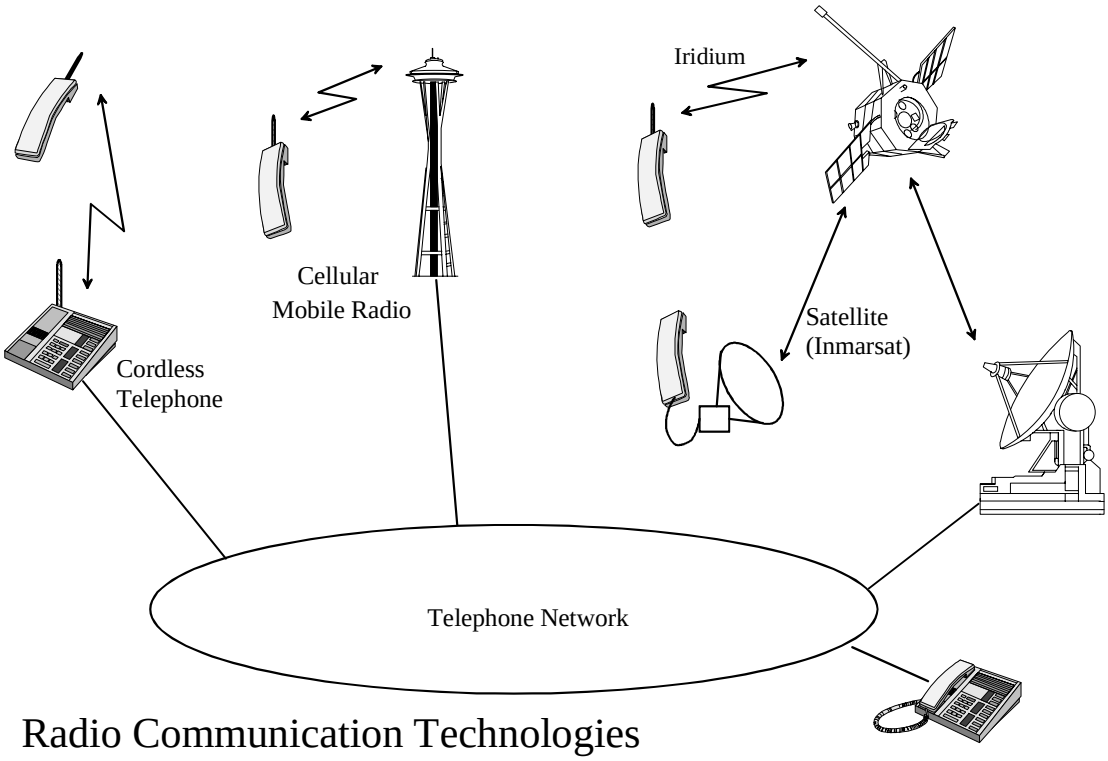
GSM

Global System for Mobile communication

alfons.eizenhoefer@fh-nuernberg.de

1 Introduction



Radio Communication Technologies

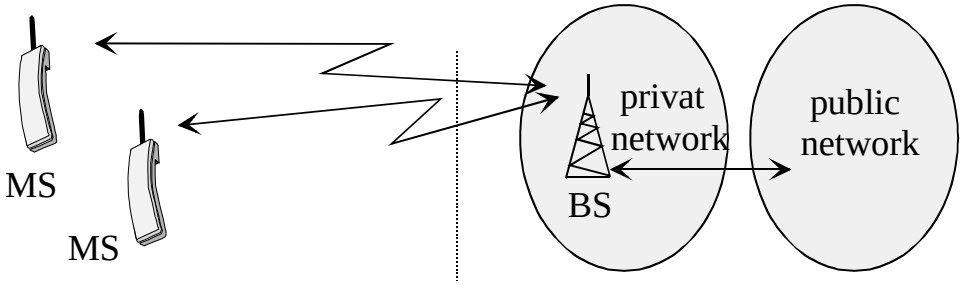
1.1 Services

Dialogdienste	Funkstrecke	System Area	Kommunikationsreichweite
Schnurloses Telefon	100m	Haus, Firma	Telefonnetze
Wireless LAN	20 m	Firmengelände	Firma, Filialen, Internet
Bündelfunk, PMR	50 km	Region	Region, Telefonnetz
Datenfunk	50 km	Land	X.25 Netze, Internet
Mobilfunk	30 km	Länder	Telefonnetze
Richtfunk	50 km	kein System	kein Teilnehmer Zugang
Satellitenübertragung	10.000 km	kein System	kein Teilnehmer Zugang
Satellitenkommunikation	10.000 km	weltweit	Telefonnetze

Verteildienste	Funkstrecke	System-Reichweite
Radio	50 km, 10.000 km	Land, Europa
Fernsehen	50 km, 10.000 km	Land, Europa
Uhrzeit	1000 km	1000 km
Ortung	10.000 km	weltweit
Paging	100 km	Land

1.2 Radio Systems

Private (Professional) Mobile Radio PMR

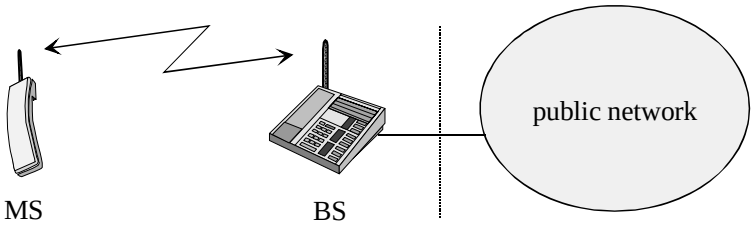


Viele analoge Systeme bei Polizei, Feuerwehr, Rettungsdienste, Taxi, Fuhrunternehmen

ETSI Standard: Tetra, Trans European Trunked Radio, digital PMR System

Cordless telephone

Cordless telephone
MS = Mobile Station
BS = Base Station
private system
full duplex



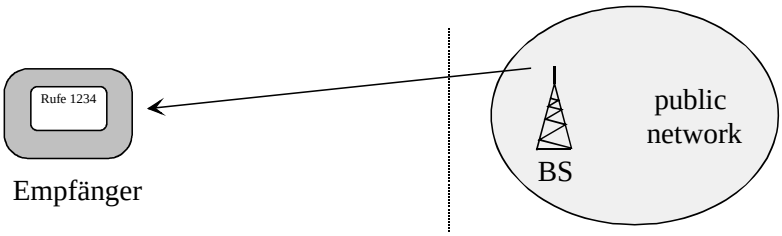
	CT1 plus	CT2 / CAI	DECT
Frequenzbereich [MHz]	885-887 up 930-932 down	864-868	1880-1900
FDMA-Faktor (Carrier)	80	40	10
TDMA-Faktor	1	1	12
Nutzkanäle	80	40	120
Modulation	analog FM	FSK, Gausfilter	GMSK (BT=0,5)
Duplexverfahren	FDD (45 MHz)	TDD	TDD
Sendeleistung (mittel, max.)	10 mW	5 mW / 10 mW	10 mW / 250 mW
Sprachcodierung	analog	ADPCM, 32 kb/s	ADPCM, 32 kb/s

Paging (Europäische Systeme)

Paging:

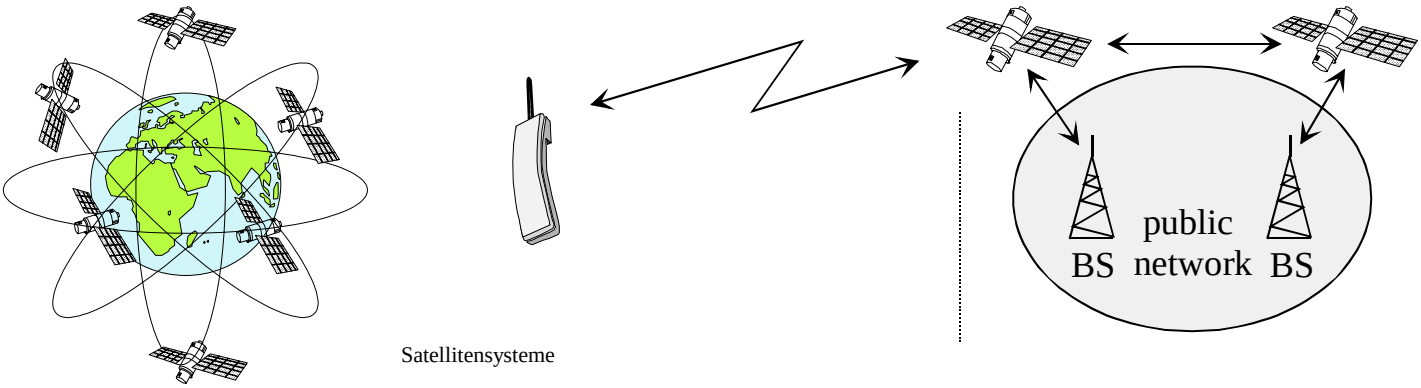
public system

simplex (not broadcast !)



	Eurosignal	Cityruf (POCSAG)	ERMES
Frequenzbereich [MHz]	87	467	169,4 - 169,8
Kanalzahl	2	3	16
Kanalabstand	25 kHz	20 kHz	25 kHz
Modulation	analoge AM	DFSK, 512 und 1200 b/s	4 PAM/FM 6.250 b/s
Sendeleistung	bis 2 kW	bis 100 W	

Satellite Systems



Satellitensysteme

	INMARSAT (ICO)	Globalstar	Odyssey	IRIDIUM
Firma	Inmarsat	Loral/Qualcomm	TRW	Motorola
Bahnhöhe	10.355 km MEO	1410 km LEO	10.355 km MEO	795 km LEO
Satellitenzahl	12	48 + 8 Reserve	12	66 + 7 Reserve
Sprachrate	4,8 kb/s	0,6 - 9,6 kb/s	4,8 kb/s	4,8 kb/s
Datenrate	2,4 kb/s	2,4 - 9,6 kb/s	9,6 kb/s	4,8 kb/s

LEO = low earth orbit; MEO = medium earth orbit

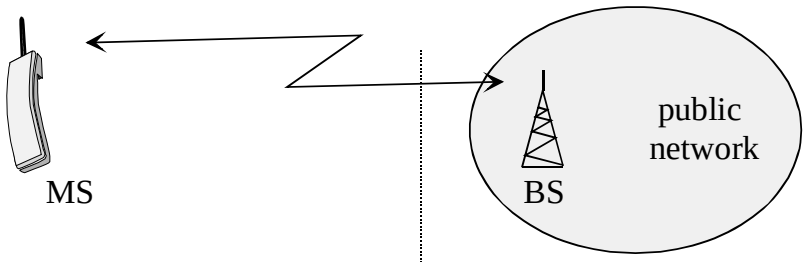
1.3 Mobile Radio Systems in Germany

Mobile Communication (Europe)

Cellular (USA)

public system

duplex



Arbeitgeber im Bereich Mobilfunk in Nürnberg:

D1 T-Mobil	Betrieb D1-Netz, Nordbayern Zentrale Betriebs-Unterstützung, Sondertechnik (SMS) internationale Ausbildungsstelle
D2 Vodafon	Betrieb
E-Plus	Betrieb E1-Netz, Nordbayern
Viag Interkom	Betrieb E2-Netz, Nordbayern und Thüringen
Ericcson	Endgeräte
Lucent	Infrastruktur
Philips TCMC	Endgeräte
Debis	SW für Endgeräte

Mobilfunksysteme

Netz			Zeitraum	Beschreibung
A		analog	1958 - 1977	Handvermittelt, D 156 - 174 MHz
B		analog	1972 - 1994	Halbautomatisch, von PKI, D, GB, NL, ... 146 - 174 MHz
NMT	1. Generation	analog	1981 -	Nordic Mobile Telephone System, vollautomatisch, Handover, 450 und 900 MHz
AMPS	1. Generation	analog	1983 -	wie NMT, USA, American Mobile Phone System 800 MHz
C	1. Generation	analog	1986 - 2000	wie NMT, von Siemens, D, Südafrika, Portugal 450 MHz
D1, D2	2. Generation	digital	1992	erstes digitales System, ETSI-GSM 900 MHz
E1, E2	2. Generation	digital	1994, 1998	wie D-Netz, jedoch 1800 MHz
F	3. Generation	digital	2003	UMTS

Mobilfunksysteme in Deutschland

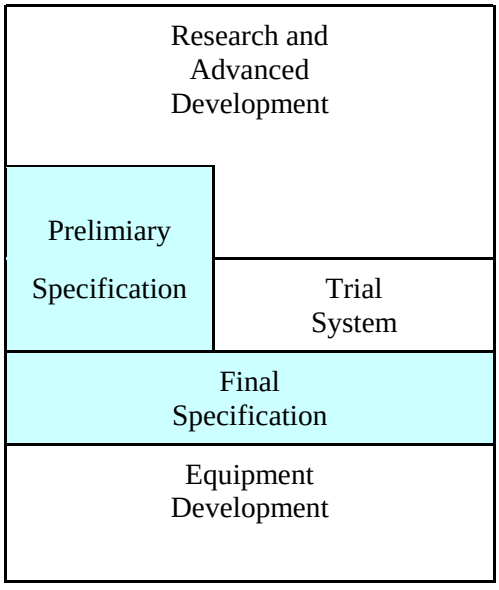
Netz	Frequenz MHz	Kanäle	MS-Power Watt	Funkzellen in Deutschland pro Netz	Teilnehmer Mio.
A	156 - 174	37	10	135	0,011
B	146 - 174	76	10	150	0,027
C	450 - 466	222	12,5	1.800	0,6
D1 + D2	890 - 960	992	10 - 0,8	20.000	je 25
E1 + E2	1710 - 1880	2992	1	30.000	je 10
F	1885-2200		< 0,8	25.000	6 * 5 Mio ???

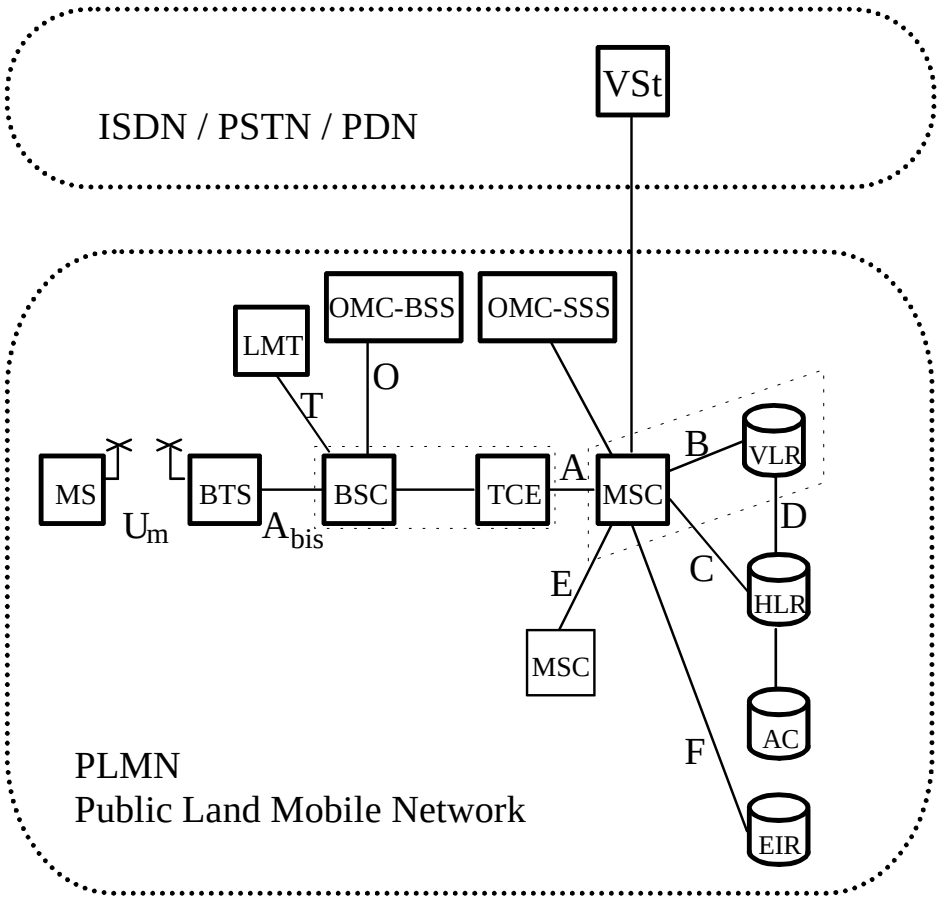
1.4 GSM Overview

Entstehung des GSM-Systems

GSM-Entstehung

1978 Important areas of research:
Digital Modulation: GMSK, TFM; Spectrum economy
Switching functions in cellular systems
1982 Groupe Spécial Mobile GSM setup by CEPT
1984 Foundation of COST 207 (propagation)
Start of trial system development
1986 Comparison of trial systems
1987 EEC Directive: Common Frequency Band in Europe
MoU Set up with 13 Countries
1988 first Letters of intent
1989 GSM becomes part of ETSI
1991 First demonstration system running (Telecom 91 exhibition)
1992 Start of commercial service





GSM System Architecture

2 Radio Propagation

P_S : abgestrahlte Leistung r : Kugelradius

E : elektr. Feldstärke Z_o : Feldwellenwiderstand = 377 Ω

λ : Wellenlänge c = $3 \cdot 10^8$ m/s

Strahlungsfeld: $S = \frac{P_S}{4\pi r^2} = \frac{E^2}{Z_o} \quad \left[W / m^2\right]$

Wirksame Fläche der Empfangsantenne: $A = \frac{\lambda^2}{4\pi} \quad \left[m^2\right]$

Empfangsleistung: $P_E = S \cdot A = \frac{P_S \cdot \lambda^2}{(4\pi r)^2} \quad \left[W\right]$ ⇒ Freiraumdämpfung: 20 dB / Dekade

Freiraumdämpfung für isotrope Strahler: ≈ $1 / r^2$ und ≈ $1 / f^2$ $\quad \frac{P_E}{P_S} = \frac{\lambda^2}{(4\pi r)^2} = \frac{c^2}{(4\pi f r)^2}$

daraus das logarithmische Freiraumdämpfungsmaß (Free space Path loss)

$L_F = 10 \log \frac{P_E}{P_S} = 20 \log \frac{c}{4\pi f r} = 20 \log \frac{c}{4\pi}$ - 20 log f - 20 log r **= 147,56 dB - 20 log f - 20 log r**

	Wellenlänge λ = c / f	20 log f	Free space Path loss
900 MHz	1 / 3 m	179,08	**- 31,52 - 20 log r**
1800 MHz	1 / 6 m	185,1	**- 37,55 - 20 log r**

Funkausbreitung: Feldstärke dBµV/m

E : elektr. Feldstärke µV/m $E^2 = S * Z_0$ Z_O : Feldwellenwiderstand 377 Ω

0 dBµV/m = 1 µV/m $\lambda = c/f$ Wellenlänge $c = 3 \cdot 10^8$ m/s

Beispiel: bei 1.800 MHz wird eine Feldstärke von 40 dBµV/m gemessen.

Welche Leistung nimmt ein isotroper Strahler bei optimaler Anpassung auf ?

0 dBµV/m = 1 µV/m ➔ 20 dBµV/m = 10 µV/m ➔ 40 dBµV/m = 100 µV/m

$E^2 = [100\ \mu V/m]^2 = [10^{-4}\ V/m]^2 = 10^{-8}\ [V/m]^2 = S * Z_0$

$S = E^2 / Z_0 = 10^{-8}\ [V/m]^2 / 377\ \Omega = 2{,}65\ 10^{-5}\ [W/m^2]$

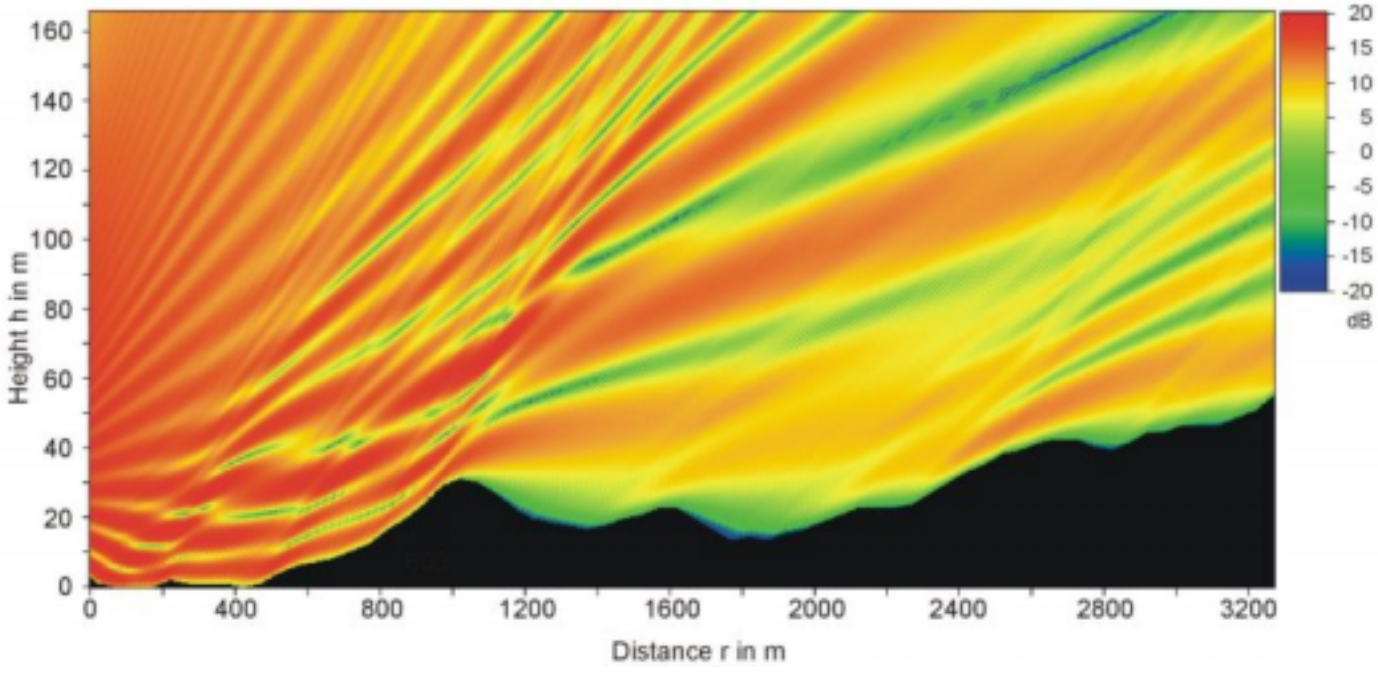
Empfangsleistung: $P_E = S * A$ Wirksame Fläche der Empfangsantenne: $A = \frac{\lambda^2}{4\pi}\ [m^2]$

$\lambda = c / f = 3\ 10^8\ m / 1{,}8\ 10^9\ Hz = 0{,}1666\ m$ ➔ $A = 0{,}166^2\ m^2 / 4\pi = 2{,}2\ 10^{-3}\ m^2$

Empfangsleistung: $P_E = S * A = 2{,}65\ 10^{-5}\ [W/m^2] * 2{,}2\ 10^{-3}\ m^2 = 5{,}85\ 10^{-8}\ W$

$5{,}85\ 10^{-8}\ W = 5{,}85\ 10^{-5}\ mW = 7{,}68\ dB – 50\ dBm =$ **-42,32 dBm**

Example for Wave Propagation over Mountains

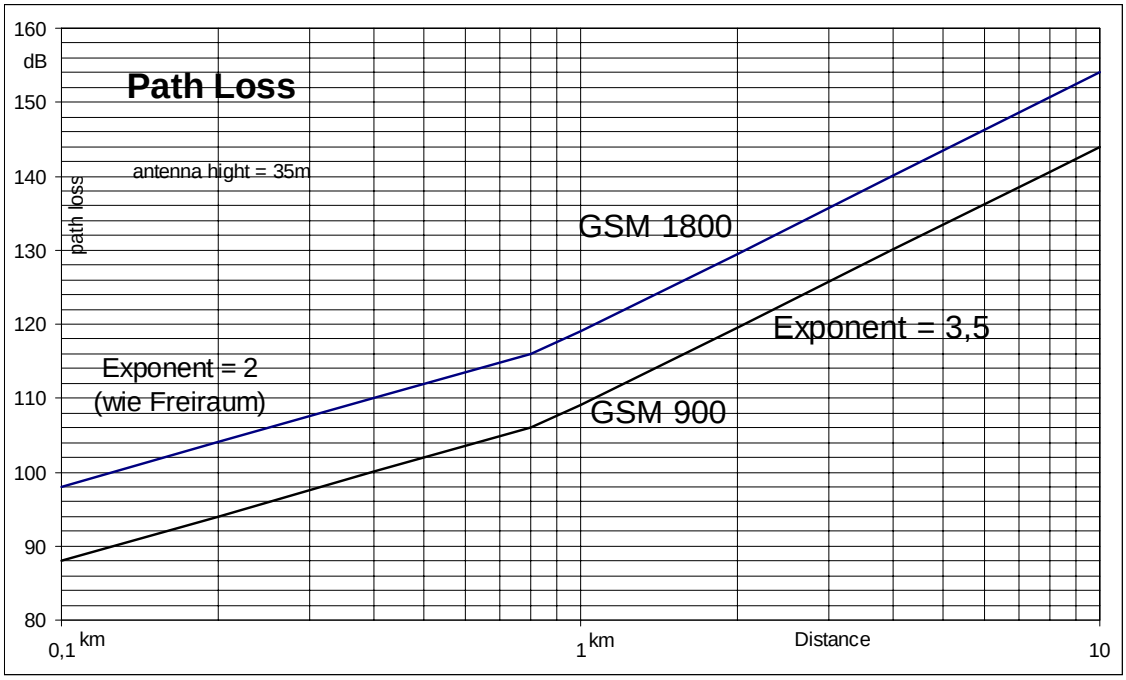


Quelle: http://www.ihf.uni-stuttgart.de/ Institut für Hochfrequenztechnik Uni Stuttgart

2.1 Path Loss

Pathloss L :

$L = a + b \log (r/r_o) = a + b \log (r) - b \log (r_o)$



Aus dem Bild ablesen (Kurve für 1800 MHz in der Stadt):

0,1 bis 1 km: r_0 = 100 m:	L = 98 + 20 log (r[km] / 0,1 km)	a = 98 dBm b = 20 dB/Dekade
ab 1 km: r_0 = 1 km,	L = 118 + 35 log(r[km] / 1 km)	a = 118 dBm b = 35 dB/Dekade

Vergleich GSM 900 / 1800

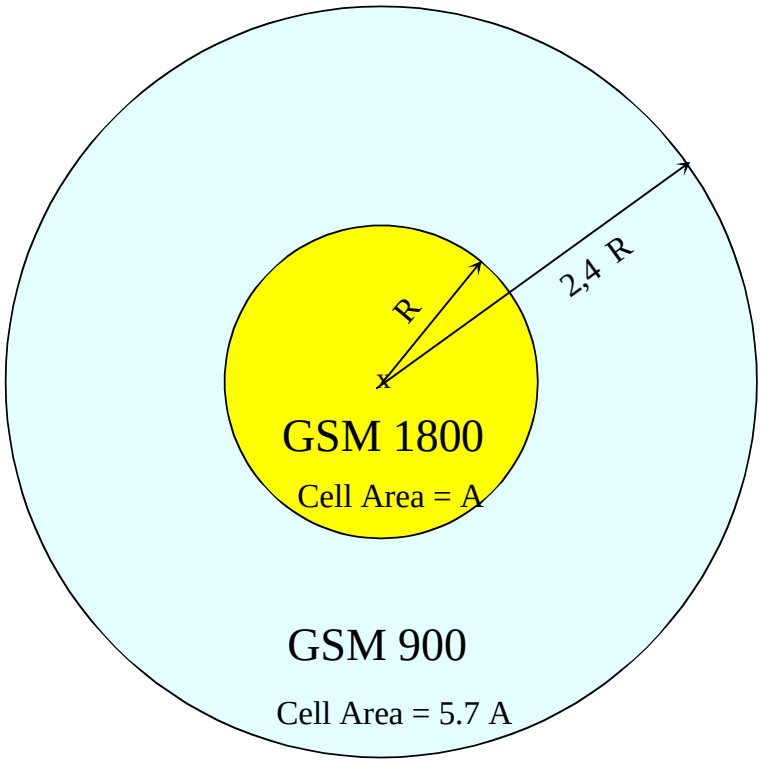
Free space Path loss :

L_F = 147,56 dB - 20 log f - 20 log r

900 MHz	1800 MHz
- 31,52 - 20 log r	- 37,55 - 20 log r

Dämpfungunterschied = 6 dB

In der Praxis rechnet man mit 8 bis 10 dB



Sendeleistung des Handy:

GSM 900: 2 Watt
GSM 1800: 1 Watt

Differenz: 3 dB

2.2 Antenna Gain

Freiraumdämpfung für isotrope Strahler: $\frac{P_E}{P_S} = \frac{\lambda^2}{(4\pi r)^2} = \frac{c^2}{(4\pi f r)^2}$

EIRP effective isotropic radiated power = die vom Kugelstrahler abgegebene Leistung

Andere Antennen haben größere wirksame Antennenfläche, z.B. Hertzscher Dipol = λ/2 - Dipol

Gewinn des Hertzschen Dipols (λ/2) gegenüber Kugelstrahler = 2,15 dB

Die vom λ/2 - Dipol abgegebene Leistung: ERP (effective radiated power) = EIRP + 2,15 dB

Antennengewinn Gain = $\frac{\text{Power density at a distance r in the direction of maximum radiation}}{P_S / 4\pi r^2}$

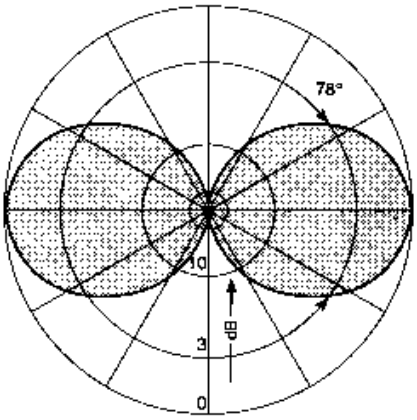
Empfangsleistung: $\frac{P_E}{P_S}$ [dB] = $L_F + G_1 + G_2$

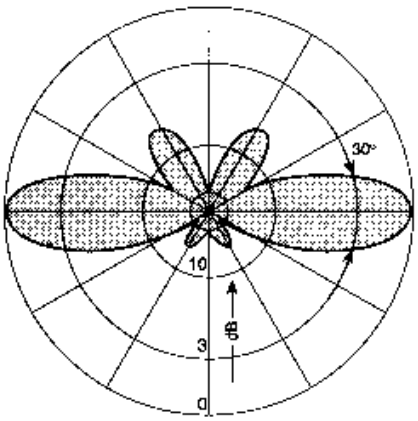
wobei gilt: P_E = Empfangsleistung,
P_S = Sendeleistung,
L_F = Freiraumdämpfung,
G_1, G_2 = Gewinn von Sende- und Empfangsantenne.

Vertical Antenna Patterns
Frequency 806 - 960 MHz

λ/2 Dipole (left)
Length: 348mm
Gain (ref. λ/2 Dipole): 0 dB

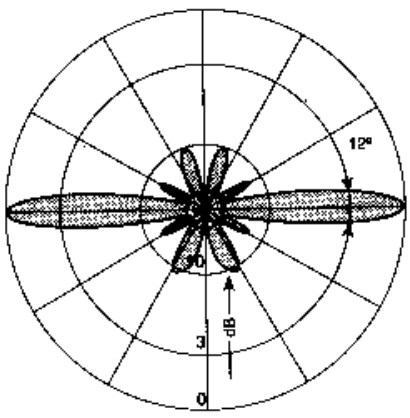
Omnidirectional Antenna (right)
Length: 710mm
Gain (ref. λ/2 Dipole): 3 dB

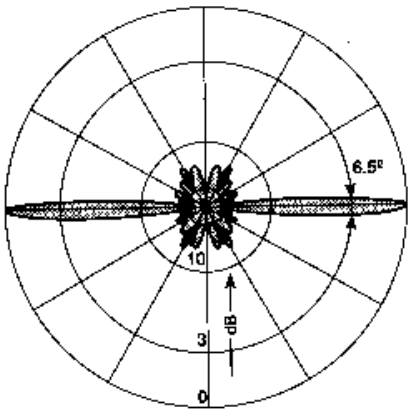




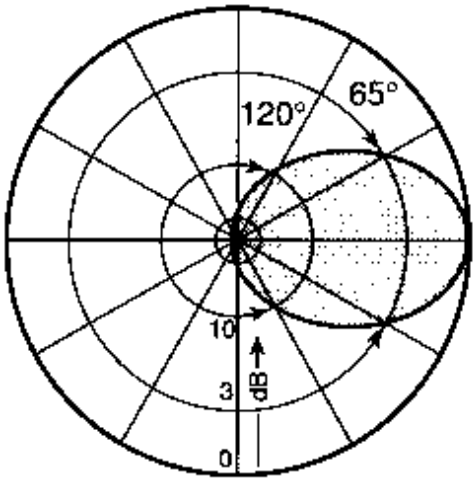
Omnidirectional Antenna (left)
Length: 1800 mm
Gain (ref. λ/2 Dipole): 6 dB

Omnidirectional Antenna (right)
Gain (ref. λ/2 Dipole): 9 dB
Length: 3030 mm

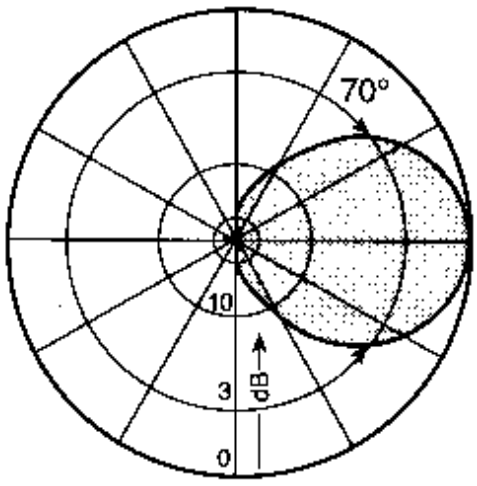




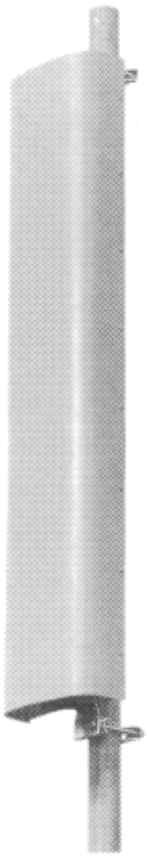
Directional Antenna
860 - 960 MHz
height 260mm
width 255mm
depth 105mm
Gain (ref. λ/2 Dipole): 7 dB



Horizontal Pattern



Vertical Pattern

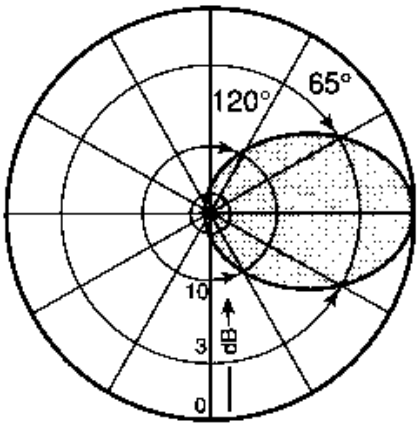


Directional Antenna

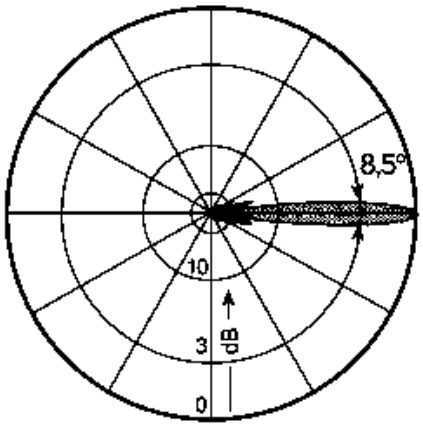
870 - 960 MHz

height 1930mm
width 255mm
depth 105mm

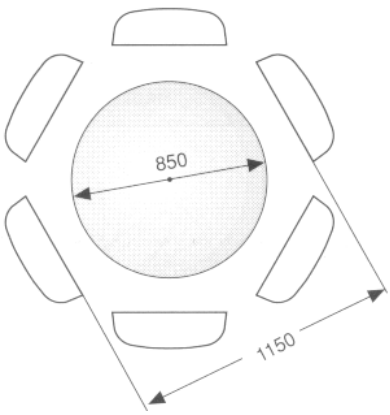
Gain (ref. λ/2 Dipole):
15 dB

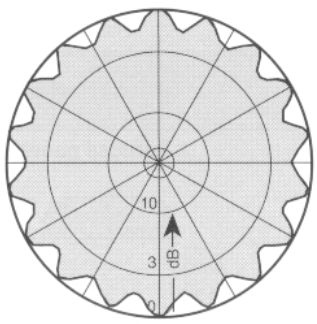


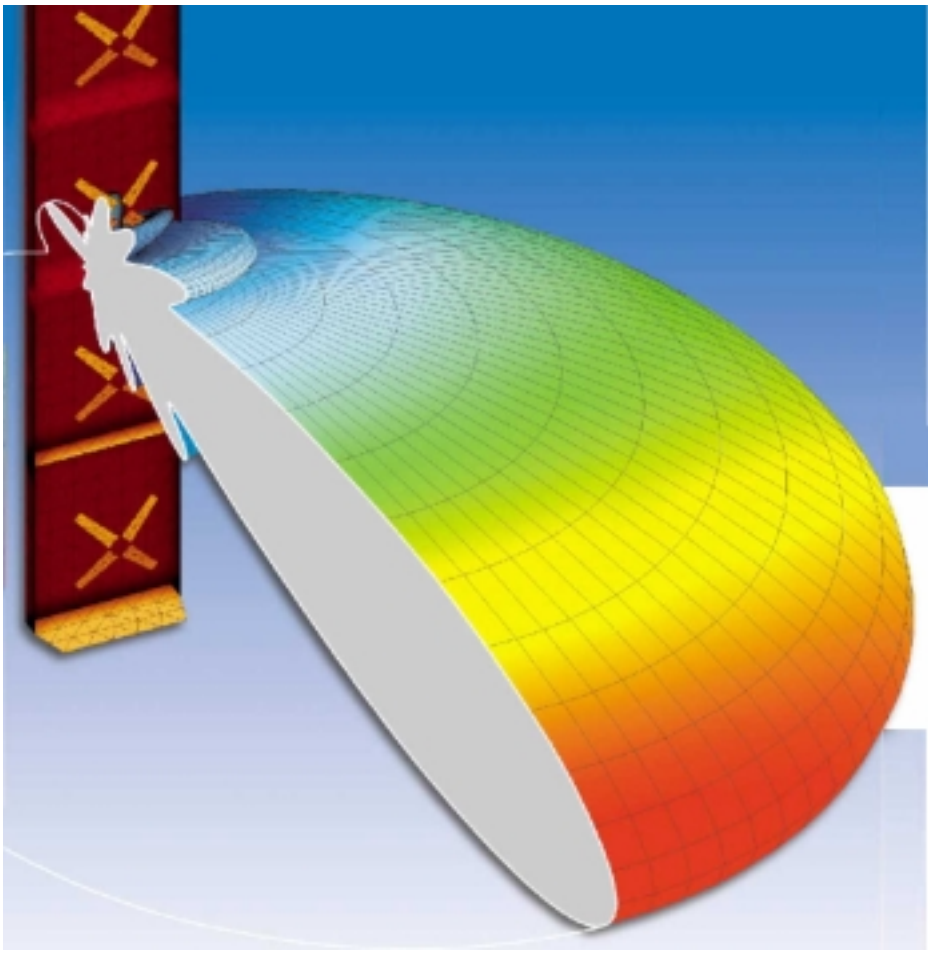
Horizontal Pattern



Vertical Pattern



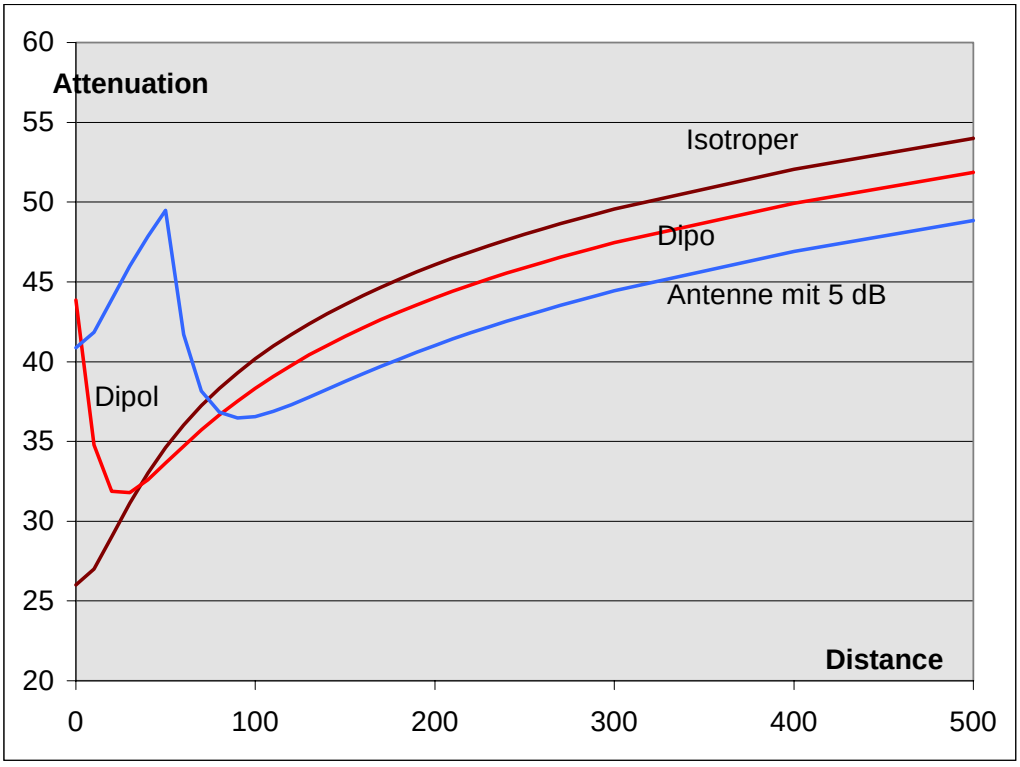




Radiation Pattern of a directional Antenna

Quelle: Kathrein

Vergleich der Dämpfung mit unterschiedlichen Antennen

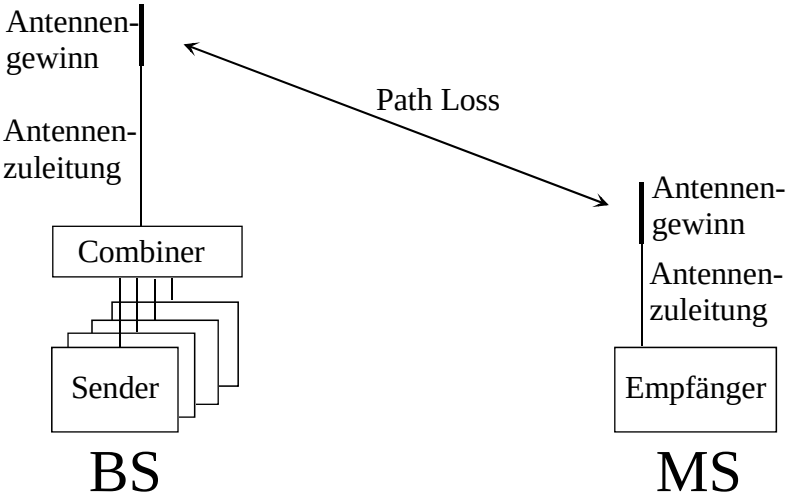


Die gesamte Dämpfung setzt sich zusammen aus

- Ausbreitungsdämpfung
- Antennengewinn
- Richtungsabhängige Dämpfung

2.3 Radio Link Budget

Leistungsbilanz: Downlink



Sendeseite (BS):

Sendeleistung, z.B. 15 W	42	dBm
Combinerverluste	- 3	dB
Verlust im Antennenkabel	- 2	dB
Verbindungsverluste	- 1	dB
Antennengewinn	+ 12	dBi
Abgestrahlte Leistung EIRP	48	dBm

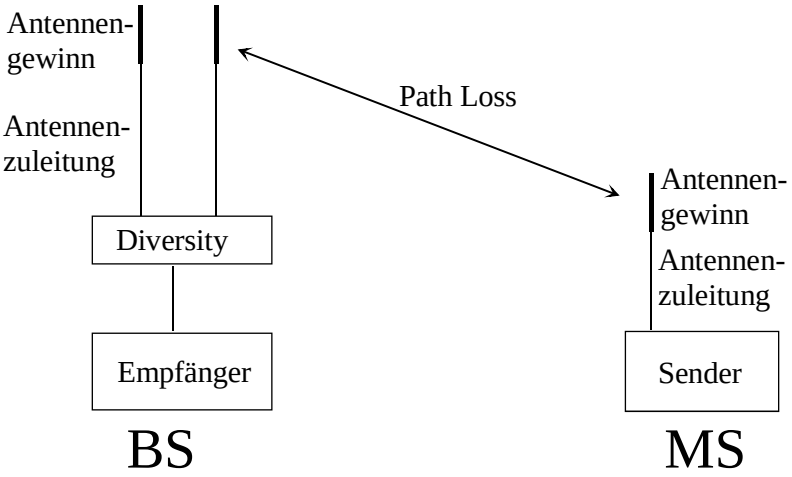
Empfangsseite (MS):

Empfängerempfindlichkeit	- 102	dBm
Zuführungsverluste (Kabel, Verbindung)	0	dB
Antennengewinn	- 2	dBi
minimale Eingangsleistung	- 104	dBm

max. Funkfelddämpfung: 48 - (-104) = 152 dB

Dabei sind aber noch Faktoren für Fading, Shadowing usw. Zu berücksichtigen.

Leistungsbilanz: Uplink



Sendeseite (MS):

Sendeleistung, z.B. 8 W	39	dBm
Zuführungsverluste (Kabel, Verbindung)	0	dB
Antennengewinn	+ 2	dBi
Abgestrahlte Leistung EIRP	41	dBm

Empfangsseite (BS):

Empfängerempfindlichkeit	- 104	dBm
Margin	+ 3	dB
Antennengewinn	- 12	dBi
Verlust im Antennenkabel	+ 2	dB
Verbindungsverluste	+ 1	dB
Diversity-Gewinn	- 4	dB
min. Eingangsleistung	- 114	dBm

max. Funkfelddämpfung: 41 - (-114) = 155 dB

Dabei sind aber noch Faktoren für Fading, Shadowing usw. Zu berücksichtigen.

Leistungsbilanz: Weitere Faktoren zur Funkfelddämpfung:

Margin Rayleigh Fading	3	dB
Margin Shadowing (log. Normal fading)	3	dB
Margin Interference	2	dB
Body Loss (Handies)	3	dB
Car Penetration Loss (Handy im Auto)	6	dB
Building Penetration Loss (Gebäude)	14	dB
Margin for Shadowing Indoor	10	dB

Beispiel für Path Loss : Downlink, Handy im Auto

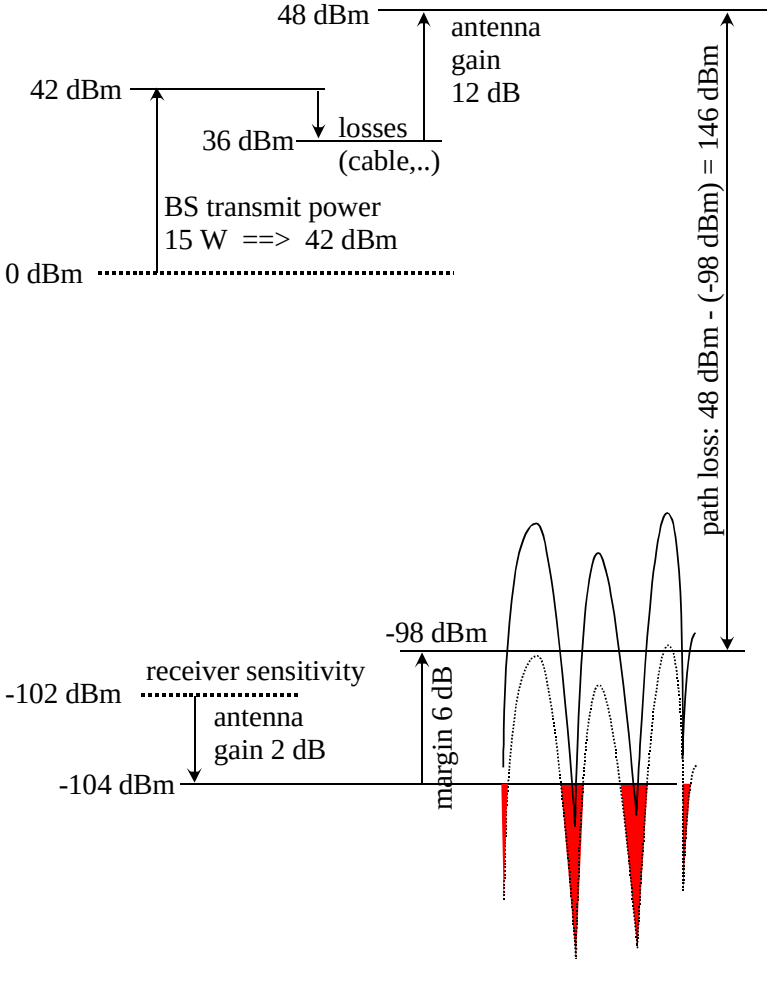
max. Funkfelddämpfung	149	dB
Margin Rayleigh Fading	3	dB
Margin Shadowing	3	dB
Margin Interference	2	dB
Body Loss (Handies)	3	dB
Car Penetration Loss	6	dB

Maximaler Path Loss:

149 – 3 – 3 – 2 – 3 – 6 = 132 dB

Funknetzplanung möglichst so auslegen, daß folgende mittlere Feldstärkewerte im Freien gemessen werden:

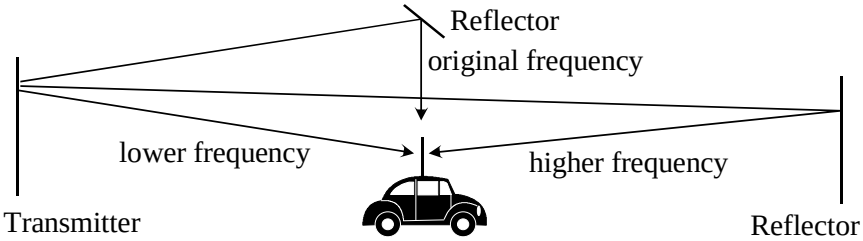
Outdoor – Versorgung	-104 +3 +3 +2 +3	= - 93 dBm
In-Carr – Versorgung	-104 +3 +3 +2 +3 +6	= - 87 dBm
Indoor – Versorgung	-104 +3 +2 +3 +14 + 10	= - 72 dBm



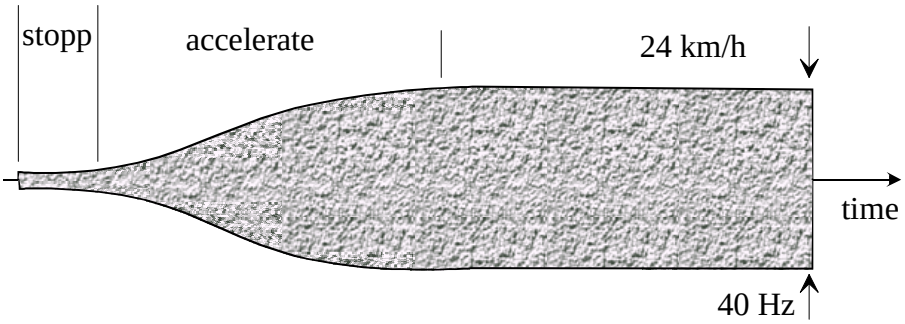
Example for Power Budget On the downlink

3 Radio Channel Characteristics

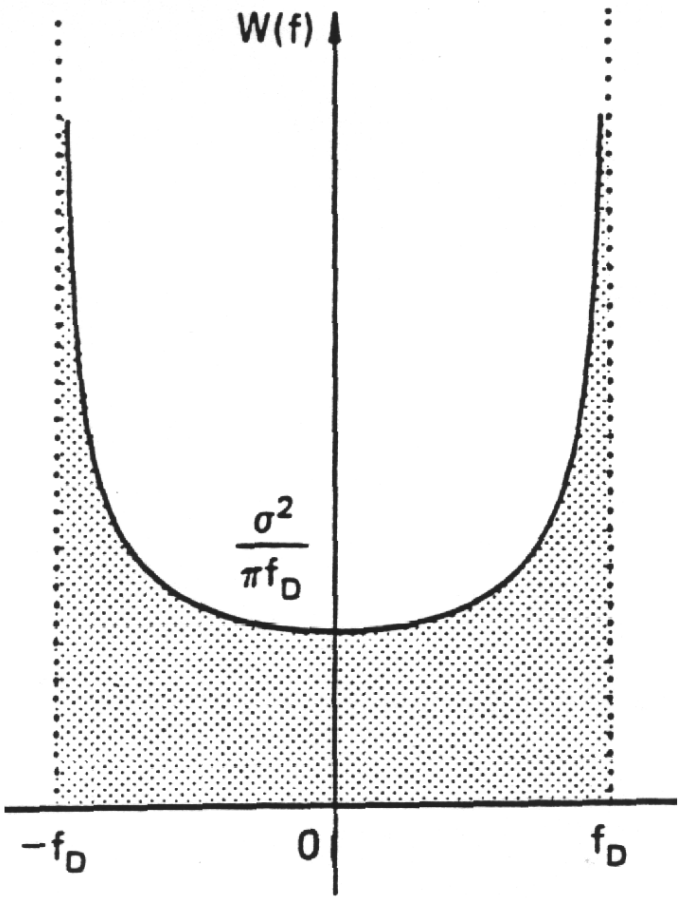
3.1 Doppler



Transmitted Frequency	f_0
Received Frequency	$f = f_0 (1 + v/c)$
Doppler Frequency	$f_D = f - f_0 = f_0 * v/c$ $\quad c = 3 * 10^{-8}$ m/s



Doppler spectrum at 900 MHz



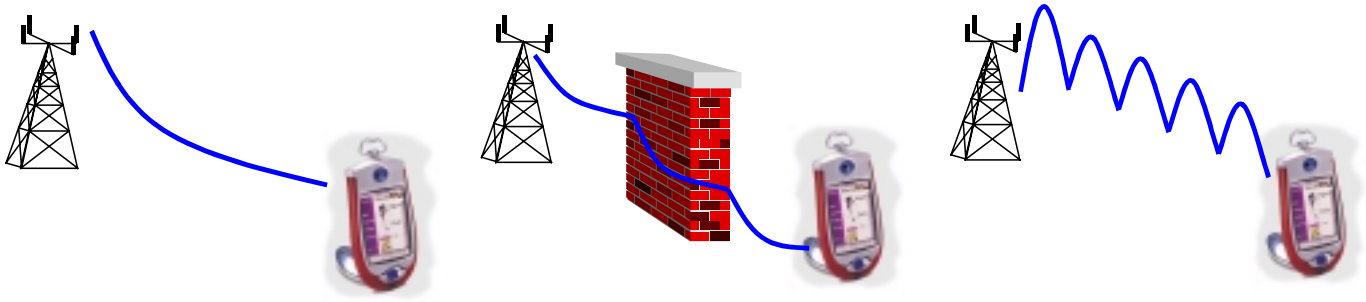
Doppler Spectrum

Doppler propability distribution:

$$W(f) = \frac{\sigma^2}{\pi \sqrt{f_D^2 - f^2}}$$

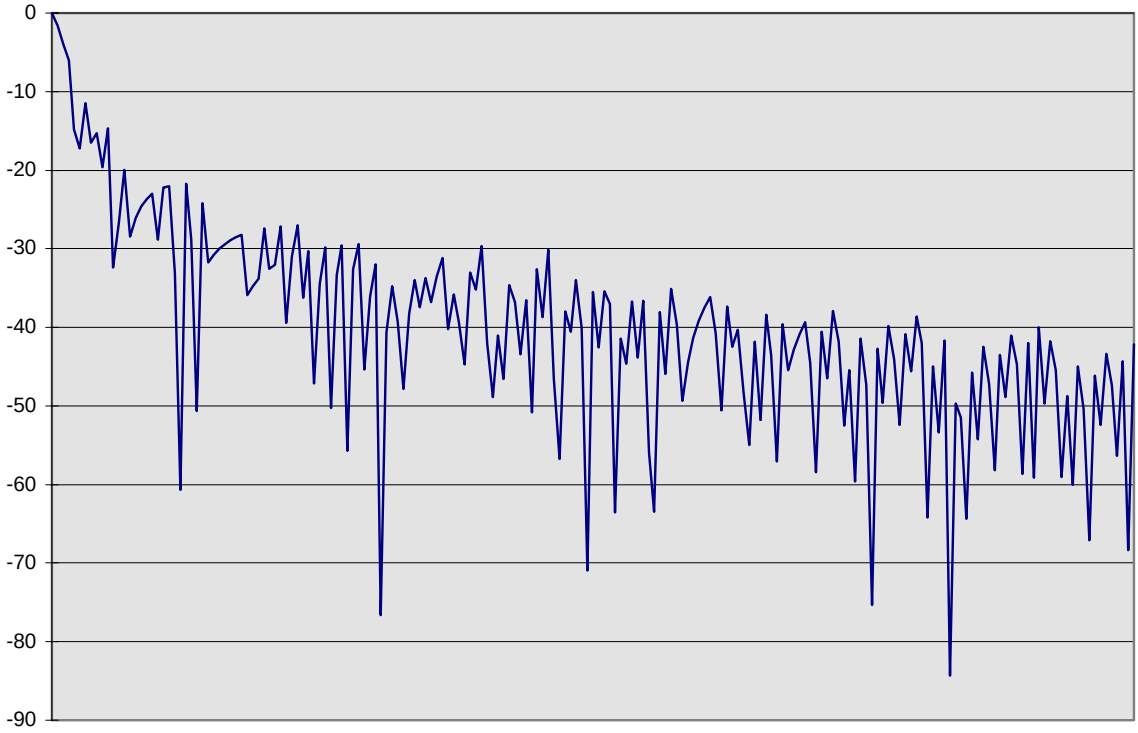
for $|f| \leq f_D$ and 0 für $|f| > f_D$

Radio Channel Characteristics

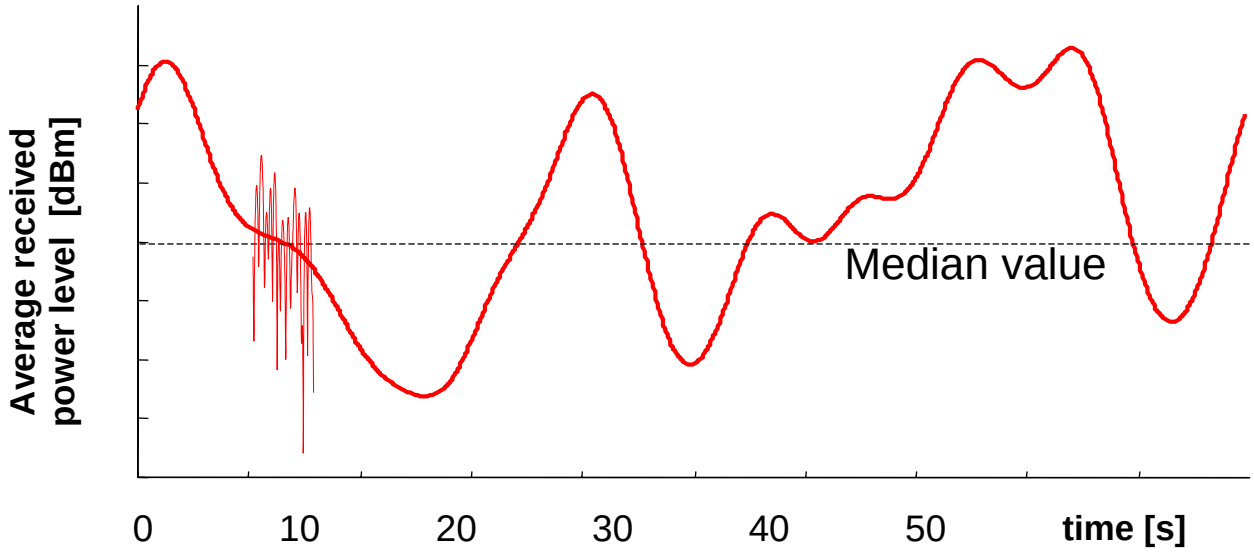


Path Loss	Shadowing	Fading
Funkfelddämpfung	Abschattung	
propagation in 3D	Obstacles	Mulripath propagation

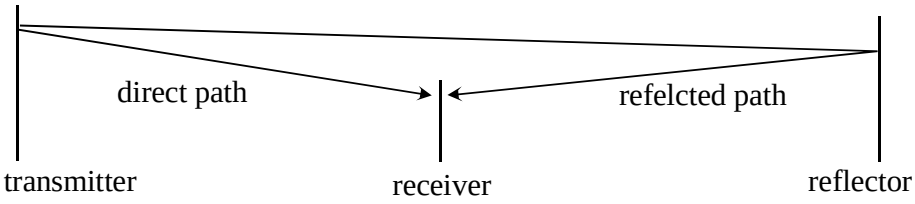
3.2 Fast Fading

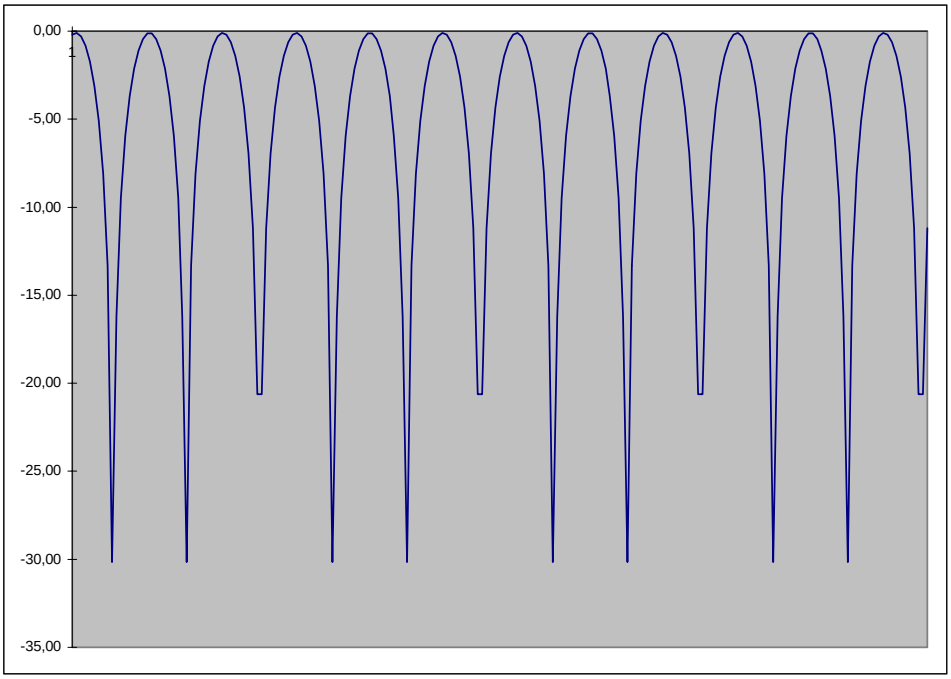


Fast Fading durch Überlagerung von Signalen: Beispiel Zweiwegeausbreitung im Bild

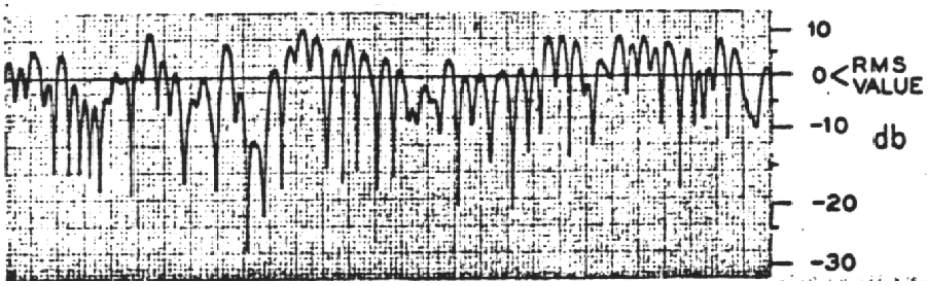


Fast Fading (2 way model)





distance between drop outs is $\lambda / 2$



Fading Statistic

Field strength measurement (11 m, 1.8 s measurement time, 836 MHz)

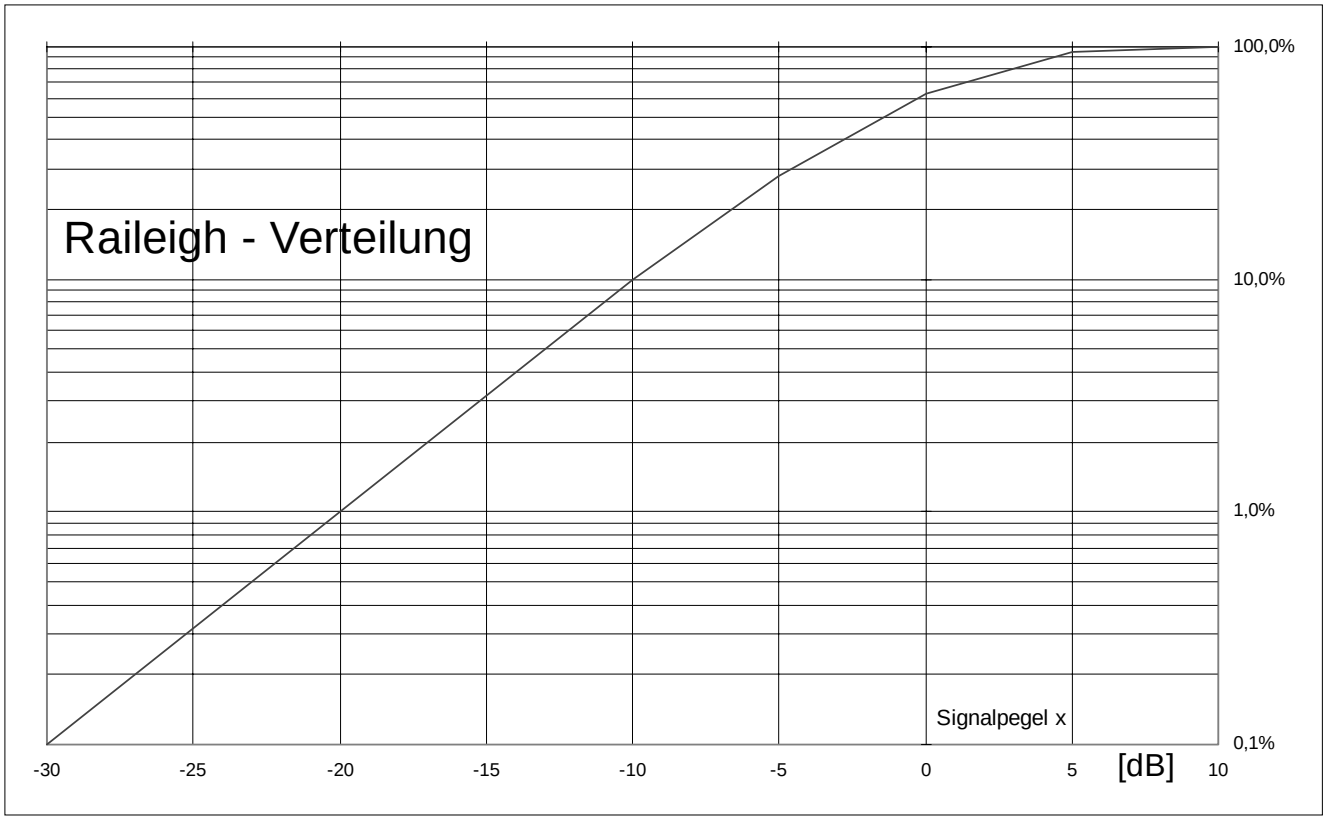
Rayleigh describes the fading statistics

Rayleigh propability function: $p(x) = \frac{x}{\sigma^2} e^{-\frac{x^2}{2\sigma^2}}$

σ^2 = average power
x = amplitude

Rayleigh distribution $P(x \le r) = \int_0^r p(x)dx = 1 - e^{-r/2\sigma^2}$

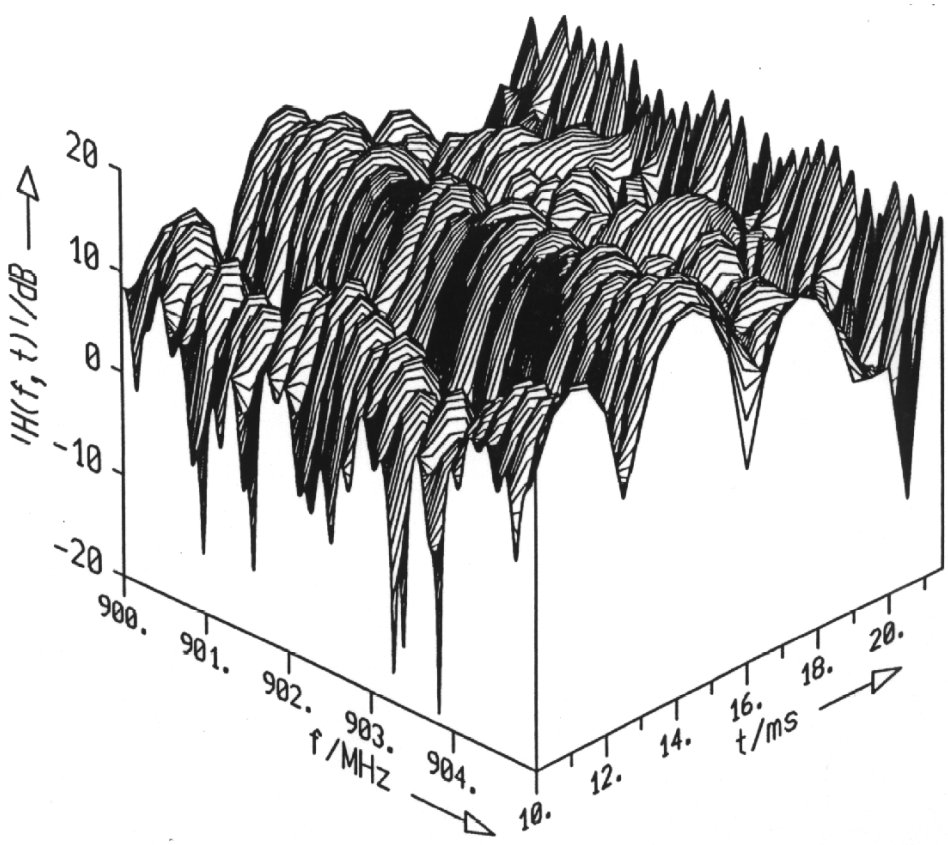
The phase of e fading signal is equally distributed: $p(\varphi) = \frac{1}{2\pi}$

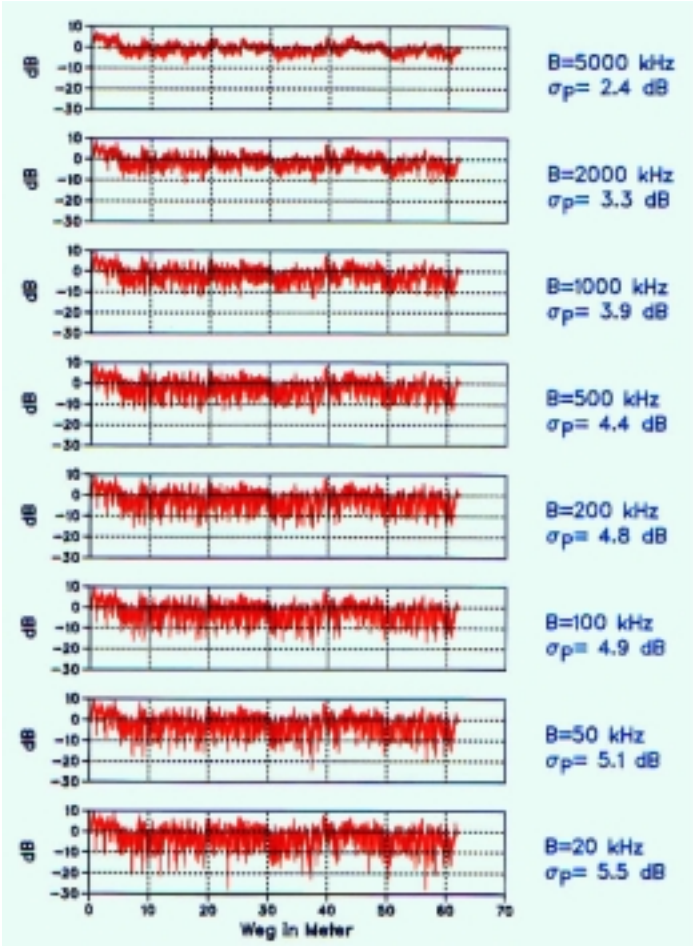


Y-Achse: die Wahrscheinlichkeit, daß der Signalpegel x kleiner oder gleich dem mittlere Signalpegel ist.

X-Achse: Signalpegel x; 0 dB = mittlerer Pegel der Einhüllenden

Fading is a Function of Location and Frequency

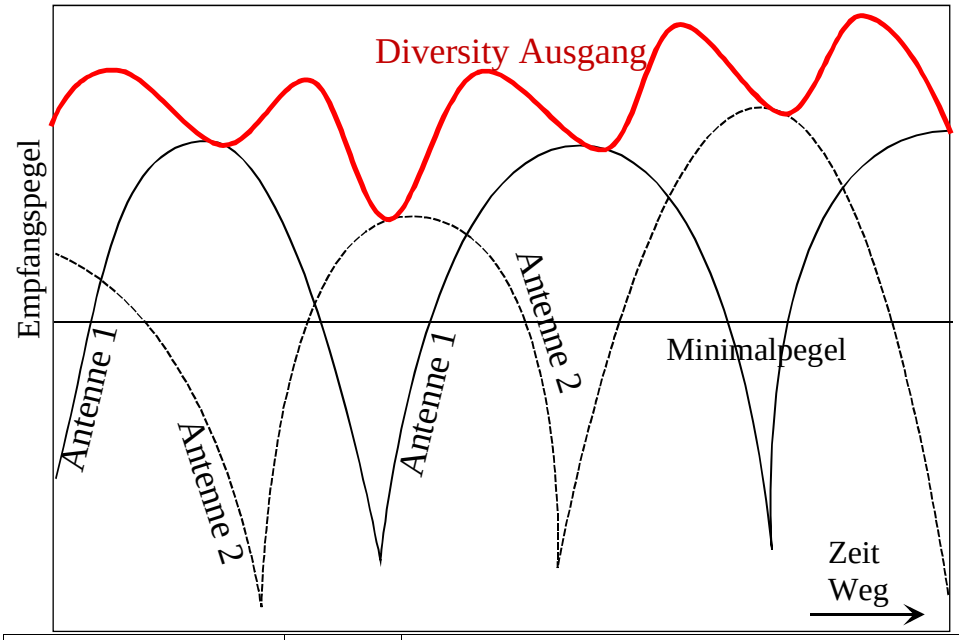




High Bandwidth reduces Fading

Every CDMA user has the same high bandwidth independent from the datarate

the figure shows the relative received power as a function of bandwidth

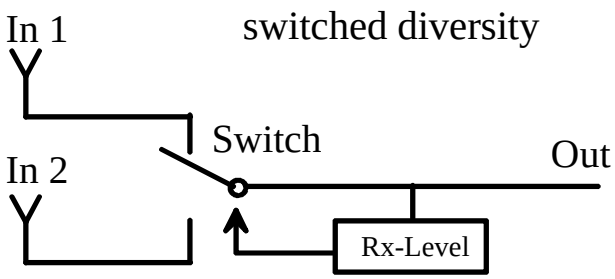


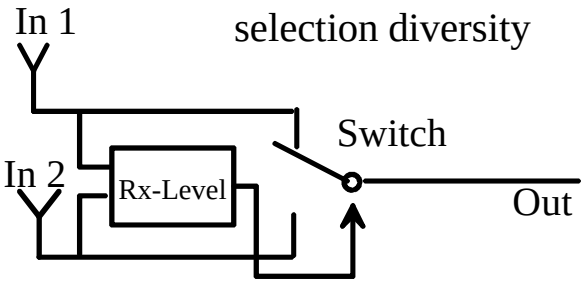
3.3 Diversity

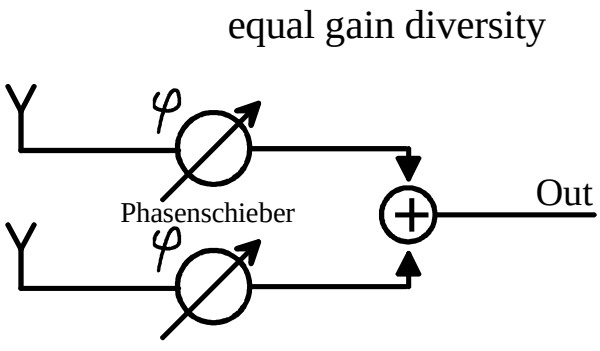
Bild: Beispeil für Maximum Ratio Combining

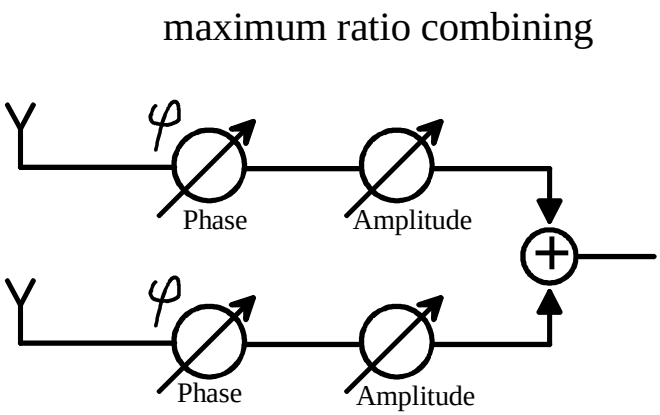
Space Diversity:	Passiv	räumlich versetzte Antennen
Polarisation Diversity	Passiv Aktiv	Antennen mit unterschiedlicher Polarisation; vertikal, horizontal, zirkular (li, re) Tx kann Polarisation der Sendeantenne wählen
Time Diversity	Passiv Aktiv	Ausnutzen der Mehrwege, Tx sendet das gleiche Signal mehrmals aus
Frequency Diversity	Aktiv	Tx sendet das gleiche Signal auf unterschiedlichen Frequenzen
Macro Diversity	Passiv Aktiv	mehrere Empfängerstandorte mehrere Senderstandorte, Gleichwellenfunk (DAB)

Space Diversity Combing Methods

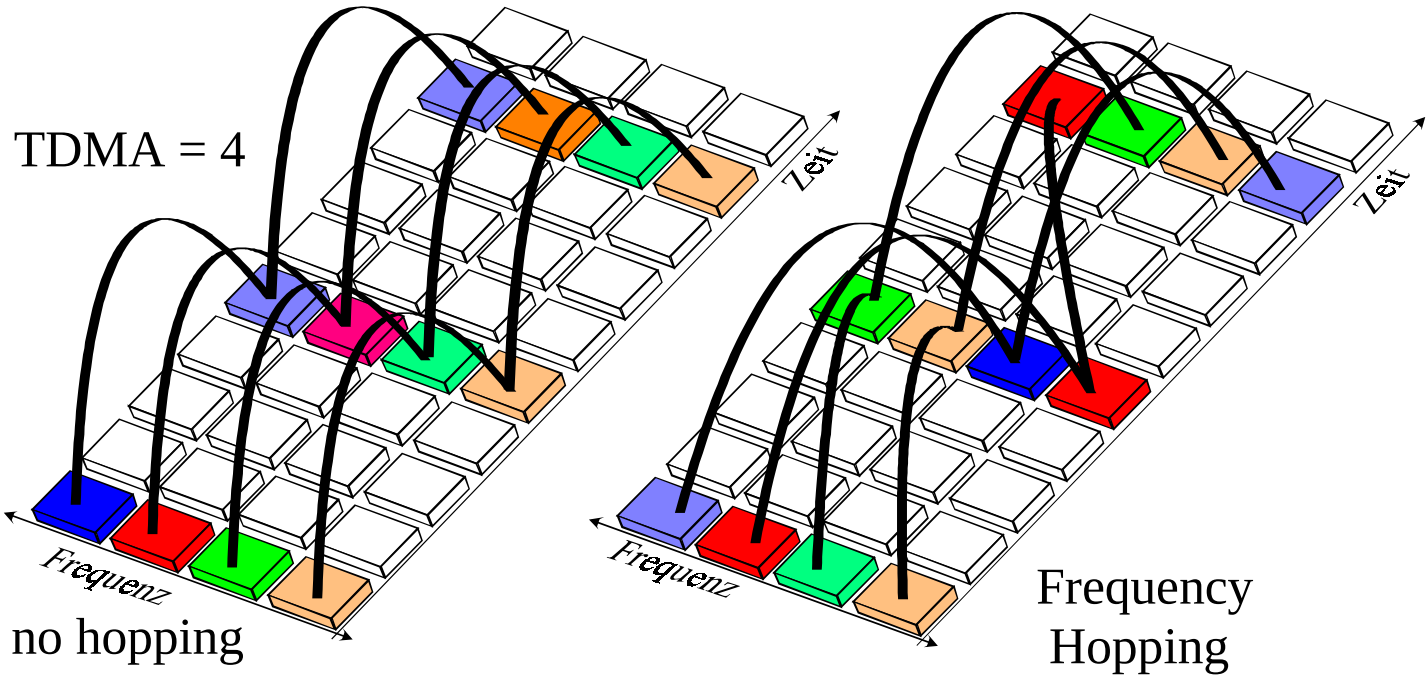


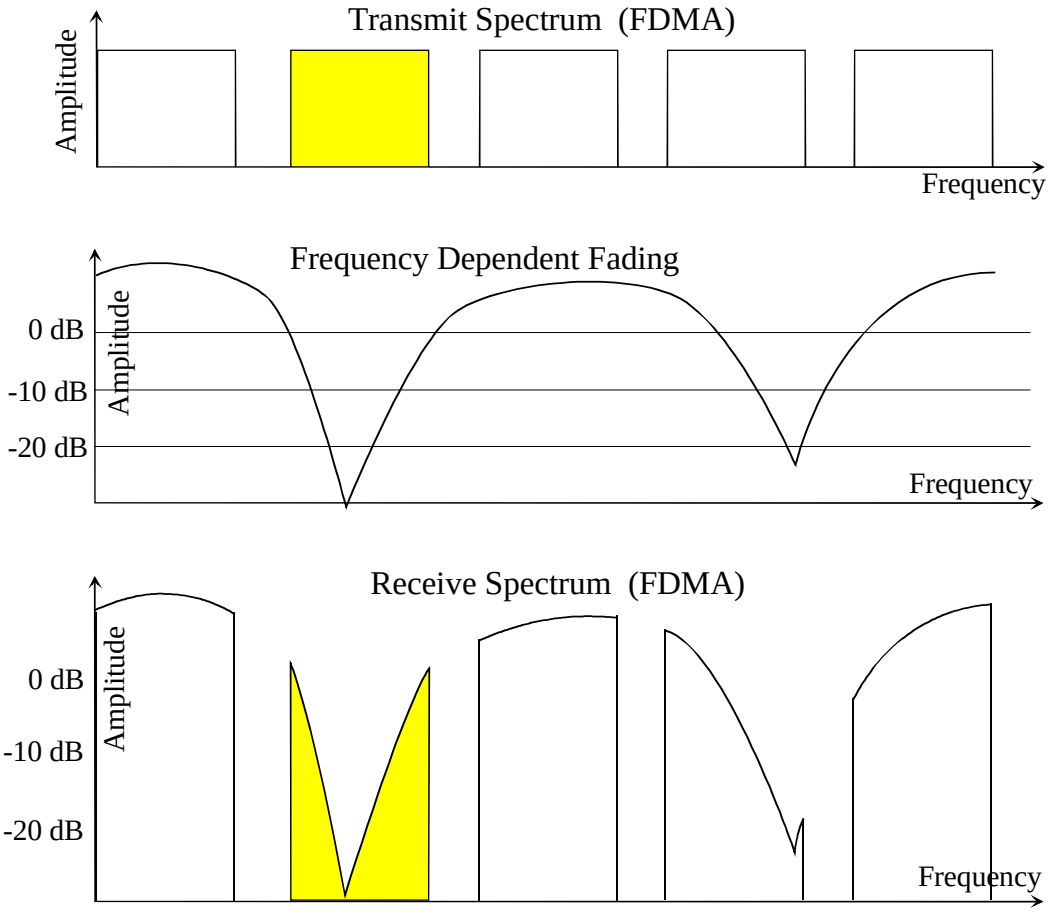






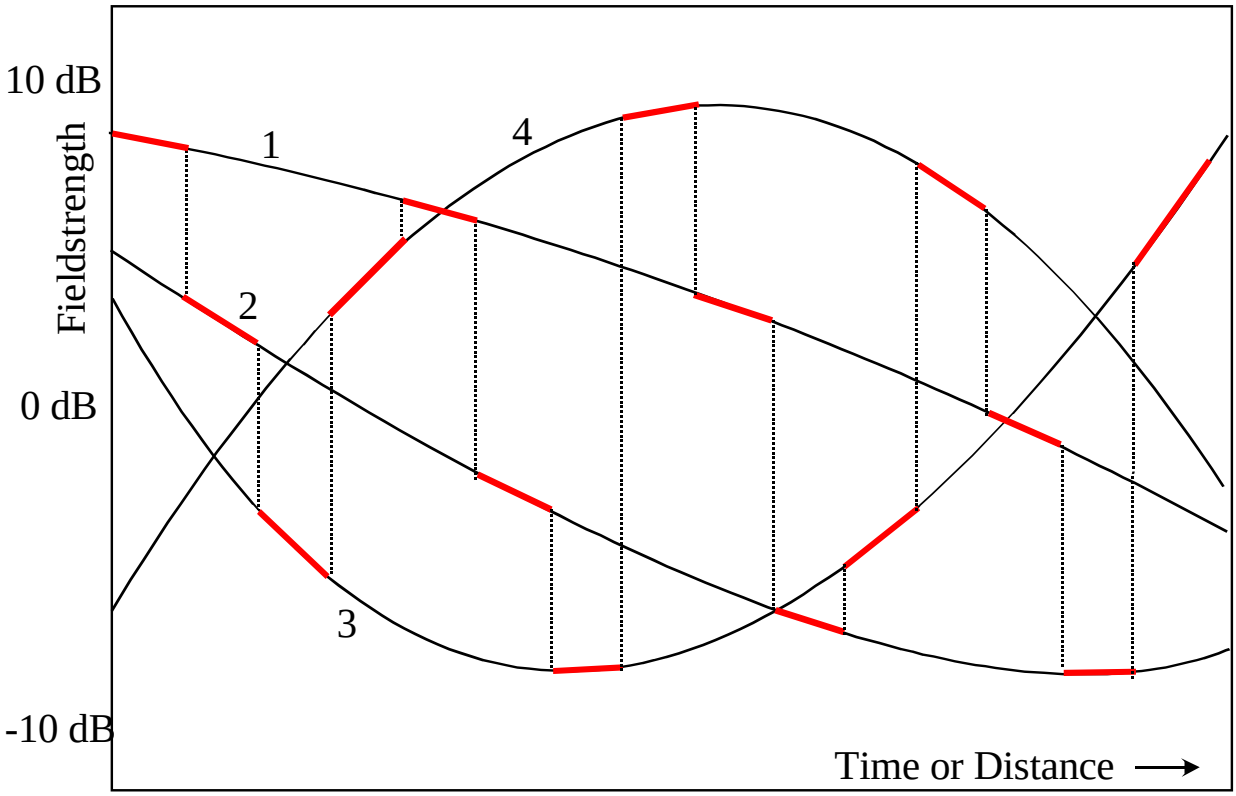
3.4 Frequency Hopping



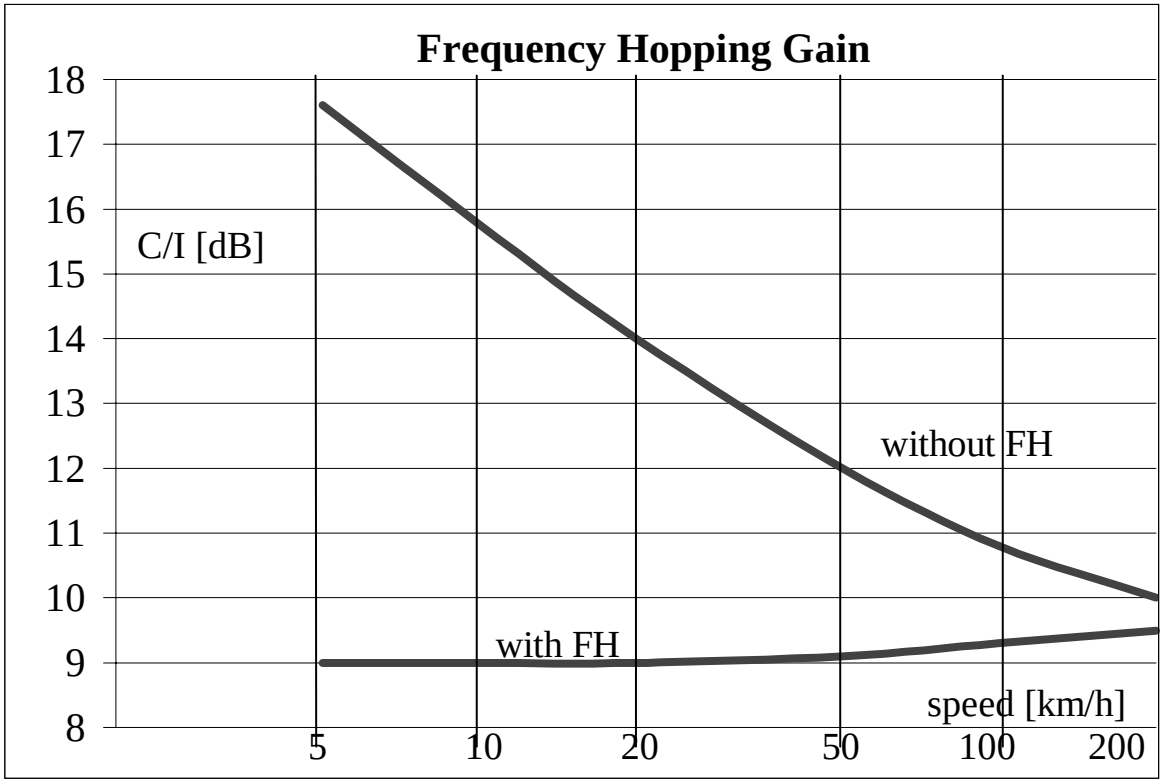


Fading in the Frequency Domain

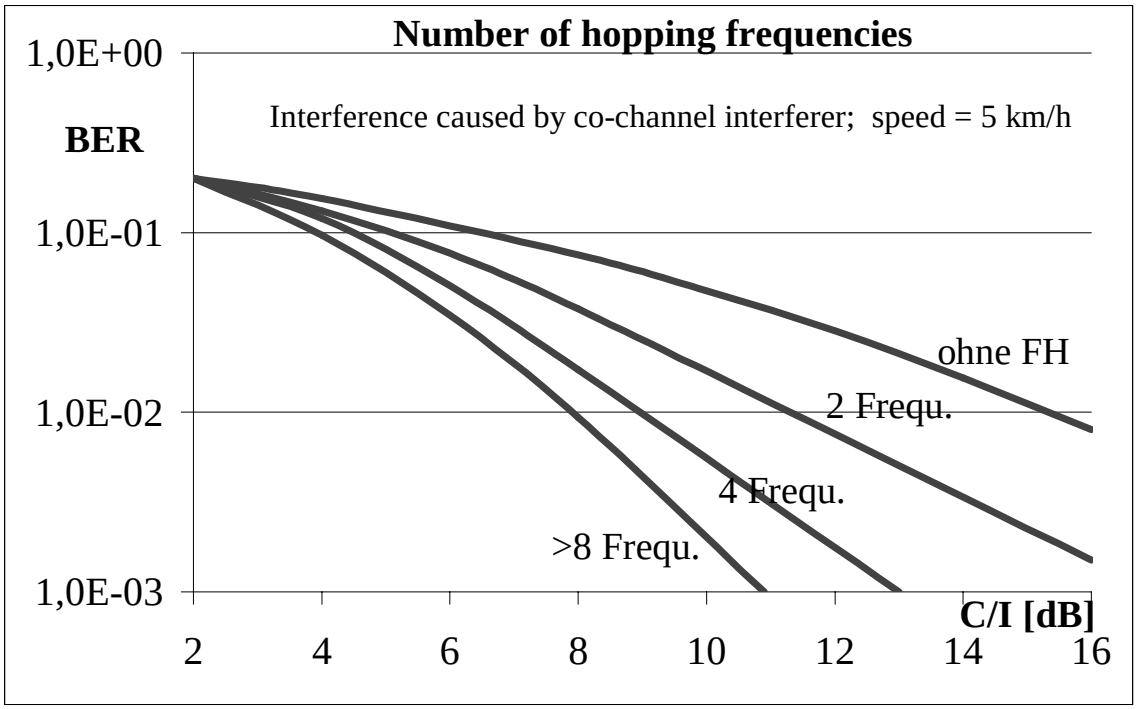
Frequency Hopping



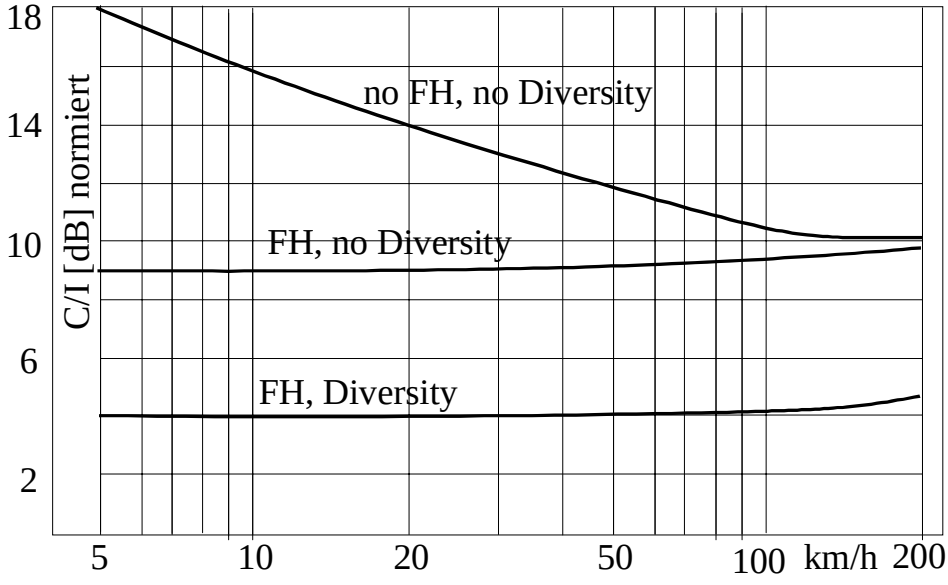
Gain with Frequency Hopping in a GSM System

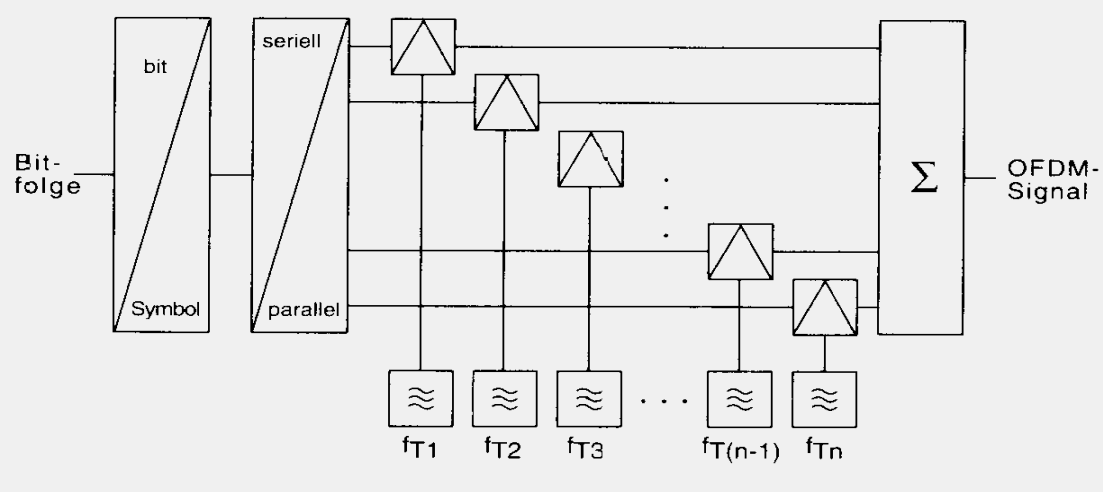


Frequency hopping gain depending on the number of frequencies

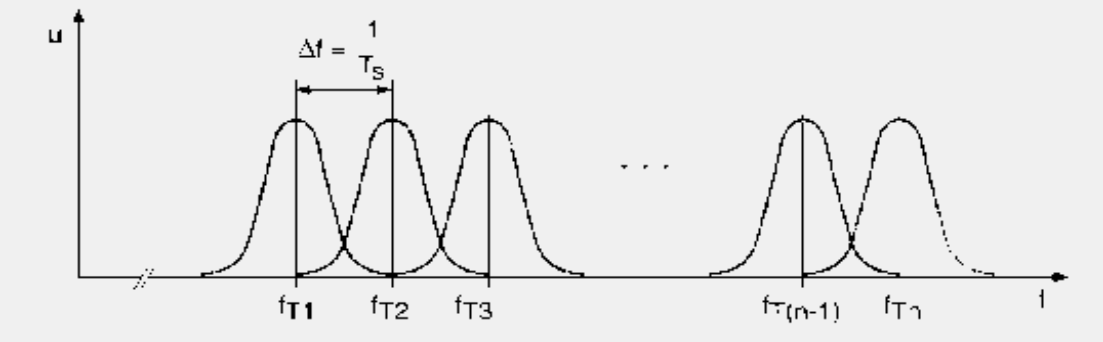


Gain with Frequency Hopping and Diversity in a GSM System





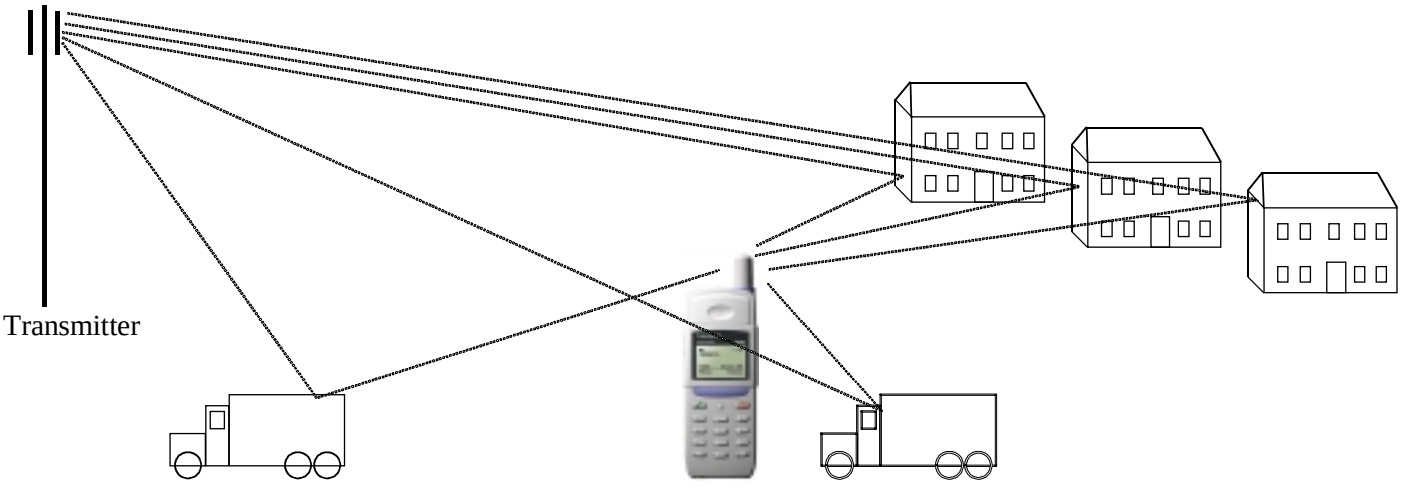
3.5 OFDM: Orthogonal Frequency Division Multiplex

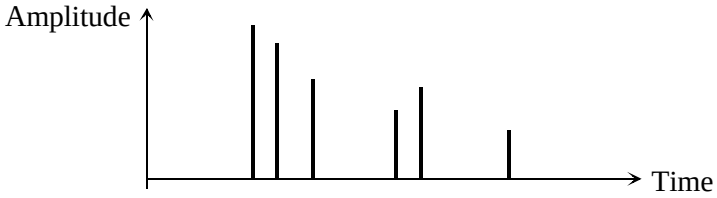


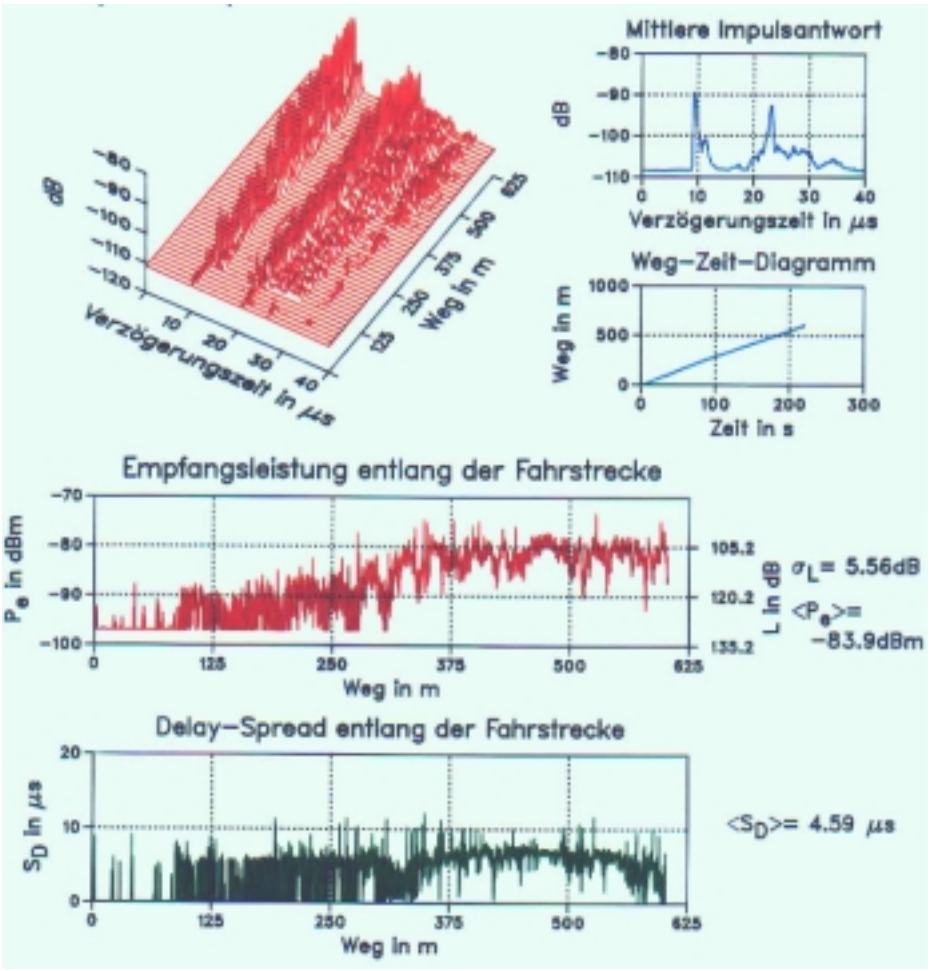
parallele Übertragung auf vielen Kanälen und Kanalcodierung.

Beim digitalen Rundfunk DAB sind es 1536 Kanäle

3.6 Multipath Propagation







High Bandwidth improves Multipath Resolution

Multipath reception and utilisation improves transmission quality

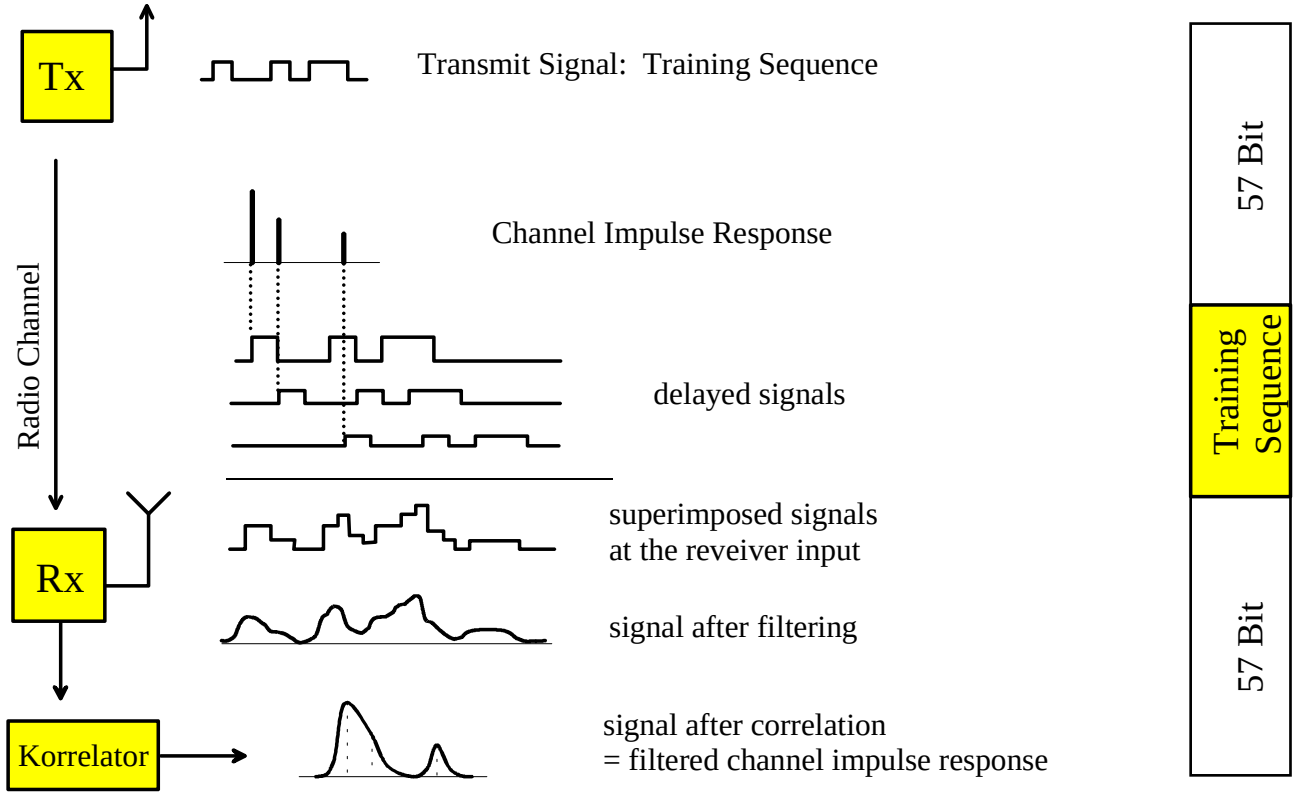
487 MHz transmitter frequency :

9122 profiles measured:

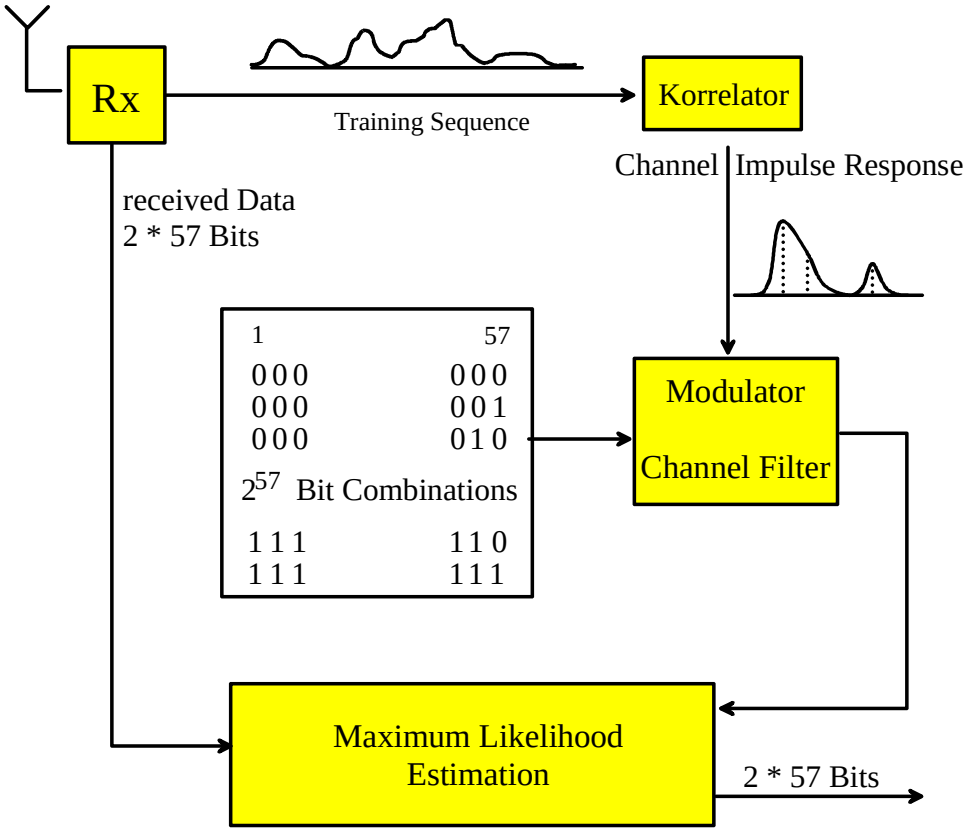
601 m distance

3.7 Equalization

GSM Channel Estimation



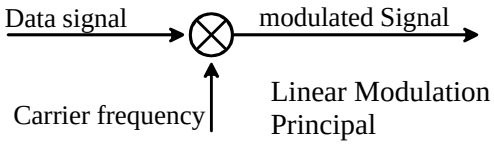
Equalizer

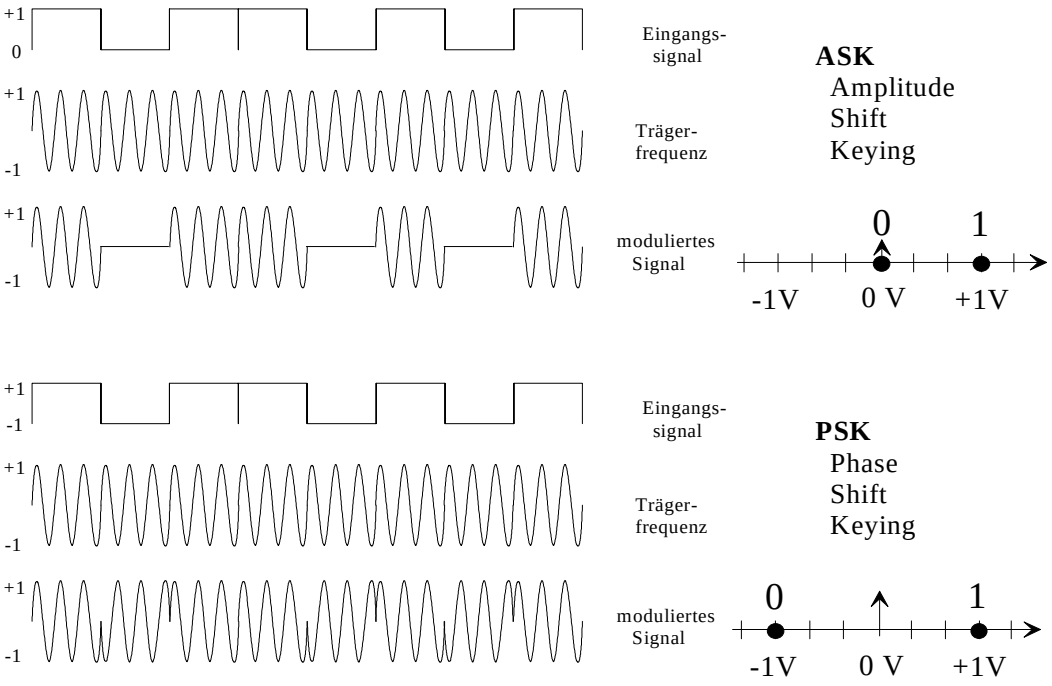

Rx
Training Sequence
Korrelator
Channel Impulse Response
received Data
2 * 57 Bits
1
57
0 0 0 0 0 0
0 0 0 0 0 1
0 0 0 0 1 0
2^57 Bit Combinations
1 1 1 1 1 0
1 1 1 1 1 1
Modulator
Channel Filter
Maximum Likelihood Estimation
2 * 57 Bits

4 Modulation

4.1 Linar Modulation

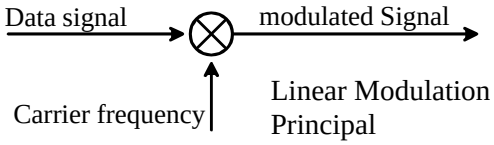
= multiplication in the time domain

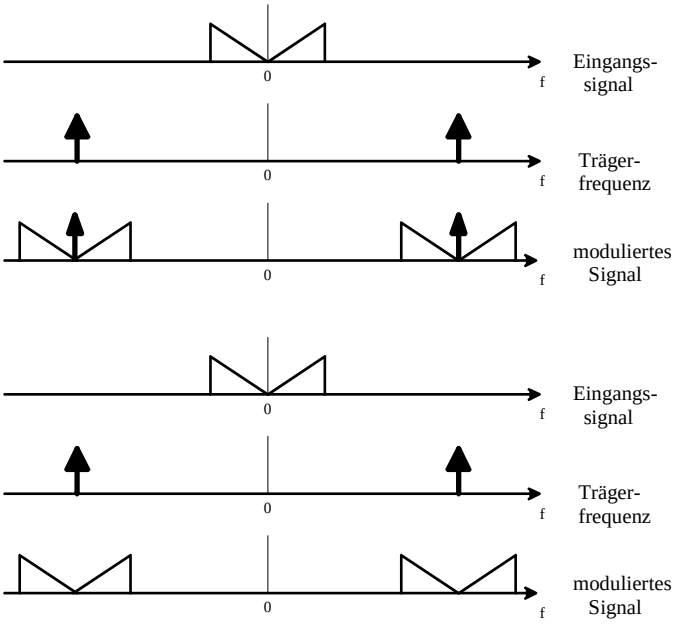




Modulation in the Frequency Domain

multiplication in the time domain =
convolution in the frequency domain





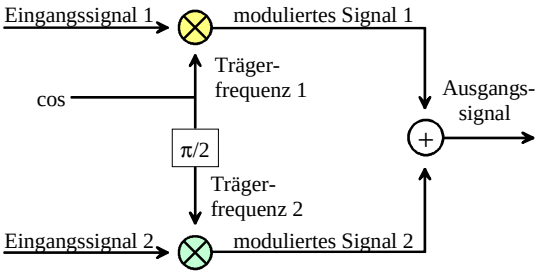
The input signal for ASK contains a DC component

➔ the modulated signal contains a carrier signal

The input signal for PSK contains **no** DC component

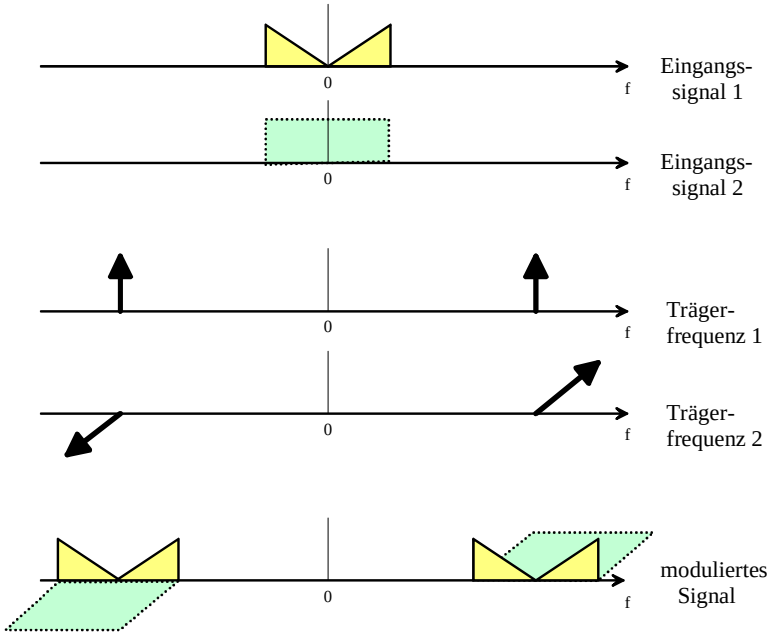
➔ the modulated signal contains **no** carrier signal

4.2 Quadratur-Modulation: QPSK

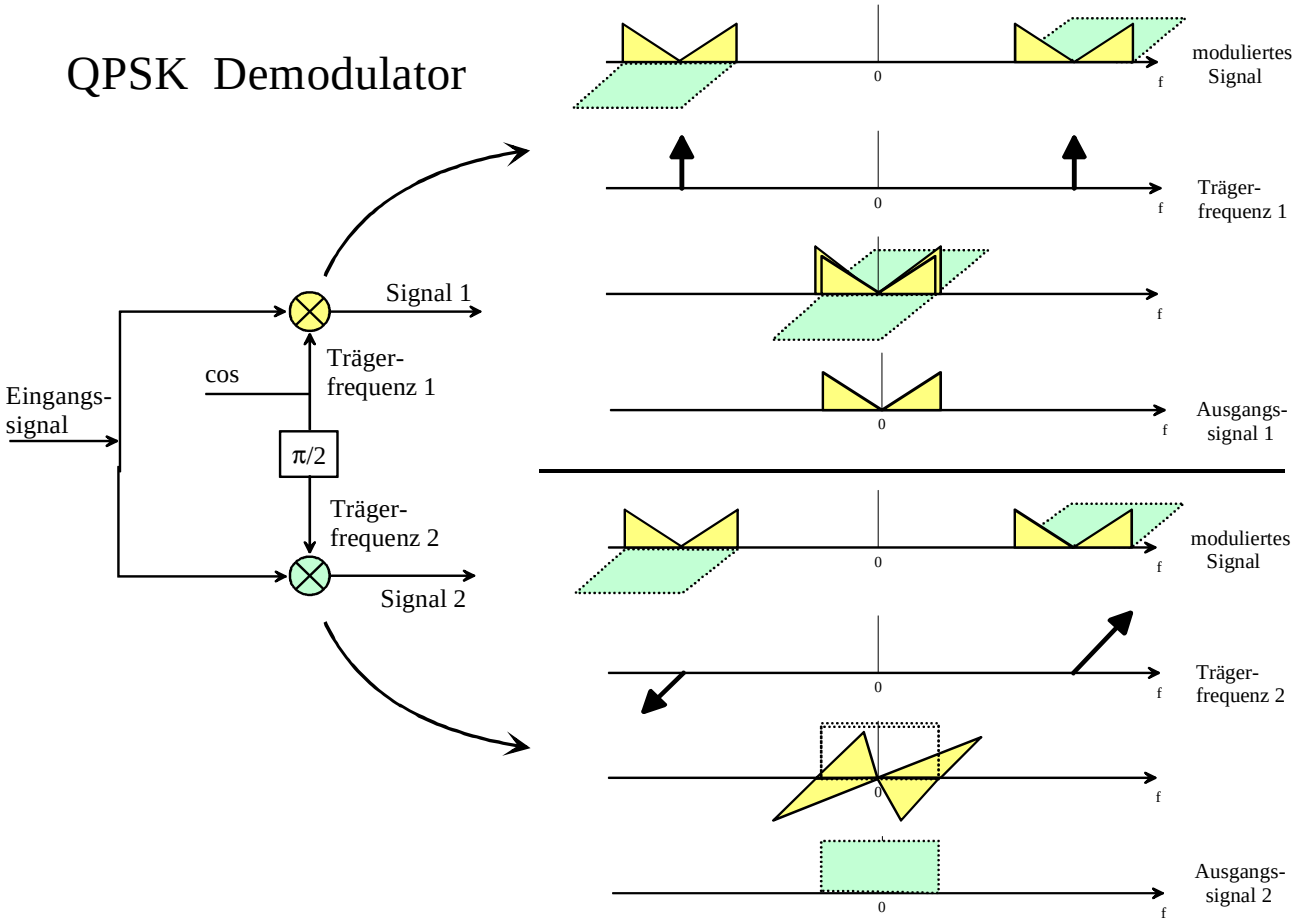


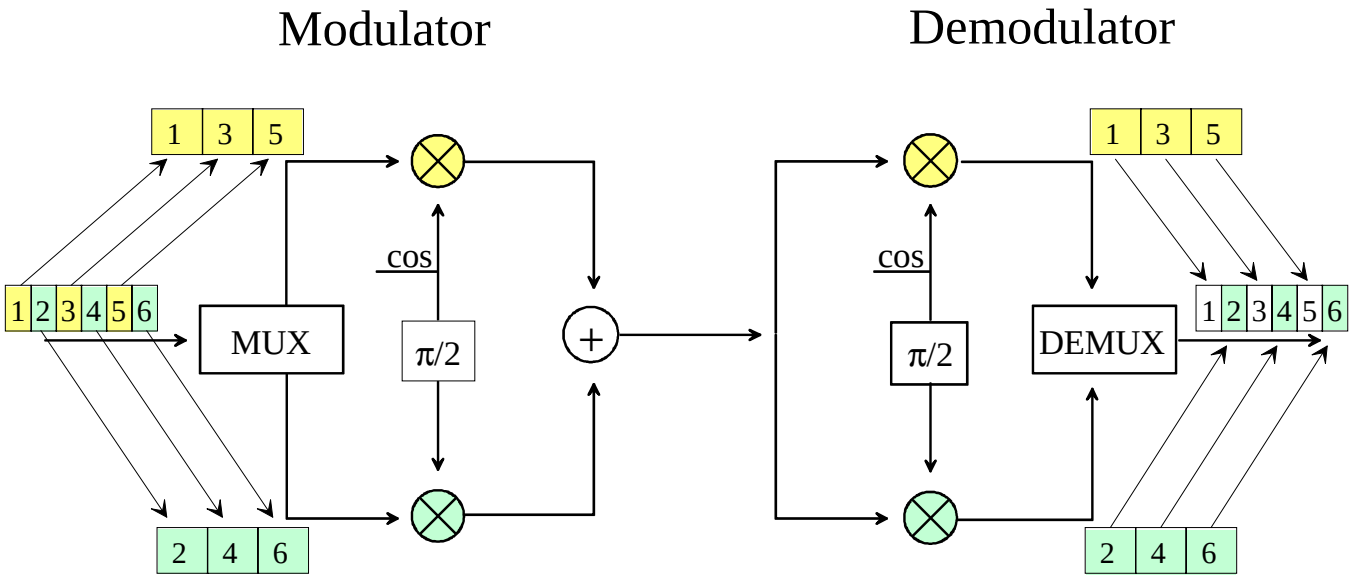
Schaltungsanordnung der
Quadratur-Modulation

Darstellung im Frequenzbereich

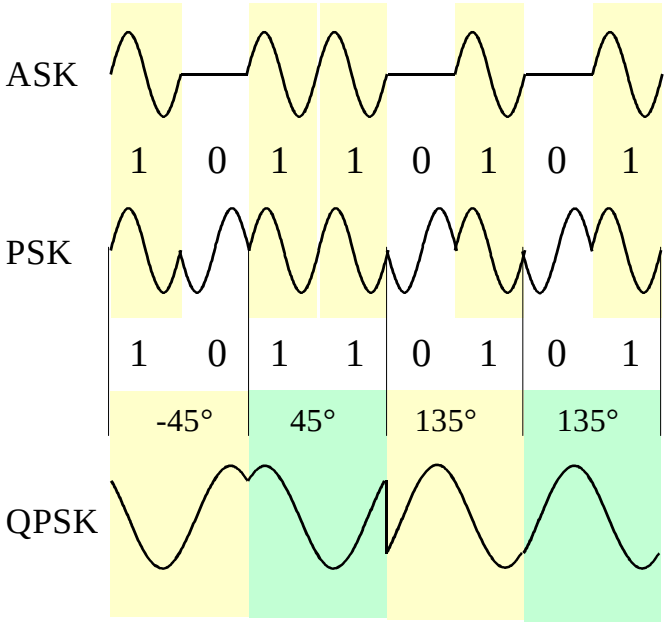


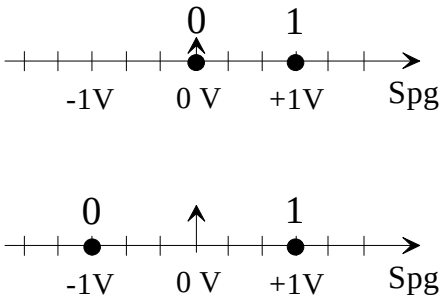
QPSK Demodulator

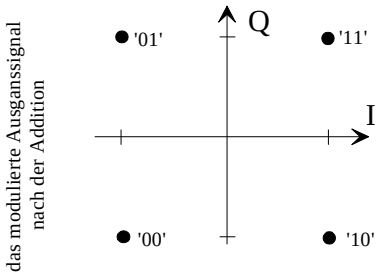


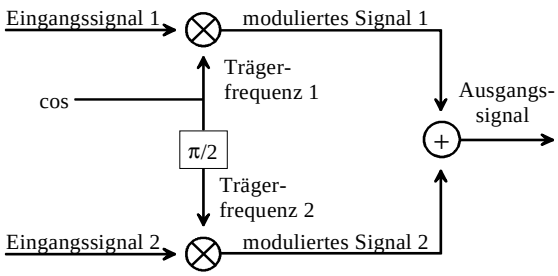


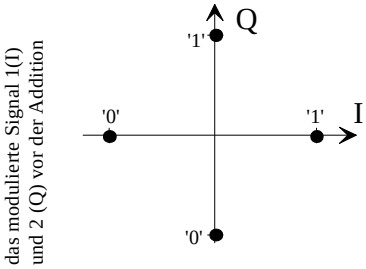
Quadraturmodulation



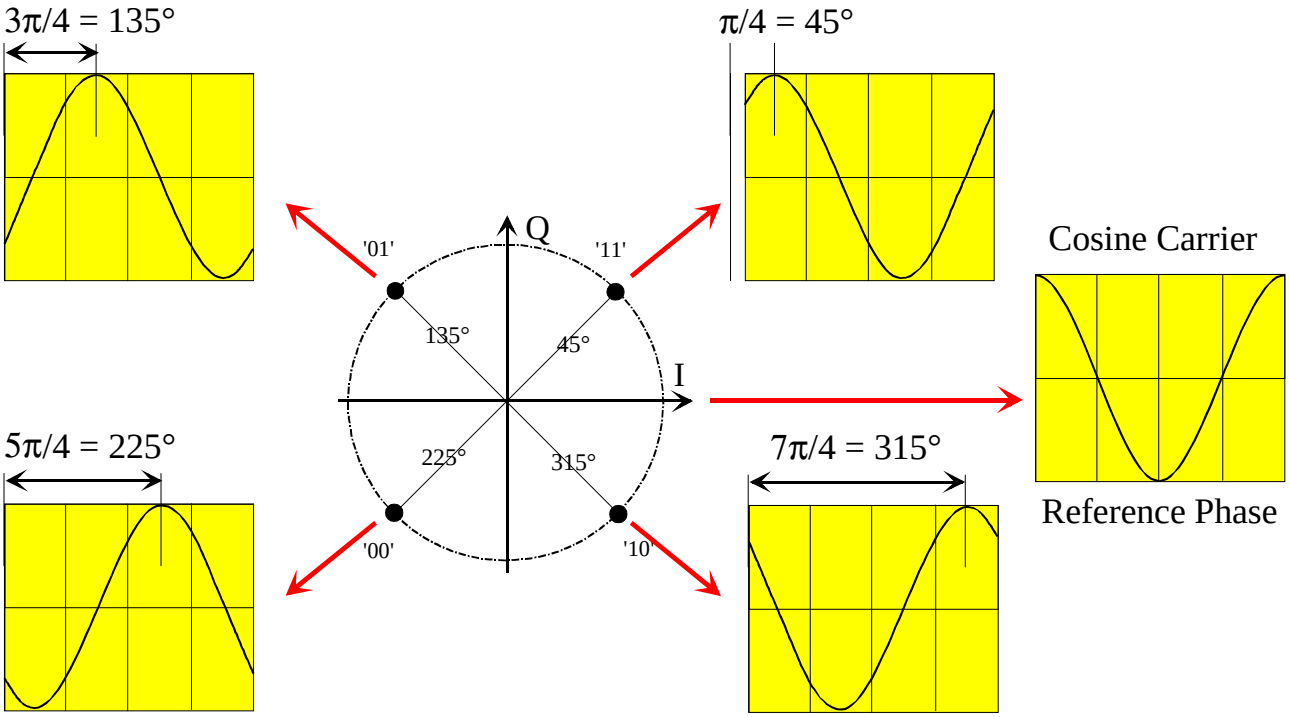




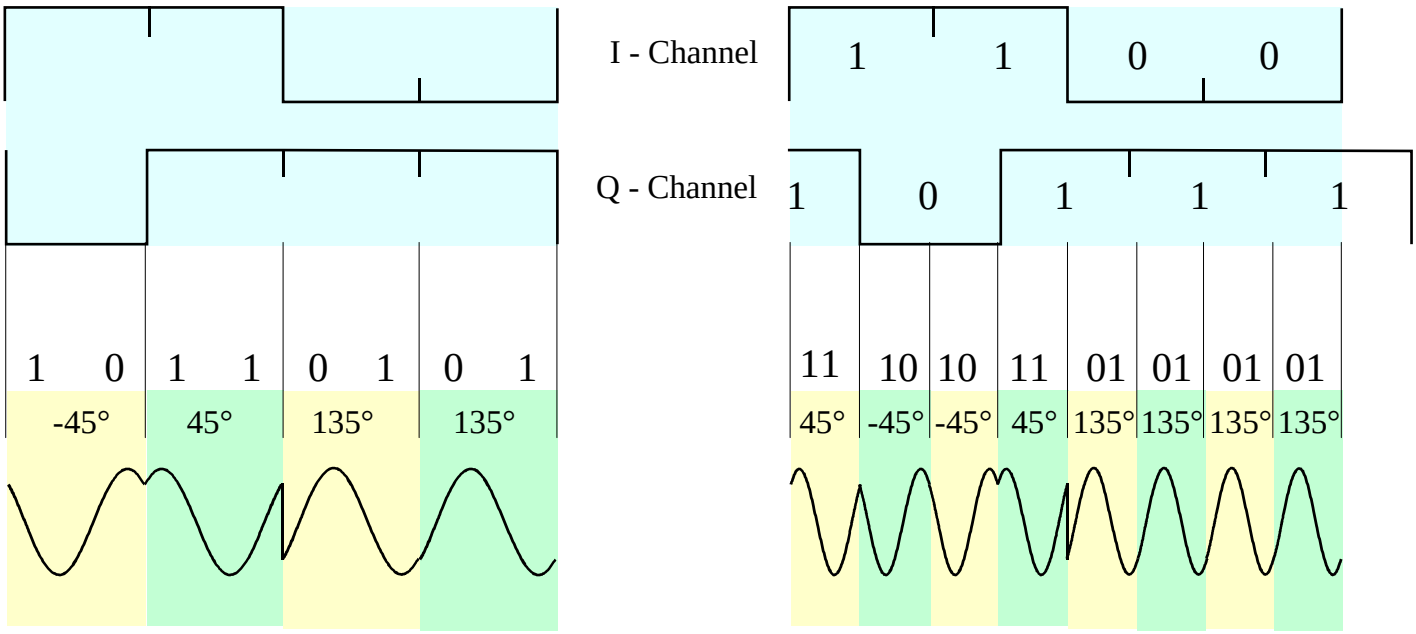




Quadrature Modulation



Quadrature and Offset-Quadrature Modulation



QPSK

Phase Shift: π/4 and π/2

OQPSK

Phase Shift: π/4

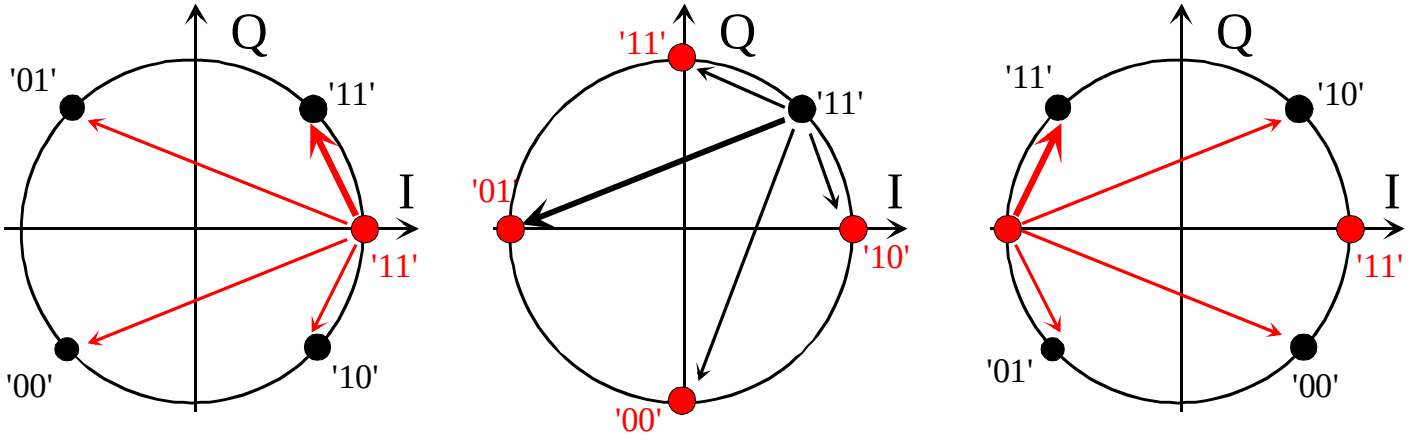
4.3 π/4 – shifted QPSK

Advantages:

– Two bits per symbol, twice as efficient as GMSK

– Phase transitions avoid center of diagram, remove some design constraints on amplifier

– Always a phase change between symbols, leading to self clocking

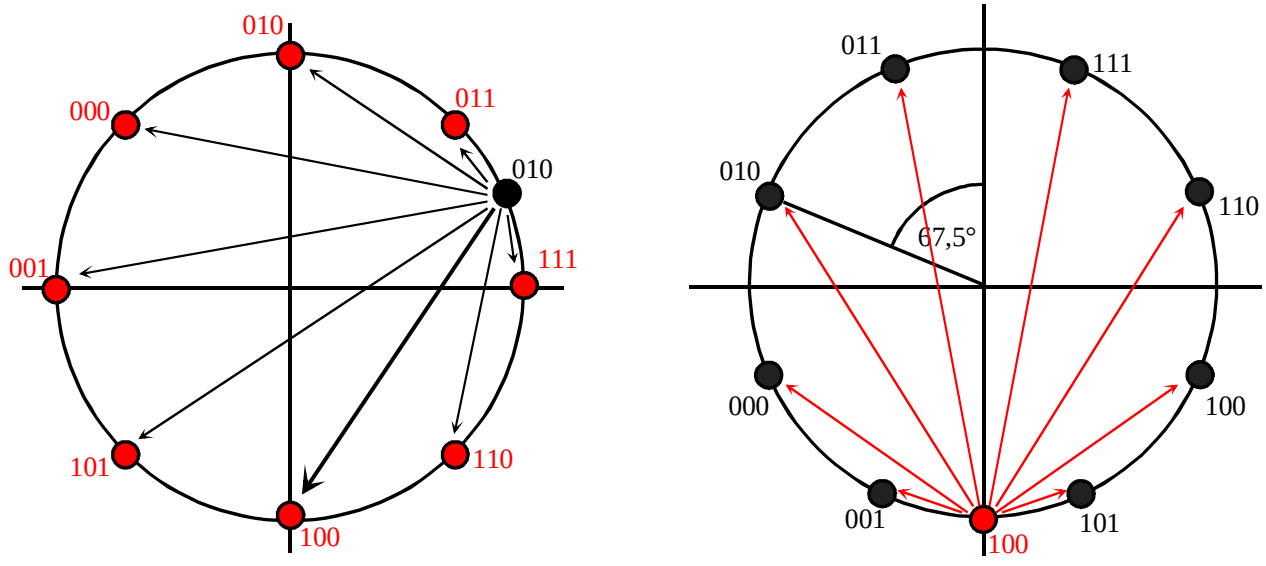


Transmit Sequence: 11 01 11

– North American Digital Cellular (IS-54): 1.62 bps/Hz – Japanese Digital Cellular System: 1.68 bps/Hz	– European TETRA System: 1.44 bps/Hz – Japanese Personal Handy Phone (PHP)

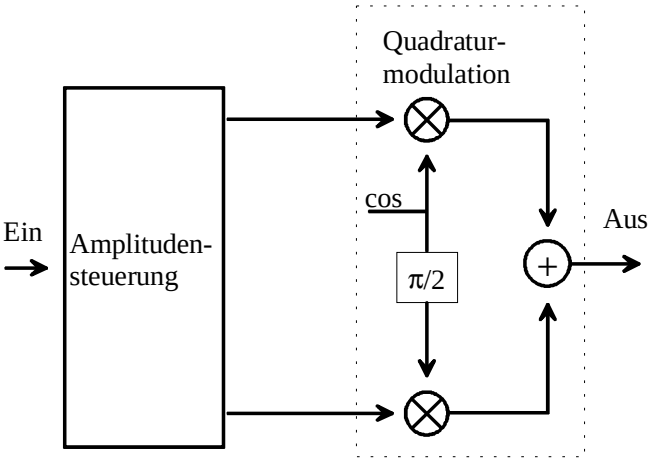
4.4 Edge : Offset-8-PSK Modulation

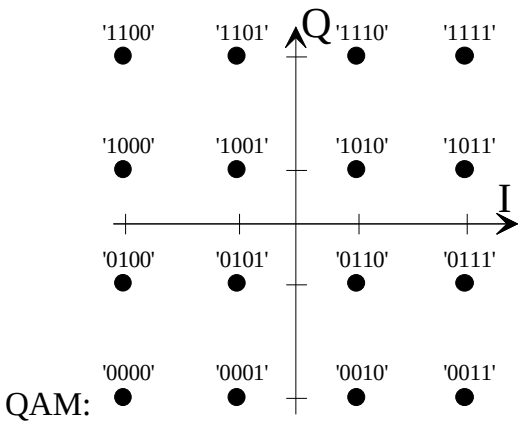
8-PSK with phase shift of 3π/8 (67.5°) every step



Transmit 010 100

Quadratur-Amplituden-Modulation QAM



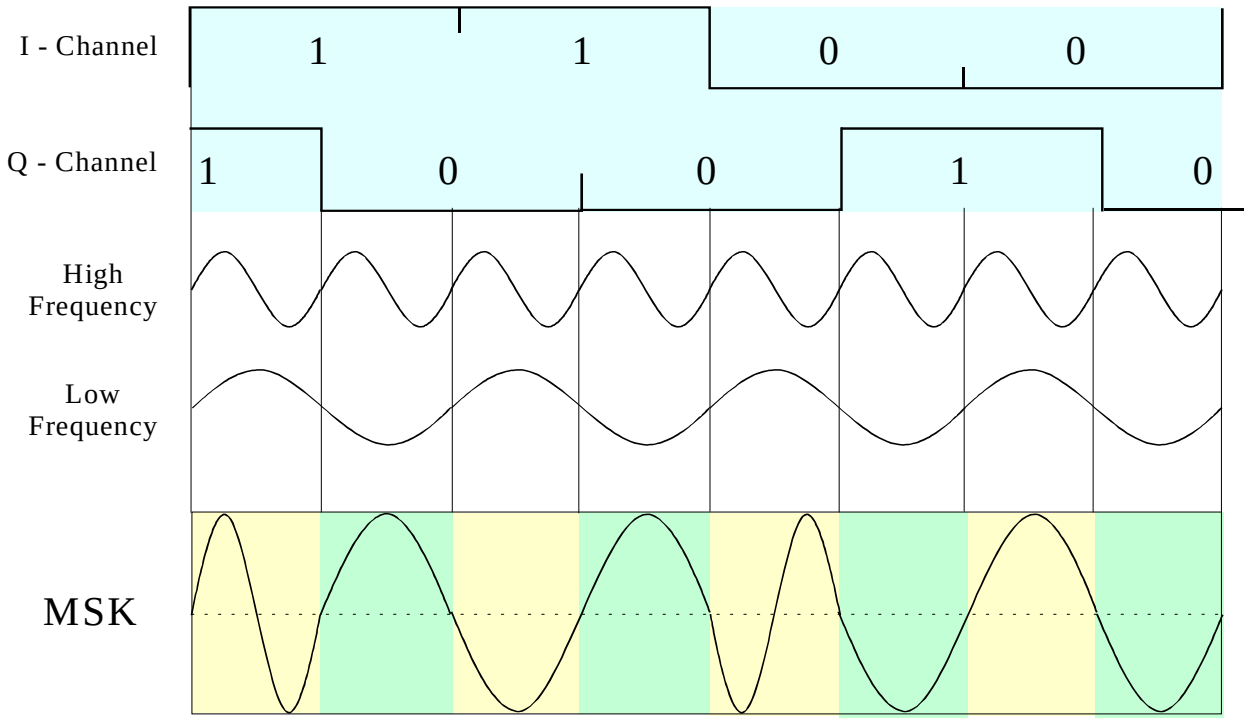


Anwendung in der Trägerfrequenztechnik

Minimum Shift Keying (MSK)

Special form of (continuous phase) frequency shift keying (Phase continuity at the bit transitions)

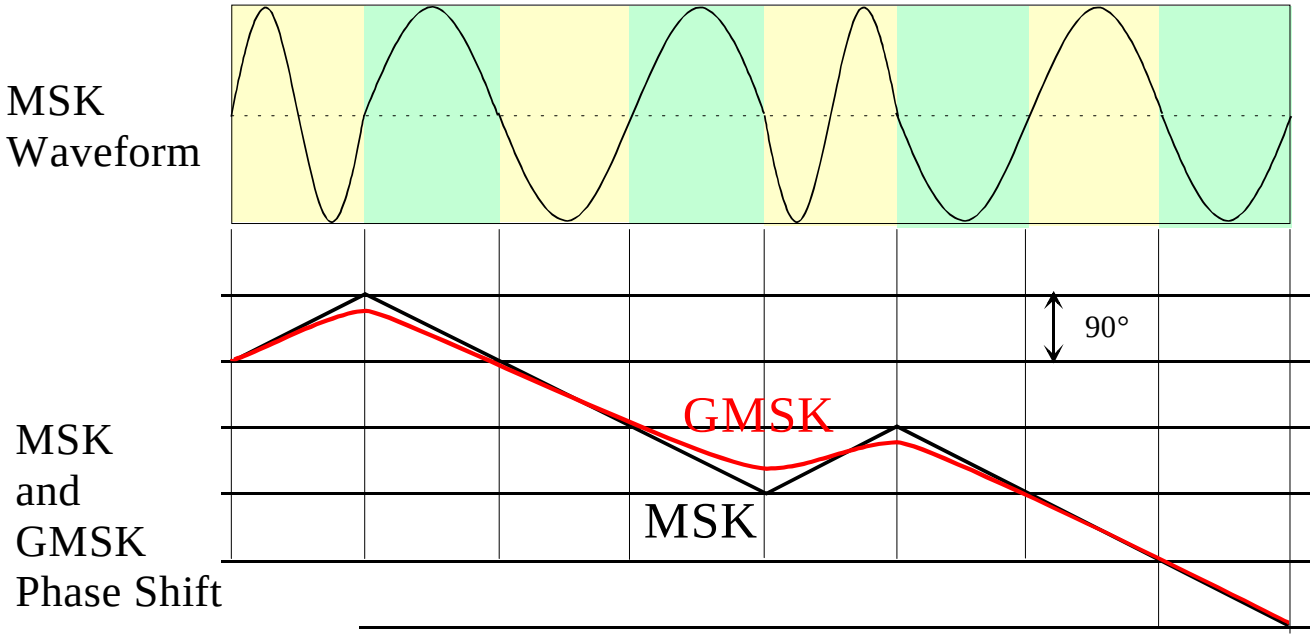
– Minimum spacing that allows two frequencies states to be orthogonal
– Spectrally efficient, easily generated



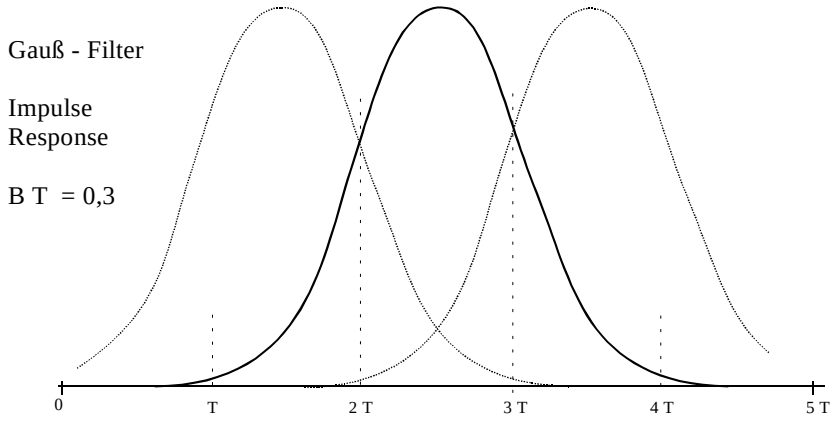
4.5 Gaussian Minimum Shift Keying (GMSK)

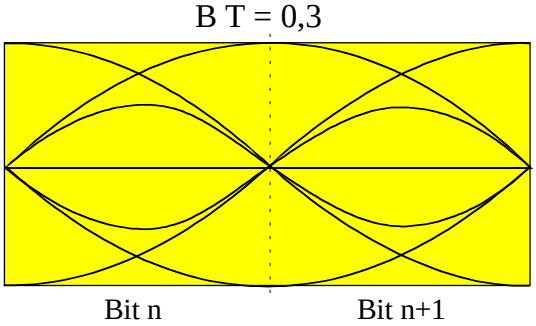
- MSK + premodulation Gaussian low pass filter (No sudden shifts in phase)
- Increases spectral efficiency with sharper cutoff,
- excellent power efficiency due to constant envelope

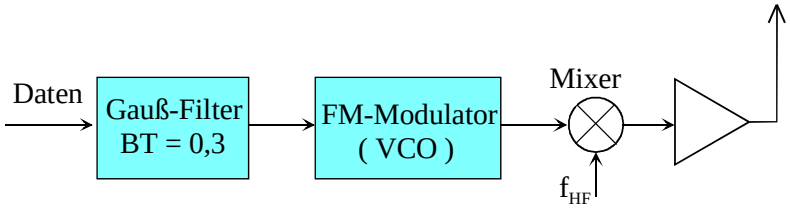
Example: GSM digital cellular: 1.35 bps/Hz DECT cordless telephone: 0.67 bps/Hz



Gaussian Minimum Shift Keying (GMSK)

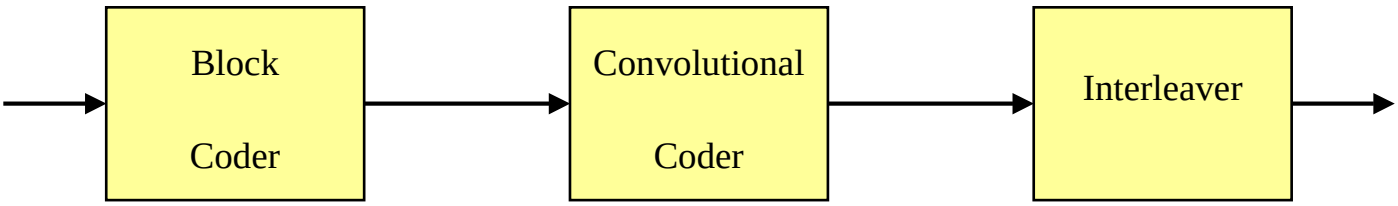






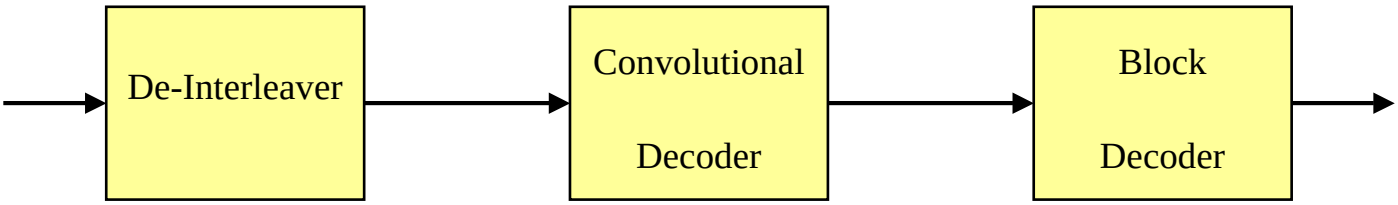
5 Channel Coding

Transmitter

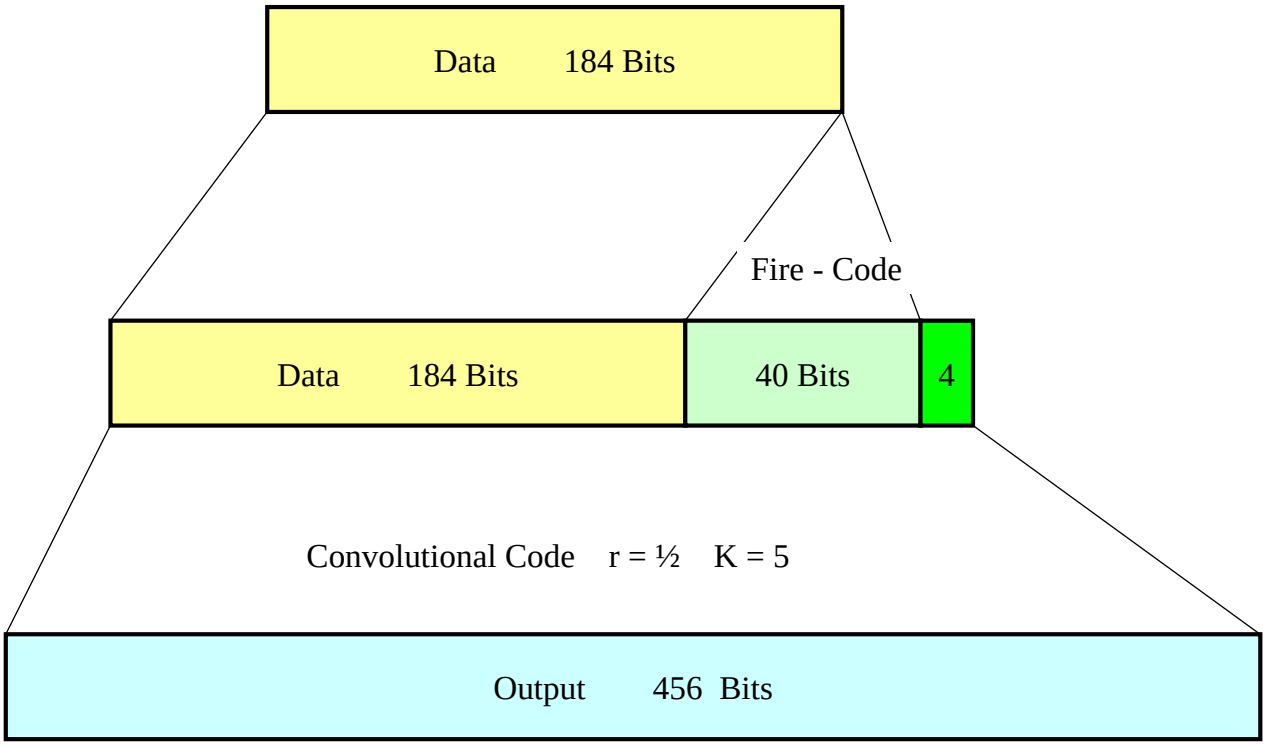


Block Coder:	Error Detection (CRC, 40 Bit Fire Code))
Convolutinal Coder:	Error Correction
Interleaver:	improve coding gain (error bursts)

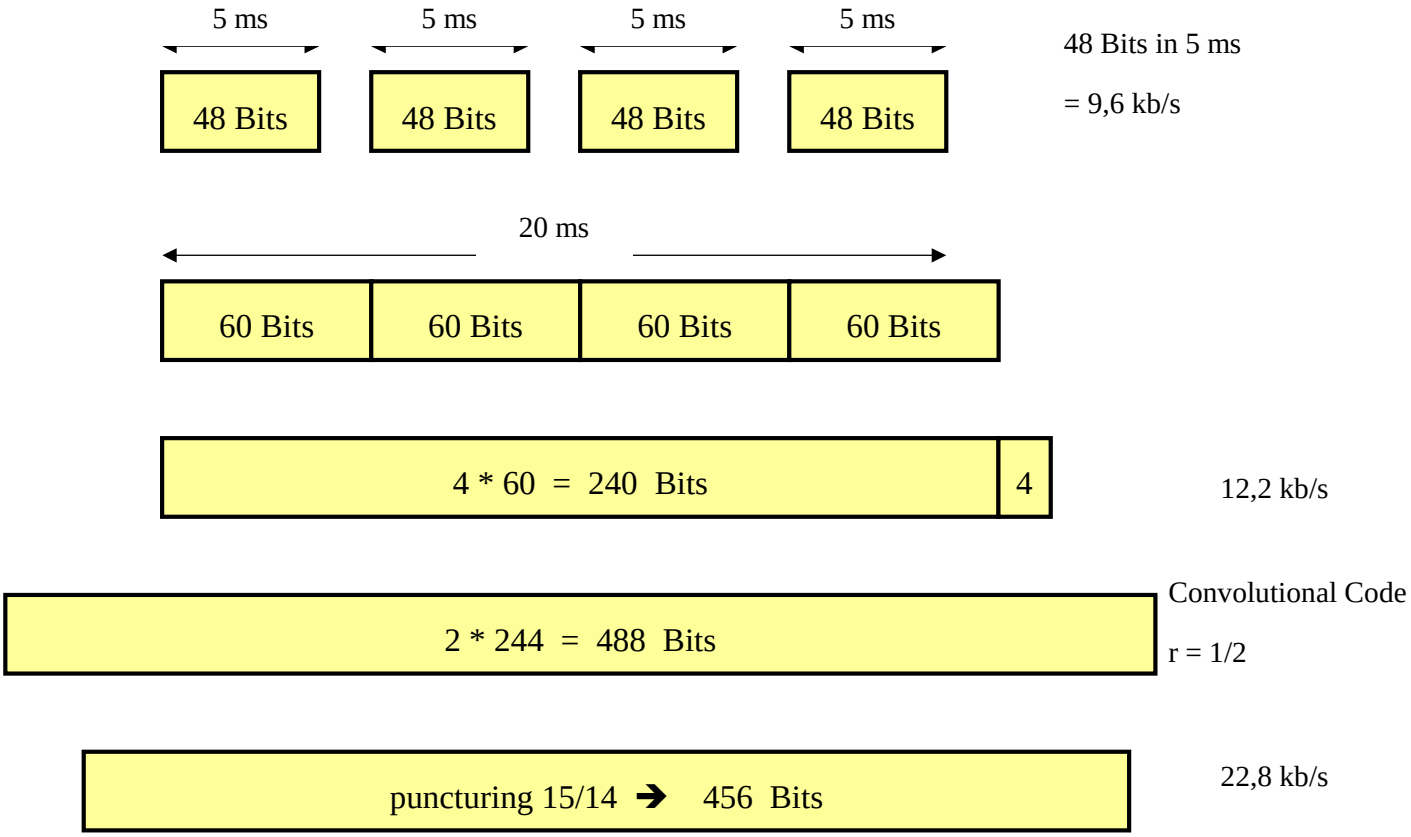
Receiver



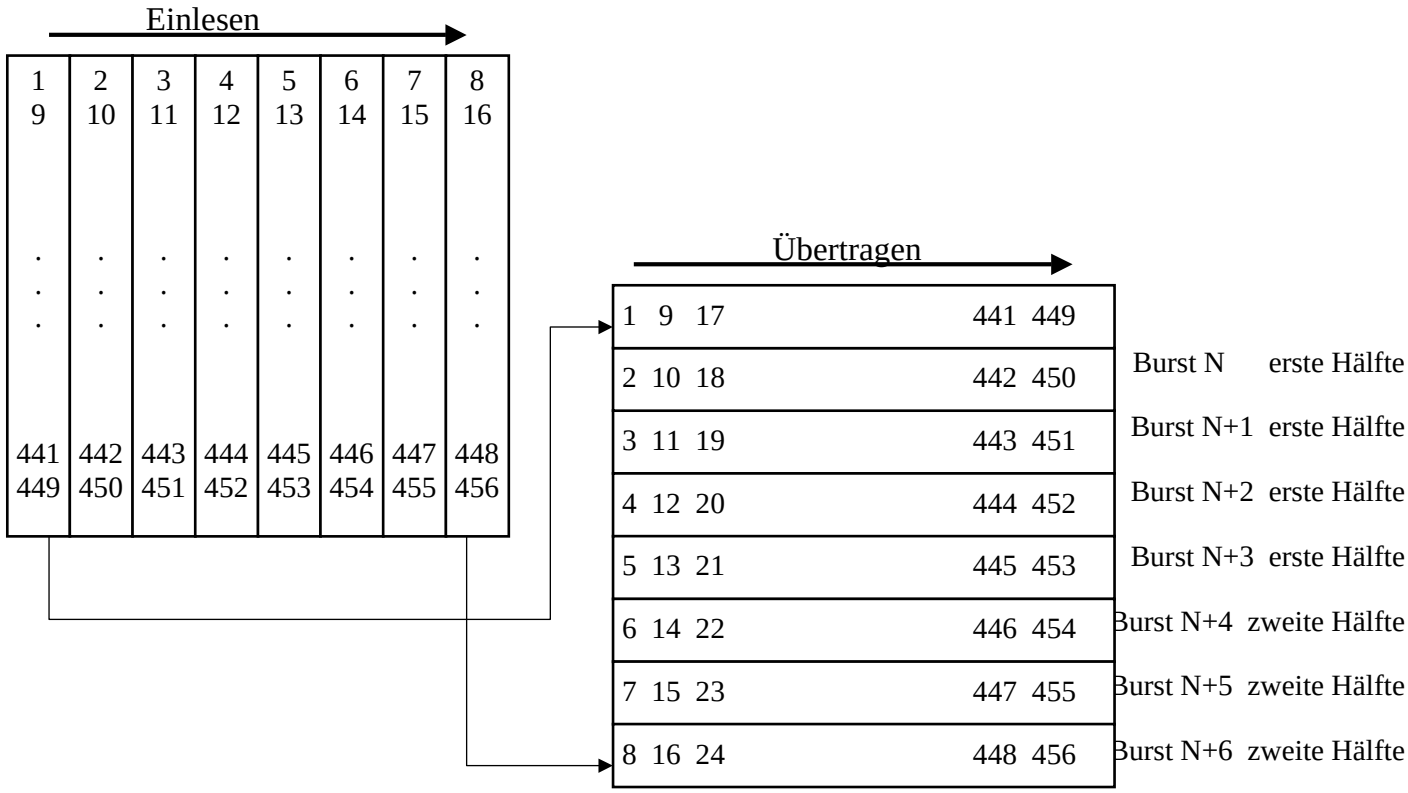
GSM Coding: Error Protection for Signalling



5.1 GSM Coding: Error Protection for Signalling

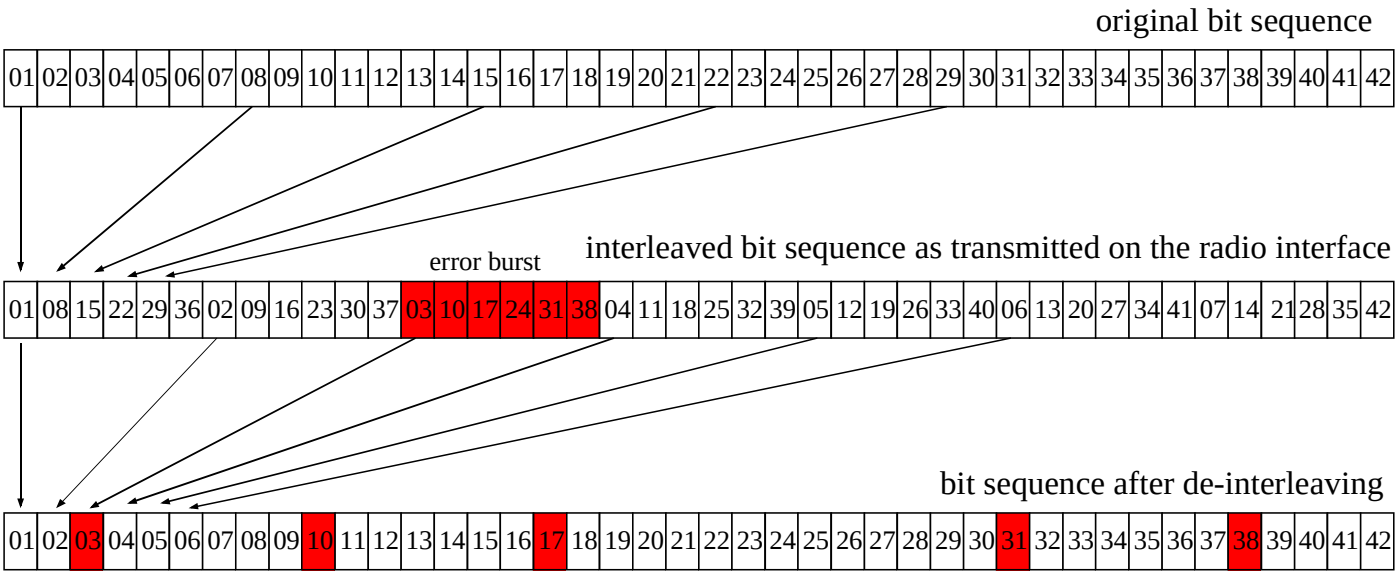


Interleaving of Signalling Messages



Burst N+7 zweite Hälfte

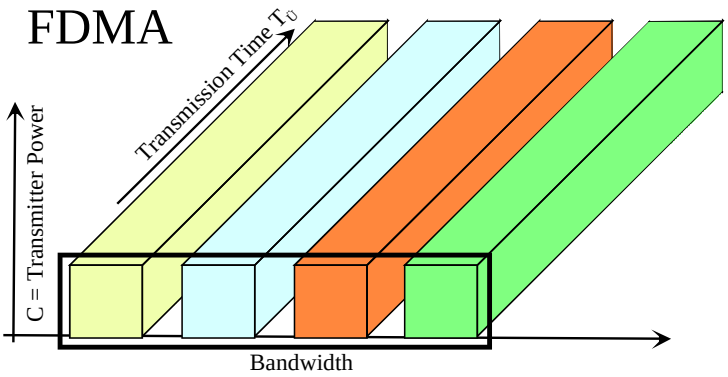
Example for the Interleaving Principle

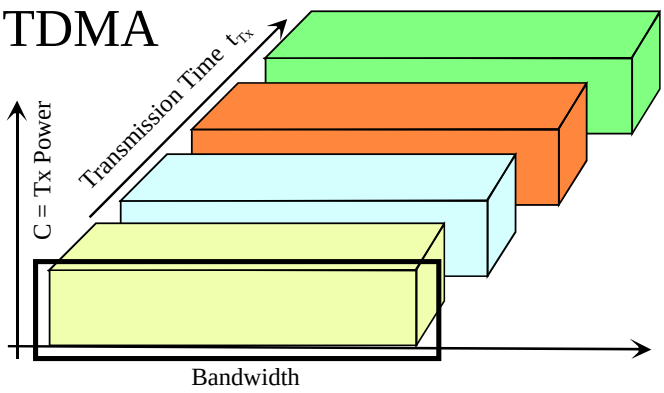


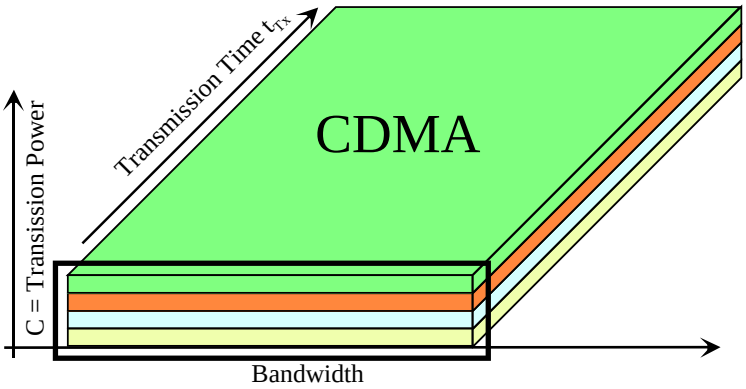
GSM Coding: Interleaving for Signalling

	1st half			2nd half		
Burst N	5	message N-1	453	1	message N	449
Burst N+1	6	message N-1	454	2	message N	450
Burst N+2	7	message N-1	455	3	message N	451
Burst N+3	8	message N-1	456	4	message N	452
Burst N+4	5	message N	453	1	message N+1	449
Burst N+5	6	message N	454	2	message N+1	450
Burst N+6	7	message N	455	3	message N+1	451
Burst N+7	8	message N	456	4	message N+1	452

6 Multiplexing and Multiple Access

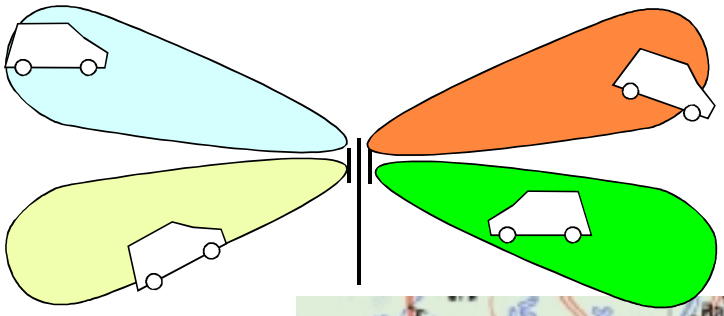






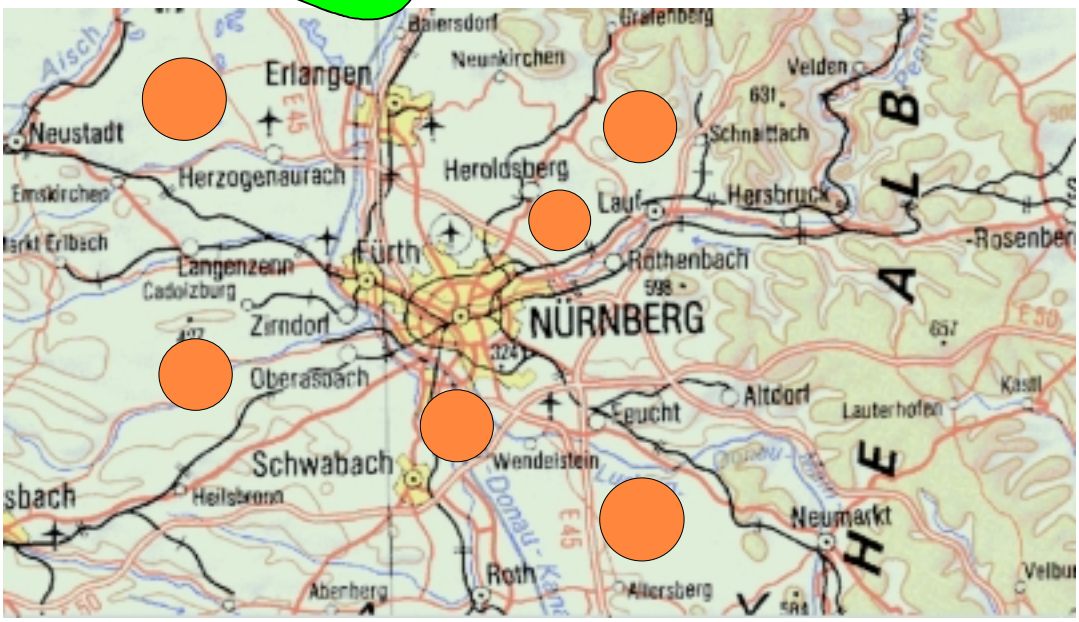
CDMA

Code Division
Multiple Access

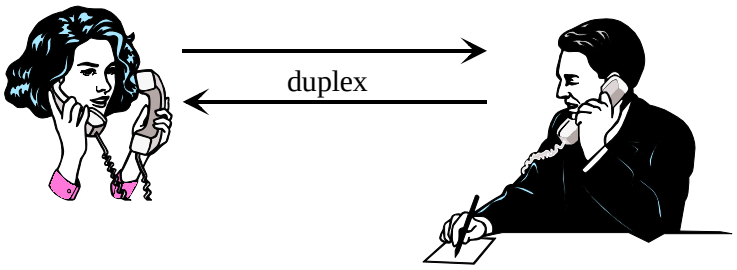


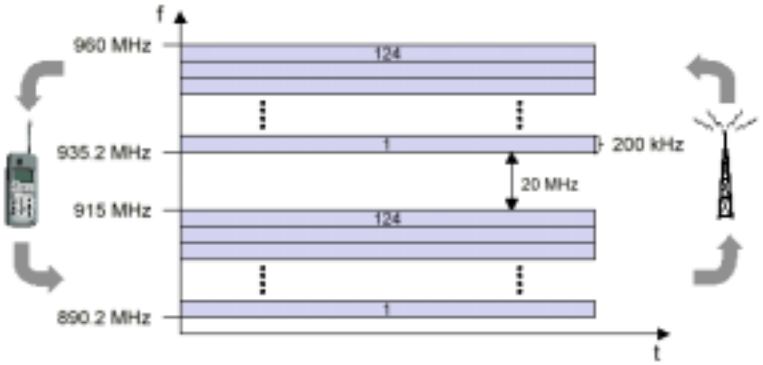
SDMA

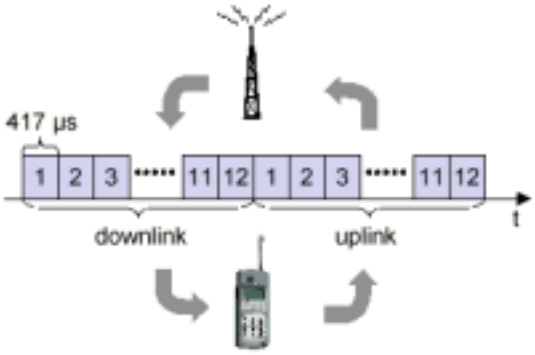
Space
Division
Multiple
Access



6.1 Duplex Transmission







FDD: Frequency Division Duplex

Netz-C, NMT, TACS, GSM, UMTS

TDD: Time Division Duplex

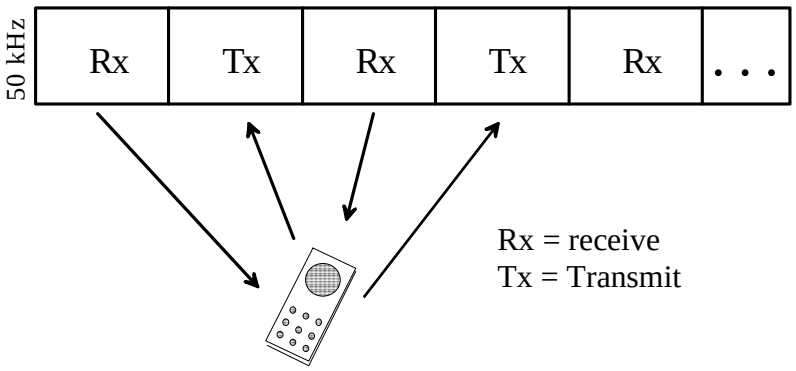
DECT

Multiplex: Dulpex

TDD

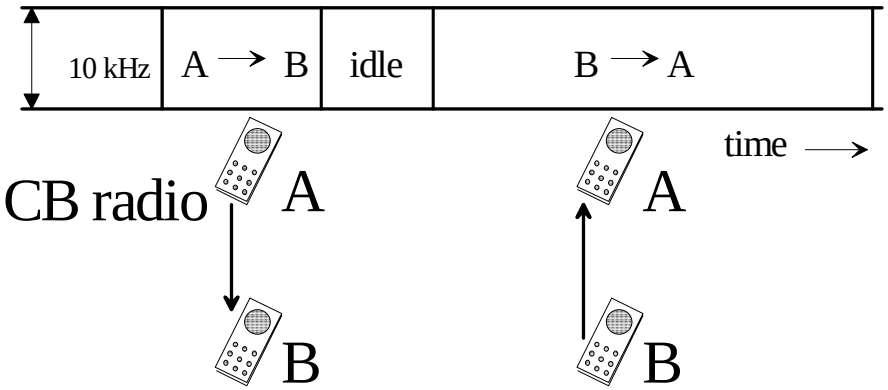
Time Division Duplex

digital systems only

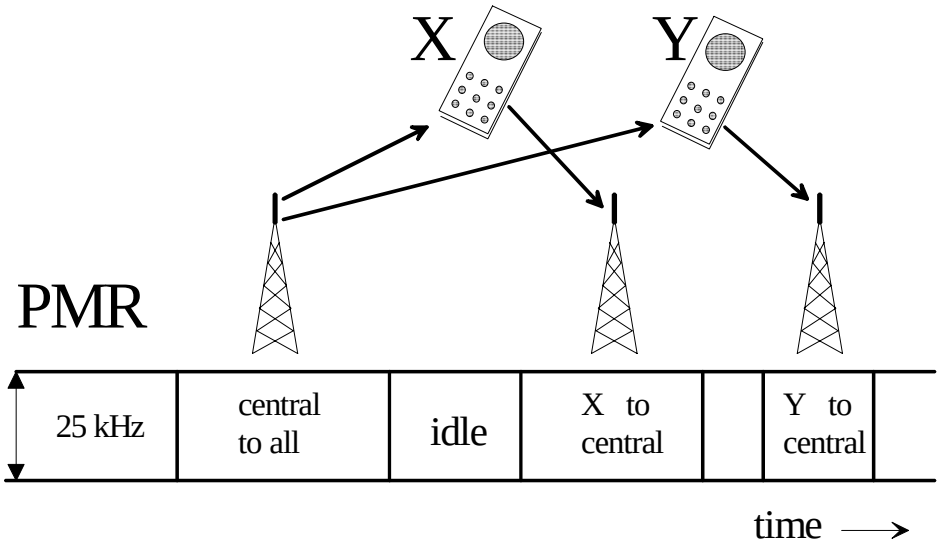


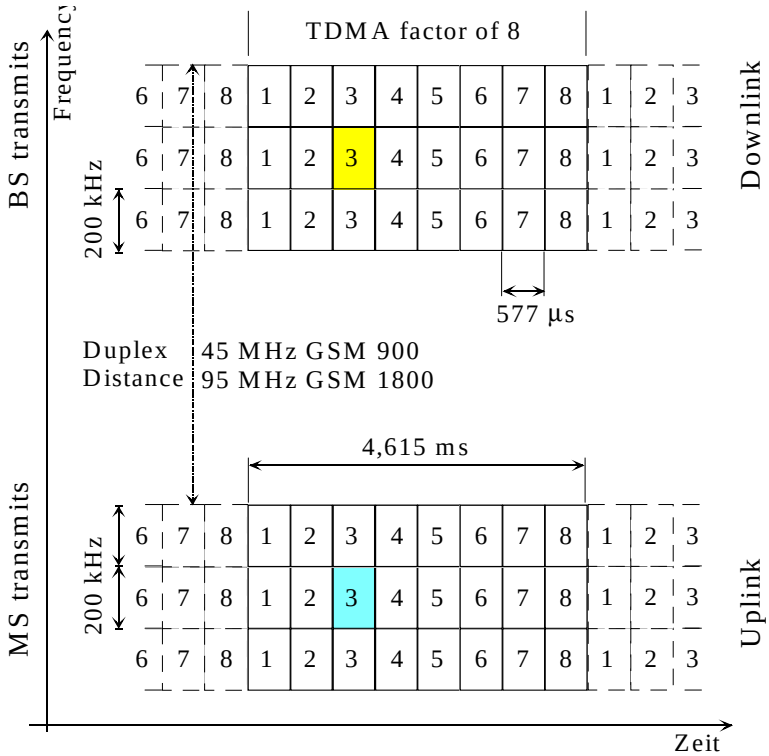
Half Duplex

Only one direction at a time



Half Duplex Transmission

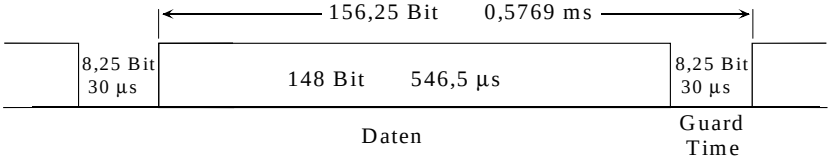




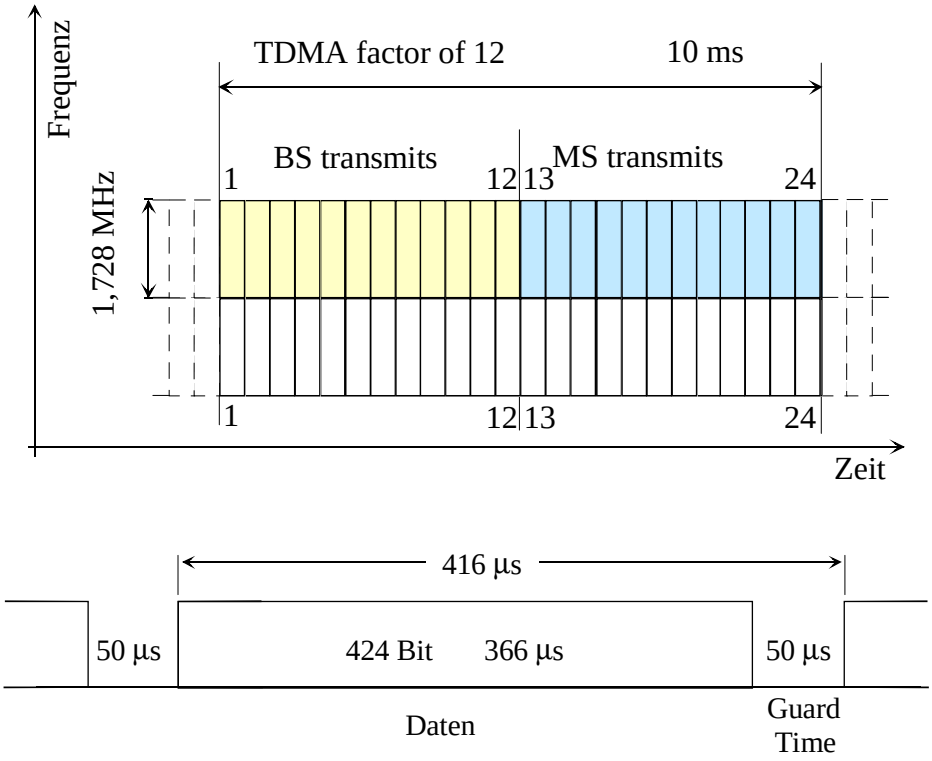
Multiple Access

FDMA	Frequ. Division Multiple Access
TDMA	Time Division Multiple Access
CDMA	Code Division Multiple Access

GSM: =
FDD + TDMA + FDMA



6.2 DECT: TDD + TDMA + FDMA

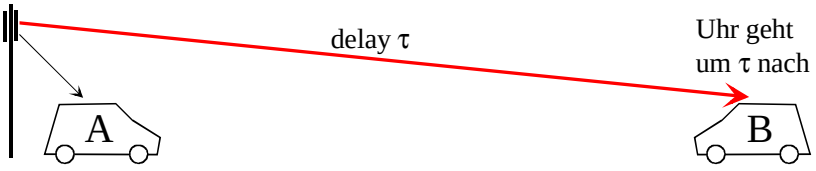


DECT Rahmen : 50 µs Guard Time = 12% des Rahmens

Beispiele

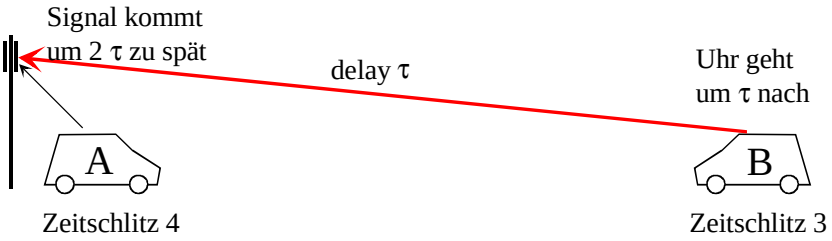
DECT:	TDD	Time Division Duplex
	TDMA	Time Division Multiple Access
	FDMA	Frequency Division Multiple Access
	SDMA	Space Division Multiple Access
GSM:	FDD	Frequency Division Duplex
	TDMA	Time Division Multiple Access
	FDMA	Frequency Division Multiple Access
	SDMA	Space Division Multiple Access
UMTS:	FDD	Frequency Division Duplex
	TDMA	Time Division Multiple Access
	FDMA	Frequency Division Multiple Access
	CDMA	Code Division Multiple Access

6.3 Laufzeitausgleich: Timing Advance

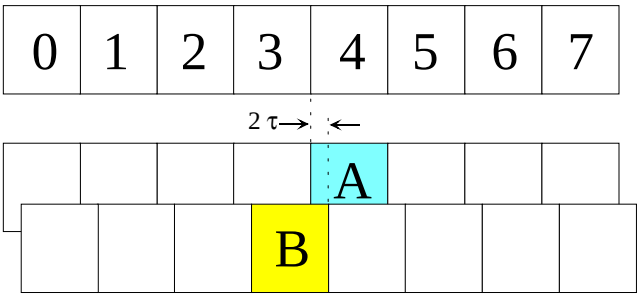


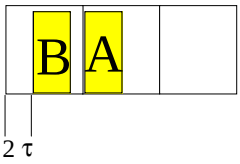
1 Bit = 3,7 µs = 1.107,7 m

1 Bit = 2 τ = 1.107,7 m



Regelbereich: 0...63 Bits



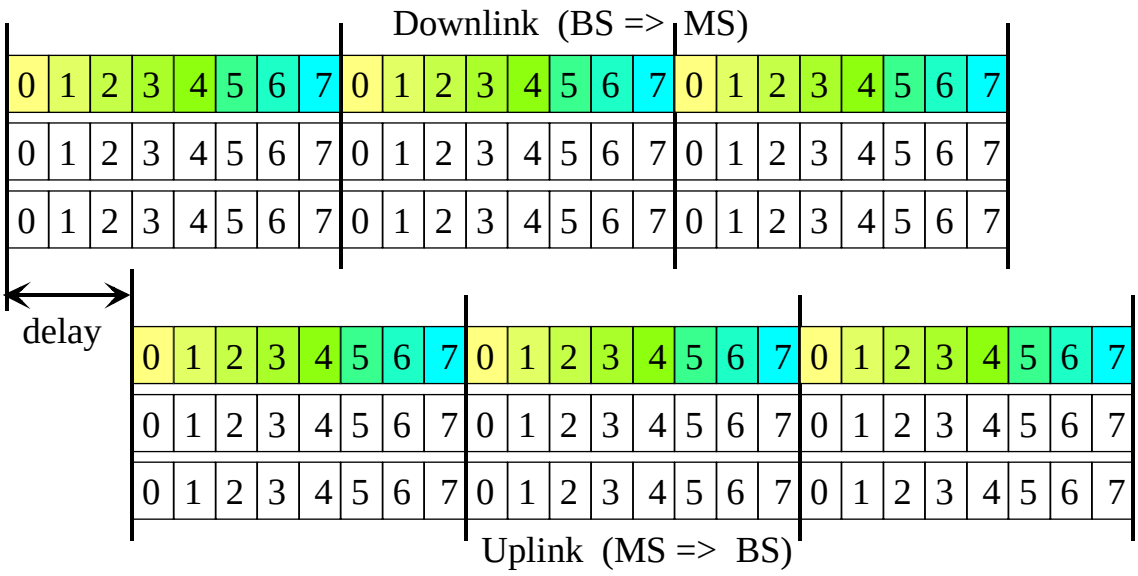


verkürzter Burst
beim ersten Zugriff

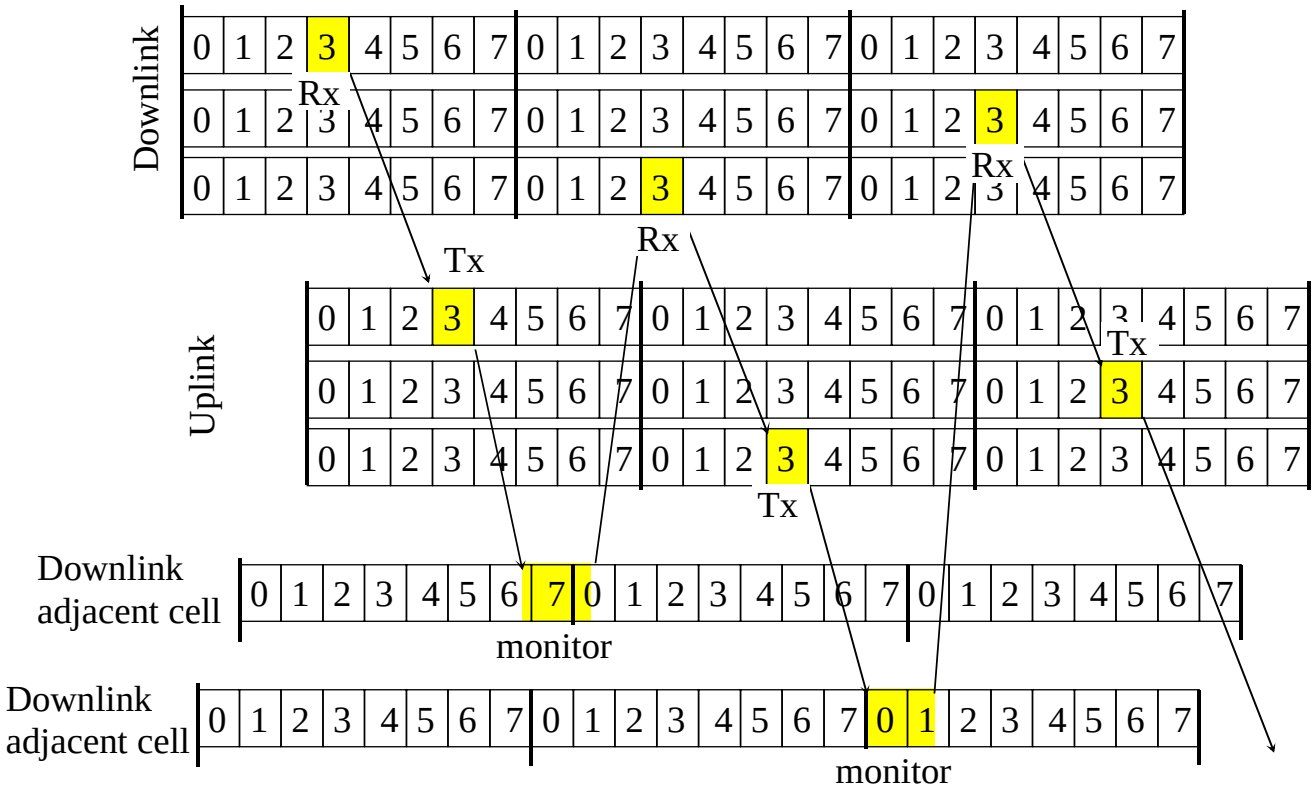
Entfernung:
τ = 0,5 Bit = 553,85 m

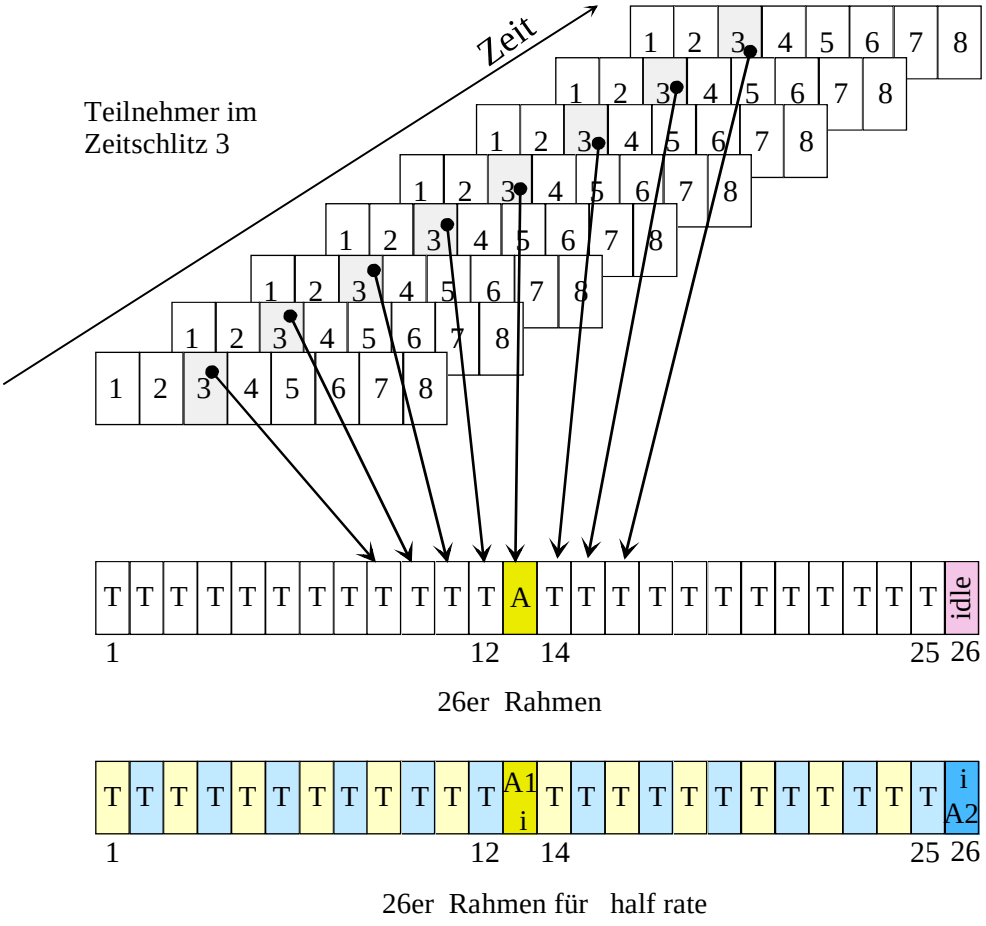
max. Entfernung:
63 Bits * 553,85 m
= 34,9 km

Time Offset between Uplink and Downlink



6.4 Monitoring Neighbour Cells





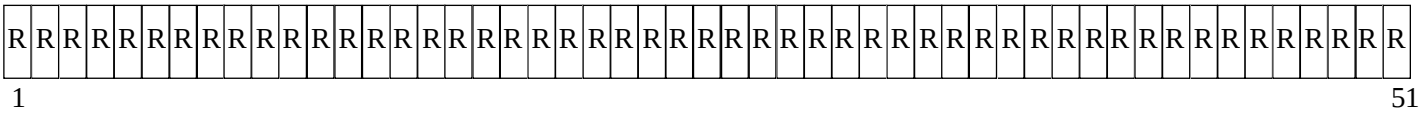
6.5 Multi Frame with 26 Frames

TCH Traffic Channel

SACCH Slow Associated Control Channel

6.6 Multi Frame with 51 Frames

Downlink:



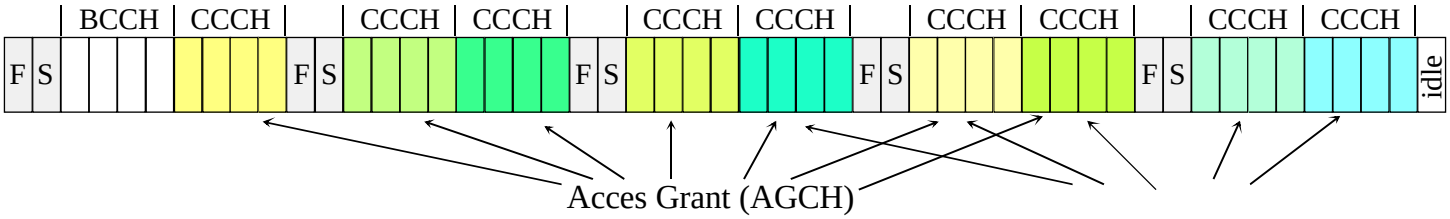
FCCH	Frequency Correction Channel	SCH	Synchronisation Channel
BCCH:	Broadcast Control Channel	CCCH	Common Control Channel
RACH	Random Access Channel		

51er Rahmen, damit ständiges zeitliches Gleiten zum 26 Rahmen gewährleistet ist (kein gemeinsamer Teiler)

Synchronisation der Mobilstation: FCCH ➔ SCH ➔ BCCH

51 - Multi Frame

Common Control Channel: Downlink



Dedicated Control Channel: 2 * 51 - multi frame

Downlink

D0	D1	D2	D3	D4	D5	D6	D7	A0	A1	A2	A3	-	-	-
D0	D1	D2	D3	D4	D5	D6	D7	A4	A5	A6	A7	-	-	-

Uplink

A5	A6	A7	-	-	-	D0	D1	D2	D3	D4	D5	D6	D7	A0
A1	A2	A3	-	-	-	D0	D1	D2	D3	D4	D5	D6	D7	A4

6.7 GSM Channels

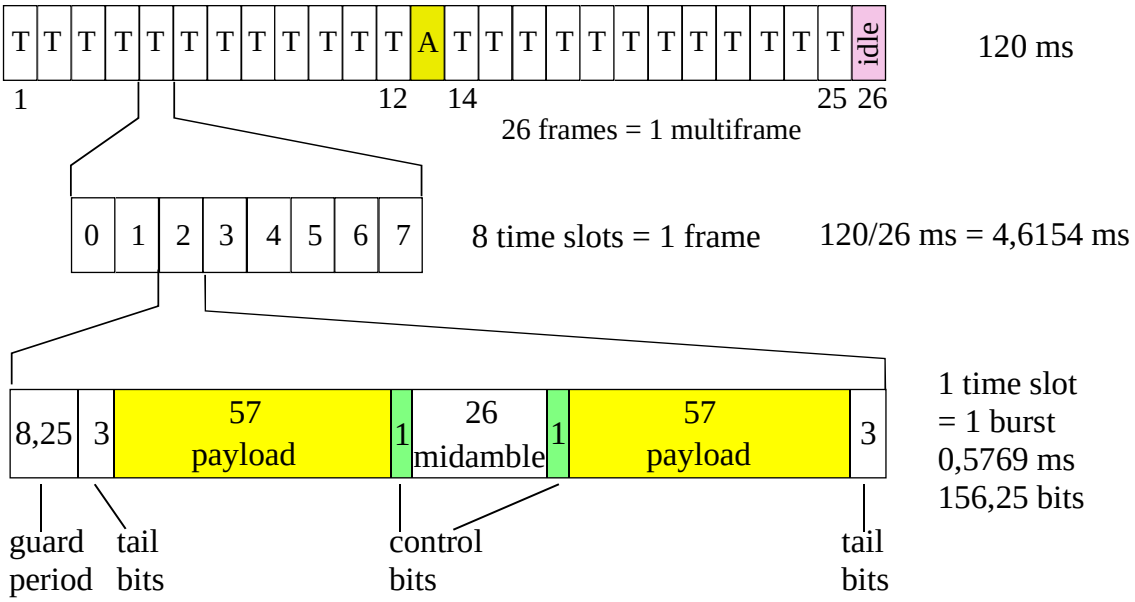
Common Control Channels (signalling)

Broadcast Channels			Common Control Channels		
FCCH	Frequency Correction Channel	downlink	PCH	Paging Channel	downlink
SCH	Synchronisation Channel	downlink	AGCH	Access Grand Channel	downlink
BCCH	Broadcast Control Channel	downlink	RACH	Random Access Channel	uplink

Dedicated Channels (user data)

Traffic Channels	Control Channels	Associated Control Channels
	SDCCH 8 (4)	SACCH 8 (4)
TCH /F	FACCH /F	SACCH /TF
TCH /H	FACCH /H	SACCH /TH
PDTCH		PACCH

GSM Multiplexing Scheme



Gross bit rate: 270,8 kb/s

Bit length; 3,692 µs

GSM Bit Rates

Festlegung: 26er Multi-Frame = 120 ms

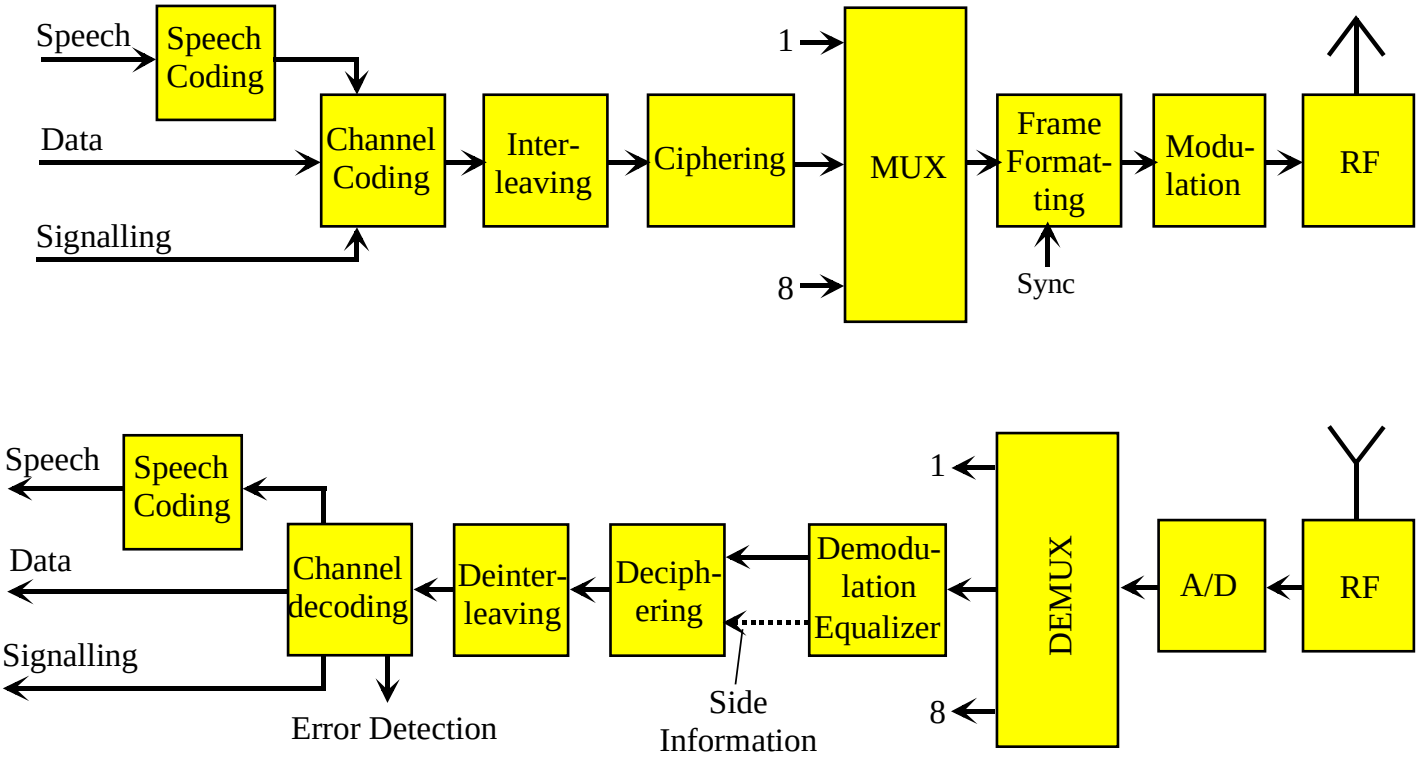
26 Frames	= 1 Multi-Frame	➔	1 Frame	= 120 ms / 26	= 4,6154 ms
1 Frame	= 8 Bursts	➔	1 Burst	= 120/(26*8)	= 0,5769 ms
1 Burst	= 156,25 Bit	➔	1 Bit	= 120/(26*8*156,25)	= 3,692 µs
1 Bit	= 3,692 µs	➔	Brutto-Bitrate	= 1/3,692 µs	= 270,833 kb/s

1 Nutzkanal: mit Overhead: 1/8 der Brutto-Bitrate = 270,833 kb/s / 8 = 33,85 kb/s

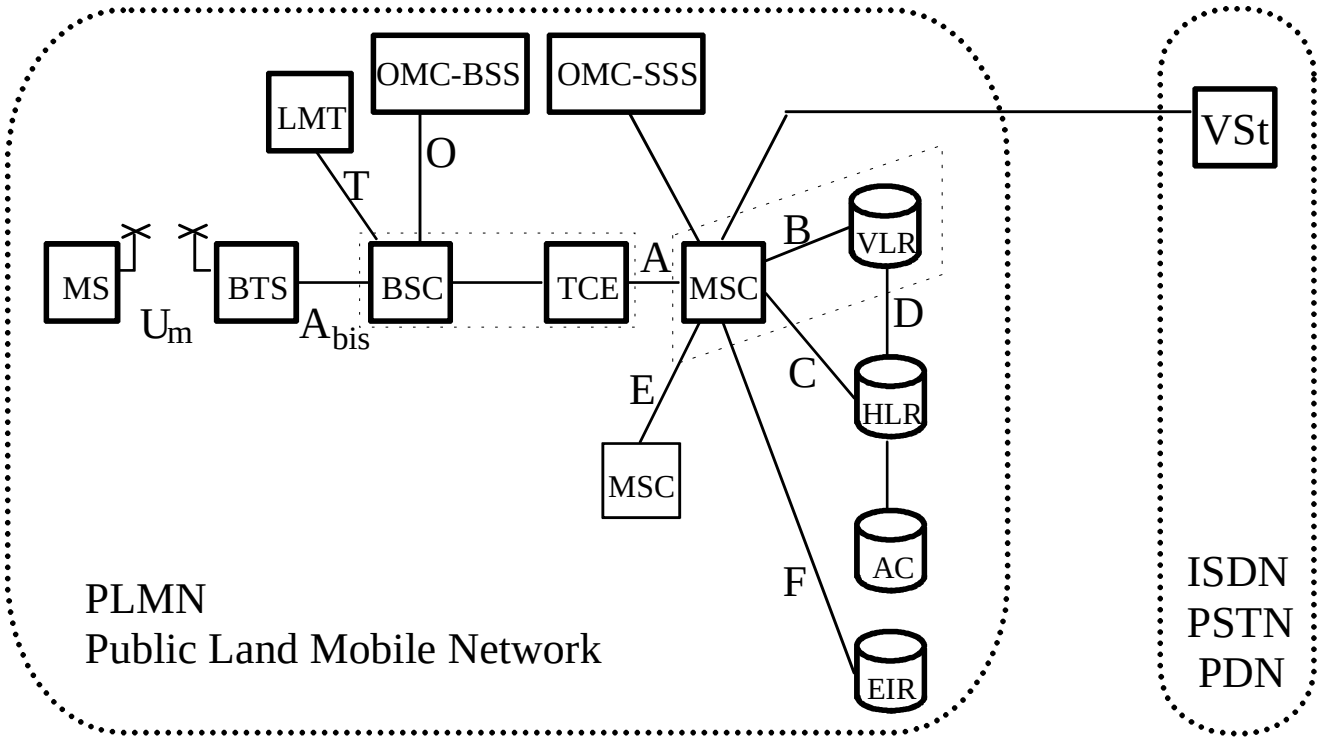
nur Nutzdaten: 2*57 Nutz-Bits / Burst = 114 Bit / 4,615 ms = 24,7 kb/s

TCH brutto:	nur 24 Frames aus dem 26er Rahmen:	24,7 kb/s * 24 / 26	= 22,8 kb/s
SACCH brutto:	1 Frame der 26er Rahmens:	24,7 kb/s (Nutzdatenrate) * 1 / 26	= 0,95 kb/s
SDCCH/8 brutto:	4 Frames im 51er Rahmen:	24,7 kb/s * 4 / 51	= 1,937 kb/s

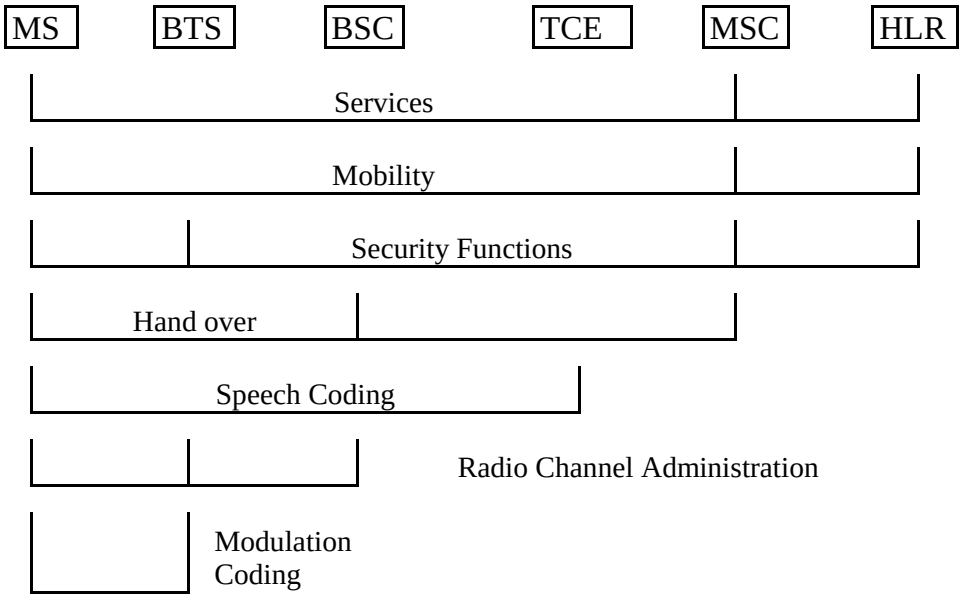
6.8 Functional Diagram of GSM Transmission Part



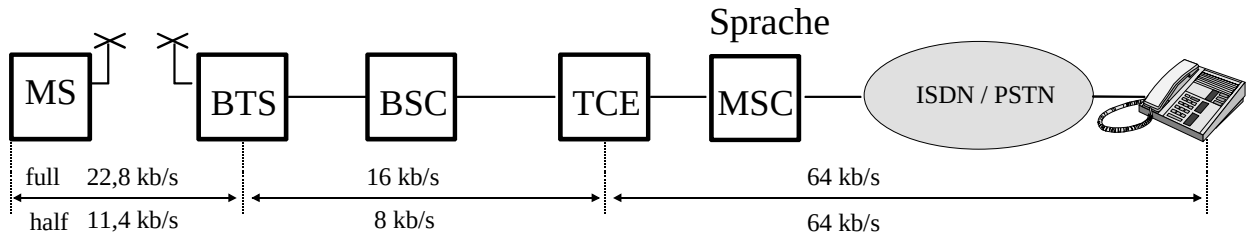
7 System Overview

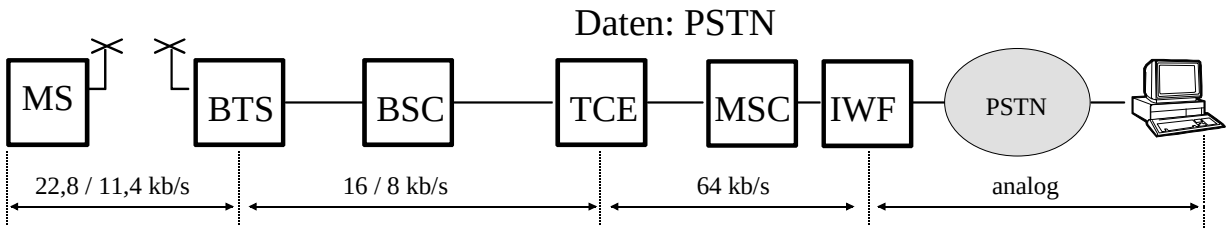


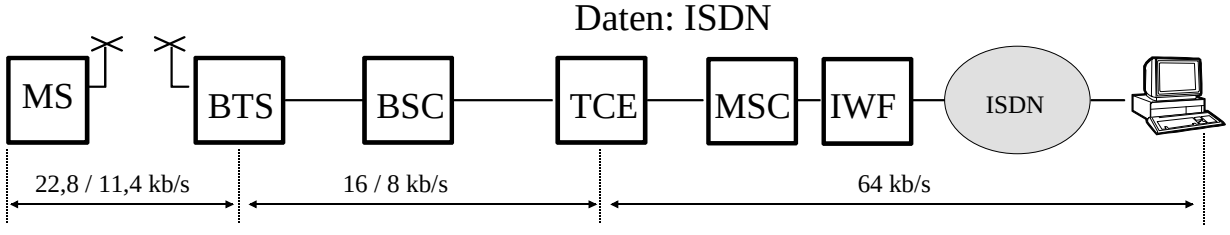
Functional Split



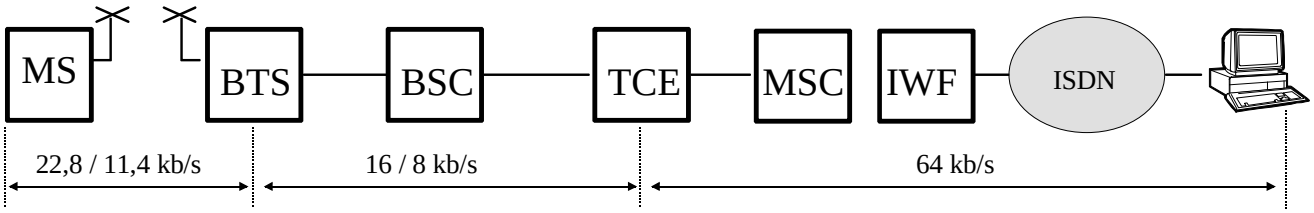
7.1 Speech / Data Transmission



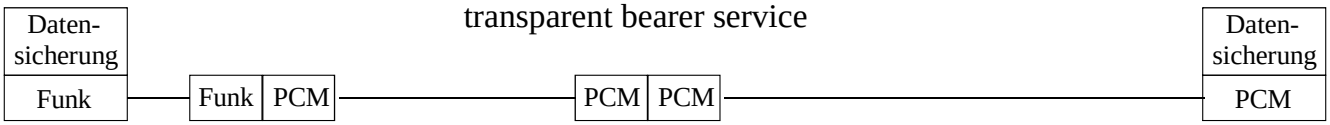




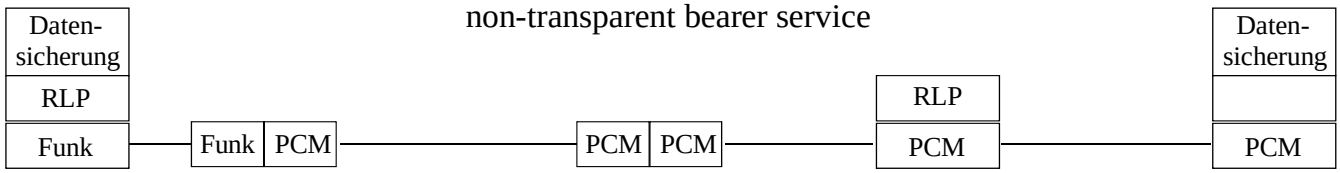
Data Transmission : T and NT



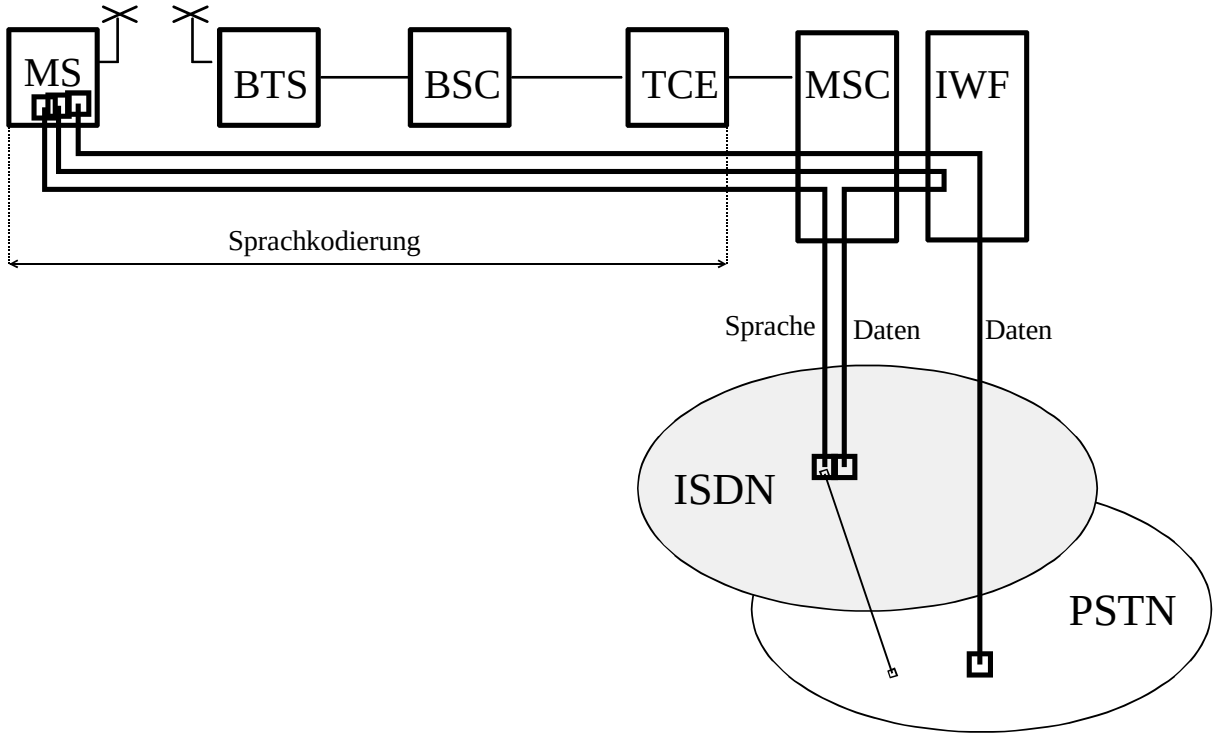
transparent bearer service



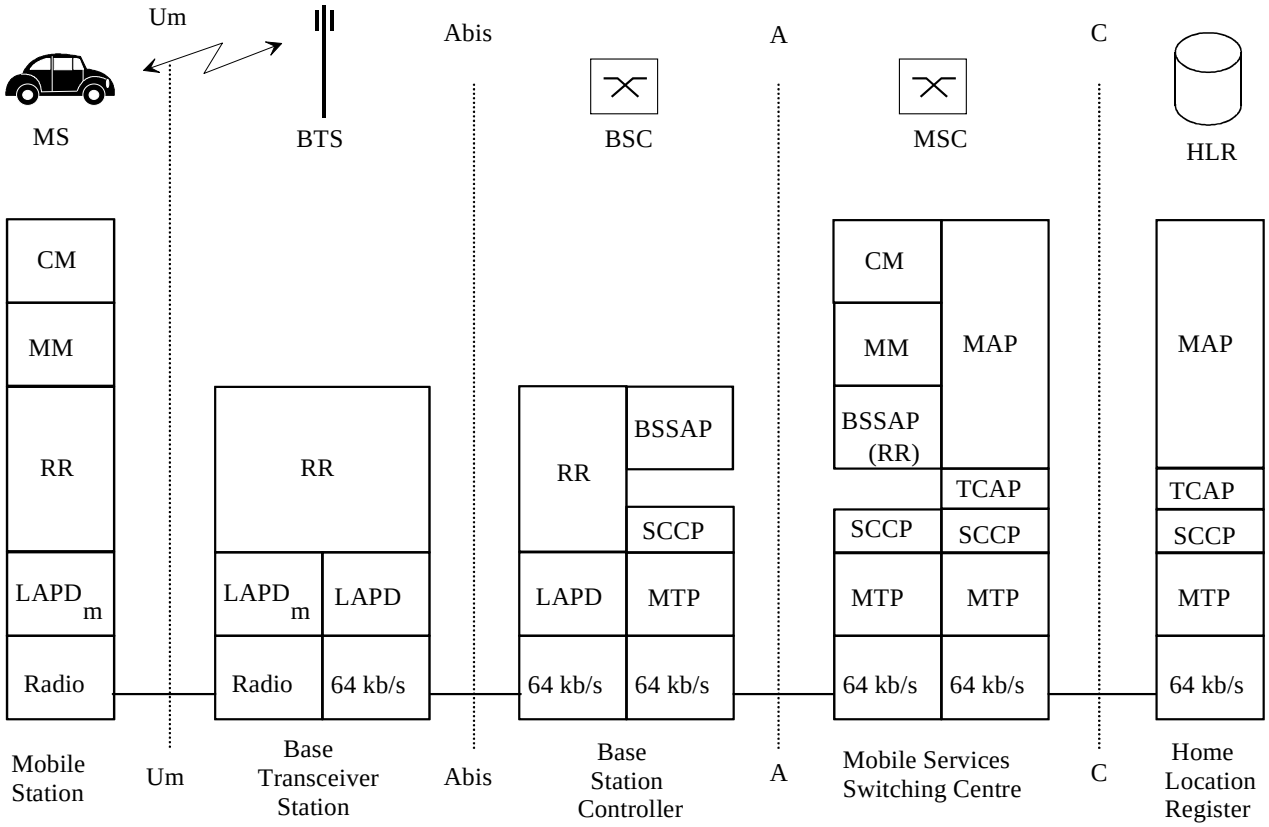
non-transparent bearer service



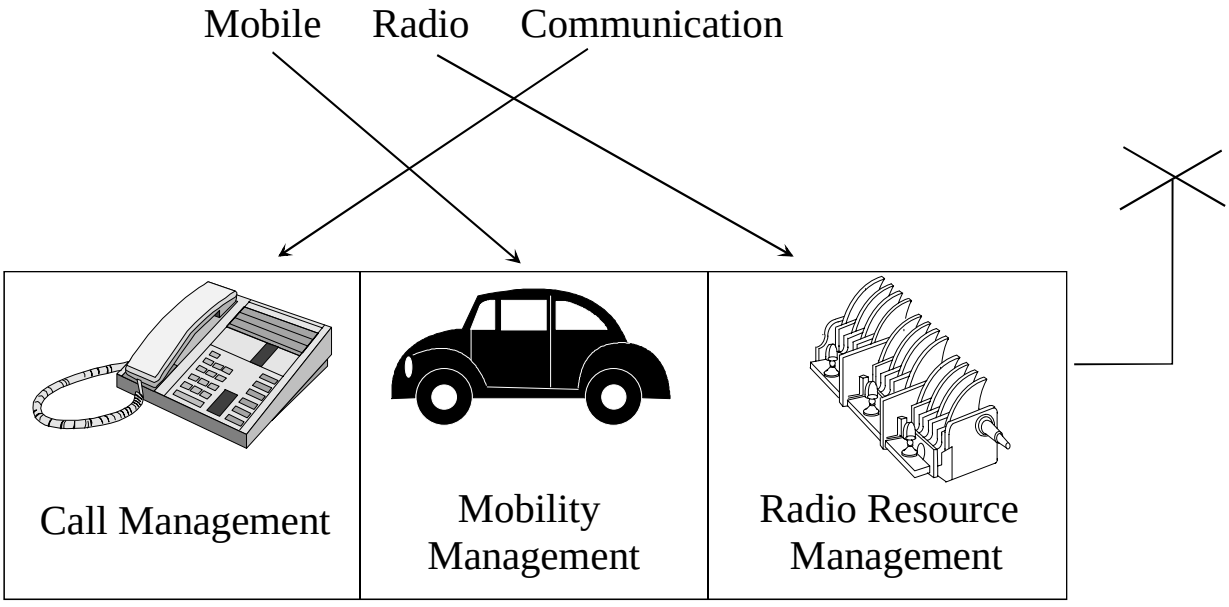
Multi - Numbering



7.2 GSM Protocol Model



Main GSM Protocol Layer



8 RR: Radio Resource Management

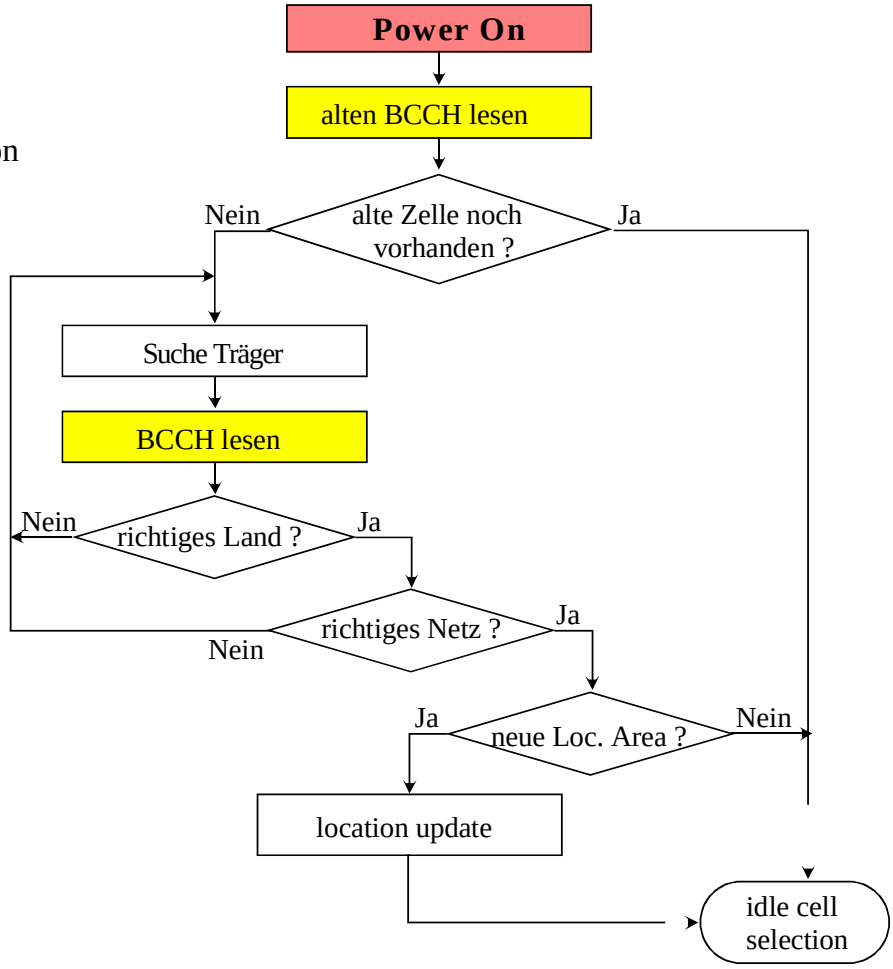
Synchronisation mit dem Netz:	Frequency Correction Channel TDMA Synchronisation (SCH) Timing Advance
Systeminformation	BCCH Broadcast
Auswahl der Zelle:	idle mode selection measurement reports
Funkkanal	paging channel request channel assignment channel mode modify channel release handover
sonstiges	class mark ciphering power control Discontinuous Transmission DTX

8.1 BCCH: System Information Broadcasting

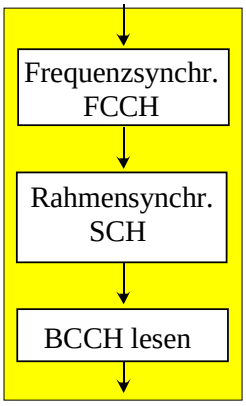
Is it the right country and operator ?	• Location area identification	MCC + MNC + LAC
	• Cell identity	
Can the MS stay in this cell ?	• Cell selection parameters	Cell selection hysteresis, min. received signal level
How is (are) the control channel(s) configured	• Control channel description blocks;	number of CCCHs & AGCH- IMSI attach on/off
	• RACH control parameters	cell barred ? access repetions
	• Cell channel description	radio frequencies used in the cell
	• Cell options	Power control (UL/DL) Discontinuous transmission
Which cell shall be monitored ?	• Neighbour cells description	frequencies of neighbour cells
	• PLMN permitted	NCC of neighbour cells permitted
	• Short Message Cell Broadcast available ?	Channel description

8.2 Cell Selection

Initial Cell Selection

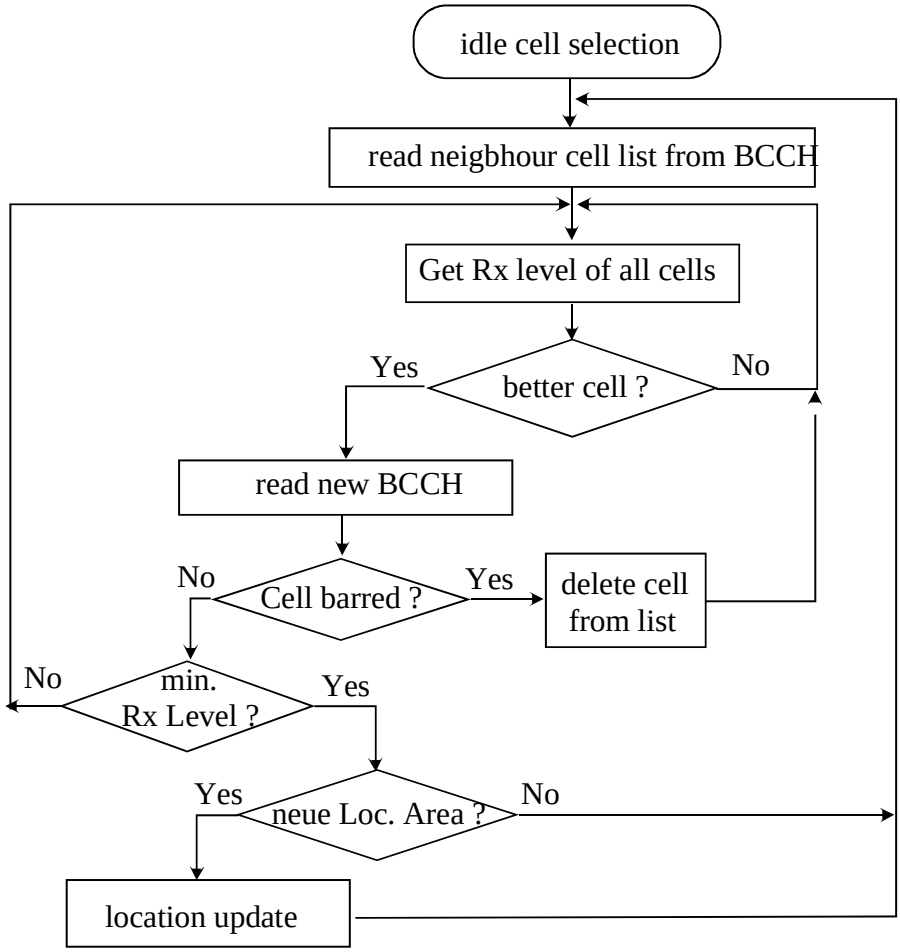


Broadcast Channel Lesen



Idle Cell Selection

The Mobile Station
has found a cell
and monitors
the neighbour cells continuously



8.3 RR - Procedures

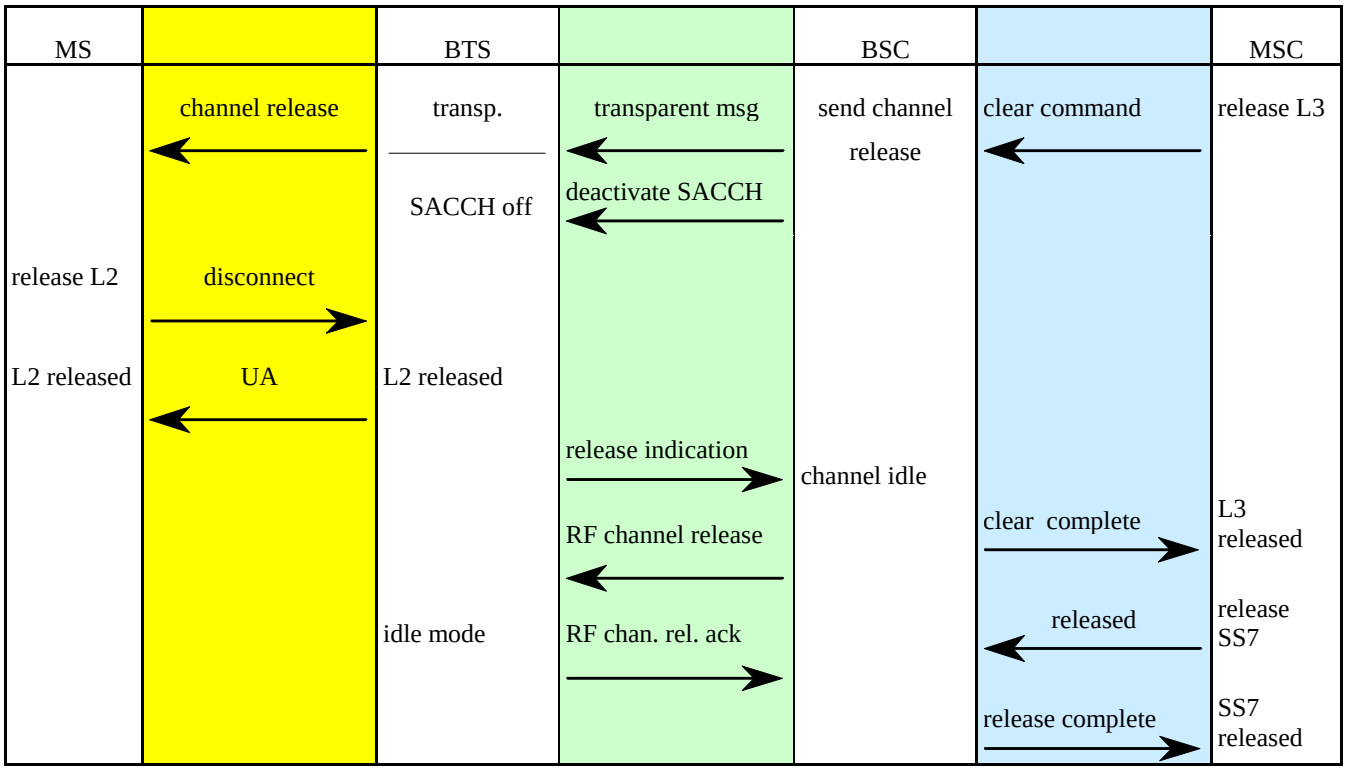
Mobile Originated RR-Connection-Establishment

MS	Um - Interface	BTS	Abis - Interface	BSC	A - Interface	MSC
send msg. on RACH	channel request →					
		forward CCH-msg.	channel required →			
		initialise DCCH: Tx, Rx on	channel activation ←	select idle DCCH		
			channel act. ackn. →	assign DCCH to MS		
tune to DCCH	immed assignment ←	send on AGCH	immed assign cmd ←			
establish L2	SABM + CM_Service_request →					
		confirm L2 establishm.	CM Service_request →	establ. SS7 connection	connect request + compl. L3 info →	
	UA + CM Service_request ←				connect confirm ←	establ. SS7 connection
	Address = individ. radio channel		Address = radio channel number		Address = local reference	

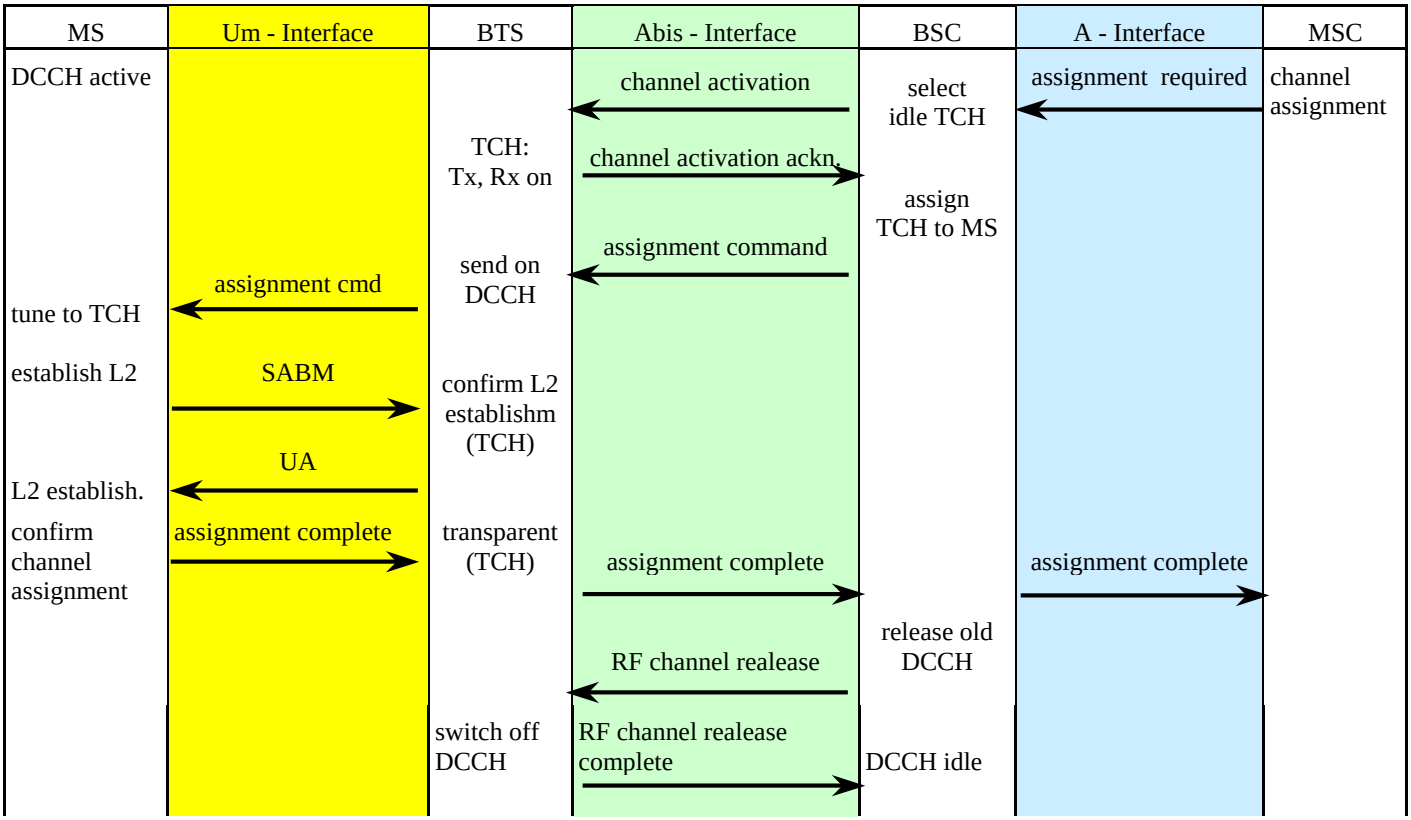
Mobile Terminating RR - Connection Establishment

MS	Um - Interface	BTS	Abis - Interface	BSC	A - Interface	MSC
establish RR-connection	paging request ←	send on AGCH	paging command ←	page all cells of locat. area	←	page MS
send msg. on RACH	channel request →					
		foreward CCH-msg.	channel required →			
		initialise	channel activation ←	select idle DCCH		
		DCCH: Tx, Rx on	channel act. ackn. →	assign		
tune to DCCH	immed assignment ←	send on AGCH	immed assign cmd ←	DCCH to MS		
establish L2	SABM + paging response →					
	UA + paging response ←	confirm L2 establishm.	paging response →	establ. SS7 connection	connect request + compl. L3 info →	
					connect confirm ←	establ. SS7 connection
	Address = individual radio channel		Address = radio channel number		Address = local reference	

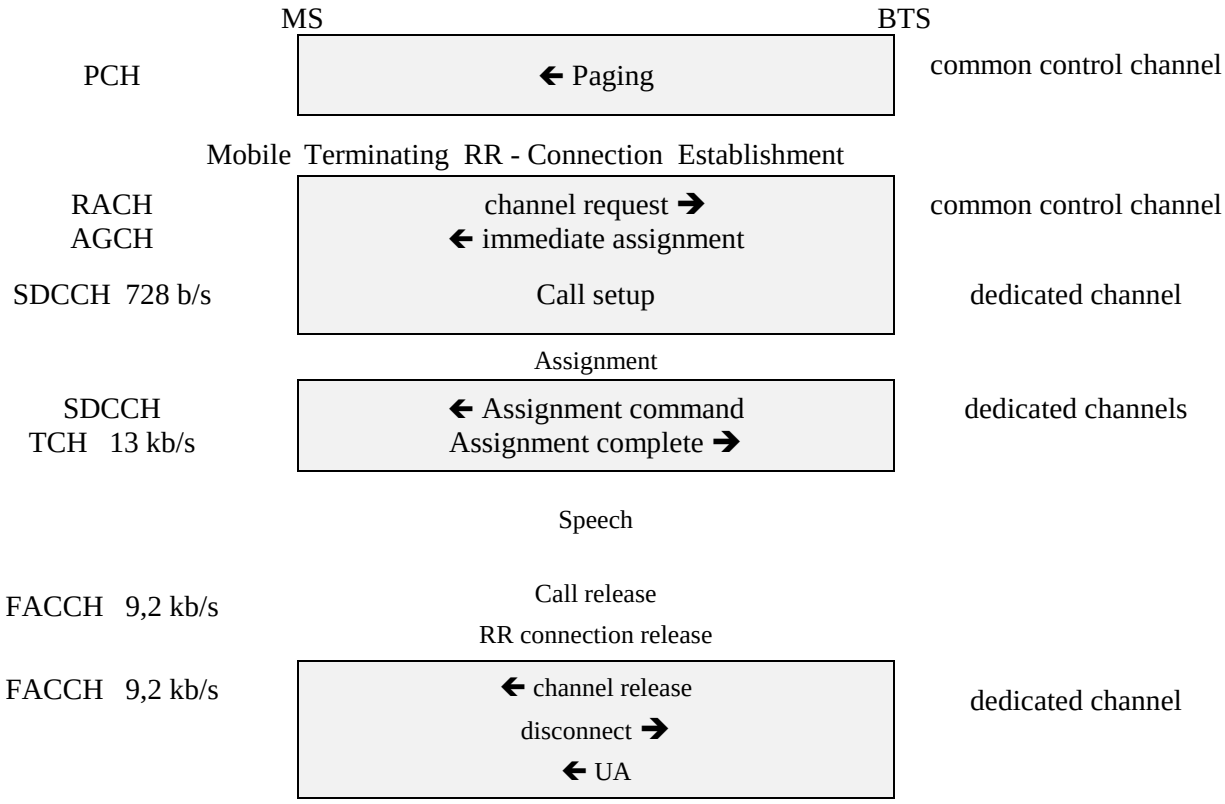
RR-Connection Release



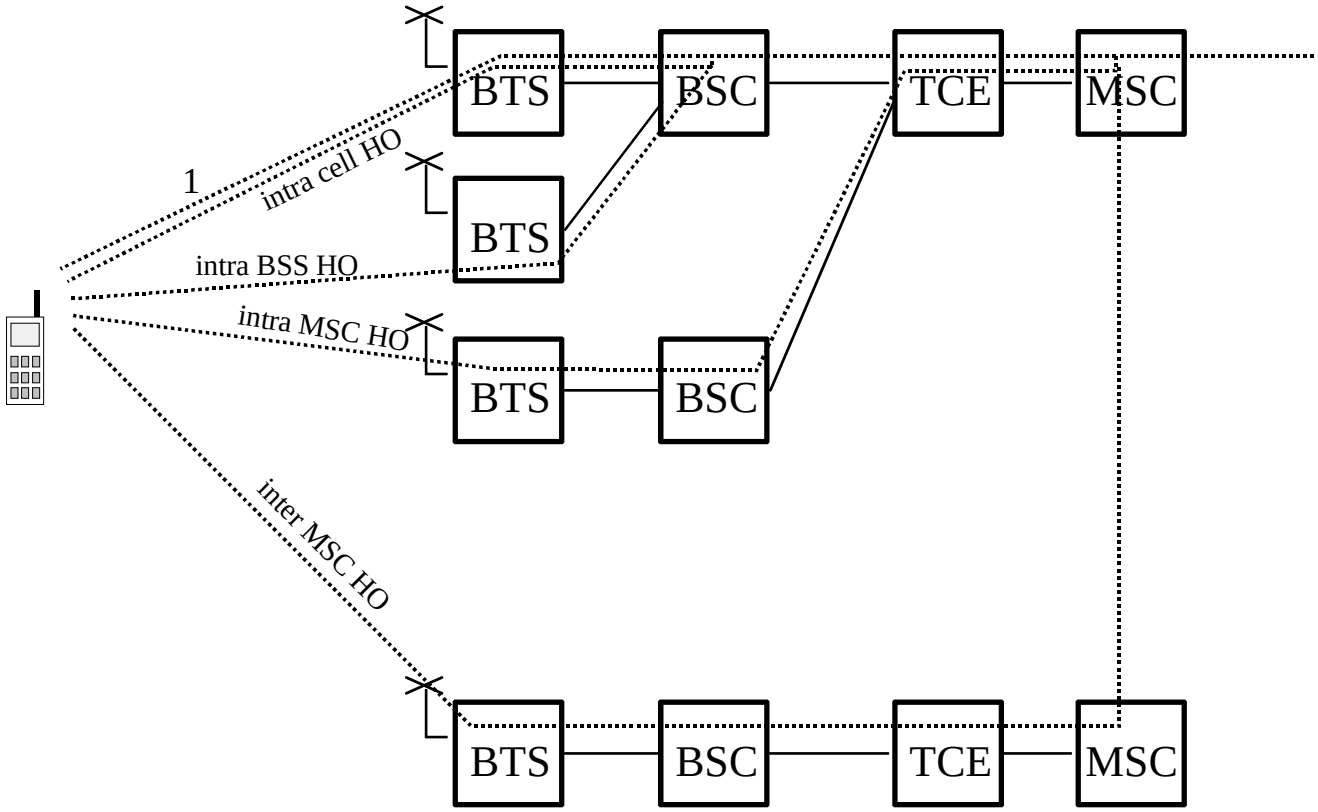
Channel change: Assignment



RR Messages during a Call



8.4 Handover



Handover Measurements

BSC: Liste der Nachbarzellen wird über SACCH zur MS übertragen

MS: Messung der Feldstärke der Frequenzen aus der Liste der Nachbarzellen

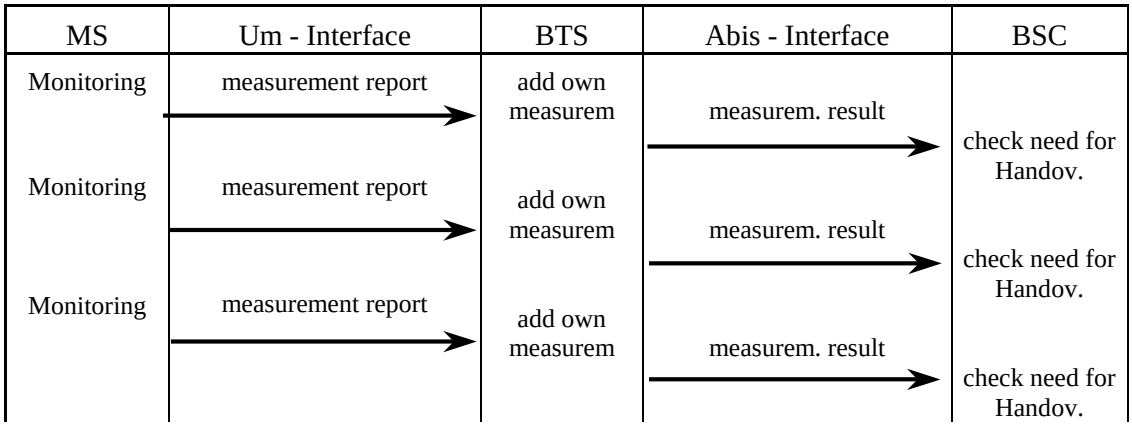
BSIC im 'Idle Slot' lesen

Mittelung der Meßwerte über 480 ms

Datenübertragung alle 480 ms über den SACCH:

- Die 6 stärksten Nachbarzellen (Frequenz, BSIC, RxLev_NCell)
- Die empfangene Leistung der Serving Cell (RxLev_DL) (Down Link)

BSC: Sortieren der Nachbarzellen und Langzeitmittelwert bilden



Handover Decision

Power Budget

Path Loss zur Serving Cell: Sendeleitung der BS - Empfangsleistung der MS: BS-TxPwr - RxLev_DL

Path Loss zur Zelle N: Sendeleitung der BS-N - Empfangsleistung der MS: BS-TxPwr - RxLev_NCell

Handover if: Path Loss from MS to cell N + Hysteresis < Path Loss from MS to Serving Cell

Minimaler Empfangspegel

Der Empfangspegel der Serving Cell wird so klein, daß das Gespräch abzureisen droht.

Distance

Die Entfernung der MS zur Serving Cell wird zu groß.

Messung über Timing Advance

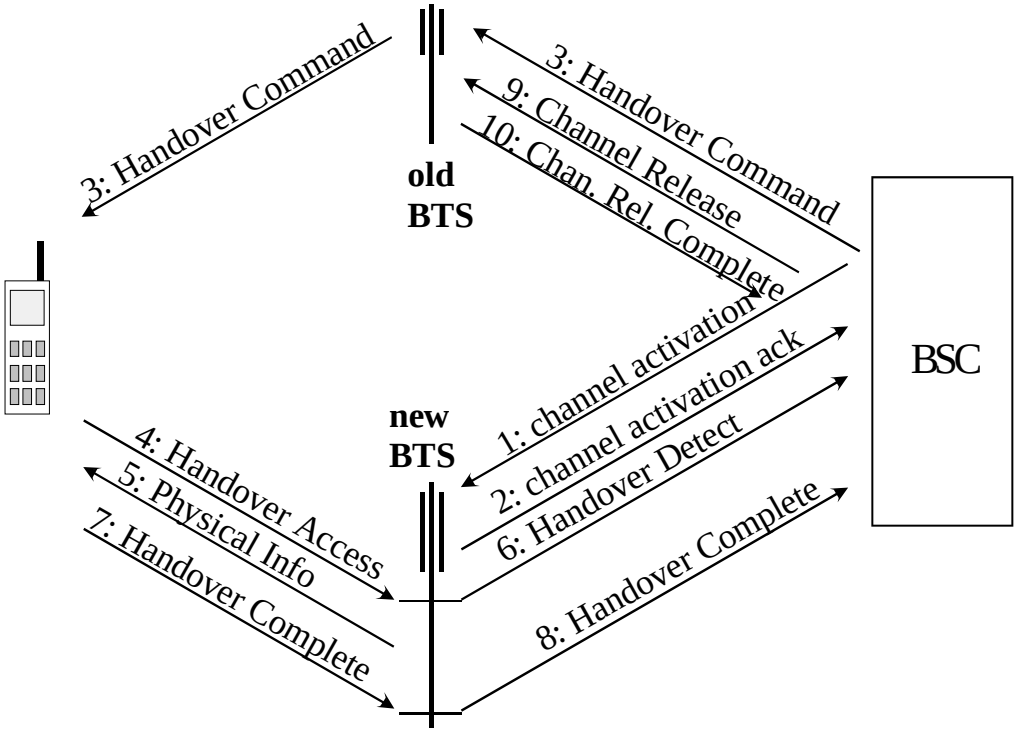
Quality

Die Qualität der Verbindung ist trotz hoher Leistung schlecht (hohes C/I).

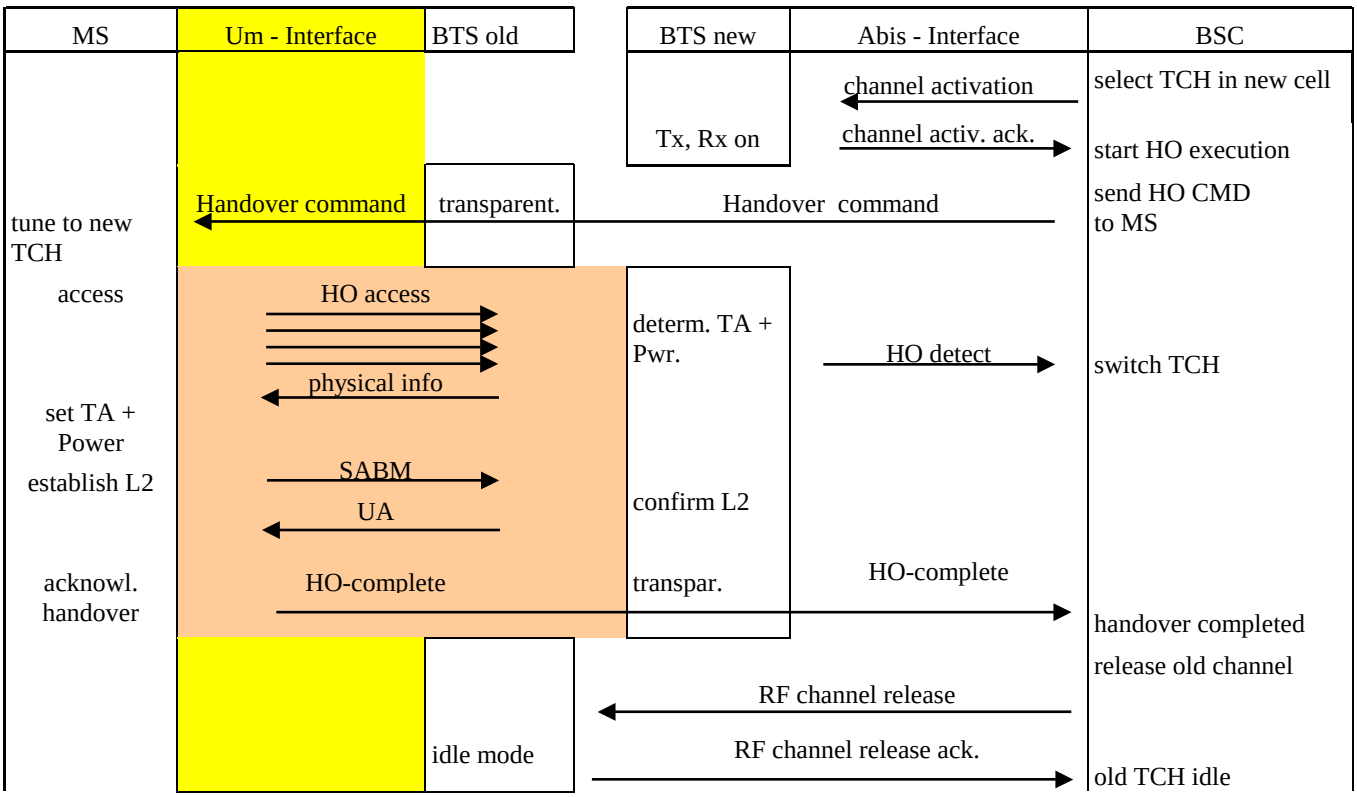
Traffic

Der Verkehr in der Serving Cell ist sehr hoch. Es wird versucht, durch Handover zu Nachbarzellen Kanäle in der überlasteten Zelle (Serving Cell) freizumachen.

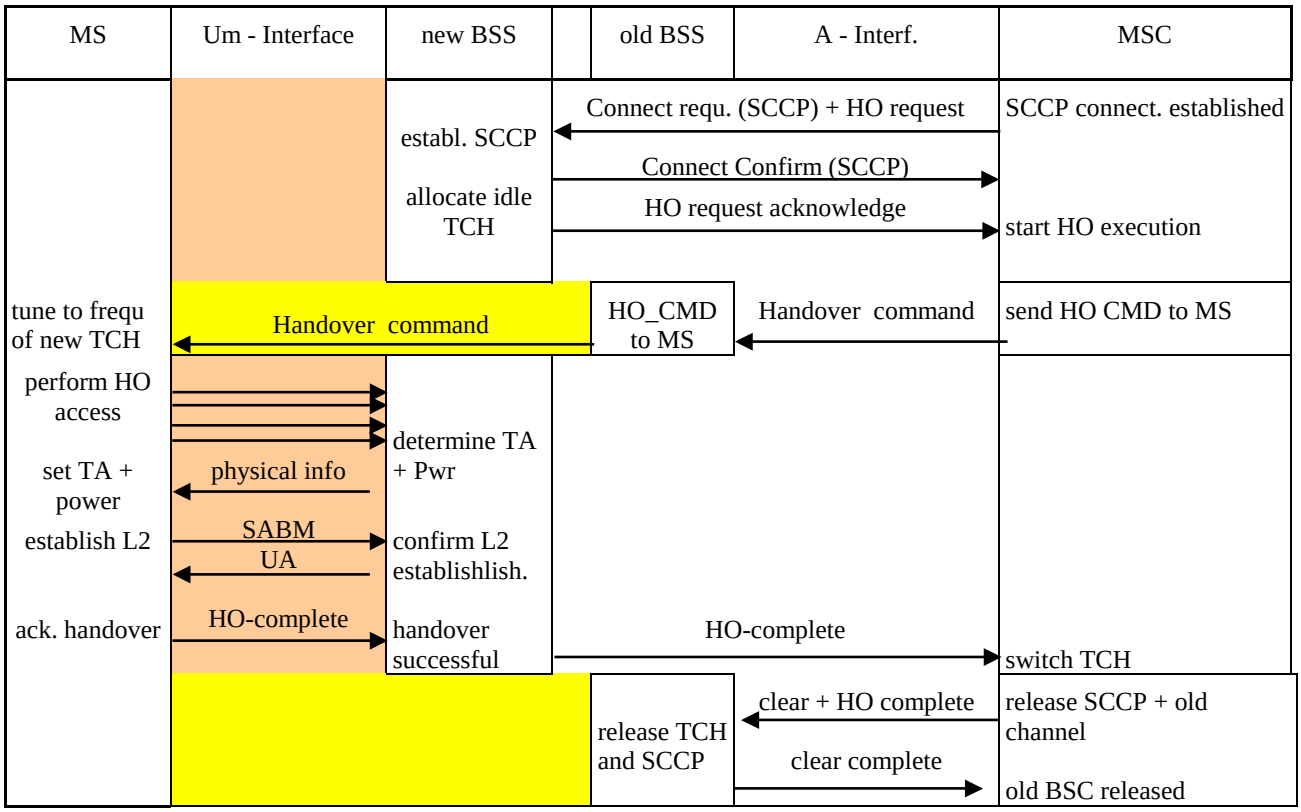
Handover Execution: BSC internal handover



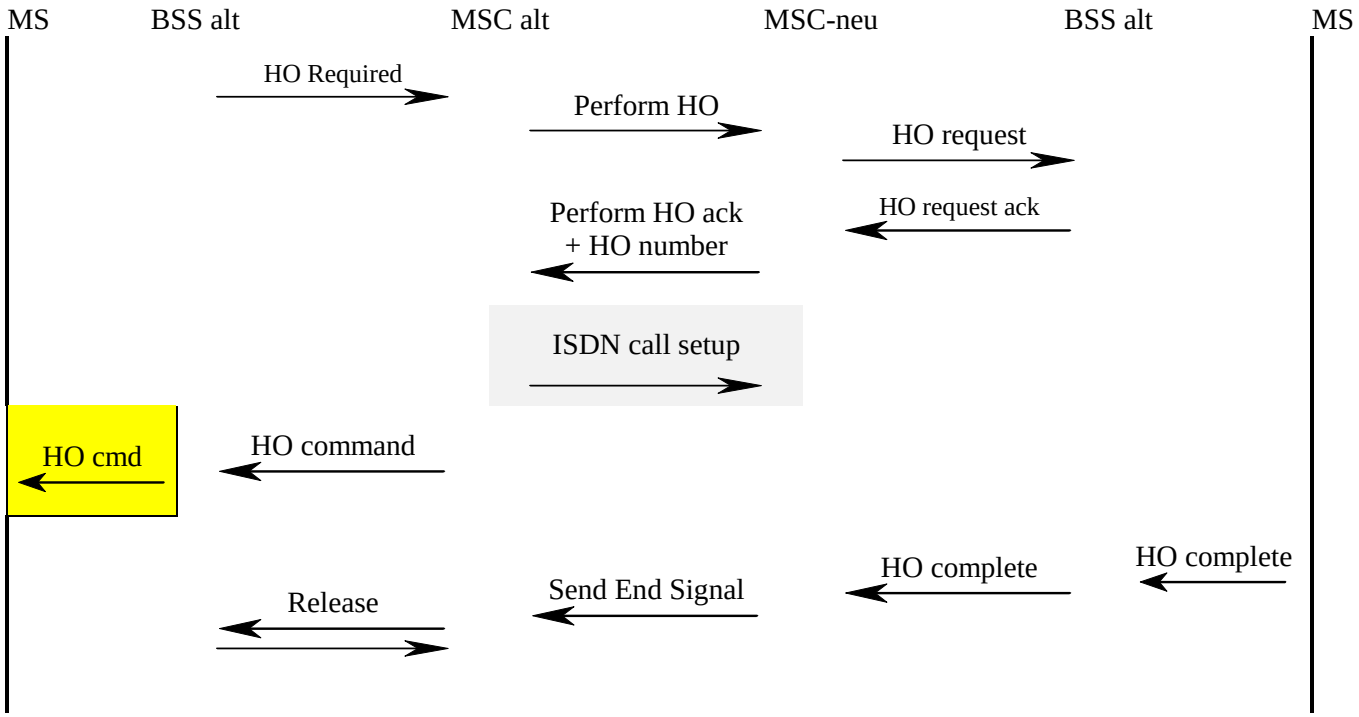
BSC internal handover



MSC controlled handover



MSC - MSC handover



8.5 Power Control

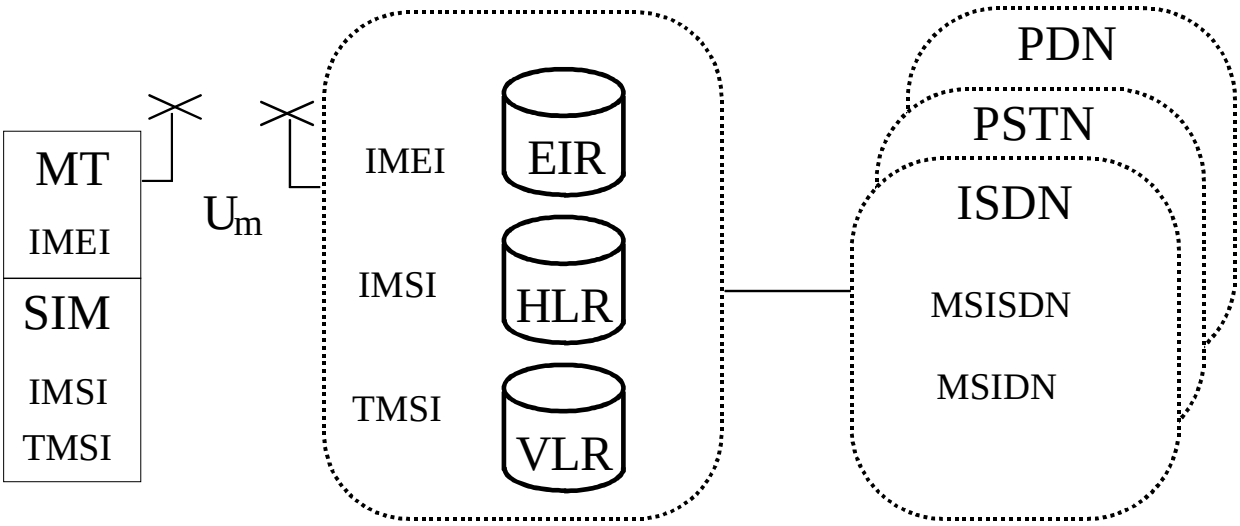
Power Class	Transmitter Power				MS Output Power [dBm] according to power command		
	GSM 900 MS	GSM 1800 MS	BTS		MS_TXPWR _MAX	GSM 900 MS	GSM 1800 MS
1	20 Watt	1 Watt	320 Watt		0	-	30 dBm
2	8 Watt	0,4 Watt	160 Watt		1	-	28 dBm
3	5 Watt	-	80 Watt		2	39 dBm	26 dBm
4	2 Watt	-	40 Watt		3	37 dBm	24 dBm
5	0,8 Watt	-	20 Watt		...	...	...
6			10 Watt				
7			5 Watt		14	15 dBm	2 dBm
8			2,5 Watt		15	13 dBm	0 dBm
					16	11 dBm	-
					17	9 dBm	-
					18	7 dBm	-
					19	5 dBm	-

Leistungsregelung in Up- und Downlink
Leistungsregelung auf unteren Empfangspegel und nach Qualität
Der Algorithmus zur Leistungsregelung befindet sich in BTS oder BSC

9 MM: Mobility Management

Numbering, Addressing, Identification:	Teilnehmernummer Gerätenummer Systemkennungen
Security	Authentication temporäre Teilnehmer-Identität Schlüsselerzeugung gestohlenen Geräte
Bewegung	Location Update MS ein- /ausschalten
Transaktionen	Parallele Transaktionen z.B. Sprache + SMS Sprache + Daten ($l_m + l_m$) Call Re-establishment

9.1 Numbering, Addressing, Identification



MT = Mobile Termination
SIM = Subscriber Identity Module
EIR = Equipment Identification Register
HLR = Home Location Register
VLR = Visited Location Register

MSISDN = Mobile Station ISDN Number
IMSI = International Mobile Subscriber Identity
TMSI = Temporary Mobile Subscriber Identity
IMEI = International Mobile station Equipment Identity

Numbering, Addressing, Identification

MSISDN
Mobile Station ISDN Number
= Rufnummer des Teilnehmer

• Country Code CC	49 (Deutschland)
• National Destination Code NDC	171 (D1-Netz)
• Subscriber Number SN	123456

- steht im Telefonbuch
- Nummerierungsplan: CCITT E.164
- entspricht der normalen, nationalen ISDN-Nummer
- kann variable Länge haben (offener Numerierungsplan)
- bis zu 15 Dezimalziffern einschließlich Länderkennzahl, Netzkennung und Teilnehmernummer
- HLR kann daraus abgeleitet werden
- steht nicht auf der SIM-Karte

***Frage**: Wer legt die Nummer fest ?*

MSIDN
Mobile Station International Data Number

- steht im Telefonbuch
- Nummerierungsplan: CCITT X.121
- ist eine optionale Nummer für PDN-Verbindungen (CSPDN, PSPDN)

Numbering, Addressing, Identification

IMSI *International Mobile Subscriber Identity*

IMSI up to 15 digits

3 digits	2 digits	up to 10 digits
Mobile Country Code MCC	Mobile Network Code MNC	Mobile Subscriber Identity Number MSIN
262 = Germany	01 = D1 Network	HLR-Num. + Subs-Num.

- Nummerierungsplan: CCITT E..212
- wird nur innerhalb des PLMN verwendet
- HLR kann daraus abgeleitet werden

TMSI *Temporary Mobile Subscriber Identity*

- 4 Oktett (32 Bit) unstrukturierte Binärzahl
- unterstützt die Anonymität des Teilnehmers
- wird vom VLR nach vergeben
- nur lokale Bedeutung innerhalb der VLR-Area

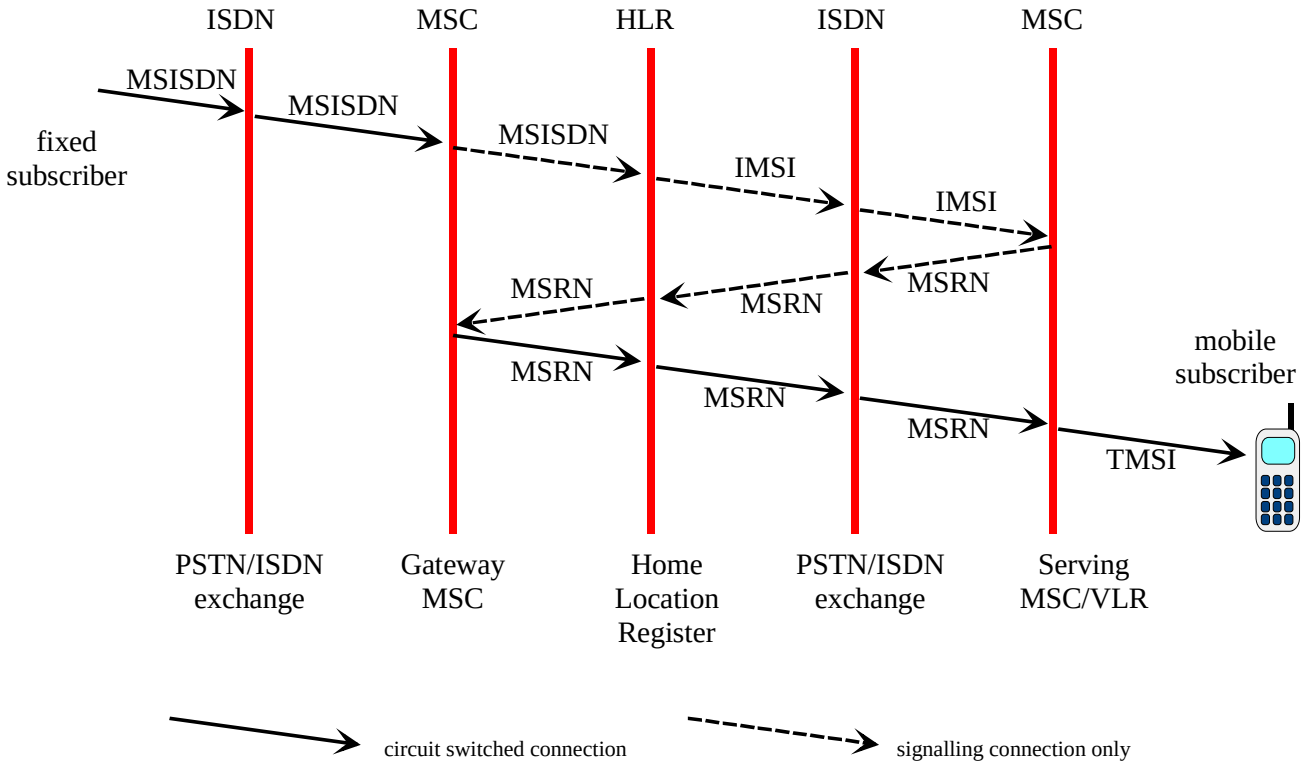
IMEI *International Mobile Station Equipment Identity*

IMEI 15 digits

6 digits	2 digits	6 digits	1 digit
Type Approval Code TAC	Final Assembly Code FAC	Serial Number SNR	Spare SP

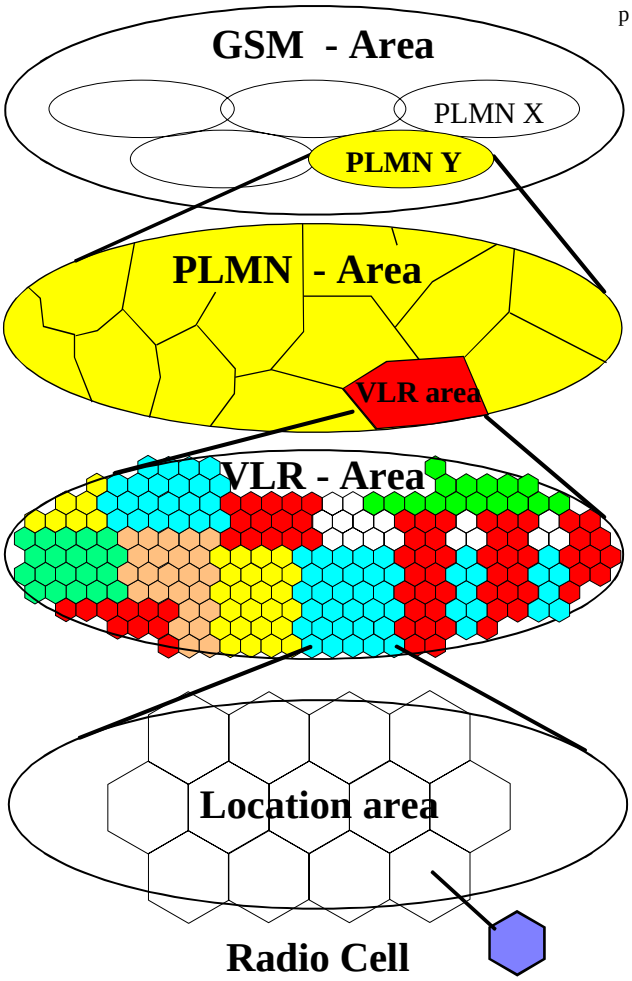
- internationale Mobilgerätenummer, identifiziert eindeutigen die HW
- auch als *International Manufacturer Equipment Identity* bezeichnet

Numbering, Addressing, Identification



GSM Hierarchy

PLMN Public Land Mobile Network
VLR Visitor Location Register



Numbering, Addressing, Identification

LAI *Location Area Identity*

- international eindeutig
- Wird über den BCCH ausgestrahlt
- wichtig für Location Update

LAI 5 octet

Mobile Country Code MCC 3 digits	Mobile Network Code MNC 2 digits	Location Area Code LAC 2 octet

CGI *Cell Global Identity*

- international eindeutig
- MS kennt die CGI nicht, nur innerhalb des PLMN verwendet

CGI 7 octet

Mobile Country Code MCC 3 digits	Mobile Network Code MNC 2 digits	Location Area Code LAC 2 octet	Cell Identity CI 2 octetts

BSIC *Base Transceiver Station Identity Code*

- lokaler Farbcode zur lokalen Identifizierung einer Zelle

BSIC 6 Bits

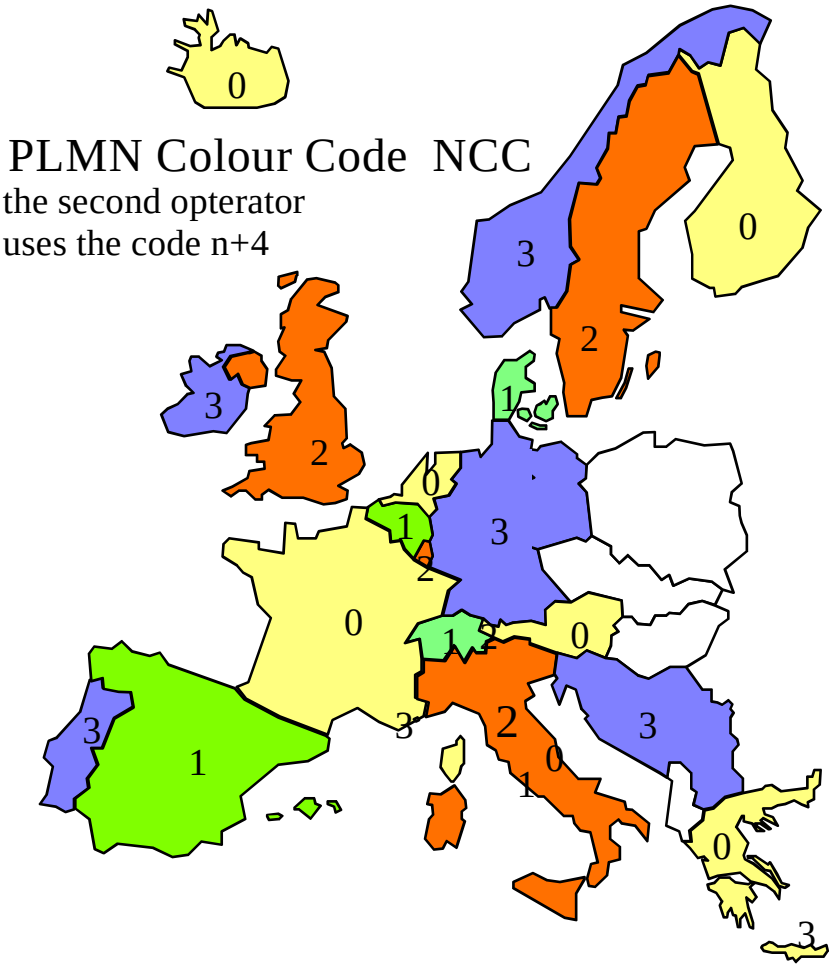
Network Colour Code NCC 3 bits	Base Station Colour Code BCC 3 bits

Numbering, Addressing, Identification

NCC, BCC

Network (Base Station) Colour Code

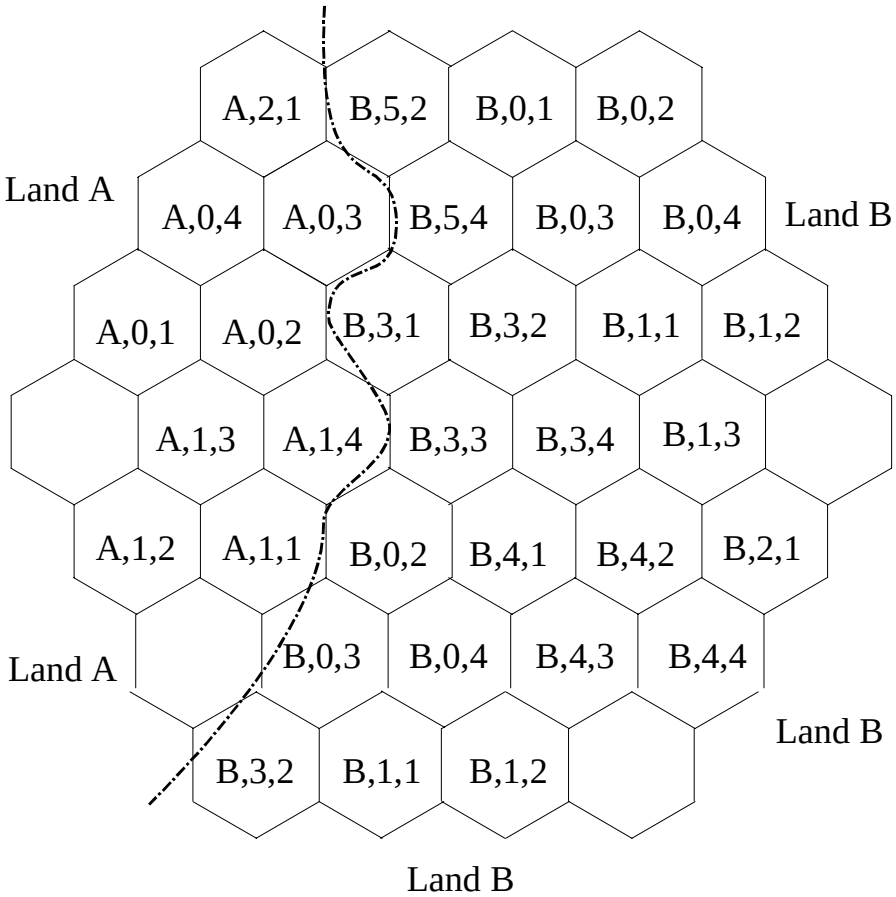
- lokaler Farbcode zur lokalen Identifizierung eines Landes (einer BTS)



Numbering, Addressing, Identification

lokale Kennzeichnung der Zellen mit BSIC und Frequenz

= **NCC + BCC + Frequenz**



9.2 Paging

BRD: 20.000 Zellen; 20 Mio. Tln., 1,5 MTC / Tln in der HVSt (mobile terminating call pro Teilnehmer in der Hauptverkehrsstunde)

Paralleles Paging: Die Teilnehmer werden in allen Zellen gleichzeitig gerufen:

20 Mio Tln * 1,5 MTC / Tln in der HVSt. = **30 Mio. MTC / HVSt**

1 MTC = 2 paging messages => 30 Mio. MTC/HVSt * 2 msg/MTC = **60 Mio. msg/HVSt.**

1 paging message = 5 Bytes => 60 Mio. msgs/HVSt * 5 Bytes/msg = 300 MBytes/h = 83,3 kByte/s

1 GSM-Kanal = 1 kbyte/s netto => 83,3 kbyte/s = **83,3 Kanäle** sind in jeder Zelle nur für Paging erforderlich

Serielles Paging Die Teilnehmer werden sequentiell gerufen:

Antwortzeit der MS $\geq$ 1 s => average response time: 2 paging * 1 s/paging = **2 s**

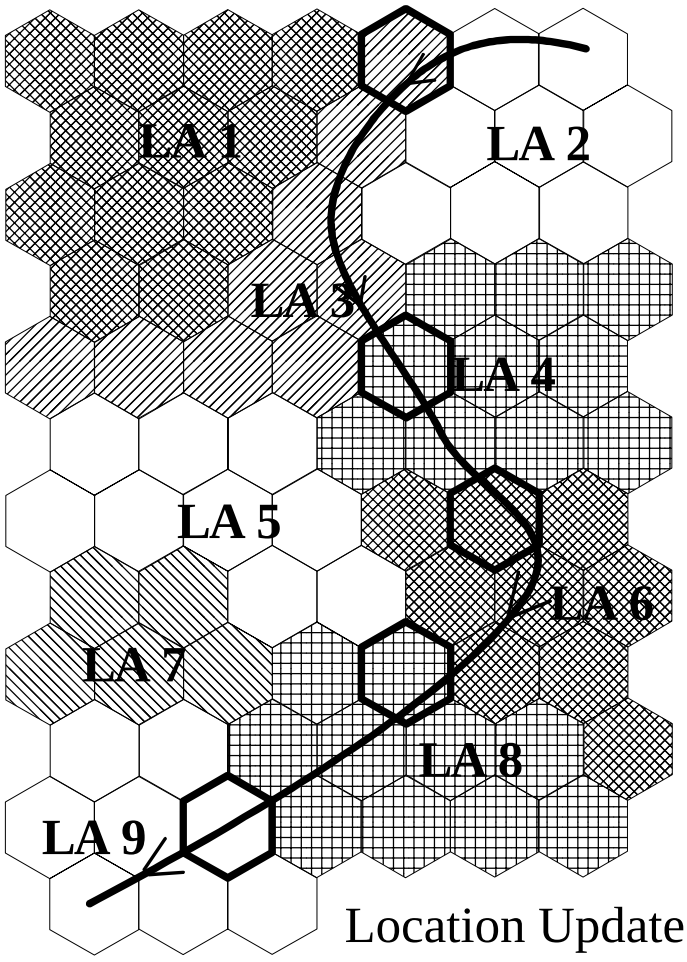
Maximale Rufzeit (bei erfolglosen Rufen): 20.000 Zellen * 2 s = 40.000s = **11 Stunden**

Mit intelligenterem Algorithmus: mittlere Rufzeit (bei erfolgreichen Rufen): 150 Zellen * 2 s = 300s = **5 Min**.

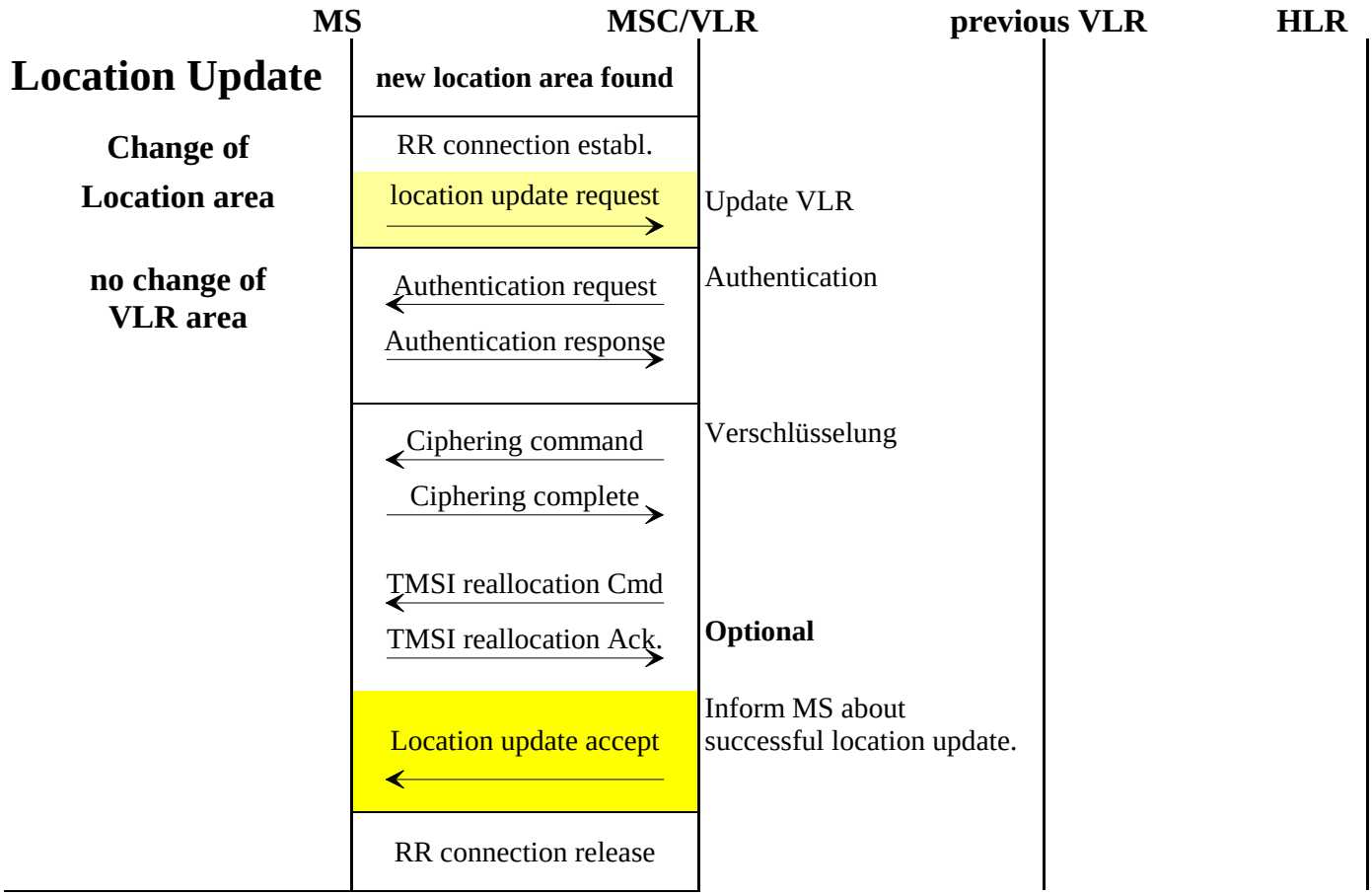
Ziel:		short response time	=>	parallel paging
	+	low paging traffic	=>	sequential paging
	=	location update	+	parallel paging in 4..10 cells (Location Area)

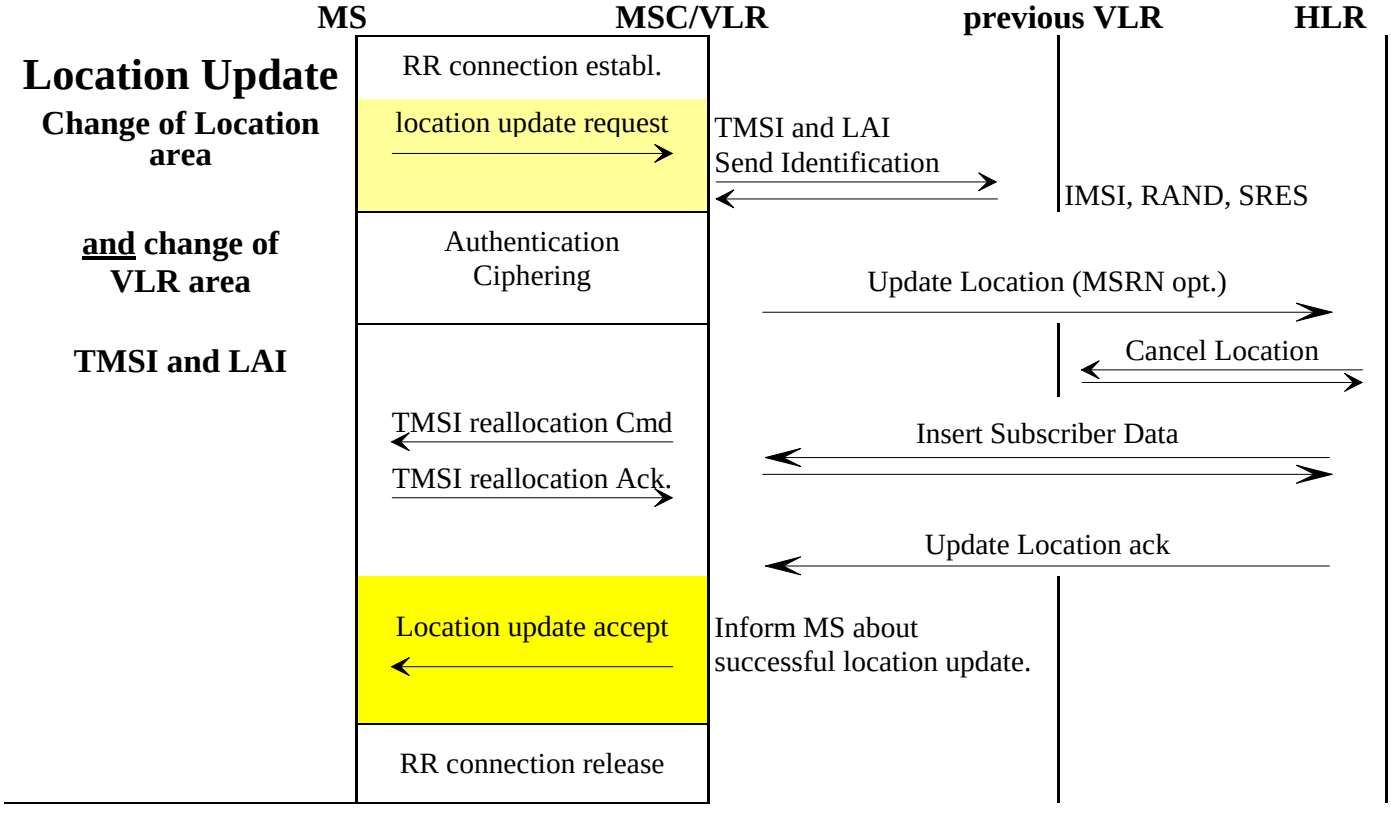
9.3 Location Update

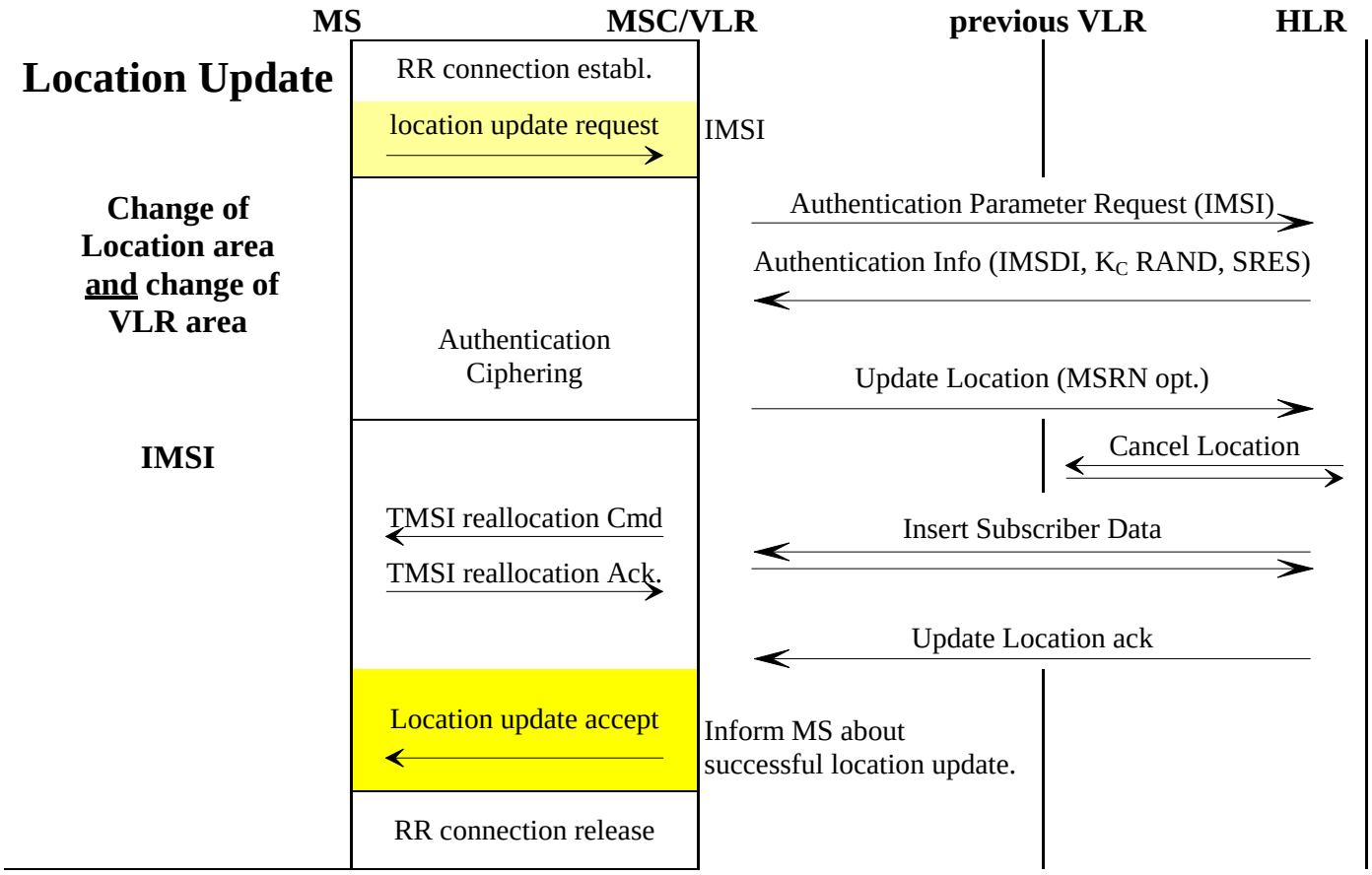
MS performs location update procedure every time a new location area is entered



Location Update

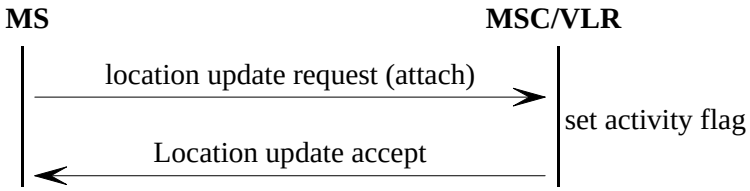

MS
MSC/VLR
previous VLR
HLR
Location Update
new location area found
Change of
Location area
RR connection establ.
location update request
Update VLR
no change of
VLR area
Authentication
Authentication request
Authentication response
Verschlüsselung
Ciphering command
Ciphering complete
TMSI reallocation Cmd
TMSI reallocation Ack.
Optional
Location update accept
Inform MS about
successful location update.
RR connection release


MS
MSC/VLR
previous VLR
HLR
Location Update
Change of Location
area
RR connection establ.
location update request
TMSI and LAI
Send Identification
IMSI, RAND, SRES
and change of
VLR area
Authentication
Ciphering
Update Location (MSRN opt.)
TMSI and LAI
Cancel Location
TMSI reallocation Cmd
TMSI reallocation Ack.
Insert Subscriber Data
Update Location ack
Location update accept
Inform MS about
successful location update.
RR connection release



IMSI attach/detach

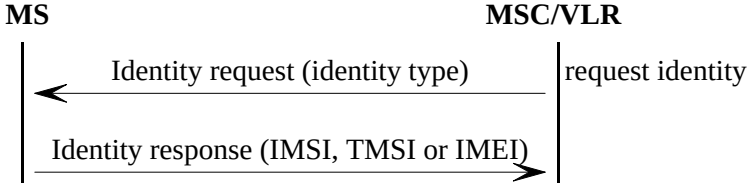
IMSI attach = insert SIM (power on)



IMSI detach = remove SIM (power off)

Periodic registration IMSI attach procedure initiated by the MS in periodic intervals.
It is used to avoid database inconsistency.

Identity request



Location Update:

U_m komplett

	MS	BTS
RR connection establ.	Channel Request →	
	← Immediate Assign	
	SABM + Identity + Service Request = location update →	
	← UA + Service Request + Identity	
optional	[Identity Request]	
Authentication	← Authentication Request	
	Authentication Response →	
Ciphering	← Ciphering command	
	Ciphering complete →	
optional	[TMSI Reallocation]	
Location update	← Location update accept	
RR connection release	← Channel Release	
	Disconnect →	
	← UA	

9.4 MM - Messages

Location updating request
- Location updating type
- Ciphering key sequence number
- Location area identification
- Mobile station classmark 1
- Mobile identity

Location updating accept
- Location area identification
- Mobile identity

Location updating reject
- Reject cause

Authentication request
- Ciphering key sequence number
- Authentication parameter RAND

Authentication response
- Authentication parameter SRES

Authentication reject
- Header only, no content

TMSI-reallocation command
- Location area identification
- Mobile identity (the new TMSI)

TMSI reallocation complete - Header only, no content

9.5 MM - Messages

CM Re-establishment request
- Ciphering key sequence number
- Mobile station classmark 2
- Mobile identity
- Location area identification

CM service accept - Header only, no content

CM service reject - Reject cause

CM service request
- CM service type
- Ciphering key sequence number
- Mobile station classmark 2
- Mobile identity

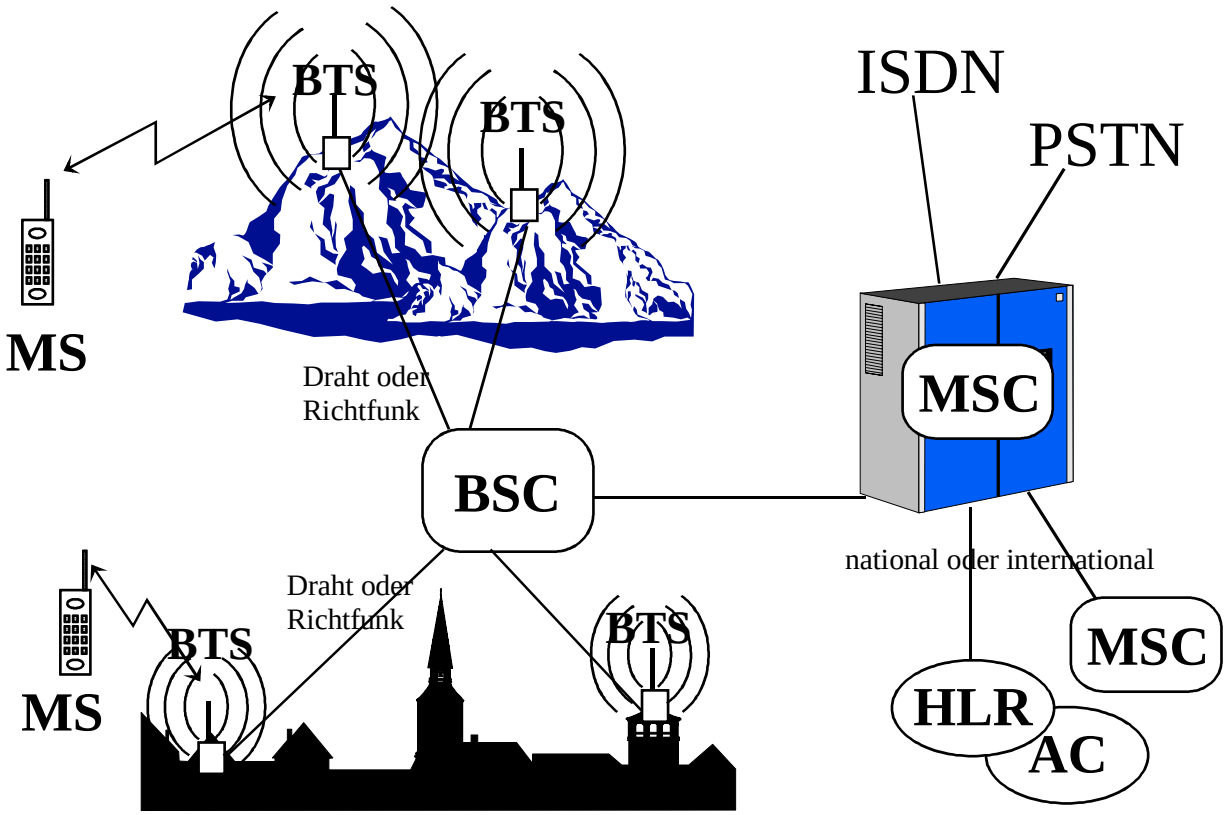
Identity request - Identity type

Identity response - Mobile identity

IMSI detach indication
- Mobile station classmark 1
- Mobile identity

MM-Status
- Reject Cause
- Control state

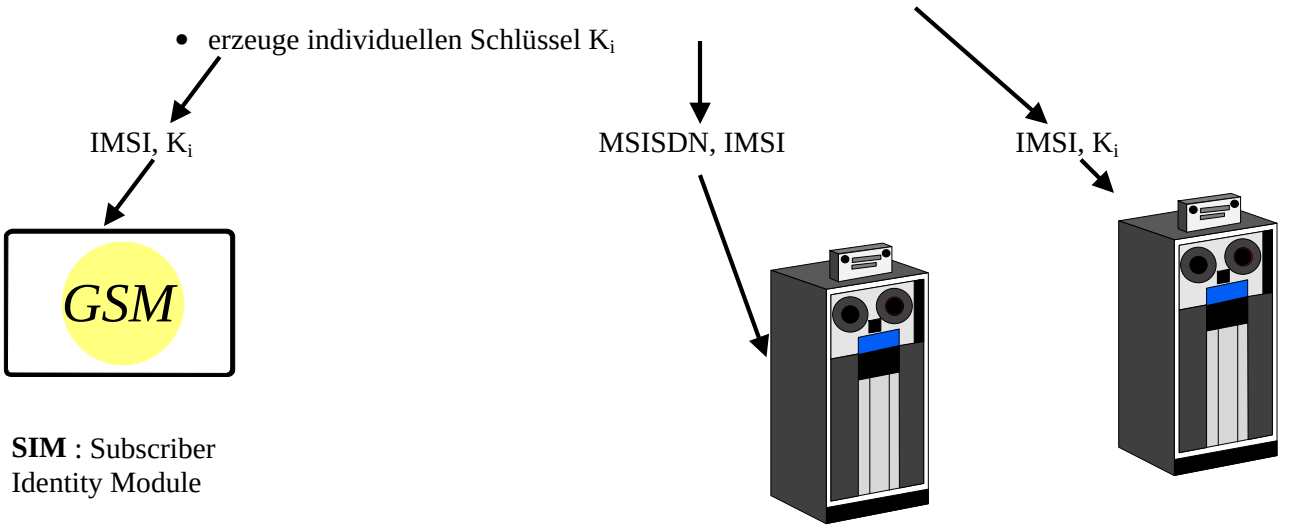
10 GSM - Security



GSM Sicherheitsmechanismus

SIM – Karte personalisieren:

- wähle Telefonnummer MSISDN (Mobile Subscriber ISDN-Number)
- erzeuge IMSI (International Mobile Subscriber Identity)
- erzeuge individuellen Schlüssel K_i

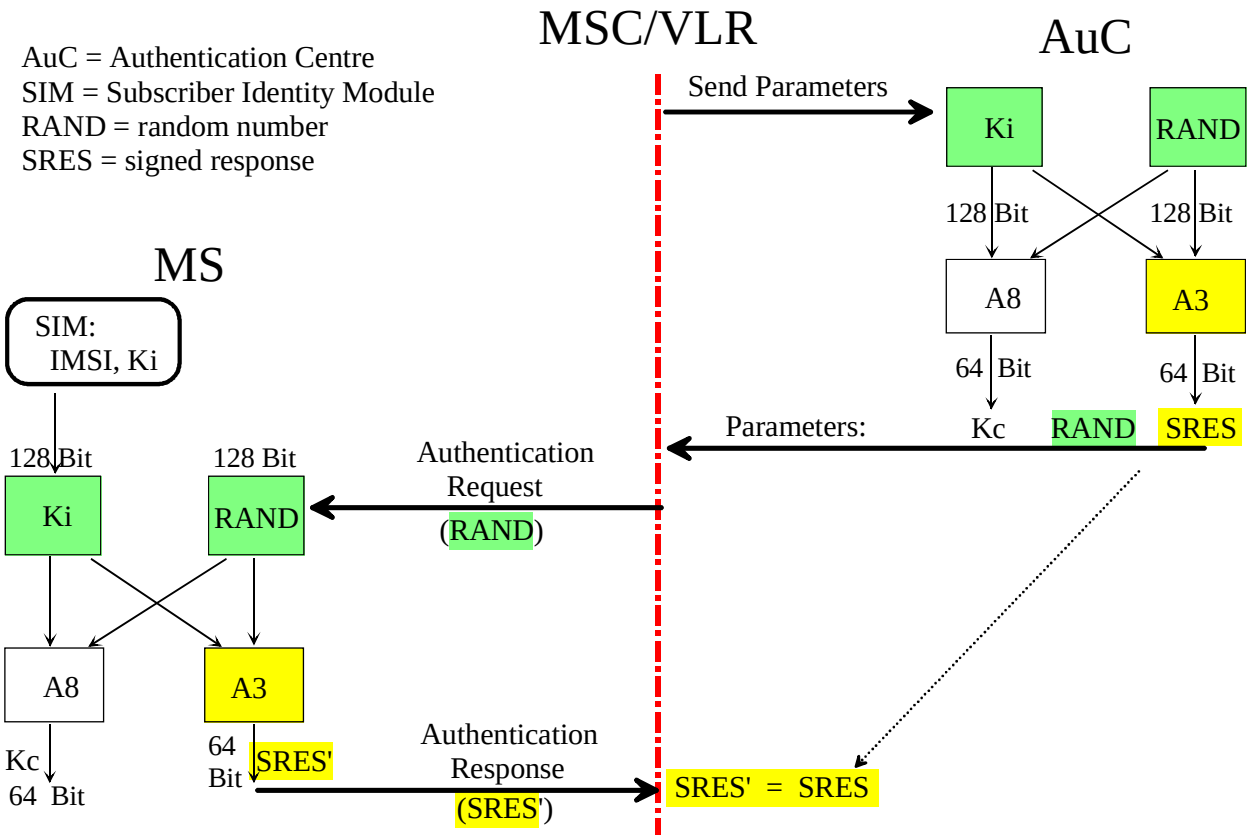


SIM : Subscriber Identity Module

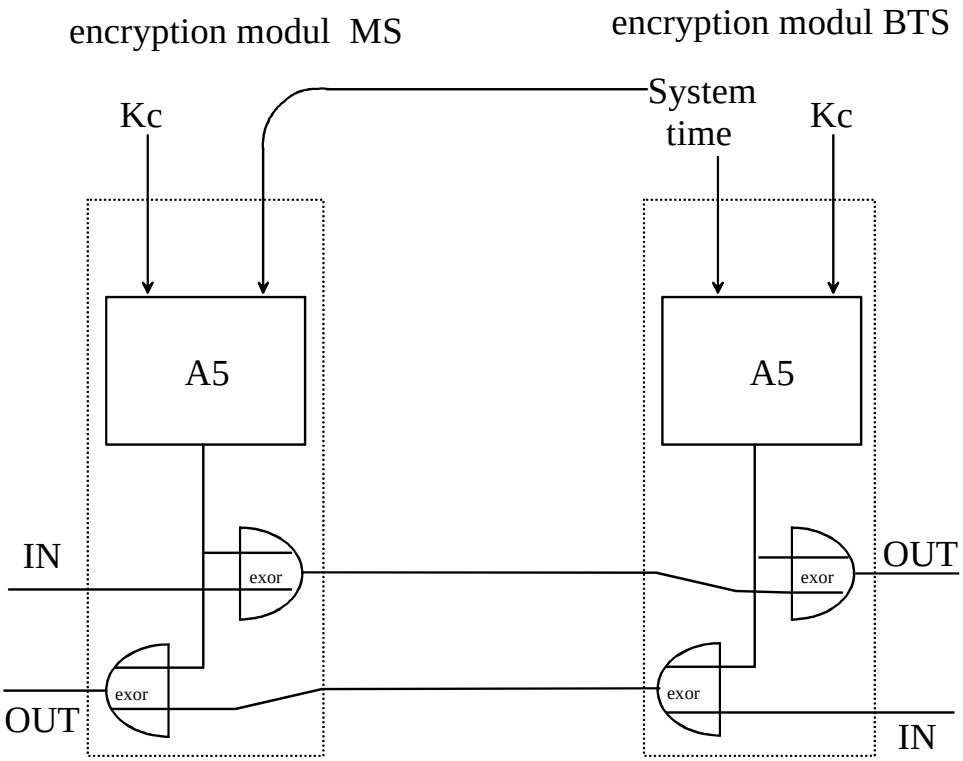
HLR: Home Location Register

AC Authentication Centre

10.1 Authentication (GSM)



10.2 Ciphering (GSM)

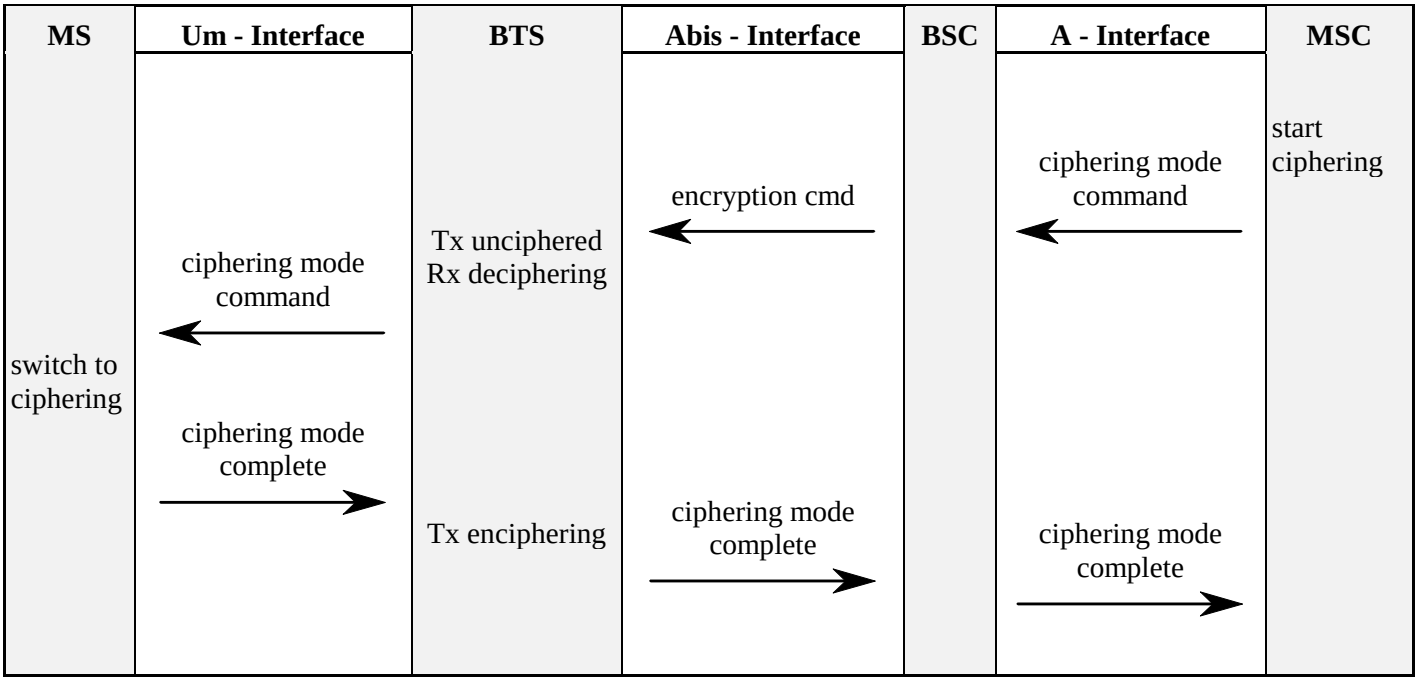


A5/1 strong key

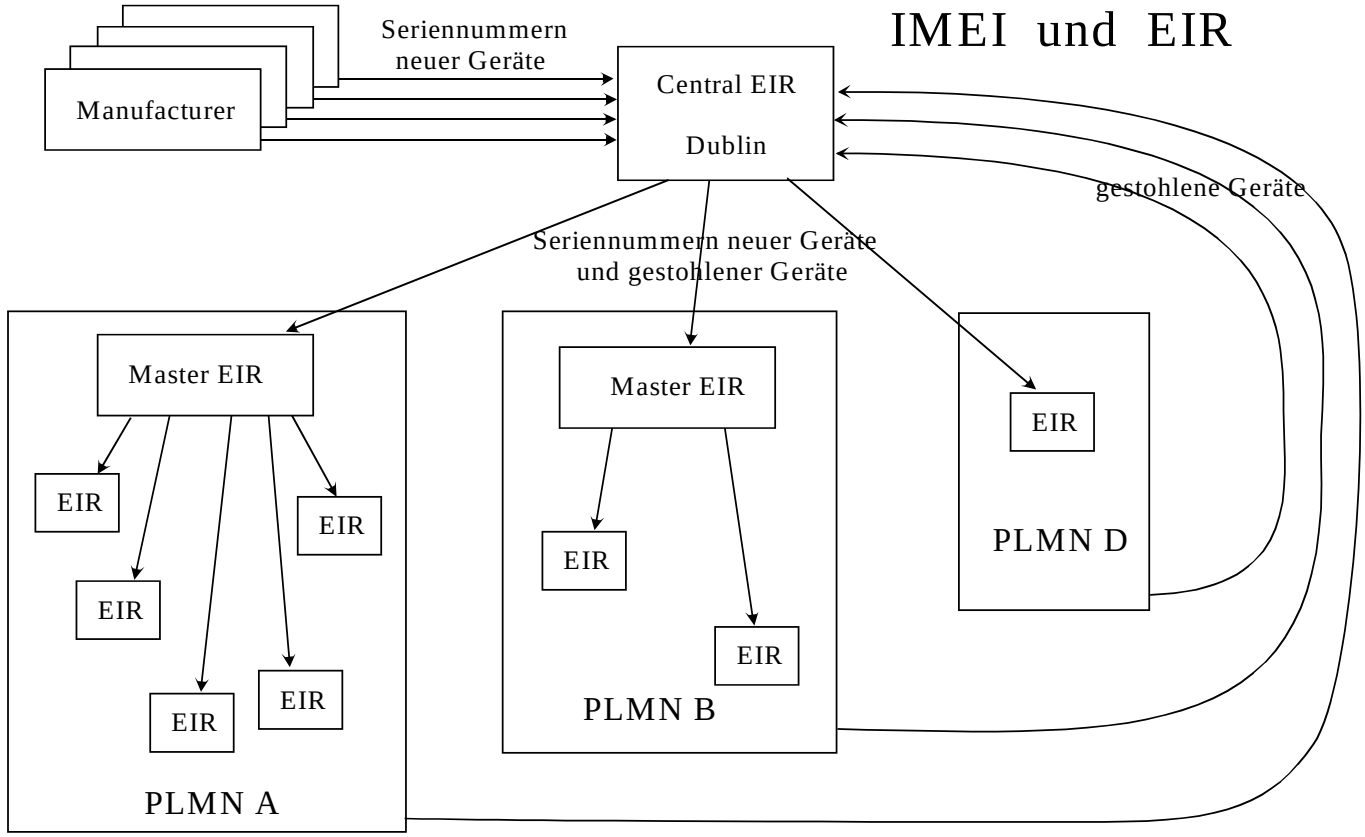
A5/2 … A5/7 weak key

Ciphering may be switched off by the network

Security: Ciphering



10.3 IMEI International Mobile Identity



10.4 Angriffe auf GSM

Verschlüsselung A5 es gibt 7 verschiedene Algorithmen; kann auch ganz abgeschaltet werden

Alex Biryukov and Adi Shamir: Real-Time Cryptanalysis of GSM's A5/1 on a PC December 5, 1999

Der Schlüssel für den A5/1 kann in einer Sekunde mit einem PC gefunden werden.
Es werden 128 MB RAM und zwei Festplatten mit 73 GB benötigt.

April 1998: Chaos Computer Club zeigt in der Praxis, wie man den K_i herausfindet.
Es wird eine Schwäche im A8 von GSM ausgenutzt. Einige Betreiber haben verbesserten A8

Dafür benötigt man die SIM-Karte für 12 Stunden und
die PIN

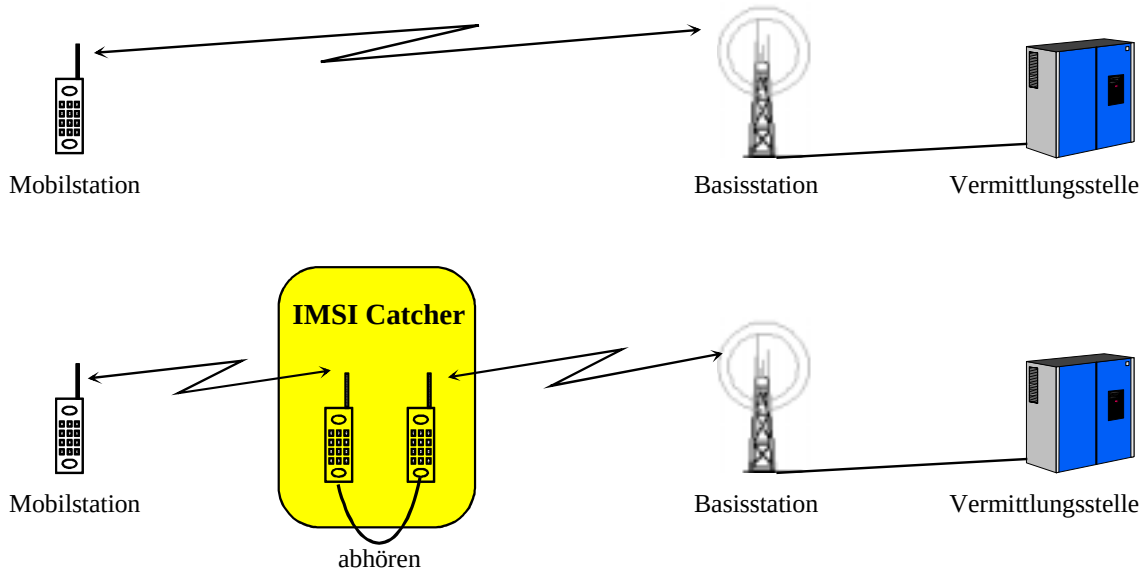
Angriffe auf Mobilfunk allgemein:

Der Schaden durch Betrug in der Telekommunikation wird weltweit auf 8 bis 26 Mrd. DM pro Jahr geschätzt
(1/99 Lisa Modisette, Ligthbridge Technologies)

Vodafon schätzt den Verlust auf 1% des Umsatzes (1996)

US providers lose over $500 million yearly to fraud in AMPS (analoger Mobilfunk)

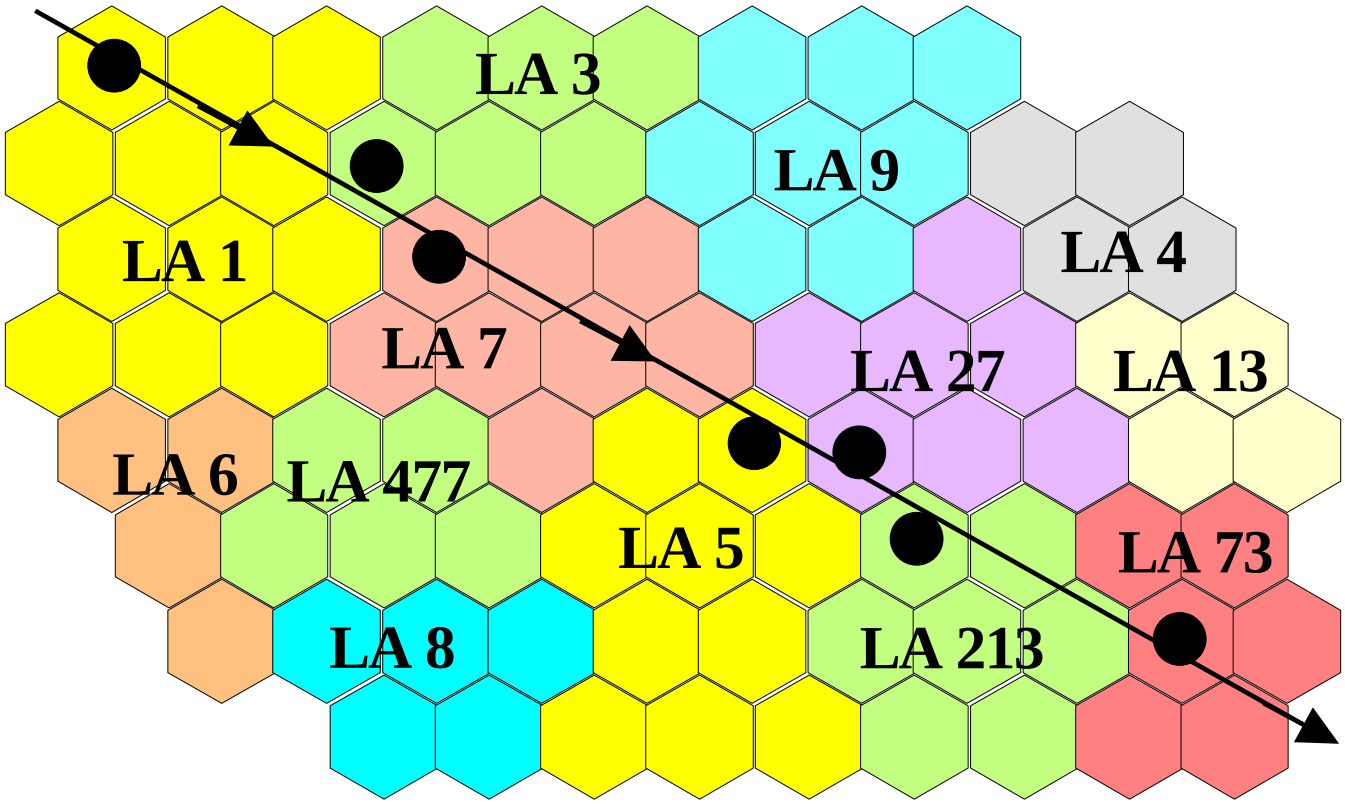
IMSI Catcher



IMSI-Catcher von der Firma Rohde und Schwarz, München; Typenbezeichnung `GA 901´; ca. 100 000 Mark ?

Experten: "Der Betrieb erfolgt aus einem Pkw heraus, damit ist ein schneller Ortswechsel unproblematisch."

Bewegungsprofile



Datenspeicherung

Individuell für jeden Teilnehmer können gespeichert werden:

- Verbindungsdaten (Tel.-Nr., Ort, Uhrzeit, Gesprächsdauer) für charging
- Aktivität: Handy ein- und ausschalten
- Bewegung: location update

Es ist möglich, den Aufenthaltsort regelmäßig abzufragen. Der Teilnehmer bemerkt dies nicht.

Während des Gespräches kann der Teilnehmer auf 100m genau geortet werden.

Mobilfunk: Abhören von Raumgesprächen

"die Wanze hat das Laufen gelernt."

Beabsichtigt:

Im einfachsten Falle können Mobiltelefone mittels Menüfunktionen als Lauschsender geschaltet werden.

Bei manchen Geräten wird dabei das Display abgeschaltet

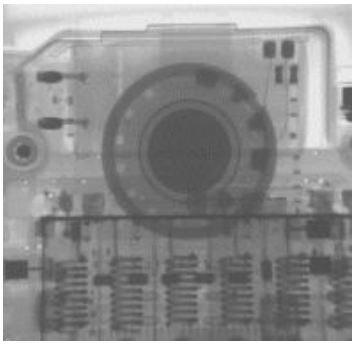
Unbeabsichtigt:

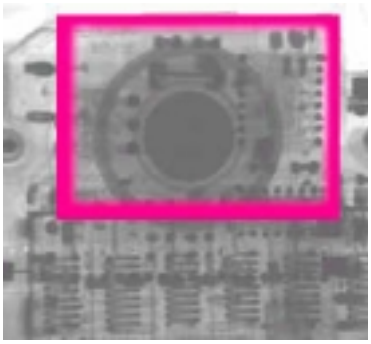
Durch spezielle Manipulation von Mobiltelefonen ist es möglich, Raumgespräche abzuhören.

- Mobiltelefon dient als Abhöranlage
- Am Handy ist dies nicht erkennbar
- Aktivierung über das Telefonnetz von jedem Ort der Welt

Diese Manipulation ist durch eine Sichtprüfung nach Zerlegen des Gerätes relativ leicht nachzuweisen.

Mobilfunk: Manipulierte Hardware





Bekannte HW-Manipulationen:

- Manipulationen der Freisprecheinrichtung
- Ruftonabschaltung
- manipulierte Akkus mit eingebautem Lauschsender (Wanze)

Ziel:

- Abhören der Raumgespräche

Problem: Der Angreifer muss das zu manipulierende Gerät für eine gewisse Zeit besitzen

Berlin: Bei Kabinettssitzungen und in vertraulichen Parlamentsgremien müssen Handys aus Sicherheitsgründen künftig draußen bleiben.

11 Call Management

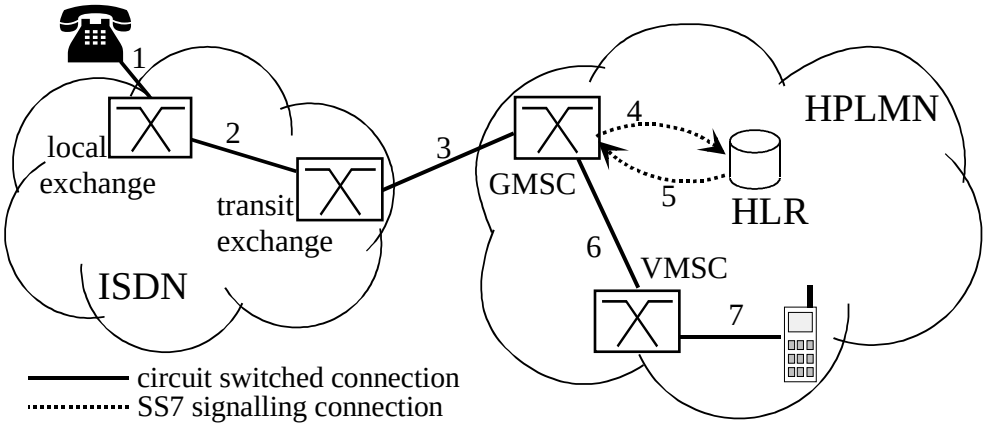
Call Management Messages

Call establishment messages	SETUP ALERTING CALL CONFIRMED PROGRESS CONNECT **EMERGENCY SETUP**	 (- PROCEEDING) (- ACKNOWLEDGE)
Call information phase messages	MODIFY USER INFORMATION	(- COMPLETE; - REJECT)
Call clearing messages:	DISCONNECT RELEASE	 (- COMPLETE)
Messages for supplementary service control	FACILITY HOLD RETRIEVE	FACILITY (- ACKNOWLEDGE; - REJECT) (- ACKNOWLEDGE; - REJECT)
Miscellaneous messages	START DTMF STOP DTMF CONGESTION CONTROL NOTIFY STATUS	(- ACKNOWLEDGE; - REJECT) (- ACKNOWLEDGE) CONGESTION CONTROL (- ENQUIRY)

11.1 Mobile Originating Call Setup MOC

MS	Um interface	MSC / VLR		ISDN
Mobile Originating RR-connection establishment				
Service indication	CM Service Request →			
Authentication Ciphering TMSI reallocation				
start call setup	Setup → ← call proceeding	accept call		
TCH assignment				
ringing tone on switch path	← alerting ← connect connect ack →	ISDN call setup switch path	Initial address message → ← address complete ← answer	B party ringing Off hook
start charging speech or data transmission phase				

11.2 Mobile Terminating Call Setup: National Call



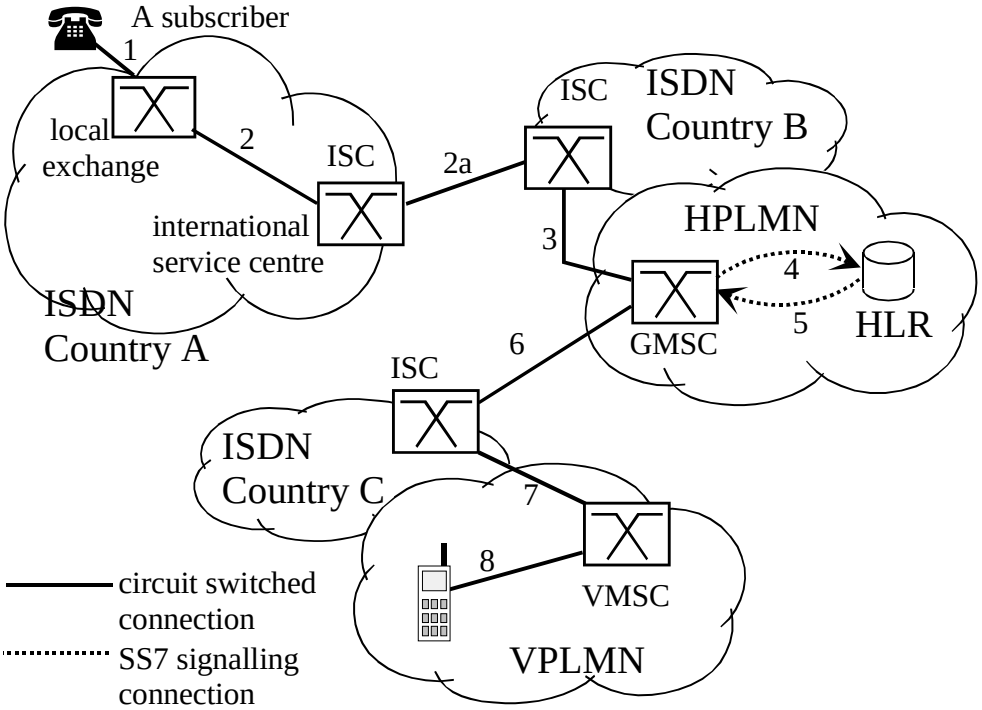
3: Call setup to the nearest GMSC of the HPLMN (NDC)

4, 5: HLR interrogation, HLR returns MSRN via SS7

6: Call setup to the visited MSC using the MSRN

HPLMN	Home Public Land Mobile Network
VPLMN	Visted Public Land Mobile Network
HLR	Home Location Register
NDC	National Destination Code

GMSC	Gateway Mobile Switching Centre
VMSC	Visted Mobile Switching Centre
MSRN	Mobile subscriber roaming number
	MSRN allocation on per call basis or at location update



MTC: International Call

1, 2, 2a:
Call setup to the home country of the mobile subscriber

3:
Call setup to the nearest GMSC of the HPLMN (NDC)

4, 5:
HLR interrogation, HLR returns MSRN via SS7

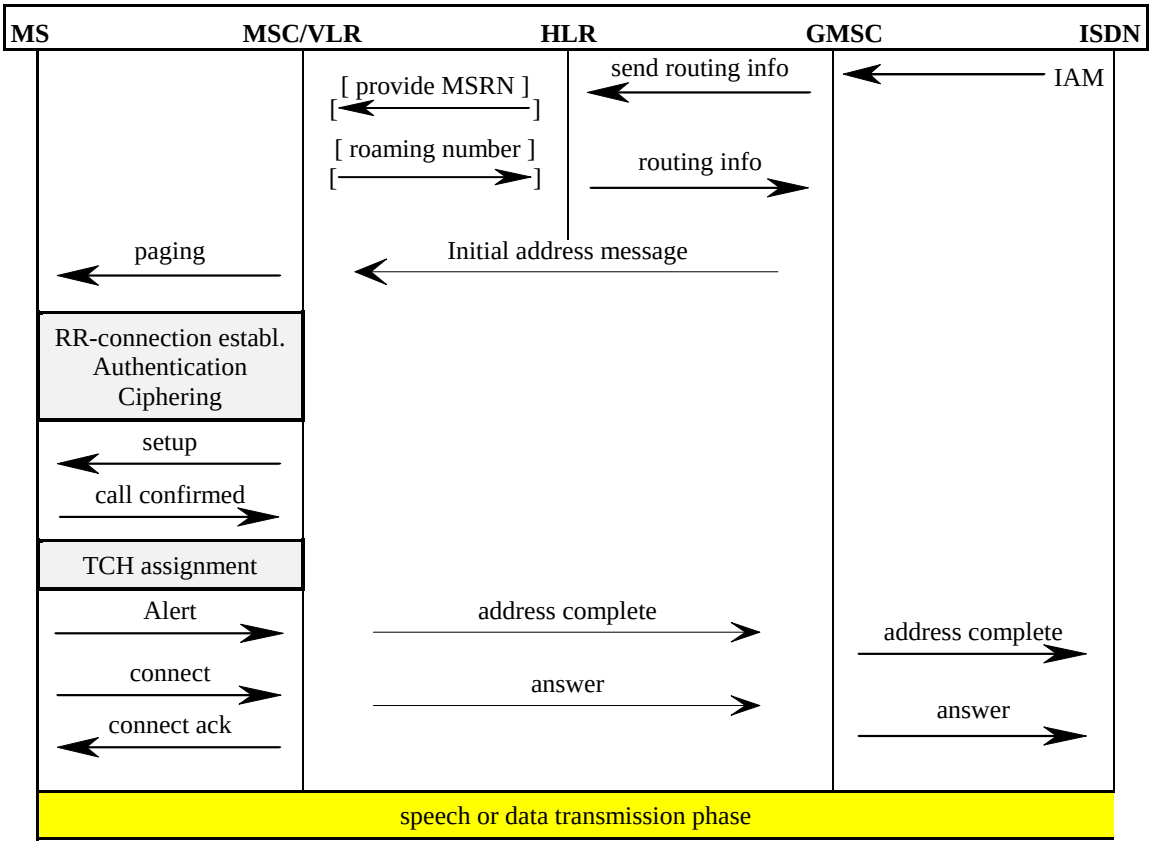
6:
Call setup to the visited country of the mobile subscriber

7:
Call setup to the visited MSC using the MSRN

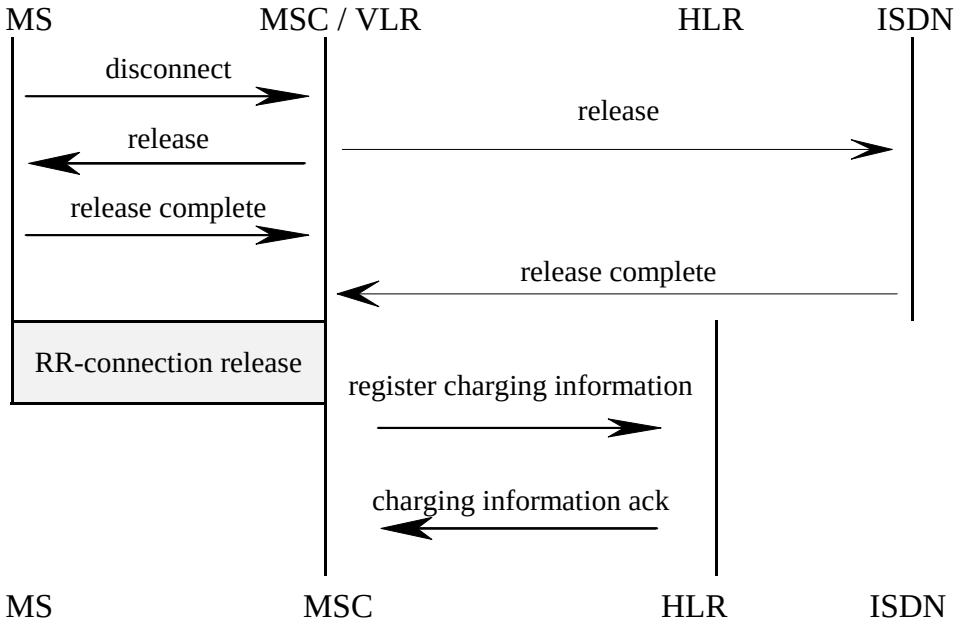
HPLMN	Home Public Land Mobile Network
VPLMN	Visted Public Land Mobile Network
HLR	Home Location Register
NDC	National Destination Code

GMSC	Gateway Mobile Switching Centre
VMSC	Visted Mobile Switching Centre
MSRN	Mobile subscriber roaming number
ISC	International Service Centre

Mobile Terminating Call Setup



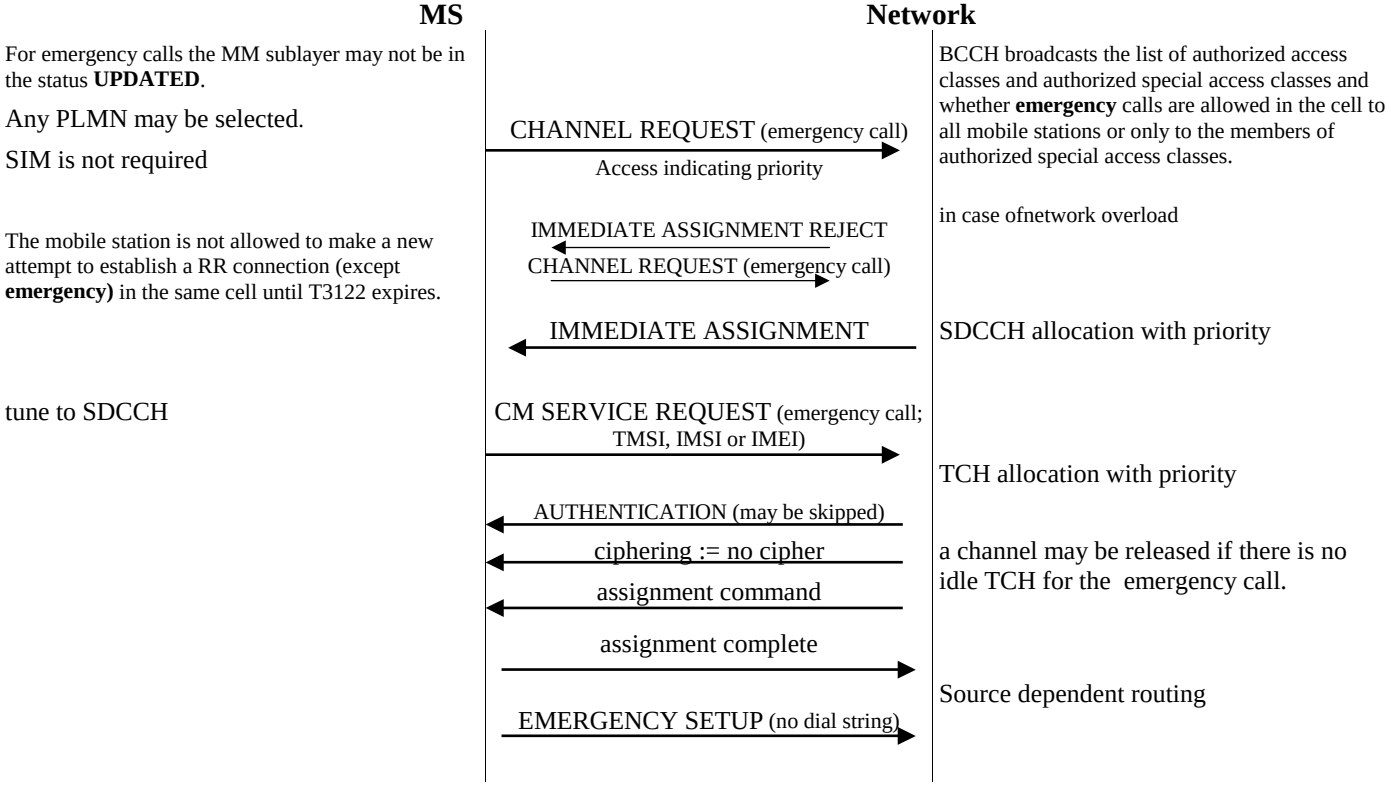
11.3 Call Release



register charging information:

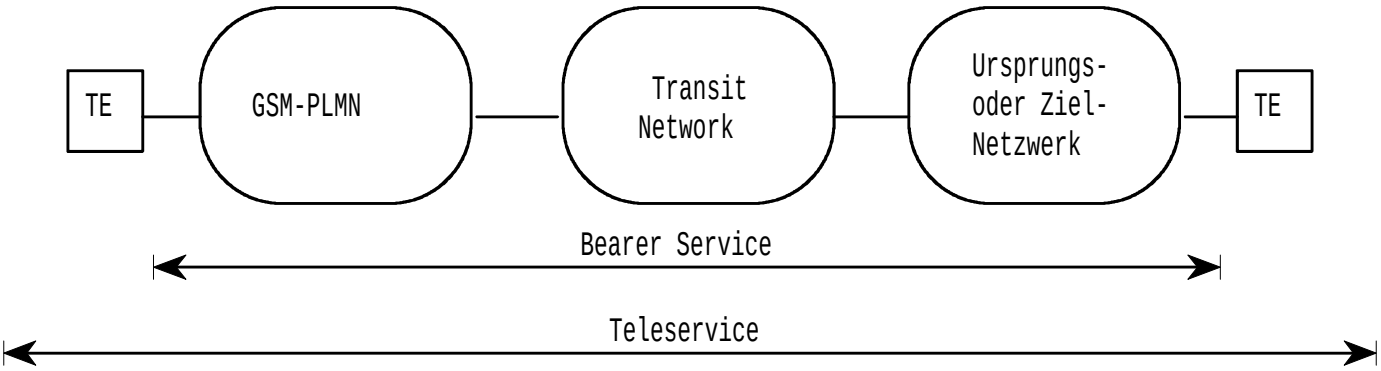
- MOC immer (außer emergency call)
- MTC wenn Gebühren für roaming anfallen

11.4 Emergency Call



12 Services

tele services bearer services supplementary services



ISDN kompatible: physikalisch: 2 B + D [$L_m + L_m$] 2 * 4,8 kb/s + 2 * FACCH
Protokoll: identisch mit ISDN

12.1 Teleservices

von Endgerät zu Endgerät, einschließlich Teilnehmerschnittstelle

Spezifikation umfaßt die Schichten 1 bis 7 des OSI-Modells.

- Telefonie: E1, d.h. von Anfang an in allen MoU-Ländern
- Notruf (emergency call) einheitliche Notrufnummer 112; ortsabhängige Routing; ohne Karte, ohne Gebühr
- Faksimile Gruppe 3 und 4. Gruppe 3: transparent und nicht transparent
- short message service SMS kurze Nachrichten bis zu 160 Zeichen; MO und MT;
- short message cell broadcast Nachrichtenverteildienst mit Meldungen bis zu 93 Zeichen
- Videotext Kompatibilitätsprobleme, 3 Standards in EU
- Teletext

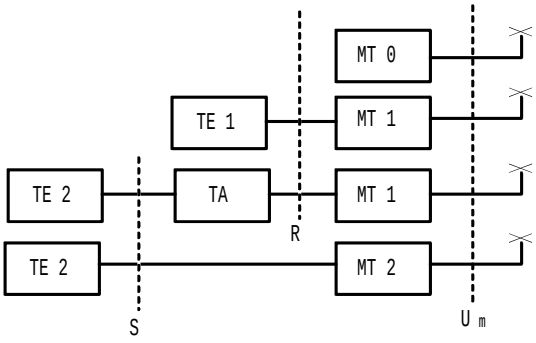
12.2 Bearer Services

Die Schichten 1 bis höchstens 4 des OSI Modells sind spezifiziert

Dienst des Telekommunikationsnetzes (ISDN oder GSM) ist die Ende-zu-Ende Übertragung von Daten zwischen den Referenzpunkten R oder S an

ISDN Datenraten von 19,2 kb/s oder 64 kb/s werden an der GSM-Luftschnittstelle durch Flußkontrolle angepaßt.

Referenzkonfiguration der Mobilstation



- ohne Datenschnittstelle
- mit R-Schnittstelle (V24)
- mit R-Schnittstelle (V24), S_0- Schnittstelle über Terminal Adapter
- mit S_0- Schnittstelle (ISDN)

MT Mobile Termination TE Terminal TA Terminal Adapter

3,1 kHz Ex PLMN	Datenübertragung mit niederfrequenten Modems im Sprachband
Leitungsvermittelte Datendienste	von 300 b/s bis 9,6 kb/s; synchron oder asynchron transparente (T) und nicht-transparente (NT) Übertragung. Bei NT sichert das Netz mit dem RLP die Datenübertragung. RLP ist an die GSM-Funkübertragung (TDMA) besonders angepaßt. Bei T muß der Benutzer selbst ein ARQ-Protokoll zur Fehlerkorrektur bereitstellen
Paketvermittelte Datendienste	Zugang zu Paketdatennetzen (X.25) asynchron mit Datenraten von 300 b/s bis 9,6 kb/s synchron mit Datenraten von 2,4 bis 9,6 kb/s transparente (T) und nicht-transparente (NT) Übertragung.

List of important Basic Services

1 Speech	TS 11 TS 12	Telephony Emergency call	
2 Short message service	TS 21 TS 22 TS 23	Short message MT/PP Short message MO/PP Short Message Cell Broadcast	
6 Facsimile services	TS 61 TS 62	Alternate speech and facsimile group 3 Automatic facsimile group 3	
7 All Data circuit asynchrone	BS 24 BS 25 BS 26	Data circuit duplex asynch. 2400 bit/s Data circuit duplex asynch. 4800 bit/s Data circuit duplex asynch. 9600 bit/s	T, NT T, NT T, NT
8 All Data circuit synchrone	BS 32 BS 33 BS 34	Data circuit duplex synch. 2400 bit/s Data circuit duplex synch. 4800 bit/s Data circuit duplex synch. 9600 bit/s	T T T
9 All PAD access	BS 44 BS 45 BS 46	PAD access circuit asynch. 2400 bit/s PAD access circuit asynch. 4800 bit/s PAD access circuit asynch. 9600 bit/s	T, NT T, NT T, NT
10 All Data packet	BS 51 BS 52 BS 53	Data packet duplex synch. 2400 bit/s Data packet duplex synch. 4800 bit/s Data packet duplex synch. 9600 bit/s	T, NT T, NT T, NT
11 12 kbit/s unrestr. digital	BS 71	12 kbit/s unrestricted digital	T

TS =Teleservice
BS = Bearerservices

12.3 Rate Adaptation

9,6 kb/s Data Transmission : ISDN Format

0	0	0	0	0	0	0	0
1	D1	D2	D3	D4	D5	D6	S1
1	D7	D8	D9	D10	D11	D12	X
1	D13	D14	D15	D16	D17	D18	S3
1	D19	D20	D21	D22	D23	D24	S4
1	E1	E2	E3	E4	E5	E6	E7
1	D25	D26	D27	D28	D29	D30	S6
1	D31	D32	D33	D34	D35	D36	X
1	D37	D38	D39	D40	D41	D42	S8
1	D43	D44	D45	D46	D47	D48	S9

ISDN-Datenblock für 9,6 kb/s

E1, E2, E3 = user data rate,

E4, E5, E6 = network independent clocking

ISDN			GSM U_m	
Bits	Bit Rate kb/s		Bits	Bit Rate kb/s
17	3,4	Frame Synchronization	0	0
48	9,6	user data (D1...D48)	48	9,6
7	1,4	house keeping (E1...E7)	4	0,8
8	1,6	status bits (S, X)	8	1,6
80	**16**	total	**60**	**12**

ISDN:
80 Bits every 5 ms = 16 kb/s

GSM U_m
48 Bits every 5 ms = 9.6 kb/s

12.4 Supplementary Services

1. Number Identification

Calling Line (/Number) Identification Presentation (CLIP/CNIP)	Nummer des Anrufers wird angezeigt
Calling Line (/Number) Identification Restriction (CLIR/CNIR)	eigene Nummer wird beim Angerufenen nicht angezeigt
Connected Line (/Number) Identification Presentation (COLP/CONP)	Nummer des Angerufenen wird angezeigt
Connected Line (/Number) Identification Restriction (COLR/CONR)	eigene Nummer wird dem Anrufers nicht angezeigt
Malicious Call Identification (MCI)	Fangen

2. Call Offering

Call Forwarding Unconditional (CFU)	Anrufumleitung
Call Forwarding on Mobile Subscriber Busy (CFB)	
Call Forwarding on no Replay (CFNRy)	
Call Forwarding on Mobile Subscriber Not Reachable (CFNRc)	
Call Forwarding on Radio Congestion	
Call Forwarding on mobile Subscriber not registered	
Call Transfer (CT)	
Mobile Access Hunting (MAH)	

3. Call Completion

Call Waiting (CW) - Anklopfen
Call Hold (HOLD) - Anruf halten
Completion of Calls to Busy Subscribers (CCBS) - Automatischer Rückruf

Supplementary Services

4. Multi Party

Three Party Service (3PTY/TPS) -Dreiergesprächsschaltung

5. Community of Interest

Conference Calling (CONF) Konferenzschaltung

Closed User Group (CUG) Geschlossene Benutzergruppe

6. Charging

Advice of Charge (AoC) Gebührenanzeige

Reverse Charging Gebührenübernahme durch den Angerufenen

Freephone Service (FPH)

7. Additional Information

User-to-User Signalling (transparentes) UUS

8. Call Restrictions

Barring of All Outgoing Calls (BAOC/OCB)

Barring of Outgoing International Calls (BOIC)

Barring of Outgoing International Calls except to the Home PLMN Country (BOIC-exHC)

Barring Of All Incoming Calls (BOAIC/ICB)

Barring of Incoming Calls when Roaming Outside the Home PLMN Country (BIC-Roam)

Interception Abhören durch Sicherheitsbehörden

12.5 Value Added Services

Mehrwertdienste sind nicht durch GSM spezifiziert.
Jeder Betreiber kann sie nach eigenem Ermessen einführen.

- Auskunft
- Sekretariatsdienst
- Weitervermittlungsdienst
- Voice mail
- Flottenmanagement

12.6 Besonderheiten

Das GSM-System weist einige Besonderheiten auf auf, z.B.

- Roaming — Durch Roaming-Abkommen kann jeder Teilnehmer sein Telefon weltweit benutzen, d.h. er kann Telefongespräche auch in Netzen anderer Netzbetreiber führen. Die Gebühren werden mit der normalen Telefonrechnung abgerechnet
- Multinumbering: — Einem Teilnehmer können mehrere Rufnummern MSISDN zugeordnet werden.
- In-Call-Modifikation — Im Gespräch zwischen Sprache und Datendienst wechseln.
- DTMF — Der Sprachcodec ist für DTFM-Töne nicht transparent. Diese Signale werden in GSM über die Signalisierung übertragen
- international calls — Damit der Teilnehmer nicht die Vorwahl für Auslandsferngespräche im jeweiligen Lande kennen muß, gibt es die '+' Taste. Sie erlaubt z.B. mit +49 von überall aus nach Deutschland anzurufen.
- Emergency call — Notruf mit der 'SOS'-Taste oder mit der einheitlichen Nummer 112

12.7 SMS

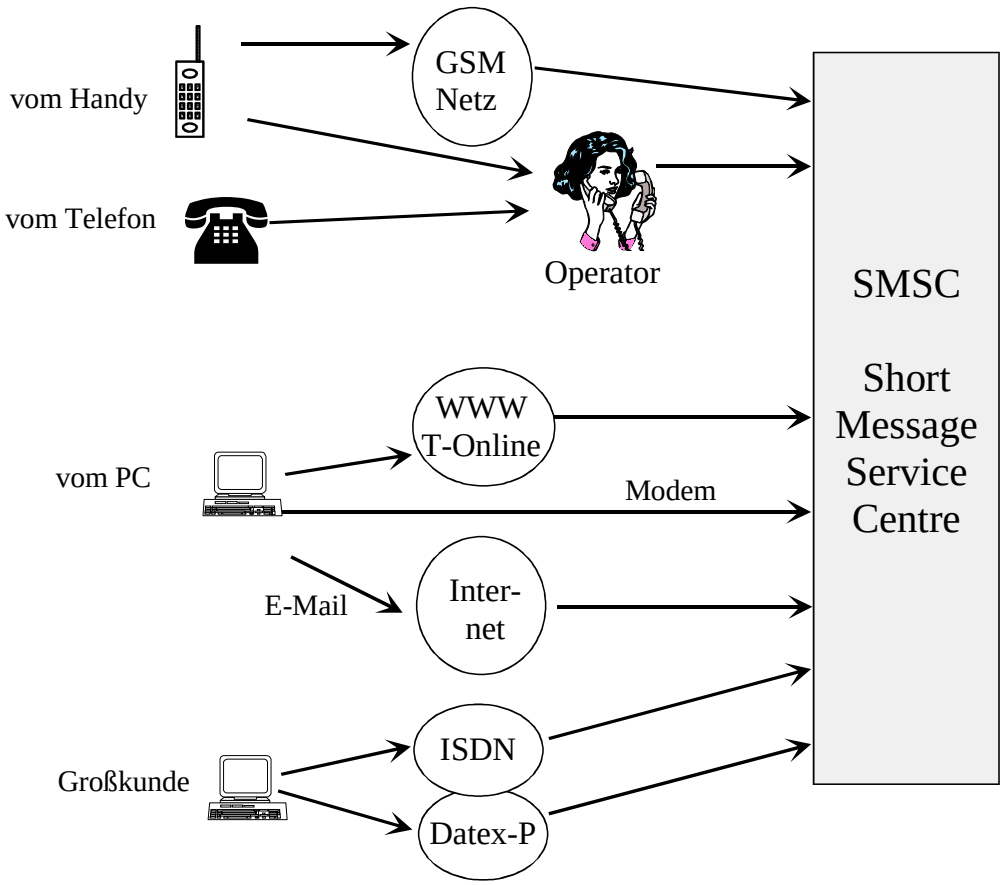
Was ist der Short Message Service

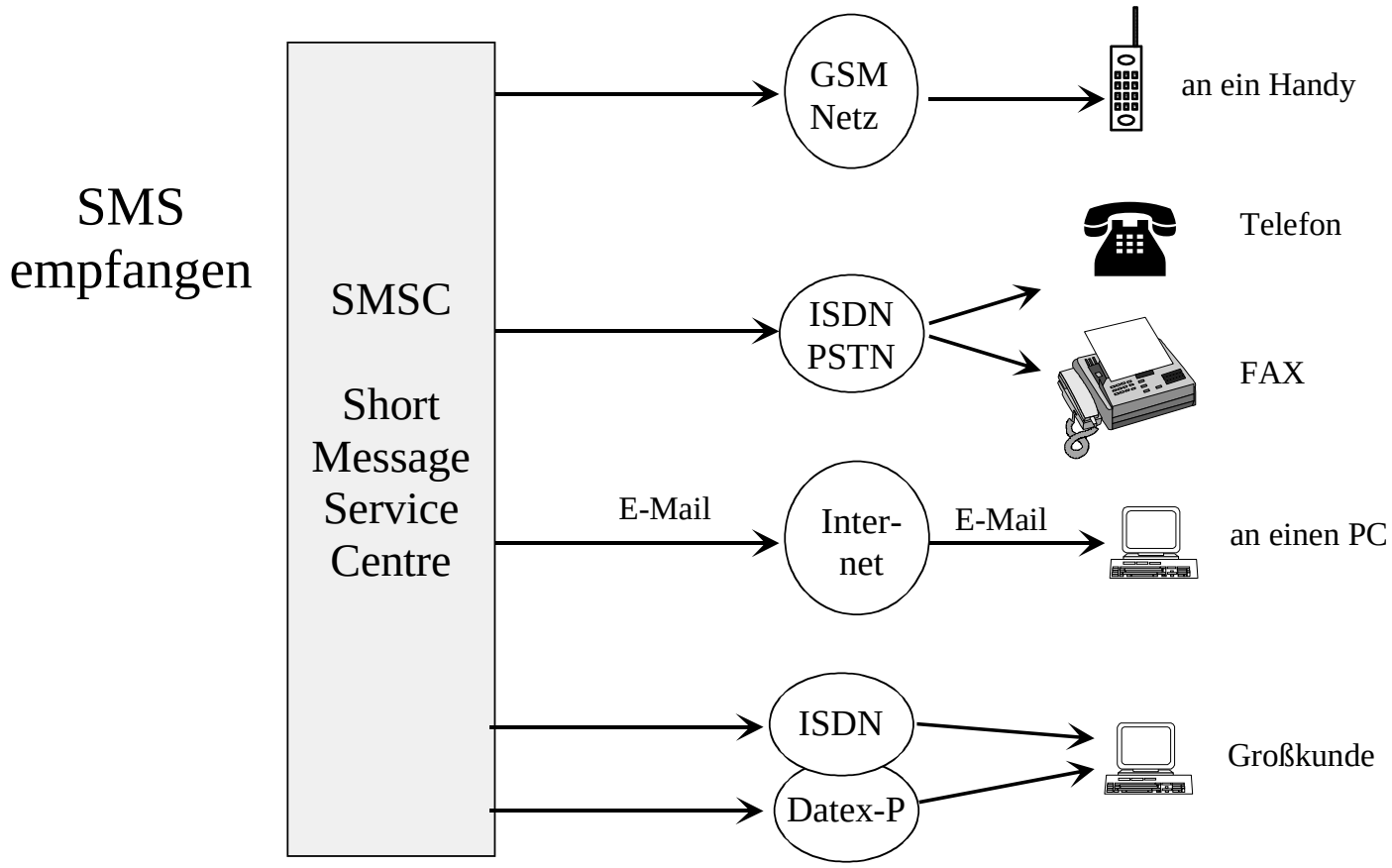
mit dem GSM-Mobiltelefon schriftliche Kurznachrichten senden und empfangen

Die Kurznachricht

- ist bis zu 160 Zeichen (140 Bytes) lang
- übermittelt eindeutige Meldungen (keine Hörfehler)
- wird sicher zugestellt (Paging ist ohne Sicherung)
- wird zwischengespeichert wenn Empfänger nicht erreichbar (je nach Netzbetreiber bis zu 7 Tagen)
- wird automatisch zugestellt, sobald Empfänger wieder erreichbar
- kann diskret angekündigt werden (z.B. mit Vibration für Meetings)
- wird direkt auf dem Display des Handys angezeigt
- wird auf der SIM-Karte gespeichert (mind. 15 Kurznachrichten)

SMS versenden





SMS Technische Realisierung

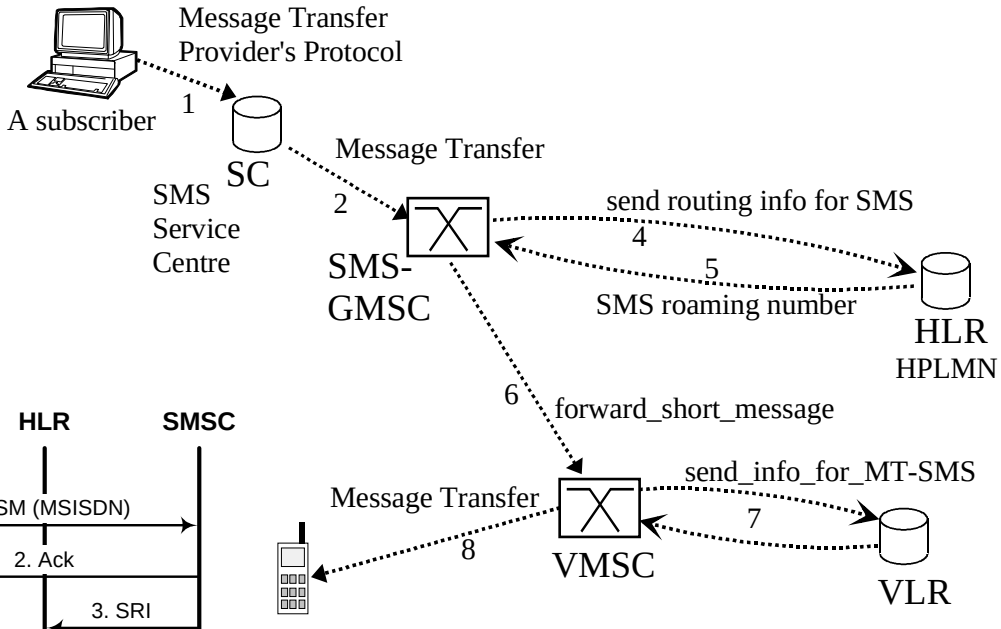
Technische Realisierung auf der Funkschnittstelle:

- Datenpaketübertragung auf SDCCH
- Parallel zu andern Diensten möglich (Telefon, Fax,..)
  dann Datenpaketübertragung auf SACCH während des Gesprächs
- Niedrige Priorität in der Schicht 2 (LAP-D_m)
- Wenn MS nicht erreichbar, dann weitere Zustellversuche
  (z.B. auf 48 Std. begrenzt)
- Gebühren werden pro SMS berechnet (3,5 .. 28 Pfennig/SMS)

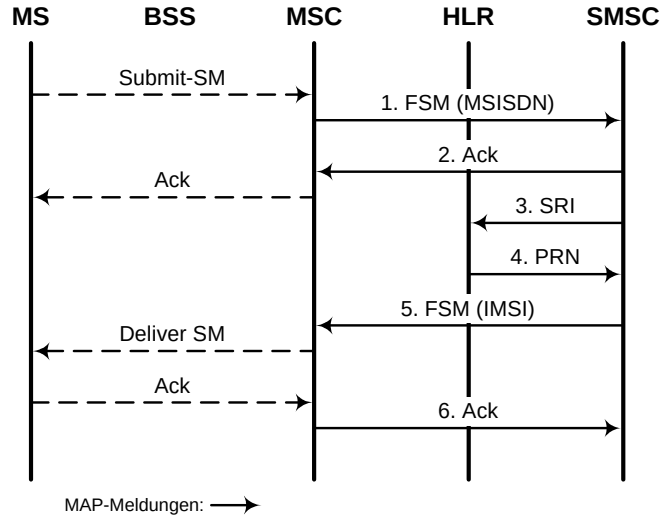
	Analoges Modem	Funktelefons (GSM-Funkmodem)	SMS-Servers Virtual Short Message Center (VSMSC)
Grundkosten	sehr niedrig	niedrig	hoch
Kosten pro SMS	Hoch	niedrig	sehr niedrig
Kapazität	sehr niedrig	niedrig	sehr hoch

VSMSC: über Datex-P mit dem »Original-SMSC« verbunden; hohe Kapazität (10.000 SMS/h)

SMS MT
(mobile terminated)



SMS Mobile to Mobile

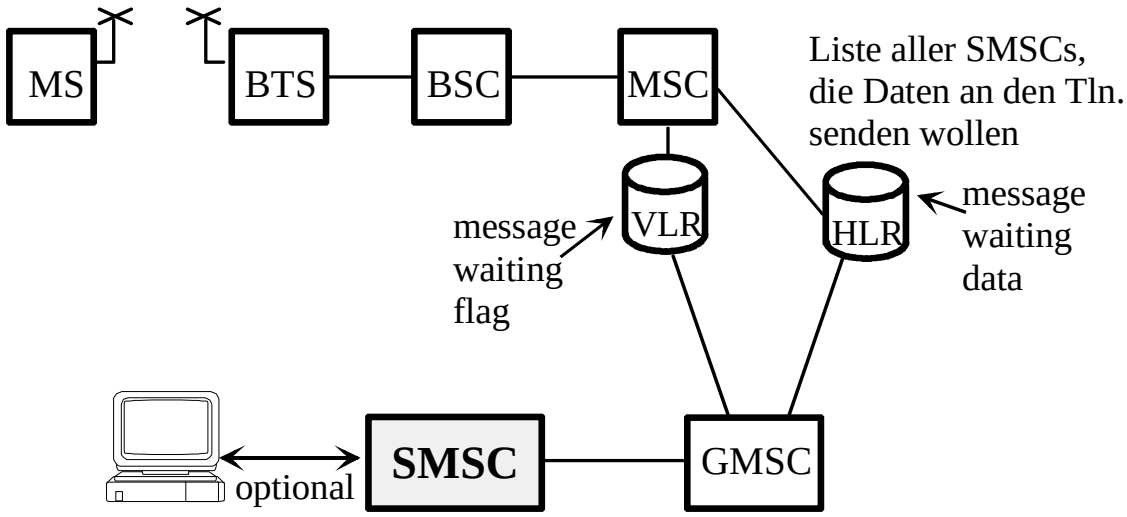


FSM *Forward Short Message*

SRI *Send Routing Info*

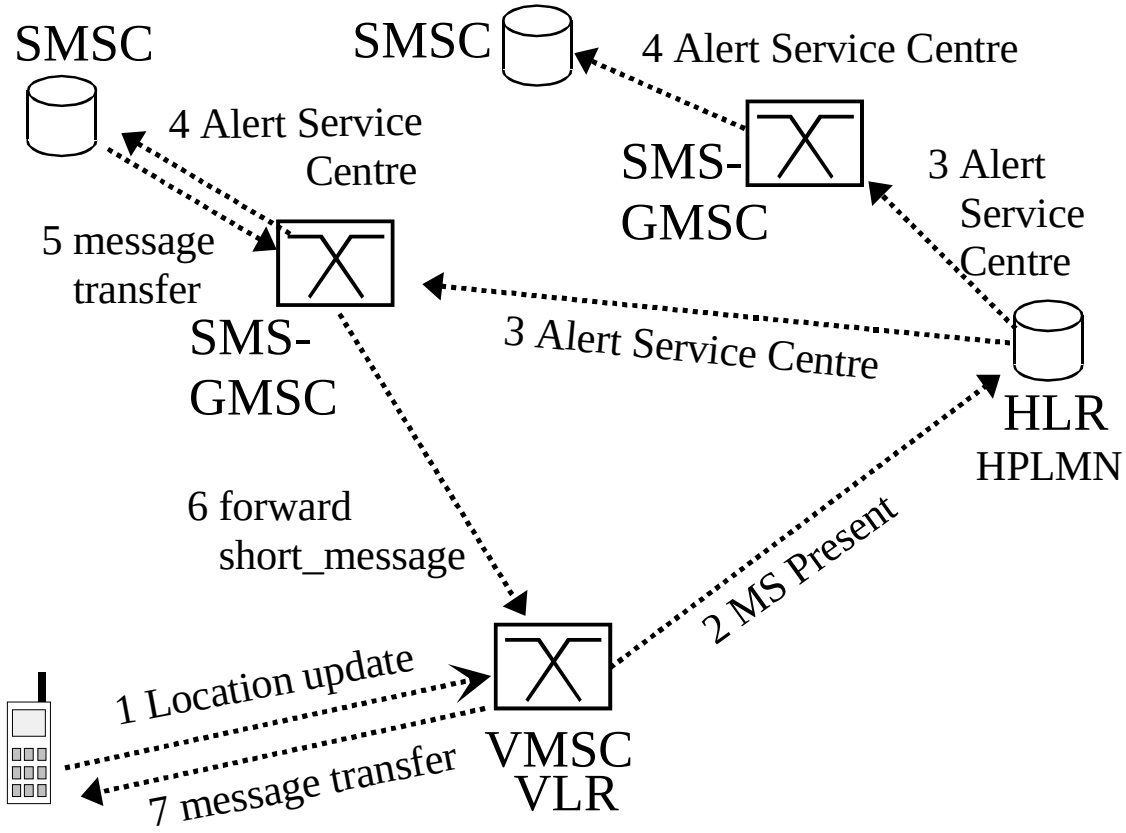
PRN *Provide Roaming Number*.

SMS-MT ist erfolglos: SMS kann nicht zugestellt werden



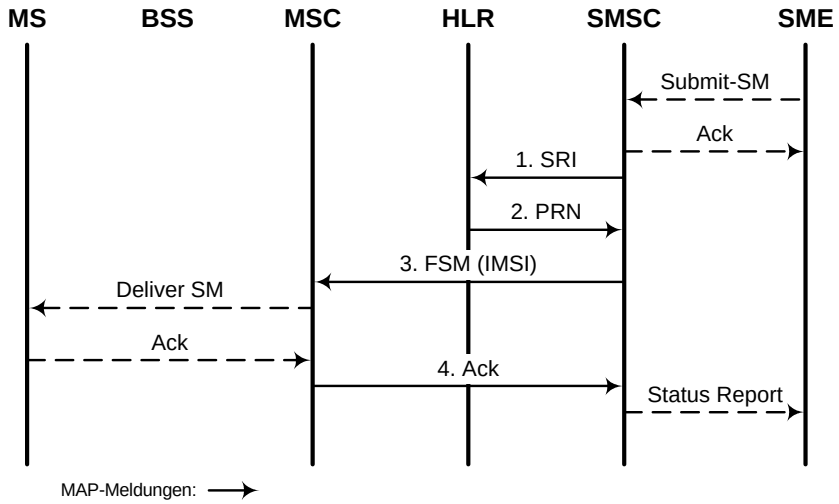
1. MS nicht erreichbar (keine Paging-Antwort)
2. Message_Waiting_Flag wird im VLR gesetzt
3. MSC schickt Error_Message zum SMS-GMSC
4. SMS-GMSC schickt Set_Message_Waiting_Data zum HLR;
   das HLR hat Liste SMSC-Adressen, bei denen noch Meldungen warten
5. Negative_Acknowledge wird zum SMSC geschickt

SMS wartet im SMSC - MS wird eingeschaltet



Signalling: Short Message Entity (SME-MT) ➔ MS

Die Kurznachricht wird von einer Short Message Entity (z.B. Großkundenzugang) abgesendet.



Die SME überträgt die SM zum MSC

1. Mit *Send Routing Info* wird der Aufenthaltsort des Empfänger erfragt
2. *Provide Roaming Number* gibt das *visited* MSC an.
3. Die SM wird mit *Forward Short Message* an das zuständige MSC weitergereicht

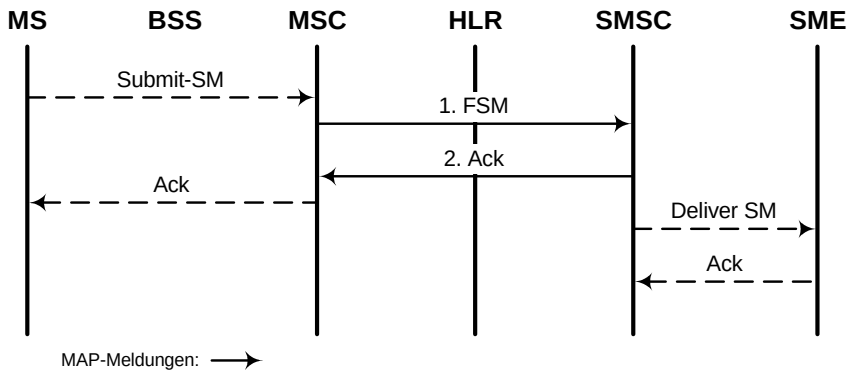
Das MSC überträgt die SM mit *Deliver SM* zur MS

4. Das MSC bestätigt dem SMSC die erfolgreiche Auslieferung

Oprtional wird ein Statusreport an die SME geliefert.

Signalling: MS ➔ Short Message Entity (SME-MT)

Signalisierung: vom Handy zu einer Short Message Entity (SME-MT)



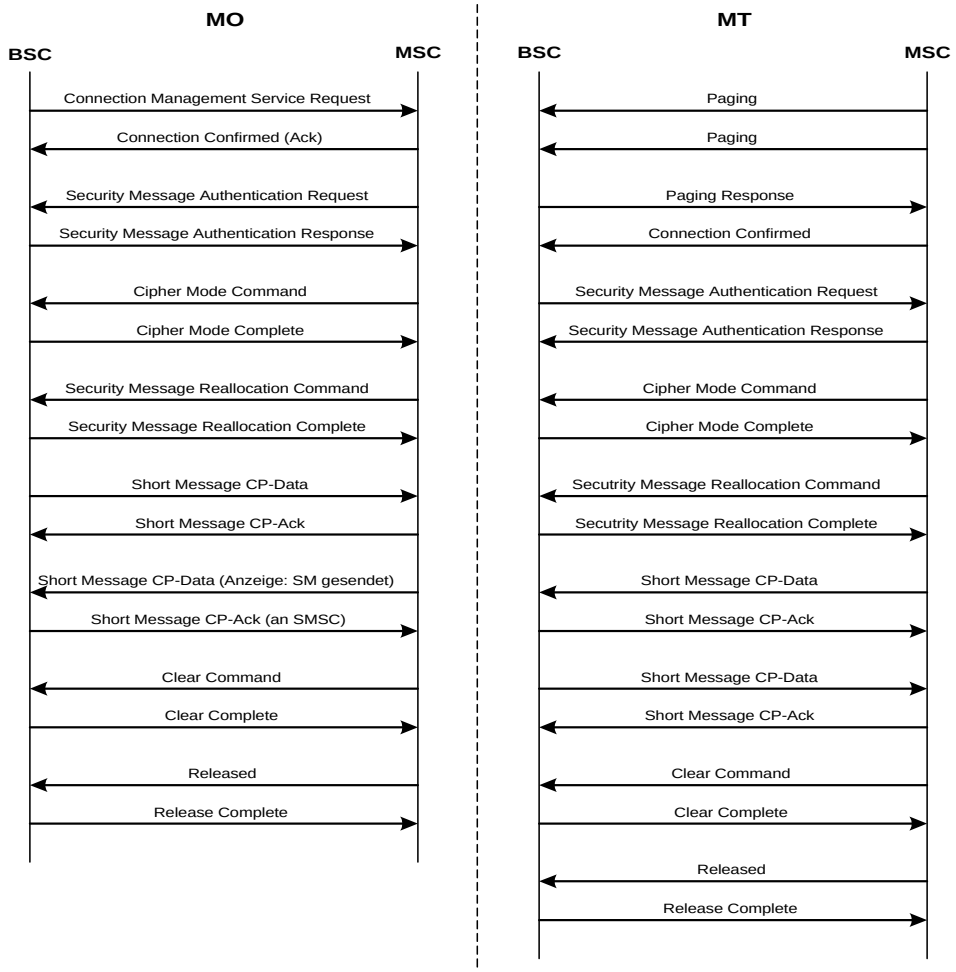
Die MS überträgt die SM zum MSC

mit *Forward Short Message* wird sie ans SMSC weitergeleitet

Das SMSC quittiert mit *Acknowledge*

Die SM wird mit *Forward Short Message* an das zuständige MSC weitergereicht

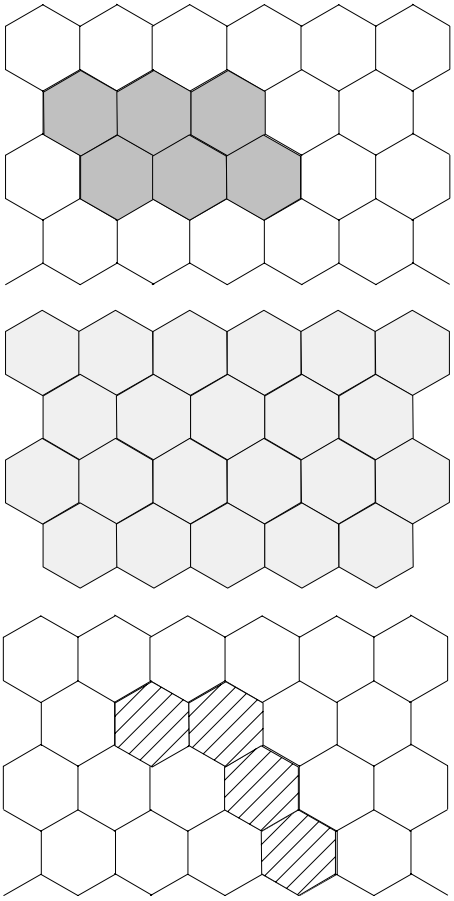
Das MSC überträgt die SM mit *Deliver SM* zum SME



Signalling

A-Interface

(BSC – MSC)



12.8 CBS : Cell Broadcast Service

SMS - Cell Broadcast

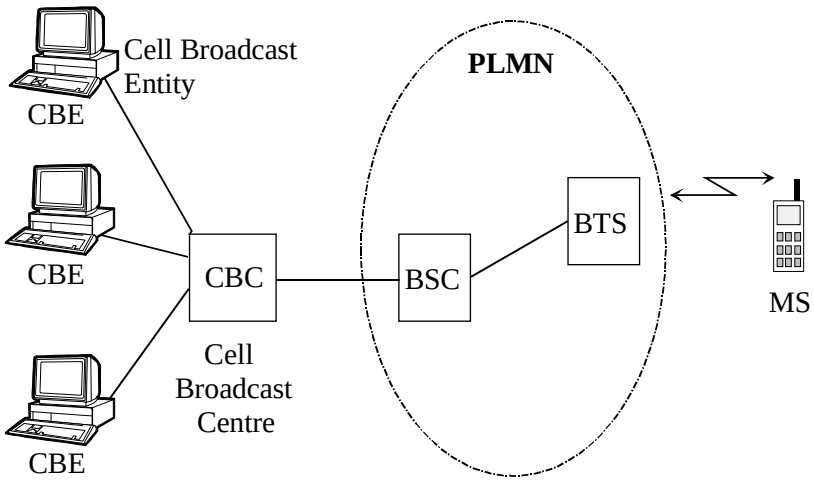
analogous to the Teletex service offered on television:

broadcast of unacknowledged messages
to **all** receivers within a particular region

broadcast to defined geographical areas (cell broadcast areas)
one or more cells, or the entire PLMN.

Individual CBS messages will be assigned their own geographical areas
(agreed between the information provider and the PLMN operator)

CBS:
Cell Broadcast Service



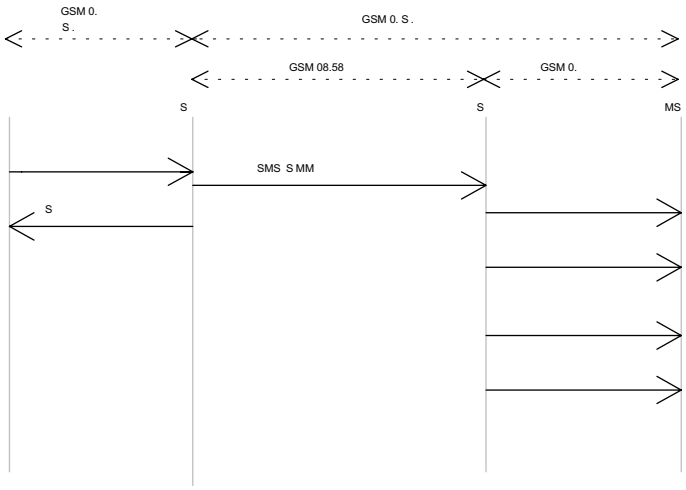
CBS messages

- originate from Cell Broadcast Entities.
- are then sent from the Cell Broadcast Centre to the BTSs, in accordance with the CBS's coverage requirements.
- are broadcast cyclically by the BTS:
  cyclically at a frequency specified by the information provider for a duration specified by the information provider

The repetition rate (frequency) of messages

- depends on the information that they contain:
  more frequent transmission of dynamic information (road traffic information)
  less frequent transmission of more static information (weather information)
- will also be affected by the speed mobiles which rapidly traverse cells.

CBS: Cell Broadcast Service



Content of Write-Replace Request/Indication message (CBC ➔ BSC)

Message-Identifier	M	
Old-Serial-Number	O	(delete or overwrite)
New-Serial-Number	M	
Cell-List	M	(geographical area)
Repetition-Rate	M	(frequency)
No-of-Broadcasts-Requested	M	(0 – 2880)
Number-of-Pages	M	
Data Coding Scheme	M	
CBS-Message-Information-Page1	M	(82 octets)
CBS-Message-Information-Lenght1	M	
CBS-Message-Information-Page2	O	(82 octets)
CBS-Message-Information-Lenght2	O	
CBS-Message-Information-Page3	O	
CBS-Message-Information-Lenght3	O	
etc.	O	
etc.	O	

BSC ➔ BTS: The SMS BROADCAST COMMAND is a 88 octet fixed lenght CBS page.

BTS ➔ MS : The BTS splits the page into four 22 octet blocks, adds the sequence number and transmits the four resulting blocks on the air.