Fachbereichsarbeit Informatik

Handies: Technik und Sicherheit des GSM-Netzwerks

Überblick über den Aufbau eines Handies, die Funktionsweise, Sicherheit, Geschichte und Zukunft des GSM-Netzwerks.

Wolfgang Mähr

Bundesgymnasium Feldkirch

Betreuer: Prof. Hubert Egger

Feldkirch, Februar 2000

1. Einleitung

Nach den charakteristischen Erfindungen des 20. Jahrhunderts wie beispielsweise das Fernsehen oder der Computer kommt gleich die Entwicklung des Handies und des GSM-Netzes. Beim Handy werden die Technologien vom Fernsehen (Funktechnik und Infrarotschnittstelle) und vom Computer (Prozessor, Smart Cards (SIM-Karte) und die Technik des Netzwerks) vereint. Dies bedeutet, dass das Handy die Kommunikation revolutionieren wird. Einerseits ist es mit seiner Hilfe schon jetzt möglich, immer und überall erreichbar zu sein; andererseits kann man mit jemandem sprechen, ohne dass man ihn sieht; trotzdem bleibt das Gespräch mehr oder weniger privat. In einigen Jahren wird sogar die mobile Bildtelefonie (Abb. 1) möglich sein. Durch die Technik von WAP (6.2) ist es inzwischen auch möglich die Inhalte des Internets in komprimierter Textform auf dem Handy darzustellen. Deshalb wird das Internet wohl bald als Informationsquelle für WAP erschlossen sein. Bald wird man mit dem Handy im Internet einkaufen und auch die Möglichkeit besitzen im Geschäft mit dem Handy statt der Kreditkarte zu bezahlen. Und in naher Zukunft wird das Handy die Steuerzentrale für das Haus werden: Es wird möglich sein mit dem Handy Fenster bzw. Türen zu öffnen, von auswärts das Licht in der Wohnung einzuschalten oder schon vor der Ankunft die Heizung einzuschalten. Dazu kommen noch Spielereien wie Kompass und Landkarte der Umgebung, Radio oder das Bestellen von Konzert- oder Kinokarten (alles schon möglich und erhältlich). Diese Aussichten, das Boomen der Telekommunikationsindustrie und die Grundlagen für das Funktionieren eines solchen Netzes waren mein Grund für diese Arbeit.

Abb. 1

Nach dem Aufbau eines Handies werde ich den Aufbau des GSM-Netzes mit den diversen Knotenpunkten erklären. Danach werde ich die Geschichte der Telekommunikation mit dem Anfang, der Morsetelegraphie, bis zum heutigen GSM-Netz kurz skizzieren. Ein weiteres wichtiges Kapitel ist die Sicherheit eines öffentlichen Netzes, einerseits muss der Kunde Anonymität wahren, andererseits sollte ein Dieb, der eines der Endgeräte stiehlt, schnell ausfindig gemacht werden. Abschießend werde ich noch die Projekte, die für die Zukunft wichtig sein werden, behandeln.

2. Aufbau eines Handy

Ein Handy besteht aus der Stromversorgung, einem Chip und zwei Schnittstellen. Diese Teile werden in eine Hülle eingebaut und fertig ist das Handy.

Als Stromversorgung sollte eine Spannungsquelle verwendet werden, die es einem einerseits ermöglicht, sich zu bewegen, und andererseits wiederverwendbar ist, also ein Akku (2.4). Als Verbindung zum Benutzer (Mensch) sollte das Handy, damit es bedienerfreundlich ist, eine graphische Anzeige (Display 2.4) und ein graphisches Eingabegerät (Touch-Screen oder Tastatur) beinhalten. Die andere Verbindung funktioniert über eine Antenne. Mit der Hilfe des Chips, der auf der SIM-Karte ist, können alle Daten, die von den beiden Schnittstellen kommen verarbeitet, auswertet und an die andere Schnittstelle weitergeben werden. Das Gehäuse hält nur all diese Teile zusammen und sollte einfachen physischen Zugriff auf das SIM (Karte des Anbieters für den Zugriff auf sein GSM-Netz) zulassen, da jeder Netzbetreiber eine eigene SIM-Karte hat. Alles in allem sollte ein Handy leicht, klein, elegant und angenehm zu bedienen, eben handlich sein. Auf die Größe, Gewicht und Eleganz konnten die Hersteller erst mit der Zeit achten, da die Techniken fehlte; und in letzter Zeit wurden diese Kriterien auch für den Kunden immer wichtiger.

2.1. Analog/Digital Konverter

Nachdem das Handy die Sprache über ein normales Mikrofon aufgenommen hat, kommt diese zu einem der wichtigsten Teile des Handies. Im A/D-Konverter (Analog/Digital) wird die analoge Information in eine digitale Information (in die binäre Form mit 0 und 1) umgewandelt. Die analoge Information ist die Sprache, die eine Modifikation der Amplitude und der Frequenz einer Sinus-förmigen elektrischen Schwingung ist; dabei entspricht die Tonhöhe der Frequenz und die Lautstärke dem Quadrat der Amplitude. Durch die Digitalisierung der Sprachdaten wird auch ihre Verschlüsselung erleichtert. Das GSM-Netz unterscheidet sich dadurch vom alten A-, B- und C-Netz, also durch den A/D-Wandler und die daraus resultierende digitale Signalübertragung.

Die Umwandlung des analogen Signals wird in drei Schritten vollführt: Im ersten Schritt wird die Amplitude des analogen Signals in gleichbleibenden zeitlichen Abständen gemessen. Dieser Vorgang wird als Sampling bezeichnet. Beim zweiten Teil, der Quantisierung, wird der Messwert dem nächsten vorgegebenen möglichen Wert zugeordnet; dies entspricht etwa dem Runden in der Mathematik. Die Codierung, die nun das quantisierte Sample (der nun „gerundete“ Wert) in das binäre Zahlensystem umwandelt, bildet den Abschluss. Nun werden die einzelnen Schritte genauer erklärt.

2.1.1.Sampling

In diesem Schritt wird in gleichbleibenden Zeitabständen die Amplitude des Analog-Signals abgetastet (Abb. 2). Die Genauigkeit und Geschwindigkeit des Samplings hängt vor allem von der Samplingfrequenz (Sampling-Rate) ab. Die Samplingfrequenz sagt aus, wie viel Samples (Proben) pro Sekunde genommen werden. Nach dem Shannonschen Abtasttheorem (E. Shannon, USA 1948) muss die Samplingfrequenz mindestens doppelt so hoch sein wie die höchste übertragene Frequenz. Deshalb muss, bevor die Samplingfrequenz berechnet werden kann, der Frequenzbereich festgelegt werden. Weiters wird normalerweise ein Reserve-Frequenzbereich mitverwendet und die Sampling-Rate wird noch mit dem Faktor 1,3 multipliziert.

Abb. 2

Damit die zu übertragende Datenmenge nicht zu groß wird, werden vor dem Sampling steilflankige Filter (schneiden am Rand viel weg, in der Mitte wenig) eingebaut, die die Obertöne und die unhörbaren Geräusche wegschneiden, aber die Nutztöne nicht beeinflussen.

Die Folge des Samplings ist eine Abfolge von Impulsen mit der genauen Amplitude des Eingangssignals oder eine Tabelle mit der Zeit und der dazugehörigen Amplitude. Diese Abfolge von Impulsen, PAM (Puls-Amplitudenmodulation) genannt, ist noch genauso störungsanfällig wie das Ausgangssignal, da eigentlich nur die Datenmenge „gelichtet“ wurde.[1]

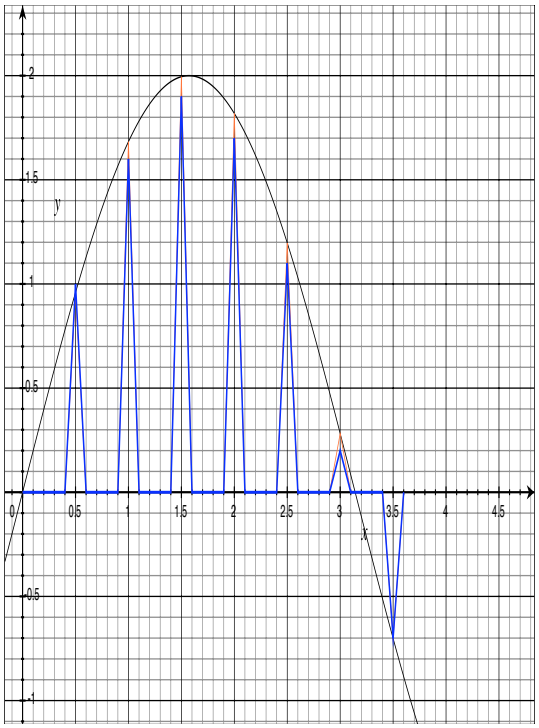
2.1.2.Quantisierung

Quantisieren bedeutet, dass jeder Messwert nun einem fest vorgegebenen Wert zugeordnet wird. Wichtig dabei ist, dass nur ganze Zahlen verwendet werden können. Aus 8,3 wird zum Beispiel 8 und aus 4,5 wird 5. Der daraus resultierende Fehler wird Quantisierungsfehler genannt. Nach der Quantisierung stimmt die Lautstärke des Ausgangssignals nicht mehr genau mit der Lautstärke des Eingangssignals überein (Abb. 2). Außerdem ist beim Ausgangsgeräusch ein störend hartes Rauschen, das sogenannte Quantisierungsrauschen, hörbar. Wird nun die Systemauflösung verfeinert, das heißt, statt den vorgegebenen Werten (1,2,3,...,6,7 also 3 Bit) werden mehr Werte (1,2,3,...,62,63 also 6 Bit) verwendet, wobei man die PAM-Werte noch mit 8 multiplizieren muss (8*8-1=63), verkleinert sich der Rundungsfehler. Diese Veränderung macht den Quantisierungsfehler 8fach kleiner. Also ergibt sich pro Bit eine Verdoppelung des Qualitätsniveaus. Die Werte 3 Bit und 6 Bit werden als Wortlänge bezeichnet. Diese Wortlänge kann nicht beliebig variieren, da dies zu einer

---

[1] Vgl. Häßler, Martin und Straub, Hans Werner: Praxis der Digitaltechnik. Grundlagen und Anwendungen. München 1993, S. 183-185.

Unmenge von Daten führen würde und so das System verlangsamen würde. Das menschliche Ohr bemerkt normalerweise das Quantisierungsrauschen, erst wenn die Wortlänge unter 14 Bit sinkt. Das entspräche 16 383 Stufen, wobei je 8191 Stufen für die positive und negative Halbachse zur Verfügung steht und ein Wert für Null.[2]

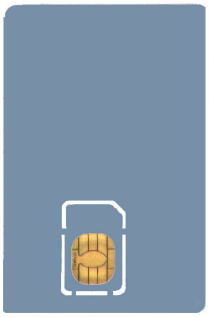


2.1.3.Codierung

Die aus der Quantisierung gewonnenen Werte werden bei der Codierung ins binäre Zahlensystem umgewandelt. Zum Beispiel wird die Amplitude 5 der Funktion mit dem Wert 101 übertragen. Diese Bits werden danach per Funk als Stromimpuls (Burst) an den Empfänger gesendet.[3]

2.2. SIM-Karte

Abb. 4



Der zentrale Teil in einem Handy ist die SIM-Karte (Subscriber Identification/Identity Module), weil in einem GSM-Netzwerk die Telefonnummern des Teilnehmers an seine SIM-Karte gebunden sind. So kann man mehrere Handies mit einer Telefonnummer benutzen, wobei die neueren Handies teilweise schon Sperren eingebaut haben, damit man nur die Karte eines bestimmten Anbieters verwenden kann. Ohne Karte kann man nur die freigeschaltenen Notrufnummern 122, 133, 144 (Österreich) und 112 (International) anrufen. Auf der SIM-Card ist ein Mikrochip eingepflanzt, der für die Sicherheit eine große Rolle spielt, wie später erklärt wird (2.2.1 und 5.2.1.2).

Die Karte selbst besteht normalerweise aus PVC (Polyvinylchlorid) und kann nach der ISO-Normung zwei verschiedene Formate besitzen: Entweder die gesamte Karte mit der Bezeichnung ID-1 (Identifikation) oder das „Plug-In“ Modul mit dem Namen ID-000. Das ID-000 Modul wird nur bei sehr kleinen Handies verwendet, da sie sehr unhandlich sind und das mehrfache austauschen nicht vereinfachen. Die SIM-Karte wird normalerweise zwischen

---

[2] Vgl. Häßler (wie Anm. 1), S. 185-187.

[3] Vgl. Häßler (wie Anm. 1), S. 188.

den Akku und das eigentliche Telefon eingelegt, das Plug-In wird normalerweise in einem kleinen Fach untergebracht.[4]

2.2.1.Speicher

Abb. 5

ROM	EEPROM
lesen	lesen/schreiben
SIM-Servive Tabelle	PIN
PUK	Gebührenzähler
A3/A8	Sprache
Ki	Telefonnummern
IMSI	zuletzt gewählte Nummer
Heim-PLMN	SMS-Texte

Der Speicher der SIM-Karte teilt sich in zwei Bereiche auf: In einen unveränderbaren (ROM, Read Only Memory) und der veränderbaren Speicher (EEPROM, Electrically Erasable Programmable Read-Only Memory). Im unveränderbaren Speicher sind vor allem die statistischen und sicherheitsbezogenen Daten (Abb. 5). Das wären der Code um den PIN zu entsperren (PUK, Pin Unblock Code), eine SIM-Service Tabelle (vom Anbieter erbrachte Dienste) und der Kartentyp, die Verschlüsselungscodes (A3 und A8, Ki (nur auf SIM und HLR bekannter Schlüssel)), die Nummer, um den Teilnehmer zu identifizieren (IMSI, International Mobile Subscriber Identity), die Telefonnummer des Kunden (MSISDN), eine Liste mit Autorisierungen zu Netzzugriff (Access Control Classes), die Identifizierung des Heimnetzes (NCC, MCC und MNC des Heim-PLMN), die Frequenzen des Heimnetzes (Heim-PLMN mit dem Namen ARFCNs). Veränderbar sind dagegen die Zugriffscodes für die SIM-Karte (PIN und PIN2), die letzte gewählte Nummer, Gebührenzähler, Sprache oder auch die gespeicherten Telefonnummern.[5]

2.3. Batterie/Akku

Die Qualität eines Handies hängt sehr oft vom Akku ab. Zum einen sollte der Akku leicht sein, zum anderen sollte er trotzdem eine gute Leistung mit langen Sprech- und Stand-By-Zeiten haben. Zu diesem Zweck werden immer neue Modelle entwickelt. Grundsätzlich werden in einem Akku zwei verschiedene Chemikalien zusammengeführt, die einen Spannungsunterschied produzieren, der dann über die Verbindung von Plus- und Minus-Pol ausgeglichen wird. Beim Ladevorgang werden diese Chemikalien wieder getrennt.

---

[4] Vgl. Störmer, Werner: Elektronische Kartensysteme. Technik und Einsatzmöglichkeiten. Heidelberg 1977 (W&S Praxiswissen), S. 14-16

[5] Vgl. Heine, Gunnar: GSM-Signalisierung verstehen und praktisch anwenden. Grundlagen, Messtechnik, Messbeispiele. Poing 1998 (Funkschau Funktechnik), S. 26-27.

In letzter Zeit sind vier verschiedene Typen von Akkus auf dem Markt erhältlich. Zuerst verwendete man Ni-Cd (Nickel-Cadmium), dann Ni-MH (Nickel Metall Hybrid), nun haben die meisten Handies Li-Ion (Lithium Ionen) Akkus oder den neuesten Li-Polymer (Lithium-Polymer) Akku.

Der Nickel-Cadmium Akku, der in den 60er Jahren entwickelt wurde, verwendet Nickeloxid für die positive Elektrode (Kathode) und Cadmium für die Anode. Sein Vorteil ist, dass er über 500 mal wiederaufladbar ist und auch nach vielen Ladevorgängen eine gute Leistung bringt. Zudem ist er kälteunempfindlich und hält so Temperaturen bis minus 20°C aus. Er verträgt es, wenn er längere Zeit nicht verwendet wird, und er ist unempfindlich gegenüber Überladen und zu starkes Entladen. Sein Nachteil ist, dass er nicht umweltfreundlich ist.

Der Ni-MH Akku verwendet eine Wasserstoff bindende Legierung am Minuspol und Nickel am Pluspol. Er ist umweltverträglicher als der Ni-Cd Akku hat aber etwa dieselbe Entladungs-Spannung wie der Ni-Cd Akku. Diese Akkus kann man auch mit einem Schnellladegerät in etwa 1,5 Stunden aufladen. Sein Nachteil ist, dass er einen so genannten Memory-Effekt hat. Dies bedeutet Folgendes: Wenn der Akku geladen wird, bevor er nicht vollständig entladen wurde, steigt der Punkt, an dem er geladen werden muss, auf die Höhe, an der er vorher geladen wurde. Er „merkt“ sich also, an welcher Stelle er das letzte Mal geladen wurde. Dies führt dazu, dass man diesen Akku vorsichtiger behandeln muss, da sonst die Zeit, in der er verwendet werden kann, immer kürzer wird.

Beim Lithiom-Ionen Akku wird ein Lithiumoxyd als Kathode und Kohlenstoff als Anode verwendet. Beim Lade- und Entladungsvorgang bewegen sich die Lithium-Ionen zwischen den Elektronen. Der Vorteil des Li-Ion Akkus ist seine Energiedichte, durch die er klein und leicht ist und eine hohe Entladungsspannung hat. Hinzu kommt, dass er durch das Gas keine dicke Hülle benötigt und deshalb Aluminium verwendet werden kann. Der wichtigste Vorteil ist aber: Er hat keinen Memory-Effekt.

Die neueste Generation an Akkus sind die Lithium-Polymer-Akkus (Abb. 6). Bei diesem Akku, der erstmals mit dem Ericsson T28 in einem Handy verwendet wurde, ist der Elektrolyt nicht flüssig. Zwar ist die Leitfähigkeit dadurch geringer, wenn aber die Kontaktfläche vergrößert wird, wird dieser Nachteil aufgehoben. Diese Akkus werden aus mehreren ca. 20 μm dicken Schichten zusammengesetzt. Dies hat nun den Vorteil, dass ein solcher Akku in jede beliebige Form geschnitten, also den Freiräumen im Inneren des Handies

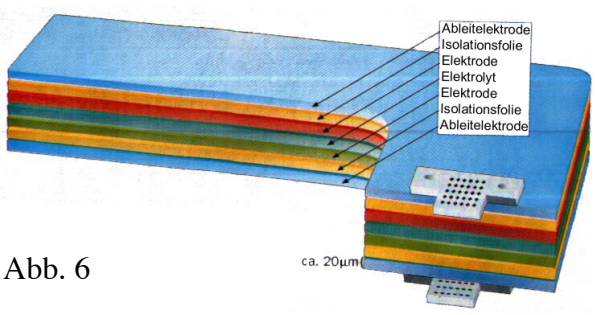


Abb. 6

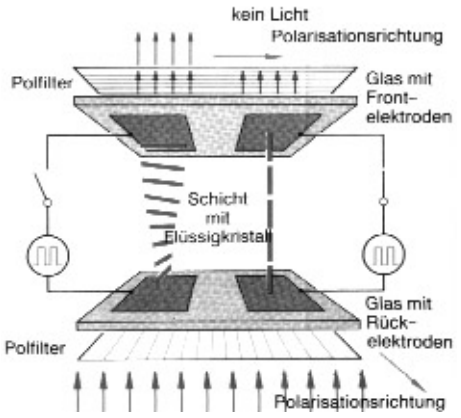
angepasst werden kann. Außerdem sind diese Folien sehr leicht und benötigen keine schweren Metallgehäuse mehr. Ansonsten entsprechen seine Eigenschaften denen des Lithium-Ionen-Akkus.

2.4. Display

Für den Benutzer ist das Display eines der wichtigsten Teile von jedem elektronischen Gerät, so auch vom Handy. Ohne Display wäre die Nutzung eines Handies in der heutigen Form gar nicht mehr möglich. Man müsste sich zum Beispiel den Speicherplatz einer Telefonnummer selber merken, man könnte nicht mehr viele Nummern speichern, das Versenden von SMS (Short Message Service = kurze Textnachricht), oder die Anzeige der Telefonnummer des Anrufenden (CLIP) wäre nicht möglich.

Es gibt drei Arten von Displays: Numerische, alphanumerische und graphische Displays. Die Verwendung von numerischen Displays beschränkt sich vor allem auf Taschenrechner, Heimtelefone und Telefonzellen, da sie nur die Zahlen 0 bis 9 und einige Sonderzeichen darstellen können. Bei Handies wurden zunächst alphanumerische Displays, die Buchstaben, Zahlen und Sonderzeichen darstellen können, verwendet. Die ersten Displays waren vor allem 1-zeilig (lange Zeit noch Ericsson und Alcatel). Heute zielen alle Hersteller auf Vollgrafikdisplays. Deren Vorteil ist, dass die Anzeigen lateinische genauso gut wie arabische oder chinesische Buchstaben oder auch Grafiken darstellen können. Hierzu ist das Display in eine Matrix (Rechteck) von Bildpunkten aufgeteilt, wobei die einzelnen Bildpunkte nicht quadratisch sein müssen, sondern auch dreieckig oder sechseckig sein könnten.

Abb. 7



Die Funktionsweise (Abb. 7) der verwendeten LCDs (Liquid Crystal Display) beruht – im Gegensatz zu Fernseher oder Computer, wo ein Elektronenstrahl auf eine fluoreszierende Platte trifft – auf dem Umstand, dass sich die Moleküle eines verwendeten Flüssigkristalls unter einem elektrischen Feld drehen: Zwischen zwei Glasplatten mit Polarisationsfiltern ist eine hundertstel-mm-dicke Flüssigkristallschicht. Das Licht, das durch diese Fläche fällt, wird durch die Kristalle gedreht (polarisiert), kann dadurch im spannungslosen Zustand die Filter ungehindert passieren. Wird nun eine Spannung an dieser Platte angelegt (je ein Pol an beiden Seiten, an „Höhe“ und „Breite“), drehen sich die Enden der Kristalle um 90° und so wird das Licht nicht

polarisiert und kann so nicht durch die Filter. An der spannungsführenden Stelle (wo sich die positive Achse mit der negativen schneidet) erscheint der Punkt dunkel.

Bei LCDs wird unterschieden zwischen reflektiven (das einfallende Licht wird an der hintersten Schicht reflektiert) transmissiven (statt dem Reflektor ist eine Lichtquelle eingebaut) und transflektiven (verbindet beide Systeme und hat so einen halbdurchlässigen Spiegel) Displays.

Bei den früheren alphanumerischen Displays wurden meist auch verschiedene Symbole (z.B. Batterie und Empfang) direkt auf der Glasplatte „eingebaut“ wodurch die Ansteuerung erleichtert wurde.[6]

3. Aufbau des GSM-Netzwerks

Das GSM-Netzwerk ist ein gutes Beispiel für zelluläre Netze. Der Vorteil von einem zellulären Netzwerk (Abb. 8) ist, dass man die von Natur aus begrenzten Frequenzen (da die Reichweite, Übertragungsqualität, Sendeleistung, etc. von der Frequenz abhängen, sind nicht unendlich viele verwendbar) öfter verwenden kann. Der Trick dabei ist, dass man sehr viele kleinere Netzwerke mit einem geringen Durchmesser (35-300 km) nebeneinander setzt. Da nun um eine solche Zelle eine geringe Anzahl von anderen Zellen ist und da die Sendeleistung stark begrenzt wird, kann man eine Frequenz mehrmals wiederverwenden, wenn man eine Zelle mit einer anderen Frequenz dazwischensetzt. Die Überlappung beträgt normalerweise etwa 10-15%. Dieses System wird auch dadurch bestärkt, dass die Sendeleistungen von Handies sehr gering sind und so die nächste Sendestation (Base Transceiver Station) näher als 5 km sein muss. Ein Problem bei Zellen mit geringem Durchmesser ergibt sich allerdings, wenn sich der Teilnehmer schnell bewegt. Dann durchquert er in kurzer Zeit (innerhalb von einem Telefonat) mehrere Zellen und die Teilnehmerdaten müssen weitergegeben werden (Handover 3.5). Außerdem muss der ungefähre Standort des Teilnehmers auch für das Handover bekannt sein; dies wird als Signalisierung bezeichnet.[7]

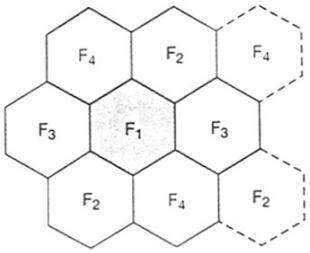


Abb. 8

[6] Vgl. Häßler (wie Anm. 1), S. 232-235.

[7] Vgl. Heine (wie Anm. 5), S. 15-16.

3.1. Bestandteile eines PLMN

Ein PLMN (Public Land Mobile Network) ist ein in sich abgeschlossenes GSM-Netzwerk (Abb. 9). Es kann ein Land oder auch ein Bundesland ein PLMN bilden. Das PLMN besteht aus mehreren MSC-Bereichen, Geräteregistern (EIR, Equipment Identity Register) und aus Teilnehmerregistern (HLR, Home Location Register). Der MSC-Bereich beinhaltet je eine Schaltzentrale für die Anrufe (MSC, Mobile Services Switching Center), ein Besucherregister (VLR, Visitor Location Register), und mehrere BSS-Bereiche. Jeder dieser BSS-Bereiche besteht aus einem BSC (Base Station Controller) und mehreren Sendestationen (BTS, Base Transceiver Station). Die verschiedenen PLMNs sind untereinander wieder über MSCs verbunden.

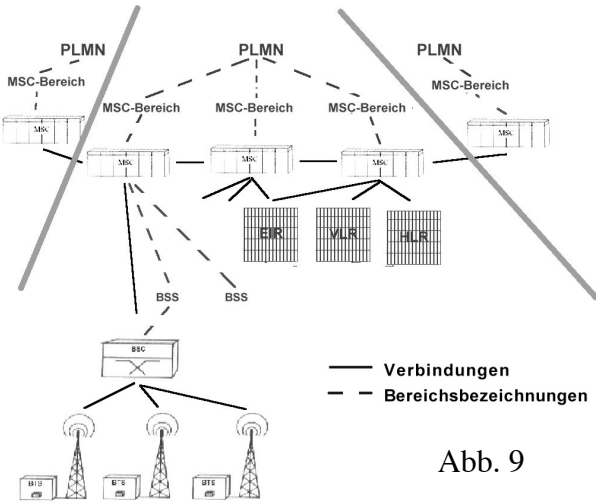


Abb. 9

3.1.1.Base Station Subsystem (BSS)

Die Zentrale der BSS ist der BSC (Abb. 10), er verbindet die einzelnen Sendestationen (BTS) mit dem übergeordneten MSC. Das BSS ist die Schnittstelle zwischen dem Kunden und den Registern. Ein Register kann mehrere BSS-Bereiche versorgen, aber ein BSS-Bereich gehört zu nur einem Register. Der Mobilfunkteilnehmer kommuniziert über sein Handy und über die eingelegte SIM-Karte mit der BTS, diese leitet die Signale weiter an den BSC. Ein BSC kann mehrere BTSs, also mehrere Funkzellen, bedienen.

3.1.1.1.Mobilstation (MS)

Die Mobilstation (Handy), die der Kunde hat, ist mit der BTS über das sogenannt Air-Interface, über Funk, verbunden. Die Sendefrequenzen sind Upstream (zur BTS) und Downstream (zur MS) verschieden. Upstream oder auch Uplink wird normalerweise eine Frequenz von 890,2 – 915 MHz und das Extended Band, das später hinzugefügt wurde, mit 880,4 – 890,0 MHz verwendet. Downlink verwendet man 935,2 – 960 MHz und 925,4 – 935,0 MHz. Bei der 1800er Frequenz ist 1710 – 1785 MHz (Uplink) und 1805 –1880 MHz (Downstream) gebräuchlich. Bei der 1800er Frequenz ist eine Sendeleistung von circa 1 Watt

gebräuchlich, im Gegensatz dazu werden im 900er Netz die Daten mit einer Leistung von 3 bis 4 Watt ausgestrahlt.[8]

3.1.1.2.Base Transceiver Station (BTS)

Die BTS hat nun die Aufgabe, die von der Mobilstation gesendeten Signale weiterzuleiten. Die Größe einer BTS hat sich in den letzten Jahren stark verkleinert, so hat derzeit eine BTS nun nur noch die Größe eines Aktenkoffers.[9]

Die BTS besteht aus Sende- und Empfangsanlagen mit einer Sendeleistung von ca. 10 Watt. Ihre Hauptaufgabe ist es, Kontakt mit der Mobilstation aufzunehmen, die Nutzdaten (Sprache, SMS,...) auszutauschen und die Signalisierung (Empfangsstärke, Lage,...) durchzuführen. Sie verbindet Funk- und Computernetzwerk.

Da die Empfangsqualität beim Handy stark von der BTS abhängt, sind für verschiedene Gelände verschiedene Konfigurationen notwendig. Normalerweise werden mindestens eine, meist aber mehrere BTSs zu einer örtliche Gruppe (LAC, Location Area) zusammengeschlossen. Der Vorteil hierbei ist, dass in dem Zeitpunkt, als die Mobilstation angerufen wird, ein Funkruf (Paging Message) an die BTS der LAC, wo sich die Mobilstation zuletzt aufhielt, gesendet wird. Die BTSs in einer solchen LAC sind untereinander nicht feinsynchronisiert, das heißt, dass die Zeitschlitze (wo die Daten übertragen werden) der einen BTS nicht genau mit denen der anderen übereinstimmen; dadurch ist keine Übergabe an eine andere BTS möglich ohne dass Zeitschlitze (synchronisiertes Handover) gewechselt werden.[10]

Um die Empfangsqualität zu erhöhen und die Belastung des Netzes durch Signalisierung (Positionsangaben, Sendedaten, Verbindungsaufbau) zu senken, kann man die BTSs in verschiedenen Formationen (Konfigurationen) aufstellen. Die Schirmzellenkonfiguration besteht aus einer leistungsstarken BTS, der Schirmzelle, und mehreren leistungsschwächeren BTSs mit kleineren Sendegebieten. Der Grund für diese Konfiguration ist, dass sich vor allem in Großstädten unterschiedlich bewegliche Handybenutzer befinden. Ein Teil dieser bewegt sich mit höherer Geschwindigkeit (im Auto) durch das Sendegebiet mehrerer Zellen, andere wiederum bleiben die ganze Zeit in einer Zelle. Normalerweise würde mit den sich schnell bewegenden Mobilstationen oft ein Handover durchgeführt, dadurch würde die

---

[8] Vgl. Heine (wie Amn. 5), S. 332

[9] Vgl. Heine (wie Anm. 5), S. 31

[10] Vgl. Heine (wie Anm. 5), S. 357.

Empfangsqualität sinken und die Signalisierung steigen, so aber bleibt der schnelle Telefonierer in einer Zelle. Die langsamen Telefonierer können hingegen die Vorteile lokaler Sender auch in Häuserschluchten verwenden.

In Großstädten werden oft auch sektorisierte (collocated) BTSs verwendet. Hierzu werden mehrere BTSs mit einem Sende- und Empfangswinkel von 120° bis 180° an einem Standort aufgebaut. Dadurch muss man nicht auf die Interferenz der Frequenzen achten, da diese Antennen sogenannte Richtantennen sind, also nur Informationen aus dem von ihnen sichtbaren Bereich empfangen. Außerdem kann man solche beisammenstehende BTSs leichter feinsynchronisieren.[11]

Ein zentraler Bestandteil der BTS ist die TRX. TRX bedeutet Transmission/Reception-Unit, also ist sie für die Signalverarbeitung zuständig. Die Signalverarbeitung beinhaltet Channel Coding/Decoding (Verfahren um die Daten nach Störungen bei der Übertragung über das Air-Interface durch Kontroll-Codes zu überprüfen), Ciphering/Deciphering (Ver-/Entschlüsselung) und GMSK-Modulation/Demodulation (von GSM verwendetes Modulationsverfahren).[12]

3.1.1.3.Base Station Controller (BSC)

16 bis 250 Basisstationen werden von einem BSC versorgt. Mit den BTSs kommuniziert der BSC durch das Abis-Interface und mit dem MSC durch das A-Interface. Die Relaisfunktion, also das Verbinden von Abis-Kanälen mit A-Kanälen, übernimmt das Koppelnetz, das in einem BSC eingebaut ist. Wichtig ist, dass, obwohl ein BSC mit nur einem MSC verbunden ist, mehrere A-Interface-Leitungen benötigt werden, da die Nutz- und Signalisierungsdaten von mehreren BTSs und somit von vielen Mobilstationen weitergeleitet werden. Weiters befindet sich in einem BSC eine Datenbank, die die Verfügbarkeit und Qualität aller Funk-Ressourcen und der BSS-Hardware verwaltet. Zusätzlich benötigt der BSC einen schnellen Zentralprozessor, da sie die Entscheidungen zum Intra-BTS-Handover (Funkkanalwechsel) und Intra-BSC-Handover (Wechsel der BTS) ohne das MSC durchführt.[13]

---

[11] Vgl. Heine (wie Anm. 5), S. 33-35 sowie Burgmer, Martin und Andreas Ehritt: D-Netz-Mobilfunktechnik. Würzburg 1995 (Vogel-Fachbuch), S. 156.

[12] Vgl. Heine (wie Anm. 5), S. 31.

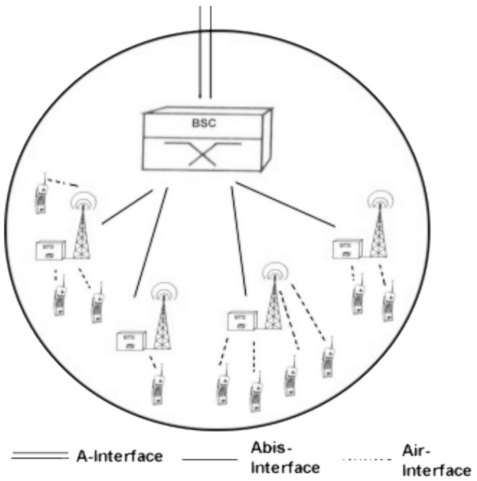
[13] Vgl. Heine (wie Anm. 5), S. 36-37 sowie Burgmer (wie Anm. 11), S. 156.

3.1.1.4.TRAU

Die TRAU (Transcoding Rate and Adaption Unit) ist für die Verpackung/Kompression und Dekompression der Sprachdaten zuständig. Für Datenverbindungen ist sie transparent, das heißt, sie komprimiert sie nicht. Sinnvollerweise wird die TRAU zwischen BSC und MSC eingebaut, da sonst der BSC durch die Datenflut überlastet würde.

Die TRAU hat eine direkte Verbindung mit der BTS durch so genannte TRAU-Frames. Diese sind für den BSC transparente („unsichtbar“) und beinhalten die Eingangs- und Ausgangswerte für die Übertragungskontrolle (Channel Coding) und alle 20 ms übertragen werden.[14]

3.1.2.Network Switching Subsystem (NSS)



Das NSS bildet das Übergangsnetz zwischen dem GSM-Netz und dem öffentlichen Partnernetz, wie dem Telefonnetz (PSTN) oder ISDN. Das NSS besteht (Abb. 11) aus einer Schaltzentrale (MSC) oder aus einer Schaltzentrale mit eingebauter Anbindung zum Festnetz oder zu anderen PLMNs (G-MSC, Gateway-MSC) und mehreren Datenbanken. Verbunden sind diese Computer durch verschiedene Schnittstellen (Interfaces) (Abb. 20). Das NSS hat eine zentrale Funktion im GSM-Netzwerk, denn in ihm sind die benötigten Datenbanken. Zusätzlich führt es Steuerungsfunktionen durch, die für Verbindungsaufbau, Berechtigungsprüfung, Verschlüsselung oder auch Roaming (Telefonieren in fremden Netzen) nötig sind.[15]

3.1.2.1.Mobile (Services) Switching Center (MSC)

Die Mobilvermittlungsstelle (MSC) führt normale Vermittlungsaufgaben aus und verwaltet die Netze. Sie führt die Signalisierung (Abstimmen von Sender und Empfänger; z.B. Sendefrequenz) durch, die für die Verbindungen und ihren Auf- und Abbau und für den

---

[14] Vgl. Heine (wie Anm. 5), S. 38.

[15] Vgl. Walke, Bernhard: Mobilfunknetze und ihre Protokolle. Bd. 1, Grundlagen, GSM, UMTS und andere zellulare Mobilfunknetze. Stuttgart 1998 (Informationstechnik), S. 146 sowie Heine (wie Anm. 5), S. 40.

Zellenwechsel (Handover) benötigt wird. Weiters führt das MSC auch Dienste wie Konferenzschaltung, Rufweiterleitung, Rufsperre und Abrechnung durch. Es ist also – im technischen Sinne gesehen – gleich wie eine ISDN-Vermittlungsstelle.

Ein MSC kann über das A-Interface mit bis zu 16 BSCs kommunizieren. Ein MSC ist sehr teuer, deshalb werden nur wenige verwendet, oft auch nur eine für mehrere Städte. Zusätzlich wird noch versucht, die Verbindungsstrecken zu den dazugehörenden BSCs aus Kostengründen möglichst gering zu halten.[16]

Unter den MSCs gibt es noch Unterschiede. Da ein normales MSC nur für das Mobilfunknetzwerk verantwortlich ist, bedarf es eigener Gateway-MSCs (Zugangs-MSC). Diese G-MSCs sind gleich wie die MSCs, nur dass sie auch für den Verbindungsaufbau nach Außen verantwortlich sind: Sie sind die Schnittstelle zum Festnetz oder dem ISDN-Netzwerk. Wenn zum Beispiel jemand von seinem Handy aus ein Telefon im Festnetz anruft, muss ein MSC ohne Gateway-Funktion die Daten über ein G-MSC umleiten.

Der Standort eines G-MSCs spielt für den Anbieter eine wichtige Rolle, da er die anfallenden Kosten von vom G-MSC zu einem angerufenen Festnetzanschluss zahlen muss. Deshalb sind genaue Analysen des Gesprächsaufkommens nötig, um die Kosten gering zu halten.[17]

3.1.2.2.Home Location Register (HLR)

Jedes PLMN beinhaltet mehrere HLR. Diese verwalten die Teilnehmerdaten (Abb. 12) der im Einzugsbereich des dazugehörigen MSCs wohnenden Kunden.

In diesem Register ist zum Beispiel eine individuelle, bis zu 16 Bit lange Zahl, die nur auf der SIM und im HLR gespeichert ist, der Ki genannt wird. Diese Zahl wird nie bekanntgegeben, da von ihr die Verschlüsselung der über Funk übertragenen Daten (Ciphering) abhängt. Da das HLR leicht überlastet werden könnte, müssen verschiedene Sicherheitsmaßnahmen getroffen werden, damit bei einem Systemabsturz nicht alle Teilnehmerdaten verloren gehen. Weiters wird das HLR vom Besucherregister (VLR) entlastet, das alle temporären Daten von Gästen beinhaltet.[18]

Bei einem Gesprächsaufbau wird zuerst über das HLR versucht, Kontakt mit dem Handy (MS) aufzunehmen. Falls dies nicht klappt, befindet sich ein Eintrag im HLR, in welchem

---

[16] Vgl. Walke (wie Anm. 15), S. 146 sowie Burgmer (wie Anm. 11), S. 156-158.

[17] Vgl. Heine (wie Anm. 5), S. 44.

[18] Vgl. Heine (wie Anm. 5), S. 41.

BSS oder NSS das Handy (MS) ist. Fall sich die MS in einem fremden NSS befindet, werden nun die Teilnehmerdaten an das dazugehörige VLR geschickt.[19]

Zum HLR gehört auch ein Teil, der nur für die Authentisierung der Benutzer zuständig ist und dafür Authentication-Datensätze, die aus den Schlüsseln SRES, RAND und Kc bestehen, berechnet. Dieser Teil ist das AuC, das dann die berechneten Schlüssel (Abb. 13) zum Verschlüsseln der Daten (Ciphering) an das Besucherregister (VRL) sendet.[20]

3.1.2.3.Visitor Location Register (VLR)

Das Besucherregister (VLR) verwaltet vor allem die dynamischen Daten (Abb. 14), also die, die sich schnell ändern. Beispielsweise werden die Daten von Roaming-Teilnehmern von einem VLR ans nächste übergeben. Der Unterscheid zwischen HLR und VLR kommt so zustande: Wenn sich ein Teilnehmer in seinem Heim-HLR-Bereich (Wohnort oder auch Bundesland) befindet, sind seine Daten trotzdem nicht nur im HLR sondern auch im VLR. Das VLR ist durch eine geographische Fläche begrenzt, die kleiner ist als die des HLR. Weiters wird normalerweise je ein VLR einem MSC zugeordnet, aber es kann ein HLR von mehreren MSCs benutzt werden.[21]

3.1.2.4.Equipment Identity Register (EIR)

Das EIR ist nur für den Diebstahlschutz zuständig. Es verhindert, dass ein gestohlenes Handy mit neuer SIM-Karte zu einem legalen Mobiltelefon wird. Durch das EIR ist es möglich, gestohlene bzw. technisch unbrauchbare Telefone zu sperren. Hierzu führt das EIR drei Listen: die weiße Liste, in der alle zugelassenen Mobiltelefone durch den Type Approval Code (TAC) (Code für den Gerätetyp) stehen, die schwarze Liste, die die IMEIs (International Mobile Station Equipment Identity) der zu sperrenden Handies enthält, und die graue Liste, die die IMEIs der zu verfolgenden Mobilstationen (Tracking) enthält.[22]

---

[19] Vgl. Burgmer (wie Anm. 11), S. 158.

[20] Vgl. Heine (wie Anm. 5), S. 41.

[21] Vgl. Heine (wie Anm. 5), S. 42-43

[22] Vgl. Heine (wie Anm. 5), S. 45-46.

3.2. ISO/OSI-Referenzmodell

Wenn Maschinen organisiert und strukturiert kommunizieren müssen, wird normalerweise das OSI-Referenzmodell (Open Systems Interconnection) verwendet. Es ist international standardisiert. Der Grundgedanke dieses Modells ist, dass die Aufgaben auf mehrere Schichten (Layer) aufgeteilt werden, die in ihrer Summe den Kommunikationsprozess bilden.[23]

Jede dieser Schichten bietet der darüber liegenden Schicht seine Dienste an. Sie kommuniziert nur mit den beiden Schichten, die direkt über bzw. unter ihr liegen. Dafür benötigt sie die Hilfe so genannter Protokolle. Die übergeordnete Schicht nennt man Dienstnutzer und die untere Dienstbringer. Das Modell besteht aus sieben Schichten an den Endpunkten und aus dreien an den Verbindungsknoten.

Alle Nachrichten, die von einer Schicht zu einer anderen Schicht gleicher Stufe gesendet werden, werden Peer-to-Peer-Protokolle (Abb. 15) genannt. Diese Peer-to-Peer-Protokolle bestimmen, wie eine Schicht die ankommenden Daten verarbeiten soll. Die grundlegende Aufgabe einer Schicht besteht darin zu ver- oder entpacken, also den Anwenderdaten einen Header hinzuzufügen bzw. zu entfernen (Abb. 16). Ein Vorteil dieses Standards besteht darin, dass die Übertragung der Daten von den physikalischen Leitungen fast unabhängig ist (außer Geschwindigkeit und Art der Leitung z.B. Kupfer- oder Glasfaserkabel).

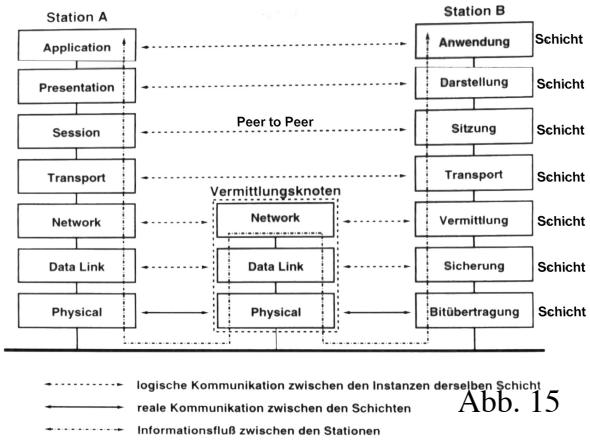
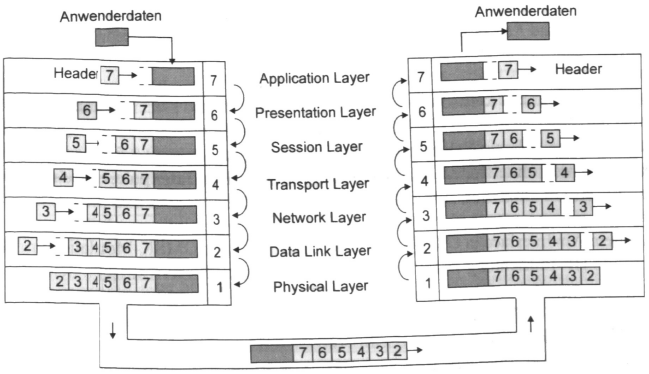


Abb. 15

Abb. 16

Im GSM-Netzwerk gibt es aber auch Daten, die zwischen verschiedenen Endpunkten die Sende- und Zielschicht wechseln. Dies sind vor allem Kontrolldaten, die von den Schichten anders interpretiert, beantwortet und an andere Ziele gesendet werden.[24]



[23] Vgl. Heine (wie Anm. 5), S. 47.

[24] Vgl. Heine (wie Anm 5), S. 49-50.

3.2.1.Application Layer/Layer 7 - Anwendungsschicht

Dies ist die Schnittstelle zum Benutzer oder zur Anwendung und ist deshalb stark vom Anwender abhängig. Ein Beispiel wäre ein Lautsprecher oder Display.

3.2.2.Presentation Layer/Layer 6 - Darstellungsschicht

Diese Schicht wandelt die Anwenderdaten in ein standardisiertes Paketformat um, verschlüsselt und komprimiert diese.

3.2.3.Session Layer/Layer 5 - Sitzungsschicht

Sie regelt den Kommunikation zwischen den Endgeräten und setzt die Datenpakete richtig zusammen.

3.2.4.Transport Layer/Layer 4 - Transportschicht

Die Transportschicht ist für den Transport der Datenpakete von einem Endpunkt zum anderen zuständig. Sie startet und beendet den Datenaustausch und kontrolliert, ob die Daten unbeschadet angekommen sind.

3.2.5.Network Layer/Layer 3 - Vermittlungsschicht

Der Layer 3 lenkt die Daten zum richtigen Ziel und leitet die Daten zur vierten Schicht, wenn sie am richtigen Endpunkt sind. Diese Schicht befindet sich an jedem Netzknoten und sie bewertet, wohin man die Daten weiterschicken muss. Im GSM-Netzwerk ist sie also für die Ruflenkung (Routing) zuständig.

3.2.6.Data Link Layer/Layer 2 - Sicherungsschicht

Hier wird der Datenstrom von Einsen und Nullen richtig gedeutet, zerteilt und als Pakete wieder an die Vermittlungsschicht weitergegeben. Hierzu werden Kontrollsummen in der Form von einem Fingerabdruck (hash-Wert) eingesetzt, die Fehler erkennen und korrigieren sollen. Um Datenblöcke zu erkennen, setzt die Sicherungsschicht vor und nach jeden Datensatz eine Bitfolge (Tag). Falls ein Datenblock fehlerhaft ist, sendet die Sicherungsschicht eine Meldung zurück, damit dieser Block noch einmal gesendet wird.

3.2.7.Physical Layer/Layer 1 - Physikalische Schicht

Dies ist die Schnittstelle zu den Datenleitungen. Sie ist wiederum – wie Schicht 7 – vom Medium abhängig, zum Beispiel ob Funk, Glasfaserkabel oder Infrarot. Diese Schicht kennt keine Datenformate und auch keine Arten, sie transportiert einfach nur eine binäre Zeichenfolge.[25]

3.3. Datenleitungen/Interfaces

Die Daten, die im GSM-Netzwerk verwendet werden, müssen an viele verschiedene Orte gesendet werden. Die Orte sind oft verstreut und durchaus nicht alle zugänglich. Also müssen die Datenleitungen und Schnittstellen zwischen zwei Stationen verschieden sein. So ist zum Beispiel die Luft (Air-Interface) die Verbindung zwischen Handy (MS) und BTS, und die BTS ist wiederum über ein Kabel (Glasfaser oder Kupfer) mit der BSC verbunden. Weiters unterscheiden sich die Daten, die über solche Schnittstellen laufen. Während es beim Air-Interface sowohl Nutzdaten als auch Signalisierungsdaten sind, übertragen die Interfaces B bis H nur noch Teilnehmerdaten, die zur Signalisierung und zur Identifizierung benötigt werden.

3.3.1.Air-Interface

Das Medium des Air-Interfaces ist die Luft und die daraus resultierende Funkverbindung zwischen Handy (MS) und BTS. Da durch die vielen Teilnehmer sehr viel Daten über dieses Interface laufen, darf die Übertragung in diesem Medium nur wenig Ressourcen benötigen. Hierzu gibt es mehrere Möglichkeiten, möglichst vielen Teilnehmern eine Verbindung mit hoher Datenrate anzubieten. Die Möglichkeiten sind: Frequenzmultiplex-Verfahren (FDMA, Frequency Division Multiple Access), Zeitmultiplex-Verfahren (TDMA, Time Division Multiple Access), Codemultiplex-Verfahren (CDMA, Code Division Multiple Access) und Raummultiplex-Verfahren (SDMA, Space Division Multiplex Access). Diese Verfahren kann man auch untereinander kombinieren.[26]

3.3.1.1.FDMA (Frequency Division Multiple Access)

Eine dieser Arten ist das Frequenzmultiplex-Verfahren (FDM-, Frequency Division Multiplexing oder auch FDMA-Verfahren), das in den analogen Funknetzen benutzt wird. Hierzu wird das gesamte zur Verfügung stehende Frequenzspektrum in kleine Frequenzbänder

[25] Vgl. Burgmer (wie Anm. 11), S. 66-68 sowie Heine (wie Anm. 5), S. 50-53.

[26] Vgl. Walke (wie Anm. 15), S. 68.

unterteilt. Zwischen zwei solcher Frequenzbänder ist ein Schutzband (Guard Band) nötig, da die Frequenzfilter nicht flankensteil genug sind und deshalb die eigenen Frequenz zu einem bestimmten Grad wegschneiden und die Fremdfrequenz nicht genug entfernen würden. Ein solches Frequenzband wird dann einer oder mehreren Stationen zugeteilt. Die Folge ist, dass nicht das gesamte Frequenzspektrum genutzt werden kann. Aber auch ohne Schutzbänder kann dieses System alleine für die heutigen Handyzahlen zu wenig Stationen bedienen. In Zukunft wird es aber wieder an Bedeutung gewinnen, da es im GPRS-System (6.5) wieder verwendet wird und den Kunden hohe Übertragungsraten anbietet.[27]

3.3.1.2.TDMA (Time Division Multiple Access)

Das Zeitmultiplex-Verfahren (TDM-, Time Division Multiplexing oder TDMA-Verfahren) ist das Gegenteil zum FDMA-Verfahren: Hier kann jeder Teilnehmer zwar das gesamte Frequenzspektrum benutzen, aber ihm wird nur ein Zeitschlitz (Timeslot) zugewiesen. Diese Zeitschlitze sind untereinander durch kurze Schutzzeiten (Guard Time) getrennt. Die Zeitschlitze verhindern, dass ein Netz beliebig viele Teilnehmer aufnehmen kann. Außerdem müssen sowohl Sender als auch Empfänger genau aufeinander abgestimmt sein, da sonst der Empfänger ein falsches Signal verwendet. Bei diesem Verfahren muss deshalb eine gute Signalisierung neben der Sprachverbindung erfolgen.[28]

Da nun beide Systeme eine zu geringe Anzahl an Teilnehmern verbinden kann, wird im GSM-Netz die Kombination (Abb. 17) von TDMA und FDMA verwendet. Hierzu wird das gesamte zur Verfügung stehende Frequenzspektrum in einzelne Frequenzbänder unterteilt. Diese Frequenzbänder werden noch in Zeitschlitze aufgespaltet. Beim GSM-Standard besteht dadurch ein Frequenzband aus 8 Zeitschlitzen, die sich immer periodisch wiederholen. Diese Zeitschlitze sind noch durch Schutzzeiten (Guard Time) und Schutzbänder (Guard Band) unterteilt. Trotzdem bietet dieses Verfahren schlussendlich vielen Kunden relativ gute Übertragungsraten. Diese sind zwar geringer als beim TDMA- oder FDMA- Verfahren, aber mit der Filterung des Eingangssignal noch für ein Gespräch ausreichend. So wird die Datenmenge reduziert, weiters werden die Sprachdaten digitalisiert, komprimiert und verschlüsselt. Dies findet im Analog/Digital-Konverter (2.1) und im Chip der SIM-Karte (2.2) statt und wird Ciphering (5.3) genannt. Ein Vorteil dieses Verfahrens, der im GSM-Netz

---

[27] Vgl. Walke (wie Anm. 15), S. 69.

[28] Vgl. Walke (wie Anm. 15), S. 70.

verwendet wird, ist das Springen zwischen Frequenzen und Zeitschlitzen (Frequency Hopping). Dabei wird die Frequenz immer wieder gewechselt. Falls nur wenige Teilnehmer telefonieren, wird nicht nur jeder achte Zeitschlitz verwendet, sondern möglicherweise jeder zweite über mehrere Frequenzen verteilt. So steigen mit der sinkenden Teilnehmerzahl die Übertragungsraten und die Gesprächsqualität. Im Gegenzug jedoch kann ein Netz nicht mehr als eine bestimmte Teilnehmerzahl, genau sieben pro Frequenzband (plus 1 Signalisierungskanal: Slot 0), in einem Augenblick bedienen. Auch bei diesem Verfahren müssen Sender und Empfänger auch genau aufeinander abgestimmt sein, damit die Daten richtig übertragen werden. Daraus folgt sehr viel Kommunikation zwischen dem Handy (MS) und BTS (Signalisierung).

3.3.1.3.Interleaving

Da die Übertragung über das Air-Interface sehr fehleranfällig ist, wurde noch ein Schutzmechanismus eingebaut, welcher Interleaving genannt wird. Außerdem treten Fehler bei der Datenübertragung vor allem bei einer Reihe von hintereinander liegenden Bits auf, da die Übertragung eines einzelnen Bits nur sehr kurz dauert. Deshalb versucht man die Gruppenfehler gering zu halten und auf einzelne Bitfehler aufzuteilen, da diese leichter erkannt und korrigiert werden können. Durch diesen Vorgang kommt es zu längeren Signallaufzeiten, da die Bits erst später gesendet werden. Also wird das Interleaving vor allem bei der Signalisierung verwendet, da dort Fehler sich auch schlimmer auswirken, als auf dem Sprachkanal.

Beim Vorgang des Dazwischenschaltens (Interleavings) (Abb. 18) werden die 456 Bits der Datenblöcke in acht 57 Bit lange Unterblöcke aufgeteilt. Diese Unterblöcke werden dann nach einer bestimmten Reihenfolge an einander gereiht (siehe Abbildung). Nach dem Durchmischen werden jeweils zwei Unterblöcke zusammengenommen; dabei wird das erste Bit des zweiten Unterblocks vor das erste Bit des ersten Unterblocks eingefügt. So kommt dann zuerst Bit 1 (U-Block 2), dann Bit 1 (U-Block 1), dann Bit 2 (U-Block 2), und so weiter. Diese zwei zusammengefügten Unterblocks ergeben einen Burst (3.3.1.4), der in seiner Mitte eine Stealing Flag hat. Diese zeigt an, welcher Burst gerade übertragen wird.

Durch diese Verschiebung kann es zu einer verlängerten Signallaufzeit von bis zu 37,5 ms bei einem Fullrate-Sprachkanal und 106,8 ms bei einem Fullrate-Datenkanal kommen. Dies wird beim Sprachkanal als störender empfunden als beim Datenkanal.[29]

---

[29] Vgl. Heine (wie Anm. 5), S. 349-350.

3.3.1.4.Burst

Diese oben genannten digitalen Zeichenfolgen werden beim Senden in Impulsen (Bursts) über das Air-Interface übertragen (Abb. 19). In jedem Zeitschlitz wird genau ein Burst übertragen. Ein Burst hat die Länge von 577 μs, was genau 156,25 Bits entsprechen würde. Zwischen den Zeitschlitzen ist eine Schutzzeit, weil sich das Handy (MS) nicht immer direkt neben der BTS aufhalten muss und sich die Zeitschlitze deshalb durch die Laufzeit verschieben. Diese Schutzzeiten sind am Anfang und werden Flanken-Bits (Tail-Bits) genannt, die in der Form von Nullen eingefügt werden. Zwischen diesen Tail-Bits sind 148 Bits (542,8 μs), die bei den verschiedenen Arten der Bursts unterschiedlich sind. Die Nettoübertragungsrate aber, ohne Tail-Bits und andere Markierungen (Tags und Header), beträgt ca. 114 Bits (= 2 mal 57 Bit). Nach diesen 577 μs kommt die Guard Period. Aus dieser Übertragungsrate ergibt sich die Definition des GSM-Standards, der besagt, dass jedes Bit mit der Länge von 3,6928 μs übertragen wird. Jedes dieser Bit wird mit einer Sendeleistung von 70 dB über der „Ruheleistung“ übertragen. Also muss der Sender in 34,2 μs innerhalb seiner Toleranz zu seiner Sendeleistung hochfahren.[30]

Es gibt fünf verschiedene Arten von Bursts: Der „Normal Burst“, der im Normalfall verwendet wird, enthält ca. 114 Bit Nutzdaten (mit. Kontrollsummen oder Check Bits) die von einer Training Sequence in zwei je 57 Bit lange Teile geteilt wird und zwei Stealing Flags, die die Art der Daten bestimmen und die Nummer des Bursts angeben. Dann gibt es den „Synchronisation Burst“, der für die Bestimmung der verwendeten Funkzelle (Serving Cell) verwendet wird, und den „Access Burst“, in dem das Handy eine Kanalzuweisung von der BTS verlangt, was beim Gesprächsaufbau und bei der Übergabe des Handies (MS) zu einer anderen nicht gleichgetakteten (Zeitschlitze) Zelle (Non-Synchronized Handover) passiert. Da das Handy die Entfernung zur BTS nicht kennt, wird sie als Null angesehen und dafür wird ein Signal mit der Länge von 88 Bits und so einer sehr langer Guard Period gesendet. Erst nachdem die Entfernung zur BTS bekannt ist, kann das Handy einen „Normal Burst“ senden, der genau ins Empfangsfenster passt. Neben diesen Arten gibt es noch den „Frequency Correction Burst“, der aus lauter Nullen besteht und durch die Eigenheit des Modulationsverfahrens die genaue Bestimmung der Signalisierungsfrequenz (BCCH-Frequenz) ermöglicht, und den „Dummy Burst“, der in den Timeslot 0

[30] Vgl. Heine (wie Anm. 5), S. 96, 316.

(Signalisierungs-Slot) gesetzt wird, falls er leer wäre, und der eine beliebige festgesetzte Bitfolge enthält.[31]

3.3.2.Abis-Interface

Das Abis-Interface ist die Schnittstelle zwischen der BTS und dem BSC. Diese Schnittstelle hat 32 Kanäle mit einer Übertragungsrate von 64 KBit/s, was gesamt 2,048 Mbit/s ergibt. Im GSM-Standard wurde vorgesehen, dass eine BTS höchstens 16 TRXs (3.1.1.2, verarbeitet die Datenpakete bezüglich Verschlüsselung) haben kann, dies ist aber nicht sehr sinnvoll, da ein Abis-Interface höchstens 10 TRXs samt Signalisierung bedienen kann. Wenn jetzt die Zahl der TRXs pro BTS herabgesenkt wird, werden Kanäle frei, die für andere BTSs verwendet werden können. Der Vorteil hierbei ist, dass dann diese BTSs zusammengeschlossen werden können und dadurch ein viel größeres Gebiet mit weniger störenden Interferenzen abdecken und weniger Ressourcen bezüglich Kabel verbrauchen, da mehrere BTSs mit einem Kabel verbunden werden. Die BTSs können auf verschiedene Arten zusammengeschaltet werden. Eine Möglichkeit ist sternförmig, was aber die oben genannten Vorteile nicht nutzt. Ansonsten gibt es noch die Kettenschaltung, die wiederum den Nachteil hat, dass falls eine Leitung oder eine BTS ausfällt, gleich mehrere BTSs ausfallen. Aus diesen Gründen wird vorwiegend die Ringschaltung verwendet, bei der es an mehreren Orten zu Ausfällen kommen müsste, um größere Teile lahm zu legen.[32]

3.3.3.A-Interface

Das A-Interface besteht meist aus mehreren 2 Mbit/s-Verbindungen zwischen dem BSC und dem MSC. Auch hier gibt es mehrere Möglichkeiten, die BSCs und MSCs aufzubauen. Man kann das MSC direkt zum BSC stellen, was co-located BSC genannt wird. Dabei muss berücksichtigt werden, dass das MSC selber weiter vernetzt werden muss. Es besteht auch die Möglichkeit mehrere BSC mit einem MSC zu verbinden. Oft wird auch noch eine TRAU zwischen das MSC und den BSC gesetzt, da sie die Daten komprimiert und so der BSC weniger Leitungen benötigt.[33]

---

[31] Vgl. Heine (wie Anm. 5), S. 317-320

[32] Vgl. Heine (wie Anm. 5), S. 59-62.

[33] Vgl. Heine (wie Anm. 5), S. 169.

3.3.4.B-Interface

Zu Beginn war das VLR ein vom MSC unabhängiger Teil, weshalb nach der Implementierung in den GSM-Standard von einander unabhängige Lösungen entwickelt wurden. Aus diesem Grund ist das B-Interface seit der 2. Phase von GSM nicht standardisiert.[34]

3.3.5.C-Interface

Das C-Interface regelt die Verbindung zwischen MSC und HLR.

3.3.6.D-Interface

Das HLR ist über das D-Interface mit dem VLR verbunden, das Daten wie beispielsweise den temporären Aufenthaltsort von der einen in die andere Datenbank überträgt.

3.3.7.E-Interface

Als E-Interface wird die Verbindung zwischen den MSCs bezeichnet. Hier stellt sich dieselbe Frage, wie die verschiedenen MSCs aufgestellt werden sollten, sternförmig oder maschenförmig.

3.3.8.F-Interface

Die Schnittstelle zwischen MSC und EIR heißt F-Interface, sie überträgt die Hardware-Daten.

3.3.9.G-Interface

Die VLR sind untereinander über das G-Interface verbunden.

3.3.10.H-Interface

Obwohl HLR und AuC normalerweise an ein und demselben Ort sind, wird ihre Verbindung auch H-Interface genannt. Sie ist nicht standardisiert.[35]

---

[34] Vgl. Heine (wie Anm. 5), S. 42.

[35] Vgl. Heine (wie Anm. 5), S. 40.

3.4. Location Update

Als Location Update wird, wie der Name sagt, der Vorgang der neuen Berechnung des Standortes bezeichnet. Dies kommt immer dann vor, wenn das Handy neu eingeschaltet wird oder wenn das Handy die aktuelle Gruppe von BTSs (LA, Location Area) wechselt. Eine Location Area ist definitionsgemäß eine Gruppe von BTSs und sie schließt mehrere Serving Cells (bedienende Zellen) ein. Jede dieser Location Areas hat einen eigenen Code, den LAC (Location Area Code). Wichtig wird nun das Location Update, wenn das Handy (MS) sich bewegt; denn einerseits muss der BSC wissen, welche BTS er verwenden muss, und andererseits ist die Entfernung wichtig, da ja Handy und BTS auf wenige μs synchronisiert sein müssen. Da sich das Handy bewegen kann und sich die Funkwellen nicht unendlich schnell ausbreiten, stimmt der Burst möglicherweise nicht mehr in den Zeitschlitz. Also muss die Zeit, die das Handy „nacheilen“ (oder die BTS „voreilen“) (TA, Timing Advance) muss, berechnet werden. Nach dieser Berücksichtigung stimmen Burst und Time Slot wieder überein. Problematisch wird das Location Update dann, wenn sich das Handy mit sehr hoher Geschwindigkeit (höher als 120 km/h) bewegt und eine Verbindung mit einem anderen Telefon besteht. Dann kann es der Fall sein, dass Burst und Time Slot nicht übereinstimmen. (Abb. 21)

3.5. Handover

Eine wichtige Funktion des GSM-Netzwerks ist das Handover. Unter diesem Begriff versteht man die Übernahme einer MS in eine andere Funkzelle durch eine andere BTS. Dies ist der große Vorteil gegenüber anderen Systemen: Der Mobilfunkteilnehmer kann sich bewegen. Beispielsweise im A-Netz (4.1) gab es keine dynamische Teilnehmerdatenbanken und keine Handover. Durch das Handover entsteht zwar mehr Signalisierungsbelastung, es bringt aber einiges an Komfort.

Es gibt vier verschiedene Arten von Handover: Unter dem Intra-Cell-Handover versteht man den Wechsel von Frequenz oder Zeitschlitz innerhalb derselben Funkzelle. Das Inter-Cell/Intra-BSC-Handover ist die Übergabe des Handies von einer Sendestation (BTS) zu einer anderen innerhalb demselben BSC. Ein Inter-BSC oder Intra-MSC-Handover ist ein Handover zwischen zwei Einzugsbereichen eines MSCs, also von einem BSS in das andere. Und zuletzt gibt es das Inter-MSC-Handover, wo die Verbindung zwischen zwei NSS-Bereichen wechselt.

Ein Handover findet immer dann statt, wenn der Empfang zu schlecht wird, was vor allem am Rand einer Funkzelle vorkommt. Deshalb überlappt sich das Sendegebiet zweier verschiedener Zellen um etwa 10%. Im Falle eines Intra-Cell-Handover und eines Intra-BSC-Handover kann der BSC das Handover selbst durchführen, sonst macht dies das MSC.[36]

3.6. Arten der Datenpakete

Grundsätzlich gibt es zwei Arten von Daten, die übertragen werden. Erstens die „Nutzdaten“, also die Daten, die ein Teilnehmer einem anderen sendet, und die entweder Sprache oder Text sein können. Die Sprache wird, wie vorher beschrieben, verschlüsselt, verpackt und in den Zeitschlitzen versendet. Für Textdaten, die nicht so dringend übertragen werden müssen (z.B. SMS- und WML-Dokumente (Wireless Markup Language, siehe 6.2 WAP)) wird der Signalisierungskanal (Zeitschlitz 0, der erste der gesamten acht Zeitschlitze) verwendet. Zweitens benötigt das Netz durch die Größe und durch die vielen verschiedenen möglichen Tätigkeiten (Bewegung, Ein- u. Ausschalten,...) viel Kommunikation und Abstimmung zwischen den Stationen (Signalisierung). Dies fängt beim Einschalten des Mobiltelefons an, geht über den Gesprächsauf- und -abbau bis zum Abschalten des Handies. Außerdem hängt an allen Nutzdaten ein Teil, der nicht genutzt werden kann, da er die „Adresse“ enthält. (3.2 OSI/ISO-Referenzmodell).

Als Beispiel für ein Signalisierungs-Burst ist hier nun ein RR-Frame (Receive Ready) im Air-Interface, das den Empfang eines I-Frames (Information-Frame), das immer ein Kommando für den Empfänger ist, bestätigen muss. Nach der Markierung (Flag), die 8 Bit lang ist (Abb. 22), kommt ein 8 Bit langes Adressfeld, das mit einer 1 (E/A Bit) beginnt, danach kommt ein C/R (Command/Resopnse) Bit, das sagt ob diese Daten ein Kommando oder eine Antwort sind, dann kommt eine 3 Bit langer Wert, der sagt ob dies ein Burst für die Einstellung von Sendeleistung u.ä. oder für einen Netzservice (SMS,...) ist, als nächstes kommt der 2 Bit lange LPD (Link Protocol Discriminator), der beim Cell Broadcast (Zelleninfos) den Wert 01, sonst aber den Wert 00 hat, und abschließend eine 0. Danach kommt das 8 Bit lange Kontrollfeld, das beim RR erst 1000_{bin}, danach ein Feld mit 0 oder 1 für eine nicht erwartete oder erwartete Antwort und dann ein Feld für die Nummer der Empfangenen Botschaft (N(R)) enthält. Danach kommt ein 8 Bit langes Feld, das angibt, wie viele Rahmen (Befehle) noch kommen werden, dieses enthält zuerst eine 1, dann eine 0 oder 1

[36] Vgl. Burgmer (wie Anm. 11), S. 230.

falls keine bzw. noch mehr Rahmen kommen und noch sechs Bits. Abschließend werden noch Fülloktette mit einem bestimmten Muster, das Uplink und Downlink verschieden sind, gesendet.[37]

3.7. Beispiele zur Signalisierung

Dies ist nur ein grober Überblick und beinhaltet die wichtigsten Meldungen ohne den Parametern, die sie enthalten. Dadurch soll er veranschaulichen, wie viele verschiedene Meldungen für das problemlose Funktionieren des GSM-Netzes benötigt werden:

Location Update: Sobald das Handy eingeschaltet wird, sendet es eine Meldung (CHANnel_REQuest) an die BTS (Abb. 23), also fordert diese auf, ihr einen Kontrollkanal zuzuweisen. Die BTS kann aus dieser Meldung die Entfernung (Timing Advance (3.4)) zwischen MS und BTS berechnen. Die Meldung wird im Abis-Interface auch von der BTS an den BSC weitergesendet (CHANnel_ReQuireD). Der BSC antwortet (CHANnnel_ACTivation), daraufhin wird die Antwort bestätigt (CHANnel_ACTivation_ACKnowledge) und eine Kanalnummer bereitstellt. Der BSC sendet nun der MS eine Meldung (IMMediate ASSign CoMmanD), die der MS einen Signalisierungskanal (SDCCH genannt) zuteilt. Nun kann die MS eine Bestimmung des Standorts (Location Update) durch eine Mitteilung (LOCation_UPDate_REQuest) verlangen. Diese Meldung wird von der BTS zurück- und weiter über den BSC zum MSC geschickt. Das MSC antwortet der MS mit einer Meldung (AUTHentication_REQuest). Nach deren Empfang sendet die MS eine Antwort (AUTHentication_ReSPonse) mit dem Authentisierungsergebnis SRES (Ergebnis einer Berechnung durch mehrere Schlüssel zur Authentifizierung) zurück an das MSC und VLR. Das VLR vergleicht diesen Wert mit dem des HLR. Falls der Wert falsch wäre, würde das MSC eine Meldung (AUTHentication_REJect) zurückschicken, um zu zeigen, dass die Authentifizierung fehlgeschlagen ist. Dann wird die Verschlüsselung durch Meldungen (CIPHering_MODe_CoMmanD und CIPHering_MODe_COMplete) eingeschaltet und der Schlüssel A5 versendet. Danach findet die Authentifizierung des Gerätes über die IMEI (Gerätenummer) auf dieselbe Weise, wie die der IMSI (Teilnehmernummer), statt. Danach wird über eine Meldung (LOCation_UPDate_ACCept) das Location Update bestätigt und die unnötigen Verbindungen werden abgebaut.38

---

[37] Vgl. Heine (wie Anm. 5), S. 106-108.

[38] Vgl. Heine (wie Anm. 5), S. 221-225.

4. Geschichte des Mobilfunks

Die Telekommunikation begann eigentlich zu dem Zeitpunkt, als im Jahre 1843 vom amerikanischen Kongress eine Versuchsstrecke für Morsetelegraphie entlang der Eisenbahn von Washington nach Baltimore bewilligt wurde. Die Übertragung von Sprachdaten war jedoch erst ab 1876 möglich, nachdem Graham Bell das Telefon erfunden hatte.

In Berlin wurde 1881 ein öffentliches Telefonnetz mit direkter Verbindung durch (meist weibliche) Vermittlungsbeamten ermöglicht. Dieses und andere Netze wurden im Laufe der Zeit erweitert und mit automatischen Vermittlungsstationen (Relais) versehen.

Durch Heinrich Hertz wurde 1888 die Theorie von Maxwell bewiesen, dass elektromagnetische Wellen, die von einem Sender ausgesandt werden, bei einem Empfänger eine Spannung induzieren.

Marconi entwickelte dann 1897 ein System, das drahtlose telegraphische Übertragung ermöglichte. Dabei benutzte er die Morsetaste, um eine Spannung im Sender zu erzeugen, deren elektromagnetische Welle beim Empfänger eine Spannungsschwankung hervorrief. Nach diesem Erfolg schaffte er 1901 die schnurlose Übertragung über den Atlantik, wobei die Sende- und Empfangsanlagen noch stationär waren.

Als nächsten Schritt baute die Firma Telefunken 1902 ein Funkgerät für militärische Zwecke. Dieses war auf zwei Karren montiert: Einer war für die Stromversorgung und einer für die Übertragung. Dazu kamen noch riesige Antennen für die verwendete Kurzwellenfrequenz.

Schon bald darauf wurden Schiffe mit solchen Funkanlagen ausgestattet. Nun war die geregelte Abgabe von Frequenzen von Nöten. Also wurden bestimmte Frequenzbänder verschiedenen Diensten freigegeben, um die Interferenzen möglichst gering zu halten. Später wurden die Frequenzen über 3 MHz als kommerziell nicht verwertbar angesehen und dem Amateurfunk freigegeben. Diese Entscheidung wurde aber mehrmals revidiert, und so stieg die Reservierung der Frequenzen für die kommerzielle Nutzung von 30 MHz 1927 über 200 MHz 1938 und 10,5 GHz 1947 auf schlussendlich 275 GHz 1979.

Nach 1945 gab es erste Empfangsgeräte für private Kunden, wie beispielsweise ein Taxi, dessen Kofferraum aber komplett ausgefüllt war. Ab 1952 war es in Deutschland möglich, von einem solchen Gerät das Festnetz anzurufen. Es wurden auch immer öfter lokale Funksysteme (CB, Citizen Band) verwendet (eine BTS für ein Gebiet von 20 – 100 km, 20 Teilnehmer pro Sprachkanal). Diese Funksysteme blieben aber auf je eine Stadt beschränkt,

da es keine Roamingabkommen gab, und so konnte man sein Gerät nur in einer Stadt verwenden.[39]

4.1. A-, B-, C-Netze

1958 ermöglichten es landesweite Mobilfunksysteme einem Handy (MS), mit jeder beliebigen BTS über freie Frequenzen zu kommunizieren. Langsam entstanden erste Netzwerke, die mit dem Festnetz verbunden waren. So entstand schlussendlich das erste PLMN, das A-Netz in Deutschland.

1972 wurde in Deutschland, Österreich, den Niederlanden und in Luxemburg das B-Netz eingeführt. Es ermöglichte Roaming innerhalb dieser vier Länder und eine automatische Vermittlung der Funkrufe. Bei einem Anruf aus dem Festnetz musste der Anrufer die Nummer der BTS kennen, in der sich der Anzurufende aufhielt, und diese vor die Nummer des Übertragungsknotens und der Teilnehmeridentifikation vorwählen. Das Handy wurde auf einer systemweiten Frequenz ausgerufen und erhielt einen Kanal zur Verfügung. Es fand damals, weder zwischen verschiedenen Kanälen noch zwischen zwei BTSs ein Handover statt; dort wurde einfach die Verbindung unterbrochen.

Ab1989 kam zum bestehenden B-Netz noch das C-Netz, das nun schon dynamische Datenbanken und Handover unterstützte. 1996 hatte dieses Netz, das vor allem noch Autotelefone enthielt, ca. 600 000 Kunden. Auch in diesem Netz wurden die Daten weder verschlüsselt noch digitalisiert. Also konnte man Gespräche über dieses Netzwerk einfach mit einem modifizierten Handy, einem Funkgerät oder einem Empfangsgerät (Scanner) mithören. In Österreich wird dieses Netz – im Gegensatz zu Deutschland – D-Netz genannt und es funkt mit einer Frequenz von etwa 450 MHz. In Deutschland hingegen wird das GSM-Netzwerk mit der Frequenz von 900 MHz D-Netz und das 1800er-Netz E-Netz genannt.

Mit der Einführung des D1-Netzes durch T-Mobil, der Tochter der Deutschen Telekom, begann schlussendlich 1992 die Verwendung des GSM-Standards.[40]

4.2. GSM

1982 wurde von der Conference of European Posts and Telegraphs (CEPT) eine Studiengruppe mit dem Namen Groupe Spécial Mobile (GSM) gebildet, die einen

---

[39] Vgl. Walke (wie Anm. 15), S. 23-27.

[40] Vgl. Walke (wie Anm. 15), S. 27-28.

europaweiten Standard für Mobilkommunikation entwickeln sollte. 1989 wurde die Verantwortung für dieses Projekt dem European Telecommunication Standards Institute (ETSI) übertragen und 1990 wurde die Phase I der GSM Specificationen veröffentlicht. Ab 1991 wurde GSM kommerziell genutzt und 1993 gab es schon 36 GSM-Netze in 22 Ländern. Danach wurde GSM in Global System for Mobile Telecommunications umbenannt.

In Deutschland nahmen D2 und D1 am 30. Juni 1992 ihr Netz in Betrieb. Die damals verwendeten Handies (z.B. Ericsson GH 172 oder Motorola International 3200 (Abb. 24)) wogen damals noch von 402 bis 581 g und funkten mit 8 Watt Sendeleistung. Zudem blieb das Motorola International 3200 lediglich 16 Stunden Stand-by (Abb. 25). 1994 entstand im Großraum Berlin das E-Plus Netz, das damals das NOKIA PT 11, benötigte. Ab 1994 war es schon möglich, Faxe per Handy zu versenden, und ab 1995 auch SMSs, deren heutige Popularität man anfänglich nicht erwartete.[41]

5. Sicherheitsstandards

Das Handy ist mittlerweile zu meist gestohlenen Gegenstand geworden. Dieses Problem wurde schon früh bemerkt, deshalb wurde bald der Versuch unternommen, die Zahl der geklauten Handies zu reduzieren. Die Hersteller versuchten dies durch den Einbau von Sicherheitsvorkehrungen, wie einer PIN-Abfrage, einem Sicherheitscode (beim Wechsel der SIM-Karte) und einer Rufnummernbeschränkung.

Doch Sicherheit beinhaltet nicht nur den Diebstahlschutz, auch die Sicherheit des Anwenders gehört dazu. Zum einen hat wohl jeder schon gehört, dass die vom Handy ausgestrahlten Wellen gesundheitsschädlich seien. Man ist sich aber immer noch nicht im klaren, ob dies wirklich stimmt. Zum einen wurde herausgefunden, dass die Messreihe einer amerikanischen Universität, die von Mobilfunkgegnern gerne hergezogen wurde, gefälscht war. Zum anderen haben sogar die Sendeanlagen von Radiosendern eine um vieles höhere Sendeleistung. Die mögliche Erwärmung des Auges ist möglicherweise sogar geringer, als wenn man von Draußen in ein Zimmer geht. Es gibt aber keine einen guten Beweise sowohl für als auch gegen die gesundheitliche Gefährdung der Umwelt durch Handies.

Weiters gehört zum Bereich Sicherheit auch die Gefährdung anderer durch den Gebrauch von Handies. Besonders in Flugzeugen oder Spitälern ist es verboten Handies zu benutzen, da die

---

[41] Vgl. Eckstein, Pia und Arnulf Schäfer: Happy Birthday. 10 Jahre Handy In: Connect. Europas größtes Magazin zur Telekommunikation. 1/2000,S. 34-39.

elektromagnetischen Wellen empfindliche Geräte stören oder eine Explosion (an Tankstellen) auslösen könnten.

Doch in diesem Kapitel werde ich mich vor allem dem Bereich Diebstahlschutz, anonyme Gesprächsübertragung und Authentisierung widmen.

5.1. Basic Service Codes

Basic Service Codes sind Tastenfolgen, die normalerweise bei jeden Handy gleich vorhanden sind und mit denen man grundlegende Einstellungen ohne Menü ändern kann. Diese Codes stammen noch von früher, als nur kleine Displays vorhanden waren mit denen man das Handy programmieren musste. Grundsätzlich gibt es zwei Arten von Basic Service Codes: Codes, die bei allen Handies gleich sind (z.B. für die IMEI *#06# oder Kapitel 5.1.3 – 5.1.5) und solche, die nur bei einem Hersteller (z.B. *#0000# oder *#9999# für Nokia-Handies (Abb. 26) für die Softwareversion) funktionieren.

5.1.1.PIN (Personal Identification Number-Code)

Der PIN ist zwar veränderbar, zählt aber trotzdem zu den Basisdiensten. Normalerweise hat jedes Handy zwei PINs, die beliebig einstellbar sind. Jeder dieser PINs kann je nach Hersteller vier bis neun Ziffern lang sein.

Den ersten PIN (meist nur PIN genannt) sollte das Handy vor unbefugter Verwendung schützen. Zur Kontrolle wird er nach dem Einschalten abgefragt. Deshalb schützt er das Handy auch nur, wenn es ausgeschaltet wird. Also empfiehlt es sich das Handy dort auszuschalten, wo es nicht gebraucht wird oder deponiert werden muss, damit ein Dieb es nicht benutzen kann. Bei manchen Handies ist es möglich, die PIN-Abfrage auszuschalten. Davon ist aber dringend abzuraten, weil dann jeder dieses Gerät benutzen könnte. Zudem sollte man als PIN keine so genannte „Schnapszahl“ verwenden, die leicht zu erraten ist.

Der PIN2 wird dazu verwendet, dass nicht jeder einfach die Einstellungen ändern kann. Die Verwendung kann von Hersteller zu Hersteller variieren.

Die PINs sind aber auch über Direktzugriff änderbar; PIN: **04*[alter PIN]*[neuer PIN]*[neuer PIN]# oder **05*[PUK]*[neuer PIN]*[neuer PIN]#; PIN2: **42*[alter PIN2]*[neuer PIN2]*[neuer PIN2]# oder **52*[PUK2]*[neuer PIN2]*[neuer PIN2]#. Anmerkung: Hier könnte man – ohne dass es der Besitzer merkt – den PIN zumindest zwei Mal ausprobieren, danach muss der richtige PIN ein Mal eingegeben werden (ein Mal Ein-/Ausschalten).

Wenn einer dieser PINs drei Mal hintereinander falsch eingegeben wird, wird er und die SIM gesperrt. Im Notfall könnte man auf diese Weise eine SIM-Karte vor unbefugter Verwendung schützen.

5.1.2.PUK (Personal Unblock Key-Code)

Wenn der PIN einmal gesperrt ist, kann er mit dem Pin Unblock Code entsperrt werden. Diese achtstellige Zahl wird vom Netzbetreiber nur dem Teilnehmer mitgeteilt und kann nicht verändert werden. Wie die PINs sind auch die PUKs, für jeden PIN einer, auf der SIM-Karte gespeichert.

5.1.3.Sicherheitscode

Wie oben gesagt wird ein gestohlenes Handy – sofern kein EIR vorhanden ist – mit einer neuen SIM-Karte legal. Dies sollte der Sicherheitscode verhindern. Dieser Code wird immer dann abgefragt, wenn eine neue SIM-Karte in ein Handy eingebaut wird. Dieser ist bei den neueren Modellen in der Werkseinstellung 12345. Da er manchmal jedoch erst durch Nachfragen bekanntgegeben wird, kann es sein, dass ein Benutzer ihn nicht kennt (oder sogar nichts von ihm weiß) und ihn also nicht ändern kann. Dies führt dazu, dass vielen Handies eine Sicherheitsstufe gegen Diebstahl fehlt.

5.1.4.Anruferidentifizierung

Die Anruferidentifizierung hat eigentlich nur indirekt mit Sicherheit zu tun. Dabei geht es um Anonymität oder Schutz vor störenden Anrufen geht. Die Rufnummer einer SIM wird bei einem Gespräch immer mitgesendet, doch es gibt die Option, die das sichtbare Mitsenden der Rufnummer ein- oder auszuschaltet.

5.1.4.1.CLIP

Die Bezeichnung CLIP (Calling Line Identification Presentation) bedeutet die Anzeige des anrufenden Telefons. Diese Möglichkeit besteht bei Mobiltelefonen und ISDN-/ADSL-Anlagen immer und grundsätzlich auch bei digitalen Telefonanschlüssen nur bei alten analogen Anschlüssen ist dies nicht möglich. In Österreich wird seit Oktober 1999 automatisch die Telefonnummer mitgesendet, früher bestand jedoch die Möglichkeit einer Anmeldung.

5.1.4.2.CLIR

Unter der Kurzform CLIR (Calling Line Identification Restriction) versteht man das Unterdrücken der Anzeige der eigenen Telefonnummer. Dies kann der Anrufer (ausgenommen sind die Notrufnummern) bewirken, indem er einerseits beim Handy das Mitsenden der Telefonnummer über eine Menüfunktion ausschaltet und andererseits bei Festnetzanschlüssen das Mitsenden bei einem Anruf über die Telekom Austria deaktiviert. Daneben besteht auch die Möglichkeit bei jedem Anruf zu entscheiden. Dazu muss man im österreichischen Festnetz *31* vorwählen, bei Mobiltelefonen ist dies unterschiedlich (z.B. #31# bei one oder *31# in Deutschland).

5.1.5.Rufumleitung

Bei jedem Handy besteht die Möglichkeit, verschiedene Anrufe umzuleiten. Dabei muss zwar die umleitende Person die anfallenden Kosten bezahlen, sie kann aber entscheiden, wo sie erreicht wird. Dabei kann man auch unterscheiden: Zum Beispiel kann ein eingehendes Fax umgeleitet werden, ein eingehender Telefonanruf erst nach 20 Sekunden und SMSs kommen alle an. Dies kann entweder im Menü oder mit Codes umgestellt werden: alles Umleiten: **[Code]*[Zielnummer]*10#[senden] zum Einschalten und ##[Code]#*10#[senden] zum Ausschalten; für die Sprache: ein: **[Code]*[Zielnummer]*11#[senden] und aus: ##[Code]#[senden]; für das Fax: ein: **[Code]*[Zielnummer]*13#[senden] und aus: ##[Code]#*13#[senden] und für Daten: ein: **[Code]*[Zielnummer]*25#[senden] und aus: ##[Code]#*25#[senden]. Für den Code gibt es vier Variationen, die bei allen Umleitungen gleich verwendet werden: 21 für sofortige Umleitung; 61 für verzögerte Umleitung; 62 bei Nicht-erreichen und 67 bei „besetzt“.

5.1.6.Rufsperren

Rufsperren (Abb. 27) haben den Sinn, dass sie den Besitzer der SIM-Karte bei unbefugter Benutzung vor zu hohen Kosten schützen sollten.

5.2. Authentisierung

Wichtig für jedes Netzwerk – egal ob reines Computernetzwerk oder nicht – ist zu wissen, wer gerade was macht und auf was Zugriff haben darf. So muss auch im GSM-Netz eine Art Login-Prozess (3.7) durchgeführt werden. Hierbei wird der Benutzer identifiziert. Um nun den Benutzer zu identifizieren, verwenden das AuC und das Handy die selben Werte, diese

werden nach einem bestimmten Schema miteinander verknüpft und schlussendlich miteinander verglichen (Wert der MS und Wert des AuC) .

5.2.1.Anwenderseitig

Anwenderseitig müssen das Handy und die SIM-Karte überprüft und die Verschlüsselungsalgorithmen berechnet werden.

5.2.1.1.IMEI

Die Seriennummer (IMEI, International Mobile Station Equipment Identity), mit dem EIR (3.1.2.4) logisch verbunden ist. Die IMEI sollte dafür sorgen, dass ein gestohlenes Handy bei Benützung verfolgt (Tracking) und letztendlich zurückgebracht werden kann. Dies funktioniert mit der weißen, grauen und schwarzen Liste, auf die die IMEI bei Diebstahl gesetzt werden muss. Der Diebstahl muss gemeldet werden, und zwar mit IMEI. Die Verfolgung eines Handies ist nur möglich, wenn ein Eintrag im EIR vorhanden ist, was nicht immer der Fall ist.

Das Format (Abb. 28) der IMEI (gesamt 60 Bit, 15 Ziffern) beinhaltet den Mobilstationstyp (TAC, Type Approval Code) (24 Bit, 6 Ziffern), die Produktionsstätte (FAC, Final Assembly Code) (8 Bit, 2 Ziffern), eine Seriennummer (24 Bit, 6 Ziffern) und ein Reserve- (Spare) Feld (4 Bit, 1 Ziffer). Beispielsweise steht die 3 als erste Ziffer für ein Mono-Band 900 MHz Handy und 4 für Dualband. Zwei Beispiele: 448903 steht für das NOKIA 3210 oder 493008 für das NOKIA 6150.

An die IMEI kann noch die Software-Versions-Nummer (Abb. 29) (SVN) angehängt werden. Dann wird sie als IMEISV bezeichnet, ist 64 Bit, also 16 Ziffern, lang und statt den letzten Spare Feld ist ein 8 Bit (2 Ziffern) langes SVN-Feld. Die SVN kann u. U. bei Software-Updates verändert werden.

Die IMEI wird bei der Identifizierung des Handies zum Beispiel beim Location Update (3.4 und 3.7) als Antwort auf die IDENT_REQ (Identity Request) Meldung in der IDENT_RSP (Identity Response) an das MSC gesendet. Dieses sendet sie weiter an das EIR, wo sie verglichen wird.[42]

Die IMEI ist eine der wenigen Nummern, die man als Handybesitzer irgendwo auffindbar stehen haben sollte.

---

[42] Vgl. Heine (wie Anm. 5), S. 347-348.

5.2.1.2.SIM-Card

Die wichtigsten Sicherheitsstufen sind bereits auf der SIM-Karte integriert. Einerseits ist das die Teilnehmernummer (IMSI) zur Identifizierung des Teilnehmers und andererseits der Schlüssel Ki und der Algorithmus A3 für die Verschlüsselung der digitalen Gesprächsbits. Mit der Hilfe der SIM-Karte werden die Datenpakete im Handy verschlüsselt.

Auf der SIM-Karte (Abb. 30) ist die Teilnehmernummer (IMSI, International Mobile Subscriber Identity) gespeichert, die sonst nur noch im HLR ist. Über sie läuft die Identifizierung des Teilnehmers und die Abrechnung der Telefonkosten. Die 15 Ziffern, also 60 Bit, lange Nummer setzt sich aus der drei Ziffern langen Landescode (MCC, Mobile Country Code), dem zwei Ziffern langen Netzcode (MNC, Mobile Network Code) (Abb. 31) und der eigentlichen Identifikationsnummer (MSIN, Mobile Station Identification Number) zusammen, die im GSM-Netz im Gegensatz zu anderen Standards nicht gleich der Rufnummer ist.[43]

Um das Tracking (Verfolgung des Standorts des Handy) für Außenstehende zu erschweren, kann einer Mobilstation beim Einschalten eine temporäre Teilnehmernummer (Abb. 30) (TMSI, Temporary Mobile Subscriber Identity) zugewisen werden. Diese Zahl ist 4 Byte, also 8 Hexadezimale Ziffern lang und kann jeden Wert außer $FFFFFFFF_{hex}$ annehmen kann, da $FFFFFFFF_{hex}$ für den Fall, dass die SIM keine gültige IMSI enthält, vorgesehen ist. Die TIMSI wird übertragen, sobald die Verschlüsselung (Ciphering) eingeschaltet ist, und gilt immer nur für eine Verbindung mit dem VLR. Trotzdem sind Geräte in Zigarettenschachtelgröße erhältlich, die es ermöglichen ein Handy zu verfolgen.[44]

Da im GSM-Netz das Public-Key-Verfahren zum Verschlüsseln (zwei verschiedene Schlüssel, einer nur zum Ver-, der andere nur zum Entschlüsseln) verwendet wird, sind sowohl auf dem SIM als auch im HLR mehrere geheime Schlüssel und Algorithmen gespeichert.

Ein solcher ist der Teilnehmerschlüssel Ki, er eine bis zu 16 Byte lange Zahl und ist für die Verschlüsselung wichtig. Er wird nur auf der SIM-Karte und im HLR gespeichert und verlässt diese nie. Die Bezeichnung kommt von Key(Individual)[45]

Der Verschlüsselungsalgorithmus A3 ist ebenfalls im SIM gespeichert und ist geheim.

---

[43] Vgl. Heine (wie Anm. 5), S. 348-349.

[44] Vgl. Heine (wie Anm. 5), S. 387-388.

[45] Vgl. Heine (wie Anm. 5), S. 353-354.

Wie der Algorithmus A3 ist auch der Algorithmus A8 auf der SIM-Karte gespeichert. Er ist 64 Bit lang, wovon die letzten zehn Bits Nullen sind und er ist ebenfalls Geheim.[46]

5.2.2.Netzwerkseitig

Im HLR sind auch diese Zahlen vorhanden, und das AuC berechnet – wie das Handy (MS) – das Ergebnis SRES. Den ersten Schritt zur Identifikation macht aber das Netz, indem es die AUTH_REQ Meldung, die RAND enthält, an die MS sendet.

RAND ist eine beliebig gewählte Zufallszahl. Die Bezeichnung kommt vom englischen „randomise“ (berechnen einer Zufallszahl). Diese Zahl hat eine Länge von 128 Bit, sie kann also einen Wert bis 2^{128}-1 annehmen und variiert von Mal zu Mal.[47]

5.2.2.1.SRES

Nach Empfang von RAND kombiniert das SIM RAND mit dem gespeicherten Schlüssel Ki über den ebenfalls gespeicherten Algorithmus A3 und erhält sein Ergebnis SRES (Signed Response). Man könnte also SRES als Funktion von A3, Ki und RAND bezeichnen. Diese Zahl hat eine Länge von 32 Bit und wird zum Vergleichen vom Handy an das AuC gesendet. Bei Erfolg beginnt die Berechnung für die Verschlüsselung, bei Misserfolg wird der Vorgang abgebrochen.[48]

5.3. Ciphering

Wenn nun der Teilnehmer richtig identifiziert worden ist, beginnt zuerst die Verschlüsselung und danach die verschlüsselte Übertragung aller Daten, also der Nutzdaten als und der Signalisierungsdaten.

Durch das Zusammenführen von Ki und der Zufallszahl RAND wird mit dem Algorithmus A8 der Übertragungsschlüssel Kc , der 64 Bit lang ist, berechnet. Daraus folgt also – wie bei SRES – Kc ist eine Funktion von A8, Ki und RAND. Die Bezeichnung Kc kommt von Key(Ciphering).

Da der Schlüssel Kc nicht per Funk übertragen wird, erhält ihn die BTS vom AuC. Damit das Netz und die Mobilstation denselben Schlüssel verwenden, wird ihm eine Nummer (COUNT) zugeordnet, die bei jeder Mitteilung ans Netz mitgesendet wird.

---

[46] Vgl. Heine (wie Anm. 5), S. 303.

[47] Vgl. Heine (wie Anm. 5), S. 371.

[48] Vgl. Heine (wie Anm. 5), S. 326.

Der Algorithmus A5 ist in der CIPH_MOD_CMD Meldung (3.7), die vom MSC versendet wird, enthalten. Die BTS entnimmt diesen und sendet die Meldung weiter zur MS. Diese weiß nun, dass jeder Burst, der versendet wird, verschlüsselt ist. Das Handy verknüpft nun den Schlüssel Kc mit dem Count über A5 und erhält so zwei 114 Bit lange Cipher-Sequenzen, von denen eine zum Ver- und die andere zum Entschlüsseln verwendet wird. Die zu verschlüsselnden Daten werden dann mit einer XOR-Funktion mit der Cipher-Sequenz verbunden, was die Übertragungsdaten des Bursts ergibt. Beim Empfang der Bitfolgen wird diese mit der zweiten Cipher-Sequenz wieder über die XOR Verknüpfung zurückgewandelt. Durch die XOR-Funktion wird das Verschlüsseln vereinfacht, da sich bei passenden Eingangswerten die XOR-Verknüpfungen aufheben. Da sich der Count bei jedem Datenpaket erhöht, ändern sich auch die Cipher-Sequenzen dynamisch. So werden die Daten asymmetrisch verschlüsselt und der Schlüssel ändert sich andauernd, wodurch die Übertragung sehr sicher ist.[49]

Am 13. April 1998 veröffentlichten die Smartcard Developer Association und die ISAAC Security Research Group eine Schwachstelle in den Verschlüsselungscodes, der es einem Cracker erlaubt, bei physischem Zugang einen Klon (identische Kopie) einer SIM-Karte herzustellen und so auf Kosten anderer zu telefonieren. Da man in Europa teilweise anonym Handies mieten kann, können Drittpersonen geschädigt werden. Dieses Problem kommt durch das Vorgehen der GSM-Industrie nach dem Grundsatz:„Security by obscurity“, (Sicherheit durch Verborgenheit) zustande, wo die Verschlüsselungsalgorithmen geheim gehalten werden. Der amerikanische Anbieter Omnipoint hat angekündigt, den Algorithmus zu wechseln.

Marc Briceno von Smart Card Developers Association hatte es geschafft, mit der Hilfe von aufgetauchten Unterlagen einen Algorithmus mit dem Namen COM128 zu finden. Dieser Algorithmus wird von fast allen Netzbetreibern, bis auf drei (T-Mobil und E-Plus), verwendet, beispielsweise von D2 Mannesmann. Ian Goldberg und Dave Wagner von der Berkeley Universität hatten eine Schwachstelle gefunden, die es ermöglichte den Ki mit Hilfe von Anfragen herauszulesen. Bei einer solchen Attacke werden etwa 150000 Anfragen auf die Karte gestartet. Dadurch kann man dann eine zweite SIM-Karte mit gleicher IMSI und gleichem Ki herstellen. Bei D2 ist es mit diesen SIMs sogar möglich sich gleichzeitig ins Netz

[49] Vgl. Heine (wie Anm. 5), S. 324-327.

einzuwählen, nur Anrufe sind nicht gleichzeitig möglich. Der Chaos Computer Club hat auch Software dazu auf seiner Homepage.[50]

Laut Dave Wagner wäre es prinzipiell sogar möglich über das Air-Interface den COMP128 der SIM-Karte zu berechnen. Zwar wurde dies noch nicht in einem Versuch bewiesen, aber nach einigen Expertenaussagen wäre es durchaus möglich, bei einer längeren Zugriffszeit und einer falschen BTS, die SIM-Karte ohne physischen Zugang zu klonen. Eine solche BTS müsste zwar nicht alle von GSM verlangten Dienste anbieten, sie würde aber trotzdem noch ca. $ 10 000 kosten und der Cracker müsste noch das nötige Know-how besitzen.

Zumindest könnten die Gespräche nach dem BSC von jedem mitgehört werden, der Zugang hat, da dort die Daten unverschlüsselt übertragen werden. Die Übertragung über das Air-Interface jedoch kann nur ein staatliches Behörde wie das Heeresnachrichtenamt in Österreich oder die NSA in den USA. Zusätzlich hängt die Stärke der Verschlüsselung der Funkdaten vom Land, in dem man sich befindet, ab. So besteht das Gerücht, dass einige Behörden der NATO in der Mitte der 80er Jahre berieten, ob man starke oder schwache Verschlüsselung verwenden sollte. Deutschland sprach sich für eine starke Verschlüsselung aus, wurde jedoch überstimmt, und so wurde eine französische Lösung verwendet. Diese Lösung verwendet den Verschlüsselungsalgorithmus A5, der 64 Bit lang ist und aus drei Schlüsseln besteht. Diese drei Schlüssel sind 19, 22 und 23 Bit lang und verändern sich mit der Zeit. A5 hängt also von der lokalen Zeit des GSM-Netzes ab. Dieser Schlüssel wird als A5/1 bezeichnet. Er darf nur in bestimmten Ländern verwendet werden, wegen der starken Verschlüsselung. Trotzdem bestehen die letzten 10 Bits nur aus Nullen. Vermutlich wurde diese Hintertür absichtlich eingebaut, um wichtige Personen, die in einem Land roamen, später problemlos im eigenen Land wieder abhören zu können. Exportiert wird normalerweise die Variante A5/2, die schwächer ist und es gibt sogar den noch schwächeren Schlüssel A5/7. Es besteht die Möglichkeit mit einer „Plaintext-Attacke“, (unverschlüsselter und verschlüsselter Text sind teilweise bekannt) den Schlüssel A5 zu „raten“ und dann zu kontrollieren; diese Attacke benötigt mindestens 2^{35} aber höchstens 2^{52} Anfragen. Trotzdem lässt diese Sicherheitsstufe auf Verschlüsselung auf Militärniveau vermuten.[51]

Zwar ist das Sicherheitsrisiko geringer als im analogen Mobilfunknetz, aber es besteht das Gespräche mitgehört werden können, oder dass sogar die SIM-Karte geklont wird.

---

[50] Vgl. Chaos Computer Club: D2 Hack: *http://www.ccc.de/D2Pirat/index.html* vom 11.8.1999.

[51] Vgl. Newsgroup: *http://jya.com/crack-a5.htm* vom 17.2.2000.

6. Zukunftsträchtige Projekte

Die Folgen daraus, dass Mikrochips immer kleiner und schneller werden, sind nirgends so offensichtlich wie beim Handy. Das Handy wird immer kleiner, verarbeitet immer mehr Daten und wird früher oder später die „Fernbedienung zur Welt“.[52] Diese Handies werden 3. Generation-Handies (Abb. 32) (3G) genannt. Zwar benötigen sie höhere Übertragungsraten, dafür werden ihre Funktionen allumfassend werden. Aber auch das Umfeld wird sich anpassen müssen: In einigen Jahren wird wohl jeder nur mehr einen Laptop und ein Handy besitzen. Diese werden über Bluetooth (6.1, Kurzstreckenfunkverbindung) miteinander verbunden. Dann kann man mit Übertragungsraten von 2 Mbit/s dank UMTS (6.6, Übertragungsstandard) surfen.

Dank WAP (6.2) ist es nun seit 1999 möglich, mit dem Handy übers Internet Daten zu übertragen. Es ist möglich, per Handy den Busfahrplan anzusehen, Kinokarten zu kaufen, Nachrichten lesen oder sogar dank dem Pilotprojekt von Nokia, Visa und MeritaNordbanken, via Handy im Internet einkaufen oder mitsteigern (z.B. eBay). Der Trend führt zum bargeldlosen Zahlungsverkehr, da dies für den Staat billiger ist, und für den Endverbraucher angenehmer ist: Dieser nimmt einfach sein Handy heraus, gibt gegebenenfalls einen PIN ein und schon wird der Betrag abgebucht. Die Realisierbarkeit hat Nokia mit der Hilfe von Sonera und Swisscom bereits auf der Telecom 1999, einer Technik-Messe in Genf, bewiesen, wo man mit seinem Handy ein Getränk an einem speziellen Cola-Automat kaufen konnte. Die Grundlage dazu bildet Bluetooth (6.1), ein System, mit dem unterschiedliche Geräte per Funk zusammengeschlossen werden können.

Ein weiteres Beispiel für die Anwendung des Handies in der Zukunft bringt das bayrische Unternehmen GAP AG. In ihrem Produkt HiConnect, einer GSM-gesteuerten Steckdose, befindet sich ein Bordcomputer und ein GSM-Terminal von Siemens (Cellular Engine M20). Wird nun von einem Handy aus eine SMS an dieses Terminal gesendet, wird es erst vom Bordcomputer nach der Berechtigung geprüft. Danach wird der Steuerbefehl, der sich im SMS befindet, ausgeführt. Die vier mitgelieferten Adapter, die zwischen den Stecker und die Steckdose hineingegeben werden, können bis zu 30 m voneinander entfernt sein. Zusätzlich sind noch vier Meldeeingänge eingebaut; also kann man dies auch als Alarmanlage benützen, die Veränderungen an das Handy oder an ein Sicherheitsunternehmen weiterleitet. Die Nummern werden auf einer SIM-Karte gespeichert, die dann nur noch in ein Handy eingelegt und deren integriertes Telefonbuch editiert werden muss. Bei den hinteren Einträgen gibt man

[52] Michael Heidemann, Produktmanager Mobile Phones Sales, Nokia.

Schlüsselworte und seine Handynummer ein. Dann kann man beispielsweise vom Auto aus den elektrischen Heizkörper einschalten. Die Entwicklung in diese Richtung der Handynutzung wird immer wichtiger. [53]

6.1. Bluetooth

Hinter Bluetooth (Abb. 33), genannt nach dem Dänischen König Harald II „Blauzahn", der Skandinavien über den Øresund verband, versteckt sich eine Technologie für kurze, billige Funkverbindungen zwischen mobilen Geräten. Die Bluetooth Special Interest Group beinhaltet führende TK-Unternehmen wie Ericsson oder Nokia, die versuchen, dieses Technologie markttauglich zu machen. Erstmals vorgestellt wurde Bluetooth im Mai 1998.

Bluetooth ist eine innovative Technologie für kabellose Verbindungen. Sie ermöglicht es Sprachdaten über eine Funkverbindung ohne Sichtkontakt und sogar durch eine Wand zwischen Sender und Empfänger zu übertragen. Diese Technik benötigt eine 9 mal 9 mm Mikrochip, der das Frequency Hopping, die Verschlüsselung der Daten und eine PIN-Abfrage ermöglicht. Da der Sender nicht weiß, wer und wo der Empfänger ist, muss der Benutzer den Empfänger von Hand auswählen. Die verwendete Frequenz geht von 2 402 GHz bis 2 480 GHz und die Verbindung kann von 10 cm bis 10 m betragen. Eigentlich wären bis zu 100 m möglich, dafür würde aber mehr Leistung nötig sein.

Der große Vorteil von Bluetooth ist, dass der Funk solide Objekte durchdringt, also kann sich der Sender in einem Gebäude zu bewegen. Zudem muss ein Anwender das Handy nicht aus der Tasche nehmen, wenn er es mit dem Laptop verbindet.

Die ersten Endgeräte werden im 2. Quartal 2000 erscheinen und werden anfänglich etwa $ 200, später aber nur noch $ 20 kosten.

6.2. WAP

Seit dem 4. Quartal 1999 ist das erste, lang angekündigte WAP-fähige Handy im Handel erhältlich. Doch was steht hinter der Abkürzung WAP? WAP bedeutet Wireless Application Protocol, also kabelloses Anwendungs-Protokoll. Dieses Protokoll weist auf eine Verbindung mit Computern hin: Durch WAP ist es möglich ins Internet einzusteigen. Freilich können die Grafiken des Internets nicht auf dem mehr oder weniger kleinen Handydisplay angezeigt

---

[53] Vgl. Pernsteiner, Peter; Frischer Kaffee wie von Geisterhand. GAP HiConnect In: Funky. Mobilfunk & Handy Magazin. 2/00 Jan./Februar, S. 20-21.

werden. Deshalb wurde die Programmiersprache WML (eine abgespeckte HTML-Variante) geschaffen, durch die reine Textdaten angezeigt werden. Diese kann man dann mit einem WAP-fähigen Handy, z.B. NOKIA 7110, mit Hilfe eines Microbrowsers, der im Handy integriert ist, abrufen.

Die Handy-Konzerne Ericsson, Motorola, Nokia und Phone.com (früher Unwired Planet) schlossen sich bereits Mitte 1997 zusammen, um WAP zu entwickeln. Inzwischen sind auch andere bedeutende Unternehmen eingestiegen: Microsoft, Alcatel, Siemens, Samsung, Philipps, Fujitsu, IBM, Psion, Intel, Anbieter wie AT&T, Sonera, Telenor (bei one beteiligt), T-Mobil, Vodafone Swisscom und Sicherheitsunternehmen wie RSA. Dieses WAP-Forum wurde einberufen, als der US-amerikanische Netzwerkprovider Omnipoint die eigenständigen (proprietäten) Lösungen wie z.B. Smart Messageing ablehnte und sich für einen gemeinsamen Standard aussprach. Der WAP-Standard für kabellose Übertragung wurde so definiert, dass er sowohl mit GSM, GPRS oder UMTS funktioniert und unabhängig vom Eingabegeräten wie Keypads oder Touchscreens ist. Wie TCP/IP wird auch WAP in mehrere Schichten unterteilt. Die übertragenen Daten sind stark komprimiert, damit die Systemressourcen des Handies nicht zu stark belastet werden. Das Maximum, das das Handy verkraftet, sind 1400 Bytes, was jedoch verglichen mit Computern vor 30 Jahren noch sehr viel ist. Seit der Einführung des WAP-Standards ist noch immer ein gewisses Gerangel zwischen den Herstellern Ericsson, Nokia und Phone.com bemerkbar. Beispielsweise glichen Nokia und Ericsson ihre Endgeräte aneinander an, um sich von Phone.com zu distanzieren. So versucht jeder den anderen durch kluge Schachzüge abzuhängen. Die besten Chancen tonangebend zu werden – sofern nicht die anderen Unternehmen gleich wieder einen neuen Standard definieren – hat NOKIA, da sie eine vertikale Produktreihe mit Toolkits, Gateways und Endgeräten hat. Grundsätzlich bleibt noch zu sagen, dass WAP nicht nur bei Handies sondern auch für Palmtops, wie Psion oder Siemens funktioniert, die Revolution jedoch erst mit der Einführung von UMTS oder GPRS beginnen wird.[54]

Es gibt zwei WAP-Standards (Abb. 34); der erste, WAP 1.0, verwendet mehrere SMS um die Daten zu übertragen (Bearer Service). Dieser Standard wird zum Beispiel beim Siemens S25 oder in Frankreich beim Alcatel One Touch Pocket verwendet. Problematisch ist, dass in einem SMS nur 160 Zeichen übertragen werden können.

Dies ist auch der Grund, weshalb sich das WAP-Forum auf den nach unten nicht kompatiblen WAP-Standard 1.1 einigte. Bei diesem Standard, der am 1.7.1999 als Standard festgesetzt wurde, wird auf den CSD-Standard (Circuit Switched Data, 6.4) zurückgegriffen. Der

[54] Vgl. WAPWEB : Infotext : Was ist WAP: *http://www.wapweb.de* vom 15.12. 1999.

Nachteil ist, dass das Einwählen rund eine halbe Minute benötigt. Doch dann wird eine Anfrage in der WML-Sprache and das WAP-Gateway gesendet, das diese Anfrage umwandelt. Die Rücksendung der geforderten Daten erfolgt entweder als HTML-Text, der vom WAP-Gateway umgewandelt wird, oder gleich als WML-Text, der dann auf dem Handy angezeigt wird. Bei der Auswahl eines Menüpunkts wird dann beim NOKIA 7110 noch ein CSD versendet, da dies analog funktioniert und so die Verbindung nicht für eine Menüauswahl aufrecht erhalten werden kann. Doch dies sollte sich bald mit dem GPRS-Standard (6.5) ändern.

Die Verbindung zwischen Handy und Gateway ist verschlüsselt und für die Übertragung von Kennwörtern oder anderen vertraulichen Daten, muss vom Gateway auch eine sichere Internet-Verbindung zum Host bestehen.

6.3. Edge

Das von Ericsson entwickelte Verfahren mit dem Namen Edge (Enhanced Data Rates for GSM Evolution = erweiterte Datenraten für die Evolution von GSM) kombiniert - wie auch HSCSD - mehrere Zeitschlitze miteinander. Der Vorteil von diesem Verfahren ist, dass nur geringe Modifikationen durch ein Softwareupdate am GSM-Netz vorgenommen werden müssen. Außerdem können die bisher geltenden 9 KBit/s auf 48 Kbit/s (bei sehr guten Funkverhältnissen sogar auf 70 Kbit) erweitert werden. Durch die mögliche Kombination (Abb. 35) von bis zu 8 Zeitschlitzen entstünden dann Übertragungsraten von bis zu 384 Kbit/s. Zwar wird dieses Verfahren in Europa wohl kaum eingeführt werden, es ist aber trotzdem ein guter Ansatz für Hochgeschwindigkeitsübertragung.

6.4. HSCSD

Hinter dieser Abkürzung von High Speed Circuit Switched Data verbirgt sich eine Technik, die bald die Übertragungsrate im GSM-Netz erhöhen wird. Dies funktioniert über die Nutzung mehrerer Zeitschlitze durch ein Handy, also mehrerer Übertragungskanäle (Abb. 36). Hierzu werden anfangs nur zwei normale Zeitschlitze „verbunden“ wodurch sich die Übertragungsrate auf 19 200 Bit/s verdoppelt. Dies geringe Aufstockung liegt daran, dass die Hersteller erst die Geräte produzieren und die Kunden diese auch kaufen müssen. Später wird dieses System möglicherweise auf zwei ganze Frequenzbänder erweitert, was eine Übertragung von bis zu 28 800 Bit/s ermöglichen würde. Sobald aber Daten in mehr als vier Zeitschlitzen übertragen werden, werden spezielle Sende- und Empfangseinrichtungen

benötigt. Wenn nun aber für Gespräche eine Leitung benötigt wird, wird diese dem HSCSD-Dienst entzogen.

HSCSD baut auf dem Prinzip des GSM-Netzes auf, also werden wieder alle Ressourcen benötigt und deshalb wird auch bei der Übertagung der Kanal codiert. Darüber hinaus muss das Handy nun mehrere Zeitschlitze empfangen, aber nur in einem senden.

6.5. GPRS

Die Alternative zu HSCSD heißt GPRS (General Packet Radio Service). Bei diesem Übertragungsverfahren werden bis zu alle acht Zeitschlitze eines Übertragungsblocks für einen Teilnehmer freigegeben (Abb. 36). Dadurch erhöhen sich die Übertragungsraten auf 57 600 Bit/s nach der ersten Ausbaustufe und auf 115 200 Bit/s nach der zweiten Ausbaustufe. Der Nachteil bei diesem Verfahren ist, dass alle Teilnehmer, die sich in einer Funkzelle befinden, diese Übertragungsraten teilen müssen. Wenn also wenige Teilnehmer in einer Zelle diesen Dienst nutzen, sind die Übertragungsraten hoch. Trotzdem könnte das System Entlastung für das GSM-Netzwerk bringen, da die Datenübertragung leitungsunabhängig ist und jedes Datenpaket einzeln geroutet wird.

Damit GPRS funktioniert, benötigt das Netzwerk zusätzliche Elemente, wie eine Außenschnittstelle (GGSN, Gateway GPRS Support Node, wandelt die Nachrichten und Adressen um), ein Register (GR, GPRS Register, beinhaltet GPRS-bezogene Daten) und eine Zugangskontrolle (SGSN, Serving GPRS Supply Node, verfolgt und authentifiziert das Handy).

Um die Überlastung des Netzes zu verhindern, könnte man volumenabhängig (Zahlung für jedes heruntergeladene MB) abrechnen und dadurch umfangreichere Downloads verhindern. Das GPRS-System wird nach Angaben der Netzbetreiber noch vor Ende 2000 nutzbar sein.

6.6. UMTS

Mit UMTS (Universal Mobile Telecommunications System), das im Jahre 2002 (in Japan sogar schon 2001) eingeführt werden soll, beginnt die Zukunft der Mobilkommunikation. Mit einer geplanten Übertragungsrate von 2 Mbit/s, wäre dieses System 30 mal schneller als ISDN (Abb. 37). Diese 2 Mbit/s gelten aber nur für ein beinahe stationäres Handy (Fußgänger), ein bewegtes hingegen wird wohl nur etwa 128 Kbit/s erreichen. Damit sollte endlich die Schallmauer in der Mobilkommunikation gebrochen sein und Videokonferenzen würden für jedermann möglich. Die Übertragung wird dann wahrscheinlich im Frequenzband

von 1885 bis 2025 MHz für das zukünftige IMT-2000 System und von 1980-2010 MHZ bzw. 2170-2200 MHz für den Satellitenbetrieb erfolgen. Es wird notwendig sein, dass Dual-Mode Handies hergestellt werden, die im GSM-Netz telefonieren, aber über UMTS Daten übertragen. IMT-2000 (International Mobile Telecommunication), das in Europa UMTS heißt, sollte der nächste weltweite Standard sein, auf den Europa, die USA und Japan hinarbeiten. Dieser Standard verwendet das sogenannte W-CDMA-Verfahren (Wideband Code Division Multiple Access), das die Daten komprimiert und in kleinen Paketen versendet, und das T-CDMA-Verfahren (Time Code Division Multiple Acess), das die Daten zeitversetzt und codiert überträgt.

Doch wichtig ist, dass nicht von einem Tag auf den anderen alle GSM-Handies nutzlos sein werden. Statt dessen wird der GSM-Betrieb immer noch weitergeführt; möglicherweise wird GSM auch noch die 450 MHz-Frequenzen übernehmen.

6.7. IRIDIUM

Eigentlich bietet die mobile Kommunikation über Satelliten die gleichen Möglichkeiten, wie terrestrischer (auf der Erdoberfläche stattfindender) Mobilfunk. Der große Vorteil von Satellitenkommunikation besteht darin, dass man dieses Netz wirklich überall auf der Erdoberfläche nutzen kann, außer vielleicht in einigen politischen Funklöchern wie Irak oder Kuba. Man kann auch an Orten telefonieren, die nicht von GSM-Netzen abgedeckt werden, wie beispielsweise in der Wüste, im Urwald, mitten im Ozean oder in der Antarktis. In Europa ist aber auch innerhalb von Gebäuden eine guter Empfang. Das hat zur Folge, dass dieses System vor allem von Forschungsteams genutzt wird. Ein weiterer Vorteil ist, dass die Kosten der Übertragung nicht von der Entfernung abhängen. Der Nachteil wiederum ist, dass auch hier die Zahl der Kanäle begrenzt ist und die Kosten für einen Kommunikationssatelliten selbst sehr hoch sind. Bis vor einigen Jahren haben diese Satelliten staatlichen Betrieben gehört, wie beispielsweise Eutelsat (für Westeuropa) oder Inmarsat (für weltweiten maritimen Funk, International Maritime Satellite Organisation).

1990 wurde das IRIDIUM-System von Motorola entwickelt (Abb. 38). Die 66 Satelliten, die dafür benötigt werden, umkreisen die Erde in Bahnen, die parallel zu den Meridianen verlaufen (polar) und die in einer Höhe von 780 km (LEO-System, Low Earth Orbit) sind. Auf jeder der sechs Umlaufbahnen befinden sich elf Satelliten. Der erste dieser Satelliten wurde im Juli 1997 in seine Umlaufbahn gebracht; der Betrieb wurde 1998 aufgenommen. Diese Satelliten kommunizieren über Zwischensatellitenverbindungen (ISL, Inter Satellite

Links), was eine große Anzahl von Gateways einspart und die Verbindung über Ozeane ermöglicht. Ein solches ISL besteht aus je vier benachbarten Satelliten. Die Schwierigkeit einer solchen Verbindung besteht darin, dass sich die Entfernung und Richtung der Satelliten andauernd verändert. Verbindung mit dem Festnetz haben die Satelliten über 13 Bodenstationen, von denen die europäische in der Nähe von Rom liegt.

Das Handy (MS) ermöglicht sowohl die Verbindung mit terrestrischem Funk, als auch mit Satellitenfunk (Dualmode). Für den Satellitenfunk wird eine Übertragungsrate von 4800 bit/s für Sprache (2,4 kbit/s UL und 2,4 kbit/s DL) und 2400 bit/s für Daten. Die Übertragung der Daten findet über 90 ms lange Zeitschlitze (TDMA-Rahmen, Time Division Multiple Access) statt, die wiederum in einen Signalisierungskanal und in je vier Up- und Downlink-Kanäle unterteilt sind,. Dem IRIDIUM-System wurde eine Frequenzbreite von 5,15 MHz (von 1621,35 bis 1626,5 MHz) zugeteilt. Durch den Frequenzabstand (FDMA, 3.3.1.1) von 41,67 kHz und der Kanalbandbreite von jeweils 31,5 kHz entstehen 124 Kanäle mit je 4 Up- und Downlink-Kanälen. Es entstehen somit 496 Kanäle Da jede Frequenz pro Satellit vier mal wiederverwendet wird, könnten prinzipiell pro Satellit 1984 Verbindungen aufgebaut werden, aber durch die Batterieleistung sind nur 1100 Verbindungen möglich.

Da sich die Zellen der Satelliten mit einer Geschwindigkeit von etwa 7 km/s fortbewegen, und eine Zelle einen Durchmesser von etwa 500 km hat, wechselt der stationäre Teilnehmer fast jede Minute die Funkzelle (Serving Cell). Daraus entstehen wiederum Handover, die der Satellit durchführen muss. Um die Belastung an Handovern gering zu halten, muss das System den Satellit automatisch auswählen, der möglichst lange verwendet werden kann. Wichtig hierbei ist, dass für einen guten Empfang Sichtverbindung bestehen sollte. Besonders in West-Ost-Richtung sollte freie Sicht sein, was in Großstädten problematisch werden kann.[55]

Der große Nachteil von IRIDIUM sind die Kosten. Aus diesem Grund hat das Raumfahrt-Unternehmen Dornier eine Ergänzung bzw. Alternative für die Satelliten gefunden: Solarbetriebene und wegen der Bedingungen robuste Zeppeline mit Helium-Füllung, die in 20 km Höhe in der Stratosphäre mit der Hilfe von GPS genau über einem Punkt schweben. Für diese Idee erhielten vier Wissenschaftler den 1,5 Mio. DM Körber-Preis für Europäische Wissenschaft. Falls dieses Projekt finanziell unterstützt wird

---

[55] Vgl. Walke, Bernhard: Mobilfunknetze und ihre Protokolle. Bd. 2, Bündelfunk, schnurlose Telefonsysteme, W-ATM, HIPERLAN, Satellitenfunk, UPT. Stuttgart 1998 (Informationstechnik), S. 337-341, 359-360.

(ca. 15 Mio. DM), könnte bereits 2001 ein Prototyp gebaut werden und das System ab 2002 verwendbar sein.

Quellen und weiterführende Literatur:

Für einen allgemeinen Überblick über den GSM-Standard:

Heine, Gunnar: GSM-Signalisierung verstehen und praktisch anwenden. Grundlagen, Messtechnik, Messbeispiele. Poing 1998 (Funkschau Funktechnik).

Burgmer, Martin und Andreas Ehritt: D-Netz-Funktechnik. Würzburg 1995 (Vogel-Fachbuch).

Überblick über die komplette Mobilkommunikation:

Walke, Bernhard: Mobilfunknetze und ihre Protokolle. Bd.1, Grundlagen, GSM, UMTS und andere zellulare Mobilfunknetze. Stuttgart 1998 (Informationstechnik).

Walke, Bernhard: Mobilfunknetze und ihre Protokolle. Bd.2, Bündelfunk, schnurlose Telefonsysteme, W-ATM, HIPERLAN, Satellitenfunk, UPT. Stuttgart 1998 (Informationstechnik).

Funktionsweise der Digitaltechnik:

Häßler, Martin und Hans Werner Straub: Praxis der Digitaltechnik. Grundlagen und Anwendungen. München 1993.

Funktionsweise und Verwendung von Chipkarten:

Störmer, Werner: Elektronische Kartensysteme. Technik und Einsatzmöglichkeiten. Heidelberg 1997 (W&S Praxiswissen).

Zeitschriften über Mobilfunk:

Connect, Europas größtes Magazin zur Telekommunikation.

http://www.connect-online.de

Funky. Handy & Mobilfunk Magazin.

http://www.funky.de

newcom. Handy, Telefon, Online & ISDN.

http://www.newcom-online.de

Informationen über Akkus oder Batterien:

http://www.sanyobatteries.net

Informationen über GSM allgemein:

http://www.gsm.org

http://www.cs.tu-berlin.de/~jutta/gsm/js-intro.html

http://www.whatis.com

http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html

http://www.prattfamily.demon.co.uk/mikep/gsmlinks.html

http://www.cellular.co.za/data_speed_evolution.htm

Klonen von SIM-Karten:

Marc Briceno

Smart Card Developers Association: http://www.scard.org/gsm/a3a8.txt

Unterlagen über COM128

Ian Goldberg und Dave Wagner: http://www.isaac.cs.berkeley.edu/isaac/gsm.html

http://www.ccc.de

Zukunftsträchtige Projekte:

Bluetooth

WAP

UMTS:

http://www.umts-forum.org

http://www.umts.org

Bild- und Tabellennachweis:

Bilder:

Abb. 1 Einleitung: Nokia: Connect 1/2000, S. 15.

Abb. 6 Lithium-Polymer-Akku: Connect 8/99, S. 61.

Abb. 7 LCD-Display: Sexl (u.a.): Physik 3 AHS, Elektrizitätslehre. 2. Aufl. Korneuburg (1992, 1998), S. 55.

Abb. 15 Verarbeitung der Daten durch OSI: Heine, Gunnar, S. 49.

Abb. 16 Schichten der Knotenpunkte: Walke, Bernd, Bd.1, S. 66.

Abb. 18 Interleaving: Heine, Gunnar, S.351.

Abb. 19 Burst: Heine, Gunnar, S. 316.

Abb. 20 NSS-Subsystem: Heine, Gunnar, S. 40.

Abb. 22 RR-Frame: Heine, Gunnar, S. 106.

Abb. 24 Evolution von Motorola: Connect 1/2000, S. 38.

Abb. 28 IMEI: Heine, Gunnar. S. 348.

Abb. 29 IMEISV: Heine. Gunnar. S. 348.

Abb. 30 IMSI und TMSI: Walke, Bernd, Bd. 1, S. 262.

Abb. 32 Ericsson: Funky 1/2000, S. 97.

Abb. 33 Bluetooth-Logo: Connect 11/99, S. 16.

Abb. 34 WAP-Bearer: Connect 10/99, S.76.

Abb. 35 Edge-Übertragung: Connect 8/99, S.60.

Abb. 36 HSCSD vs. GPRS: Connect 11/99, S.88.

Abb. 37 Datenübertragungsraten: Funky 10/99, S. 31.

Tabellen:

Abb. 5 Speicher: Heine, Gunnar, S. 26-27.

Abb. 12 Teilnehmerdaten: Heine, Gunnar, S. 43.

Abb. 14 Daten im VLR: Heine, Gunnar, S. 43.

Abb. 25 Entwicklung von Handy u. Nutzer: Connect 1/2000, S. 36-39.

Abb. 30 MCCs: Heine, Gunnar, S.359-361.

Abb. 38 Iridium: Walke, Bernd, Bd. 2, S. 339-341.