Lösungsheft zu Mobilkommunikation, 2. Auflage

Jochen H. Schiller, Freie Universität Berlin

schiller@computer.org, www.jochenschiller.de

1. Einführung

1.1 Gute Quellen für Teilnehmerzahlen und weitere Statistiken sind beispielsweise www.gsmworld.com, www.3gpp.org, www.3gpp2.org, www.emc-database.com, www.3g.co.uk, www.regtp.de …

1.2 Die heutigen GSM-Netzbetreiber fügen die neuen 3G-Luftschnittstellen von UMTS zu ihren bereits existierenden GSM/GPRS-Infrastrukturen hinzu. Heutige GSM/GPRS-Netze bieten bereits paket- und leitungsvermittelte Datenübertragung nach Release 99 von UMTS. Die Betreiber müssen natürlich neue Funkzugangsnetze installieren, also Antennen, Funksteuerungen etc., wie in Kapitel 4 beschrieben. Die Situation ist ähnlich für Netzbetreiber, die heute die cdmaOne-Technik (IS-95) einsetzen. Allerdings werden diese Betreiber cdma2000 wählen, da dieses System eine Weiterverwendung der bereits existierenden Infrastruktur erlaubt. Daher wird die (sehr grobe) Aufteilung heutiger Netze in CDMA- und GSM-Systeme auch zu zwei unterschiedlichen 3G-Systemen führen: cdma2000 und UMTS (inklusive ihrer zukünftigen Versionen). Derzeit sieht es nicht so aus, als könnte sich ein drittes 3G-System etablieren. Heutige TDMA-Netzbetreiber werden vermutlich mit EDGE erweiterte Systeme einsetzen oder ebenfalls auf UMTS setzen. Es ist allerdings noch offen, was in China passieren wird. Das chinesische System TD-SCDMA wurde anfänglich stark von der Regierung gefördert, allerdings fehlen noch entsprechende Netze und Geräte. Heute nutzen die meisten Teilnehmer in China GSM, einige Betreiber bieten auch CDMA an – sogar PHS wird in manchen Städten als Alternative genutzt.

2. Drahtlose Übertragung

2.1 Überprüfen Sie auch die unterschiedlichen WRCs, die versuchen, die globalen Frequenzbelegungspläne zu harmonisieren.

2.2 Unterhalb 2 MHz folgen Funkwellen weitgehend der Oberfläche (Bodenwellen). Ein Grund hierfür ist die Beugung (Wellen werden in Richtung von Objekten gebeugt, deren Größe in etwa der der Wellenlänge entspricht), ein weiterer Faktor ist der Strom, der in der Erdoberfläche induziert wird. Dies verlangsamt die Wellenfront in der Nähe der Erdoberfläche, was dann diese Wellenfront nach unten in Richtung der Oberfläche biegt. Mehrere Gründe verhindern in den meisten Fällen den Einsatz niedriger Frequenzen in Rechnernetzen:

- Niedrigere Frequenzen bedeuten niedrigere Datenraten nach Nyquist/Shannon, da auch die verfügbare Bandbreite kleiner ist.
- Niedrige Frequenzen benötigen auch große Antennen für eine effiziente Übertragung und einen guten Empfang. Diese Antennen mögen für U-Boote sinnvoll sein, nicht für Mobiltelefone.
- Tiefe Frequenzen durchdringen gewisse Materialien leichter. Daher ist Raummultiplex schwerer zu verwirklichen – die Zellgrößen würden sehr stark anwachsen und eine Wiederverwendung von Frequenzen ist praktisch nicht machbar.

2.3 Frequenzen im THz-Bereich, z.B. infrarotes oder sichtbares Licht, können sehr leicht durch verschiedene Objekte blockiert werden und stören daher kaum andere Übertragungen. In diesem Fall müssen nur gewisse Sicherheitsbestimmungen eingehalten werden (z.B. Laser-Emissionen). Die meisten Funksysteme bleiben deutlich unter 100 GHz, da es nicht einfach ist, höhere Frequenzen (im unteren THz-Bereich) zu erzeugen.

2.4 Der klassische europäische Ansatz basierte auf Standardisierung und Regulierung bevor irgendwelche Produkte verfügbar waren. Die Länder der EU gründeten ETSI zur Harmonisierung der nationalen Regulierungen. ETSI entwarf die Standards, alle

Länder müssen folgen. In den USA entwickeln Firmen Systeme und versuchen sie zu standardisieren oder lassen die Marktkräfte über den Erfolg entscheiden. Die FCC reguliert beispielsweise nur die Fairness zwischen verschiedenen Systemen, favorisiert jedoch nicht ein bestimmtes System. Die Auswirkungen der beiden Ansätze sind dann auch unterschiedlich. Viele durch offizielle Organisationen oder Regierungen geschaffene Standards versagten komplett, wie z.B. HIPERLAN 1, einige hatten nur in Europa richtig Erfolg, z.B. ISDN, und wenige wurden dann doch eine weltweite Erfolgsstory, wie GSM. Für die meisten Systeme arbeitet der US-Ansatz besser – zuerst die Produkte, dann die Standards. Ein gutes Beispiel hierfür ist die WLAN-Familie 802.11, ein gutes Gegenbeispiel ist der Markt der Mobilfunksysteme: mehrere, zueinander inkompatible System versuchen erfolgreich zu sein, viele typische Möglichkeiten der Netze, seit langem Standard in Europa, sind in den USA (noch) nicht einmal richtig bekannt (freies Roaming, MMS, GPRS-Roaming, keine Kosten, wenn man angerufen wird etc.).

2.5 Computer im Gegensatz zu beispielsweise Fernsehern reisen rund um die Welt als Laptops, PDAs etc. Nutzer wollen ihre Geräte natürlich möglichst überall einsetzen. Aus diesem Grund ist es auch sehr wichtig, dass integrierte Funkmodule rund um die Welt ohne Rekonfiguration und ohne Lizenzierung genutzt werden dürfen. Weiterhin ist es natürlich auch für WLAN-Hersteller deutlich billiger, wenn nur ein System für einen riesigen Markt entwickelt werden muss im Vergleich zu vielen Systemen für vergleichsweise kleine Märkte.

2.6 Nein. Eine verlustfreie Übertragung von analogen Signalen ist nicht möglich. Dämpfung, Dispersion usw. werden immer die Signale stören. Zudem wird ja jedes Signal als „Bündel“ von analogen Sinuswellen (Fourier!) übertragen. Ein perfektes digitales Signal mit einem rechteckigen Signalverlauf würde eine unendliche Zahl an Sinuswellen benötigen, um exakt nachgebildet werden zu können (das digitale Signal könnte als Summe einer unendlichen Zahl von Sinusfunktionen nach Fourier dargestellt wer-

den). Allerdings kann kein Medium unendlich hohe Frequenzen übertragen. Daher kann unter anderem auch ein digitales Signal nicht störungsfrei übertragen werden.

2.7 Ohne zusätzliche „Intelligenz“ sind gerichtete Antennen nicht sinnvoll in normalen Mobiltelefonen, da ein Nutzer sicher nicht immer sein Telefon in Richtung einer Basisstation ausrichten will. Nutzer bewegen sich, drehen sich, rotieren beliebig Mobiltelefone usw. Handys befinden sich weiterhin in Taschen, Jacken, ... während die Freisprecheinrichtung genutzt wird. Daher gibt es keine Möglichkeit einer gerichteten Übertragung. Allerdings umfassen neue Entwicklungen auch schnelle Signalprozessoren und viele Antennen, um damit eine dynamisch anpassbare Richtwirkung zu erzeugen (Strahlformung). Es gibt mehrere Möglichkeiten den Antennengewinn zu steigern: richtige Dimensionierung (z.B. halbe Wellenlänge), mehrere Antennen plus Signalprozessoren zur Rekombination der Signale, aktive oder passive Komponenten an der Antenne (vgl. klassische Fernsehantennen, Satellitenempfänger etc.).

2.8 Probleme: Dämpfung, Streuung, Beugung, Reflexion, Brechung. Abgesehen von der Dämpfung können alle anderen Effekte die Wellen von einer geradlinigen Ausbreitung abbringen. Nur im Vakuum und ohne weitere Gravitationseffekte folgen Radiowellen einer geraden Linie. Ohne Reflexion wäre der Funkempfang in Städten praktisch unmöglich, da nur sehr selten eine direkte Sichtverbindung zwischen Antennen existiert. Allerdings sind Reflexionen maßgeblich für die Mehrwegeausbreitung verantwortlich, welche ISI erzeugt.

2.9 Verringerung der ISI-Effekte: genügend große Schutzabstände zwischen Symbolen/niedrige Symbolrate (z.B. OFDM: Verteilung eines Symbolstroms auf viele unterschiedliche Träger), Kanalschätzung/Berechnung der n stärksten Pfade und entsprechende Anpassung der Empfänger. Der Einsatz höherer Frequenzen verringert die Effekte der Mehrwegeausbreitung und damit ISI (die Wellen verhalten sich mehr und mehr wie Licht). Je höher die Symbolrate, desto höher ISI-Effekte. Sobald sich Sender und/oder Empfänger schnell bewegen, sind die Chancen für ISI höher, da sich die Position von Hindernissen schnell verändert und damit auch die Anzahl, Stärke

und die Ankunftszeit der sekundären Impulse. Es ist somit schwerer den Signalen zu folgen und entsprechend die Verzögerungsglieder in den Empfängern für die Rekombination der Signale richtig einzustellen. ISI verringert die mögliche Bandbreite eines TDM-Verfahrens deutlich, da auch die Schutzzeiten eine gewisse Zeit beanspruchen.

2.10 Es gibt mehrere Mechanismen, welche schmalbandige Störungen verringern (die natürlich auch durch andere Sender hervorgerufen werden können):

- Dynamische Frequenzwahl: Sender können vor einem Zugriff auf ein Medium dieses zunächst auf Störungen hin abtasten, um dann einen Frequenzbereich zu wählen, auf dem keine oder zumindest wenige Störungen vorhanden sind. HiperLAN2 und 802.11h verwenden dieses Verfahren. Netzbetreiber können dieses Verfahren auch dazu verwenden, dynamisch die Funkfrequenzen zu Zellen in Mobilfunksystemen zuzuweisen. DFS hat eine vergleichsweise geringe Komplexität.
- Frequenzspringen: Das langsame Wechseln der Trägerfrequenz (slow frequency hopping), bei dem mehrere Symbole auf einer Frequenz gesendet werden, kann zumindest die meiste Zeit bzw. mit einer gewissen Wahrscheinlichkeit Frequenzen mit Störungen vermeiden. Dieses Verfahren kann z.B. in GSM eingesetzt werden. Weiterhin kann dieses Verfahren auch als Mehrfachzugriffstechnik eingesetzt werden, wie dies beispielsweise Bluetooth-Systeme tun. Dies ist immer noch ein langsamer Wechsel der Trägerfrequenz (1600 Mal pro Sekunde), da Bluetooth viele Symbole, im Prinzip sogar ein ganzes Datenpaket auf der gleichen Frequenz sendet. Verfahren mit einem schnellen Frequenzwechsel (fast frequency hopping) verteilen ein Symbol über mehrere Frequenzen und erzeugen so ein stark gespreiztes Spektrum. FH-Systeme haben eine mittlere Komplexität. Ein wichtiger Systemaspekt ist die genaue Synchronisation der Geräte.
- DSSS (Direct sequence spread spectrum): Die Daten werden Exklusiv-Oder verknüpft mit einer Chipping-Sequenz, was in einem gespreizten Signal resultiert. Dieses Verfahren wird in allen CDMA-Systemen eingesetzt, aber ebenso in

WLANs, welche einen Barker-Code zum Spreizen einsetzen (z.B. 802.11). Das Signal wird dabei über ein großes Spektrum gespreizt und daher zerstört eine schmalbandige Störung auch nur einen kleinen Anteil des Signals. Das Verfahren ist recht leistungsfähig, benötigt jedoch auch leistungsstärkere Empfänger, die das Originalsignal wieder aus der Mixtur der empfangenen gespreizten Signale herausfiltert.

2.11 Die weltweiten Regulierungen verwenden immer FDM um verschiedene Systeme voneinander zu trennen (Fernsehen, WLAN, Radio, Satelliten usw.). Aus diesem Grund müssen Funksysteme ihr digitales Signal auf eine Trägerfreqeunz mit Hilfe einer analogen Modulation aufmodulieren. Das klassische und bekannteste Beispiel ist hierbei der traditionelle Rundfunk: Musik und Sprache verwenden stets Frequenzen im Bereich von etwa 10 Hz bis 22 kHz. Es wollen jedoch viele Rundfunkstationen ihr Programm gleichzeitig in der gleichen Region ausstrahlen. Daher müssen die ursprünglichen Signale, die ja alle die gleichen Frequenzen nutzen, auf unterschiedliche Trägerfrequenzen moduliert werden. Weitere Motivationen für eine Modulation sind Antennen- und Medieneigenschaften. Wesentliche Merkmale einer digitalen Modulation sind die spektrale Effizienz, die Leistungseffizienz und die Robustheit. Typische Verfahren sind ASK, FSK und PSK.

2.12 Der Empfänger kann den Abstand zwischen einem empfangenen „Punkt“ und benachbarten Punkten im Diagramm überprüfen. Danach kann der nächstgelegene Punkt ausgewählt und somit angenommen werden, dass der Sender tatsächlich die Daten gesendet hat, welche von diesem Punkt repräsentiert werden. Je mehr Punkte allerdings von einem PSK-Schema eingesetzt werden, desto höher sind die Chancen, dass Störungen (Rauschen) einen übertragenen „Punkt“ auf einen anderen schieben. Sind die Abstände zwischen den Punkten zu klein, insbesondere kleiner als die Stärke des Rauschens während der Übertragung, so sind die Chancen sehr groß, dass ein Empfänger die empfangenen Signale auf einen falschen Punkt im Konstellationsdiagramm abbildet. (Achtung: Die Daten werden mit Hilfe von PSK co-

diert, die Punkte im Konstellationsdiagramm repräsentieren bestimmte Codes, diese Codes werden dann gesendet – es ist lediglich anschaulicher in „Punkten“ zu denken.)

2.13 Hauptvorteile: sehr robust gegenüber Interferenzen, inhärente Sicherheit (falls der Spreizcode nicht bekannt ist, dann ist es auch sehr schwer, die Übertragung mitzuhören), Basis für CDMA-Techniken, kann im Hintergrund zu existierenden Systemen eingesetzt werden solange der Signalpegel niedrig genug ist. Die Bandspreizung kann durch die Exklusiv-Oder-Verknüpfung eines Bits mit einer Chipping-Sequenz oder durch Frequenzwechsel erreicht werden. Die Schutzabstände werden dann durch die Orthogonalität der Chipping-Sequenzen oder Sprungfolgen erzeugt. Je „besser“ diese Orthogonalität ist (dies ist natürlich keine mathematisch saubere Formulierung, jedoch recht intuitiv), desto niedriger ist die Korrelation der gespreizten Signale oder desto niedriger ist die Kollisionswahrscheinlichkeit der FHSS-Systeme. DSSS-Systeme verwenden typischerweise Rake-Empfänger, welche die Signale, die auf unterschiedlichen Pfaden entlang laufen, wieder kombinieren. Diese Kombination der Signale resultiert in einem stärkeren Signal, als es das stärkste Einzelsignal auf einem Pfad ist.

2.14 Der Hauptgrund ist die Unterstützung einer größeren Teilnehmerzahl. Zellen-basierte Mobilfunksysteme können das gleiche Spektrum immer wieder nach bestimmten Wiederholungsmustern verwenden. Kann man dabei mehr Zellen pro Quadratkilometer verwenden, so steigt auch die Zahl der möglichen Nutzer pro km^2. Zudem können Zellen die Ortung eines Teilnehmers und ortsabhängige Dienste unterstützen. Kleinere Zellen (also mehr Antennen) ermöglichen auch eine niedrigere Sendeleistung (daher weniger Strahlung!), eine längere Betriebsdauer für mobile Systeme und eine geringere Verzögerung zwischen Sender und Empfänger. Der große Nachteil sind natürlich die enormen Geldmittel, die für die Einrichtung einer solchen Infrastruktur mit vielen Zellen aufgebracht werden müssen. Typischerweise bekommt jede Zelle eine gewisse Zahl an Frequenzbändern zugewiesen. Benachbarte Zellen dürfen dabei al-

lerdings nicht die gleichen Frequenzen verwenden. Nach bestimmten Mustern (z.B. 7er-Gruppen) können Frequenzen wieder verwendet werden. Sobald das System dynamisch Frequenzen lastabhängig Zellen zuweisen kann, ist eine Reaktion auf eine plötzliche Erhöhung der Last durch eine „Leihen“ einer gewissen Kapazität von Nachbarzellen möglich. Jedoch müssen dann die „geborgten“ Frequenzen in den Nachbarzellen blockiert werden.

2.15 TDM/FDM-Systeme haben eine feste obere Grenze für die Zahl gleichzeitiger Nutzer. Das System weist einen bestimmten Zeitschlitz auf einer bestimmten Frequenz einem Nutzer zu. Sobald alle Zeitschlitze auf allen Frequenzen belegt sind, können keine weiteren Nutzer mehr akzeptiert werden. Im Vergleich zu dieser harten Kapazitätsgrenze haben CDM-Systeme eine so genannte „weiche“ Kapazitätsgrenze (in etwa vergleichbar mit dem Füllen einer Kiste mit Ziegelsteinen oder eben mit Papiertaschentüchern). Für CDM-Systeme beschränkt normalerweise der Signal-Rausch-Abstand die Anzahl der gleichzeitig aktiven Nutzer. Zwar kann das System im Prinzip immer noch einen weiteren Nutzer mit aufnehmen, jedoch könnte dann der Rauschpegel irgendwann über einen Schwellwert steigen, ab dem eine Übertragung nicht mehr möglich ist. In TDM/FDM-Systemen beeinflusst ein Nutzer, nachdem er einmal vom System akzeptiert wurde, nicht die anderen Nutzer, da er in der Zeit und Frequenz getrennt ist (es gibt sicherlich gewisse Interferenzen, die aber hier vernachlässigt werden sollen). In CDM-Systemen verringert jeder zusätzliche Nutzer die Übertragungsqualität aller anderen Nutzer (der Platz in der Kiste mit Papiertaschentüchern wird also immer enger).

3. Medienzugriffsverfahren

3.1 Stationen in einem Festnetz „hören“ sich gegenseitig. D.h. die Länge einer Leitung ist derart begrenzt, dass die Dämpfung nie so stark wird, um das Signal auszulöschen. Sobald also irgendeine Station ein Signal auf die Leitung sendet, können alle Stationen, die mit der Leitung verbunden sind, dieses Signal empfangen. Das beste Bei-

spiel hierfür ist das klassische Ethernet, 10Base2, das eine Bustopologie aufweist und CSMA/CD als Zugriffsverfahren einsetzt. Heutige Festnetze weisen eine Sterntopologie im lokalen Bereich auf, Weitverkehrsnetze hingegen bestehen aus vielen Direktverbindungen, die insgesamt ein teilvermaschtes Netz ergeben. In drahtlosen Netzen ist es allerdings oft der Fall, dass Stationen mit einer Zentrale kommunizieren, jedoch sich nicht gegenseitig empfangen können. Dies führte bereits in den frühen Siebzigern zum Aloha-Zugriffsschema (Universität von Hawaii). Aber inwiefern könnte CS (Carrier Sense) in drahtlosen Netzen helfen? Das Problem liegt darin, dass Kollisionen immer nur Probleme beim Empfänger verursachen – das Abhören des Mediums findet jedoch beim Sender statt! In leitungsgebundenen Netzen spielt dies keine große Rolle, da die Signalstärke mehr oder weniger die gleiche entlang der Leitung ist (natürlich nur in gewissen Grenzen). In drahtlosen Netzen machen CS und CD beim Sender keinen großen Sinn. Sender können meist nicht die Signale anderer Sender während des Sendens hören, ebenso wenig Kollisionen bei Empfängern. Der Grund liegt darin, dass rein funktechnisch die Sendeleistung um Größenordnungen höher als die Empfangsleistung ist.

3.2 Im Fall von Aloha kümmern sich Stationen nicht um andere Stationen, sondern greifen einfach auf das Medium zu, sobald sie Daten zu senden haben. Es gibt keine ausgelieferten Stationen, da Stationen nie vorher das Medium abhören. Versteckte Stationen können natürlich Kollisionen verursachen. Das gleiche gilt für Slotted Aloha, wobei der einzige Unterschied darin besteht, dass der Medienzugriff auf Zeitschlitzen beruht. Reservierungsverfahren arbeiten typischerweise mit einer zentralen Reservierungsstation, die von allen anderen Stationen empfangen werden kann. Ohne diese Bedingung oder vergleichbare Mechanismen, die Reservierungsnachrichten verteilen können, würden diese Verfahren nicht funktionieren. Bei diesen Verfahren gibt es weder versteckte noch ausgelieferte Endgeräte. MACA wurde entworfen, um versteckte oder ausgelieferte Endgeräte in einem verteilten WLAN ohne eine zentrale Reservierungsstation zu beherrschen. MACA kann jedoch versagen, sobald die

Kommunikationsbedingungen asymmetrisch oder die Topologien sehr dynamisch sind (Stationen können sich sehr schnell in einen Kollisionsbereich hineinbewegen).

3.3 So lange eine Station ein Signal empfangen kann und dieses Signal zum richtigen Zeitpunkt ankommt, damit es in den richtigen Zeitschlitz fällt, spielt es in TDMA-Systemen keine Rolle, ob Endgeräte nah oder fern sind. In TDMA-Systemen messen Endgeräte die Signalstärke und den Abstand zwischen Sender und Empfänger. Dann passen die Endgeräte die Sendeleistung an und senden Signale im Voraus in Abhängigkeit von der Entfernung zum Empfänger. Endgeräte in CDMA-Systemen müssen ihre Sendeleistung sehr oft anpassen (z.B. 1500 Mal pro Sekunde in UMTS), so dass alle Signale, die beispielsweise von einer Basisstation empfangen werden, mehr oder weniger die gleiche Stärke besitzen. Ohne diese recht präzise Leistungssteuerung könnte ein Signal leicht andere übertönen, da die Signale nicht in der Zeit getrennt sind.

3.4 Typischerweise wird SDMA durch den Netzbetreiber durchgeführt bzw. unterstützt. Ein Netzbetreiber plant das Netz, d.h. platziert die Basisstationen anhand der Topologie, speziellen Geländesituationen, Kapazitätsplanung etc. Sobald das System am Laufen ist, unterstützen die Basisstationen die Infrastruktur in der Entscheidung, welche Basisstation einem Endgerät zugewiesen wird. Dies beruht recht oft auf der aktuellen Signalstärke oder der aktuellen Zellenauslastung. Das mobile Endgerät unterstützt die Infrastruktur, indem es Informationen über die Stärke des empfangenen Signals übermittelt. Ein Endgerät kann zudem den Wechsel des Zugangspunktes initiieren.

3.5 Modulation – Sender müssen alle Basisbandsignale auf eine bestimmte Trägerfrequenz bringen. Dies ist typischerweise ein analoger Vorgang und benötigt auch analoge Komponenten. Klassische Empfänger benötigen auch Filter, um Signale auf bestimmten Frequenzen empfangen zu können. In Abhängigkeit von der Trägerfrequenz sind unterschiedliche Antennen erforderlich. Reine TDMA-Systeme verbleiben auf einer Frequenz und daher können auch alle Empfänger auf der gleichen Fre-

quenz auf Daten warten. In FDMA-Systemen müssen Empfänger nach unterschiedlichen Trägerfrequenzen suchen, bevor sie Nutzdatensignale empfangen können. Die Steuerung des Medienzugriffs kann auf verschiedenen Schichten geschehen. Die WRCs (World Radio Conferences) werden für eine weltweite Frequenzzuweisung genützt, wie z.B. im Fall des 2 GHz-Bereichs für IMT-2000. Die ITU überwacht die weltweite Frequenznutzung. Nationale Organisationen regulieren Frequenzen in unterschiedlichen Ländern. Auf den nächst tieferen Schichten regeln die Netzbetreiber den Medienzugriff: Die Frequenznutzung wird durch die Netzplanung und die aktuelle Last geregelt. Schließlich weisen Basisstationen in Mobilfunknetzen Frequenzen den Endgeräten je nach aktueller Verfügbarkeit zu. In WLANs legen Systemverwalter die genutzten Frequenzen fest und formen so Funkzellen (typ. 3 Kanäle bei 802.11b).

3.6 Drahtlose Netze können unterschiedliche Frequenzen, verschiedene Zeitschlitze oder auch unterschiedliche Codes verwenden, um Duplex-Kanäle zu realisieren. Typische leitungsgebundene Netze nutzen oft einfach verschiedene Drähte (ausgefeiltere Verfahren nutzen zudem z.B. Echo-Cancellation).

3.7 Solange Kommunikationssysteme ein festes TDM-Schema verwenden, können Endgeräte sehr einfach gehalten werden. Die einzige Anforderung ist die, dass alles synchronisiert bleibt, um so Daten empfangen zu können. Dieses Verfahren ist ein Klassiker in Telekommunikationssystemen (z.B. ISDN, PCM-30, SDH usw.). Ethernet-Systeme, das Internet, drahtlose LANs usw. arbeiten hingegen anforderungsgesteuert. In diesem Fall hat man nur einen geringen Mehraufwand, will man mit einer Datenübertragung beginnen: Rechner müssen nicht zunächst eine Verbindung aufbauen, indem sie zuvor bereits Zeitschlitze hierfür reservieren. Es ist zu bedenken, dass Nutzer immer mehr Daten im Vergleich zu Sprache übertragen. Viel der heutigen Netze sind klar von Daten dominiert (solange die reine Menge der Daten betrachtet wird und nicht der dadurch erzeugte Gewinn). Aus diesem Grund muss auch die Datenübertragung optimiert werden. Während WLANs für eine Datenübertragung von Anfang an optimiert wurden (und isochrone Audio-Datenströme entsprechend Prob-

leme verursachen), starteten Weitverkehrs-Mobilfunknetze als reine Sprachkommunikationssysteme. Das Vermittlungsverfahren ist normalerweise leitungsvermittelt, nicht paketvermittelt. So wie mehr und mehr Daten übertragen werden müssen, so müssen auch mehr und mehr datenorientierte Techniken integriert werden: GPRS in GSM, IP im Kernnetz von UMTS usw.

3.8 Interferenzen und Gegenmaßnahmen in:

- SDMA: Interferenzen passieren, sobald die Sender zu nahe zusammen sind. Endgeräte oder Basisstationen müssen einen minimalen Schutzabstand einhalten.
- TDMA: Interferenzen passieren, sobald Sender gleichzeitig ihre Daten senden. Gegenmaßnahmen sind eine präzise Synchronisation und Schutzabstände (Zeit zwischen Übertragungen).
- FDMA: Interferenzen passieren, sobald Sender Daten auf der gleichen Frequenz übertragen. Aus diesem Grund müssen unterschiedliche Frequenzen den Sendern durch Organisationen, Algorithmen in Basisstationen, koordinierte Sprungfolgen etc. zugewiesen werden. Zudem müssen Schutzbänder zwischen belegten Frequenzen eingerichtet werden, um Interferenzen zu vermeiden.
- CDMA: Interferenzen passieren, wenn Sender Daten mit Codes übertragen, die eine gewisse Korrelation aufweisen. Aus diesem Grund sollten Sender orthogonale oder quasi-orthogonale Codes verwenden.

3.9 Auch im Vakuum weisen Funkwellen eine maximale Geschwindigkeit auf: die Lichtgeschwindigkeit. Sobald sich irgendwelche Materie im Weg der Wellen befindet, so verlangsamen sich die Wellen. Aus diesem Grund kann es passieren, dass ein Sender das Medium als unbelegt erkennt, mit der Übertragung beginnt und genau in dem Moment, bevor die Wellen einen anderen Sender erreichen, lauscht der Sender in das Medium hinein, erkennt es als unbelegt und beginnt mit der Übertragung. Aus diesem Grund gibt es auch CD (listen while talk) und Mindestsendedauern in klassischen CSMA/CD-Ethernets.

3.10 Nachdem die Reservierung des Mediums erfolgreich war, können keine weiteren Kollisionen auftreten (solange das System fehlerfrei arbeitet). Reservierungsverfahren können auch eine gewisse Bandbreite, eine maximale Verzögerung oder eine maximale Verzögerungsschwankung garantieren. Es kann also im Prinzip während einer Übertragung nichts Störendes mehr auftreten. Im Vergleich zu klassischen Aloha-Verfahren ist die Kollisionswahrscheinlichkeit geringer, da die Wettbewerbsperiode im Vergleich zur wettbewerbsfreien Periode, in der die eigentliche Datenübertragung stattfindet, sehr kurz ist. Ein Nachteil von Reservierungsverfahren ist die höhere Verzögerung vor einer Datenübertragung. Bevor nämlich ein Gerät Daten übertragen kann, muss zunächst das Medium reserviert werden. Dies verschwendet eindeutig Zeit, insbesondere bei einem nur sehr gering ausgelasteten Medium.

3.11 Stellen Sie sich asymmetrische Übertragungsbedingungen und beispielsweise ein verstecktes Endgerät vor. Was passiert, wenn Station C in Abbildung 3.10 mit einer sehr hohen Leistung sendet, während sie nichts von B empfangen kann? Dann versagt auch MACA, da CTS nicht empfangen wird, C jedoch eine Kollision bei B verursacht.

3.12 Feste TDMA-Verfahren können harte Garantien abgeben. Dies ist auch der Grund, warum sie in klassischen Telefonsystemen, wie ISDN, SDH, GSM/CSD, ... eingesetzt werden. Ebenso können implizite Reservierungen Garantien abgeben, nachdem die Reservierung erfolgreich war. Weiterhin können alle zentralisierten Systeme, also solche mit einer Basisstation oder einem Zugangspunkt, Garantien abgeben. Alle nicht-deterministischen Verfahren, wie beispielsweise CSMA/CA, MACA, können keine harten Garantien abgeben.

3.13 Der Schutzabstand zwischen Nutzern in einem CDMA-System ist z.B. durch die (Pseudo-) Orthogonalität der Spreiz- oder Verwürfelungscodes gegeben. Je niedriger die Korrelation ist, desto besser werden die Teilnehmer voneinander getrennt.

3.14 Das übertragene Signal in diesem sehr vereinfachten Beispiel ist (-2,0,0,-2,+2,0) + (1,-1,0,1,0,-1) = (-1,-1,0,-1,+2,-1). Der Empfänger berechnet für A: (-1,-1,0,-1,+2,-1) *

(-1,+1,-1,-1,+1,+1) = 1-1+0+1+2-1 = 2. Für B ergibt sich: (-1,-1,0,-1,+2,-1) * (+1,+1,-1,+1,-1,+1) = -1-1+0-1-2-1 = -6. Der Empfänger kann sich nun „einfacher“ für die binäre 0 im Fall von B im Vergleich zur binären 1 im Fall von A entscheiden. Rauschen kann offensichtlich Signale stark beeinflussen. Aber immer noch kann ein Empfänger zwischen den beiden Signalen unterscheiden – das hier gezeigte einfache Beispiel geht von perfekt synchronisierten Signalen aus (die gespreizten Symbole sind exakt in Phase). Fügt man noch das Problem naher/ferner Endgeräte hinzu, so ändert sich in diesem einfachen Beispiel nicht viel: Der Empfänger kann immer noch das Signal erkennen, solange das Rauschen nicht zu stark im Vergleich zum Signal wird. Multiplizieren wir für das Beispiel einfach Bs Signal und das Rauschen mit 20. Das übertragene Signal ist dann: A_s+20*B_s+20*Rauschen = (-1,+1,-1,-1,+1,+1) + (-20,-20,+20,-20,+20,-20) + (+20,-20,0,+20,0,-20) = (-1,-39,19,-1,+21,-39). Der Empfänger erhält dann für A: (-1,-39,19,-1,+21,-39) * (-1,+1,-1,-1,+1,+1) = 1-39-19+1+21-39 = -74, und für B: (-1,-39,19,-1,+21,-39) * (+1,+1,-1,+1,-1,+1) = -1-39-19-1-21-39 = -120. Beide Ergebnisse sind negativ, der Empfänger kann nicht mehr die Originaldaten von A rekonstruieren, jedoch aber die von B. Dieses Beispiel soll nur ein gewisses Gefühl dafür vermitteln, was die Probleme sind. In diesem einfachen Beispiel sieht man bei weitem nicht alle Effekte, denn die Spreizcodes sind viel zu kurz und alles ist synchronisiert.

4. Telekommunikationssysteme

4.1 Wesentliche Merkmale: GSM (große Flächendeckung, Bandbreiten 9,6-50 kbit/s, Sprache, SMS, MMS), DECT (lokale Abdeckung, Sprache und Daten, sehr hohe Kapazität pro qm), TETRA (regionale Abdeckung, Ad-hoc-Modus, sehr schneller Verbindungsaufbau, Gruppenruf, Sprache und Daten, sehr robust), UMTS (mittlere Flächendeckung, höhere Datenraten bis zu 384 kbit/s, flexible Bandbreitenzuweisung). Gemeinsame Merkmale sind die traditionelle Sprachunterstützung (leitungsvermittelt), die Integration in klassische Telekommunikationsnetze, ISDN-Kernnetz. Die

Systeme haben jedoch auch ihre spezifischen Merkmale: GSM bietet eine Flächendeckung, TETRA den Ad-hoc-Modus und schnellen Verbindungsaufbau, DECT kann sehr hohe Nutzerdichten unterstützen. Falls modifiziert, kann GSM auch Teile von TETRA ersetzen (z.B. GSM-Rail), bietet jedoch keinen Ad-hoc-Modus. Aber auch UMTS hat seine spezifischen Vorteile: höhere Datenraten im Vergleich zum klassischen GSM (aber auch eine geringere Abdeckung), eine höhere Abdeckung als WLANs (aber auch niedrigere Datenraten).

4.2 Systeme, die für eine Sprachübertragung optimiert wurden, unterstützen bestimmte feste Datenraten und arbeiten leitungsvermittelt. Datenübertragungen geschehen jedoch häufig spontan mit ganz unterschiedlichen Datenraten. Daher ist dann bei diesen Systemen entweder zu viel Bandbreite reserviert, um die maximal erwarteten Datenraten zu unterstützen, oder die Datenübertragung erfährt recht lange Verzögerungen auf Grund des zunächst benötigten Verbindungsaufbaus. Ein möglicher Schritt hin in Richtung der Unterstützung einer Datenübertragung ist die Einführung von paketvermittelnden Diensten, wie sie vom Internet her bekannt sind. Ein Beispiel ist GPRS in GSM. An Stelle einer zeitbasierten Abrechnung können Netzbetreiber nun volumenorientiert abrechnen. Allerdings würde eine anwendungsorientierte Abrechnung weitaus mehr Sinn machen, da Nutzer nicht an Bits interessiert sind, auch nie das benötigte Datenvolumen abschätzen können, sondern lediglich sinnvolle Dienste nutzen wollen.

4.3 Die drei großen Kategorien sind Träger-, Tele- und Zusatzdienste. Die Trennung der Dienste unterstützt eine phasenweise Einführung neuer Dienste und trennt auch Tätigkeitsbereiche: Netzbetreiber, Dienstanbieter, Gerätehersteller usw. können sich jeweils auf bestimmte Dienste konzentrieren (z.B. Teledienste zwischen Endgeräten) und können sich auf bestimmte Schnittstellen verlassen (z.B. zu Trägerdiensten).

4.4 Der Hauptgrund ist die Vorwärtsfehlerkorrektur zur Verringerung der Übertragungsfehler. Zudem wird auch für die Signalisierung Bandbreite benötigt. Ebenso brauchen Schutzabstände eine gewisse Zeit, die dann der Datenübertragung fehlt.

4.5 Siehe Abbildung 4.4. Werden alle (oder fast alle) internen Schnittstellen spezifiziert, so können sich mehr Hersteller an einem System beteiligen. So lange ein Hersteller sich an die standardisierten Schnittstellen hält, können Geräte unterschiedlicher Hersteller miteinander kombiniert werden und Netzbetreiber sind nicht vollständig von einem einzigen Hersteller abhängig. Allerdings sieht die Realität oft anders aus und Netzbetreiber verlassen sich nur auf einen oder maximal zwei Hersteller, da ansonsten doch nicht immer alles so reibungslos funktioniert.

4.6 Eine MS enthält alle gerätespezifischen Funktionen: Gerätekennung, Codierer/Decodierer, Funkmodul usw. Das SIM enthält teilnehmerbezogene Funktionen (Authentifizierung), PIN und Nutzerkennung. Diese Trennung unterstützt beispielsweise den Wechsel eines Telefons, während persönliche Daten weiter verwendet werden können. Ein Teilnehmer steckt hierzu einfach sein SIM in ein neues Telefon und kann sofort z.B. sein privates Telefonbuch und seine PIN nutzen. Ausnahmen hiervon sind so genannte SIM-locked-Handys. In diesem Fall akzeptiert ein Mobiltelefon nur ein bestimmtes SIM. Allerdings ist dies eher eine Vermarktungs- denn eine technische Frage. Neben dem SIM kann natürlich auch das Telefon selbst viele nutzerrelevante Daten speichern. Weitere Teilnehmer-bezogene Daten werden in dem VLR gespeichert, das für den Aufenthaltsbereich zuständig ist, in dem sich der Teilnehmer derzeit aufhält. Schließlich speichert noch das HLR des Netzbetreibers Daten, mit dem der Teilnehmer einen Vertrag hat. Die Nutzerdaten sind auf verschiedene Weisen gesichert: Authentifizierungszentren sind besonders geschützte Bereiche des HLRs, die sich beim Netzbetreiber befinden. Im Kernnetz werden lediglich temporäre Kennzeichnungen verwendet. Daten werden über die Luftschnittstelle typischerweise nur verschlüsselt gesendet (schwach verschlüsselt, aber immerhin). Der Inhalt eines SIM ist über eine PIN geschützt (manche Karten zerstören sich automatisch, falls sie zu oft angegriffen werden). Die Ortsbestimmung kann durch das Endgerät unterstützt werden: Das Endgerät kann die aktuellen Signalstärken von allen umliegenden Basisstationen auswerten. Weiterhin kann die Ankunftszeit der Signale

herangezogen werden, um die Entfernung zu berechnen. Reflexion und Dämpfung machen die Berechungen aber deutlich schwerer.

4.7 GSM nutzt nur zwei Hierarchieebenen: Netzbetreiber speichern alle Teilnehmer-relevanten Daten im HLR und alle Informationen über Besucher innerhalb eines Aufenthaltsbereichs in einem VLR. Die Kapazität von HLRs geht bis zu einigen Millionen Teilnehmern, bei VLRs bis zu einer Million. D.h. innerhalb eines Aufenthaltsbereichs können bis zu einer Million Nutzer aktiv, also registriert sein. Sobald Teilnehmer zwischen Aufenthaltsbereichen wechseln, muss eine Aktualisierung im Kernnetz durchgeführt werden: Das HLR bekommt immer die Informationen über das aktuelle VLR. Diese Aktualisierungen werden unabhängig von der Teilnehmeraktivität durchgeführt (Datenübertragung, Anrufe usw.). In den allermeisten Fällen verbleiben Teilnehmer die meiste Zeit im gleichen Aufenthaltsbereich, die zweistufige Hierarchie funktioniert in diesem Fall gut. Wenn sich jedoch z.B. viele Touristen häufig hin- und herbewegen verursacht die Aktualisierung eine gewisse Last auf dem Netz, da das HLR im Heimatnetz der Touristen immer aktualisierte Ortsnachrichten benötigt – und dies rund um die Welt. Weitere Hierarchieebenen könnten die Skalierbarkeit des Systems verbessern, vergrößern jedoch auch die Komplexität.

4.8 HSCSD arbeitet immer noch leitungsvermittelt wie auch CSD. Es kombiniert „einfach“ mehrere Verbindungen. GPRS führt eine neue Technik in GSM ein, die Paketvermittlung. Im Prinzip braucht das Kernnetz Router, die den Paketstrom weiterleiten können. Diese Router (SGSN, GGSN) arbeiten mit IP und verlassen sich auf das herkömmliche GSM-Netz für die Teilnehmerlokalisierung. Eine weitere neue Komponente findet sich im HLR, ein Datenbank für alle vom Teilnehmer nutzbaren GPRS-Dienste. Zudem muss das System einen Kontext für jeden aktiven Nutzer einrichten, die übertragenen Daten zählen, IP-Adressen zuweisen etc.

4.9 Traditionelles GSM hat Zellendurchmesser von bis zu 70 km. Ein Nutzer kann also bis zu 35 km Abstand zur Basisstation haben. Diese Grenze rührt nicht notwendigerweise von der Signaldämpfung her, sondern beruht auf der maximal erlaubten Sig-

nalverzögerung. Alle Signale müssen relativ exakt synchronisiert an einer Basisstation ankommen. Mit Hilfe der Variable „Timing Advance“ kann der Sendezeitpunkt angepasst werden (je weiter ein Endgerät von der Basisstation weg ist, desto früher müssen die Signale abgesendet werden). Mit gewissen Tricks kann die Reichweite verdoppelt werden. Die Kapazität wird durch die Zahl der Kanäle * Anzahl der Zeitschlitze – Signalisierungsmehraufwand bestimmt. Die Zahl der Kanäle hängt von der Regulierung und dem Netzbetreiber ab. Die Kapazität ist unabhängig von der Nutzung von GSM/CSD, HSCSD oder GPRS. Alle drei Systeme nutzen die gleiche Rahmenstruktur und Modulation. Erst neue Modulationsverfahren können auch eine höhere Kapazität bieten. EDGE ist ein Bespiel hierfür. Weiterhin bieten Systeme wie GPRS unterschiedliche Ebenen des Fehlerschutzes, die unter guten Ausbreitungsbedingungen auch höhere Nutzdatenraten bieten können. Die Gesamtkapazität des Systems wird dadurch aber nicht erhöht.

4.10 GSM nutzt SDM, FDM und TDM:

- SDM: Netzbetreiber planen die Funkzellen, platzieren Basisstationen und nutzen Frequenzen immer wieder nach bestimmten Wiederholungsmustern.
- FDM: Regulierungsorganisationen oder -behörden weisen Kanäle Netzbetreibern zu, Netzbetreiber weisen aus diesen Kanälen wiederum eine gewisse Zahl den jeweiligen Basisstationen zu. Schließlich weist eine Basisstation einem Endgerät einen Kanal für eine Datenübertragung zu.
- TDM: Basisstationen weisen einen oder mehrere Zeitschlitz(e) einem Endgerät für die Datenübertragung zu.

4.11 Ein BSS muss die Rahmenstruktur erzeugen. Endgeräte hören in das Medium hinein, empfangen Signale über Rundrufkanäle und synchronisieren sich mit der Rahmenstruktur. Während einer Übertragung wird innerhalb eines Zeitschlitzes ein Trainingsfeld mitgesendet, welches die Synchronisation weiter verbessert. Das Endgerät ist immer selbst für die exakte Synchronisation innerhalb einer Zelle verantwortlich. Dies

ist deshalb so wichtig, weil ansonsten leicht im Rahmen benachbarte Daten zerstört werden könnten.

4.12 Beispiele für Verzögerungen bei der Paketübertragung:

- CS: Verbindungsaufbau (einige Sekunden), FEC-Codierung/Decodierung und Verschachtelung (etwa 100 ms), Signallaufzeit (einige Millisekunden/Festnetz eingerechnet).
- PS: Kanalzugriff (abhängig von der aktuellen Last), FEC-Codierung/Decodierung und Verschachtelung (etwa 100 ms), Signallaufzeit und Routing (einige Millisekunden). Experimente zeigen, dass Pakete in GPRS-Netzen eine recht große Verzögerung auf Grund von Verzögerungen beim Kanalzugriff erfahren können: 200-500 ms für 128 byte Pakete, mehrere Sekunden für 1-4 kbyte Pakete.

4.13 Neben eventuellen Problemen aufgrund von Störungen können Kollisionen in GSM-Systemen nur während eines Verbindungsaufbaus vorkommen. Endgeräte müssen auf eine Basisstation mit Hilfe eines Slotted-Aloha-Verfahrens zugreifen, um eine Schicht-2-Verbindung für die Signalisierung aufzubauen. Während dieser Verbindungsaufbauversuche können die Wünsche mehrerer Endgeräte kollidieren, so dass Versuche wiederholt werden müssen. Während einer Datenübertragung oder eines Gesprächs kann dann keine Kollision mehr stattfinden. Datenübertragungen werden im traditionellen GSM (CSD) praktisch wie Gespräche behandelt. HSCSD hat das zusätzliche Problem, dass es mehrere Kanäle gleichzeitig braucht. Diese stehen oft nicht zur Verfügung. Dies verursacht jedoch keine Kollision sondern schlichtweg eine Verweigerung des angeforderten Dienstes für mehrere Kanäle. Die Kanalzuweisung und –rückgabe wird in GSM-Systemen dynamisch geregelt. Für GPRS verursachen Datenübertragungen ebenfalls keine Kollisionen, da ein Endgerät immer warten muss, bis es zuvor angeforderte Zeitschlitze auch zugewiesen bekommt. Nachdem Zeitschlitze zugewiesen wurden, können diese ohne weitere Kollisionsgefahr genutzt werden. In Abhängigkeit von der aktuellen Last kann es aber sein, dass nicht allzu viele Zeitschlitze zur Verfügung stehen. Netzbetreiber garantieren oft jedoch mindes-

tens ein Zeitschlitz pro Zelle für GPRS-Verkehr, damit dieser nicht vollständig zum Erliegen kommt.

4.14 GSM spezifiziert viele verschiedene Kanäle zur Übertragung von Steuerdaten. Solange kein Verkehrskanal (TCH) existiert, verwendet ein MS einen SDCCH für die Signalisierung, beispielsweise für die Authentifizierung und Registrierung, welche vor der Einrichtung eines TCHs durchgeführt werden muss. TCH und SDCCH nutzen einen SACCH zur Signalisierung der Kanalqualität bzw. Signalstärke. Sobald ein TCH vorhanden ist und mehr Signalisierungsdaten übertragen werden müssen (z.B. während einer Verbindungsübergabe), nutzt ein MS einen FACCH, der in den Zeitschlitzen übertragen wird, die ansonsten vom TCH belegt werden.

4.15 Das GSM-System speichert lediglich den aktuellen Aufenthaltsbereich für einen Nutzer im VLR. Jedes Mal, wenn ein Nutzer den Aufenthaltsbereich wechselt, wird dies im VLR vermerkt. Zudem sind auch periodische Aktualisierungen möglich. Roaming umfasst auch den Wechsel des Netzbetreibers. Dies kann innerhalb eines Landes geschehen (national roaming) oder sobald man sich in ein anderes Land begibt (international roaming). Der zweite Falls ist natürlich der Standardfall, da das nationale Roaming typischerweise zwei direkte Wettbewerber mit einschließen müsste. Voraussetzungen für Roaming sind immer gewisse Roaming-Verträge zwischen den Netzbetreibern. Ein HLR speichert immer das aktuelle VLR für einen Nutzer, unabhängig davon, ob sich dieser im eigenen oder in einem fremden Netz befindet. Die genaue Ortsbestimmung eines Teilnehmers wird während des Verbindungsaufbaus durchgeführt (Ausrufen innerhalb eines Aufenthaltsbereichs).

4.16 Teilnehmer in einem GSM-Netz arbeiten natürlich mit Telefonnummern. Das ist auch alles, was ein Nutzer von der Adressierung mitbekommen sollte. Diese Telefonnummern sind vollkommen vom aktuellen Aufenthaltsort eines Teilnehmers unabhängig. Das System selbst benötigt einige weitere Informationen, darf jedoch nicht die Identität eines Teilnehmers preisgeben. Die internationale Identifikation eines Nutzers geschieht anhand der IMSI (= Ländercode + Netzcode + Teilnehmerkennung). Während

des Betriebs innerhalb eines Aufenthaltsbereichs ist lediglich eine temporäre Kennung, die TMSI, notwendig. Dies versteckt die wahre Identität eines Nutzers. Die TMSI wird nicht an das HLR weiter geleitet. Das sind zwar schon ein paar Beispiele für Kennungen in GSM, es gibt jedoch noch einige weitere:

- *IMEI:* MS-Kennung (vergleichbar mit einer Art weltweit eindeutigen Seriennummer); besteht aus einer zentral vergebenen Typzulassung (type approval code) und den vom Hersteller zugewiesenen Kennungen Herstellungscode (final assembly code), Seriennummer (serial number) und Reserve.
- *IMSI:* Teilnehmerkennung, im SIM abgelegt. Bestandteile sind die Länderkennung (mobile country code, 3 Zifern, z.B. 262 für Deutschland), die Netzbetreiberkennung (mobile network code, 2 Ziffern, z.B. 01 für T-Mobile) und die eigentliche Kennung des Kundens (mobile subscriber identification number, 10 Ziffern). Die Netzbetreiberkennung zusammen mit der Kundenkennung ergibt eine landesweit eindeutige Teilnehmerkennung, die so genannte national mobile subscriber identity.
- *MSISDN:* Mobile subscriber ISDN Number, dies ist die Telefonnummer, die einem Teilnehmer zugewiesen wird, nicht einem Telefon. Die MSISDN ist öffentlich bekannt, nicht jedoch die IMSI oder die Abbildung MSISDN-IMSI. Eine MSISDN besteht aus einer Länderkennung (country code, bis zu 3 Ziffern, z.B. 49 für Deutschland), der nationalen Vorwahl (national destination code, typischerweise 2 oder 3 Ziffern) und der Teilnehmernummer (bis zu 10 Ziffern).
- *MSRN:* MSRN (mobile station roaming number) ist eine temporär zugewiesene, ortsabhängige ISDN-Nummer. VLRs weisen MSRNs zu und leiten sie an das HLR oder GMSC weiter, damit Anrufe weitergeleitet werden können. Die Zuweisung geschieht entweder beim Eintritt in einen neuen Aufenthaltsbereich (LA, location area) oder auf Anforderung durch das HLR (Verbindungsaufbau).
- *LAI:* Die Kennung des Aufenthaltsbereichs (location area identity) kennzeichnet Aufenthaltsbereiche eines Netzbetreibers. Sie besteht aus einer Länderkennung

(country code, 3 Ziffern), eine Netzbetreiberkennung (mobile network code, 2 Ziffern) und einem Code für den Aufenthaltsbereich (location area code, 16 bit). Die LAI wird über den BCCH einer Zelle zur Identifikation des LAs ausgesendet.

- *TMSI:* Das VLR, das aktuell für eine MS zuständig ist, kann eine temporäre 32 Bit-Kennung (temporary mobile subscriber identity) der MS mit einem SIM zuweisen. Das Paar (TMSI, LAI) identifiziert dann eindeutig einen Teilnehmer. Für laufende Verbindungen kann also die IMSI durch (TMSI, LAI) ersetzt werden.
- *LMSI:* Eine zusätzliche lokale Kennung (local mobile subscriber identity, 32 bit) kann von VLR/HLR für ein schnelleres Finden von Teilnehmern in den Datenbanken eingesetzt werden.
- *CI:* Innerhalb eines LAs hat wiederum jede Zelle eine eindeutige Kennung (cell identifier, 16 bit). Aus diesem Grund identifiziert auch das Paar (LAI, CI) eine Funkzelle weltweit eindeutig (global cell identity).
- *BSIC:* Basisstationen können durch den base transceiver station identity code identifiziert werden (6 bit) und bestehen aus einem 3 bit Netzfarbcode (network colour code) und einem 3 bit Senderfarbcode (base transceiver station colour code).
- Alle MSCs, VLRs und HLRs haben eindeutige ISDN-Nummern zur Identifikation.

4.17 Der typische Grund für eine Verbindungsübergabe ist ein schwächer werdendes Signal von der aktuellen Basisstation im Vergleich zu Signalen anderer Nachbarbasisstationen. Ein weiterer Grund könnte die aktuelle Lastverteilung sein: Ein Netz könnte einen Teil der Nutzer von einer Zelle in eine andere verschieben, um so zur Entlastung einer Zelle beizutragen. Für die typischen Schritte während der Übergabe wird auf die Abbildungen 4.11-4.13 verwiesen. Damit HSCSD-Verbindungen erfolgreich übergeben werden können, müssen zumindest die gleichen Ressourcen in der neuen Zellen vorhanden sein, wie sie in der alten genutzt wurden. Es müssen also genügend Zeitschlitze frei sein, um die gleiche Anzahl simultaner Verbindungen zu unterstützen. Ansonsten wird sich die verfügbare Datenrate verringern. Natürlich ist die

Wahrscheinlichkeit, dass mehrere Kanäle in einer neuen Zelle frei sind, wesentlich kleiner als sie dies für einen einzigen Kanal ist. Im Falle von GPRS schwanken die Datenraten sowieso in Abhängigkeit von der aktuellen Zellauslastung. Das gleiche gilt während und nach einer Übergabe. Ohne eine Vorabreservierung können weder HSCSD noch GPRS irgendwelche Dienstgütegarantien abgeben. Es gibt ja nicht einmal eine Garantie für eine Sprachverbindung – falls die nächste Zelle, in die hineingewechselt werden muss, bereits vollständig belegt ist, bricht die Verbindung ab.

4.18 Der erste Schritt ist die Authentifizierung des Nutzers gegenüber dem SIM durch die Eingabe einer einfachen PIN. Danach muss sich das SIM gegenüber dem GSM-System authentifizieren. Diese zweite Authentifizierung ist deutlich stärker im Vergleich zur PIN. Ein Grund hierfür ist, dass ein Netzbetreiber nicht so sehr daran interessiert ist, wer sein System benutzt, solange es ein gültiger und zahlender Kunde ist. Dazu muss nur die Authentizität des SIMs sichergestellt sein. Die Authentifizierung mit dem System nutzt ein Challenge-Response-Verfahren mit einem gemeinsamen Geheimnis im SIM und im AuC. Weder das SIM noch das AuC übertragen dieses Geheimnis über die Luftschnittstelle oder offenbaren es Kunden. Eine Verschlüsselung findet nur zwischen MS und BSS statt. GSM bietet keine starke Verschlüsselung Ende-zu-Ende oder MS-zu-Netzübergang an. Die Systementwickler entschieden damals, dass eine Verschlüsselung über die Luftschnittstelle ausreichend ist, da das Festnetz vertrauenswürdig ist. Aus diesem Grund gibt es auch keine Authentifizierung einer Basisstation gegenüber einer MS. Dies eröffnete Möglichkeiten, ein Netz bzw. Basisstationen vorzugaukeln. Erst UMTS führt eine volle Authentifizierung aller Komponenten ein.

4.19 Die klassische Datenrate von GSM ist 9,6 kbit/s. Sobald weniger Redundanz für FEC genutzt wird, sind auch 14,4 kbit/s möglich. Diese Datenraten werden unter Nutzung eines einzelnen Zeitschlitzes pro Rahmen auf einem bestimmten Kanal erzielt. HSCSD kombiniert mehrere Zeitschlitze, lässt aber ansonsten die Codierung unverändert. GPRS kann dynamisch mehrere Zeitschlitze pro Rahmen nutzen und setzt

auch vier andere Codierverfahren ein, die höhere Datenraten pro Zeitschlitz ermöglichen. EDGE führt schließlich ein anderes Modulationsverfahren (PSK) in Ergänzung zu GMSK ein, das unter guten Ausbreitungsbedingungen noch höhere Datenraten ermöglicht. Nur EDGE kann wirklich die Kapazität einer GSM-Zelle erhöhen. Unabhängig von Codier- und Modulationsverfahren bleiben die Komplexität der Signalisierung für einen Zellwechsel, die Verzögerung beim Wechsel und die hohen Verzögerungen durch die Vorwärtsfehlerkorrektur und Verschachtelung.

4.20 Existierende Geräte können (derzeit) nicht alle im Standard festgelegten Datenraten anbieten. Während im Standard im Prinzip vorgesehen ist, dass alle 8 Zeitschlitze pro Rahmen in beiden Richtungen genutzt werden können, vermögen reale Geräte meist nicht gleichzeitig zu senden und zu empfangen. Ältere Geräte benötigen sogar etwas Zeit, um zwischen Senden und Empfangen umzuschalten. Damit wird mindestens ein weiterer Zeitschlitz unbrauchbar. Weiterhin bieten verfügbare GPRS-Telefone nicht alle Codierschemata an (typischerweise nur CS-1 und CS-2).

4.21 Die Verzögerung ist zwischen der MS und dem Austrittspunkt aus dem GPRS-Netz festgelegt. Die beste mittlere Verzögerung beträgt 0,5 s. Wird eine Datenrate von 115,2 kbit/s (eine typische Datenrate von seriellen Schnittstellen, über die mit Mobiltelefonen kommuniziert wird) und eine Verzögerung von 2*0,5 s angenommen, so sind 115,2 kbit = 14,4 kbyte in der Übertragung. TCP wurde für die Übertragung einer größeren Menge an Daten entwickelt (Dateitransfers etc.). TCP ermöglicht die gerechte Aufteilung der verfügbaren Bandbreite, sobald es sich in einem eingeschwungenen Zustand befindet. Dies erfordert den Empfang von Bestätigungsmeldungen, die Anpassung von Sendefenstern und Schwellwerten. Beträgt die insgesamt zu übertragende Datenmenge jedoch nur 10 kbyte, so bekommt TCP entweder nie während der Datenübertragung eine Bestätigung zurück, um so seine Sendecharakteristik anzupassen (falls das initiale Sendefenster groß genug war), oder TCP verschwendet Bandbreite, da es ein zu kleines Sendefenster am Anfang verwendet (Standardfall). Echte Messungen mit GPRS deuten auf sehr hohe reale Verzögerun-

gen hin (die Beispiele sind Umlaufzeiten gemessen für unterschiedliche Paketgrößen mit einem Klasse-8-Mobiltelefon): 0,8 s/64 byte, 1,4 s/128 byte, 2,2 s/1024 byte, 2,9 s/2048 byte, und 4,8 s/4096 byte. Zudem zeigen die Messungen eine sehr hohe Verzögerungsschwankung. Unter diesen Umständen bricht die Leistung von TCP stark ein. Kapitel 9 präsentiert einige Verbesserungen von TCP (z.B. große initiale Sendefenster).

4.22 GPRS benötigt weiterhin den klassischen leitungsvermittelten Kern (CS) für die Lokalisierung, Authentifizierung usw. Allerdings werden die MSCs nicht mehr für den eigentlichen Datentransport benötigt. Dieser wird von den Routern im PS-Kern (SGSN und GGSN) durchgeführt (vgl. Abbildung 4.16).

4.23 DECT bietet 120 Vollduplexkanäle, jeder mit einer Standarddatenrate von 32 kbit/s (ungeschützt). DECT wendet TDM zur Strukturierung der Rahmen und zur Verschachtelung der Teilnehmer ein (24 Zeitschlitze pro Rahmen, 12 in Aufwärts-/12 in Abwärtsrichtung). Weiterhin wird FDM eingesetzt, um die Kapazität zu erhöhen (mehrere DECT-Zellen am gleichen Ort, 10 Kanäle). Anwender können natürlich auch SDM einsetzen, indem sie die Basisstationen weit genug auseinander stellen. Diese Multiplex-Verfahren zusammen ergeben eine sehr hohe Kapazität des Systems, die beispielsweise in Bürogebäuden auch benötigt wird. Im Vergleich zu GSM ist das System einfacher. Obwohl auch für DECT Datenbanken definiert wurden, besteht ein normales DECT-System einfach aus einer Basisstation und mehreren mobilen Endgeräten. Die meisten Szenarien benötigen keine komplizierten Verbindungsübergaben (obwohl diese bei DECT möglich sind). Weiterhin brauchen die meisten Systeme keine komplexen Abrechnungssysteme, da sie einfach an das Festnetz bzw. an Nebenstellenanlagen angeschlossen sind.

4.24 Polizei, Feuerwehr, Rettungsdienste, Bergungsteams, öffentliche Verkehrssysteme, Taxis usw. sind typische Nutzer von Bündelfunksystemen. Diese Systeme sind deshalb so attraktiv, weil sie über ganz besondere Eigenschaften, wie schnellen Verbindungsaufbau (unter einer Sekunde), Gruppenruf, hohe Robustheit, billiger Betrieb,

zuverlässige und schnelle Nachrichtenübermittlung und Ad-hoc-Vernetzungsfähigkeiten verfügen. Oft basieren vorhandene Systeme für diese Zwecke noch auf analoger Technik, die auf gesonderten Frequenzen, aber ohne starke Verschlüsselung arbeiten. Dies macht insbesondere die gesicherte Zusammenarbeit von unterschiedlichen Organisationen, wie Feuerwehr, Polizei und Rettungsdiensten im Katastropheneinsatz schwierig – die Teams müssen oft Geräte austauschen, um miteinander kommunizieren zu können. Bündelfunksysteme können billiger als GSM-Netze errichtet werden, da sie mit weniger Basisstationen eine höhere Abdeckung erreichen (auch aufgrund der niedrigeren Belastung). Zudem werden meist komplexe Abrechnungsmechanismen nicht benötigt.

4.25 Wesentliche Merkmale: höhere und flexiblere Datenraten, bessere Sprachqualität auf Grund neuer Codecs, Nutzung von CDMA (in beinahe allen Systemen), Betrieb bei 2 GHz. Höhere Zellkapazitäten und höhere Datenraten vorrangig erzielt durch leistungsfähigere Modulationsverfahren, bessere Sprachcodierer mit höherer Kompression, CDMA als zusätzlichem Multiplex-Verfahren und leistungsfähigere Endgeräte (präzisere Leistungssteuerung, Nutzung von Mehrwegeausbreitung, ...). UMTS realisiert asymmetrische Datenraten und unterschiedliche Datenraten in der gleichen Richtung über unterschiedliche Spreizfaktoren. Da die Chipping-Rate von UMTS immer konstant ist, hängen die Datenraten direkt vom Spreizfaktor ab. Je mehr die Daten gespreizt werden, desto niedriger ist die Datenrate.

4.26 Derzeit ist die Situation noch nicht ganz übersichtlich, da unterschiedliche Länder auch in unterschiedlichen Phasen hinsichtlich des Ausbaus von 3G-Systemen sind. Allerdings glaubt derzeit niemand mehr an ein weltweit einheitliches System, nicht einmal die gleichen Frequenzbereiche sind überall verfügbar:

- Europa: Nach viel diskutierten Lizenzierungen über Auktionen oder Schönheitswettbewerbe installieren derzeit viele Netzbetreiber 3G-Systeme. Einige Betreiber haben inzwischen wieder aufgegeben, andere sind Bankrott gegangen. Alle Betreiber von 3G-Systemen haben sich für UMTS entschieden, zunächst soll nur

der UTRA/FDD-Modus zum Einsatz kommen (es ist derzeit unklar, wann und ob überhaupt UTRA/TDD zum Einsatz kommt). Obwohl die Lizenzbedingungen nicht den Einsatz von UMTS vorschreiben, gab es nur wenige Betreiber, die über andere Systeme am Anfang nachdachten. Der Start der Systeme war 2002 (Isle of Man), bereits 2005 sollten 50% der Bevölkerung in Deutschland Zugang zu UMTS haben.

- Japan: Hier sind zwei unterschiedliche 3G-Systeme verfügbar. NTT DoCoMo verwendet eine Variante von UMTS in ihrem W-CDMA-System, das als FOMA vermarktet wird. KDDI installiert ein cdma2000-System, das ab der Version 1x EV-DO ein 3G-System ist.
- China: Da derzeit die überwältigende Mehrheit in China GSM als Mobilfunksystem der zweiten Generation verwendet (und damit den weltweit größten nationalen GSM-Markt erzeugen) kann spekuliert werden, dass UMTS auch eines der großen 3G-Systeme in China werden wird. So kann das existierende Kernnetz nach Release 99 weiter verwendet werden. Die chinesische Entwicklung TD-SCDMA wurde in UMTS aufgenommen (UTRA/TDD, slow chipping option, Release 4). Allerdings ist es derzeit noch nicht klar, wann und ob überhaupt diese Variante zum Einsatz kommt. Weiterhin gibt es auch in China Betreiber, die auf cdma2000 setzen wollen.
- Nordamerika: Die Situation in den USA und in Kanada ist aktuell noch nicht klar zu bewerten. Bereits heute existieren mehrere Systeme parallel ohne einen klaren Gewinner, auch wenn GSM die größten Zuwachsraten aufweisen kann. Zudem nimmt die Lizenzierung des 3G-Spektrums nun schon eine lange Zeit in Anspruch, da nicht sicher ist, welche Bereiche genau verfügbar sind. Aus diesem Grund bietet sich eine Verbesserung existierender Systeme mit der EDGE-Technik an (TDMA und GSM), so dass mit EGPRS höhere Datenraten angeboten werden können im Vergleich zu heutigen Systemen. Betreiber von cdmaOne-Netzen werden klar auf cdma2000 setzen.

4.27 OVSF erlaubt nur bestimmte feste Datenraten (bestimmte Vielfache von 15 kbit/s). Falls ein Nutzer Daten mit einer Rate zwischen zwei Werten senden möchte, so müssen entweder Teile der Daten verworfen werden (die dann mit FEC unter Umständen wieder hergestellt werden können) oder Fülldaten müssen eingeschoben werden. Im FDD-Modus kann nur über die Veränderung des Spreizfaktors auf die Datenrate Einfluss genommen werden. TDD bietet zusätzlich die Möglichkeit an, mehr oder weniger Zeitschlitze in Aufwärts- bzw. Abwärtsrichtung zu nutzen.

4.28 Die Spreizcodes können in UTRA FDD immer die gleichen sein, um die Systemkomplexität zu verringern. Jedoch besitzt jedes UE einen individuellen Verwürfelungscode, der quasi-orthogonal zu anderen Verwürfelungscodes ist. In UTRA TDD ist ein Verwürfelungscode zellspezifisch.

4.29 Ein wesentliches Merkmal des Zusammenfügens bzw. Aufteilens eines Datenstromes ist, dass dies nie innerhalb des (traditionellen) Kernnetzes geschieht. Dies bedeutet, dass die MSCs nichts von diesen neuen Fähigkeiten dank CDMA bemerken (Empfang der Daten über mehr als nur eine Basisstation). In Abhängigkeit des Übergabeszenarios (zwischen zwei Antennen desselben Node B, zwischen zwei Node B, zwischen zwei RNC) müssen die Node Bs oder das SRNC Datenströme aufteilen bzw. zusammenführen. Die Schnittstelle I_{ur} wird benötigt, um Daten zwischen den RNCs für das Zusammenführen/Aufteilen zu transportieren, ohne dass das CN hierbei involviert ist. Für CDMA-Systeme sehen Signale, die von unterschiedlichen Basisstationen stammen, im Prinzip wie eine Mehrwegeausbreiteung aus. Aus diesem Grund können die Rake-Empfänger auch beides gleich behandeln. Die Übergabe kann dann so weich von statten gehen, wie der Wechsel des aktuell stärksten Signals in einer Situation mit Mehrwegeausbreitung. TDMA/FDMA-Systeme wie GSM können dies nicht machen, da der aktuell belegte Zeitschlitz und/oder die aktuelle Sendefrequenz eventuell in der nächsten Zelle nicht mehr zur Verfügung steht.

4.30 Die Endgeräte müssen 1500 Mal in der Sekunde die empfangene Signalstärke messen und die eigene Sendeleistung den Gegebenheiten anpassen, damit bei

UTRA/FDD alle Signale möglichst mit der gleichen Stärke an der Basisstation ankommen. In GSM-Systemen ist dies nicht so oft nötig, da es eigentlich nie vorkommen sollte, dass zwei Sender gleichzeitig auf der gleichen Frequenz innerhalb einer Zelle senden.

5. Satellitensysteme

5.1 Die traditionelle Anwendung von Satelliten in der Datenübertragung ist die eines „dicken Kabels im Himmel“ („big cable in the sky”). Satelliten verbinden also weit entfernte Orte weltweit. Heute dominiert diese traditionelle Nutzung von Satelliten nicht mehr. Tausende von Glasfasern durchkreuzen alle Ozeane und verbinden damit alle Kontinente mit weit mehr Kapazität als aktuell gebraucht wird. Satelliten werden jedoch weiterhin benötigt, um beispielsweise TV/Rundfunkprogramme auszustrahlen und Telekommunikationsdienste auch in den entlegensten Ecken der Welt anzubieten bzw. in Gegenden mit zerstörter Infrastruktur, in feindlichen Umgebungen etc.

5.2 Die Verzögerung Erde-GEO-Satellit-Erde beträgt etwa 250 ms. Dies ist sehr hoch im Vergleich zu Glasfasern. Dieser Umstand kann auch nicht verbessert werden, da (derzeit) die Lichtgeschwindigkeit die absolute Obergrenze für Fortpflanzungsgeschwindigkeiten von Signalen darstellt und der Abstand der GEOs beinahe dem Erdumfang entspricht.

5.3 Die Inklination bestimmt die Abdeckung eines Satelliten. Bei einer Inklination von 0° wird der Äquator abgedeckt. Bei einer Inklination von 90° kreisen Satelliten über beide Pole. Geostationäre Satelliten können nur über dem Äquator verwirklicht werden, dann jedoch ist der Empfang bei höheren Breitengraden relativ schlecht. Die Elevation beeinflusst direkt die Signalqualität. Bei einer Elevation von 0° ist ein Empfang beinahe unmöglich. Normalerweise lassen sich Satellitensignale ab einer Elevation von 10° sinnvoll nutzen. Eine optimale Signalqualität herrscht bei 90° Elevation. Hohe Elevationen werden auch in den Bergen oder in dicht bebauten Gegenden benötigt,

wo Berge oder Gebäude ansonsten die Signale von Satelliten mit geringer Elevation blockieren.

5.4 Eigenschaften, pro und kontra bestimmter Orbits (siehe Kapitel 5 für weitere Parameter):

- GEO: Die Satelliten erscheinen wie festgebunden am Himmel;

  Pro: feste Antennen möglich, große Flächendeckung, einfacher Systementwurf;

  Kontra: hohe Verzögerungen, große Sendeleistung nötig, geringe Systemkapazität (SDM schwierig), schwache Signale bei hohen Breitengraden, überfüllte Idealpositionen im All über dem Äquator.
- LEO: Tief fliegende Satelliten;

  Pro: niedrige Verzögerung, geringe Sendeleistung möglich, Routing zwischen den Satelliten;

  Kontra: hohe Komplexität, sehr hohe Systemkosten
- MEO: Irgendwo zwischen GEO und MEO
- HEO: Kein kreisförmiger Orbit;

  Pro: höhere Kapazität über bestimmten Stellen;

  Kontra: komplexes System

5.5 Dämpfung durch die Atmosphäre, Staub, Regen, Nebel, Schnee, ... Blockieren der Signale durch Objekte (Berge, Gebäude). Je geringer die Elevation ist, desto länger ist der Weg der Signale durch die Atmosphäre. Ohne eine Strahlformung wird eine sehr hohe Ausgangsleistung benötigt.

5.6 Klassische Satelliten waren einfache Verstärker, die das eingehende analoge Signal verstärken und es dann wieder auf einer anderen Frequenz verstärkt aussenden. Ein Fortschritt kam mit digitalen Signalen. Satelliten konnten als Repeater arbeiten. Dies umfasst die Regeneration der digitalen Daten und die Übertragung von Signalen, welche die empfangenen Daten ohne Rauschen darstellen (im Vergleich zu analogen Verstärker, die auch Rauschen mit verstärken). Viele der heutigen Satelliten sind Re-

peater. Der nächste Schritt ist dann der Übergang zu Switches/Router. Damit können Satelliten auch Weiterleitungsfunktionen in Abhängigkeit von der Empfängeradresse vornehmen. Ebenso können Daten im All von Satellit zu Satellit weitergeleitet werden.

5.7 Ohne zusätzliche Repeater auf der Erde können Satellitentelefone nur im Freien oder zumindest in der Nähe eines Fensters eingesetzt werden. Satellitensignale sind im Allgemeinen zu schwach, um damit Dächer zu durchdringen. Weiterhin benötigen Satellitentelefone auch im Freien oft eine Sichtverbindung. Aus diesem Grund können bereits Hochhäuser eine Satellitenkommunikation erschweren.

5.8 Damit ein GEO-Satellit synchron mit der Erdrotation bleibt, muss er in einer Höhe von 35786 km kreisen. Weiterhin muss die Inklination 0° betragen. Dies führt dazu, dass die Satelliten wie auf einer Schnur aufgereiht erscheinen. Zudem sollen sich die Satelliten ja über dicht besiedelten Gegenden aufhalten. Also sind die Gegenden über dem Äquator, von denen aus die Satelliten Europa, Amerika oder Asien abdecken, dicht bevölkert. Daher müssen auch alle Satelliten einen Rest ihres Treibstoffes dazu aufbewahren, um sich am Ende ihrer Lebensdauer (die im Wesentlichen durch den Treibstoffvorrat bestimmt ist) aus dem Orbit zu schießen. Auf jeden Fall dürfen sie ihre Position nicht blockieren.

6. Rundfunksysteme

6.1 DAB und DVB bieten beide weit höhere Datenraten als 2G/3G-Mobilfunknetze. Allerdings arbeiten sie nur unidirektional und müssen ihre Bandbreite auf alle Empfänger aufteilen (natürlich teilen sich auch alle Teilnehmer in einer 2G/3G-Zelle die Gesamtkapazität). Aus diesem Grund sind Rundfunksysteme ideal für die Verteilung von Massendaten zu vielen, im besten Fall allen Teilnehmern. Gute Beispiele sind Rundfunk- und Fernsehprogramme, aber ebenso Systemaktualisierungen, populäre Web-Inhalte, Nachrichten usw. Typischerweise ist es viel zu teuer, individuelle Inhalte über ein Rundfunkmedium zu senden. Ist jedoch Bandbreite verfügbar, so ist auch

dies möglich. DAB/DVB können komplementär zu 2G/3G-Systemen betrachtet werden. Dies gilt insbesondere, wenn viele Daten mit einer hohen Bandbreite auf ein mobiles Endgerät geladen werden sollen. Mobiltelefonsysteme müssen ihre Datenraten drastisch bei höheren Relativgeschwindigkeiten reduzieren, während Rundfunksysteme auch noch bei recht hohen Geschwindigkeiten mit der vollen Bandbreite arbeiten.

6.2 Beispiele sind Nachrichten, Suchmaschinen, Wetterberichte, große Portale usw., also Web-Seiten, die viele Nutzer betreffen oder interessieren. Aber auch innerhalb individueller Seiten könnten gemeinsame Komponenten (Werbung, Videos) das Rundfunksystem verwenden, wohingegen die individuellen Komponenten Mobilfunksysteme nutzen.

6.3 Sobald der Aufenthaltsort eines Nutzers dem System bekannt ist, können ortsabhängige Dienste, ganz individuelle, an den aktuellen Ort bzw. die aktuelle Situation angepasste Dienste anbieten (nächste Pizzeria, Geldautomat, billigster Buchladen in der Umgebung, Spielpartner innerhalb einer gewissen Entfernung usw.). In Abhängigkeit vom Ort können Datenkarusselle von Rundfunkbetreibern so programmiert werden, dass sie Daten für einzelne Nutzer oder ganze Nutzergruppen aussenden. Falls ein ortsabhängiger Dienst eine Gruppe Menschen vor einem Museum erkennt, könnte er beispielsweise einen Videodatenstrom starten, der Bilder der aktuellen Ausstellung zeigt.

7. Drahtlose lokale Netze

7.1 Ohne zusätzliche Mechanismen ist die Mobilität in drahtlosen LANs auf den Abdeckungsbereich eines einzelnen Zugangspunkts beschränkt. Damit Roaming unterstützt werden kann (in WLANs ist „Roaming“ der Begriff für „Handover“ in Mobilfunksystemen wie GSM), werden Protokolle zur Kommunikation zwischen den Zugangspunkten benötigt (IAPP, Inter Access Point Protocol). Die Zugangspunkte müssen sich gegenseitig darüber informieren, welche Endgeräte derzeit in ihrem Bereich aktiv

sind. Dieser Ansatz funktioniert nur in räumlich eng begrenzten Gebieten, ansonsten werden Datenbanken etc. ähnlich zu GSM benötigt. Die Zugangspunkte arbeiten typischerweise als transparente, selbstlernende Brücken, die Zusatzinformationen benötigen, um Stationen schneller wieder zu „vergessen“ im Vergleich zu den Alterungsmechanismen für Einträge in Brücken für Festnetze. Die Stationskennung basiert auf MAC-Adressen. Roaming benötigt typischerweise ein Schicht-2-Netz, das auf Switches basiert.

7.2 Unterschiede: Abdeckung (GSM 70 km Zellen, WLAN 100 m), Datenraten (GSM 50 kbit/s, WLAN 50 Mbit/s), Dienstgüte (WWAN Sprache/Datenrate, WLAN keine/gewisse mit HiperLAN2), Sendeleistung (leistungsfähige Basisstationen für WWANs, einige hundert mW für WLANs), Betrieb (WWAN lizenziert, WLAN lizenzfrei/Ausnahmegenehmigungen), Verwaltung (WWAN öffentliche Betreiber, WLAN private Nutzer), Frequenzen (WWAN viele verschiedene nationale Frequenzen, WLAN beinahe identische internationale ISM-Bänder). Gemeinsamkeiten: ähnliches Ausbreitungsverhalten, ähnliche Probleme.

7.3 WLANs führen eine Luftschnittstelle in lokale Netze ein, die sehr einfach abzuhören ist. Aus diesem Grund beinhalten viele WLAN-Standards auch mehr oder weniger starke Verschlüsselungsmechanismen. Der bekannteste davon, WEP, wurde schon bald nach seiner Einführung geknackt. Zudem kennt die bekannteste WLAN-Familie, 802.11, keine leistungsfähigen Authentifizierungsmechanismen. Neue Standards sollen mehr Sicherheit einführen (802.11i), trotzdem sollten Nutzer immer ein zusätzliches VPN oberhalb des WLANs nutzen, um damit Privatheit und Datenintegrität zu sichern. WLANs nach Bluetooth oder HiperLAN2 bieten fortschrittlichere Sicherheitsmechanismen im Vergleich zu 802.11.

7.4 Alle drei Standards bieten Ad-hoc-Funktionalität, wobei nur Bluetooth mit einem Schwerpunkt auf Ad-hoc-Netze entworfen wurde. 802.11 verlässt sich für viele Funktionen stark auf den Zugangspunkt (z.B. Leistungssteuerung, Frequenzwahl, Dienstgüte, Medienzugriff usw.). Bluetooth implementiert hingegen alle Funktionen in allen

Knoten, so dass auch alle ein Netz etablieren können. Der Schwerpunkt von HiperLAN2 ist ebenfalls der Infrastrukturmodus. Ganz grob kann gesagt werden, dass 802.11 alle Büroanwendungen abdeckt, Bluetooth seinen Schwerpunkt bei der Anbindung von Peripheriegeräten hat und schließlich HiperLAN2 auf eine Dienstgüteunterstützung setzt (auch wenn noch keine Produkte verfügbar sind).

7.5 Ein Grund für Infrarot sind immer noch die Kosten. Infrarot-Sender und -Empfänger sind sehr billig und sehr einfach zu integrieren. Ein weiterer Vorteil ist der einfache Schutz vor Mithörern. Ein Angreifer kann wesentlich einfacher eine Bluetooth-Kommunikation abhören, unvorsichtige Nutzer lassen sogar ihre Bluetooth-Geräte offen für einen freien Zugang (suchen Sie einfach einmal mit einem Bluetooth-Gerät an einem öffentlichen Platz nach anderen – viele können gefunden werden). Infrarot-Kommunikation ist weitaus sicherer, da die Geräte zur Kommunikation recht genau ausgerichtet sein müssen und eine Sichtverbindung brauchen (zumindest bei IrDA).

7.6 802.11 deckt eine ganze Familie von drahtlosen LAN-Standards ab. Verschiedene Bitübertragungsschichten wurden für unterschiedliche Übertragungstechniken, Bandbreiten, Frequenzen etc. definiert. Alle nutzen eine gemeinsame MAC-Schicht. Damit die unterschiedlichen Bitübertragungsschichten eine gemeinsame MAC-Schicht nutzen können, führt eine Zwischenschicht die Anpassung durch und bietet einheitliche Funktionen der MAC-Schicht an, wie z.B. Carrier Sensing. Die HiperLAN-Familie spezifiziert mehrere Bitübertragungsschichten. So wie es derzeit allerdings aussieht, hat höchstens noch HiperLAN2 eine Chance zu überleben. Dieser Standard spezifiziert nur eine Bitübertragungsschicht. Alle Bluetooth-Systeme nutzen die gleichen Schichten.

7.7 Alle Systeme sparen Energie durch periodisches Schlafen. Insbesondere Bluetooth-Geräte bieten mehrere Energiesparmodi, da sie typischerweise mit Batterien arbeiten. Die negativen Auswirkungen des Energiesparens sind die höheren Verzögerungen bei spontanen Datenübertragungen – die Geräte müssen ja zunächst wieder aufwachen (was dauert und relativ viel Energie benötigt). Je kürzer also die Zugriffs-

zeiten sein sollen, desto weniger Energie kann gespart werden. Weiterhin brauchen hohe Datenraten auch mehr Energie. Wenn das periodische Schlafen nicht beispielsweise mit einem periodischen Datentransfer synchronisiert wird, ergeben sich sehr große Verzögerungsschwankungen.

7.8 802.11 bietet keine Dienstgüte im Ad-hoc-Modus, da es immer einen Zugangspunkt zur Strukturierung des Medienzugriffs braucht. Im Gegensatz dazu kann HiperLAN2 eine zentrale Steuerung im Ad-hoc-Modus einrichten (hier direct mode genannt), welche die Dienstgüte überwachen und steuern kann. Bluetooth arbeitet immer im Ad-hoc-Modus – allerdings nur im Prinzip, da eigentlich eine Leitstation bis zu sieben Folgestationen steuert und sozusagen der Zugangspunkt ist. Daher kann Bluetooth Dienstgüte auch im Ad-hoc-Modus anbieten. Diese Dienstgüte wird in Bluetooth dadurch realisiert, dass die Leitstation periodisch die Folgestationen abfragt. Dies garantiert gewisse Datenraten und Verzögerungszeiten. HiperLAN2 kann harte Dienstgütegarantien abgeben, da es die Zugriffsverzögerung, Bandbreite usw. steuert. Nachdem eine Leitstation gewählt wurde, kann Bluetooth harte Garantien für SCO-Verbindungen geben. 802.11 kann Garantien abgeben, wenn keine Wettbewerbsphase zugelassen wird (reine Abfrage durch den Zugangspunkt). Sobald es eine Wettbewerbsphase gibt, kann das System nur schwer eine Zugriffsverzögerung garantieren.

7.9 802.11 verwendet den MACA-Mechanismus mit RTS/CTS, um das Problem versteckter Endgeräte zu lösen. Für HiperLAN2 existiert das Problem nicht, da der Zugangspunkt jeglichen Medienzugriff steuert. Sobald ein Gerät versteckt ist, kann es überhaupt nicht kommunizieren und stört daher auch nicht. In Bluetooth gibt es ebenfalls keine versteckten Endgeräte, da die Leitstation alle sichtbaren Folgestationen steuert und überwacht. Kann eine Folgestation nicht mit einer Leitstation kommunizieren, so kann es an keiner Kommunikation teilhaben. Sendet dieses Gerät trotzdem, so stört es nicht weiter, da es nun selbst eine Leitstation mit einer anderen Sprungfolge ist.

7.10 802.11 bietet einen Mechanismus zum Medienzugriff, der zumindest im Standardfall eine gewisse Fairness bietet (ohne Abfrage durch den Zugangspunkt). Verhalten sich alle Systeme korrekt, so verteilt das Verfahren die verfügbare Bandbreite gerecht auf alle Nutzer. In HiperLAN2 und Bluetooth wird der Medienzugriff durch einen Zugangspunkt bzw. eine Leitstation geregelt. Die Fairness hängt dann von diesen besonderen Knoten im Netz ab, die auch über die Wartezeit eines Paketes bestimmen, bevor es übertragen wird. In 802.11 beeinflusst diese Wartezeit direkt die Chancen für eine Übertragung nach der nächsten Wettbewerbsphase.

7.11 802.11 bietet eine unmittelbare Bestätigung. Bluetooth und HiperLAN2 implementieren verschiedene ARQ- und FEC-Verfahren.

7.12 Während der Abfrage gibt es keine Kollisionen auf der MAC-Schicht von HiperLAN2 und Bluetooth, da der Zugangspunkt bzw. die Leitstation das Medium im Griff haben. Um mit dem Zugangspunkt zu kommunizieren, können Knoten bei HiperLAN2 Daten während einer Phase des wahlfreien Zugriffs übertragen (Kanal für den wahlfreien Zugriff mit direkter Rückmeldung vom Zugangspunkt). Zu diesen Zeitpunkten können Kollisionen auf der MAC-Schicht stattfinden. Für 802.11 sind Kollisionen auf der MAC-Schicht nichts Ungewöhnliches. Der MAC-Algorithmus sieht hier ein Zurückziehen vom Medium vor, um die Kollisionen aufzulösen. Kollisionen auf der Bitübertragungsschicht können in Bluetooth nur dann passieren, wenn ein anderes Pikonetz zufälligerweise auf die gleiche Frequenz zur gleichen Zeit springt. In diesem Fall werden die Daten für diesen Zeitschlitz zerstört. In HiperLAN2 werden unterschiedliche Netze durch unterschiedliche Frequenzen getrennt. Aus diesem Grund sollten keine weiteren Kollisionen vorkommen, außer den weiter oben beschriebenen während der Phase des wahlfreien Zugriffs. In 802.11-Netzen sind MAC-Kollisionen auch immer Kollisionen auf der Bitübertragungsschicht. Wichtige Pakete haben bei 802.11 eine höhere Priorität, die durch kürzere Wartezeiten widergespiegelt wird (SIFS, PIFS).

7.13 802.11 hat den niedrigsten Mehraufwand, da jeder Knoten einfach auf das Medium zugreifen kann, falls es frei ist. Aus diesem Grund bietet 802.11 auch die kürzeste

Zugriffsverzögerung bei freiem oder nur leicht belastetem Netz. Das System bricht zusammen, sobald die Last im Netz groß ist, da dann nur noch Kollisionen vorkommen und kein Knoten mehr in der Lage ist, Nutzdaten zu senden. Aus diesem Grund hat 802.11 eher eine weiche Kapazitätsgrenze. HiperLAN2 und Bluetooth benötigen immer zunächst eine Art von Verbindungsaufbau. Dies erhöht die Zugriffsverzögerung, auch wenn die aktuelle Netzlast nur sehr gering ist. Sobald eine Verbindung vorhanden ist, sind auch die Verbindungsqualität und die Zugriffsverzögerung praktisch unabhängig von der Netzlast. Beide Systeme können bis an ihr Maximum belastet werden, ohne dass sie zusammenbrechen. Für Bluetooth gilt dies nur in einem Pikonetz, nicht jedoch in einem Streunetz. Die Skalierbarkeit ist allgemein niedrig (8 Knoten im Pikonetz). Bei HiperLAN 2 hängt die maximale Knotenzahl von den Dienstgüteanforderungen ab. In 802.11-Netzen hängt die maximale Knotenzahl von den Verkehrsmustern ab.

7.14 HiperLAN 2 und 802.11 brauchen ein IAPP, Bluetooth unterstützt kein Roaming. Knoten, die zwischen Pikonetzen wechseln, müssen sich immer im neuen Pikonetz synchronisieren. Es gibt keine Signalisierung zwischen Leitstationen unterschiedlicher Pikonetze hinsichtlich Knoten, welche die Netze wechseln. Normalerweise gibt es ein IAPP nur für Infrastruktur-basierte Netze (man könnte sich so etwas wie ein Leitstation-Leitstation-Protokoll in Bluetooth vorstellen...). Für Ad-hoc-Netze wäre dieser Mehraufwand nicht vertretbar. Roaming kann über selbstlernende Brücken realisiert werden, die ihre Filterregeln austauschen (welche MAC-Adressen sind bei welchen Brücken sichtbar). HiperLAN2 bietet zusätzlich eine Unterstützung für den Schlüsselaustausch während des Roamings oder einer Sektor/Funk/Netzübergabe usw.

7.15 Die Weiterleitung von Daten in Bluetooth zwischen Pikonetzen verlangt einen Knoten, der zwischen diesen Pikonetzen hin und her springt. Dies erfordert auch eine Authentifizierung in beiden Netzen, Knoten, die praktisch immer aktiv sind und synchronisierte Uhren, falls die Leitstation in ein anderes Pikonetz springt. Sobald die Leitstation aus einem Netz herausspringt, wird jeglicher Verkehr angehalten und die Folgestati-

onen müssen warten, bis die Leitsatin zurückkehrt. Alle Sprungfolgen müssen während dieser Zeit synchronisiert bleiben. Bis jetzt unterstützt kaum ein Gerät die Möglichkeit, ein Streunetz zu bilden, indem es hin und her springt.

7.16 Als die Entwicklung von WATM begann, war ATM in Festnetzen gerade „in“. ATM wurde als die große vereinheitlichende Technik angesehen, die verschiedene Verkehrsarten mit Dienstgüte unterstützt. Im Prinzip ist dies auch heute noch wahr, jedoch hat sich schon bald herausgestellt, dass diese Technik für viele Anwendungen viel zu kompliziert ist (aber ATM dominiert immer noch in Weitverkehrsnetzen). ATM bietet harte Dienstgütegarantien und dies Ende-zu-Ende. Das Internet von heute bietet keinerlei Dienstgüte. Die meisten Dienstgütearchitekturen sind in sich zusammengefallen oder konnten sich bis heute nicht durchsetzen (Integrated Services, Differentiated Services). Allerdings gab es nie viele Anwendungen, die direkt am Arbeitsplatz die Dienstgüte nutzen konnten, die von ATM angeboten wird. Die meisten der heutigen Anwendungen können sich an die wechselnden Dienstgüten des Internets anpassen. WATM hat sich nie durchsetzen können, aber einige der Ideen haben überlebt, da einige der Entwickler von WATM auch z.B. bei UMTS, HiperLAN2 etc. beteiligt waren (und wiederum ist es fraglich, ob es HiperLAN2 je auf den Markt schaffen wird).

8. Mobile Vermittlungsschicht

8.1 Siehe die Einführung von Kapitel 8. Das Hauptproblem ist die große Dynamik. Routing-Protokolle aus dem Internet (genauso wie die Routing-Protokolle in traditionellen Telefonnetzen) wurden niemals für Netze mit mobilen Knoten oder gar mobilen Routern entwickelt. Ohne zusätzliche Mechanismen versagt die Adressierung, Knoten würden topologisch falsche Adressen nutzen usw. Standard Routing-Protokolle vom Internet (z.B. OSPF innerhalb autonomer Systeme, BGP zwischen diesen Systemen) können Verbindungsausfälle, Router-Versagen oder Überlastsituationen handhaben, solange sie nicht zu oft vorkommen.

8.2 Schnelle Lösungen könnten die permanente Anpassung der aktuellen IP-Adresse eines Knotens an den aktuellen Aufenthaltsort einschließen. Aber dann könnte kein Kommunikationspartner diesen mobilen Knoten finden (oder eine Menge an Signalisierung wäre notwendig, um die Adresse bekannt zu machen). Alternativ könnten alle Router ihre Routing-Tabellen so anpassen, dass dadurch der aktuelle Ort eines mobilen Knotens aufgezeigt wird. Dieser Ansatz skaliert nicht und ist zudem noch sehr unsicher – eine häufige Änderung der Routing-Einträge destabilisiert das gesamte Netz.

8.3 Siehe 8.1.1. Obwohl Mobile IP versucht, die Mobilität transparent zu unterstützen, kann es doch nicht z.B. die erhöhte Verzögerung aufgrund größerer Entfernungen oder geringere Dienstgüte aufgrund schlechterer Verbindungen zum mobilen Knoten verbergen. Die Mobilität ist nur dann einigermaßen transparent, wenn nur „best-effort“ Verkehr betrachtet wird. Skalierbarkeit ist ebenfalls ein Problem, sobald sich sehr viele Knoten zwischen Subnetzen hin- und herbewegen. Mobile IP verursacht auch einen großen Mehraufwand auf Grund der Registrierungsnachrichten. Dies ist eine der Motivationen für Ansätze, welche die Mikromobilität unterstützen. Zudem ist auch die Sicherheit problematisch, da topologisch falsche Adressen nicht zusammen mit Firewalls eingesetzt werden können und die Optimierung der Wege den aktuellen Aufenthaltsort bekannt gibt.

8.4 Siehe Abbildung 8.2. Eine Kapselung wird zwischen HA und COA benötigt. Letztere könnte im FA oder MN angesiedelt sein. Dies wird benötigt, um die Mobilität transparent zu machen. Das innere Datenpaket sollte nichts von der Übertragung durch den Tunnel mitbekommen. Aus diesem Grund bleibt die TTL unberührt.

8.5 Siehe Abbildung 8.4. Die Schicht-2-Registrierung wird z.B. durch ein WLAN oder ein festes LAN abgearbeitet.

8.6 Angenommen ein MN entdeckt ein stärkeres Signal von einem Zugangspunkt, der nicht der aktuelle ist. Falls möglich auf Schicht 2, könnte ein MN sich von seinem alten Zugangspunkt lösen, nachdem er sich an den neuen angebunden hat. Zunächst

müsste eine Schicht-2-Assoziation aufgebaut und auf „Agent Advertisements“ gewartet werden. Alternativ könnte ein MN „Agent Solicitations“ senden. Nachdem ein Advertisement empfangen wurde und sich der MN an einen neuen FA gebunden hat, könnte die Authentifizierung starten. Parallel dazu könnte der FA den alten FA über den Knoten informieren. Siehe Abbildung 8.13 plus Schicht 2, z.B. 8.3.5 für 802.11.

8.7 Wenn MN_a und MN_b beide in Fremdnetzen angebunden an FA_a und FA_b sind, ist der Paketfluss wie folgt. MN_a sendet Pakete zu MN_b über das Internet zum HA_b (in Wirklichkeit sendet MN_a an MN_bs Adresse, HA_b fängt lediglich die Pakete ab). HA_b kapselt die Pakete zu FA_b, der die Pakete dann zum MN_b weiterleitet. Sobald Rücktunnel erforderlich sind, ist der Paketfluss wie folgt: MN_a sendet seine Pakete über FA_a durch den Rücktunnel über HA_a und das Internet zu HA_b. HA_b leitet dann die Pakete durch den Tunnel zum FA_b, der sie dann wiederum zum MN_b weiterleitet.

8.8 Tunneln bedeutet einfach, dass ein Paket am Tunneleingang gekapselt wird und am Tunnelausgang wieder entkapselt wird. Das Paket ist also die Nutzlast des äußeren Pakets im Tunnel. IP-in-IP-Kapselung ist der einfache Fall, bei dem IP zur Kapsleung von IP-Paketen genutzt wird. Dies ist deswegen einfach, weil bereits alle Geräte wissen, wie man eine Nutzlast in IP-Pakete einfügt. Bandbreite wird dadurch verschwendet, dass einige Felder mehrfach übertragen werden. Minimale Kapselung versucht diese Verschwendung von Bandbreite zu vermeiden. Allerdings kann sie nicht im Fall von Fragmentierung eingesetzt werden. GRE ist ein allgemeineres Schema, nicht nur für IP-Verkehr, sondern auch z.B. für die Kapselung von Ethernet-Paketen in IP-Paketen. Zudem kann es die Ebenen der Kapselung steuern. Verschiedene Versionen existieren.

8.9 Dreiecks-Weiterleitung über CN-HA-FA-MN ist ineffizient. Eine Optimierung sind Aktualisierungen der Binding-Tabellen im CN. Ein CN kann die COA eines MNs in seine Weiterleitungstabelle eintragen. Dies ermöglicht es dem CN seine Daten direkt zum MN zu senden. Diese Lösung enthüllt den aktuellen Aufenthaltsort des MNs und ist

nicht mehr transparent (ein CN weiß nun, dass der MN mobil ist – zudem kennt er den Ort mit Hilfe der COA).

8.10 Viele Funktionen zur Unterstützung der Mobilität sind bereits in IPv6 integriert. Ein besonders ausgewiesener FA ist nicht mehr notwendig. Weiterhin beherrschen alle Router Agent Advertisements, Tunnel, Datenweiterleitung, Aufbau von Sicherheitsassoziationen. Eine Authentifizierung ist ebenso wie vielfältige Optimierungen bereits integriert.

8.11 Mobile IP erhöht nicht die Sicherheit im Vergleich zu IP, im Gegenteil. Die einzige zusätzliche Sicherheitsfunktion ist die Authentifizierung von MN und HA. Wollen jedoch MN und HA gemeinsam einen FA angreifen, so kann dies nicht verhindert werden. Firewalls und Mobile IP arbeiten zudem nicht wirklich zusammen. Entweder bohren Rücktunnel oder Tunnel im Allgemeinen ein Loch in die Firewall oder MNs können in Fremdnetzen schlichtweg nicht arbeiten. Eine Firewall muss auf jeden Fall in die Sicherheitsassoziation mit integriert werden. IP unterstützt keine Dienstgüte. Falls Dienstgüte-unterstützende Mechanismen wie DiffServ oder IntServ eingesetzt werden sollen, so werden auch für Mobile IP neue Funktionen benötigt, um die Dienstgüte während und nach einer Übergabe zu unterstützen. Weiterhin müssen Pakete mit einer bestimmten Dienstgüte entsprechend dieser Anforderungen auch innerhalb eines Tunnels richtig behandelt werden.

8.12 DHCP ist ein Mechanismus zur Konfiguration von Rechnern. Die Parameter, die über DHCP erhalten werden können, sind beispielsweise IP-Adresse, Standard-Gateway, DNS-Server, Subnetz-Maske usw. Ohne DHCP müssten alle Parameter von Hand konfiguriert werden. Ein DHCP-Server bietet DHCP-Informationen an, ein Relay kann die Daten in verschiedene LANs weiterleiten.

8.13 Falls Nutzer nur auf einen anderen Server zugreifen wollen, z.B. zum Surfen im WWW, wird Mobile IP nicht gebraucht. Nachdem ein Knoten mit Hilfe von DHCP eine neue IP-Adresse erhalten hat, kann er als Client das Netz nutzen. Sobald ein Knoten allerdings Dienste anbieten möchte, sollte er seine IP-Adresse immer beibehalten.

Anderenfalls ist es schwer den Knoten zu finden oder weitere Mechanismen wie DDNS werden benötigt, um den Namen eines Rechners auf dessen Adresse abzubilden. DHCP kann als Quelle für COAs in Mobile IP genutzt werden.

8.14 Ad-hoc-Netze brauchen generell keine Infrastrukur, um zu funktionieren (sie können allerdings mit einem Infrastrukturnetz verbunden sein). Multi-hop Ad-hoc-Netze erlauben es zusätzlich, dass sich nicht alle Knoten gegenseitig empfangen müssen. Knoten können Daten für andere Knoten weiterleiten. Vorteile sind die niedrigere Sendeleistung (vergleichbar mit dem Flüstern in das Ohr des Nachbarn im Vergleich zum lauten Hinausbrüllen) und die erhöhte Robustheit (das Versagen einzelner Knoten kann toleriert werden).

8.15 Die Wegewahl ist kompliziert auf Grund der häufigen Topologieänderungen, der unterschiedlichen Knotenfähigkeiten und der unterschiedlichen Ausbreitungsbedingungen. Zudem kann keine zentrale Instanz die Weiterleitung unterstützen.

8.16 Beide Algorithmen gehen mehr oder weniger von einem stabilen Netz aus. Zumindest sind die Veränderungen relativ selten im Vergleich zum Austausch von Routing-Daten. Zudem bauen beide Algorithmen Weiterleitungstabellen unabhängig von der Notwendigkeit zu kommunizieren auf. Dies verursacht nicht nur viel unnötigen Datenverkehr, sondern kann sich auch als vollständig unnötig erweisen, sobald sich die Topologie vor einer Kommunikation verändert hat.

8.17 AODV ist ein reaktives Protokoll. Die Berechnung eines Weges wird nur dann vorgenommen, wenn es notwendig ist. Dies erhöht deutlich die Skalierbarkeit unter leichter Last, verursacht jedoch eine höhere initiale Verzögerung.

8.18 DSR trennt das Finden eines Weges von dem Aufrechterhalten des Weges. Wird keine Kommunikation benötigt, so versucht DSR nicht, einen Weg aufrecht zu erhalten. Sobald dann ein Weg für Daten benötigt wird, versucht DSR einen solchen zu finden. Solange die Kommunikation andauert versucht DSR, den Weg aufrecht zu erhalten. In Festnetzen können Wege immer im Voraus berechnet werden.

8.19 Die meisten Algorithmen versagen, sobald die Verbindungen asymmetrisch sind (bis hin zu dem extremen Fall unidirektionaler Verbindungen). Betrachtet man DSR, so ist hier vorgesehen, dass ein Empfänger einfach das Paket, welches den Weg vom Sender bis zum Empfänger über alle Router aufgezeichnet hat, zurück zum Absender schickt, indem die aufgezeichneten Router in umgekehrter Reihenfolge abgearbeitet werden. Was aber, wenn einige Verbindungen in umgekehrter Richtung überhaupt nicht vorhanden sind? Dann muss DSR nach dem gleichen Prinzip auch einen Rückweg finden. Danach haben Sender und Empfänger beide einen Weg, allerdings jeweils in der falschen Richtung. Irgendwie muss also die Information die jeweils andere Seite erreichen. Ohne einen Weg ist dies schwierig (ein Rundruf, also das Fluten des Netzes ist natürlich immer eine Lösung...).

8.20 Mobile IP verursacht einen zu großen Mehraufwand während der Registrierung, wenn es für sehr mobile Knoten eingesetzt wird (also Knoten, die ihr Netz sehr häufig wechseln). Zudem werden alle Registrierungsnachrichten quer durch das Internet vom Fremdenetz in das Heimatnetz übertragen (zudem enthüllen Registrierungen den aktuellen Aufenthaltsort). Ansätze, welche die Mikromobilität unterstützen, fügen im Wesentlichen eine weitere Hierarchieebene ein, um etwas von der Komplexität und der Last vom HA zu nehmen (vergleichbar mit HLR und VLR).

8.21 Ortsinformation kann sinnvoll für eine Wegewahl eingesetzt werden (Geo-Routing), da so eventuell Routen optimiert werden können. Falls man bereits seinen Ort kennt, ist es häufig einfacher z.B. Daten über einen Router in der richtigen Richtung zum Ziel zu senden. Allerdings können auch hier wiederum Probleme mit der Privatheit entstehen, da nicht allzu viele Menschen ihren Aufenthaltsort jedem offen legen wollen.

8.22 Falls sich Autos in einer Innenstadt sehr schnell bewegen, so ist eine effiziente Paketweiterleitung sehr schwer, da sich die Topologie zu schnell ändert. Das Fluten des Netzes mit einigen Optimierungen könnte der einzig verfügbare Weg sein. Befinden sich jedoch die Autos auf einer Autobahn, stellt sich die Situation einfacher dar: Die

Autos bilden ganz typische Gruppen pro Richtung. Ein Auto der Gruppe könnte der Kopf sein, alle andere Autos leiten über diesen Kopf die Daten in Richtung Internet weiter. Die Wegewahl und Paketweiterleitung könnte dann entlang der Spuren der Autobahnen gehen.

9. Mobile Transportschicht

9.1 Paketverluste auf Grund von Übertragungsfehlern: Relativ gering in Festnetzen (10^{-10}-10^{-12}), relativ hoch in drahtlosen Netzen (10^{-2}-10^{-4})/große Variation/typischerweise kompensiert durch ARQ/FEC; Paketverlust auf Grund von Stau: kein Unterschied zwischen drahtlosen und leitungsgebundenen Netzen; Paketverlust auf Grund der Mobilität: passiert nur in Mobilnetzen …

9.2 TCP geht typischerweise von einer Stausituation im Falle von Paketverlusten aus. Diese Annahme ist in Festnetzen meist korrekt, nicht aber in drahtlosen Netzen. Übertragungsfehler auf Grund von Interferenzen und Mobilität sind weitaus häufiger. In Festnetzen hilft TCP das Internet zu stabilisieren, in drahtlosen und mobilen Netzen hat ein unverändertes TCP nur eine relativ schlechte Leistungsfähigkeit.

9.3 Würden nur einige Nutzer TCP durch UDP ersetzen, dann würden sie in der Tat einen höheren Durchsatz erzielen. Allerdings würden die fehlenden Mechanismen zur Stauvermeidung schon bald zu einem riesigen Paketverlust im Internet führen. Zudem müssten Mechanismen integriert werden, die eine zuverlässige Datenübertragung bieten, da UDP keinerlei Garantien abgeben kann. Es gibt eine Menge an Forschungsarbeiten auf dem Gebiet „TCP-freundlicher“ Protokolle, zuverlässigem UDP etc.

9.4 I-TCP teilt die Verbindung in zwei Teile auf – einen leitungsgebundenen/festen und einen drahtlosen/mobilen Teil. Dies isoliert die Probleme der drahtlosen Anbindung vom Festnetz. Dies erfordert allerdings auch, dass Zwischensysteme in ein IP-Paket hineinschauen können, um die Verbindung entsprechend aufzutrennen. Damit kann

eine Technik wie IPsec nicht mehr eingesetzt werden. Ende-zu-Ende-Sicherheit und I-TCP (oder Proxy-Lösungen auf dieser Ebene) passen nicht zusammen.

9.5 Siehe Abbildung 8.2 für den Paketfluss. TCP arbeitet nicht direkt mit IP zusammen, da Mobile IP versucht, die Mobilität transparent zu machen. TCP könnte allerdings höhere Paketverlustraten während einer Übergabe bemerken. Mobile IP steuert die Übergabe, alte FAs können, müssen aber nicht Pakete weiterleiten. Sobald eine Bestätigung zu spät eintrifft, geht TCP von einer Stausituation aus und reagiert mit seinen Stauvermeidungsmechanismen (slow start). Allerdings ist Slow-Start absolut kontraproduktiv in dieser Situation. Weitersenden mit der gleichen Datenrate wäre das einzig Sinnvolle.

9.6 Vergleichen Sie mit Abbildung 9.2. FA, CN, HA, MH sollten sich so verhalten wie in Mobile IP spezifiziert. Ohne PEP würde TCP Paketverluste auf Grund des Subnetz-Wechsels bemerken, falls der alte FA Pakete nicht weiterleitet. Sobald PEPs eingesetzt werden, muss der alte PEP den gesamten Kontext (Puffer für die Übertragungswiederholung, Sockets, …) an den neuen PEP übertragen. Weder CN noch MH sollten etwas von der Existenz der PEPs mitbekommen. Ein guter Platz für einen PEP ist der FA. Natürlich könnte sich ein PEP auch an der Grenze zum Festnetz befinden. PEPs arbeiten (in diesem Beispiel) auf Schicht 4, während Mobile IP auf Schicht 3 arbeitet. Die Komponenten können miteinander interagieren, müssen aber nicht.

9.7 Sobald Ende-zu-Ende-Verschlüsselung eingesetzt wird, kann nicht gleichzeitig ein Proxy genutzt werden – außer der Proxy kann in die Sicherheitsbeziehung mit aufgenommen werden. Dies ist allerdings oft nicht möglich, da das Fremdnetz zusammen mit dem Proxy zu einer anderen Organisation gehört. Sobald IPsec mit Verschlüsselung eingesetzt wird, kann kein Proxy mehr in das Paket hineinschauen und den TCP-Paketkopf für eine weitere Bearbeitung nutzen.

9.8 Selektive Übertragungswiederholung ist immer eine gute Idee. Fast alle anderen Optimierungen haben teilweise schwere Nachteile: siehe Abschnitt 9.3. Es gibt derzeit

nicht „die“ Lösung für das Problem und auch die Standards/Standardisierungsvorschläge widersprechen sich teilweise gegenseitig.

9.9 Zunächst der trickreiche Teil. Fehlerraten auf Verbindungen, so wie sie in der Frage gegeben sind, sind immer Bitfehlerraten (BER, Bit Error Rate). Unter der Annahme, dass diese Fehler voneinander unabhängig sind (und auch nur unter dieser Annahme), kann die Paketverlustrate p, die in der Formel genutzt werden soll, wie folgt berechnet werden: $p = 1 - ((1-BER)^{Paketgröße})$. Mit Hilfe dieser Formel können nun die Paketverluste unter Vernachlässigung von FEC und ARQ berechnet werden.

- Festnetz: $BER = 10^{-10}$, MSS = 1000 byte = 8000 bit, daraus ergibt sich eine Paketverlustrate $p = 1 - ((1-10^{-10})^{8000}) \approx 8*10^{-7}$. RTT = 20 ms: Geht man von der einfachen Formel aus, dann ergibt sich eine maximale Bandbreite von $0.93 * 8000 / (0.02 * \sqrt{(8*10^{-7})})$ bit/s ˜ 416 Mbit/s.
- WLAN: Die gleiche Berechnung mit einer typische WLAN-Fehlerrate von 10^{-3} und zusätzlichen 2 ms Verzögerung ergibt eine Paketverlustrate von 0.99966 und eine Bandbreite von $0.93 * 8000 / (0.022 * \sqrt{0.99966})$ bit/s ˜ 338 kbit/s. Dies ist ein gutes Beispiel, das zeigt, warum große Pakete in WLANs Probleme verursachen – und warum FEC/ARQ auf jeden Fall gebraucht werden… Der Durchsatz in der Praxis für WLANs liegt bei etwa 6 Mbit/s für 802.11b, falls gerade keine anderen Nutzer aktiv sind.
- GPRS: Verwendet man GPRS mit zusätzlichen 2 s RTT und einer BER von 10^{-7} (also einer Paketverlustrate von $8*10^{-4}$) erhält man lediglich $0.93 * 8000 / (2.02 * \sqrt{(8*10^{-4})})$ bit/s ˜ 130 kbit/s. Derzeit bietet ja GPRS sowieso nur etwa 50 kbit/s an, aber dies ist eine Einschränkung, die in dieser einfachen Formel nicht berücksichtigt wird.
- In der Praxis hängt die Leistungsfähigkeit von Funktechniken sehr stark von den Fehlerkorrekturfähigkeiten der unteren Schichten ab. Solange FEC und ARQ auch Schicht 2 gute Arbeit leisten, merkt TCP kaum etwas von den höheren Feh-

lerraten. Jedoch wird die Verzögerung, die von ARQ und der Verschachtelung verursacht wird, die Bandbreite verringern. Weiterhin muss das langsame Steigen der Datenrate durch TCP für sehr kurzlebige Verbindungen berücksichtigt werden. Auf jeden Fall kann man aber erkennen, dass eine einfache Erhöhung der Datenraten in GPRS nicht notwendigerweise auch in höheren Datenraten für einen Nutzer von TCP über GPRS resultiert.

9.10 Unabhängig davon wie geschätzt wird, TCP kann nie eine Datenrate zur Verfügung stellen, die über der maximalen Datenrate der Verbindung liegt. Diese Datenrate der Verbindung taucht nicht in der Formel auf, da jeder Versuch, schneller als die langsamste Verbindung auf der Strecke von einem Sender zum Empfänger zu senden, unweigerlich ein Wachsen der Warteschlange beim Sender zur Folge hat. Damit erzeugt ein Flaschenhals automatisch auch höhere RTTs (Pakete müssen länger in der Ausgangswarteschlange verweilen), die sich dann direkt auf die erreichbaren Datenraten auswirken.

10. Mobilitätsunterstützung

10.1 Es ist schlichtweg zu teuer, eine starke Konsistenz der Daten aufrecht zu erhalten. Kontinuierliche Aktualisierungen erfordern auch eine permanente Anbindung. Ohne diese Anbindung müssten alle Zugriffe geblockt werden. Alternativen führen immer eine gewisse Schwächung der Konsistenz ein. Viele Verfahren umfassen periodische Aktualisierungen, automatische Rückintegrationsverfahren oder zur Not eine manuelle Rückintegration der Daten.

10.2 Entweder stürzt das Dateisystem gleich zusammen mit dem Rechner ab oder der Rechner zeigt einfach an, dass das Verzeichnis derzeit nicht zur Verfügung steht. Versuchen Sie es einfach mit verschiedenen Systemen aus (speichern Sie aber bitte vorher alle Daten).

10.3 Ohne Zustand benötigt man auch keine komplexe Zustandsverwaltung. Bricht eine Verbindung ab, so spielt das keine Rolle, da die notwendigen Zustandsdaten mit der

nächsten Anfrage wieder geliefert werden. Trotzdem ist natürlich ein Zustand sinnvoll, wenn unnötiger Mehraufwand vermieden werden soll oder der Nutzer Sitzungen wieder aufnehmen können soll. Heute wird jeglicher Zustand für HTTP zusammen mit dem Ergebnis der Anfrage zurückgeliefert. Längerfristige Zustände können in Cookies gespeichert werden. Damit lebt der Zustand so lange wie der Cookie existiert. Kurzlebige Zustände werden im Browser abgelegt. Insbesondere HTTP/1.1 unterstützt Browser, welche die Geschichte einer Sitzung mit einbeziehen (teilweise Übertragung von Inhalten, Wahl einer bevorzugten Sprache, Behandlung von Inhalten der Zwischenspeicher,…).

10.4 HTTP ist textorientiert und lesbar durch den Menschen. Dadurch kann HTTP sehr einfach durch Menschen nachvollzogen werden; allerdings verschwendet das Verfahren auch Bandbreite im Vergleich zu binären Repräsentationen. Setzt man HTTP/1.0 ein, so wird zusätzlich Bandbreite dadurch verschwendet, dass jede Anfrage eine neue TCP-Verbindung nutzt. Dies erfordert einen Verbindungsaufbau, einen Datentransfer und einen Verbindungsabbau für jedes einzelne Element auf einer Web-Seite. HTTP/1.1 nutzt persistente Verbindungen. D.h. eine TCP-Verbindung kann mehrere Anfragen und Antworten übertragen.

10.5 Je näher sich ein Zwischenspeicher zum Browser befindet, desto besser können Anfragen mit einer geringen Verzögerung beantwortet werden. Befindet sich dieser Speicher sogar auf dem mobilen Endgerät, können viele Anfragen direkt lokal beantwortet werden und man vermeidet damit unnötige Übertragungen über die Funkstrecke. Befindet sich der Zwischenspeicher an der Grenze zwischen Fest- und Funknetz, so können damit die Probleme im Fest- bzw. Funknetz jeweils voneinander getrennt werden. Ein Zwischenspeicher im Festnetz kann auch einem Nutzer nachfolgen.

10.6 In einem Zwischenspeicher kann man nur die Inhalte ablegen, die sich im Mittel nicht häufiger verändern als Zugriffe erfolgen. Allerdings enthalten heutige Web-Seiten sehr viele individualisierte Komponenten: Zähler, Werbung, Browser-abhängige Inhal-

te etc. Zudem wollen Inhalteanbieter oft nur einen direkten Zugriff der Nutzer auf ihre Inhalte, damit gewisse Nutzungsprofile besser erstellt werden können. Ein Zwischenspeicher ohne zusätzliche Mechanismen macht Zugriffszähler und eine Profilbildung ziemlich sinnlos. Ist das Endgerät mobil, so sollte der Zwischenspeicher auch dem Endgerät nachfolgen.

10.7 HTML beschreibt heute nicht nur einfach den Inhalt sondern sehr oft auch das Aussehen einer Seite. Die ursprüngliche Idee von HTML sah die Unterstützung der Beschreibung einer Textstruktur vor (Überschriften, Listen, Aufzählungen etc.). Jetzt wird HTML aber oft zur Formatierung eingesetzt. Die meisten Seiten gehen von einer Auflösung von 1024x768 Bildpunkten und Echtfarbendarstellung aus. Drahtlose Endgeräte haben jedoch meist immer noch relativ kleine Anzeigen mit z.B. 4096 Farben, 320x240 Bildpunkten. Aus diesem Grund passen auch viele Seiten nicht auf die Anzeigen. Lösungen umfassen eine Skalierung der Bilder, eine Inhaltsextraktion oder die Beschreibung des Inhalts mit speziellen Sprachen (WML, cHTML). Viele Seiten enthalten zusätzliche Inhalte, die bestimmte Plug-Ins benötigen: Flash, 3D-Animationen, Streaming Media usw. Typischerweise funktionieren diese Erweiterungen auf mobilen Endgeräten einfach nicht.

10.8 Zwischenspeicherung (caching), Inhaltstransformation, Skalierung von Bildern, Inhaltsextraktion, textuelle Beschreibung von Bildern. Viele der Vorschläge aus den Neunzigern waren proprietär. WAP wurde zur ersten standardisierten, gemeinsamen Lösung, die von vielen Netzbetreibern und Geräteherstellern unterstützt wurde. Es ist eine ganz andere Geschichte, warum WAP anfangs alles andere als ein Erfolg war (falsches Marketing, falsche Transporttechnik für die Daten).

10.9 Proxys. Proxys können sich an verschiedenen Stellen befinden – siehe Abbildungen – und Proxys können zudem in zwei Hälften aufgeteilt werden, wobei ein spezielles Protokoll zwischen den Hälften genutzt werden kann. Proxys verhalten sich wie ein Client in Richtung Server und wie ein Server in Richtung Client. Ein guter Ort für einen Proxy ist möglichst nahe am mobilen/drahtlos angebundenen Nutzer, jedoch im-

mer noch im Festnetz. Beispiele für Orte können FAs in Mobile IP oder Router in einem GPRS-Netz sein.

10.10 Siehe Abschnitt 10.3. Generelle Ziele sind ein effizienter Datentransfer (binäre Repräsentation), Vermeidung von redundantem Datentransfer (zustandsbehaftete Protokolle), Unterstützung von heterogenen Geräten (WML), Zugang zu Telefoniefunktionen (WTAI), eingebaute Sicherheit (WTLS) und Unterstützung von praktisch allen Transportplattformen.

10.11 Telefonieanwendungen werden über spezielle Schnittstellen in WAP 1.x unterstützt (WTAI). Spezielle Gateways werden benötigt, um auf Internet-Inhalte zugreifen zu können. WAP 2.0 kombiniert Internet-Protokolle mit WAP 1.x. Dies ermöglicht einen direkten Zugriff auf Internet-Inhalte.

10.12 WDP ist kein festes Protokoll. Die Schnittstelle zu WDP ist festgelegt, WDP selbst hingegen hängt vom darunter liegenden Transportnetz ab. An der WDP-Schnittstelle wird ein unzuverlässiger Datagramm-Transfer angeboten. Bietet das darunter liegende Netz bereits IP-Dienste an, so wird als WDP schlicht UDP, wie es vom Internet her bekannt ist, eingesetzt. Aus diesem Grund gibt es auch keinen festgelegten Dienstzugangspunkt (SAP), den WDP nutzen könnte.

10.13 Nicht alle Mobiltelefonnetze bieten die gleiche Sicherheit an. GSM bietet beispielsweise lediglich eine Verschlüsselung über die Luftschnittstelle. WAP 1.x fügt Sicherheit vom Endgerät bis zum Gateway hinzu. Dies ist jedoch ein Problem, da WAP 1.x keine Ende-zu-Ende-Sicherheit garantieren kann. Die Sicherheitsassoziation wird am Gateway aufgebrochen. Daher implementieren z.B. Banken ihre eigenen Sicherheitsmodule auf den Endgeräten. Dieses Aufbrechen ist auch ein Unterschied zu Mechanismen wie SSL/TLS im Internet, die Ende-zu-Ende arbeiten.

10.14 Vorteile: Nutzer können direkt die Bestätigung steuern; Nutzer möchten eventuell wissen, dass etwas schief gelaufen ist; manchmal ist es auch sinnvoll, einen Sender durch künstliche Verzögerungen der Bestätigung abzubremsen; die Bestätigung

durch einen Nutzer ist „stärker“, da es dem Sender zeigt, dass der eigentliche Empfänger und nicht nur der WTP-Prozess die Nachricht erhalten hat. Nachteile: Nutzer müssen interagieren, das benötigt mehr Zeit. Klassische Transaktionsdienste können typischerweise von einer Bestätigung durch Nutzer profitieren. Für die meisten Push-Dienste sind diese Bestätigungen nicht notwendig. WTP-Bestätigungen können aber dennoch die Zuverlässigkeit erhöhen.

10.15 WSP/B zusammen mit Klasse-2-Transaktionen wären eine gute Wahl für normale Anfragen/Antworten im Web. Das Web erwartet ein zuverlässiges Protokoll, darum wird normalerweise auch TCP eingesetzt, und arbeitet mit Transaktionen (in dem hier benutzen Sinn: Anfrage/Antwort im Gegensatz zu einem Datenstrom).

10.16 WSP bietet Sitzungsverwaltung, Aushandlung der Fähigkeiten, Push und Pull, asynchrone Anfragen und effiziente Inhaltecodierung. Einige dieser Fähigkeiten hat auch HTTP/1.1. In mobilen und drahtlosen Umgebungen resultiert eine effiziente Codierung direkt in einer billigeren Nutzung des Webs.

10.17 Die Nutzerzufriedenheit mit einem System ist meist viel besser, wenn etwas auf dem Bildschirm geschieht. Muss man erst warten, bis alle Antworten in der richtigen Reihenfolge angekommen sind, würden diese langen Pausen doch die meisten Nutzer sehr irritieren. Sobald also eine Antwort ankommt, sollte der Browser auch deren Inhalt anzeigen, um einen Fortschritt zu signalisieren. Zudem können Nutzer oft schon bereits angezeigten Verweisen weiter folgen, obwohl erst Teile der Seite angezeigt werden.

10.18 Verbindungslose Dienste haben meist einen deutlich geringeren Mehraufwand im Vergleich zu Verbindungsaufbau/Datenübertragung/Verbindungsabbau verbindungsorientierter Dienste. Im Vergleich zu einem reinen Datagramm-Dienst bietet der verbindungslose Sitzungsdienst zusätzlich Kennungen für die Transaktionen und Funktionen, die mit denen anderer WSP-Dienste vergleichbar sind.

10.19 Neben der Sprache und Inhaltsformaten definiert das WAE Gateways zwischen Client und Server. Da mobile Endgeräte oft nicht mit den Standardformaten und -protokollen aus dem Internet umgehen können (TCP, HTTP, SSL etc.), müssen Gateways zwischen den klassischen Festnetzen und der neuen mobilen und drahtlosen Welt übersetzen.

10.20 WML bietet nur recht wenige Formatierungsanweisungen. Es definiert eher die Absichten des Autors einer Seite. Soll ein Gerät Daten einem Nutzer präsentieren, so kann dies entweder als Text oder durch Sprachausgabe geschehen. Dieser Ansatz ist flexibler als HTML, das sich eher auf leistungsfähige Anzeigen verlässt. Natürlich schrumpft der Abstand zwischen kleinen, mobilen Geräten und PCs immer weiter. Weiterhin sind häufige Schlüsselwörter binär codiert. Anstelle der Übertragung von “http://www.” kann ein einzelnes Byte das Gleiche ausdrücken.

10.21 Skriptsprachen können helfen, den Datenverkehr zu reduzieren, indem sie Eingaben direkt auf einem Mobilgerät überprüfen. Ohne diese Funktionalität müssten alle Eingaben zunächst zur Überprüfung an einen Server übertragen werden. Zudem können über entsprechende Funktionen in Skripten viele Gerätefunktionen angesprochen werden.

10.22 Call indication, call accept, call setup, … WTAI bietet spezielle URLs und WTAscript-Funktionen für Telefonieanwendungen. Eine URL kann automatisch einen Anruf einleiten, WTAscript-Funktionen können Telefonbucheinträge verändern usw.

10.23 WTA-Server können die Dienstgüte weitaus besser steuern, da sie typischerweise zum Netz des Mobilnetzbetreibers gehören. Normale Server im Internet haben viele Probleme bei der Unterstützung von Dienstgüte, es gibt nicht einmal weit verbreitete Dienstgütearchitekturen im Internet. Im Prinzip gibt es viele Orte für WTA-Server: im Betreibernetz, in den Netzes anderer Betreiber, im Internet (dann aber mit den bereits erwähnten Dienstgüteproblemen).

10.24 Ein Push ist sinnvoll, um damit unerwartete Ereignisse anzukündigen. Eine regelmäßige Abfrage (pull) durch das Mobilgerät würde Bandbreite und Energie verschwenden. Der Unterschied zwischen SI und SL besteht darin, dass im Fall von SL der Nutzeragent des Client darüber entscheidet, wann die URI gesendet wird (dies ist dann ein Pull, was aber vom Nutzer nicht bemerkt wird). Ein SI wird lediglich angezeigt und es liegt am Nutzer, wann und ob der Dienst genutzt wird.

10.25 WAP 1.x wurde von einem Konsortium aus Netzbetreibern und vielen Geräteherstellern entwickelt, während i-mode eine proprietäre Entwicklung von NTT DoCoMo aus Japan ist. i-mode wurde von Anfang an über einem paketorientierten Transportdienst eingesetzt (PDC-P) und es umfasst zusätzlich ein Geschäftsmodell: Inhalteanbieter bekommen z.B. 80% des Umsatzes, den ein Kunde erzeugt, der Netzbetreiber übernimmt für den Rest die Abrechnung. WAP hatte starke Probleme in seinen Anfangstagen, da es als „Internet auf dem Handy“ vermarktet wurde, was es sicherlich nicht ist. Zudem startete es fatalerweise auf einem verbindungsorientierten Transportsystem, die Web-Nutzung ist jedoch hochgradig interaktiv. Diese beiden Faktoren ließen WAP recht bald zu einem Fehlschlag werden. Die Übertragung des Erfolgs von i-mode in Japan auf andere Länder ist alles andere als einfach. NTT DoCoMo versuchte dies in Europa, hatte jedoch nicht den gleichen Erfolg. Ein Grund hierfür war der hohe Anteil an PC-Besitzern in Europa – viele Menschen nutzen bereits täglich das Internet über eine recht schnelle Anbindung. Zudem haben sich nur wenige Betreiber für i-mode entschieden und schon bald lockten andere Dienste, wie MMS, die Kunden an.

10.26 Synchronisation ist wesentlich für eine Vielzahl an Anwendungen. Hierzu gibt es bereits mehrere inkompatible Ansätze, sogar Anwendungen haben hierzu oft ihre eigenen Mechanismen. Jedoch ist das grundlegende Problem einer Synchronisation immer noch nicht gelöst: Wie sollen zwei veränderte Kopien eines Objekts synchronisiert werden? Ohne Anwendungswissen ist hier eine Synchronisation nicht möglich.

10.27 WAP 2.0 umfasst i-mode und Internet-Komponenten. Die Entwicklung wurde sehr stark vom Erfolg der Internet-Anwendungen beeinflusst, aber auch von der immer größeren Leistungsfähigkeit mobiler Geräte.

10.28 Siehe Abbildung 10.38.

- WAP 1.x Stapel: Dieser Protokollstapel unterstützt alle „klassischen“ WAP-Geräte und –Anwendungen. Wie in diesem Abschnitt dargestellt, gibt es viele Gründe für Sitzungsdienste und effiziente Transaktionsdienste. Aus diesem Grund kann dieser Teil auch nützlich im neuen WAP sein.
- WAP mit profiled TCP: Dieses i-mode-ähnliche Szenario bietet optimiertes HTTP und TCP an. Dies kann effizienter sein als die direkte Verwendung von „reinen“ Internet-Lösungen, bedingt aber Änderungen in HTTP und TCP – und benötigt einen Proxy für die Übersetzung.
- WAP mit TLS-Tunnel: Sobald Ende-zu-Ende-Sicherheit gefordert wird, darf die Architektur nicht die Verbindung aufbrechen. Aus diesem Grund bietet dieser Stapel Ende-zu-Ende-TLS, kann aber trotzdem von einem optimierten TCP profitieren.
- WAP direkt: Falls die Endgeräte leistungsfähig genug und die Verzögerungen nicht zu hoch sind, kann auch ganz einfach der normale Internet-Protokollstapel verwendet werden. Dies wäre die einfachste Lösung, die auch keinerlei spezielle WAP-Protokolle mehr benötigt. Während die Geräte zwar sicherlich irgendwann leistungsfähig genug sein werden, so bleibt doch das Problem der Verzögerung.