

EFREI M1

Mobile Networks

GSM Networks

Paul Simmons

Tamum Consulting February 2013

GSM Networks-1

- The GSM radio interface:
 - Radio interface basics
 - Structure of the GSM radio interface

GSM Networks-2

- GSM Architecture
 - Call routing
 - Location Updating and Cell Selection
 - Dedicated Channel Assignment
 - GSM Protocol Structure

GSM Networks-3

- GSM Features
 - Handover
 - Power Control
 - Security
 - Call Establishment
 - Short messages
 - Data Services
 - Voice Services
 - GSM for PMR
- Advanced GSM Features
- GSM Issues

EP 4.5 Handover

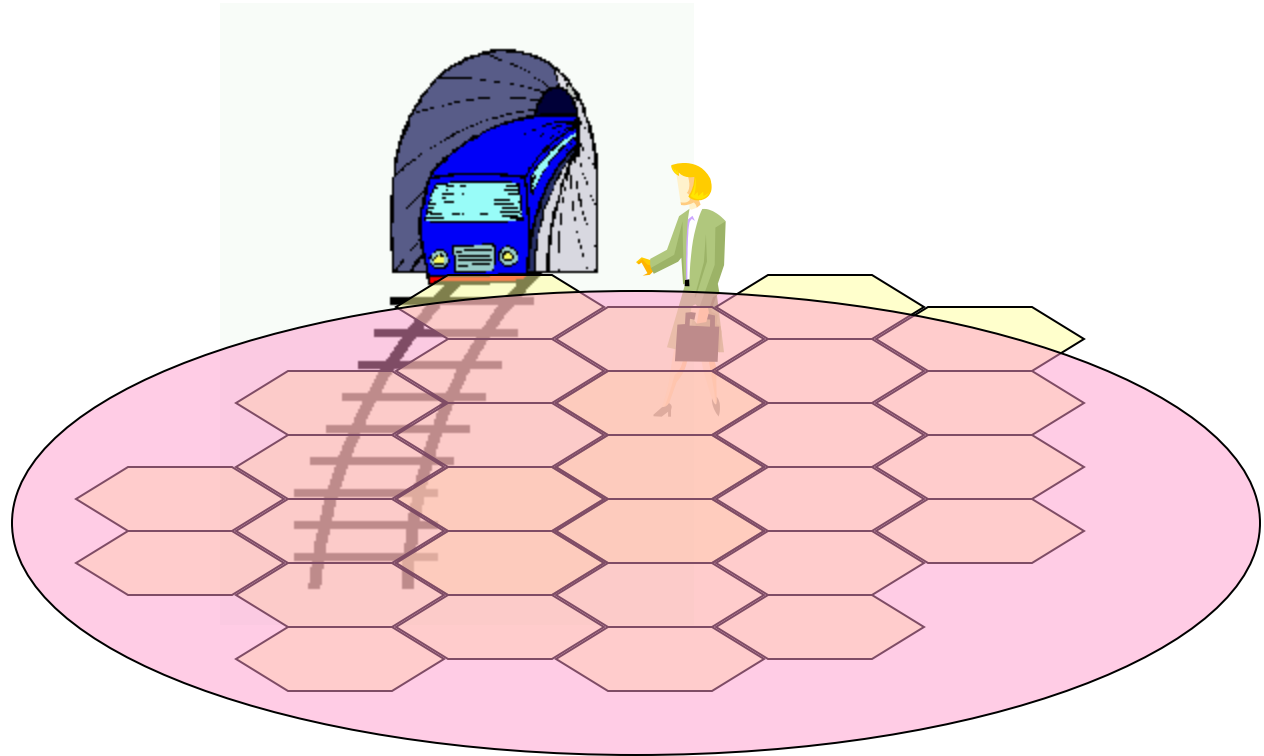
- Problem:
 - Mobile station may change cell during a call
 - This occurs when cell conditions are relatively poor
 - How to successfully change the cell transparently to the user?

Handover reasons

- “Rescue handovers” when the call will be lost if the cell is not changed
- “Confinement handovers” when there is a better cell and interference can be reduced
- “Traffic handovers” to manage load between cells



Microcells, umbrella cells



In cities, dense populations of pedestrians require many small *microcells*. However, some users are better served by larger *umbrella cells*

Information needed to control the handover process

At the MS

- Downlink RXLEV from serving cell
 - the BCCH carriers are measured and averaged over a SACCH block (480 msec)
 - The 6 strongest received RXLEV for surrounding BSs are transmitted to the serving BS.
- Downlink RXQUAL from serving cell (from channel error rate).
- Downlink RXLEV from surrounding cells (BCCH carriers do not use DTX or Power Ctrl.)
- BSIC from surrounding cells (in order to determine which BS is being measured)

• At the BS

- Uplink RXLEV from each MS served by the cell
- Uplink RXQUAL from each MS served by the cell
- Received signal strength on unused timeslots (= interference measurements).

• Using the above information, plus:

- power budget consideration
- threshold comparisons with presettable values (through Network Management)

the BSS (BSC) determines when and what kind of handover is recommended



RxQual and RXLEV, Key measurements for handover

- RXQual

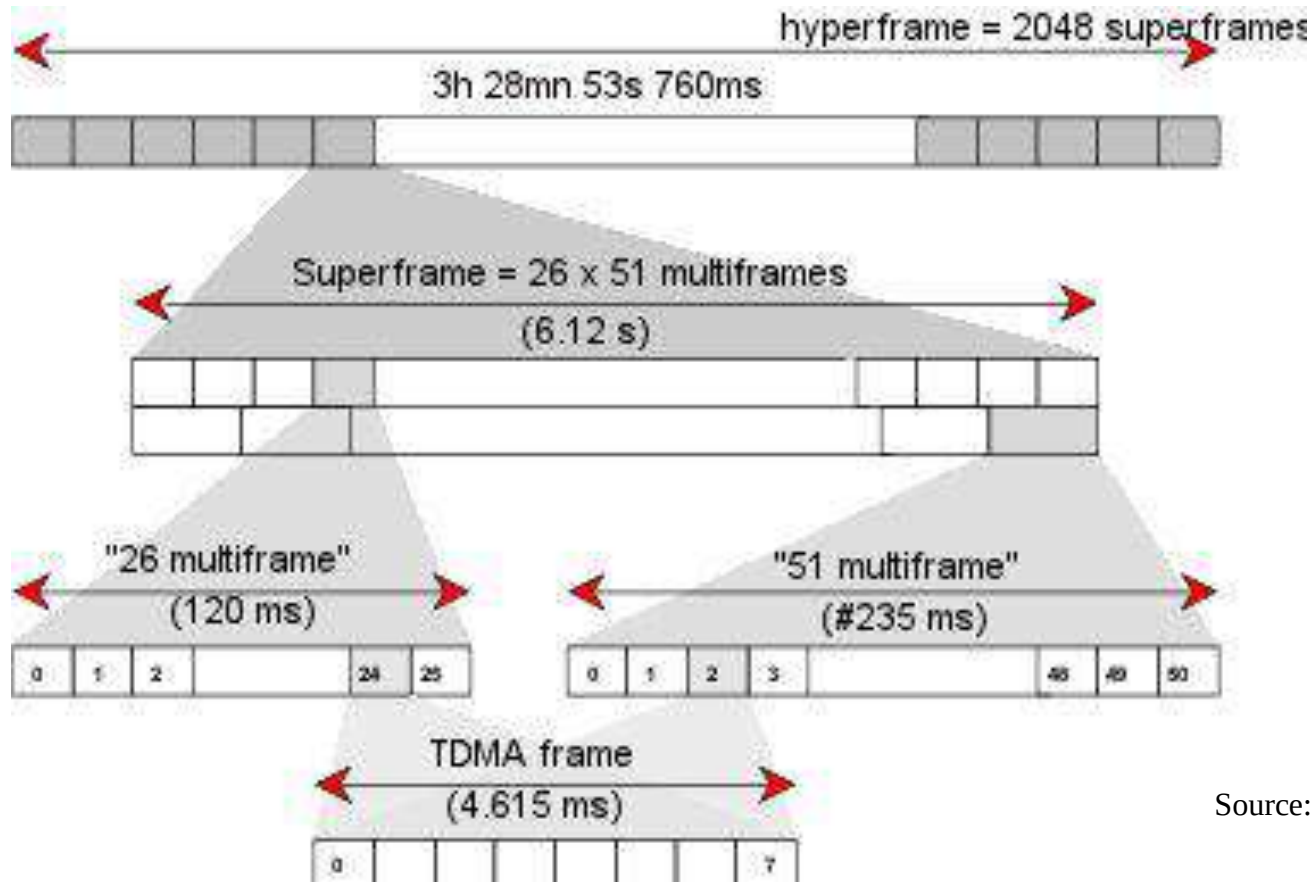
- RXQUAL_0 BER < 0,2 % Assumed value = 0,14 %
- RXQUAL_1 0,2 % < BER < 0,4 % Assumed value = 0,28 %
- ...
- RXQUAL_7 12,8 % < BER Assumed value = 18,10 %

- RXLEV

- RXLEV 0 = less than -110 dBm + SCALE.
- RXLEV 1 = -110 dBm + SCALE to -109 dBm + SCALE.
- ...
- RXLEV 62 = -49 dBm + SCALE to -48 dBm + SCALE.
- RXLEV 63 = greater than -48 dBm + SCALE.

- Note: SCALE is an offset used in enhanced measurement reporting, else 0
- Reference TS 45.008

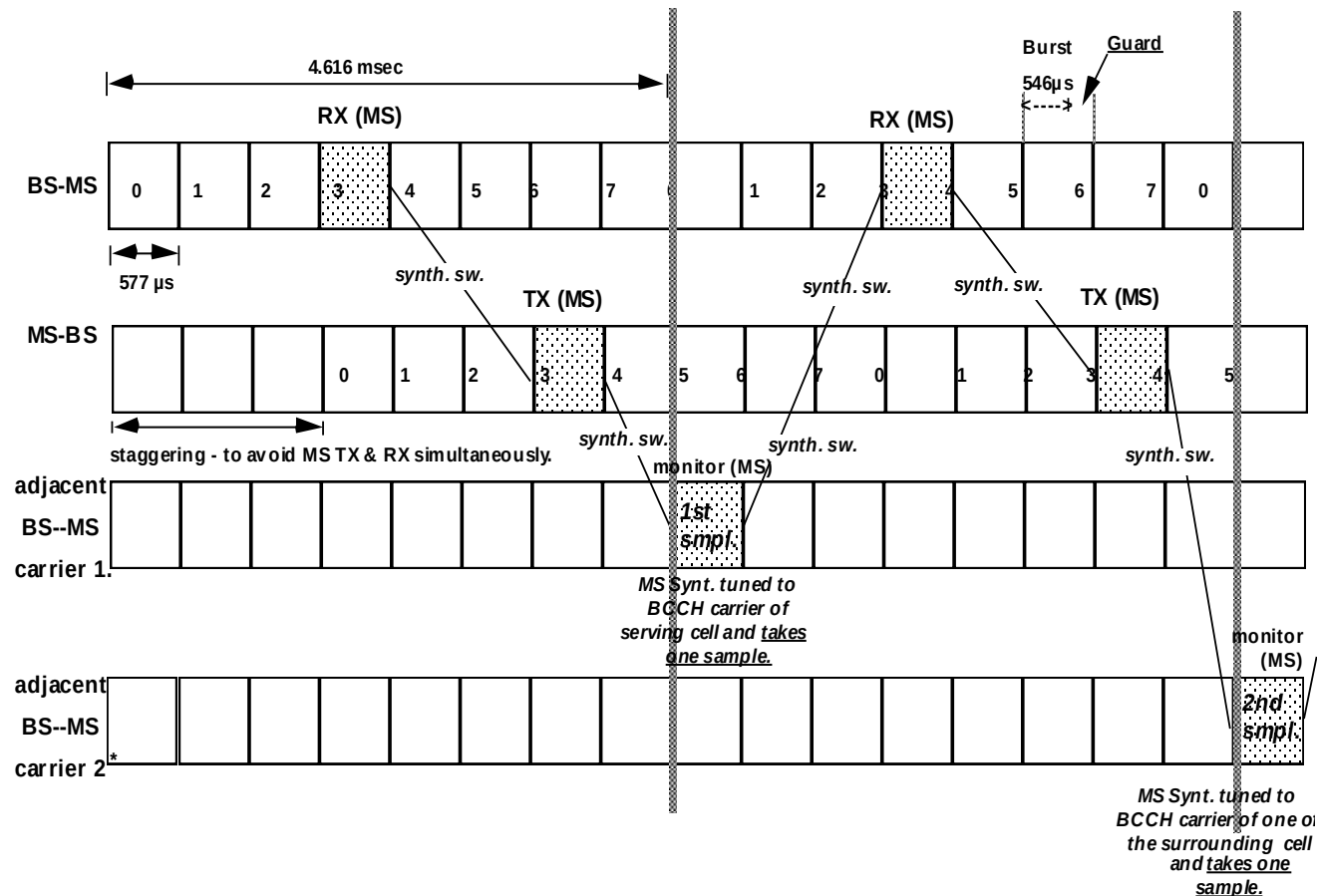
Multiframe structure



Source: Mouly & Pautot



Handover: Measuring Adjacent Cells BCCH Carriers Signal Level.



- In one SACCH block (480ms) there are $480/4.616 = 104 \approx 100$ active frames during which measurement are taken + 4 idle frames (one idle/multiframe = 120 msec) when the rec. syncs and demodulate the BSIC from the SCH.

*The # of samples taken of each BCCH carrier depends on the number of carriers being scanned. (e.g. 8 carriers x 12 samples/ carrier < 100)

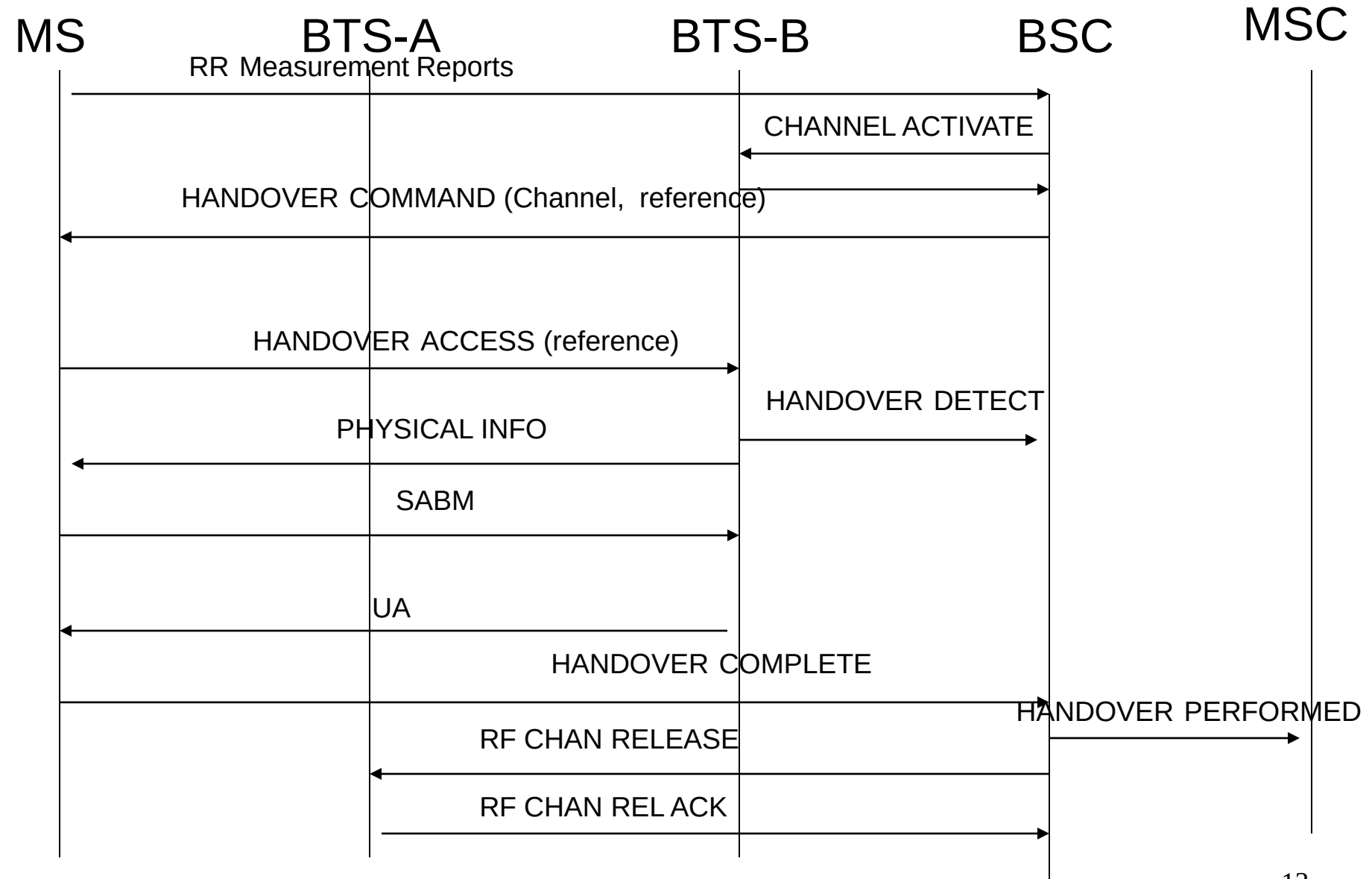
Handover execution

A handover may be:

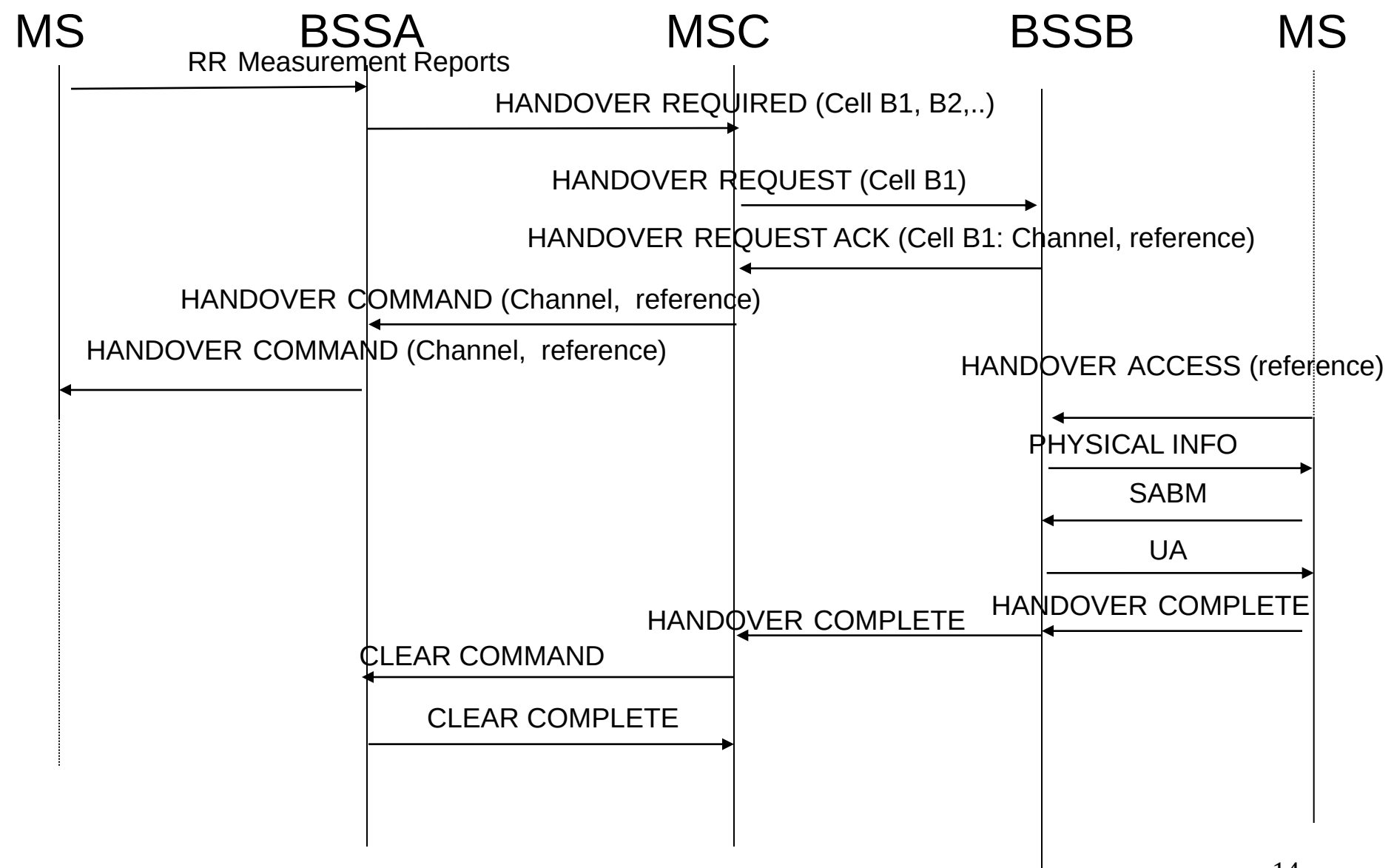
1. intra-cell
 2. inter-cell, intra-BSS
 3. inter-BSS, intra-MS
 4. inter-MS
- In cases 1 & 2 the BSC sends a "HANDOVER COMMAND" to the mobile containing the target cell and channel, and a reference number [44.018]
 - In cases 3 & 4 the BSC sends a "HANDOVER REQUIRED" message sent to the MS including a preferred list of target cells and the cause (Uplink quality, Uplink strength, etc.)
 - The MS then signals to a target BSS, which then formats the HANDOVER COMMAND to be sent to the MS (via the source BSS)



Successful Handover intra-BSC



Successful Handover inter-BSS



EP 4.5 Handover

- Problem:
 - Mobile station may change cell during a call
 - This occurs when cell conditions are relatively poor
 - How to successfully change the cell transparently to the user?
- Solution:
 - Monitor conditions at MS and report to BSC
 - Using MS and network information, BSC decides when and how to handover, if necessary passing via the MSC(s)



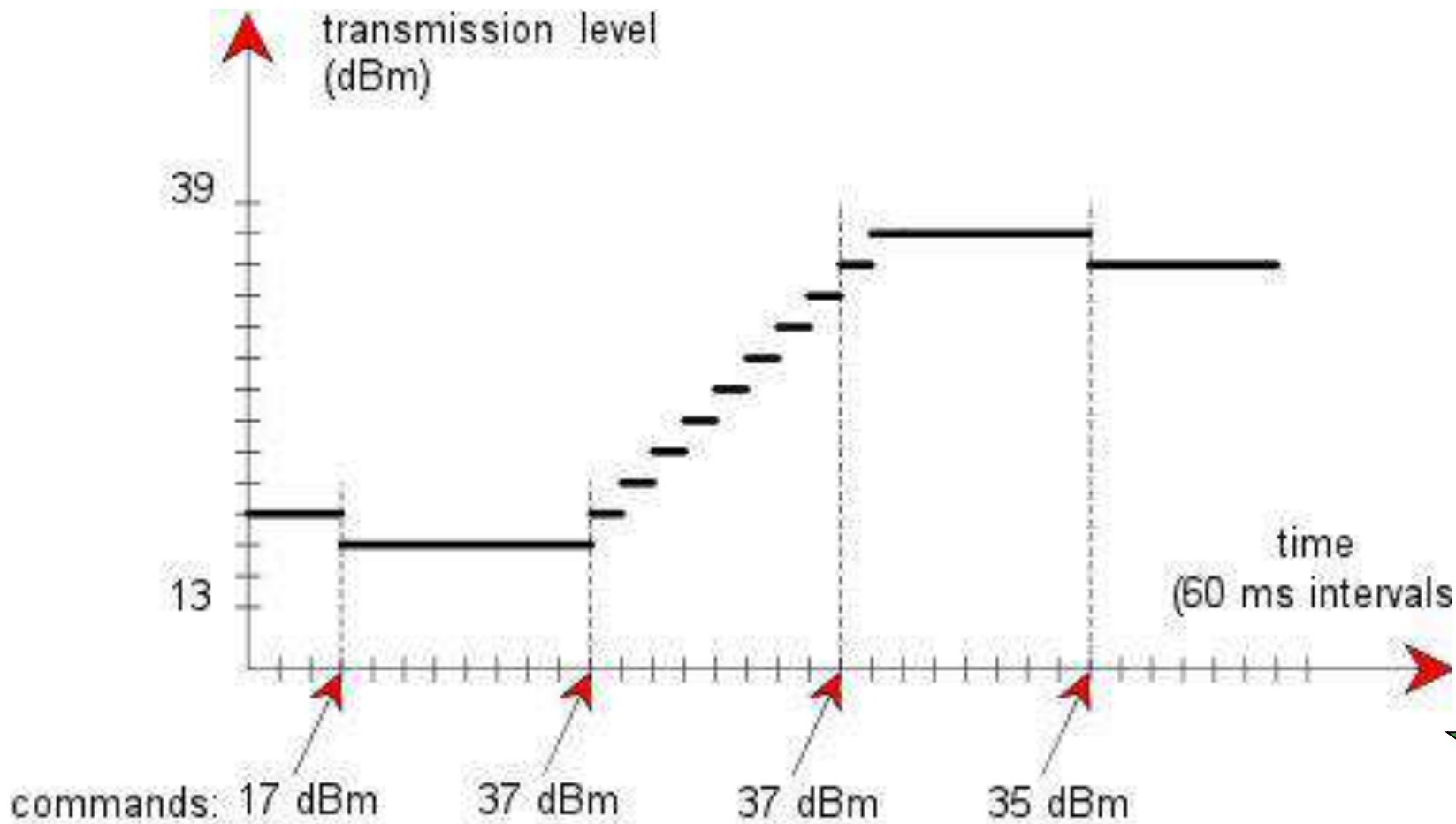
EP 4.6 Power Control

- Problem:
 - How to keep the power levels used in a communication between BTS and MS to the optimum - not too high to raise interference with other mobiles, not too low as to cause too many errors?

Power Control

- As for handover, the mobile reports its conditions to the network, which (BSC or BTS) uses these plus its own information to instruct the mobile and BTS to change power
- Power commands are sent on the SACCH (min 120ms cycle) and provide 60ms steps 

Power Control



EP 4.6 Solution: Power Control

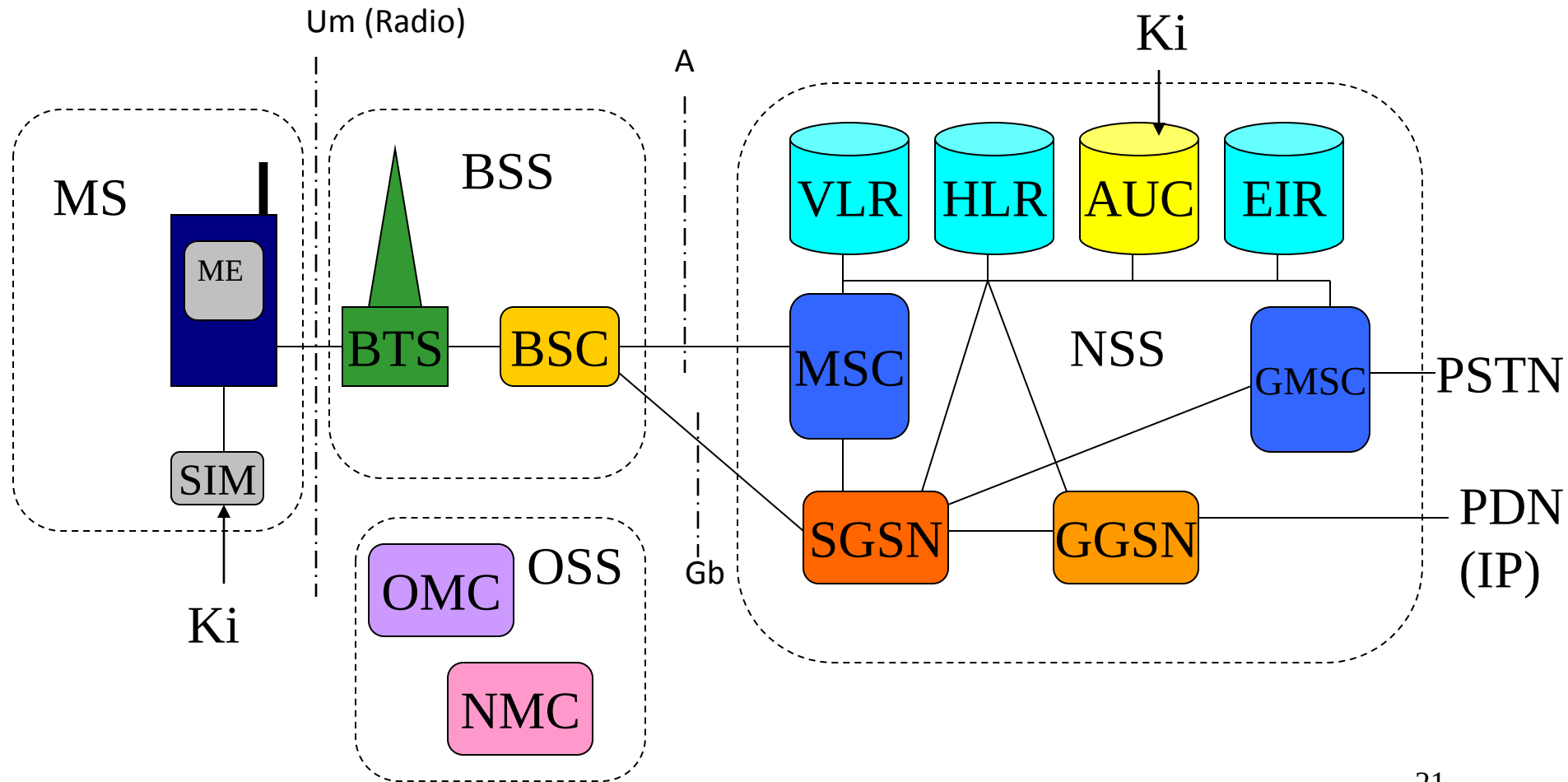
- Problem:
 - How to keep the power levels used in a communication between BTS and MS to the optimum - not too high to raise interference with other mobiles, not too low as to cause too many errors?
- Solution
 - MS and network monitor conditions
 - network instructs MS and BTS to change as required



EP 4.7 Security

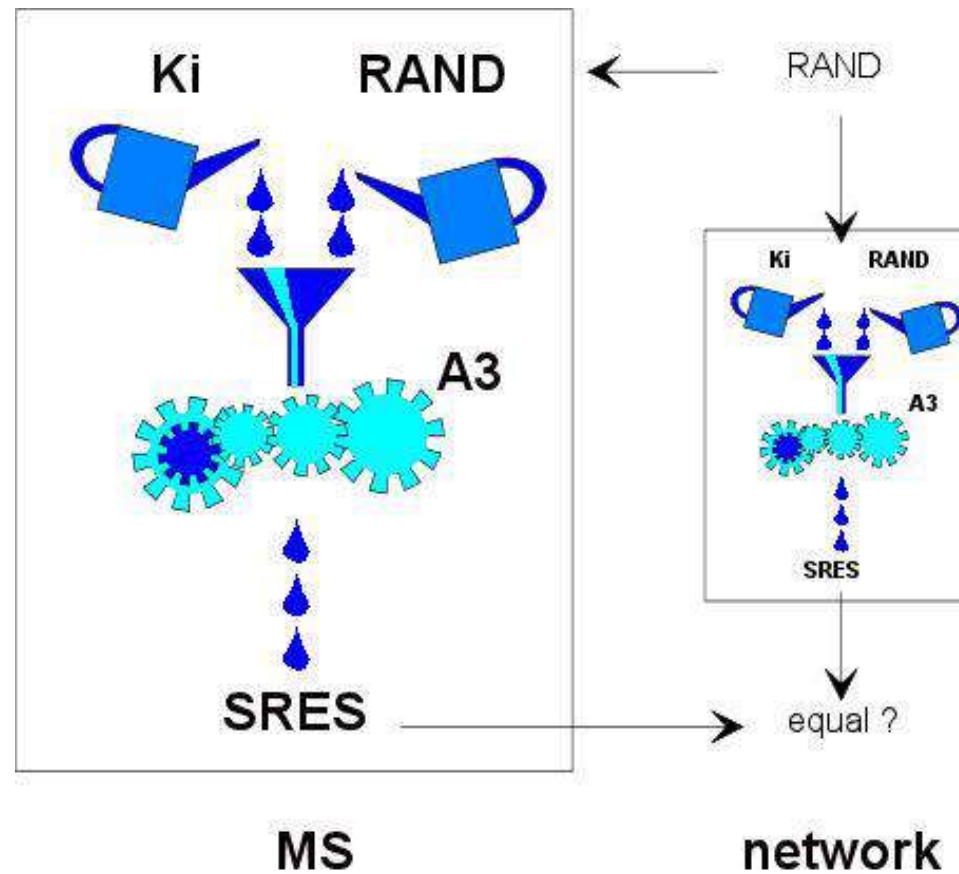
- Problem: How to protect the system from malicious loss of data or privacy?
 - Fraudulent use of the system
 - Eavesdropping on calls
 - Illegal surveillance
 - Identity theft

GSM Secret Key Architecture

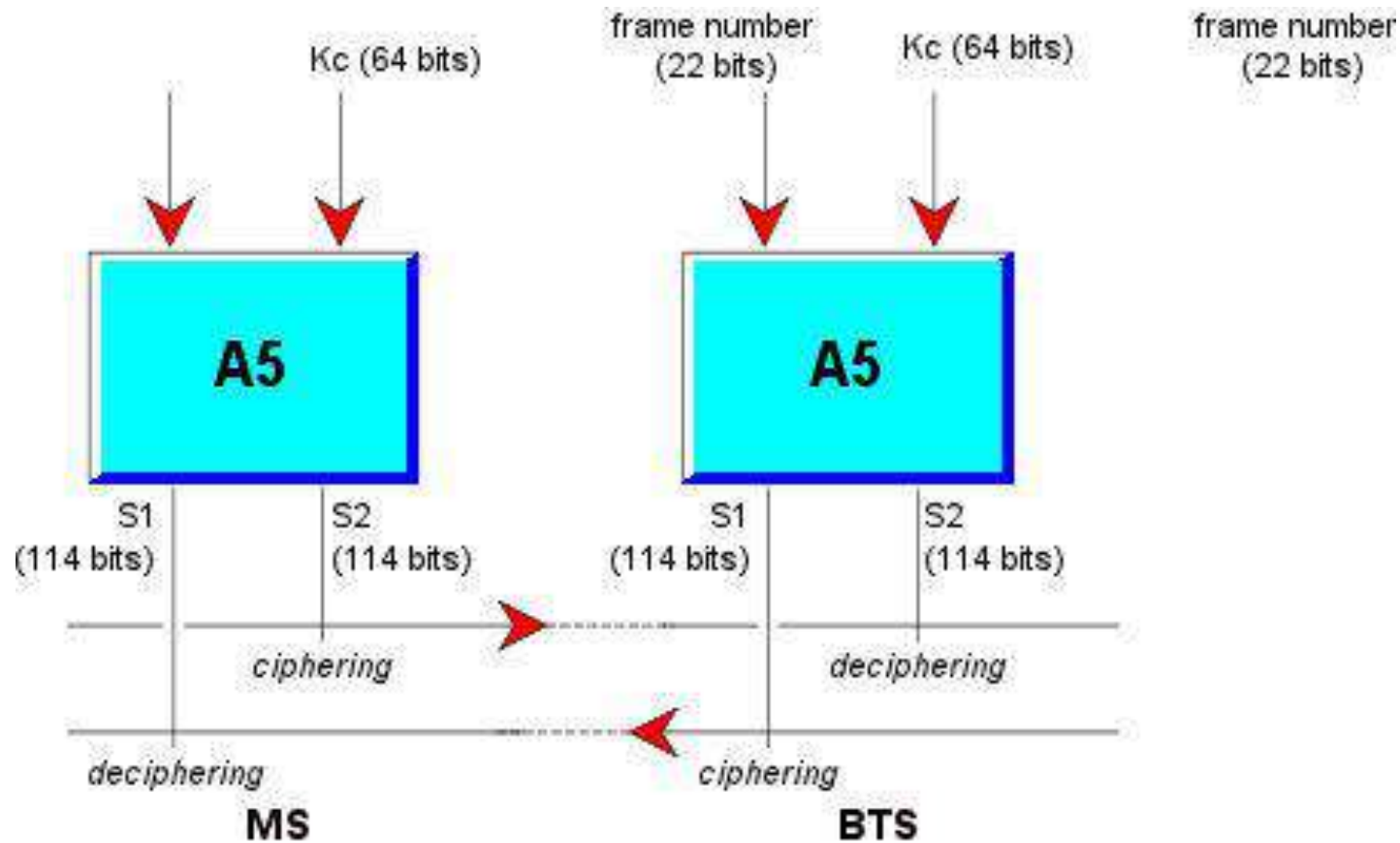


Authentication

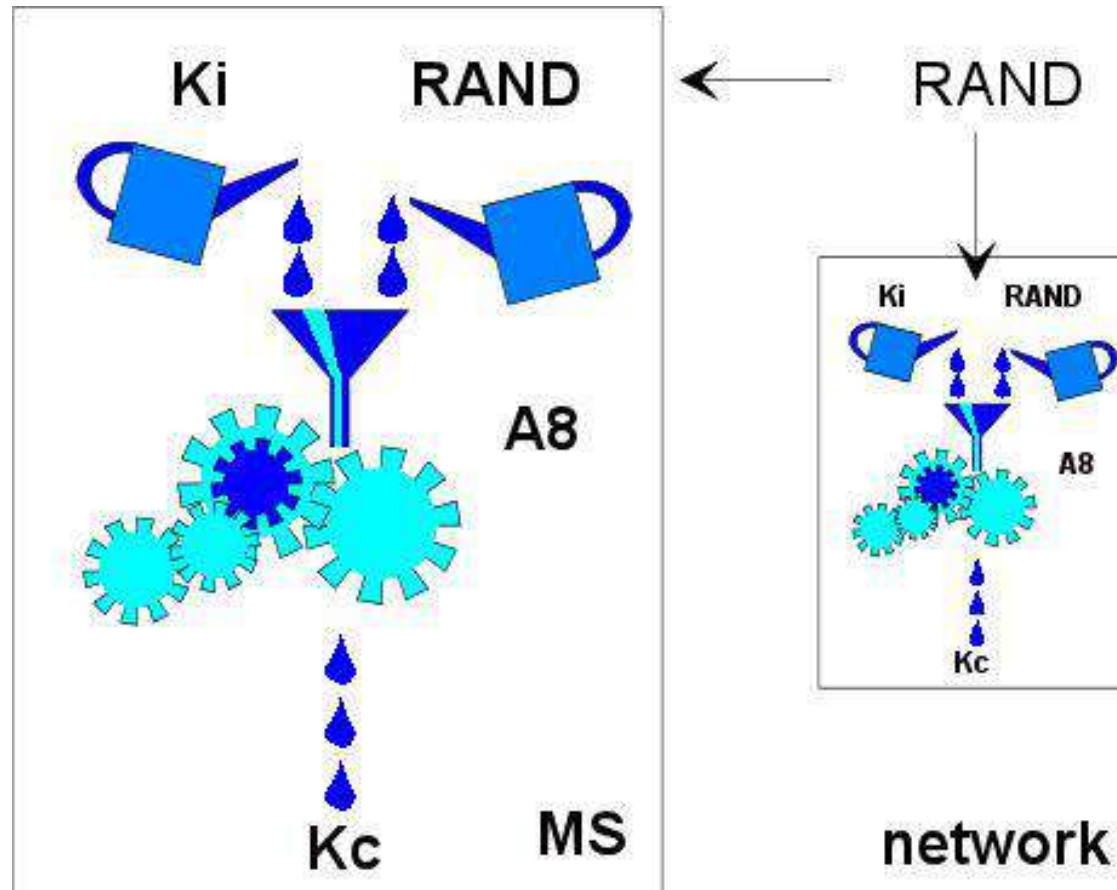
Ki is never sent over network, only RAND to the MS, and SRES for comparison.



Ciphering and Deciphering



Cipher key K_c generation



A5 algorithms

- A5/1 First algorithm. At first controversially strong, in recent years has been subject to (largely theoretical) demonstrations of attack
- A5/2 Deliberately weak A5 to overcome export controls of A5/1. Use discontinued
- A5/3 Intended to replace A5/1, it has recently been shown to be insufficiently strong
- A5/4 new proposed replacement for A5/1
- GSM protocols remain unchanged; Kc key lengths may change.



EP4.7.1 Identity privacy

- Speech, user data and most dedicated signalling is enciphered
- Common channels and the first exchange of messages, up to the transmission of an unambiguous user identity (linked to Ki) are not
- The first message carrying this unambiguous user identity carries a risk of being intercepted and possibly revealing the identity of the user.

TMSI allocation

- When a mobile switches on in a new network, without a history, the first identification (typically location update) will be by IMSI.
- The network (VLR) will then encrypt the communication, and allocate the SIM an identity associated with the Location Area, a TMSI (Temporary Mobile Station Identity)
- The TMSI can be passed to other VLRs in the network. In future communications with the network, the TMSI (+LAI) is used across the radio interface to identify the SIM, thus protecting the user identity.

EP4.7.1 solution: Identity privacy

- Problem:
 - The first exchange of messages, up to the transmission of an unambiguous user identity (linked to Ki) are not encrypted
 - The first message carrying this unambiguous user identity carries a risk of being intercepted and revealing the identity of the user
- Solution:
 - Allocate a temporary identity (TMSI) to the user



EP 4.7 Solution: Security

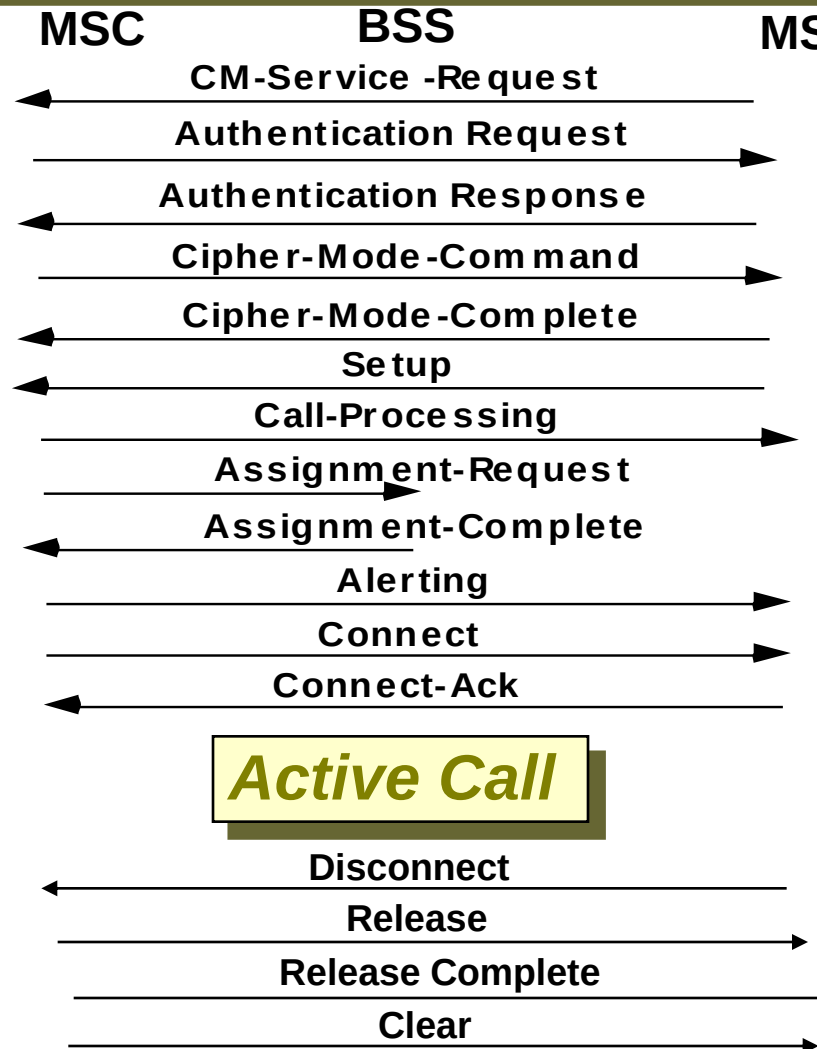
- Problem: How to protect the system from malicious loss of data or privacy?
- Solution:
 - Authentication of users
 - Ciphering of user data and signalling
 - Secret Key K_i placed in SIM and AUC
 - Structure protocols to be independent of n in algorithms $A_{m/n}$
 - Use TMSI



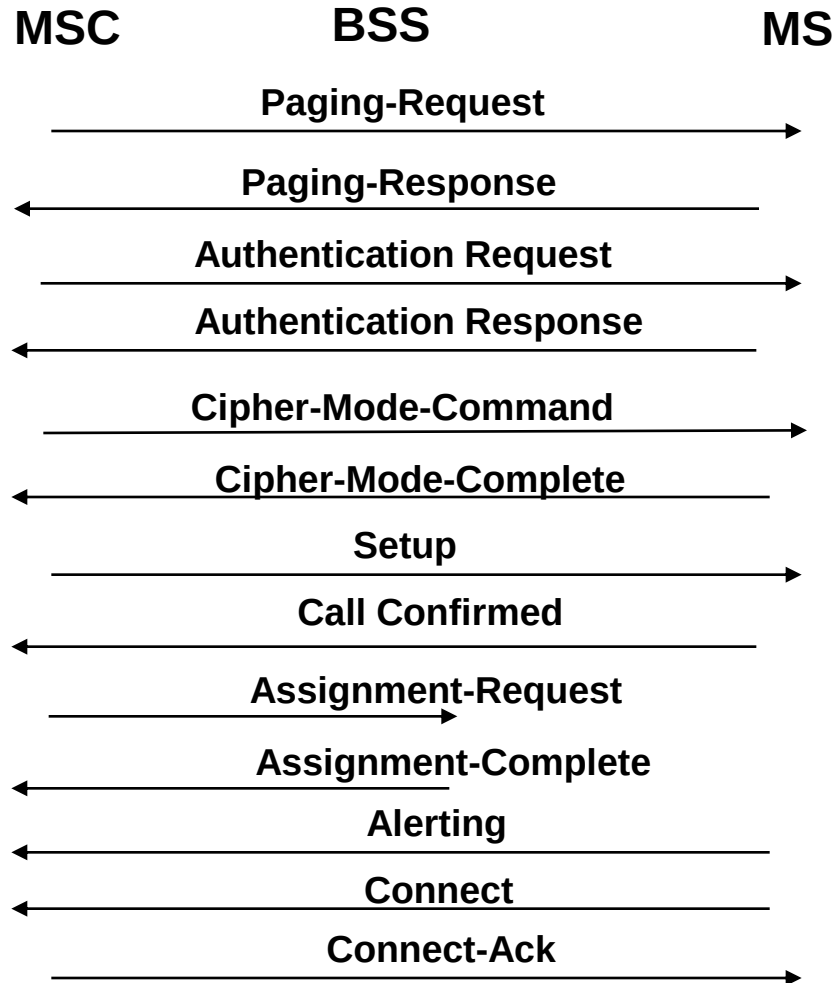
EP 4.8 Call establishment

- Problem: How to set up a secure call to or from a mobile?

Message Flow - Mobile Origination



Message Flow - Mobile Termination



EP 4.8 Solution: Call establishment

- Problem: How to set up a secure call to or from a mobile?
- Solution: Structure the procedure in a sequence of messages which establish the call parameters stepwise.

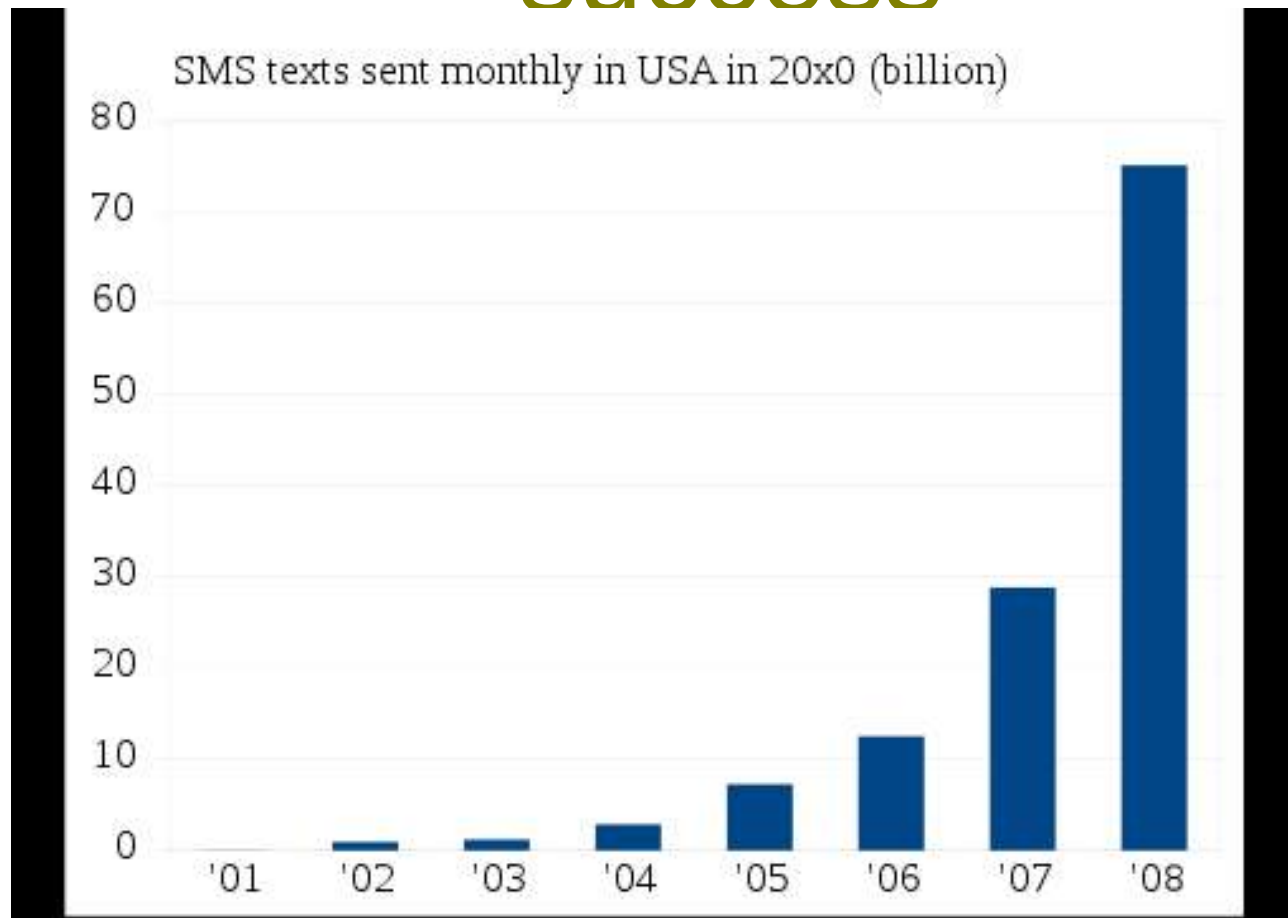
EP5 Short messages

- Problem:
 - How to send short text messages
 - Non-real time (non-intrusive) delivery service
 - Simple user interface needed
 - Without a big data overhead

SMS- implementation

- 3 services: Point-Point Mobile Originating and Terminating, Cell Broadcast
- Radio access via SDCCH (or SACCH in call) using LAPDm
- Network Transport using SS7/MAP
- 140 octet limit: typically 160 characters (default 7-bit alphabet); international character sets. Segmentation possible
- Multimedia (MMS) and CB: limited use so far (Tsunami, Amber Alerts..) 

SMS_PP: the surprising success



In 2008, 4.1×10^{12} SMS text messages were sent globally.

EP 5 Solution:SMS

- Problem
 - How to send short text messages
 - Non-real time (non-intrusive) delivery service
 - Simple user interface needed
 - Without a big data overhead
- Solution:
 - Re-use GSM signalling architecture, security etc.
 - Add predictive text to terminal implementations
 - Permits easy low-cost messaging
 - GSM security and reliability aids e.g. banking applications



EP 6 GSM Data Services

- Problem:
 - Increasing use of data networks (pre-WWW) require a means to transmit data
 - GSM initial radio interface optimized for circuit (ISDN) not for packet data
 - Higher speeds need fundamental radio enhancements

Data 1: Initial GSM data services

- Circuit-switched data up to 9.6kbps
- Compatibility with modems, CSPDNs PSPDNs and ISDN
- Transparent (no ARQ*) and non-transparent (ARQ*) modes
- Facsimile service (with in-call modification: alternate speech/fax)

*ARQ: automatic ReQuest for re-transmission

Data 2. HSCSD (High Speed Circuit Switched Data)

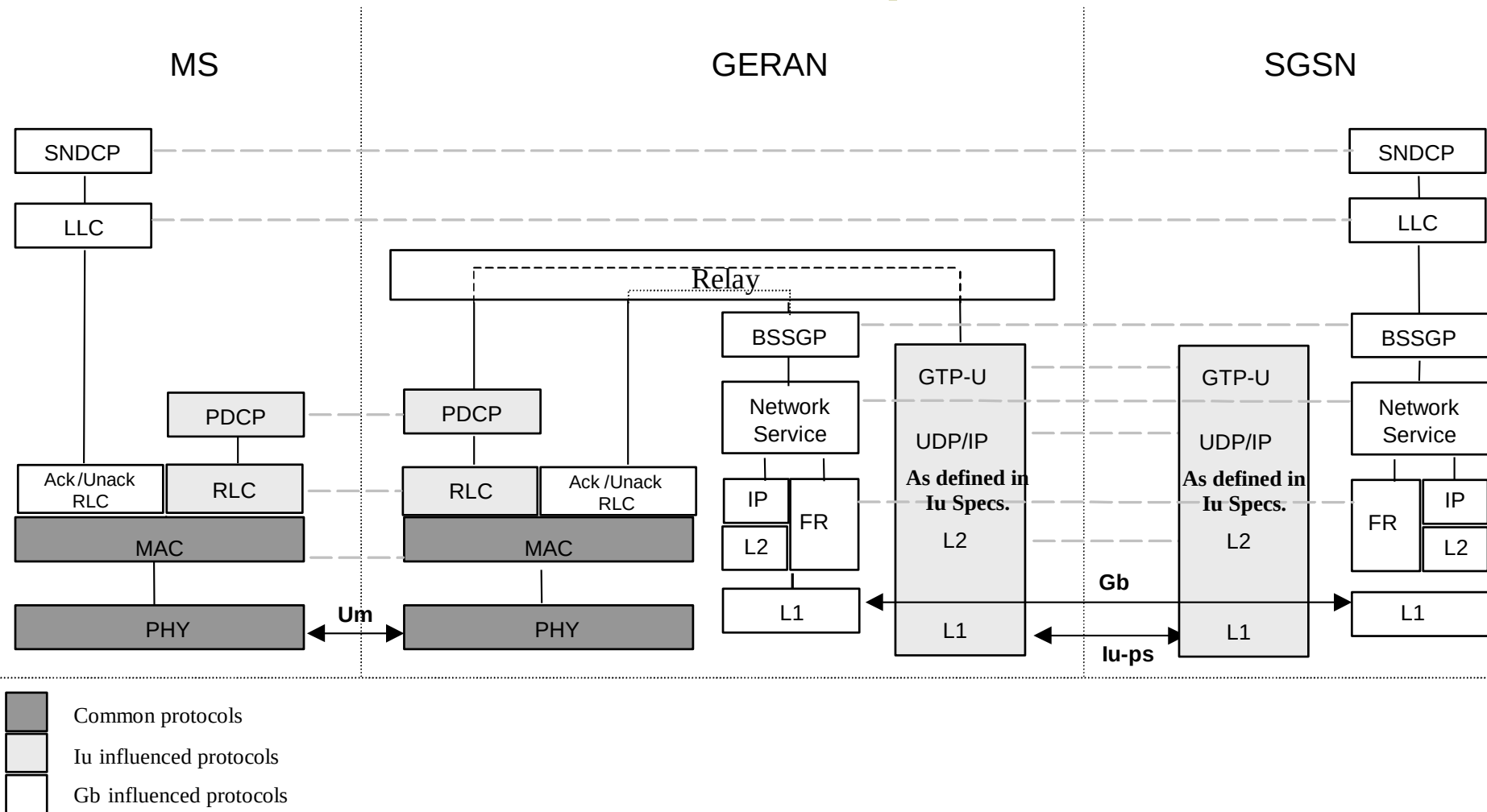
- Multiple time slots (per TDMA frame)
 - Mobile slot classes: “d+u” (downlink, uplink)
 - Allows asymmetric rates
 - Resource negotiation
 - RF duplexer if simultaneous Tx & Rx
- Flexible error correction
 - Up to 14.4 kbps per slot
- Backward compatibility
 - No conflict with existing services: no cell replan: no interference increase

Data 3. GPRS

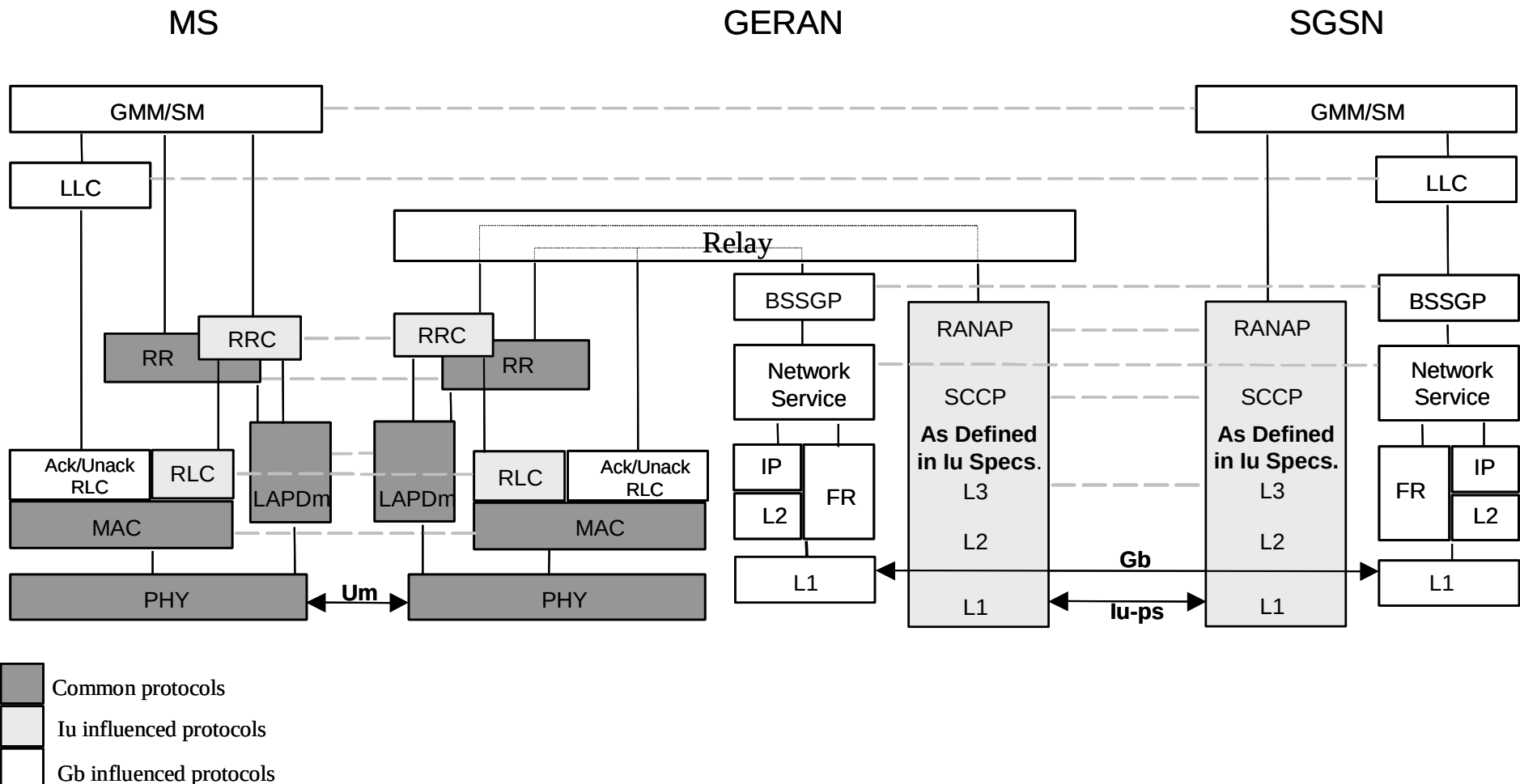
- General Packet Radio Service
- Provides cost-effective “always on” internet access without need to set up and clear down dedicated radio circuits
- Timeslot aggregation used
- 8/12/14.4/20 kbps per slot coding
- R97 typically 40kbps DL, 14kbps UL
- R99 theoretically up to 170 kbps DL



GPRS user plane



GPRS Control plane

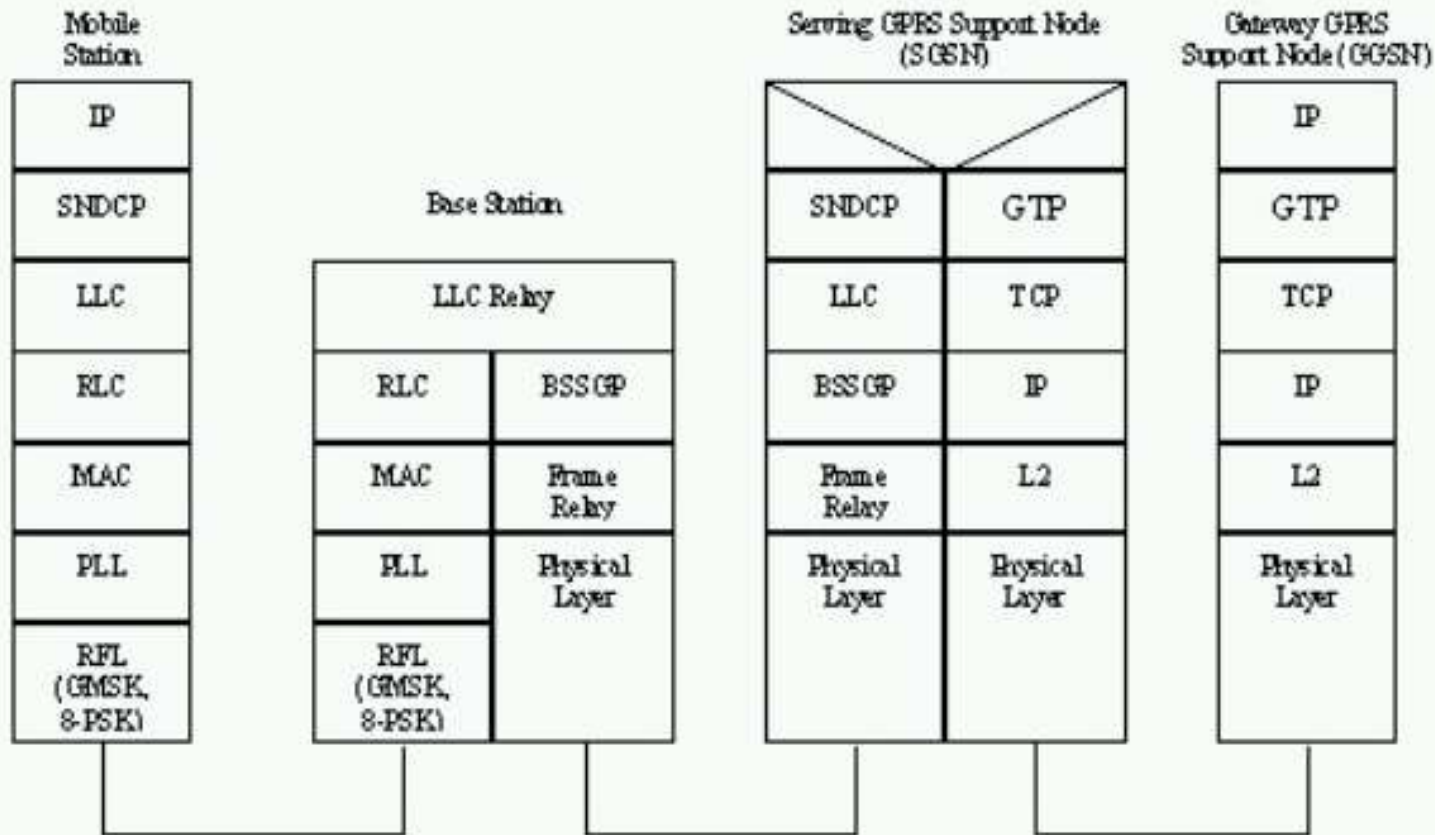


Data 4. EDGE, EGPRS

- EDGE=Enhanced Data rates for Global Evolution,
- EDGE+GPRS= EGPRS (Enhanced GPRS)
- New modulation technique (8PSK replacing GMSK) yields a x3 bit rate
- new channel coding for spectral efficiency
- No change to cell frequency plans



EGPRS Protocol Stack

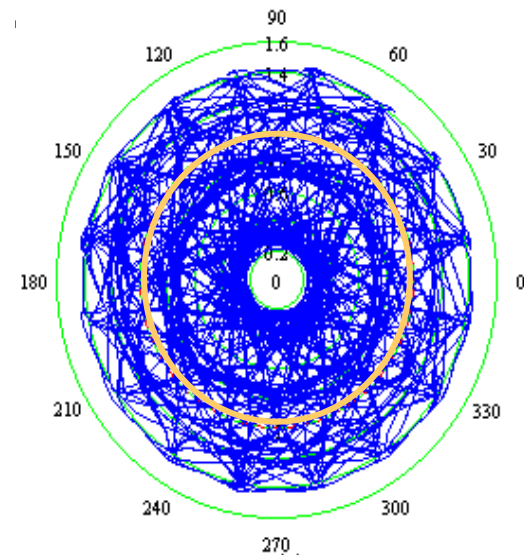


EDGE RF layer (1/4)

- New Modulation :
 - 8-PSK ($3\pi/8$ shift)
 - Robust fall back mode still in GMSK
- Same symbol rate as GSM : 270.833 ksps (13/48 Mhz)

Non constant amplitude modulation :

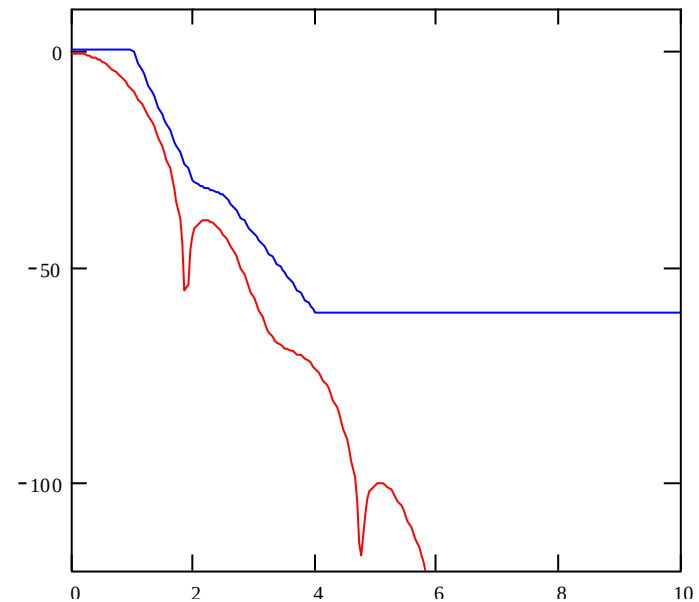
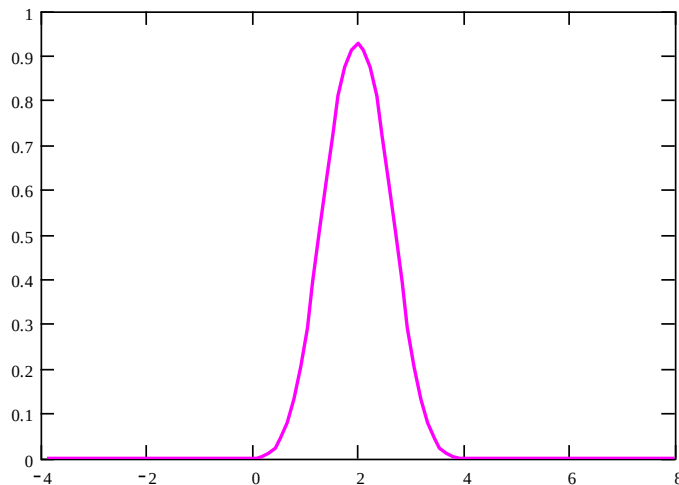
- PAR = 3.2 dB ; PMR = 17 dB



EDGE RF layer (2/4)

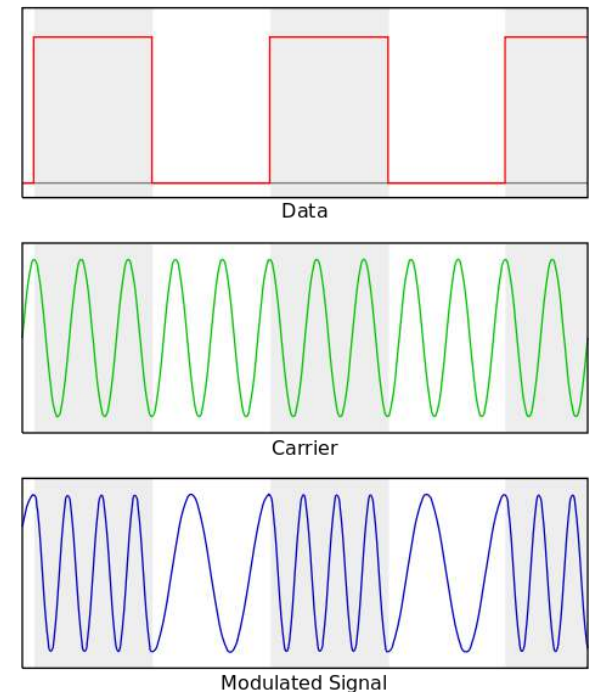
- Same C_0 pulse shape as linearized GMSK
 - same spectrum as GMSK

$$s(t) = \sum_k e^{\frac{3.k.\Pi}{8}.j} . e^{I_k \cdot \frac{\Pi}{4}.j} . C_0(t - k.T)$$



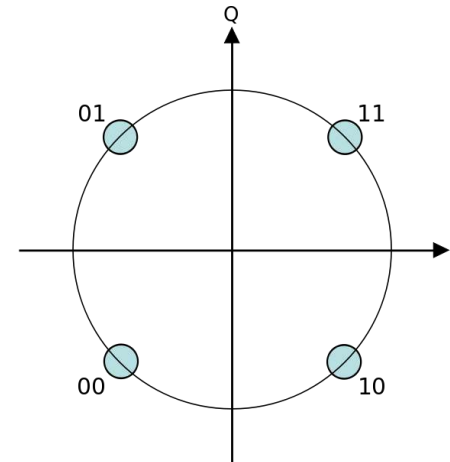
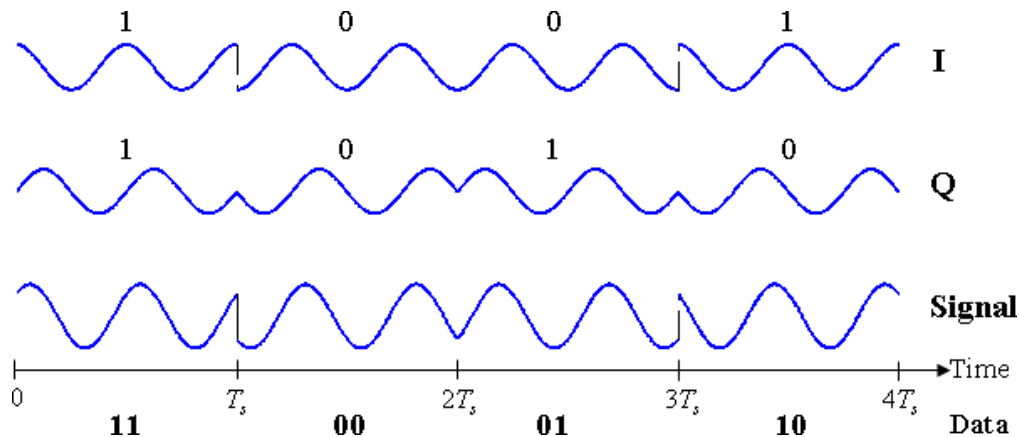
Frequency Shift Keying

- Data encoded by changing frequency
- GSM uses a type of FSK called GMSK (Gaussian Minimum Shift Keying)
 - 1 bit per symbol



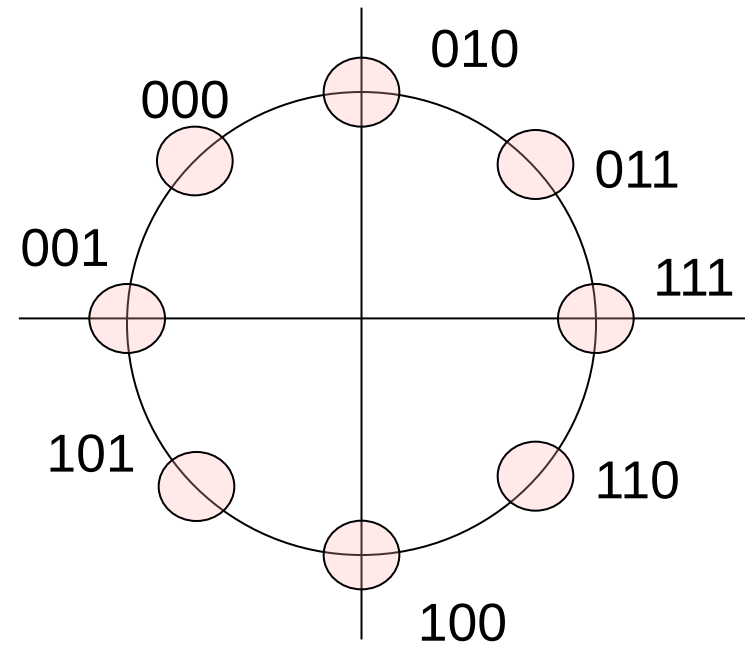
Phase Shift Keying

- Bits are encoded by phase shifting
- Example: QPSK (Quadrature PSK)
 - 2 bits per symbol



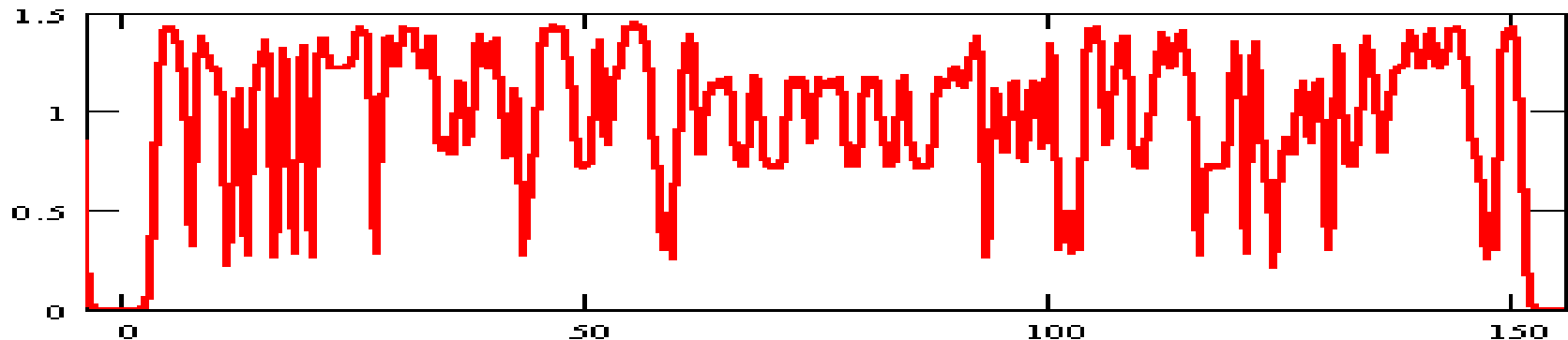
EDGE RF layer (3/4)

- 8PSK: 3 bits/symbol
- Gray coding of symbols
 - Most likely errors only create single bit change
 - Minimizes BER (Bit Error Rate)
- $3\pi/8$ phase shifted



EDGE RF layer (4/4)

- Burst topology
 - Same structure as for GSM
 - Same training sequence correlation
 - 8-PSK symbol 0 and 4 replace GMSK bit 0 and 1
 - PAR = 1.5 dB ; PMR = 4.3 dB
 - Mobile blind detection GMSK/8-PSK thanks to rotation within Training Sequence



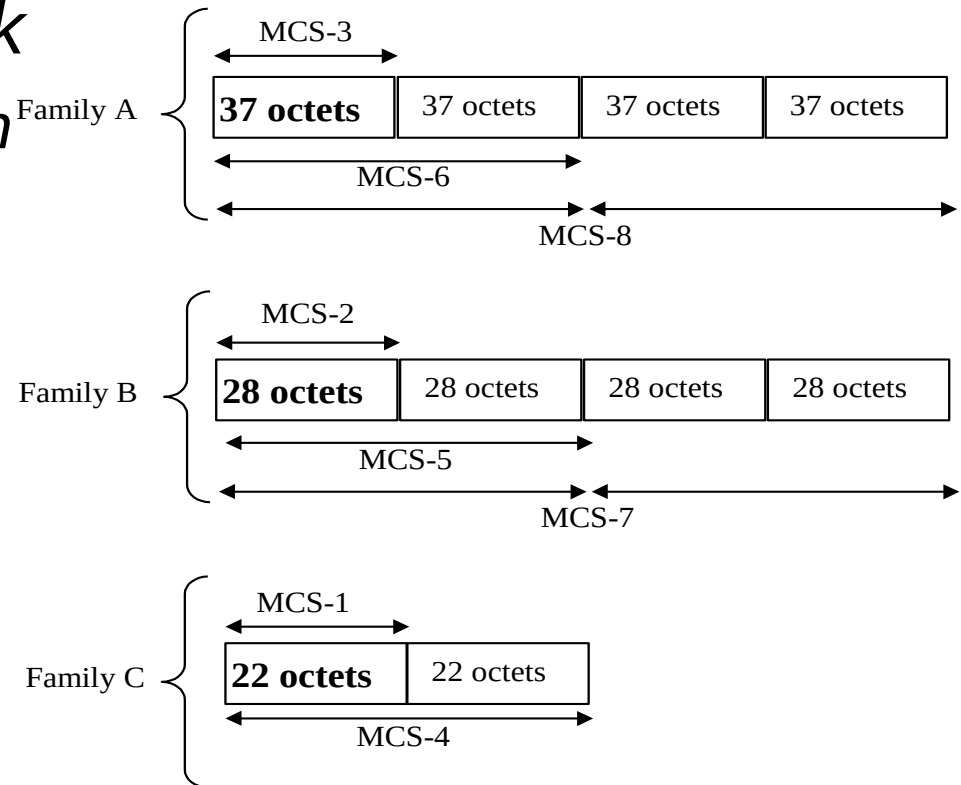
3 Sy.	Payload 58 symbol 8-PSK 174 bits	Training Sequence 26 symbol [same correlation as GMSK]	Payload 58 symbol 8-PSK 174 bits	3 Sy.	GP
-------	---	---	---	-------	----

Link Quality Control (RLC layer)

- *Assure optimum data rate is used to cope with propagation condition*
- *EGPRS is based on SR ARQ*
- *Two strategies*
 - *Link adaptation (Hybrid type I ARQ)*
 - *measurement ==> coding scheme adaptation*
 - *Incremental redundancy (Hybrid type II ARQ)*
 - *dynamic redundancy added with block repetition*
- *SMG2 agrees on :*
 - *compromise between efficiency and architecture impact*
 - *both mode (LA/IR) available*

Channel coding (1/4)

- 8 Modulation and Coding Schemes (MCS)
 - split in 3 families
 - each family transmit an integer number of fixed size RLC data block
 - easy retransmission with LQC



Channel coding (2/4)

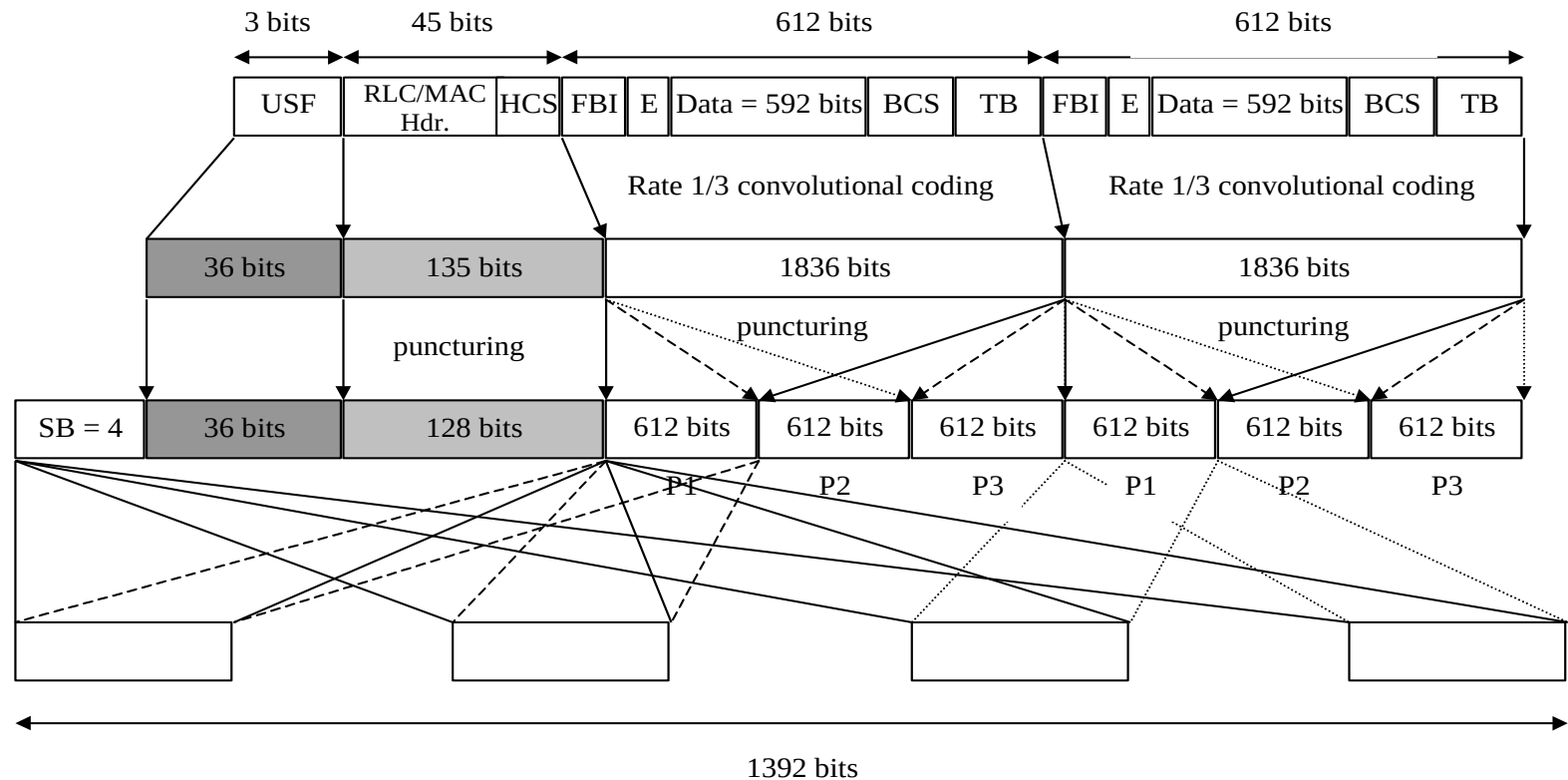
- Block code CRC
 - Header (HCS) and RLC data block (BCS) separately encoded
- Punctured Convolutional coding
 - CL = 7
 - mother rate : 1/3 (133;171;143)
 - tail biting for header vs zero tail bits for data
- Interleaving
 - Coded/Punctured Header always interleaved on 4 radio burst
 - Coded/Punctured RLC data block interleaved on 4 radio burst
 - **EXCEPT** MCS-8 and 7 interleaved on 2 radio bursts

Channel coding (3/4)

Scheme	Code rate	Header Code rate	Modulation	RLC blocks per Radio Block (20ms)	Raw Data within one Radio Block	Family	BCS	Tail payload	HCS	Data rate kb/s
MCS-8	1.0	0.35	8PSK	2	2x592	A	2x12	2x6	8	59.2
MCS-7	0.76	0.35		2	2x448	B				44.8
MCS-6	0.49	1/3		1	592	A	12	6		29.6
MCS-5	0.37	1/3		1	448	B				22.4
MCS-4	1.0	1/2	GMSK	1	352	C				17.6
MCS-3	0.80	1/2		1	296	A				14.8
MCS-2	0.66	1/2		1	224	B	11.2			
MCS-1	0.53	1/2		1	176	C	8.8			

Channel coding (4/4)

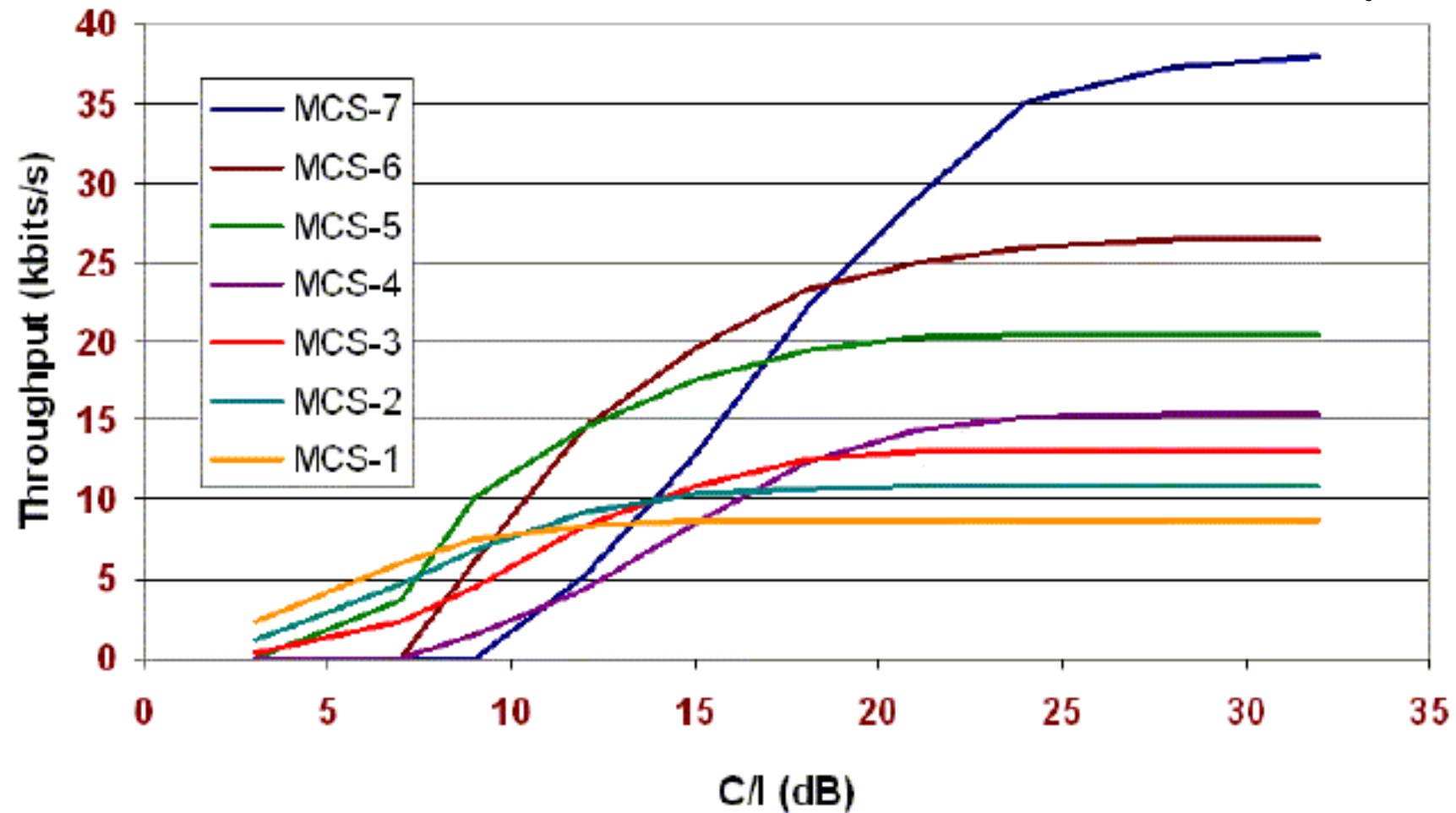
- MCS-8 example



- IR is achieved by successive retransmission of different Puncturing scheme: P1, P2, P3

EGPRS performance

Source: University of Surrey



Data 5 Evolved EDGE

- Latency reduced by halving transmission interval to 10ms
- Bit rate increased by:
 - dual carrier,
 - higher symbol rate and higher order modulation (32QAM and 16QAM as well as 8PSK, QPSK),
 - improve error correction (turbo-codes)
 - Dual antennas
- 0.5-1Mbps DL potential
- R7 feature tbi: competes with UMTS/LTE



EP 6 Solution:Data

- Solution:
 - Begin with basic service compatible with existing (CS) data services
 - Add packet services
 - Increase data rates by
 - timeslot aggregation
 - new channel coding and modulation
 - Additional antennas
 - Reduce latency by halving frame



EP 7 Voice services

- Problem:
 - Original GSM voice quality is less than many fixed lines
 - Adding voice capacity is relatively costly

GSM voice codecs

- FR: Full Rate (original). 13kbps RPE-LTP
- HR: Half Rate: 5.6 kbps, lower quality
- EFR: Enhanced Full Rate. 12.2kbps
- AMR: Adaptive Multi-Rate. A range of rates up to 12.2 kbps (EFR)
- Wideband AMR: 7kHz replaces 3.1kHz audio bandwidth



VAMOS- Voice services over Adaptive Multi-user channels on One Slot

Release 9 (under development) The objective is to further enhance the voice capacity of GERAN by means of multiplexing two users simultaneously on the same radio resource both in downlink and in uplink.

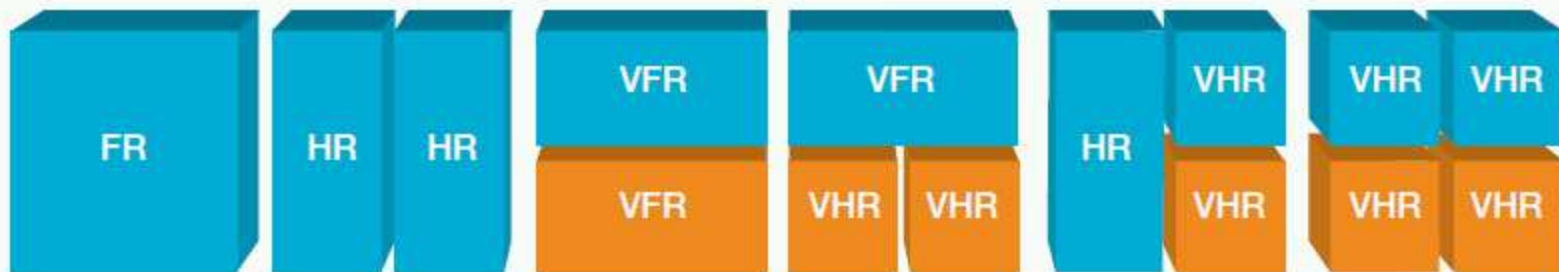
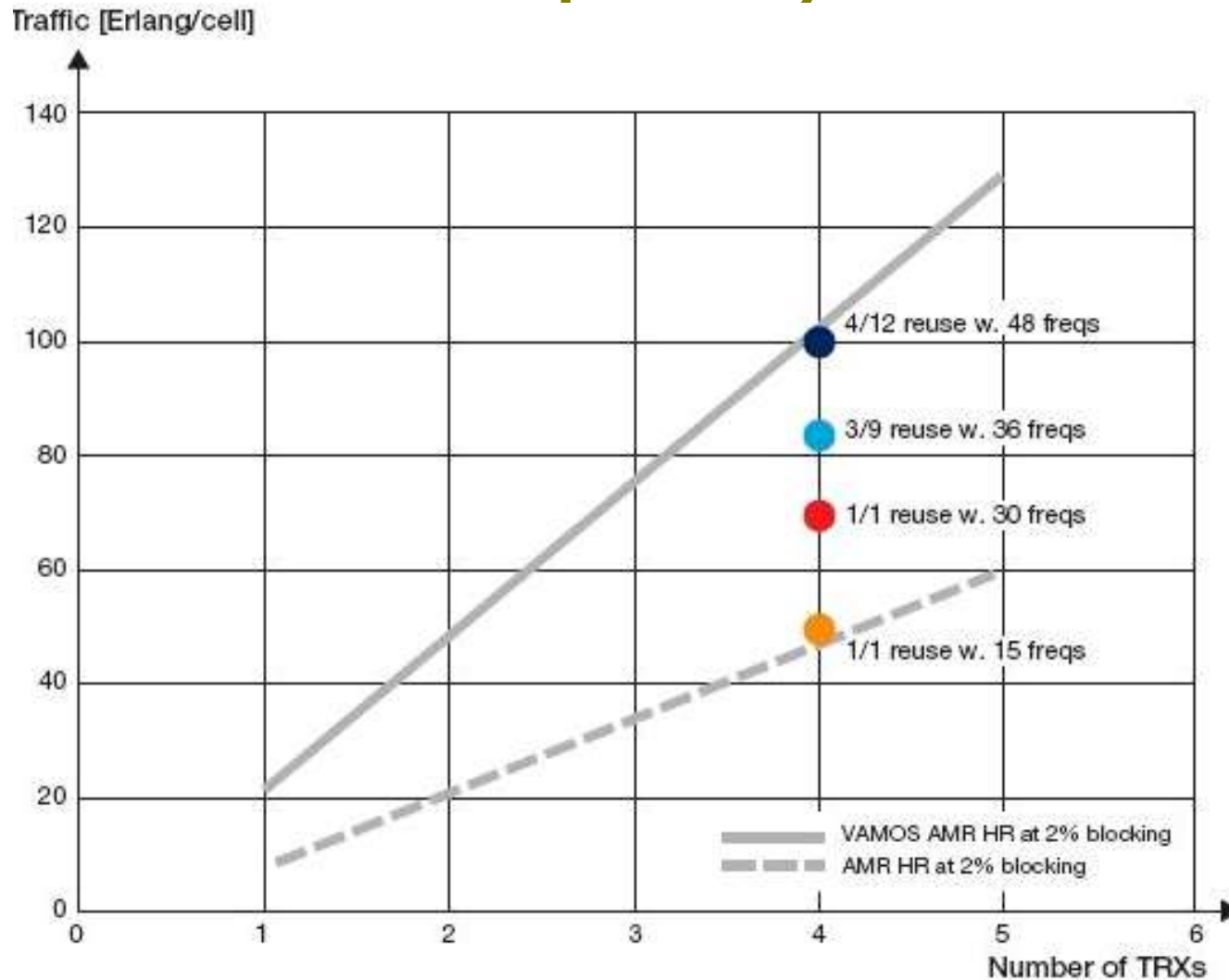


Figure 1: Full rate (FR), half rate (HR), VAMOS FR (VFR) and VAMOS HR (VHR) allocations on a single time slot

VAMOS Capacity increase



EP 7 Solution: Voice services

- Problem:
 - Original GSM voice quality is less than many fixed lines
 - Adding voice capacity is relatively costly
- Solution:
 - New codecs permit higher quality or lower channel occupancy
 - DTX reduces interference
 - New modulation, power control techniques permit further gains compatible with old equipment



EP8 GSM for PMR

- Problem:
 - How to adapt GSM for PMR applications
 - Railways
 - Emergency services (Police, Fire, Ambulance)
 - Reliability is paramount

GSM-R

- New Services: Advanced Speech Call Items (ASCI) specified:
 - Voice Group Call
 - Voice Broadcast Service
 - Enhanced Multi- Level Precedence and Pre-emption Service (EMLPPS)
- Reliability increased using system-level engineering

EP 8 Solution: GSM for PMR

- Problem:
 - How to adapt GSM for PMR applications
 - Reliability is paramount
- Solution
 - Design Specific Services to meet requirements
 - System Engineering Optimization

Advanced GSM Features(R7+)

Rel-7

DTM Handover
DARP Phase II
Dual Carrier DL
SIGTRAN support in
GERAN
Latency Reduction
EGPRS2 UL
EGPRS2 DL

Rel-8

GERAN-LTE
interworking
U-TDOA
enhancement
GAN enhancement
AoIP in GERAN
MultiCarrier BTS
Additional Navigation
Satellite Systems

Rel-9

VAMOS
CEBRO
Hybrid Location

Rel-10

LCLS
TIGHTER
MOCN

GSM Issues: Coverage

- Mountainous regions
 - GSM reaches many remote mountains (Everest, Kilimanjaro,...) but mountain country also suffers from deep shadowing
- sparsely populated regions
 - Double-slot GSM can be used
- oceans
- deep building interiors, tunnels, underground railways
 - Radio relays
 - Directed antennas



GSM Issues: Capacity

- Dense Urban voice
 - Microcells
- High Speed data, dense usage
 - Femtocells
 - Complementary technologies
 - UMTS
 - LTE
 - WiFi
 - WiMax
 - New spectrum?



EFREI M2 ST245

Mobile Networks

Fundamentals of Cellular
Networks; **GSM**
Paul Simmons