



UNIVERSITETET
I OSLO

Den teknologiske utviklingen til mobiltelefonen

Under panseret på mobiltelefonen

Sverre Holm

Universitetet i Oslo



Mobiltelefon

1. Mobil – historie og statistikk
2. Cellenettverk
3. GSM-nettet
4. Digital representasjon av lyd og koding
5. GSM ++: HSCD, GPRS, EDGE, EGPRS
6. Stråling
7. Avlytting
8. Posisjonering
9. GSM-R
10. 3G: UMTS



?

- Hvorfor slår mobiltelefonen inn på PC-høytalerne?
- Kan mobiltelefoner gi skadelig stråling?
- Kan mobiltelefonen avlyttes?
- Hvordan finner man ut hvor en mobiltelefon er?
- Hva er GSM, GPRS, EDGE og UMTS?



UNIVERSITETET
I OSLO

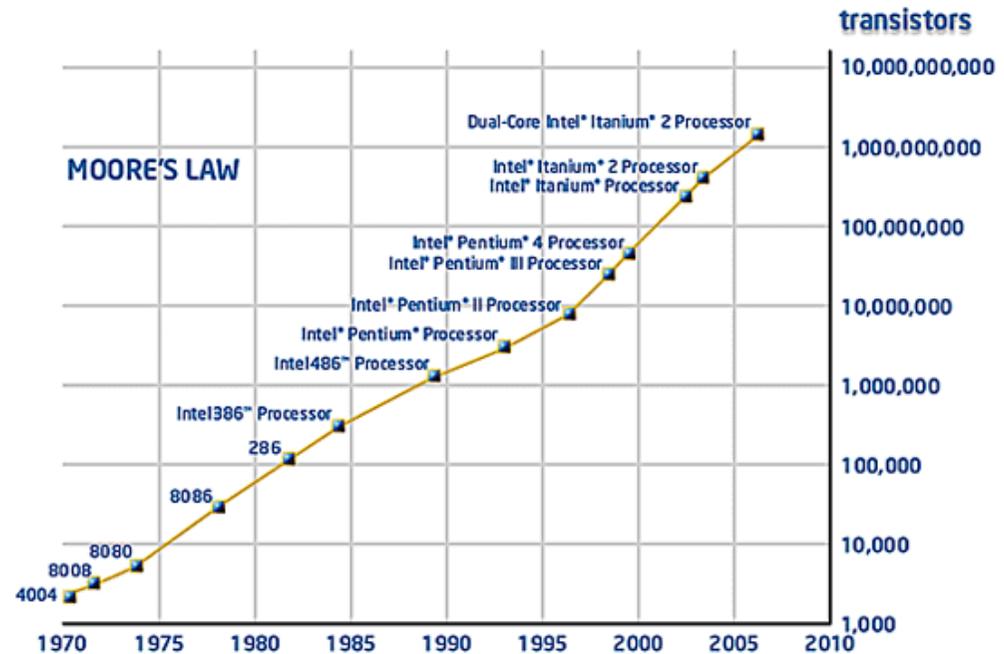
Forskjell mellom mobiltelefon og Walkie-Talkie?





Raskere og raskere

- Mobiltelefon + PC:
Moore's lov merkes direkte i produkter
- Moore's lov:
 - Dobling av antall funksjoner på en integrert krets pr ~18 måneder
 - Siden 60-tallet
- Teknologioptimisme
 - Lett å tro den gjelder all teknologi
 - Generelt lav realfagskompetanse?



<http://www.intel.com/technology/mooreslaw/index.htm>

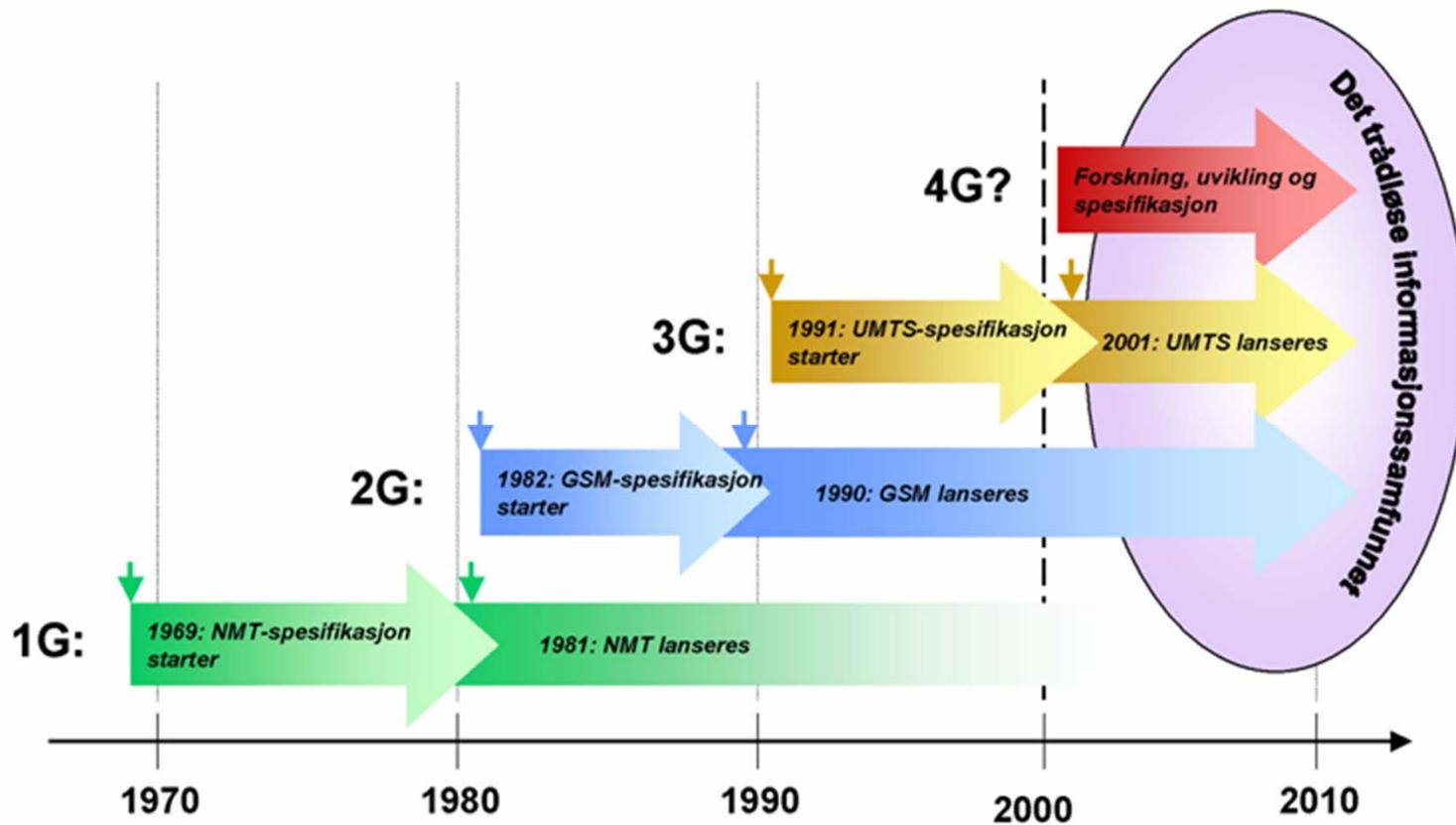


Mobiltelefon

1. Mobil – historie og statistikk
2. Cellenettverk
3. GSM-nettet
4. Digital representasjon av lyd og koding
5. GSM ++: HSCD, GPRS, EDGE, EGPRS
6. Stråling
7. Avlytting
8. Posisjonering
9. GSM-R
10. 3G: UMTS



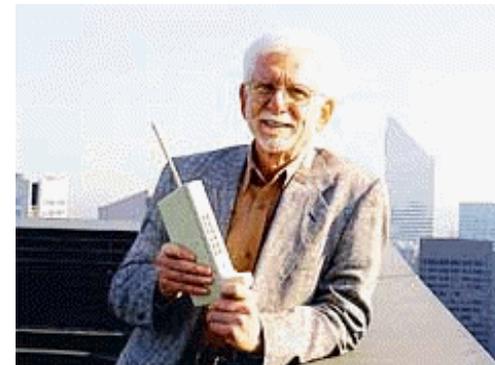
GSM = Globalt System for Mobilkommunikasjon





0'te generasjon: Mobiltelefon siden 1956

- Ericssons "Mobile Telephony A"
 - 40 kilo, Dreieskive for å slå nummeret.
 - Stockholm og Göteborg, maks 100 samtaler av gangen
- Norge fra 1966: manuelt system til midten av 80-tallet
 - Offentlig Landmobil Telefoni
- Begge ~160 MHz, FM
- Første forsøk med cellebasert system: Motorola 1973





UNIVERSITETET
I OSLO

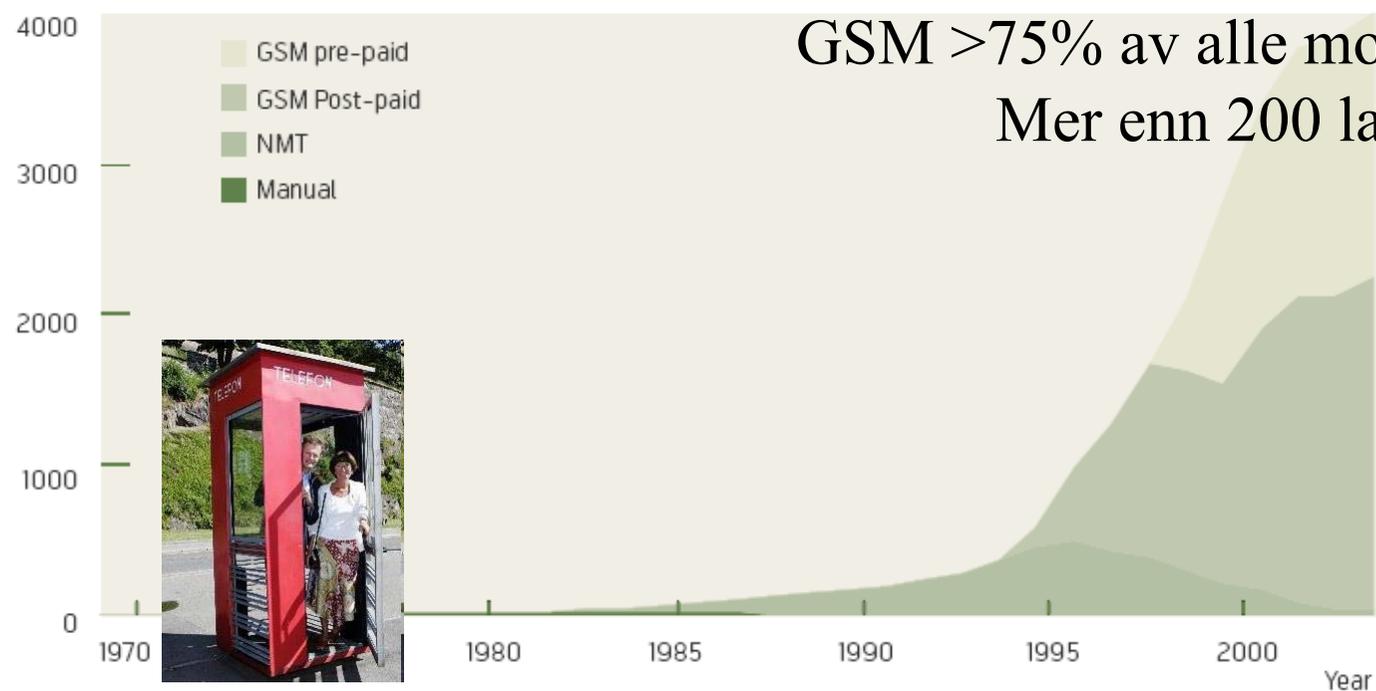


I 1981 kom de første "bærbare" NMT-telefonene.
Til venstre en Simonsen 450-telefon i bæremeis.
Foto: Ulrichsen, Rolf Chr., Aftenposten



Mobiltelefonbruk i Norge

Number of subscriptions x 1000



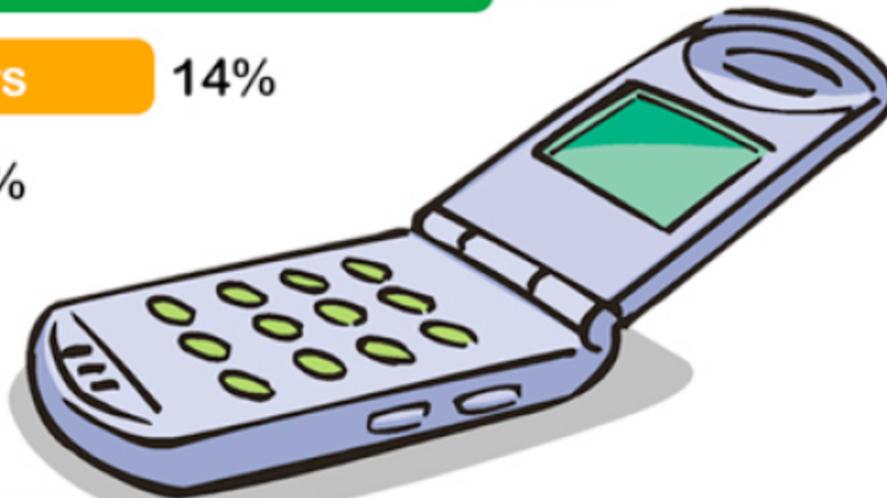
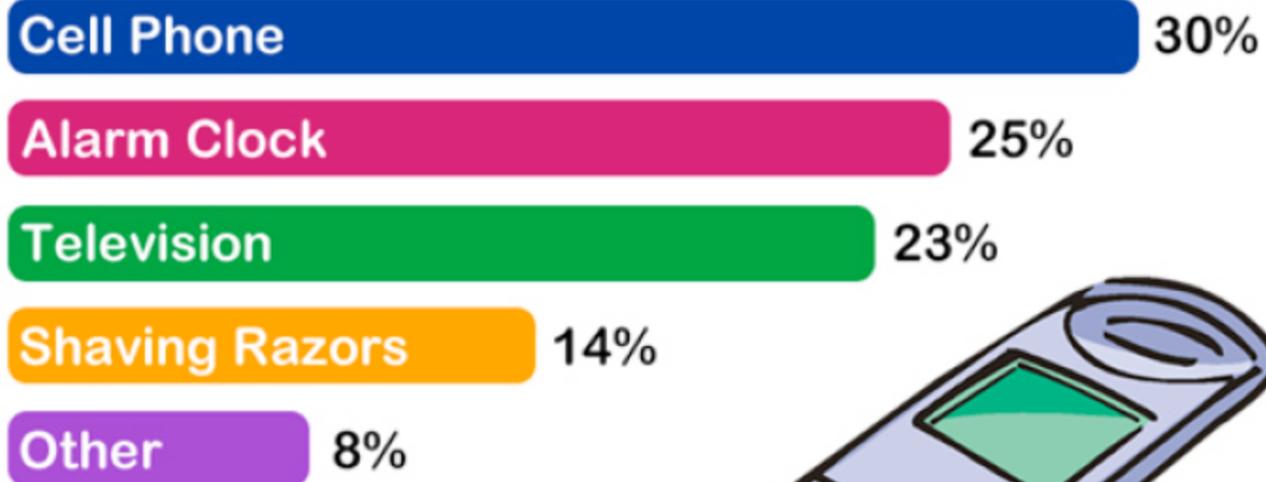
Mer enn 2 milliarder brukere (2006)

GSM >75% av alle mobilbrukere

Mer enn 200 land



Inventions we hate most but can't live without



Source: Lemelson-MIT Program



Fast- og mobiltelefon, Norge

Mean minutes per day

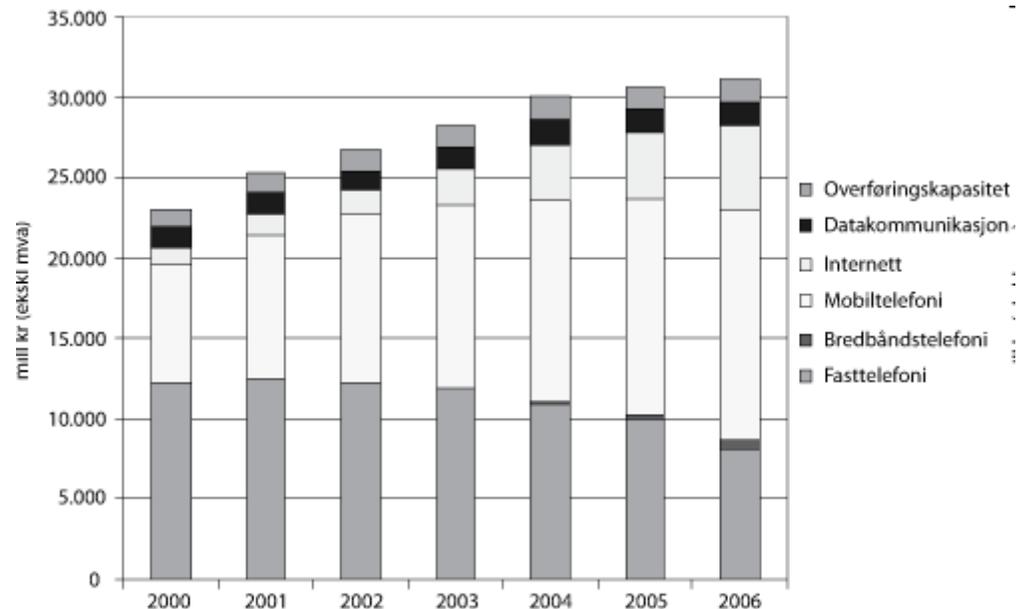


Mobil:

- Telenor 54% i 2006, fallende
- NetCom og Chess (begge TeliaSonera) bortimot 31%



Omsetning - teletjenester



- Økende:
 - Mobiltelefoni
 - Internett
 - Bredbåndstelefon
- Fallende:
 - Fasttelefoni

Sluttbrukeromsetning for teletjenester 2000-2006. Samlet og de enkelte delmarkeder.

<http://www.regjeringen.no/nb/dep/sd/dok/regpubl/otprp/2006-2007/Otprp-nr-72-2006-2007-3.html?id=472560>



Mobiltelefon

1. Mobil – historie og statistikk
2. **Cellenettverk**
3. GSM-nettet
4. Digital representasjon av lyd og koding
5. GSM ++: HSCD, GPRS, EDGE, EGPRS
6. Stråling
7. Avlytting
8. Posisjonering
9. GSM-R
10. 3G: UMTS



Utvikling mot dagens mobilnettverk

1. Punkt til punkt kommunikasjon
2. Kommunikasjon via en enkel basestasjon
 - 0'te generasjons mobil
 - Dagens systemer for politi, brann, taxi etc
 - Eget for byer
3. Kommunikasjon via mange basestasjoner
 - Celler
 - Svitsjing mellom celler uten at brukeren merker det

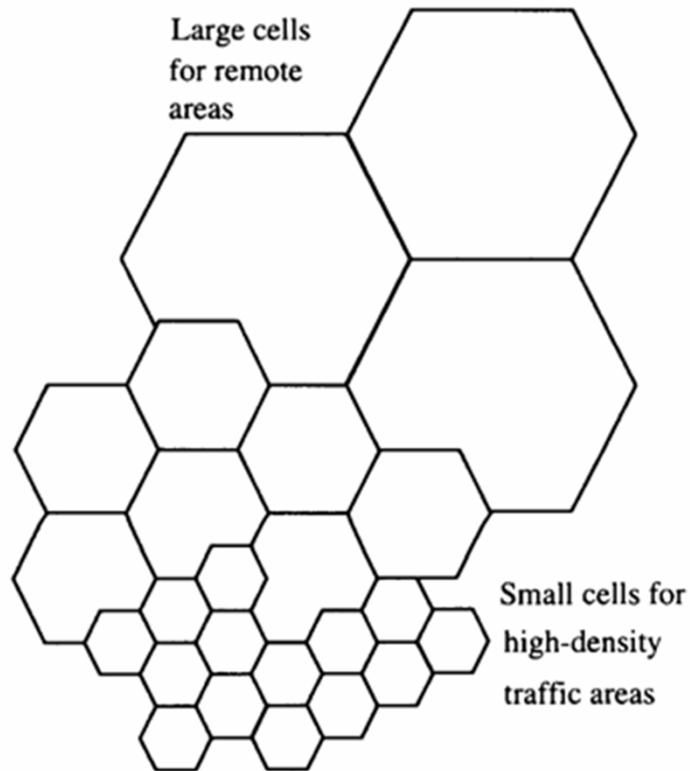


UNIVERSITETET
I OSLO

Cellenettverk

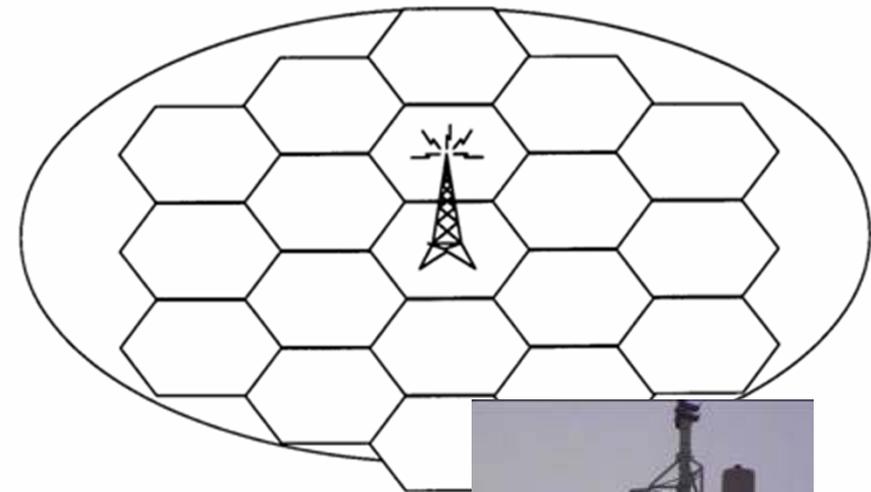
Gjenbruk av frekvenser

Max radius ca 35 km



Mikrocelle: for stillestående tlf

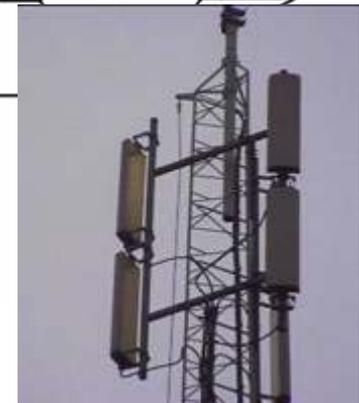
Paraplycelle: for biler i fart



Boundary of a Micro Cell



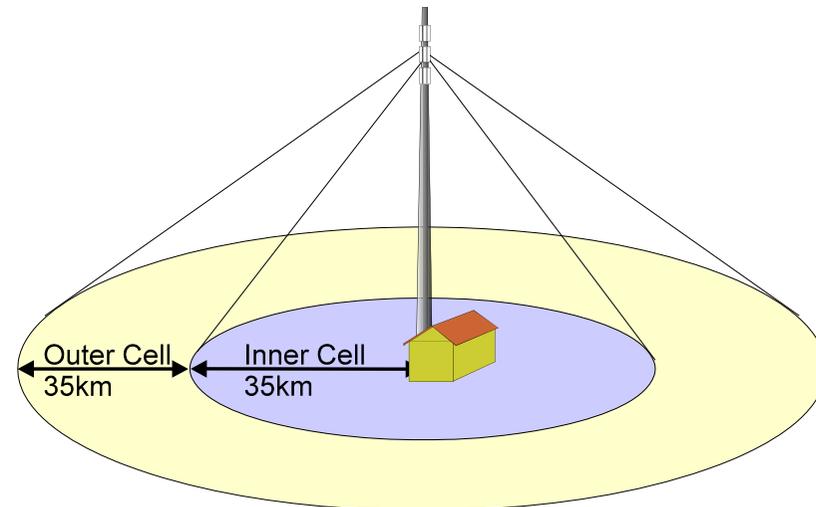
Boundary of the Umbrella Cell





Utvidet celle

- Timing advance – kompensasjon for forsinkelse i 64 trinn:
 - 1 bit \Leftrightarrow 3.63 us \Leftrightarrow $3.63 \text{ us} * 3e8/2 = 545 \text{ m}$
 - 64 trinn \Leftrightarrow $64 \times 545 \text{ m} = 34.88 \text{ km}$
 $\sim 35 \text{ km}$
- 35 km er i utgangspunktet maksimal cellestørrelse
- Telenor bruker utvidede celler langs kysten, rekkevidde begrenses av
 - Jordas krumning
 - Utgangseffekt, antenne
 - 80 km, i heldige fall 120 km
 - Bruker av de 8 time-slots





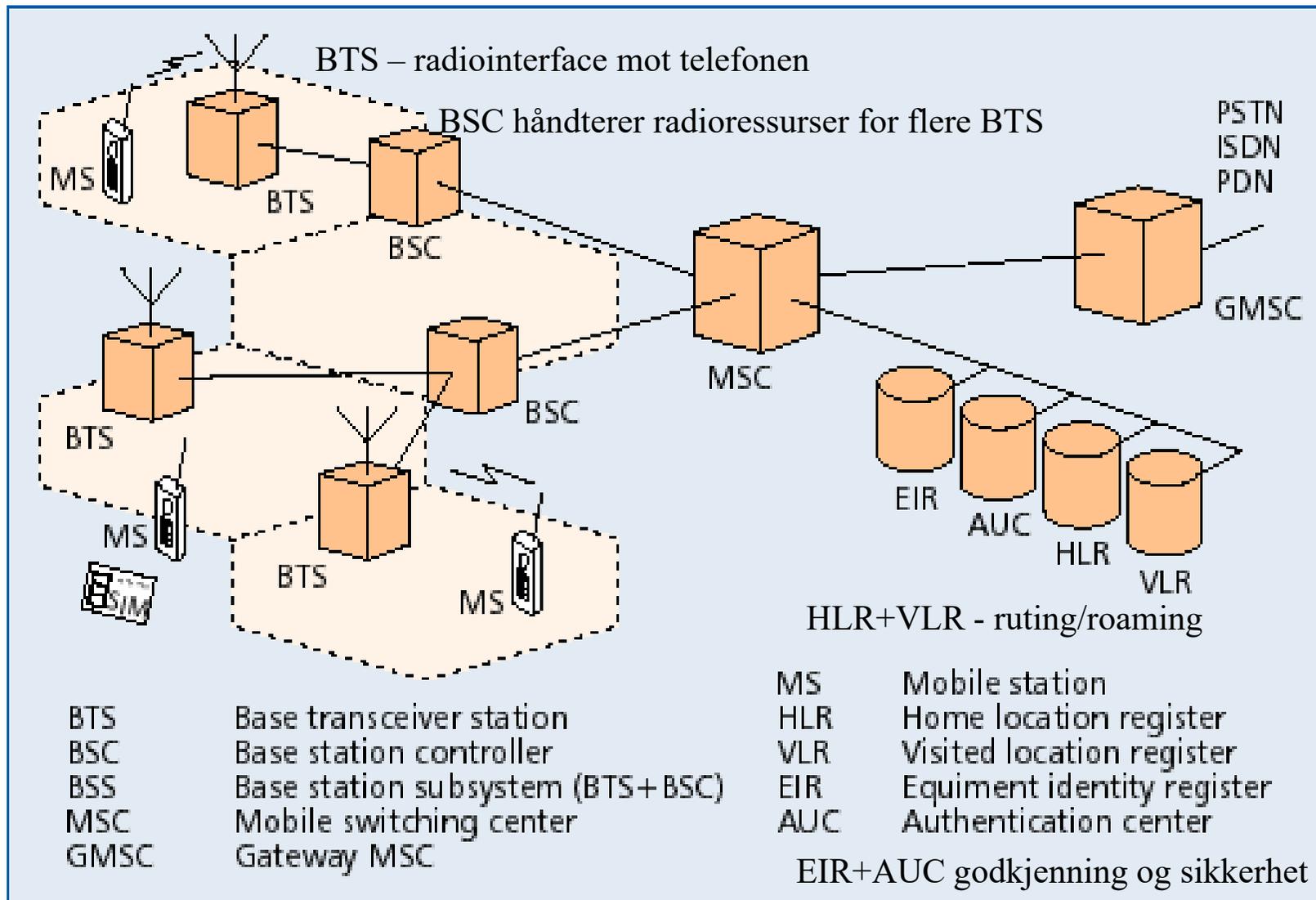
Mobiltelefon

1. Mobil – historie og statistikk
2. Cellenettverk
3. **GSM-nettet**
4. Digital representasjon av lyd og koding
5. GSM ++: HSCD, GPRS, EDGE, EGPRS
6. Stråling
7. Avlytting
8. Posisjonering
9. GSM-R
10. 3G: UMTS



GSM-nettet

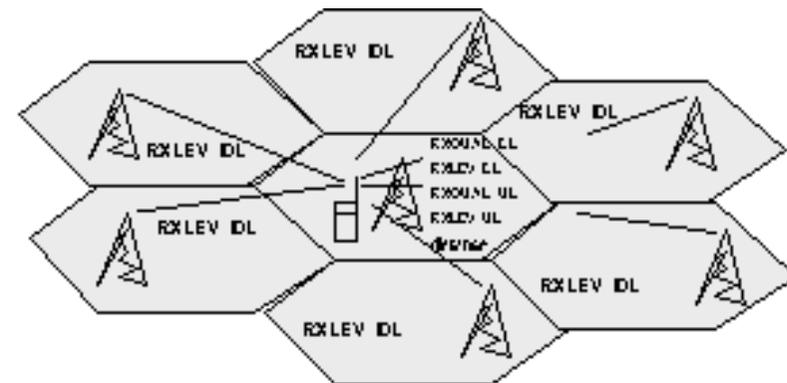
SIM – Subscriber Identity Module lagrer bl.a.
IMSI – International Mobile Subscriber Identity





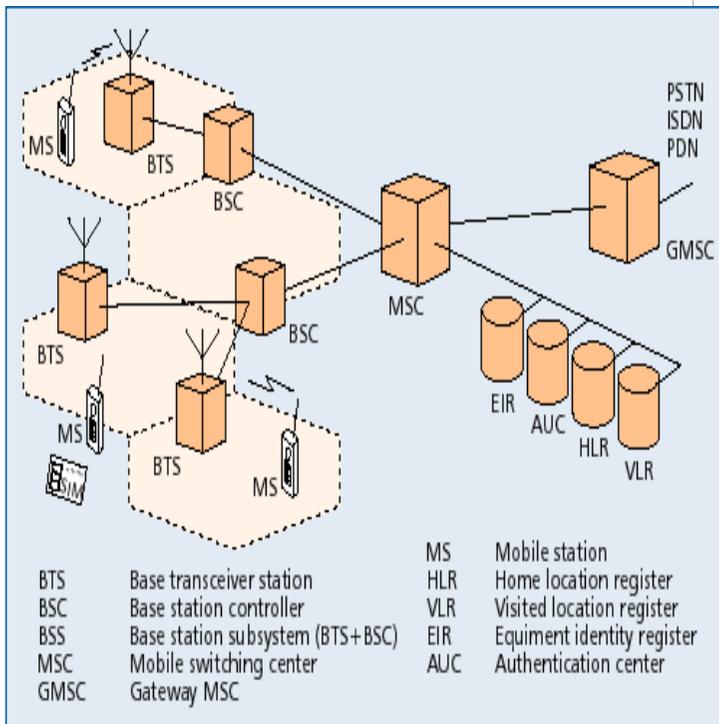
Handover

- Mellom kanaler i samme celle (forskjellige tidsluker)
- Mellom celler under kontroll av samme Base Station Controller,
- Mellom celler under kontroll av forskjellige BSCs, men tilhørende samme nettverk - Mobile services Switching Center (MSC)
- Celler under kontroll av forskjellige MSCs.





Oppringing fra mobil



MS	BTS	Action
→		Channel Request
	←	Channel Assignment
→		Call Establishment Request
	←	Authentication Request
→		Authentication Response
	←	Ciphering command
→		Ciphering complete, from now on ciphering is in place
→		Setup message, indicating the desired number
	←	Call Proceeding, the network routes the call to the desired number
	←	Assignment of a traffic channel for the designated use "exchange of user data"
→		Assignment complete, from now on all messages are exchanged on the traffic channel
	←	Alerting, the called number is not busy and the phone is ringing
	←	Connect, the called party accepted the call
→		Connect acknowledge, now the call is active and both parties can talk to each other
	←	Exchange of speech data

Figure 3.9 Mobile-originated call establishment.



Registrering i nettverket

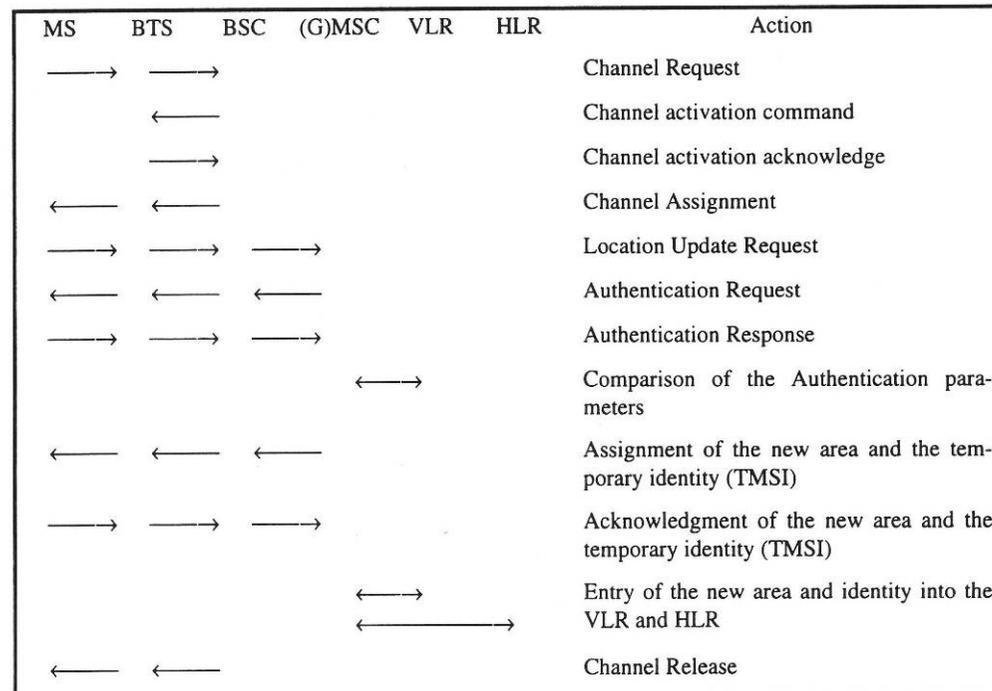
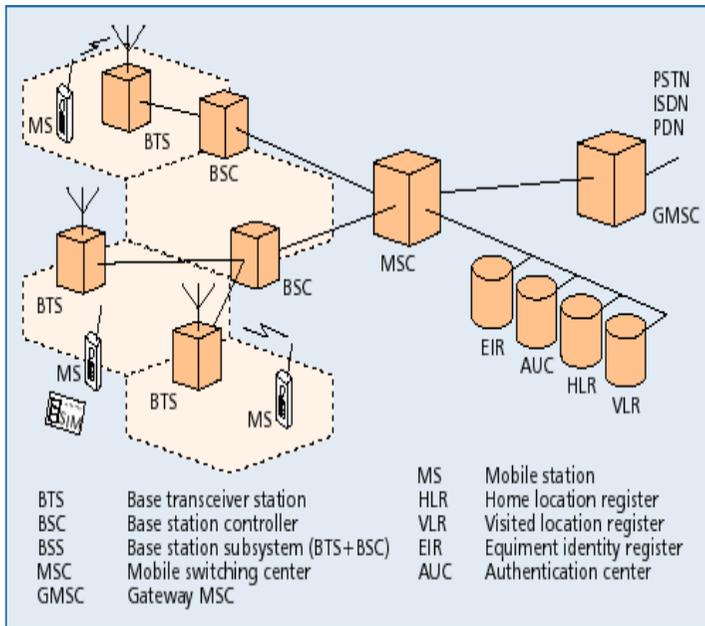


Figure 3.8 Registration in the network.

TESTER

OMTALE

ARKIV

MOBILTELEFONER

MPS/LYD

SPILL

TILBEHØR

TJENESTER

ALLE OMTALER

RÅD OG HJELP

PRISER

DOWNLOAD

EKSPERTPANEL

FORUM

MMS

BLOGG

SELG MOBILNUMMER

KONKURRANSER

BRUKTMARKED

SPILL OG MUSIKK

TEST DEG SELV NY

FINN DIN MOBIL! NY

MIN SIDE

OM MOBILEN.NO

Windows Live Alerts +

mobilen.no / Omtale / Arkiv / Mobiler rett i dass

Mobiler rett i dass

Vannverket i den finske hovedstaden Helsingfors slår alarm etter at mobiltelefoner i kloaknettet har blitt et økende problem. Mobiler som blir skylt ned i toaletter kan nemlig blokkere avløpsrørene.

Publisert: 21.nov 2005 kl.16:17
Sist oppdatert: 18.apr 2006 kl.13:35
Skrevet av: Henriette Skyseseth

[Utskriftsvennlig versjon](#)

Stadig flere mobiltelefoner får en illeluktende død i kloaknettene. Dette har ført til hodebry for det finske Vannverket.

- Med litt flaks flyter mobilene helt ned til renseanlegget, men av og til setter de seg fast og blokkerer kloaknettet. Da blir det katastrofe, sier Yrjö Lundström i det finske Vannverket, til Helsingin Sanomats nettavis.

Hvor mange mobiler som har endt sine dager i det finske kloaknettet er ikke kjent, men i følge VG viser tall fra Storbritannia at 600 000 britiske mobiler årlig lider den grusomme toalett-skjebnen.

Slik ødelegger vi mobiler

Det er mange mer eller mindre uforklarlige grunner til at vi mister mobilene våre. Cellular-News.com har gjengitt en liste over dette, utarbeidet av Siemens. Nedenfor finner du oversikten over de vanligste mobil-skjebnene.



Søk i alle omtalene

Søk!

CHESS PRESENTERER

MER



MINDRE

DU FINNER DITT
MOBILABONNEMENT



Slik ødelegger vi mobiler

1. Mistet i bakken
2. Klemmt i stykker i en trang lomme
3. "Druknet" i regnvær
4. Kastet i bakken i raseri
5. Hunden eller babyen tok den
6. Mistet i toalettet
7. Mistet i sjøen
8. Glemte den igjen på biltaket
9. Ble ødelagt av svette under trening
10. Mistet i snøen

Cellular-News.com,

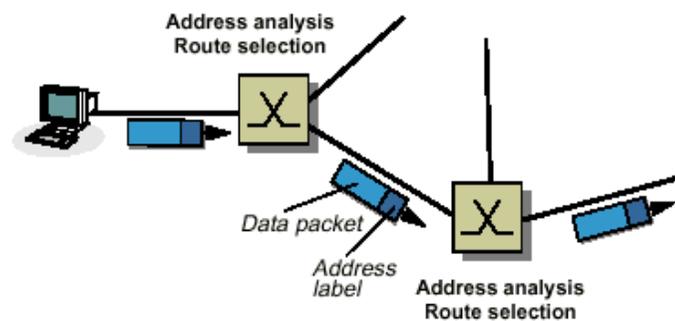
<http://www.mobilen.no/default.asp?page=131&article=16814>



Linje-/pakkesvitsjet nett



Tradisjonelt telefonnett

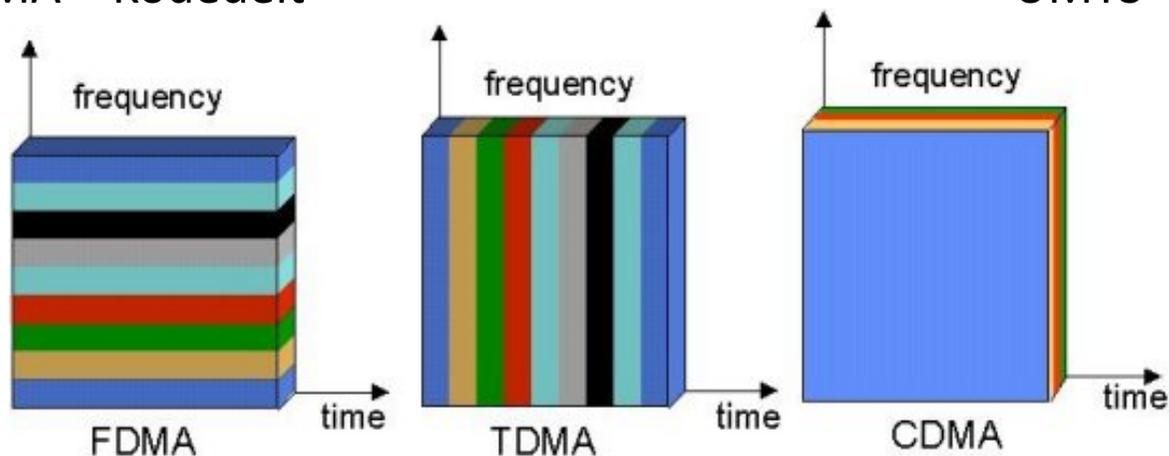


Datanett



Deling av kanal

- FDMA – Frekvensdelt moltipel aksess
- TDMA – Tidsdelt / Frekvenshopping
- CDMA – Kodedelt



Som radio:

- P1 88,7 MHz
- P2 100 MHz

Som en samtale:

- Først du
- så meg ...

4 rundt et bord:

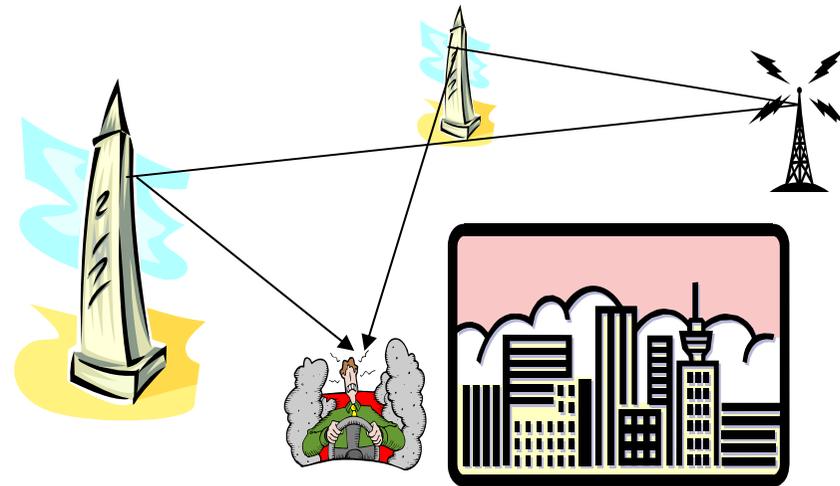
Samtale på "kryss"



Modulasjon

Alternativer:

- Sende hurtig i smalbandet kanal
 - Må teste kanalen jevnlig som en radar: sende kjente data
 - Så kompensere for ekko
 - “Gaussian minimum shift keying” – GMSK
- Sende langsomt i mange kanaler
 - OFDM
 - Brukes i DAB og digitalt TV nett





Paris februar 1987

In February 1987 *New Scientist* wrote:

- “Cars equipped with the various technologies on offer were driven around Paris. The winner was a surprise – it was a system called ELAB, that was developed not by a large company but by Trondheim University in Norway.”



Figure 4 The Paris field trials [From *New Scientist*, Feb 1987]



Torleiv Maseng
is Director of
Research at the
Norwegian
Defence
Research
Establishment



Figure 1 Odd Trandum: The brain behind the prototype development. Here he is skiing with what eventually ended up becoming a GSM terminal. I am behind him outside the picture with car batteries

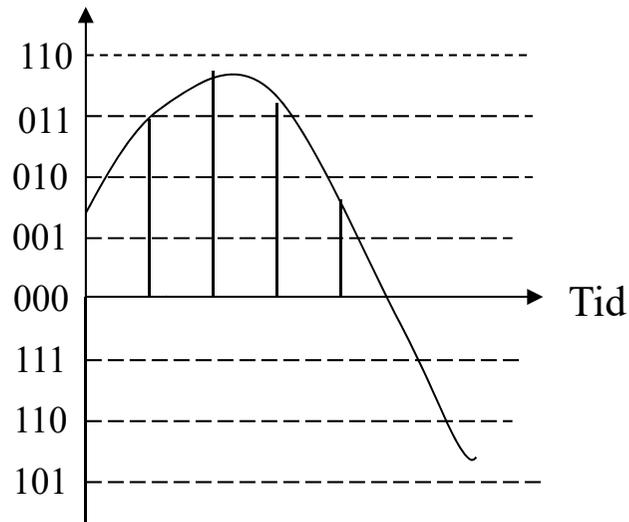


Mobiltelefon

1. Mobil – historie og statistikk
2. Cellenettverk
3. GSM-nettet
4. Digital representasjon av lyd og koding
5. GSM ++: HSCD, GPRS, EDGE, EGPRS
6. Stråling
7. Avlytting
8. Posisjonering
9. GSM-R
10. 3G: UMTS



Digital representasjon av lyd



- Mikrofonen gjør lydbølgene om til et elektrisk signal
- Signalet leses av ved faste tidspunkter (8000 ganger per sekund)
- Verdiene kan bare tilnærmes med et gitt antall faste nivåer (diskretisering)
- Hvert nivå representeres med en bestemt sekvens av 0-er og 1-ener

Med 3 bit: $2^3 = 8$ nivåer

13 bit gir $2^{13} = 8192$ nivåer, dvs $13 * 8000 = 104\ 000$ bits/sek

Fasttelefon: Tar log til amplitude: 13 bit \rightarrow 8 bit: 64 000 bits/sek



Koding

Inn 104 kbit/s

Talekoder:

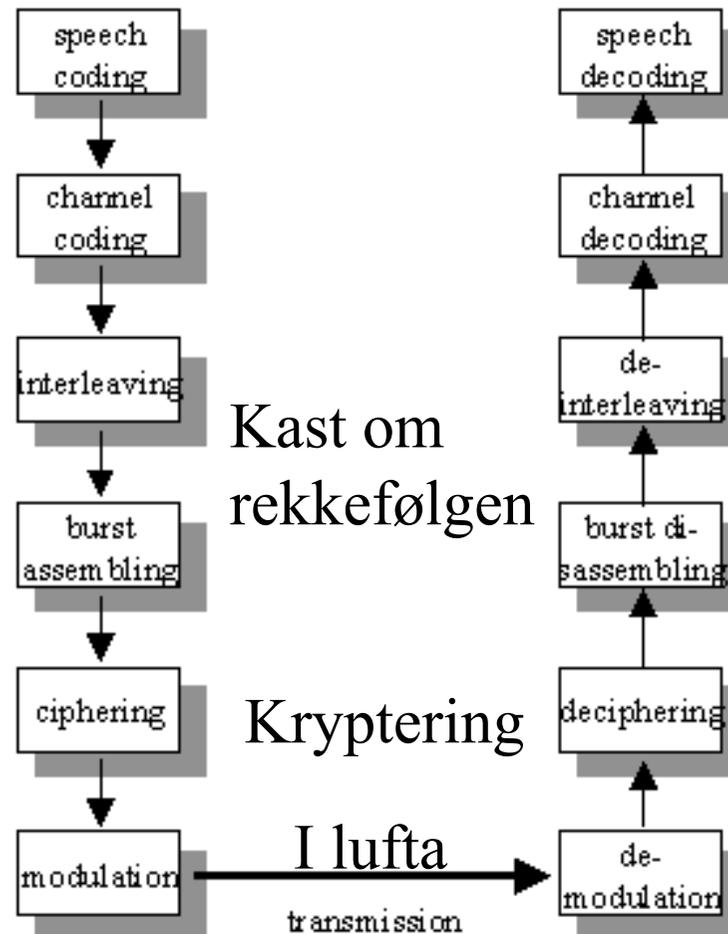
-Full rate: 13 kbps

-Half rate: 6.5 kbps

-Extended fullrate: 12.2

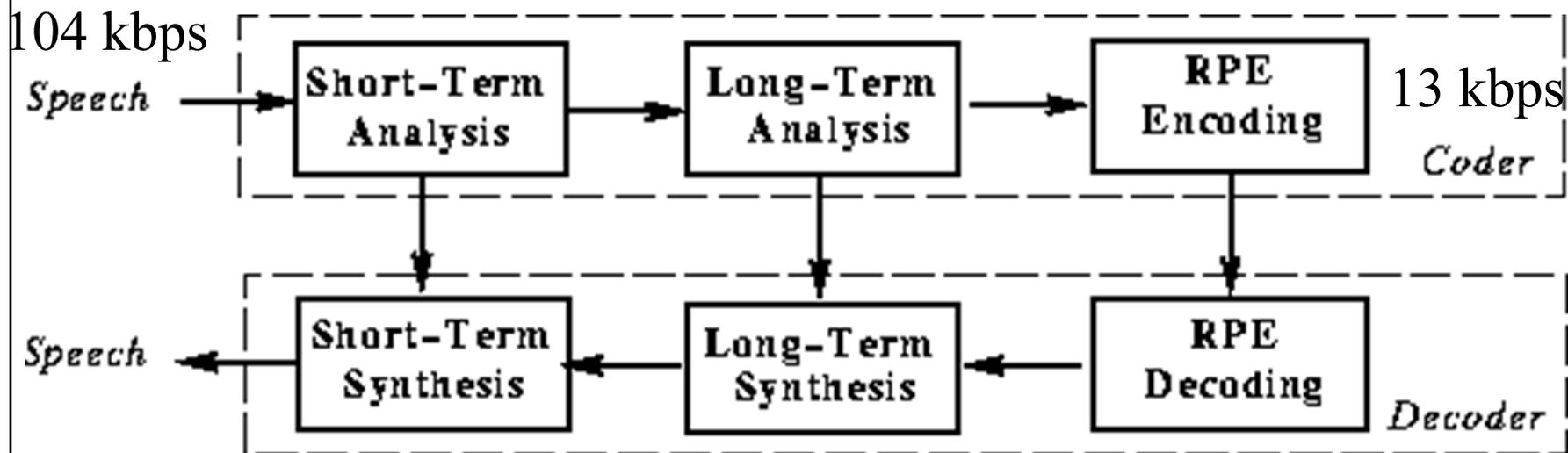
Kanalkoding:

13 kbps -> 22 kbps





Talekoding i GSM



Kort-tid = 50 ganger i sekundet oppdateres spektralenvelope (AR)

Lang-tids = estimerer grunnfrekvens til stemt lyd

RPE - Regular Pulse Excitation = restsignal kodes

Discontinuous Transmission - pauser detekteres, sparer strøm,
setter inn støy i mottaker (Comfort Noise)



Mobiltelefon

1. Mobil – historie og statistikk
2. Cellenettverk
3. GSM-nettet
4. Digital representasjon av lyd og koding
5. **GSM ++: GPRS, EDGE, EGPRS**
6. Stråling
7. Avlytting
8. Posisjonering
9. GSM-R
10. 3G: UMTS



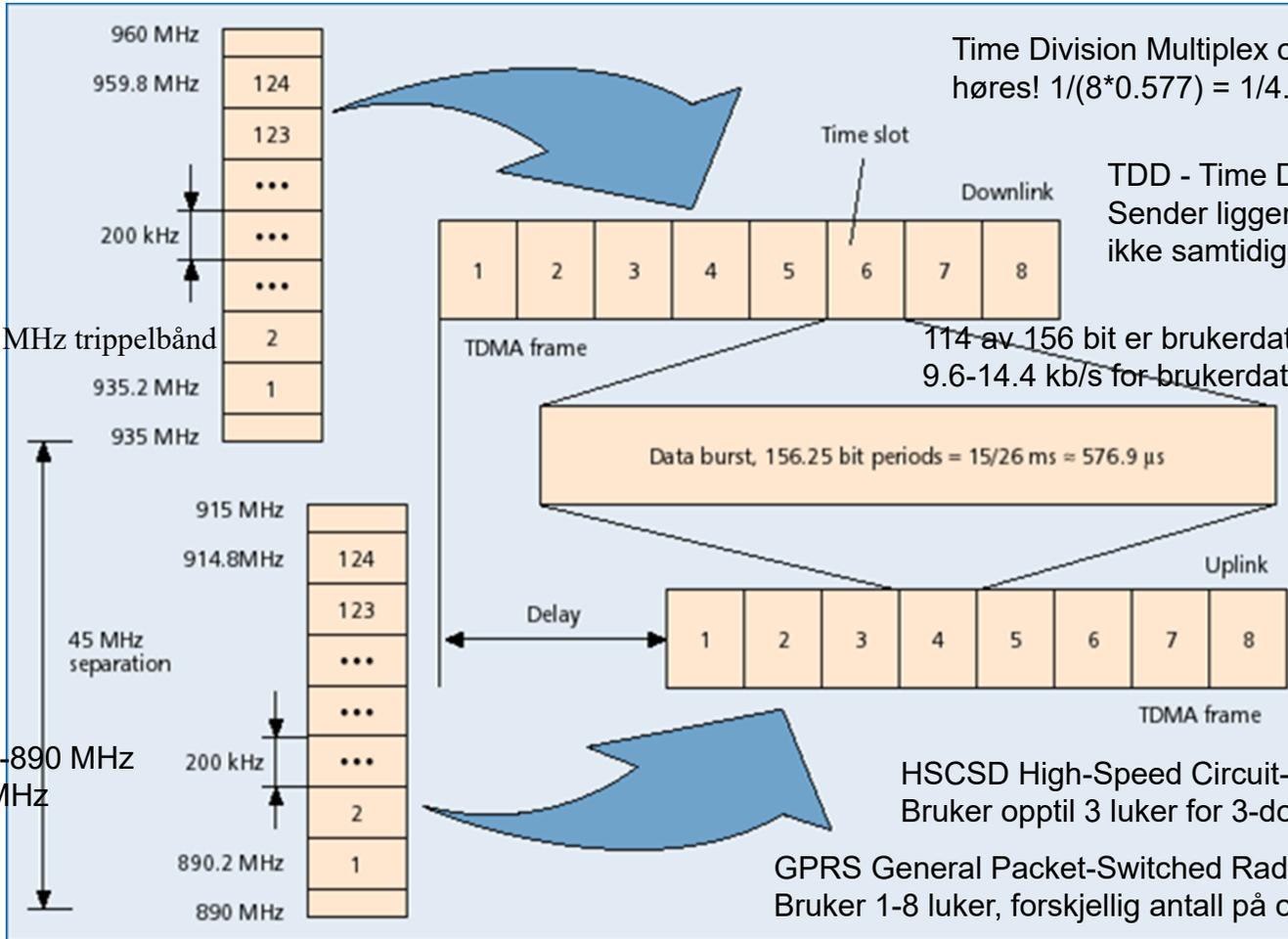
Generasjoner

- 1. generasjon: Analog
 - Nordisk Mobiltelefon, NMT-450, NMT-900, bare tale
- 2. generasjon: Digitalt
 - GSM: Global System for Mobile Communications
 - Tale, data (fase 2+: 14.4 kbit/s)
 - SMS: Short Message Service
- Utvidete tjenester i GSM-nettet (nærmest glemt nå):
 - WAP: Wireless Application Protocol
 - HSCSD: High Speed Circuit-Switched Data; linjesvitsjet, 3 x datarate: 43.2 kbit/s
- 2.5. generasjon: Pakkesvitsjet
 - GPRS: General Packet-Switched Radio Services
 - opp til 8 x datarate, 115 kbit/s
 - Kobler bare opp når data, IP-basert
- 2.75. generasjon: EDGE: Enhanced Data Rates for Global Evolution
 - EGPRS: Enhanced General Packet Radio Service. 3-dobling av GPRS datarate (236.8 kbit/s kbit/s) (8-PSK) hvis kvaliteten på radiokanalen er god
 - EDGE Evolution: opp til 1 Mbit/s peak, to frekvenser, 32 eller 16 QAM, doble antenner
- 3G: UMTS: Universal Mobile Telecommunications System
 - 384 kbit/s ned, 64 kbit/s opp, opptil 2 Mbit/s datarate
 - HSDPA High Speed Downlink Packet Access
 - » 3,6 Mbit/s, normalt 0,5-1,5 Mbit/s.



Tid- og frekvensmultipleks

FDD – Frequency Division Duplex: 45 MHz (900) og 95 MHz (1800) avstand rx og tx



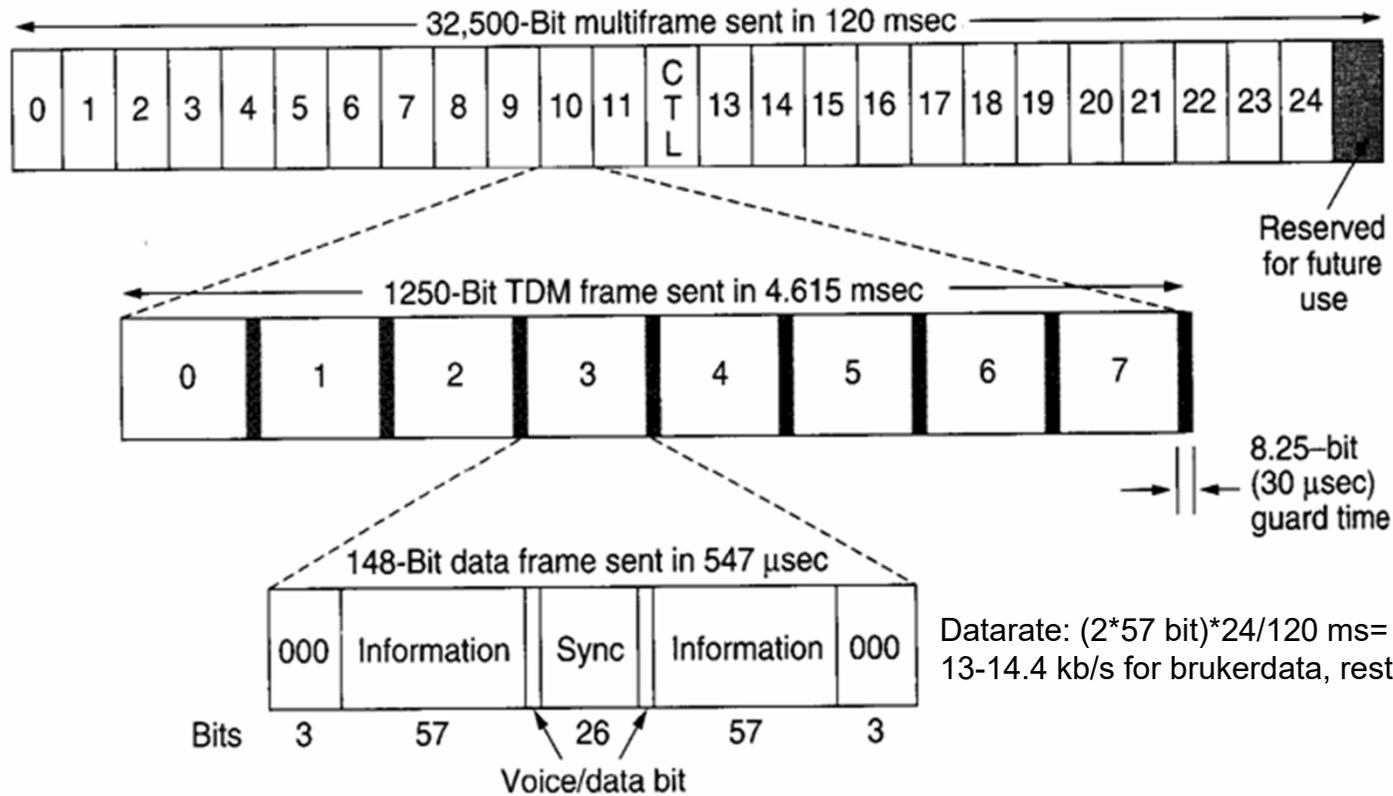
Nord-Am: 1900 MHz trippelbånd

E-GSM: 880-890 MHz
1710-1880 MHz

EDGE/EGPRS Øker datarate med faktor 3 pr luke i 4 luker
(8-PSK istfor GMSK)



Rammer i GSM



Datarate: $(2 \cdot 57 \text{ bit}) \cdot 24 / 120 \text{ ms} = 22.8 \text{ kb/s}$,
13-14.4 kb/s for brukerdata, resten feilkorreksjon

26 bit (~19%) kjente data for å finne kanalkarakteristikk



Dekningstriksene

- Jeg står i skapet med lyset av.
- Jeg står på høye ting som stoler eller i sofaen.
- Jeg står på soverommet til datteren min og holder i snoren fra takvifta hennes.
- Jeg går en etasje opp.
- Andre sverget til å henge ut av vinduet, å være i nærheten av, men ikke røre metallgjenstander, eller å ligge helt musestille uten å bevege så mye som en muskel.
- Veiv med armene!
- Løp fram og tilbake.
- Beveg armen din rundt omkring.
- Hold hodet i en rar vinkel.

http://www.mobilen.no/wip4/undersøkelse_avslører_merkeligste_dekningstriksene/d.epl?id=12371



Mobiltelefon

1. Mobil – historie og statistikk
2. Cellenettverk
3. GSM-nettet
4. Digital representasjon av lyd og koding
5. GSM ++: HSCD, GPRS, EDGE, EGPRS
6. **Stråling**
7. Avlytting
8. Posisjonering
9. GSM-R
10. 3G: UMTS



Utsendt effekt

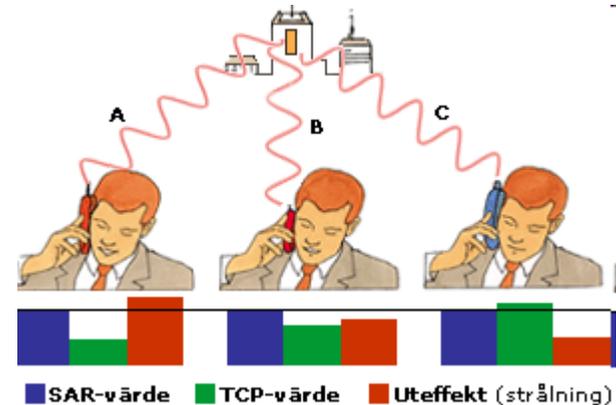
- Klasse I 20W (Fastmontert og testutstyr)
 - Klasse II 8W (Portabel, Fastmontert)
 - Klasse III 5W (Portabel)
 - Klasse IV 2W (Håndholdt)
 - Klasse V **0.8W (Håndholdt)**
- Effektkontroll - **15 trinn a 2dB:**
 - 20, 13, 8, 5, 3 W
 - 2, 1.3, **0.8, 0.5, 0.3, 0.2, 0.13, 0.08, 0.05, 0.03, 0.02 W**
 - Telefonen regulerer seg så lavt den kan hele tiden, avhengig av avstand til basestasjonen og hindringer
 - forstyrrer andre minst mulig
 - sparer batteri
 - bedrer sikkerhet mhp stråling





Sikkerhet

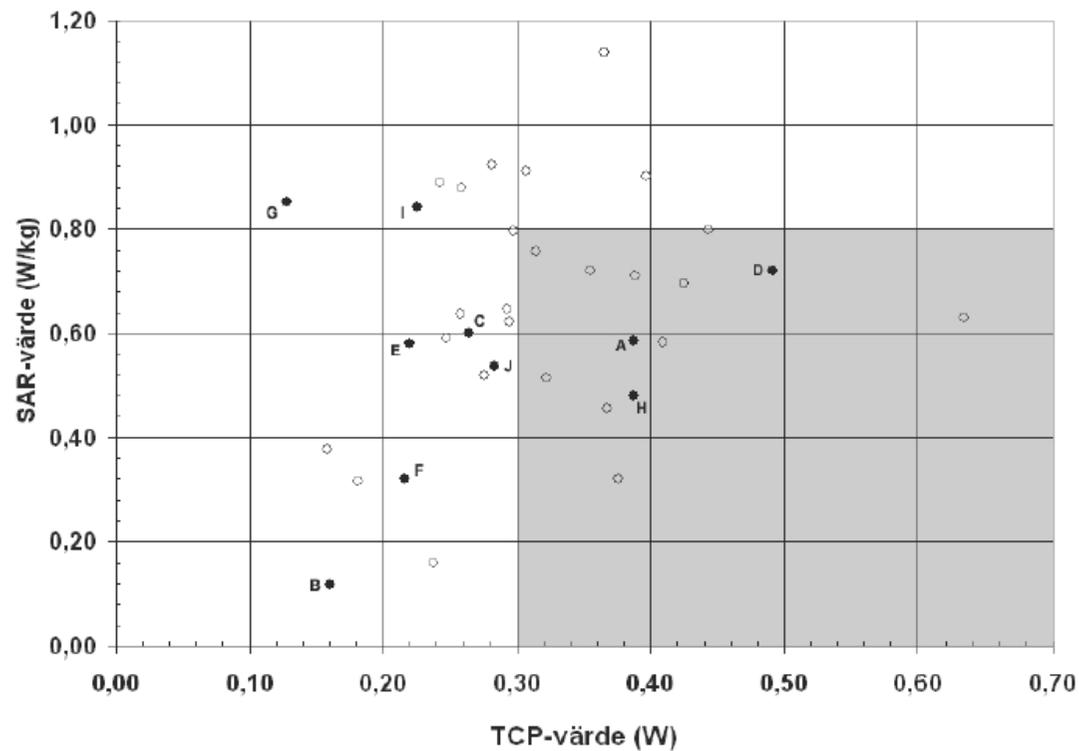
- TCO'01 Mobile Phones: Krav til merking
 - Tjånstemännens Centralorganisation
 - Utstråling, ergonomi, økologi
 - SAR (Specific Absorption Rate): Energi som opptas i hodet ved max effekt (TCO < 0,80 W/kg, EU < 2,0 W/kg)
 - TCP (Telephone Communication Power) bare TCO som har denne (> 0,30 W) – hvor lavt ned regulerer telefonen seg ved en samtale
 - » Hvor mye av telefonens effekt som brukes for kommunikasjon i motsetning til det som stråles inn i brukerens hode.
 - Liten SAR, stor TCP er bra



<http://www.tcodevelopment.com/>



TCO-målinger 2004



Åtte av ti mobiler strøk på test (nov 2007)



Rekommenderade mobiltelefoner (TCO)

November 2007-11-29

- Sony Ericsson S500i
- Sony Ericsson W580

December 2006

- Nokia N93
- Nokia 6233
- Qtek 9000
- Sony Ericsson P990i
- Sony Ericsson W850i

Juni 2006

- Nokia 6103
- Nokia E60
- Qtek 8500
- Samsung SGH-E360
- Sony Ericsson Z300i



Er mobiltelefoner farlige?

- Ikke vist klart og entydig
- Førre-var prinsipp
- Termiske og ikke-termiske effekter
 - Hjernesvulst?
 - Kreft i hørselsnerven?
 - Menn, som har mobilen i bukselomma eller hengende i beltet, risikerer at sædkvaliteten reduseres med ~30% ([juni 2004](#))



Mobiltelefon

1. Mobil – historie og statistikk
2. Cellenettverk
3. GSM-nettet
4. Digital representasjon av lyd og koding
5. GSM ++: HSCD, GPRS, EDGE, EGPRS
6. Stråling
7. **Avlytting**
8. Posisjonering
9. GSM-R
10. 3G: UMTS



Kryptering og sikkerhet

Kryptering brukes for

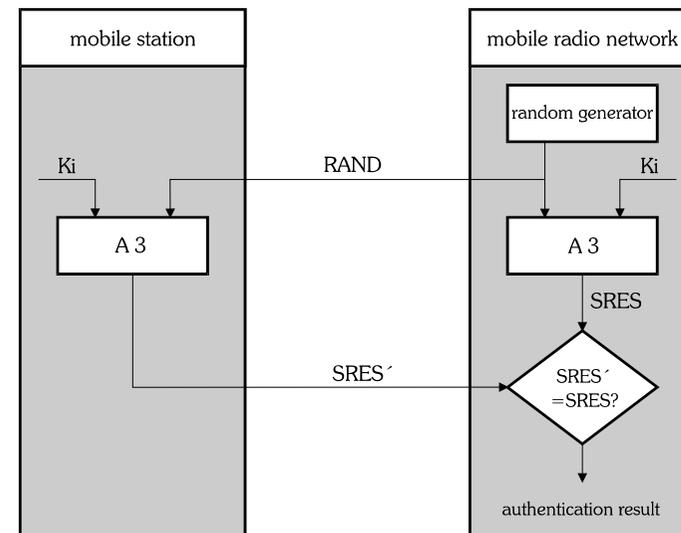
1. Autentisering = å verifisere identiteten til en avsender som forsøker å kommunisere
2. Generering av nøkler for kryptering
3. Kryptering = sikring av informasjon mot innsyn eller modifikasjon

<http://www.gsm-security.net/>



Autentisering – A3

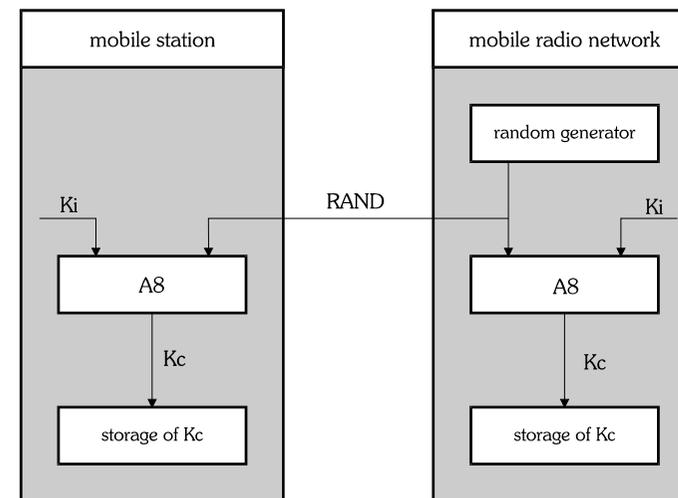
- Autentisering = å verifisere identiteten til en avsender som forsøker å kommunisere
- Algoritme A3 ligger i SIM-kortet (Subscriber Identity Module)
 - Inn:
 - » 128-bit data fra Home Location Register (HLR)
 - » 128-bit Individual Subscriber Authentication Key (Ki) fra SIM-kortet
 - Ut: 32-bit Signed Response (SRES)
- Ofte at den droppes





Generering av nøkkel – A8

- Nøkkel genereres som inngang til kryptoalgoritmen A5
- A8 skal generere 64-bits sesjonsnøkkel (Kc) fra
 - 128-bit random challenge (RAND) fra Mobile Services Switching Center (MSC)
 - 128-bit Individual Subscriber Authentication Key (Ki) fra SIM-kortet eller fra Home Location Register (HLR).
- En sesjonsnøkkel brukes så lenge MSC vil. Det kan ta dager før den skiftes ut.
- A8 genererer Kc bestående av 54 bit, 10 nuller legges til før 64 bit sendes til A5 algoritmen.
- A8 algoritmen er implementert i SIM-kortet.





Kryptering – A5

- Kryptering = sikring av informasjon mot innsyn eller modifikasjon
- Mange versjoner av A5:
 - A5/0 – ingen kryptering
 - A5/1 – Den originale, sterk talekryptering, Europa, USA (64 bit nøkkel, 10 brukes ikke)
 - A5/2 – svak talekryptering for land som er underlagt eksportbegrensninger (16 bit), 2006: Brukes ikke lenger.
 - A5/3 – ny kryptering utviklet for utvidet sikkerhet



Kryptering og sikkerhet i GSM

- A3 (autentisering) og A8 (nøkkel) – publ. i april 1998
- A5/2 (svak) - publisert i august 1998
 - Det er vist at bare noen få millisekunder med data – avlest over lufta – er nok til å dekode denne algoritmen
- A5/1 (sterk) - publisert i mai 1999
 - hevdes at utgang ikke er helt tilfeldig, men har små innslag av struktur (64 = 54 + 10 nuller => 41 bit effektivt?)
 - A5/1 nøkkel ble funnet på < 1 sek med:
 - » PC med 128 MB RAM og 150 Gbyte harddisk
 - » basert på to min kryptert tale
 - Nå går det på mindre mye data (<< 1 sek)
- A8 nøkkelen kan dekodes fra data som går over radiosambandet (2002)



Svakheter ved GSM krypto

- "Security by obscurity"
- Vanskelig å oppgradere (må bytte SIM-kort)
- Bruker vet ikke om kryptering er på eller av
- Ikke helt gode algoritmer
 - 64-bits nøkkel er bare 54-bits, burde ha vært enda lenger (256)
 - Security researcher Ross Anderson, 1994 "*there was a terrific row between the NATO signals agencies in the mid 1980's over whether GSM encryption should be strong or not. The Germans said it should be, as they shared a long border with the Warsaw Pact; but the other countries didn't feel this way, and the algorithm as now fielded is a French design.*" (<http://en.wikipedia.org/wiki/A5/1>)
- Gjelder bare radiosambandet, ikke over resten av telenettet
- Det er bare mobiltelefonen som blir spurt om å bevise sin ID, nettverket må ikke autentisieres
 - Enveis autentisering gjør det mulig for en angriper å late som en representerer et GSM nettverk med falske basestasjoner



GSM avlytting

Aktive GSM lyttesystemer, 1. generasjon

- "Mini" basestasjon
- Første utgaver: bare lytte i simplex (dvs kun på den ene parten i samtalen).
- Nye utgaver tar full duplex, bl.a. Rhode & Schwartz

Passive GSM lyttesystemer, den nye generasjonen:

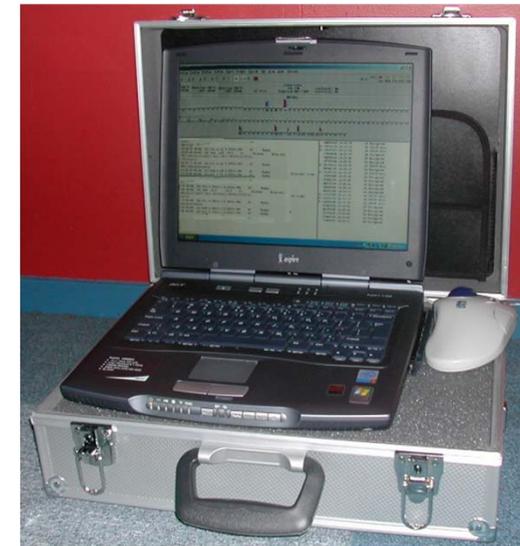
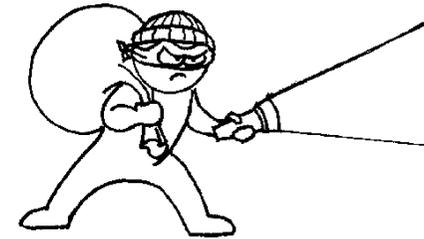
- Totalt "usynlige" for offeret, og nettoperatøren (NetCom/Telenor).
- Må ha telefonnummeret og Ki koden (en hemmelig tallrekke som ligger innbakt i SIM-kortet, + den befinner seg hos nettoperatøren).
- Finnes helt ned til laptop størrelse.
- De nyeste trenger ikke Ki koden, kun telefonnummeret. Disse lytter i duplex.

<http://www.scannernytt.net/phpBB2/viewtopic.php?t=13235&highlight=avlytte>



Sikkerhet

- Tilbys utstyr for 1-2 mill bestående av kraftig PC + GSM radiodel på illegale marked ([Dagens Næringsliv des 2000](#))
- PT mener utstyret blir leid ut til næringslivet for [avlytting av konkurrenter](#). (2002)
- "Mobiltelefoner avlyttes systematisk på Arlanda lufthavn" (mars, 2004)
- Bildet: GSS ProA - GSM Interceptor
 - Fully passive (non-detectable) off air interception of GSM communications
 - Intercepts GSM phones operating on both the 900MHz and also on 1800/1900MHz bands.
 - It intercepts both the base station and the mobile station at the same time, independently.
 - Interception of A5.1, A5.2, A5.3 Encrypted Voice Channels
 - Extraction of Ki code (Ki-Grab) off air from a distance of 4 miles! NEW Feature!
 - *** The GSS-ProA Passive Intercept system is strictly limited to Government authorities and their authorized suppliers. The sale of this product is secured via end-user certificate!
 - <http://www.global-security-solutions.com/ProA-GSMInterceptandTracking.htm>





Jammere

- Kjøpes på internett, eks \$166
- 10-meters radius.
- På toget, i møtelokaler, kaféiere, frisører, hoteller, teatre, bussjåførere, ...
- Fare for liv (112-anrop?)
- Ulovlig – Post og Teletilsynet har bare gitt Telenor, Netcom og Network Norway konsesjon til å sende på disse frekvensene
- Lovforslag på høring: Politiet, Forsvaret, påtalemyndigheten og kriminalomsorgen kan få lov til å bruke dette utstyret.
- Lovlig alternativ: Skjermede vegger
 - Eks: et trelaminat, hvor det er partikler av nikkelsink-ferrit mellom to trepaneler





Usynlig GSM-program for avlytting

- GSM spionprogram som fjernstyres via SMS
- Virus-lignende program som må installeres på en telefon
- Avlytter rom via telefonens mikrofon selv om telefonen er av
 - Av-knapp er bare en softwarefunksjon så den kan overstyres fra programmet
 - En telefon er ikke virkelig avskrudd før batteriet er ute
 - Telefonen starter avlytting ved oppringing fra et forhåndsdefinert nummer – uten at bruker merker det
 - Ved oppringing fra andre numre får man bare standard beskjed om at abonnenten ikke er tilgjengelig
- Kan og rapportere om alle inn- og utgående SMS og samtaler, og rapportere telefonens posisjonshistorie (nøyaktighet: celle ID)
- http://www.endoacustica.com/details_gsm-interceptor_en.htm
- *LAW ENFORCEMENT ONLY



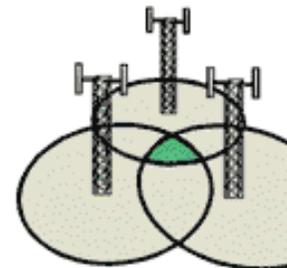
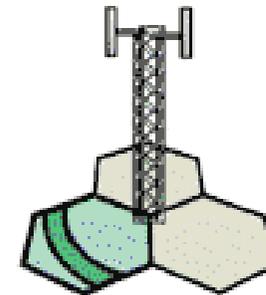
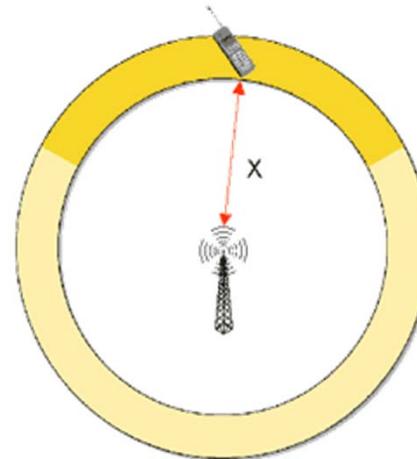
Mobiltelefon

1. Mobil – historie og statistikk
2. Cellenettverk
3. GSM-nettet
4. Digital representasjon av lyd og koding
5. GSM ++: HSCD, GPRS, EDGE, EGPRS
6. Stråling
7. Avlytting
8. Posisjonering
9. GSM-R
10. 3G: UMTS



Posisjonering

- Vet alltid hvilken celle
- For å få til tidsdivisjonsmultiplex må alle telefoner mottas på rett tid
- Timing advance – kompensasjon for forsinkelse i celler opp til 35 km radius = 64 trinn:
 - $1 \text{ bit} \Leftrightarrow 3.63 \text{ us} \Leftrightarrow 3.63 \text{ us} * 3e8 / 2 = 545 \text{ m}$
- Vet hvor langt vekk du er med $\sim 0.5 \text{ km}$ nøyaktighet
- Forbedringer
 - Direktive antenner
 - Flere basestasjoner





GPS – Global Positioning System

- I dag kommer GPS i telefonene for fullt så posisjonering i nettverk utover celle og time-of-arrival er ikke så aktuelt lenger





Mobiltelefon

1. Mobil – historie og statistikk
2. Cellenettverk
3. GSM-nettet
4. Digital representasjon av lyd og koding
5. GSM ++: HSCD, GPRS, EDGE, EGPRS
6. Stråling
7. Avlytting
8. Posisjonering
9. **GSM-R**
10. 3G: UMTS



Åsta-ulykken

- 4. januar 2000
- Fantes ikke ATC (Aut. Train Control) eller togradio.
- Bare mobiltelefon
- Numrene til lokomotivførerne og konduktørene var blitt oppført på feil lister
- Toglederen på Hamar visste hvor han skulle ringe





Hvorfor er ikke GSM godt nok for NSB og nødetatene?

- GSM-R: GSM-rail
 - Gruppeanrop, kringkasting
 - **Hurtigkall** med push-to-talk
- TETRA = TERrestrial TRunked RADio
 - for politi, brann, osv
 - Både **en-til-en** og gruppekommunikasjon
 - Fokus på sikkerhet og robusthet.



GSM-R Rail

- GSM m/GPRS + togfunksjoner
- Enhetlig system over grenser
- Togkommunikasjon:
 - » Gruppeanrop, kringkasting
 - » Hurtigkall med push-to-talk
- Togkontroll: ATC (Aut. Train Control), fjernkontroll
- Tog-signalering
- Standardisert 1993-97



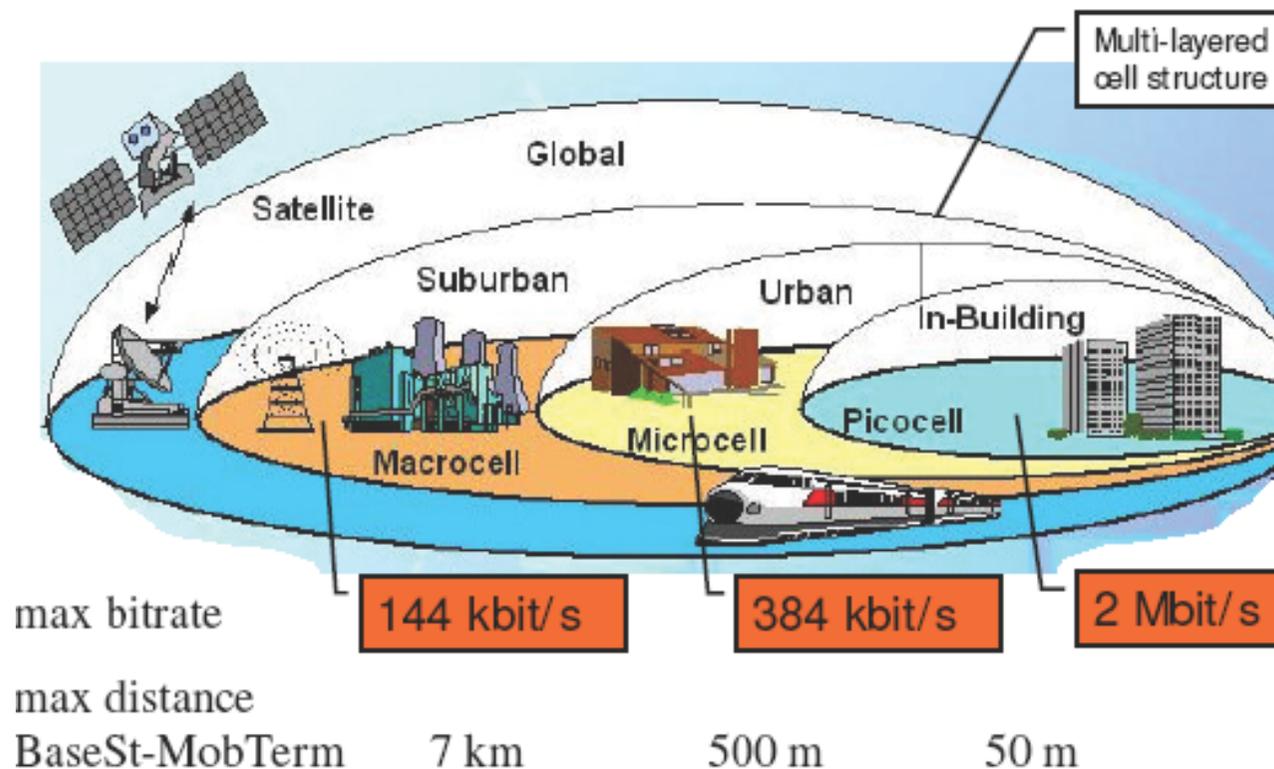
Mobiltelefon

1. Mobil – historie og statistikk
2. Cellenettverk
3. GSM-nettet
4. Digital representasjon av lyd og koding
5. GSM ++: HSCD, GPRS, EDGE, EGPRS
6. Stråling
7. Avlytting
8. Posisjonering
9. GSM-R
10. 3G: UMTS



UMTS – Universal Mobile Telecomm System

- Data blir viktigere enn tale





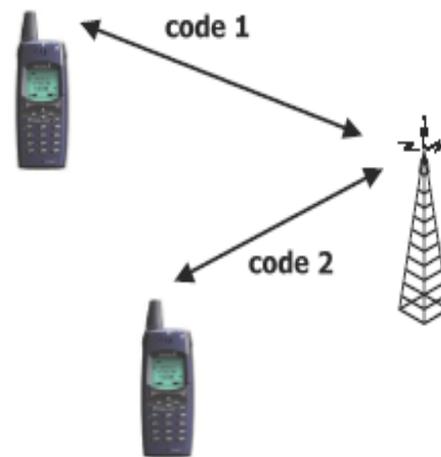
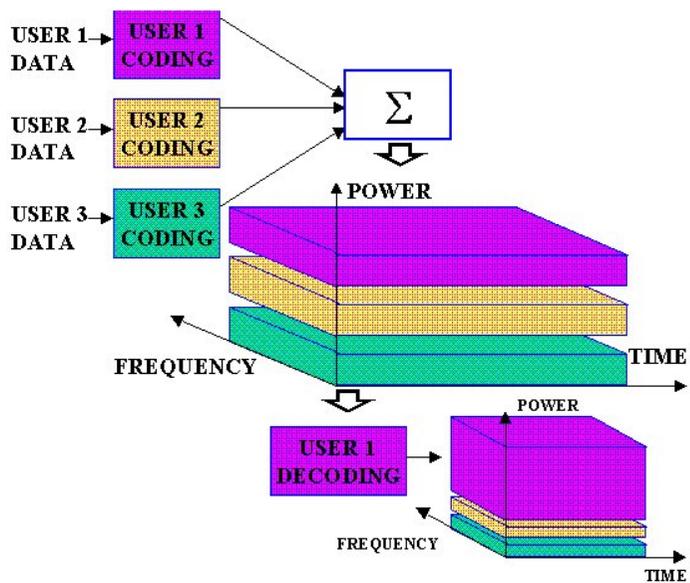
3G i Norge: på vei mot internetthastighet

- Telenor:
 - UMTS:
 - » >80% av Norges befolkning,
 - » alle steder med >200 innbyggere
 - » 12,8% av landarealet.
 - HSDPA High Speed Downlink Packet Access
 - » 3,6 Mbit/s, normalt 0,5-1,5 Mbit/s.
 - » Er i de største byene, bygges stadig ut
- Netcom:
 - UMTS:
 - » 77% av befolkningen
 - HSDPA
 - » opp til 3,6 Mbit/s
 - » Nå i Oslo, i løpet av 2008 hele landet



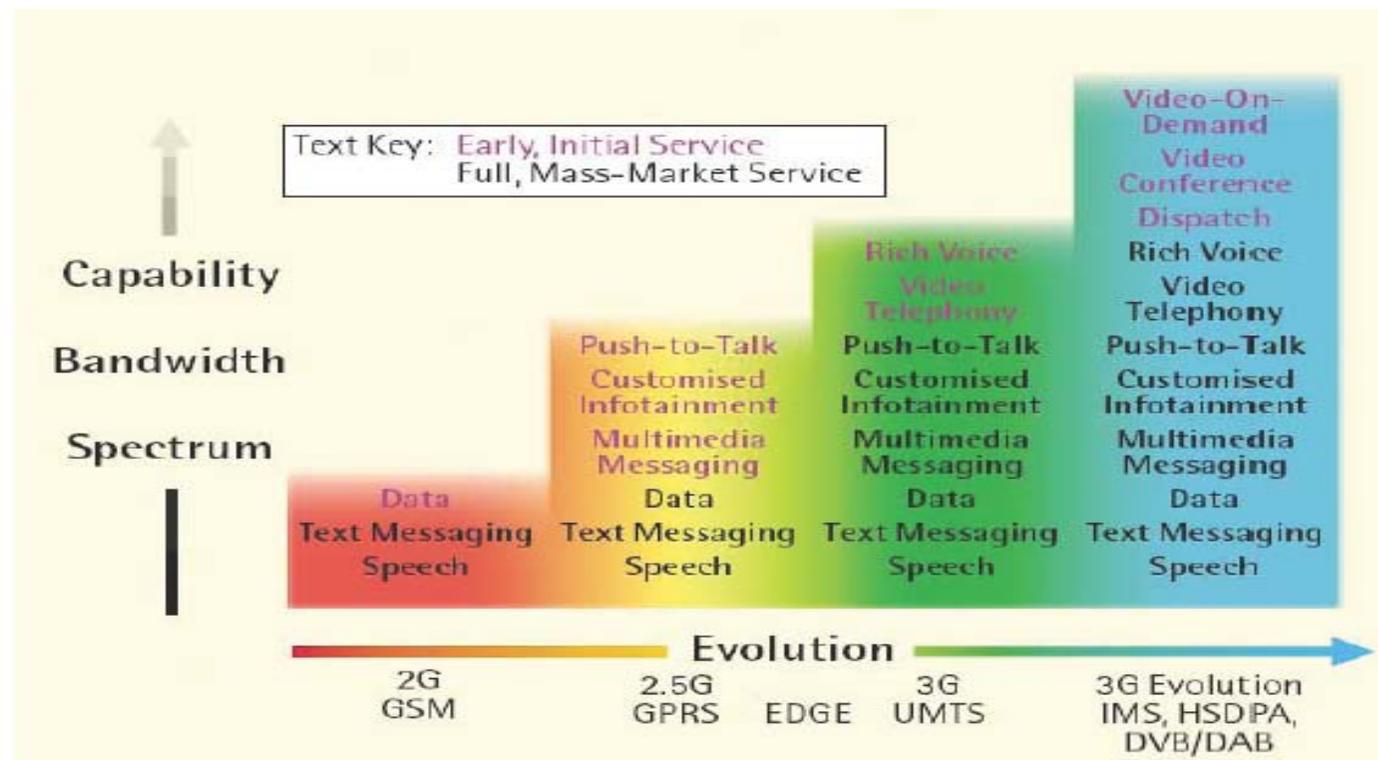


CDMA koding





Utvikling av tjenester

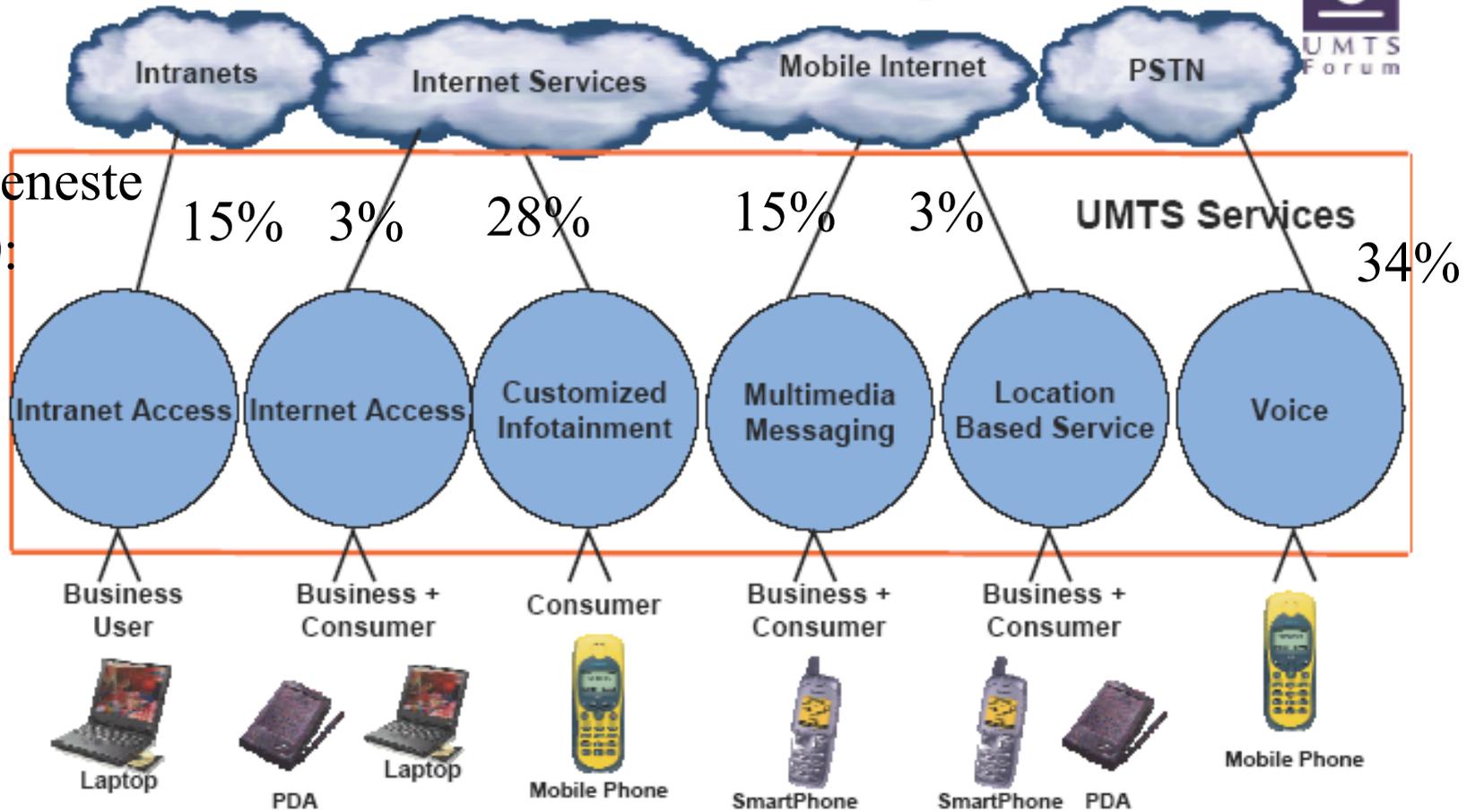




UMTS Service Categories

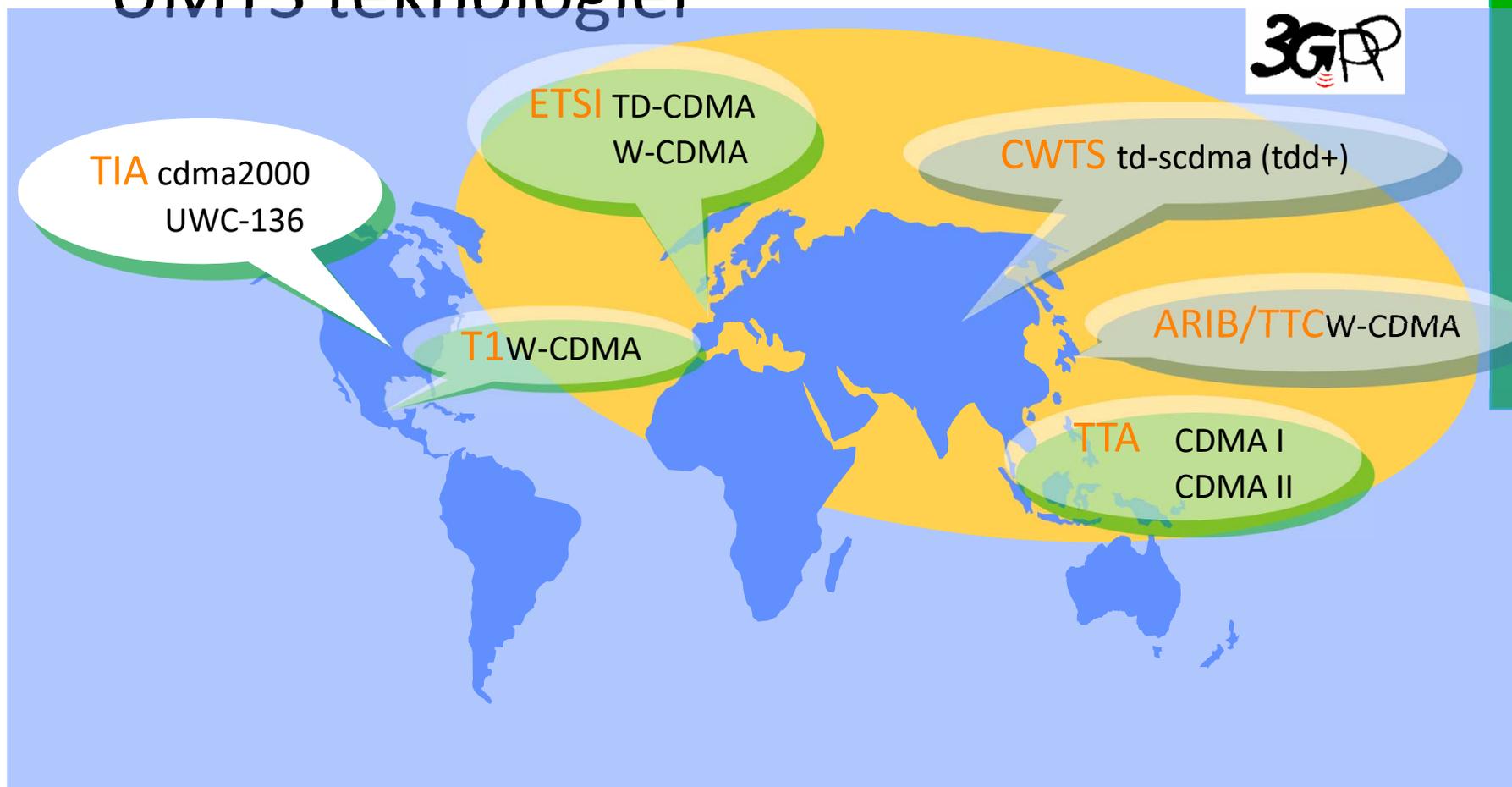


Fortjeneste
2010:



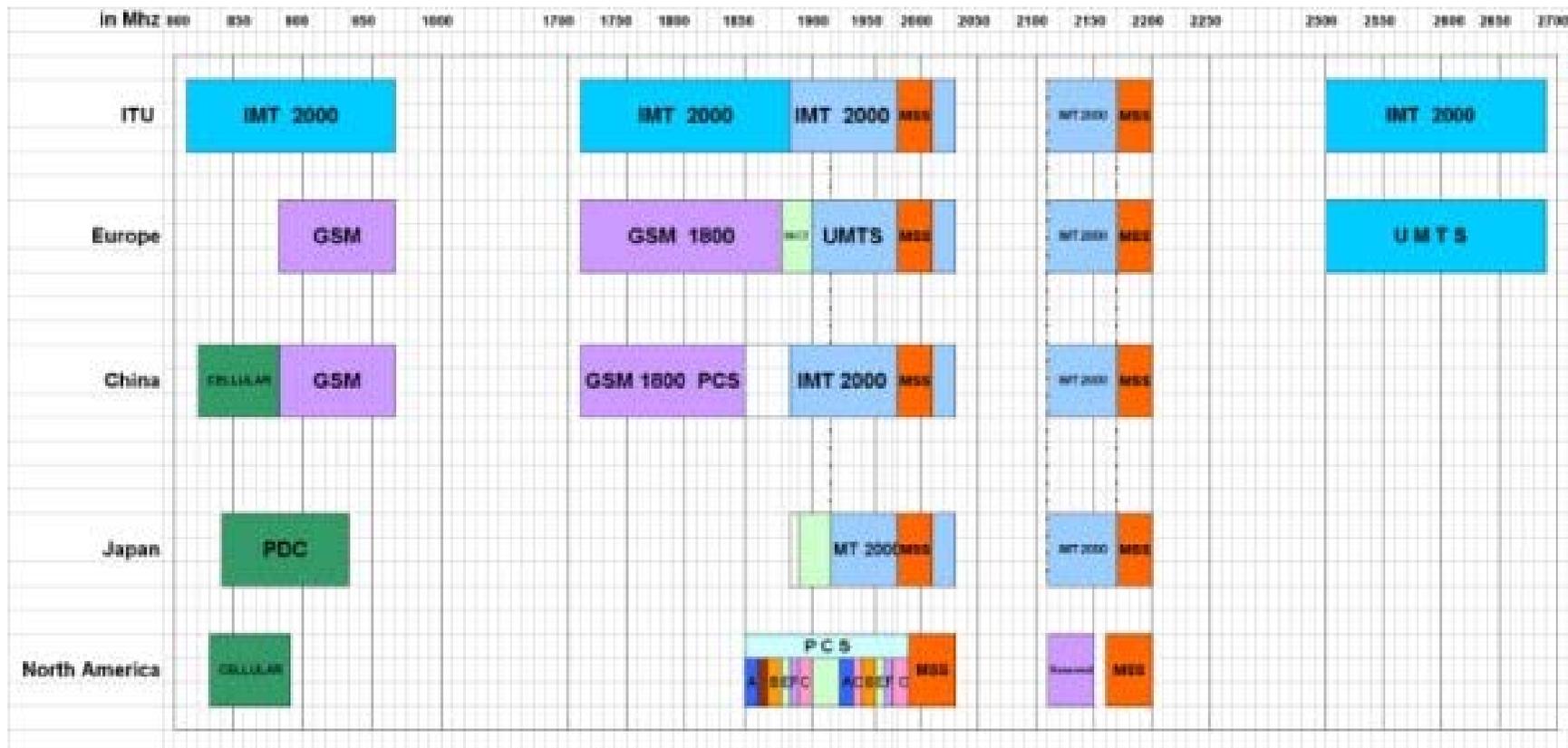


UMTS teknologier





UMTS - Universal Mobile Telecommunications Service





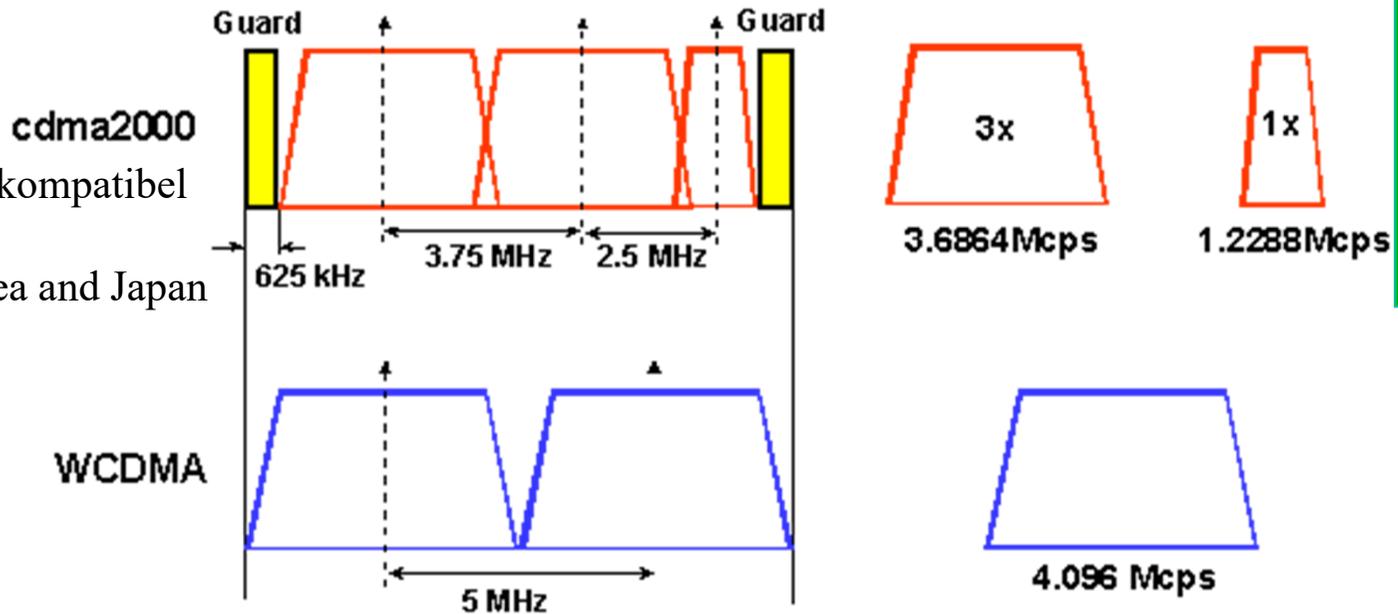
UMTS teknologier IMT-2000 (International Mobile Telephony)

- **W-CDMA – Wideband CDMA (UTRA FDD) – Bredbånd (5MHz) CDMA med symmetrisk sende og mottakerkanal**
- **TD-CDMA – Time Division CDMA (UTRA TDD) – Bredbånd (5MHz) CDMA med 16 tidsdiskrete kanaler, asymmetrisk**
- **CDMA2000 – Basert på multicarrier modus som definert i IS-95 (Amerikansk 2G standard) med 1,25MHz kanaler – 3 kanaler gir 3,6864Mcps**
- **UWC-136 – EDGE (TDMA) i 1900MHz båndet**
- **TD-SCDMA – TD-CDMA spesifisert for Kina med lavere "chip rate" (1,28Mcps)**
- **CDMA I – Synkron W-CDMA (Korea)**
- **CDMA II – Asynkron W-CDMA (Korea)**



CDMA - mange kanaler deler bånd

cdma2000: nedover kompatibel
med cdmaOne
North America, Korea and Japan

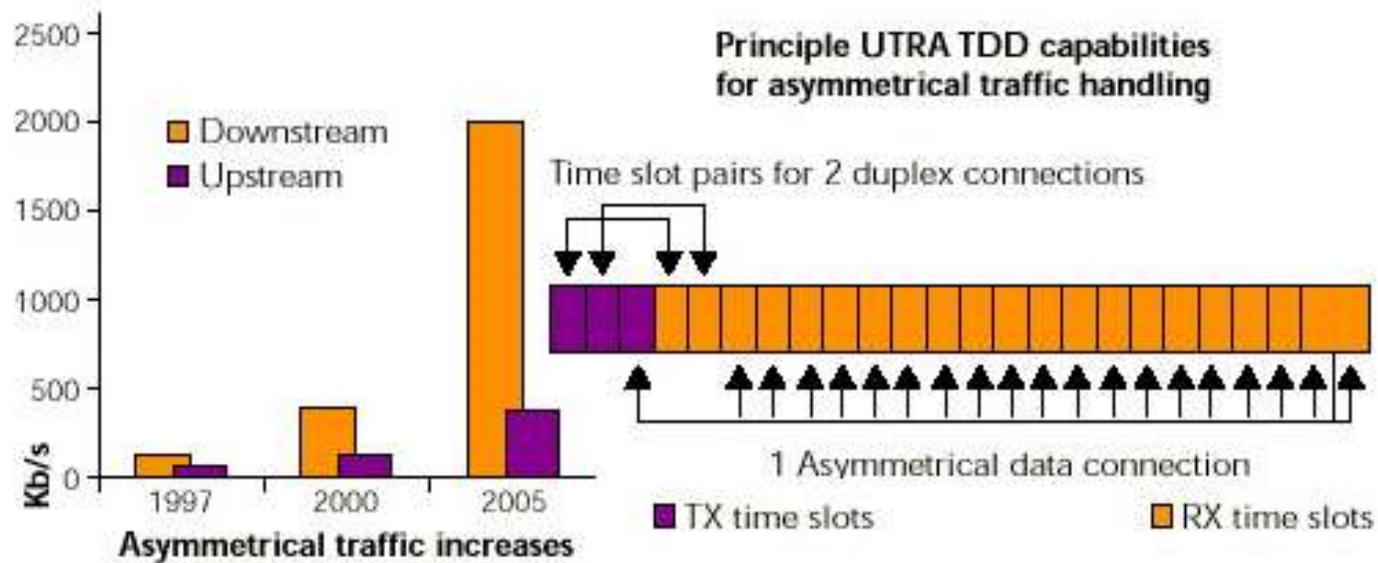


W-CDMA is mainly used in Europe
kalles og FDD-CDMA (Frequency Division Duplex)
(Other variations are cdma2000 and TD-CDMA.)

Antall chips/symbol varierer
med SNR



UMTS - Time Division Duplex



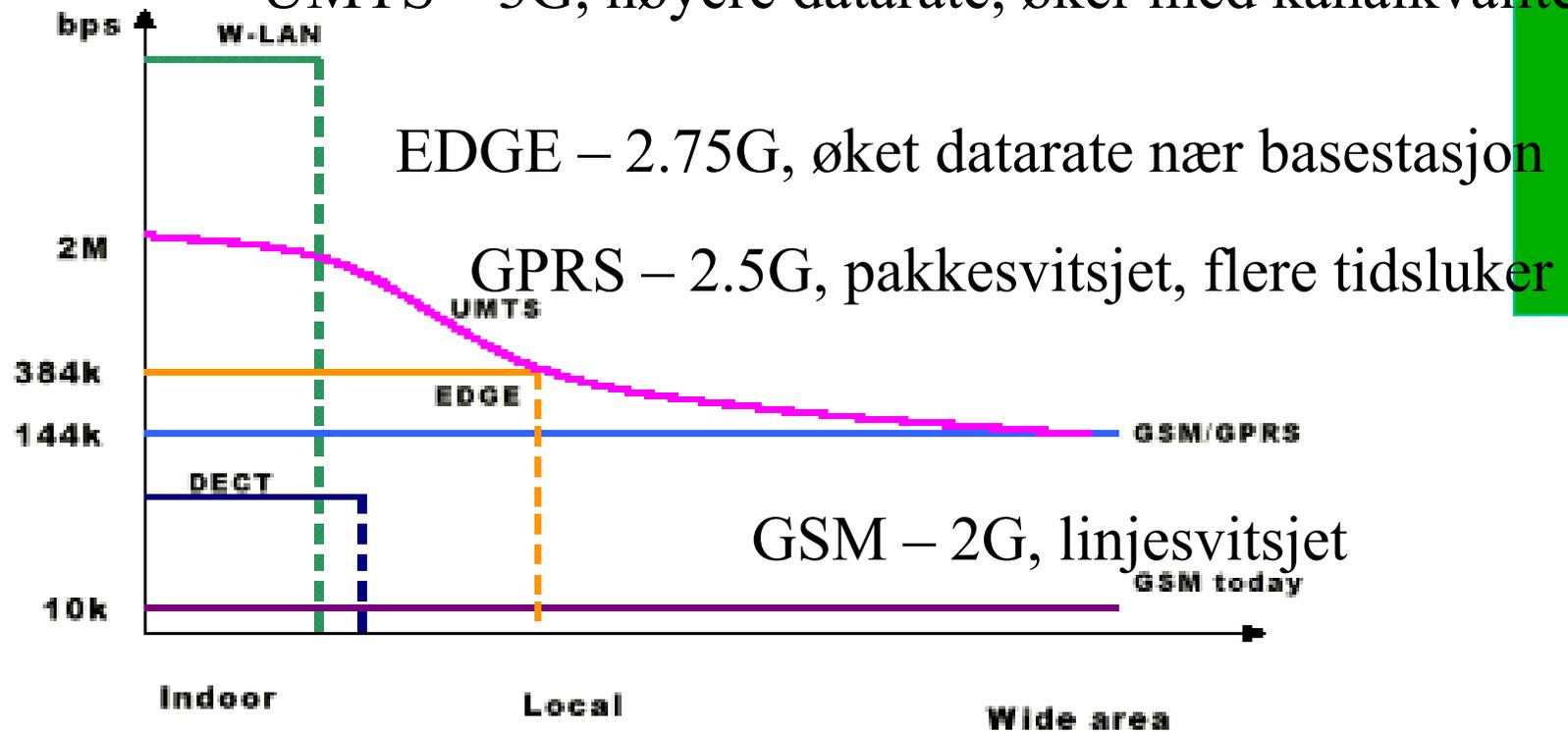
- TDD mode (using TD-CDMA)
 - For asymmetrical and symm. data rates up to 2 Mbps
 - In public micro and pico cell environment
 - For unlicensed cordless and public wireless local loop
- FDD mode (using W-CDMA)
 - In public macro and micro cell environment
 - For data rates up to 384 kbps/2 Mbps
- Multimode terminals: GSM and UMTS (FDD and TDD)



Kapasitet - avstand

WLAN – flere basestasjoner enn UMTS, 100:1

UMTS – 3G, høyere datarate, øker med kanalkvalitet





Forskjell mellom mobiltelefon og Walkie-Talkie?



- "PTT"-knapp og "over": Duplex – simplex
- Infrastruktur: Én til mange – én til noen få
- Alltid dekning – bare dekning hvis nær hverandre
 - celler



Alt var bedre før?

