

Geschichte des Mobilfunks, GSM-
Netzwerkarchitektur, Technik und
Prozeduren

Geschichte des Mobilfunks, GSM-Netzwerkarchitektur, GSM-Technik und GSM-Prozeduren.

Inhaltsverzeichnis

GSM und wie alles begann - Ein geschichtlicher Abriss.....	2
Die Netze A-E.....	2
Ziele von GSM.....	2
Merkmale von GSM.....	3
Ein Überblick über die verschiedenen Spielarten des GSM.....	3
Luftschnittstelle.....	3
Sprachkodierung.....	4
Aufbau eines GSM-Netztes.....	5
Base Transceiver Station (BTS).....	6
Base Station Controller (BSC).....	6
Transcoding Equipment (TCE).....	6
Home Location Register (HLR).....	6
Visitors Location Register (VLR).....	6
Mobile Service Switching Center (MSC).....	6
Equipment Identity Register (EIR).....	7
Short Message Service Center (SMSC).....	7
Authentication Center (AC).....	7
Operations and Maintenance Center (OMC).....	7
GSM Prozeduren.....	7
Authentifizierung und Verschlüsselung.....	7
Datenübertragung im GSM-Netz.....	8
Einbuchen.....	8
Anruf von A zu B.....	8
IMSI-Catcher.....	8
Ergänzung.....	9
Fragen.....	9
Linksammlung.....	9
Haftungsausschluß.....	9
Das hatte keinen Patz mehr.....	11
Rahmenstruktur.....	11
Erhöhung der Datenredundanz.....	11
Daten-/FAX-Übertragung.....	11

GSM und wie alles begann - Ein geschichtlicher Abriss

Die Netze A-E

Entwicklung der Netze von A-E des öffentlichen, bewegten Landfunknetz (öbL):

Netz	Von-Bis	Übertragung	Netzstruktur	Vermittlung	Vorw.
A	1958-1977	UKW 157,60-162,94 MHz	Landfunkstelle (30-50 km Radius)	600 Fräulein, Kanalsuche + anpiepsen	010-#
B	1972-1994	UKW 148,40-153,74 MHz	Landfunkstelle (30-50 km Radius)	selbst Wählen, variable Nummer	0711-xx-#
C	1985-2000	450 MHz	Zellen	selbst Wählen, konstante Nummer, Handover	0161-#
D	1991/92-?	TDMA 900 MHz	Zellen	selbst Wählen, konstante Nummer, Roaming, Handover	...
E	1994/98-?	TDMA 1,8/1,9 GHz DCS-1800 und PCS-1900	Zellen	selbst Wählen, konstante Nummer, Roaming, Handover	...

Bemerkungen

A-Netz ist Ende der 50er das größte flächendeckende öffentliche Mobilfunknetz der Welt.

B-Netz ist Exportschlager zu seiner Zeit (Roaming mit (A), (LUX), (NL))

B-Netz 1972 auf die Frequenzen des A-Netzes ausgeweitet (B2-Netz)

C-Netz ließ endlich DATEX und Fax-Verbindungen zu (2400 bit/s)

C-Netz hatte 100% Deckung.

D-Netz später mit HalfRate Übertragung erweitert. 8->16 Teilnehmer pro Kanal

E-Netz ist das sog. High Quality-Netz (neuere CODECs=>bessere Qualität).

seit 1999 haben D1 und D2 auch Träger im 1,8 GHz-Band

Netz	Benutzer max	Ben. gehabt	Grundgebühr	Telefon
A	10500	10500	66 DM später 270,00 DM	8000-15000 DM
B	16000	16000	270 DM später 120 DM	8000-15000 DM
B2	27000	27000	270 DM später 120 DM	8000-15000 DM
C	500.000 später 850.000	803000	120 DM später 19 DM	3000-12000 DM

Und GSM?

1982 beschließt die Nordic PPT der CEPT einen Vorschlag zu einem einheitlichen Mobilfunknetz zu machen. Daraufhin wird die Groupe Speciale Mobile gegründet, wovon sich GSM ableitet. Nachher stand GSM für Global System for Mobile communication. Seither gibt es GSM in über 100 Ländern.

Ziele von GSM

Ziel war es, einen offenen und erweiterbaren Mobilfunkstandard zu definieren. Er sollte voll kompatibel zu ISDN sein, hoch skalierbar, digital und sicher. Dies ist offensichtlich geglückt. GSM bietet heute Sprachdienste, Faxdienste, Datenübertragung, Kurznachrichten und Mehrwertdienste.

Merkmale von GSM

- Digitaler Standard. Dadurch DV-Algorithmen anwendbar
- Vollständige Kompatibilität zu ISDN
- Erhöhung der Teilnehmerkapazität durch Zeitmultiplexverfahren
- Mit OSI(Open System Interconnection) eine offene Schnittstelle für Erweiterungen
- Höhere Übertragungskapazität und bessere Sprachqualität durch Sprachkompressions- und Fehlerkorrekturalgorithmen
- Gleiche Endgeräte und Roaming in allen GSM-Netzen
- Für gleichbleibende Qualität. Frequency Hopping, variables Interleaving, variierende Kompressionsalgorithmen, Extrapolation von Zeitschlitten, variable Sendeleistung
- Extrapolation von bis zu 16 verlorenen Zeitschlitten. Durch Wederholung wird dem Benutzer ein störungsfreier Kanal suggeriert.
- Unbeständige Übertragung d.h. Sendepausen und „Comfort Noise“ bei niedrigem Geräuschpegel
- Verschlüsselung auf der Luftschnittstelle (momentan 8 Algorithmen)
- 8/16 Teilnehmer Pro Träger
- SMS - war ursprünglich mal als Konfigurationsschnittstelle gedacht. Daher nur 160 Zeichen
- Zallradien von 100m bis 35km (neuerdings sogar 70 oder gar 120 km)
- Idr. 7-Zellschema für die Frequenzwiederholung
- Seit 2000 Kanalbündelung mit HSCSD und Paketorientierung mit GPRS.
- Verschiedene Frequenzbänder für Up- und Downlink. Daher auch das bekannte „Ich höre dich, hörst du mich nicht?“-Phänomen
- Ein Träger speziell für Steuerkanäle

Ein Überblick über die verschiedenen Spielarten des GSM

Es gibt das klassische, verbindungsorientierte GSM, das die meisten Mobiltelefone verwenden. Es beinhaltet Sprachkommunikation, SMS und Datenübertragung. Bei Datenübertragungen stehen 9,6 kBit/s zur Verfügung, bei ausgeschalteter Fehlerkorrektur auch mehr. Daneben gibt es noch GSM-R (GSM-Railway), welches Rundrufe und Konferenzen durch Anrufen einer Gruppennummer erlaubt und sich durch erhöhte Zuverlässigkeit und strengere Spezifikationen auszeichnet. Es dient den Bahnen als Ersatz für Funkgeräte und zur Steuerung von Zügen. Die nächsthöhere Spielart ist das HSCSD (High Speed Circuit Switched Data). Es ist ebenfalls verbindungsorientiert und erreicht durch Kanalbündelung Übertragungsraten bis 43,2 kBit/s. Fast gleichzeitig erschien GPRS (General Packet Radio Service). Wie der Name schon suggeriert handelt es sich hierbei um eine paketorientierte Übertragung. Durch Zusammenschalten mehrerer Kanäle erreicht man hier Datenübertragungsraten von theoretisch 171,2 kBit/s mit allen acht Zeitschlitten. In der Praxis sind jedoch 56 kBit/s üblich. Die nächste Generation heißt EDGE (Enhanced Data rates for GSM Evolution) und bringt uns Datenraten bis 384 kBit/s. Hinter EDGE steckt ein anderes Modulationsverfahren als beim herkömmlichen GSM. Bei GSM wird GSMK mit Bi-phase-shift-keying verwendet, was 1 Bit/Symbol erlaubt. Bei EDGE dagegen wird Eight-phase-shift keying (8 PSK) verwendet. Durch das EDGE-Prinzip steigt die Datenrate bei HSCSD (ECSD) und bei GPRS (EGPRS) um den Faktor 3. Dennoch ist EDGE dem WCDMA-Verfahren von UMTS unterlegen. Überdies gibt es noch die Spielart CorporateGSM, bei dem das Unternehmensnetz eng mit dem eines GSM-Netzbetreibers gekoppelt wird, was Kostenvorteile bringt.

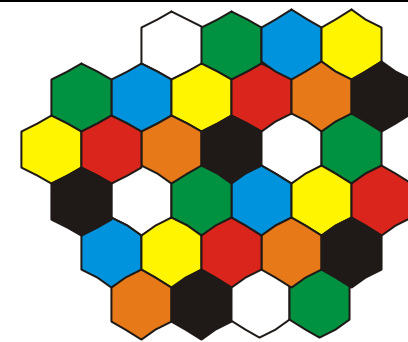
Luftschnittstelle

Die Luftschnittstelle ist ein wesentlicher Teil eines Mobilfunksystems. Aus deren Definition bestimmen sich Größen wie die Gesprächskapazität pro Zelle oder Übertragungsgeschwindigkeit. Für die Übertragung der Bits wird die Digitale GSMK-Modulation (Gaussian Minimum Key Shifting) zusammen mit 2-PSK (Bi-Phase-Shift-Keying) verwendet. Diese erlaubt 1 Bit pro Symbol zu übertragen. Die Bandbreite ist jeweils 25 MHz für Up-/Downlink bei GSM900 bzw. je 75MHz bei GSM1800. Jeder Träger hat eine Bandbreite von 200 kHz. Daraus ergeben sich 124 bzw. 374 Träger. Meist teilen sich mehrere Netzbetreiber die

Trägerfrequenzen (so haben z.B. D1 und D2 jeweils 62 Träger). Jeder Träger ist in 8 bzw. 16 Zeitschlitz/Bursts unterteilt (TDMA). Die Abfolge von 8/16 Zeitschlitz heißt Frame. Nachdem ein TDMA-Frame 4,615ms dauert, stehen in jedem Zeitschlitz 156,25 Bit zur Verfügung. Brutto ergibt sich daraus also eine Datenrate von 22,8 kBit/s (Fullrate) bzw. 11,4 kBit/s (Halfrate bei 16 ZS). Durch die Fehlerkorrektur und Steuerinformation bleiben dann netto für Sprache noch 13 bzw. 6,4 kBit/s übrig. Datenübertragungen werden nur in Fullrate-Kanälen gemacht, doch auch dort hat man nur 9,6 von 13 kBit/s zur Verfügung. Man kann aber irgendwie ohne Fehlerkorrektur auch die volle Nettorate erreichen. Die Funkversorgung erfolgt über eine Zellstruktur mit einer Zellgröße zwischen 100m und 35km. Dabei dürfen benachbarte Zellen allerdings nicht die gleichen Frequenzen benutzen. Daher wiederholt man die Frequenzen in nicht benachbarten Zellen. Aus Symmetriegründen sind 3er, 4er, 7er, 9er und 12er-Cluster für die Frequenzwiederholung möglich. Es werden aber hauptsächlich 7er-Cluster verwendet. Daraus ergeben sich bei 7er-Clustern folgende Maximalzahlen für Gespräche:

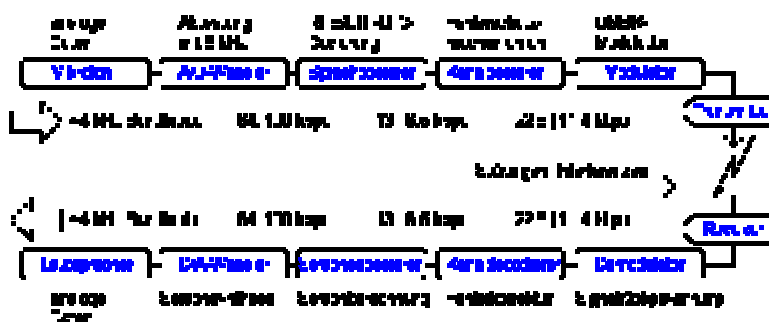
	GSM	D1/D2	GSM1800
Träger	124	62	374
Kanäle bei 8 Zeitschlitz	992	496	2992
Kanäle bei 16 Zeitschlitz	1984	992	5984
Kanäle pro Zelle bei 7er-Cluster und 8 Zeitschlitz	141,71	70,86	427,43
Bei 7er-Cluster und 16 Zeitschlitz	283,43	141,71	854,86

Zu beachten ist, daß ein Träger jeweils für Steuerkanäle reserviert ist und daher nicht für Gespräche nutzbar ist.



Sprachkodierung

Für Sprachübertragung muß ein hoher Kodierungsaufwand getrieben werden - schließlich muß die Bitrate von 64 auf 13 kBit/s reduziert werden. Außerdem sollen Fehler über die Zeit auf allen Kanälen möglichst unauffällig gehalten werden, und Luft ist ein sehr störanfälliges Medium. Dann gibt es noch die Halfrate-Spezifikation, bei der sogar nur 6,5 kBit/s zur Verfügung stehen - nicht von ungefähr gibt es daher bei

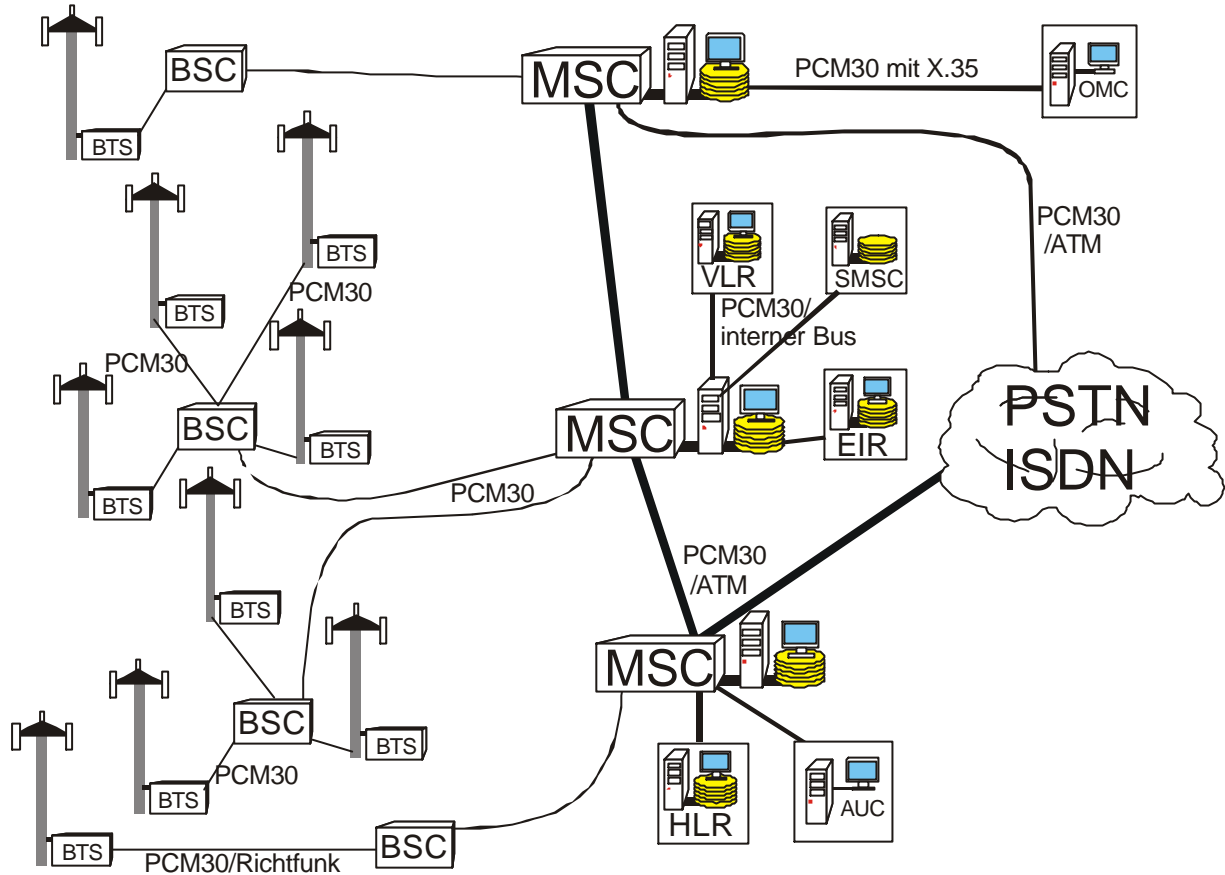


GSM inzwischen 15 verschiedene Kompressionsalgorithmen.

Sprache wird bei GSM in Häppchen von 20ms Länge verarbeitet. Die Kodierer unterscheiden die Sprache in sehr wichtige, wichtige und weniger wichtige Bits. Diese Gruppen werden unterschiedlich stark gegen Fehler gesichert. Zusätzlich werden sie noch über mehrere Zeitschlitz verteilt, so daß ein

ausgefallener Zeitschlitz noch keine Unterbrechung bewirkt. Durch das Frequency hopping bei GSM werden die 20ms Sprache noch auf mehrere Frequenzen verteilt. Da die Frequenzen unterschiedlich stark gestört sind, sind die Kanäle im Mittel alle gleich stark/wenig gestört, und eine erfolgreiche Übertragung fast immer möglich. Sollten doch einmal mehrer Zeitschlitz hintereinander ausfallen, reagiert der Dekoder mit Wiederholung bzw. Extrapolation der letzten intakten Informationen. Nach 16 ausgefallenen Zeitschlitz wird die Verbindung stumm geschaltet. Die Kür dieser Disziplin ist es Sprechpausen ausfindig zu machen und deren Kapazität dem Rest zukommen zu lassen. Der Gesprächspartner hört in dieser Zeit ein sogenanntes Comfort Noise um nicht durch die digitale Stille irritiert zu werden.

Aufbau eines GSM-Netztes



AC - Authentication Center (auch AUC)
 BSC - Base Station Controller
 BTS - Base Transceiver Station
 EIR - Equipment Identity Register
 GSM - Global System for mobile Communication
 HLR - Home Location Register
 MS - Mobile Station
 MSC - Mobile Switching Center

SIM - Subscriber Identity Module
 SMS - Short Message Service
 TDMA - Time Division Multiple Access
 TMSI - Temporary Mobile Subscriber Identity
 VLR - Visitor Location Register
 SMSC - Short Message Service Center
 TCE - Transcodin Enquipment (auch TRAU)
 INE - Inter Networking Equipment

IMEI - International Mobile Equipment Identity

Diese Nummer identifiziert weltweit eindeutig eine MS (Mobile Station). Auf diese Weise ist es möglich ein geklautes Handy wertlos zu machen oder etwa das Mißbrauchen des Notrufs zu ahnden. Anscheinend läßt sich die IMEI leicht fälschen.

IMSI - International Mobile Subscriber Identity

Die IMSI-Nummer setzt sich aus mehreren Teilnummern zusammen und dient zur internationalen Identifizierung von GSM-Mobilteilnehmern. MCC-MobileCountryCode, MNC-MobileNetworkCode, HLR-Nummer + SN-SubscriberNumber

TMSI - Temporary Mobile Subscriber Identity

Die TMSI-Nummer ist eine temporäre Nummer, die zur Signalisierung auf der Funkschnittstelle dient, und hat daher nur eine begrenzte Gültigkeitsdauer sowie eine lokale Bedeutung. Auf diese Weise wird vermieden, daß die IMSI über die Luft wandert und ein Bewegungsprofil möglich wird. Die TMSI-Nummer wird im VLR und auf der SIM-Karte gespeichert.

MSRN - Mobile Station Roaming Number

Die MSRN-Nummer ist eine vom VLR der Mobile Station MS zugewiesene Nummer. Sie bleibt während eines Gesprächs für jene Zeit aufrecht, die die MS im Wirkungsbereich dieses VLRs verbringt. Die MSRN-Nummer setzt sich aus mehreren Teilnummern zusammen und dient zur internationalen Lokalisierung von GSM-Mobilteilnehmern: VCC - Visitor Country Code, VNDC - Visitor National Destination Code, SN - Subscriber Number VMSC - Visitor Mobile Switching Center + VSN - Visitor Subscriber Number

Base Transceiver Station (BTS)

Die BTS oder auch Basisstation versorgt unmittelbar eine oder mehrere Funkzellen. Zumeist werden Sektorantennen verwendet, die einen Bereich von 120° ausleuchten. Die Sendeleistung liegt bei 0,5- 20 Watt bzw. 2,5-50 Watt. Neben dem Mast befindet sich am Boden die eigentliche BTS. Sie enthält Komponenten zur Modulation und Kodierung der Signale, zur Fehlerkorrektur, zum Nachregeln der Sendeleistung. Ebenfalls in der BTS wird die Fehlerkorrektur, Ver-/ Entschlüsselung für die Luftschnittstelle und das Verpacken von je vier GSM- in einen PCM30-Kanal durchgeführt. Die Verbindung zur BSC wird in der Regel mit PCM30 oder Richtfunkstrecken realisiert.

Base Station Controler (BSC)

In der BSC befinden sich die Steuerungen, Kontroll- und Überwachungsmechanismen für mehrere BTSen. Sie steuert die Pegel und weitere Sendeparameter der BTSen. Eine weitere Aufgabe ist der lokale Handover - also wenn ein Nutzer von einer Zelle zur nächsten wechselt, und diese ebenfalls unter der Kontrolle dieser BSC ist. Bei einem nichtlokalen Handover delegiert die BSC alles weitere an ihre MSC. BSCs sind i.d.R über mehrere PCM30-Strecken an ihre MSC angebunden.

Transcoding Equipment (TCE)

Die Sprach- und Signalisierungsdaten auf der Luftschnittstelle werden mit nur 16 kBit/s (13 kBit/s Sprache, 3 kBit/s Steuerinformationen) übertragen. Das TCE führt daher eine Bitratenanpassung an die im Festnetz üblichen 64 Kbit/s durch. Logisch gehört das TCE zwar zum Basestation Subsystem, um teure Leitungskapazität einzusparen wird das TCE aber eher nahe dem MSC aufgestellt.

Home Location Register (HLR)

Jeder MSC sind immer ein HLR zugeordnet. Im Home Location Register sind sämtliche Teilnehmerdaten gespeichert. Es enthält Daten über das Vertragsverhältnis des Teilnehmers, seine Rufnummern, Tarife, sowie Informationen über zugelassene Dienste. Wenn sich ein Teilnehmer einbucht, wird im HLR zusätzlich verzeichnet in welchem VLRs sich seine temporären Daten befinden. In einem GSM-Netz kann es durchaus mehrere HLR geben. An welches HLR eine MSC sich dann wenden muß kann sie aus der IMSI (Nummer der SIM-Karte) herausfinden (HLR-Feld).

Visitors Location Register (VLR)

Das VLR ist eine Datenbank und speichert Informationen über die eingebuchten Teilnehmer der angeschlossenen MSCen. Gespeichert wird die Telefonnummer, die IMSI, eine Roaminginformation, Sicherheitsinformation und eine TMSI (Temporary Mobile Subscriber Identity). Zur Sicherheit wird die Mobilstation nicht mit ihrer IMSI identifiziert sondern mit der TMSI. Fast alle Anbieter spendieren jedem MSC ein eigenes VLR, da die beiden einen regen Datenaustausch pflegen. Bewegt sich ein Teilnehmer, oder bucht er sich wieder ein, wird im VLR ein Location Update durchgeführt. Wenn der Teilnehmer dabei in den Bereich einem neuen MSC gelangt (Handover), werden vom HLR die Daten zum VLR der neuen MSC geschickt. Im HLR wird im gegenzug die Nummer dem neuen MSC verzeichnet. Ist ein Teilnehmer einige Tage nicht mehr aktiv, so wird er aus dem VLR gelöscht. MSC und eigene VLR sind i.r.R. im gleichen Rack.

Mobile Service Switching Center (MSC)

Dies ist die eigentliche Vermittlungsstelle im Mobilfunknetz. Ein MSC besteht im wesentlichen aus einer Prozessorkarte, Hilfsperipherie und einem Koppelfeld. Dazu gesellen sich noch Festplatten und andere Peripherie - alles i.d.R. redundant ausgelegt. Je nach Wunsch wird dort dann zusätzliche Software für VLR, HLR, AUC und EIR installiert. Das Koppelfeld erledigt SW-gesteuert die tatsächliche Vermittlung. Das MSC macht die Routenplanung, schaltet Verbindungen und übernimmt die komplette

Anrufverwaltung, Ortsverwaltung, Handoversteuerung und die Realisierung von GSM-Merkmalen. Für diese Zwecke sind dem MSC mehrere Funktionseinheiten angeschlossen, die auf Anfrage des MSC Dienste erledigen oder bestimmte Daten liefern. Die MSCen sind untereinander über PCM30 -Strecken verbunden oder sind gleich am ATM-Backbone des Betreibers. Wenn ein MSC einen Anschluß an das Festnetz oder an andere GSM-Netze hat, was i.d.R. alle haben, nennt man es Gateway MSC.

Equipment Identity Register (EIR)

Ursprünglich bestand die Idee alle IMEI-Nummern in einer eigenen Datenbank zu speichern. Das EIR hat drei Listen, die weiße, die graue und die schwarze Liste. In der weißen Liste werden alle Geräte eingetragen, die in Ordnung sind und dem Standard des jeweiligen GSM-Netzes entsprechen, in der grauen Liste werden Geräte eingetragen, die für einige Services überprüft werden müssen und in der schwarzen Liste werden die Geräte eingetragen, die zB. als gestohlen gemeldet wurden. Es gibt aber so gut wie keinen GSM-Netzbetreiber das EIR in seiner Netzarchitektur realisiert hat, da die IMEI-Nummern sehr leicht manipulierbar sind und somit der Sinn des EIR verloren geht.

Short Message Service Center (SMSC)

SMSC sind für Speicherung und Zustellung von Kurznachrichten zuständig. Es kann mehrere SMSC geben. Ein SMSC wird per PCM30 über eine MSC in das GSM-Netz integriert. SM werden mit dem Signalisierungsprotokoll SS7 übertragen.

Authentication Center (AC)

Damit das Netz seine Dienste zur Verfügung stellen kann, muß sich die Mobilstation gegenüber dem Netz authentifizieren und identifizieren. Dazu wird im AC eine Zufallszahl erzeugt und an die SIM-Karte übermittelt. Die SIM-Karte berechnet aus der Zufallszahl und aus einem der Karte und dem AC bekannten Schlüssel eine Antwort. Diese wird dann im AC verifiziert. Aus diesen Informationen wird auch der Schlüssel für die Verschlüsselung auf der Luftschnittstelle gewonnen. AC und HLR sind i.d.R auf derselben Workstation realisiert.

Operations and Maintenance Center (OMC)

Das OMC ist quasi das Cockpit des GSM-Netzes. Hier können Parameter für alle Komponenten des Netzes festgelegt werden. Es dient zur Behebung von Störungen, Einspielen von Softwareupdates, Routenplanung und es erfasst statistische Daten zur Netzauslastung etc. Bei einem OMC handelt es sich eigentlich nur um eine Software, die überall installiert werden kann und per X.25 oder per IP mit dem Netz kommuniziert.

GSM Prozeduren

Authentifizierung und Verschlüsselung

Bei der Authentifizierung kommt ein sog. Challenge-Response-Verfahren zum Einsatz. Zu diesem Zweck generiert das AC nach dem Zufallsprinzip eine 128 Bit lange Zahl RAND (Random Number). Bei der Länge von 128 Bit gibt es etwa $3,4 \times 10^{38}$ verschiedene Möglichkeiten, sodass ein zweimaliges Auftreten der gleichen Zahl – hier der gleichen Frage – sehr unwahrscheinlich ist. Die Zahl RAND wird an die MS übertragen. Dort wird in der SIM-Karte die Zahl RAND zusammen mit einem geheimen teilnehmerspezifischen Schlüssel Ki in dem ebenfalls geheimen Algorithmus A3 verarbeitet. Das Ergebnis, der 32 Bit lange Wert SRES (Signed Response), wird ans Netz zurückgegeben. Im AC wird der Wert SRES ebenfalls berechnet. Das Netz vergleicht die beiden Werte und nur wenn sie übereinstimmen wird der Mobilstation die Zugangsberechtigung erteilt. Die MS verwendet im Folgenden dann den Schlüssel Ki zur Verschlüsselung der Funkverbindung. Außerdem bekommt sie vom VLR noch eine temporäre

Nummer (TMSI), die die MS zur weiteren Identifizierung nutzt. Die TMSI wird in kurzen Intervallen erneuert.

Datenübertragung im GSM-Netz

Für Datendienste stehen im GSM zwei Protokolle zur Verfügung: V.32 und V.110. Bei GSM-internen Übertragungen erfolgt eine automatische Erkennung. Bei einer Verbindung vom GSM zu einer ISDN-Karte kommt das Protokoll V.110 zum Einsatz. V.110 ist ein Bitratenadaptionsprotokoll, das die konstanten 64 kBit/s des ISDN mit entsprechend vielen Füllbits versieht. An der Schnittstelle zwischen GSM und Festnetz sitzen sog. INEs (Inter Networking Equipment), die die Bitratenanpassung und die eigentliche Kommunikation mit der ISDN-Karte durchführen. Da V.110 keine 13 kBit/s kennt belibt man auf 9,6 kBit/s beschränkt. Baut man vom GSM aus eine Verbindung zu einem Festnetzmodem auf, kommt V.32 zum Einsatz. Die Datenübertragung bis zur Schnittstelle zwischen GSM und Festnetz erfolgt natürlich weiterhin digital. Erst die o.g. Wandlerbausteine bauen eine Verbindung zu dem Zielmodem auf (über ISDN). Diese IWEs sind idr. bei einer MSC.

Einbuchen

Bei der Location Registration passiert zunächst nur auf Mobilseite etwas. Das Mobiltelefon beginnt auf den vorgesehenen Frequenzbändern zu lauschen und synchronisiert sich dabei auf eine Trainingsfolge in einem der Steuerkanäle. Hat es das geschafft, lauscht es auf anderen Steuerkanälen nach der Länder-, Anbieter- und Ortskennung. Hat es den eigenen Anbieter oder einen auf der SIM-Karte verzeichneten gefunden, wählt es diesen aus. Ansonsten wählt es einen per Zufall. Jetzt erst sendet die Mobilstation ihre IMSI und die Ortskennung an das BTS. Anhand der Kennziffern der IMSI wird das AC und HLR ausfindig gemacht, bei dem sich die Mobilstation authentifizieren muß. Nach erfolgreicher Authentifizierung wird im örtlichen VLR ein Datensatz angelegt und im heimischen HLR die Nummer des örtlichen VLRs eingetragen. Die Mobilstation bekommt vom VLR, nun bereits verschlüsselt, noch eine Temporäre Identität (TMSI) und eine Roamingnummer (MSRN). Wenn die MS nur kurz ausgeschaltet war, sendet sie ihre alte TMSI und es erfolgt im VLR lediglich eine Aktualisierung.

Anruf von A zu B

Anrufer A wählt die Nummer von Teilnehmer B. MS-A signalisiert nun seinem MSC (über BTS, BSC) daß sie eine Verbindung zu Teilnehmer B wünscht. Das MSC prüft ob die TMSI gültig ist und ob der angeforderte Dienst zugelassen ist. Nun extrahiert das A-MSC aus der MSISDN (Telefonnummer) das Zielland und den Zielbetreiber. Als nächstes baut das A-MSC evtl. eine PCM-Verbindung zum GMSC von B auf und delegiert die weitere Arbeit an selbiges. Das GMSC hat auch nur die MSISDN zur Hand, kann aber das zuständige HLR herausfinden (HLR-Feld). Im HLR steht die MSRN (Roaminginfo). Daraus kann das GMSC dann die (international eindeutige) SS7-Adresse des B-MSC extrahieren. Dem B-MSC wird nun vom GMSC As Wunsch B anzurufen mitgeteilt. Daraufhin sucht das B-MSC aus seinem VLR das richtige BSC, signalisiert ihm den Verbindungswunsch und reserviert per SS7 auch gleich eine Verbindung dorthin. Das BSC gibt nun auf die Paging-Kanäle seiner BTSen ein Rufsignal für die B-MS, welche sich daraufhin bemerkbar macht. Sobald der Teilnehmer den Anruf annimmt wird die reservierte Verbindung entgeltlich aufgebaut. Aus dieser Vorgehensweise ergibt sich auch Folgendes: Sind zwei Teilnehmer per Roaming in einem fremden Netz und rufen sich an, so wird für den Anruf eine multinationale Verbindung aufgebaut.

IMSI-Catcher

Ein Fehler des GSM-Netzes ist, daß sich zwar die SIM-Karte/Teilnehmer gegenüber dem Netz authentifiziert, aber das Netz nicht gegenüber dem Teilnehmer. Dadurch ist es mit einem IMSI-Catcher möglich, einer SIM-Karte einen Netzbetreiber vorzugaukeln. Dadurch kommt man an sensible Daten der Karte. Mit diesen Daten ist es möglich eine Kopie anzufertigen.

Ergänzung

Das Billing wird durch Auswerten von Logdateien der MSCen gemacht (Perlskripte?)

Fragen

1. Worin unterscheiden sich GSM, GPRS und EDGE ?

GSM ist verbindungsorientiert, GPRS dagegen paketorientiert. EDGE erlaubt durch ein anderes Modulationsverfahren als GSM/GPRS höhere Datenraten.

2. In einem GSM-Netz können beliebig viele HLRs (Home Location Register) sein. Woher weiß „das Netz“, in welchem HLR es nach den Teilnehmerdaten zu suchen hat?

Auf der SIM-Karte des Teilnehmers befindet sich als wichtigste Nummer die IMSI (International Mobile Subscriber Identity). Diese enthält u.a. ein Feld HLR, die einen Teilnehmer einem HLR zuordnet.

3. Was für eine Route nimmt die Verbindung, wenn zwei Teilnehmer im Fremdnetz direkt nebeneinander stehen, und Teilnehmer A ruft Teilnehmer B an?

Das A-MSC baut eine Verbindung in Bs Heimat auf. Das dortige GMSC ermittelt Bs Position und baut nun eine Verbindung zu B auf.

Linksammlung:

GSM-Association: <http://www.gsmworld.com/>

GSM: <http://umtslink.at/GSM-Start.htm>

GSM: <http://www.physik.uni-erlangen.de/Didaktik/vortrag/kolb/handy.pdf>

GSM-R: <http://www.senderlisteffm.de/gsm-r.html>

GSM-R: <http://www.telko-net.de/heftarchiv/pdf/2001/fs1601/fs0116056.pdf>

Sprachkodierung: <http://webserver.et.fh-merseburg.de/informat/vortrag/17-06-98/17-06-98.pdf>

Sprachkodierung: <http://home.arcor-online.de/atzeat/mf/gsmtech.htm#GSMTechSysArchitektur>

Zellgrößen bis 120km: <http://www.funkschau-handel.de/heftarchiv/pdf/1998/fs16/fs9816034.pdf>

DAtenFUunk: <http://www.dafu.de/redirect/redirect-datens.html>

GSM-verschlüsselung: <http://de.gsmbox.com/gsm/tecnologia/index.gsmbox>

GSM-Verschlüsselung geknackt: <http://www.teltarif.de/arch/1999/kw49/s1170.html>

GSM-Verschlüsselungsmängel: <http://www.ccc.de/congress/1998/doku/281298-gsm.html>

SIM-Karten ausgelesen: <http://www.heise.de/newsticker/data/dz-07.05.02-000/>

IMSI-Catcher: <http://www.vieweg.de/dud/dud/imsicatc.htm>

PCM30: http://home.zhwin.ch/~kls/pdf_kt/kap_9.pdf

SS7-Protokoll http://www.nokia.ch/german/download/pr/html/Nokia_Avenue_d_000223.htm

Bilder von Sendern: http://www.nobbi.com/gallery_tf.htm

Betreiberkennziffern: http://www.umtslink.at/GSM/operatorliste_gsm.htm

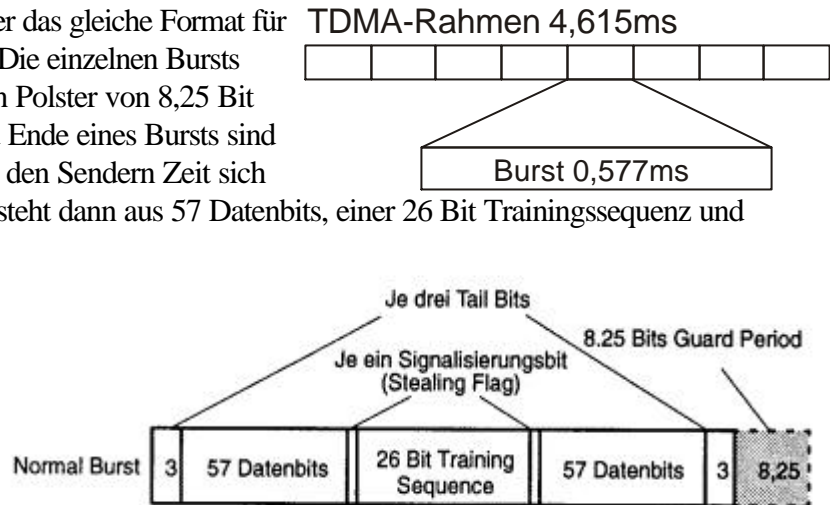
Haftungsausschluß

Das Wissen wurde mit aller Sorgfalt und bestem Wissen und Gewissen hier für diesen Vortrag zusammengestellt. Fehler sind also mitnichten gewollt und im Zweifelsfalle einfach falsch abgeschrieben.

Das hatte keinen Patz mehr.

Rahmenstruktur

Unabhängig vom Dienst kommt immer das gleiche Format für Zeitschlitz bzw. Bursts zum Einsatz. Die einzelnen Bursts eines TDMA-Rahmens sind durch ein Polster von 8,25 Bit voneinander getrennt. An Anfang und Ende eines Bursts sind noch einmal 3 sog. Tailbits. Sie geben den Sendern Zeit sich einzupegeln. Der eigentliche Burst besteht dann aus 57 Datenbits, einer 26 Bit Trainingssequenz und weiteren 57 Datenbits. Die 114 Datenbits dienen der Informationsübermittlung, während die Trainingsfolge dazu dient, daß sich die Mobilstation ständig nachsynchronisieren kann.



Erhöhung der Datenredundanz

Bei GSM wird penibel unterschieden zwischen Sprach-, Fax- oder Datenübertragung. Bei Sprache kann eine verlustbehaftete Komprimierung eingesetzt werden und Bitverluste können in der Regel auch auftreten, ohne die Kommunikation unmöglich zu machen. Bei dieser isochronen Übertragung sind im Gegensatz zu Fax keine Wiederholungen von fehlerhaften Rahmen möglich. Bei Fax wären sogar kleine Bitfehler noch passabel. Dagegen sind bei einer Datenübertragung schon kleine Fehler fatal. Dafür sind Wiederholungen von fehlerhaften Daten kein Problem. Die Kodierung und Sicherung gegen Fehler ist daher für die einzelnen Dienste unterschiedlich.

Daten-/FAX-Übertragung

Die Übertragung von Daten ist bei GSM besonders gegen Fehler gesichert. Pro Sekunde steht eine Bruttodatenrate von 22,4 kBit zur Verfügung. Durch die Fehlerkorrekturmaßnahmen bleiben davon noch 12 kBit für Daten (bei Sprache bleiben noch 13 k über). Da es allerdings keinen Standard für diese Datenrate gibt, mußte man bis auf 9,6 kBit/s hinuntergehen. Also GSM hat eigentlich 1/3 mehr Übertragungsleistung als realisiert ist.

Existierende GSM Sprachcodierstandards:

- FR (1987)
 - 13.0 kbit/s
 - RPE-LTP
- HR (1995)
 - 5.6 kbit/s
 - Sprachqualität fast wie FR
 - Komplexität weniger als 4 x FR
 - Technologie: VSELP mit adaptivem Codebuch
 - Multimodal (stimmhaft-/stimmlos- Unterscheidung)
- EFR (1996)
 - 12.2 kbit/s
 - Sprachqualität deutlich besser als FR
 - Komplexität ca. 5 x FR
 - Technologie: ACELP mit adaptivem Codebuch