Ziele

1982 Macht die Nordic PPT der CEPT einen Vorschlag
kompatiblilität mit ISDN
roaming

Spielarten des GSM

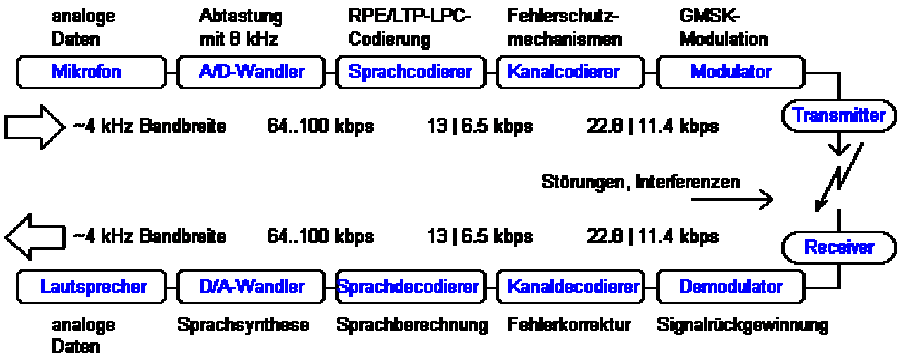
Klassisch GSM 9600
GSM-R - Multicast, auf 800 MHz
HSCSD - verbindungsorientiert, bis zu 43 kBit
GPRS - paketorientiert, 172/56 kbit
EDGE - anderes Modulationsverfahren, bis 384 kbit, 8-PSK
Kombination EDGE+(HSCSD|GPRS)
CorporateGSM - Netze werden gekoppelt

Luftschnittstelle

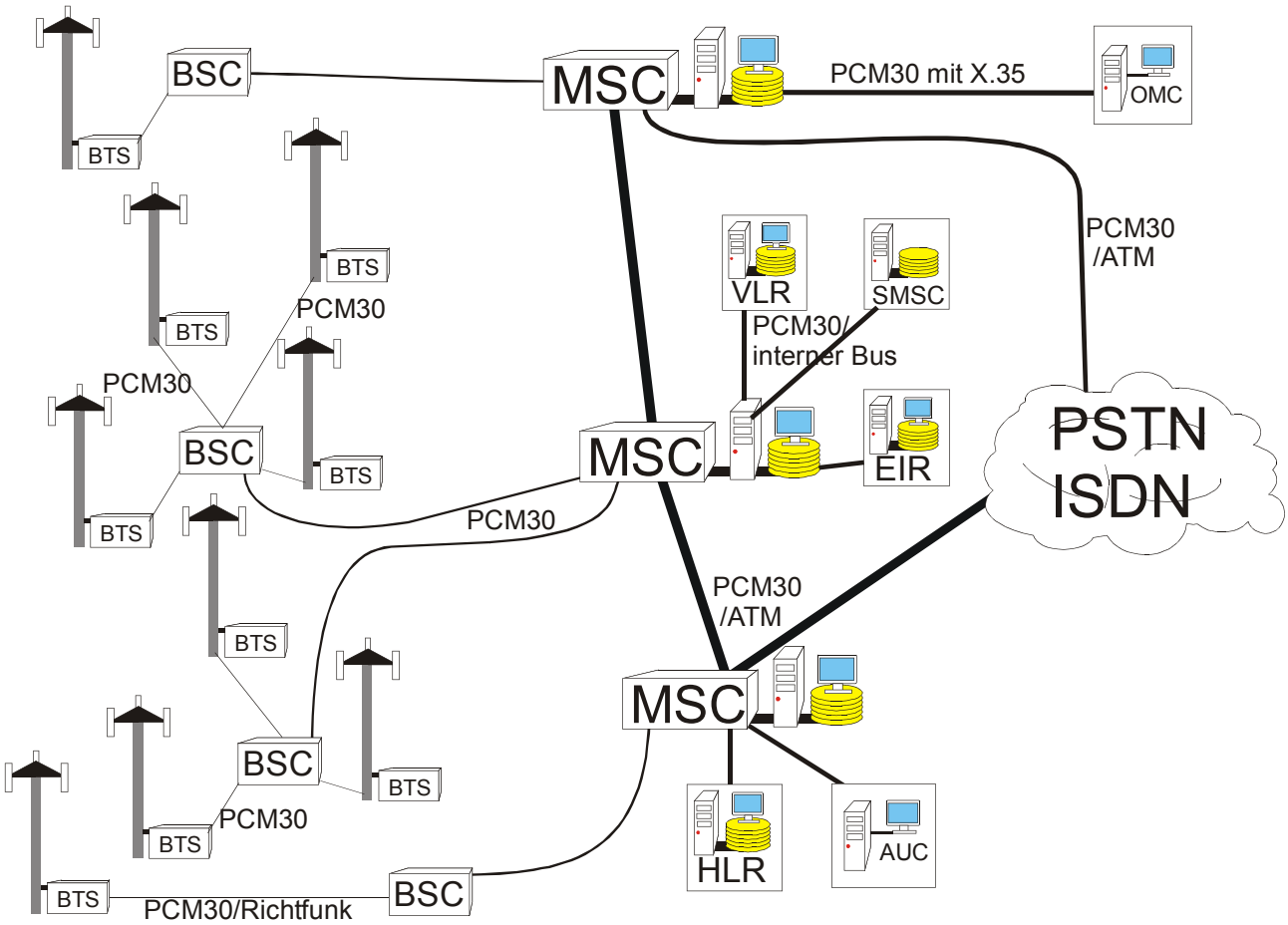
25 bzw 75 MHz Bandbreite für up/downlink
200 kHz Trägerbreite
142 oder 378 trägerfrequenzen
Zellstruktur, Nachberfrequenzen disjukt
7er Cluster nebst 3er 4er 9er 12er

Kodierung

von 64 auf HAlfrate fullrate 13 / 6,4 kbit/s
15 verschiedene algorithmen
in 20ms häppchen verarbeitet
bits in wichtig usw. klassifiziert und unterschiedlich gesichert
info verteilt über mehrere bursts übertragen
frequenzhopping verfahren zur mittelung der störungen
diskontinuierliche übertragung und compfort noise



Netzstruktur



Base Transceiver Station (BTS)

Ist der Antennenturm 2,5-320 W
Macht die Pegelregelung, Fehlerkorrektur, Ver/Entschlüsselung
Verpackt je 4 Kanäle in einen PCM30 Kanal

Base Station Controler (BSC)

Steuerungen, Kontroll- und Überwachungsmechanismen für mehrere BTSen.
lokaler Handover
mit mehreren PCM30 an MSC verbunden

Transcoding Equipment (TCE)

Bitratenanpassung von GSM an Festnetzübliche 64k
bei der MSC aufgebaut.

Home Location Register (HLR)

sämtliche Teilnehmerdaten gespeichert
Daten über das Vertragsverhältnis, seine Rufnummern, Dienste.
welcher VLR ist momentan zuständig.

Visitors Location Register (VLR)

speichert temporäre Informationen über die eingebuchten Teilnehmer
Telefonnummer, die IMSI, eine Roaminginformation, TMSI
MSC und VLR örtlich zusammen betrieben. Sonst per PCM30 an MSC

Mobile Service Switching Center (MSC)

eigentliche Vermittlungsstelle
Rack mit Prozessorkarte, Hilfsperipherie und einem Koppelfeld
Software für VLR HLR AC.
Anrufverwaltung, Ortsverwaltung, Handoversteuerung und Realisierung von GSM-Merkmalen.
PCM30 untereinander oder gleich am ATM-Backbone
alles sind GMSC
i.d.R. redundant ausgelegt.

Equipment Identity Register (EIR)

weiße, die graue und die schwarze Liste
DB für Gerätenummern (IMEI)

Short Message Service Center (SMSC)

SMS senden
per PCM30 an eine MSC angebunden

Authentication Center (AC)

Authenifizierung der Teilnehmer

Operations and Maintenance Center (OMC)

Steuerzentrale. Routenplanung Statistik, Problembehebung
Software per X.25 oder IP am GSM dran

GSM Prozeduren

Authenifizierung und Verschlüsselung

AC generiert 128 Bit lange Zahl RAND
RAND wird an die MS übertragen
SIM-Karte die Zahl RAND mit Schlüssel Ki, Algorithmus A3 verarbeitet
Ergebnis, der 32 Bit lange Wert SRES zurückgegeben.
Im AC wird SRES verglichen
Ki zur verschlüsselung der Luftschnittstelle

Datenübertragung im GSM-Netz

zwei Protokolle zur Verfügung: V.32 und V.110
GSM zu einer ISDN-Karte : V.110
GSM zu einem Festnetzmodem: V.32
V.110 ist ein Bitratenadaptionsprotokoll
Wandlerbausteine (IWE) machen die eigentliche Kommunikation

Einbuchen im Innland

Location Registration, nur Mobilstationsseite erst.
auf Frequenzbändern lauschen und synchonisieren
Wählt Anbieter
Authentifiziert sicht bei diesem
VLR und HLR werden aktualisiert.
MS bekommt TMSI zugewiesen

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 angefordete 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 entgültig aufgebaut.

IMSI-Catcher

Fehler des GSM-Netzes: Keine symmetrische Authenifizierung.
Daher IMSI-Catcher (Netzemulatoren) möglich.

Billing

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

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, knostante 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 Qwolliti-Netz (neuere CODECs=>bessere Quallität).
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

Kapazität im GSM

	GSM	D1/D2	GSM1800
Träger	124	62	374
Kanäle bei 8 Zeitschlitzen	992	496	2992
Kanäle bei 16 Zeitschlitzen	1984	992	5984
Kanäle pro Zelle bei 7er-Cluster und 8 Zeitschlitzen	141,71	70,86	427,43
Bei 7er-Cluster und 16 Zeitschlitzen	283,43	141,71	854,86
Zu beachten ist, daß ein Träger jeweils für Steuerkanäle reserviert ist und daher nicht für Gespräche nutzbar ist.