informationen rund um den Mobilfunk in Deutschland: http://www.nobbi.com

Heise Mobilfunknachrichten: http://www.heise.de/mobil

Auswahl von Herstellern von GSM, GPRS und UMTS Netzwerkinfrastruktur:

http://www.nortel.com

http://www.nokiasiemensnetworks.com/

http://www.ericsson.com

http://www.motorola.com

http://www.alcatel-lucent.com

http://www.huawei.com

Sony Ericsson Softwareentwickler Website:
http://developer.sonyericsson.com

Nokia Softwareentwickler Website:
http://www.forum.nokia.com

Sachwortverzeichnis

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z