University of Antwerp
Faculty of Science

Advanced Wireless & 5G Networks

Prof. Dr. Ir. Michael Peeters — 2023–2024

Topics for today

- **2. Technology baselining/refresher**
  - 2G !

Planning

Session	Date	Topic
1	20231006	~~Introduction, history, market, industry, bands, licensed vs. unlicensed, …~~
2	20231013	~~Technology baselining (a.k.a. refreshing what you should have known): 2G, WiFi, …~~
3	20231020	~~Cancelled~~
4	20231027	~~Shannon/Friis continued. 2G as a ”low-complexity” example~~
5	20231110	L 2G
6	20231117	L 3GPP 2G-3G-4G-5G architecture evolution. 5G
7	20231124	L: Other licensed and special cases (CBRS, LAA, Public Safety, Loon, V2V, Satellite)
8	20231201	U IEEE Wifi Network Architecture: 802.11 abgn
9	20231208	U QoS, 802.11 ac,ax and 802.11 ad,ay
10	**20231215 – 3h**	U short range 802.15.4: Zigbee, BLE, and UWB
11	**20231222 – 3h**	U Specials: LoRa, Sigfox (perhaps), proprietary, 802.11p
	TBD	Extra: Technology enablers and acronyms you need to be aware of: ADC, FEM, PA, LSA, and other key analog and digital HW blocks, mMIMO, Beam management, 802.11be, AI, 6G, THz and their implications to the network

University of Antwerp
Faculty of Science

Your expectations

- How it is possible that, in a world where the number of devices continue to grow, every device can get mobile wireless connectivity with the internet without saturating the network.
- How do 4G/5G/... technologies actually work.
- How do you go about designing a good WiFi network, both on the physical end (devices, access point locations, ...) and on the configuration end.
- What are the technologies behind the current advancement in Cellular and Wi-Fi networks?
- Be able to understand the need for improved and efficient networking technologies, and how to approach solving the drawbacks of current technologies.
- What are the limitations of 5G in regard to the latest trends in Ai, AR/VR and technologies that require very low latency.
- What is next?
- Wifi 6 & 7 – new features.
- Link to cloud.
- How do modern mobile networks work and how have they changed from the previous ones?
- What are the main problems or limitations faced by different types of networks? If it is possible, what are the best ways to solve them?
- How will wireless and mobile networks possibly evolve in the near future?
- ~~To better understand historical challenges in wireless that companies such as blackberry faced.~~
- To better understand wireless technologies such as Zigbee and LoRaWan and their use in IOT projects.
- What role data science could have in this field?
- Can networks be perfected to the point where we don't need to keep on creating new ones or upgrade the existing ones?
- ~~Can governments stop the development of networks?~~
- ~~Will connectivity ever be available underwater or underground?~~
- Security of wireless networks.

2. Baselining

(concepts & toy examples)

What will we cover

- ~~Mobile vs. Wireless vs. Fixed~~
- ~~Shannon's law, to calculate capacity and compare technologies~~
- ~~Friis's equation, to calculate coverage~~
- Cellular and 2G as a reference system

Calling a cat a cat

Fixed Networks

- Tied to infrastructure
  - Physical configuration is required
- Reliable
  - Dedicated link
- Robust
  - Scales to high bandwidths
- Powered
  - Mains
  - PoE
- Mostly unicast
  - Highly secured

Wireless Networks

- Not tied to infrastructure/walls
  - Ad-hoc networking
- Error-prone
  - Traffic Management
- Frequent Disconnections
  - Resource Management
  - Quality of Service for multimedia
- Battery operated
  - Media access and networking while sleeping
  - Time synchronization
- Broadcast
  - Security

Mobile Networks

- Location matters
  - And changes dynamically
  - Can be nonlocal (WAN vs. LAN, roaming)
- Movement matters
  - Doppler shift of f due to velocity
- Addressing
  - IP addresses indicate how to get data
  - But they are tied to an entity
- Hand Off/Over
  - Seamless

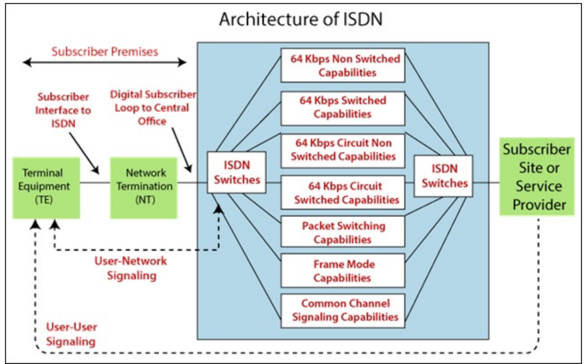
2G a.k.a. GSM

Requirements

- It should offer good subjective speech quality
- It should have a low phone or terminal cost
- Terminals should be able to be handheld
- The system should support international roaming
- It should offer good spectral efficiency
- The system should offer ISDN compatibility

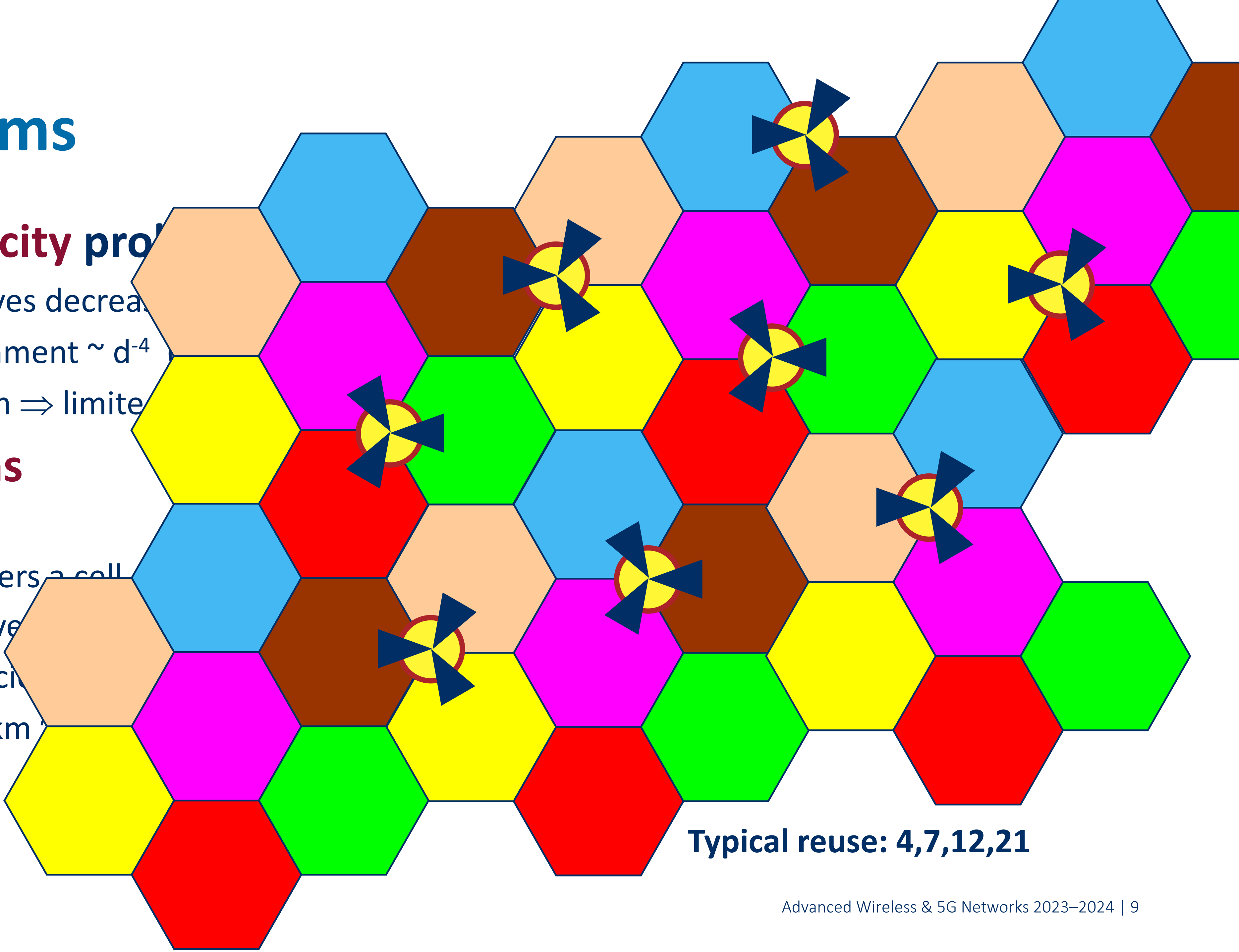
SPECIFICATION SUMMARY FOR GSM CELLULAR SYSTEM

Multiple access technology	FDMA / TDMA
Duplex technique	FDD
Uplink frequency band	890 - 915 MHz (basic 900 MHz band only)
Downlink frequency band	933 -960 MHz (basic 900 MHz band only)
Channel spacing	200 kHz
Modulation	GMSK
Speech coding	Various - original was RPE-LTP/13
Speech channels per RF channel	8
Channel data rate	270.833 kbps
Frame duration	4.615 ms



Cellular systems

- **Coverage/capacity pro**
  - power radio waves decrea
  - in urban environment ~ d^{-4}
  - limited spectrum ⇒ limite
- **Cellular systems**
  - Bell Labs, 1971
  - base station covers a cell
  - “small” cells solve
  - reusing frequenci
  - GSM cell size 1 km

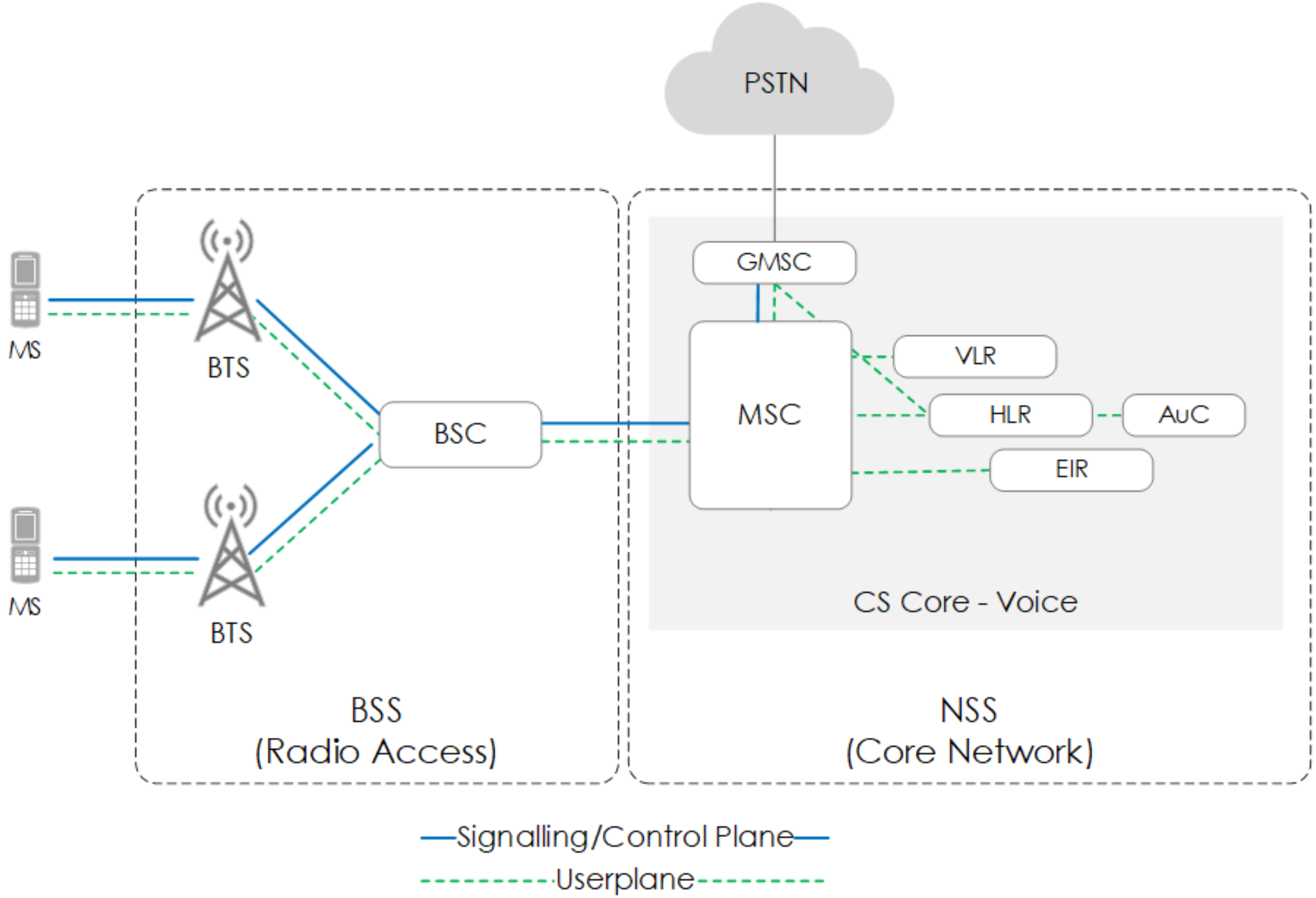


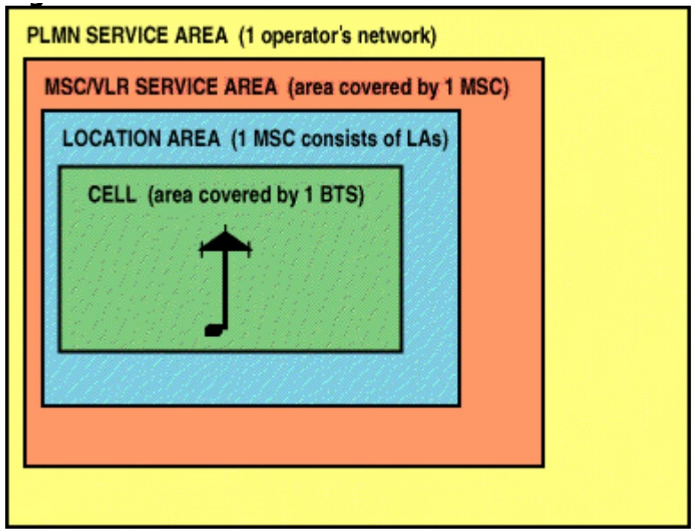
Typical reuse: 4,7,12,21

Cellular Systems: Additional complexity

- **Radio Interface Management**
- **Locating a subscriber (mobility aspects for idle terminal)**
- **Handover (mobility aspects for terminals in dedicated mode)**
- Roaming

2G architecture





Mobile Station (MS)

- **Functions:**
  - radio and processing function to access the network through radio interface
  - human user interface (microphone, loudspeaker, display)
  - interface to other equipment
- Subscriber Identity Module (SIM)
  - smart card with subscriber related information
  - PIN code
  - list of phone numbers, settings, etc.

Base Station Subsystem (BSS)

- **Connects MS with NSS controlled by OSS**
- **BSS consists of:**
  - Base Transceiver Station (BTS)
    - BTS contains radio transmission/reception devices
    - connects with MS via radio interface
    - Transcoder/Rate Adaptor Unit (TRAU) contains GSM specific speech codec and data traffic adaptation
  - Base Station Controller (BSC)
    - connects with NSS (A interface) and BTS (Abis)
    - management of radio channels
    - handover
    - 1 BSC controls a number of BTS

Network & Switching Subsystem

- **Mobile Service Switching Center (MSC)**
  - basic switching function (for millions of users)
  - interface to BSS and external network (IWF)
  - one MSC controls a few BSCs
  - databases for mobility management and subscriber data

- **Home Location Register (HLR)**
  - database with subscriber information independently of actual location
  - information related to actual location of subscriber
  - contains Authentication Center

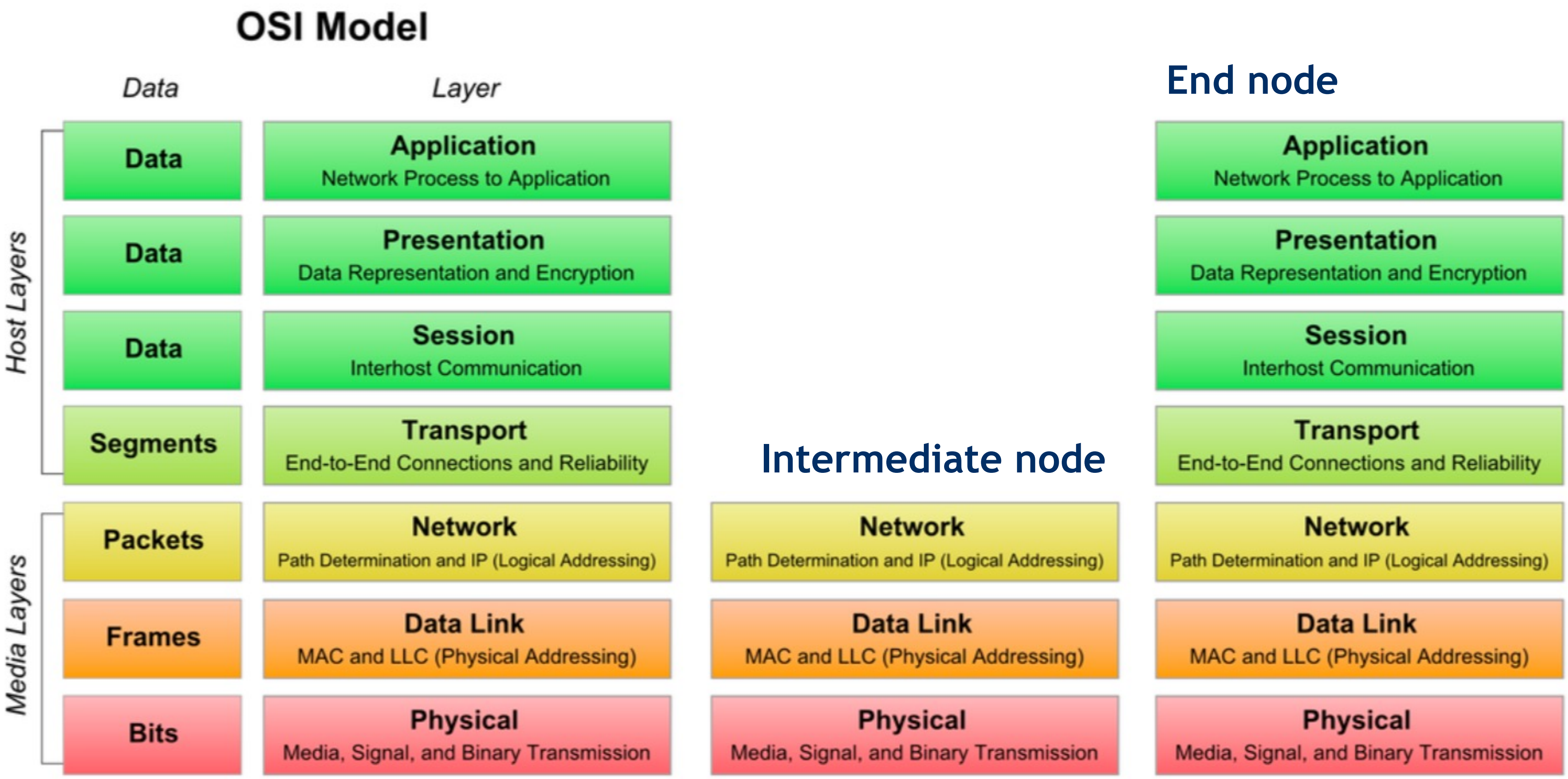
Network & Switching Subsystem

- **Visitor Location Register (VLR)**
  - VLR related to one or more MSC
  - database with information of subscribers currently in these MSCs
- **Gateway Mobile Switching Center (GMSC)**
  - An MSC fetches the location information of a subscriber (using HLR)
  - GMSC routes call to visited MSC
- **Signaling System 7 (SS7)**
  - signalling between NSS machines

Operation Subsystem (OSS)

- **Functions of OSS**
  - Network operation and mainatenance
  - Subscription management (SIM)
    - subscriber data management (HLR)
    - call charging
  - Mobile station management (Terminal equipment)
- **Interface with NSS machines through SS7 signalling**

OSI STACK


OSI Model
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Packets
Network
Path Determination and IP (Logical Addressing)
Frames
Data Link
MAC and LLC (Physical Addressing)
Bits
Physical
Media, Signal, and Binary Transmission
Intermediate node
Network
Path Determination and IP (Logical Addressing)
Data Link
MAC and LLC (Physical Addressing)
Physical
Media, Signal, and Binary Transmission
End node
Application
Network Process to Application
Presentation
Data Representation and Encryption
Session
Interhost Communication
Transport
End-to-End Connections and Reliability
Network
Path Determination and IP (Logical Addressing)
Data Link
MAC and LLC (Physical Addressing)
Physical
Media, Signal, and Binary Transmission

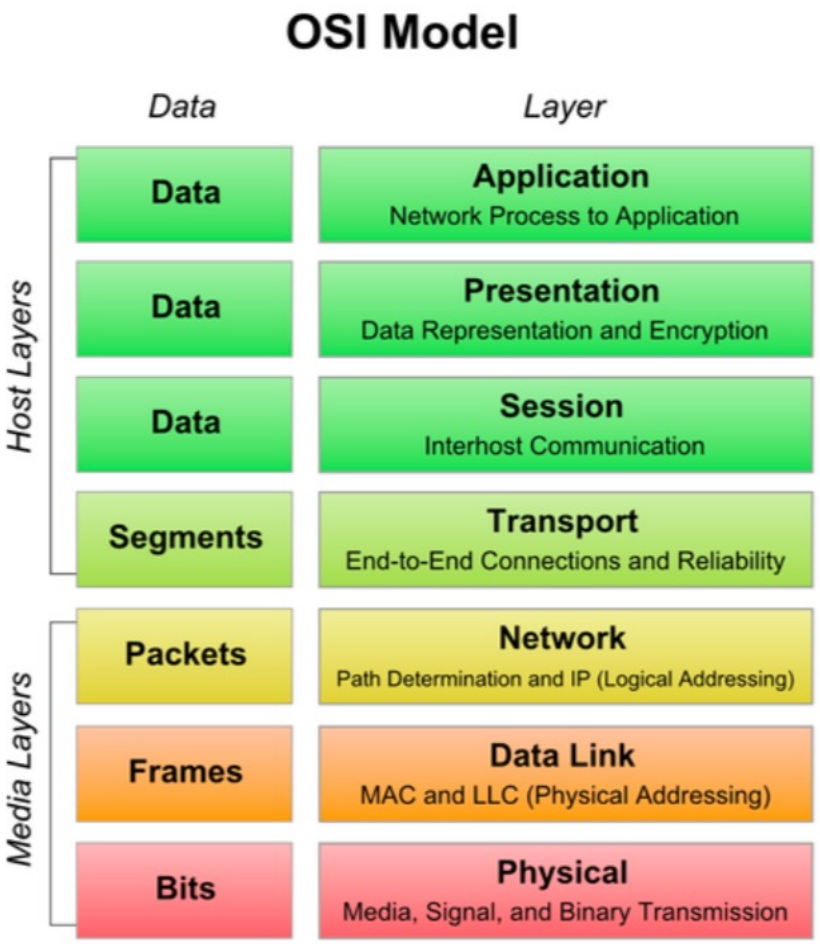
ISO-OSI Layers (1)

- **Physical Layer**
  - rules by which bits are passed (duration of a bit, voltage of a bit, frequency used, …)
- **Data Link Layer**
  - error detection/correction
  - flow control
- **Network Layer (IP)**
  - Addressing
  - Routing (statical/dynamical)
  - IP Protocols: ARP, DHCP, NAT, ICMP, GTP
  - Standard protocols: IPv4, IPv6

ISO-OSI Layers (2)

- **Transport Layer**
  - end-to-end protocols (UDP, TCP)
  - data arrives error-free, in sequence, without losses, without duplicates
  - end-to-end flow control, congestion control
- **Session Layer**
  - dialogue between applications (1/2 way, alternate)
- **Presentation Layer**
  - compression, encryption, conversion
- **Application Layer**
  - e-mail , FTP, HTTP,...

OSI STACK



FOCUS OF THIS COURSE

We’re making a 2G voice call (simplified)

Now, let’s really start from the application

Circuit Switching Vs Packet Switching

Circuit Switching	Packet Switching
Physical path between source and destination	No physical path
All packets use same path	Packets travel independently
Reserve the entire bandwidth in advance	Does not reserve
Bandwidth Wastage	No Bandwidth wastage
No store and forward transmission	Supports store and forward transmission

We are going to ignore this (for now)

3

What are the steps?

0. Buy a mobile phone.

1.

2.

3.

4.

5.

6.

7.

8.

9.

10.

11.

12.

PROFIT !

What are the steps?

1. Switch on the mobile (& infrastructure)
2. Select a frequency band to receive & send
3. Pick a way to send and receive digital bits
4. Define how we are going to organize the bits
5. Listen to synchronize and get system information
6. Pick a time to send
7. Wait for a response (try again)
8. Get a control channel assigned
9. Ask to make a call
10. Authenticate
11. Get voice channel and talk
12. … (location update, release call, handover, etc …)

What are the steps?

1. ~~Switch on the mobile (& infrastructure)~~
2. Select a frequency band to receive & send
3. Pick a way to send and receive digital bits
4. Define how we are going to organize the bits
5. Listen to synchronize and get system information
6. Pick a time to send
7. Wait for a response (try again)
8. Get a control channel assigned
9. Ask to make a call
10. Authenticate
11. Get voice channel and talk
12. … (location update, release call, handover, etc …)

2G system specification

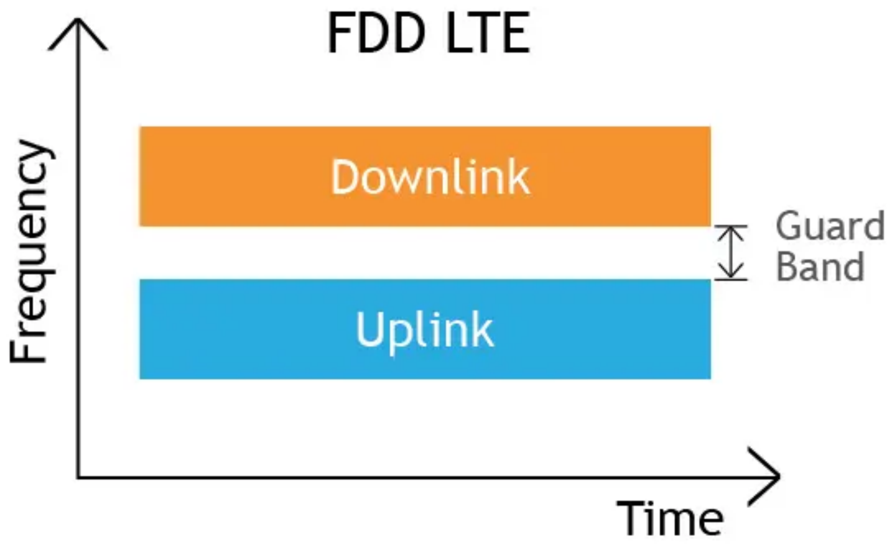
SPECIFICATION SUMMARY FOR GSM CELLULAR SYSTEM

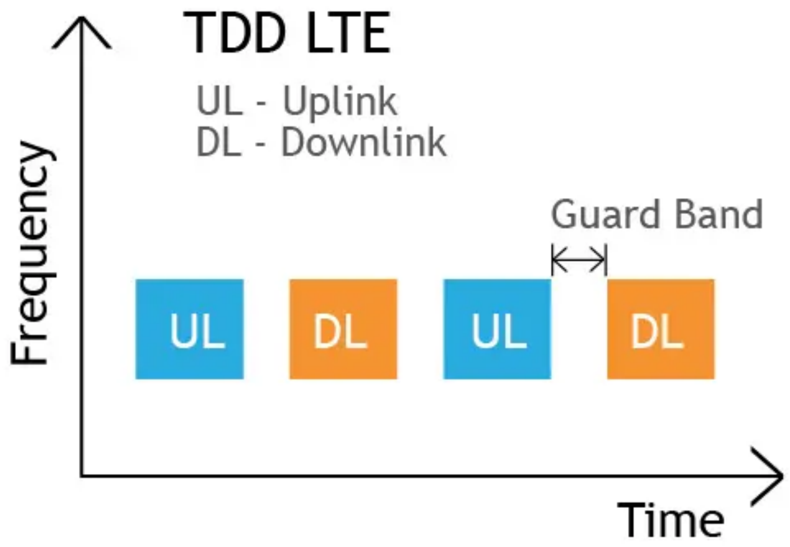
Multiple access technology	FDMA / TDMA
Duplex technique	FDD
Uplink frequency band	890 - 915 MHz (basic 900 MHz band only)
Downlink frequency band	933 -960 MHz (basic 900 MHz band only)
Channel spacing	200 kHz
Modulation	GMSK
Speech coding	Various - original was RPE-LTP/13
Speech channels per RF channel	8
Channel data rate	270.833 kbps
Frame duration	4.615 ms

Important: application influences the PHY most of all (e.g. 5G NSA/SA)

FDD vs TDD

- **Frequency Division Duplexing**
  - We talk at the same time, but in different bands
- **Tim Division Duplexing**
  - We alternate talking, but we stay in the same band.

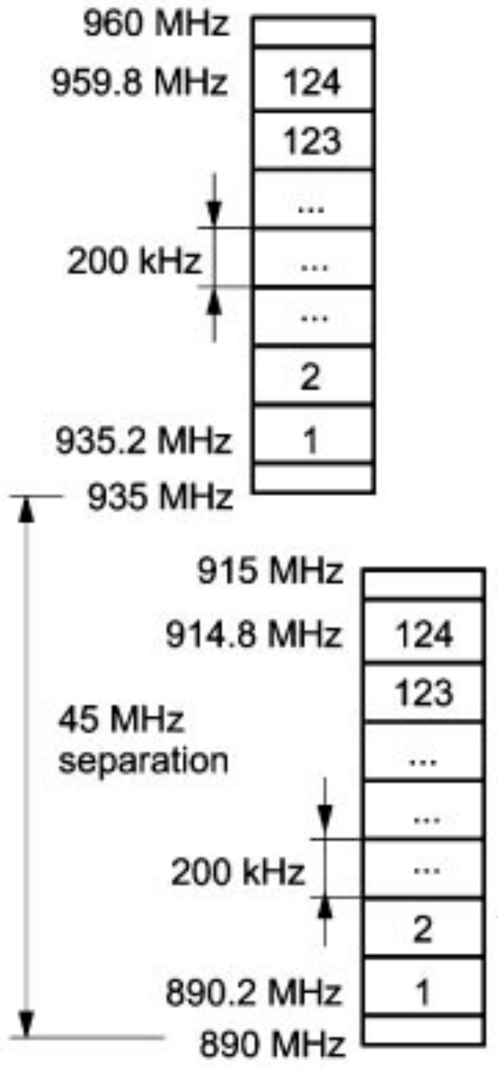




GSM FDD Spectrum

Downlink

Uplink



Requires:

- Ability to change frequency, "tune"
- Filters to listen to only what you are interested in
    - Can be analog or digital

Today: can all be done digitally, in SDR, software defined radio

ARFCN

- **Absolute Radio Frequency Channel Number**
  - 890-915 MHz band for subscriber-to-base transmission(reverse link or uplink)
  - 935-960 MHz band for base-to-subscriber transmission(forward link or downlinkl)

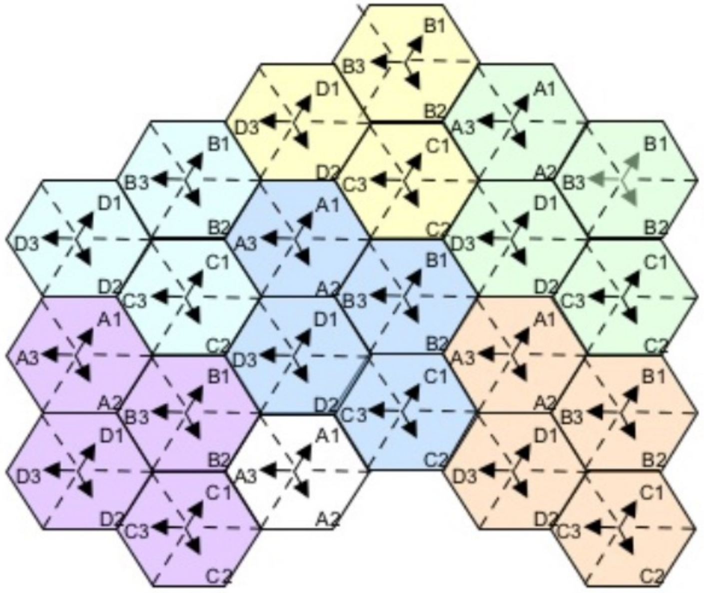


Fig.- (1.2) 4 x 3 Re-use pattern

- **ARFCN denotes a forward and reverse channel pair which is separated in frequency by 45 MHz**
  - each channel is *time shared between as many as eight subscribers using TDMA*

- https://www.cellmapper.net/arfcn?net=GSM&ARFCN=0&MCC=0

ARFCN

Band	Designation	ARFCN	f_{UL}	f_{DL}
GSM 500	GSM 450	259–293	450.6 + 0.2·(n–259)	f_{UL}(n) + 10
	GSM 480	306–340	479.0 + 0.2·(n–306)[1]	f_{UL}(n) + 10
GSM 700	GSM 750	438–511	747.2 + 0.2·(n–438)[2]	f_{UL}(n) + 30
GSM 850	GSM 850	128–251	824.2 + 0.2·(n–128)	f_{UL}(n) + 45
GSM 900	P-GSM	1–124	890.0 + 0.2·n	f_{UL}(n) + 45
	E-GSM	0–124 975–1023	890.0 + 0.2·n 890.0 + 0.2·(n–1024)	f_{UL}(n) + 45
	GSM-R	0–124 955–1023	890.0 + 0.2·n 890.0 + 0.2·(n–1024)	f_{UL}(n) + 45
GSM 1800	DCS 1800	512–885	1710.2 + 0.2·(n–512)	f_{UL}(n) + 95
GSM 1900	PCS 1900	512–810	1850.2 + 0.2·(n–512)	f_{UL}(n) + 80

Later expanded for all other tech: EARFCN

Result

Network Type	GSM (TDMA)
E/U/ARFCN	10
Band Name	GSM 900
Uplink Frequency (phone to base station)	892 MHz
Downlink Frequency (base station to phone)	937 MHz
Band Number	900
Possible Bandwidths	0.2 MHz
Sector Color	

What are the steps?

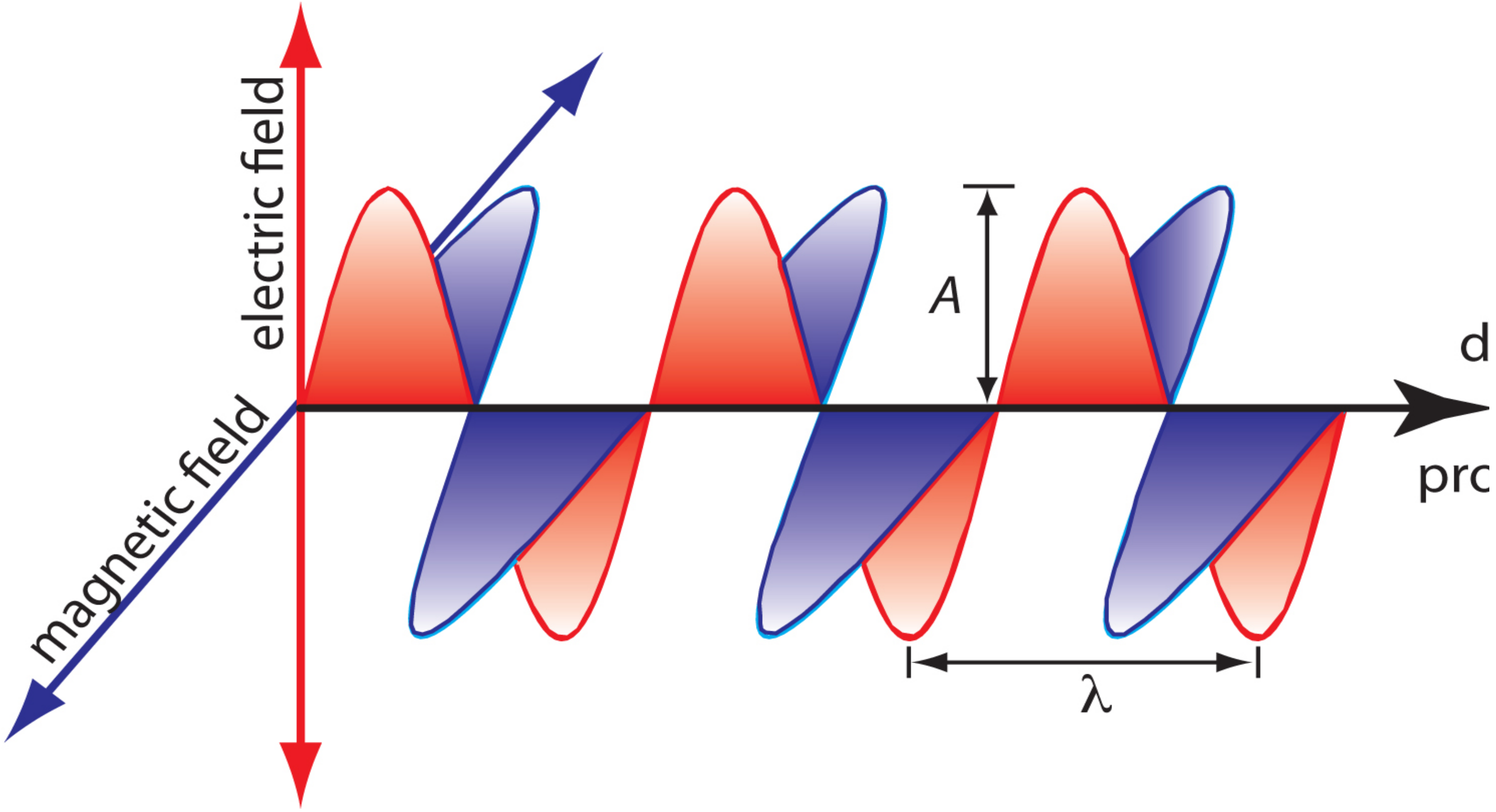
1. ~~Switch on the mobile (& infrastructure)~~
2. ~~Select a frequency band to receive & send~~
3. Pick a way to send and receive digital bits
4. Define how we are going to organize the bits
5. Listen to synchronize and get system information
6. Pick a time to send
7. Wait for a response (try again)
8. Get a control channel assigned
9. Ask to make a call
10. Authenticate
11. Get voice channel and talk
12. … (location update, release call, handover, etc …)

2G system specification

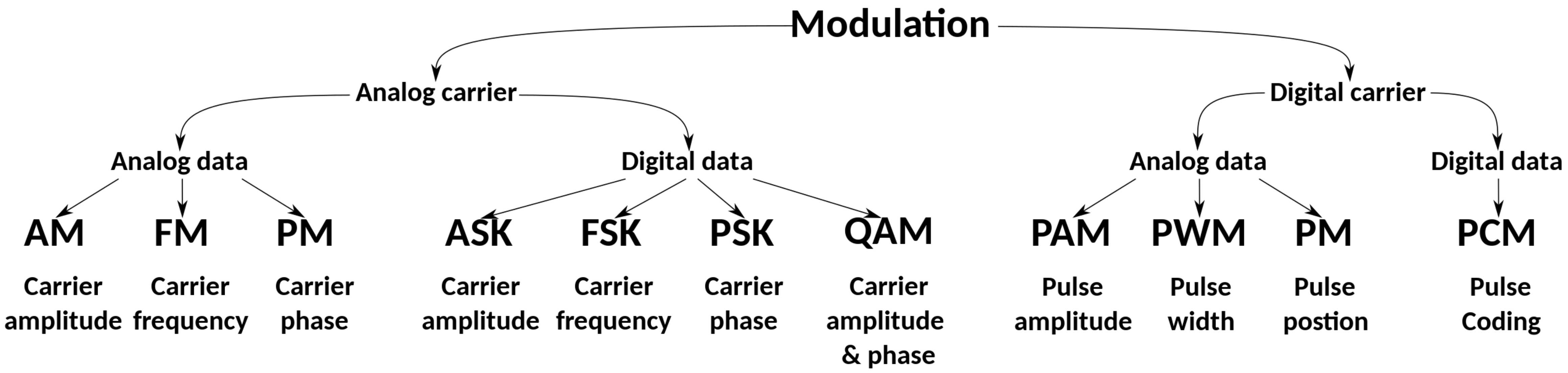
SPECIFICATION SUMMARY FOR GSM CELLULAR SYSTEM

Multiple access technology	FDMA / TDMA
Duplex technique	FDD
Uplink frequency band	890 - 915 MHz (basic 900 MHz band only)
Downlink frequency band	933 -960 MHz (basic 900 MHz band only)
Channel spacing	200 kHz
Modulation	GMSK
Speech coding	Various - original was RPE-LTP/13
Speech channels per RF channel	8
Channel data rate	270.833 kbps
Frame duration	4.615 ms

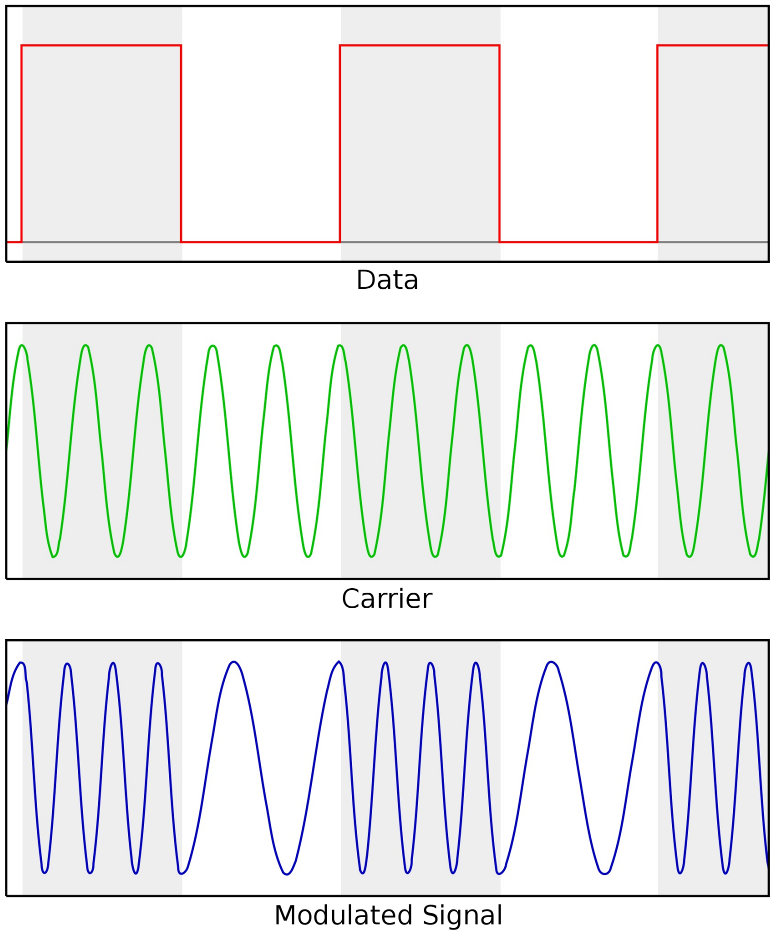
Electromagnetic Waves



Modulation zoo



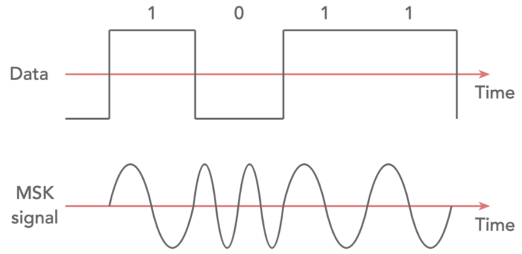
Frequency Shift Keying



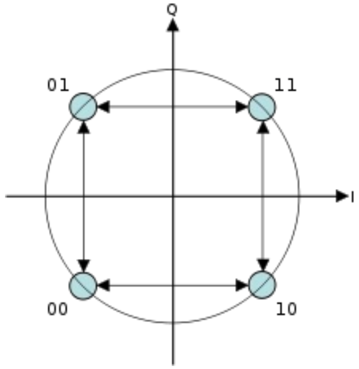
https://www.researchgate.net/publication/2575678_GMSK_in_a_nutshell

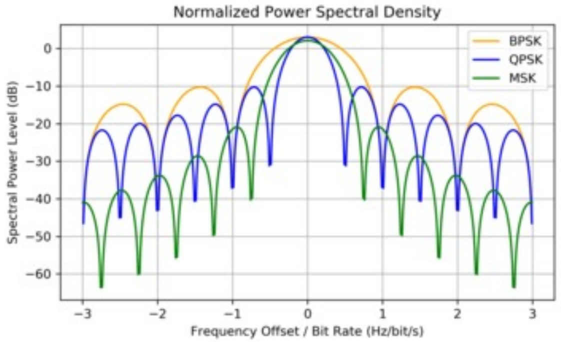
GMSK

Gaussian Minimum Shift Keying



Concept of a minimum shift keying, MSK signal





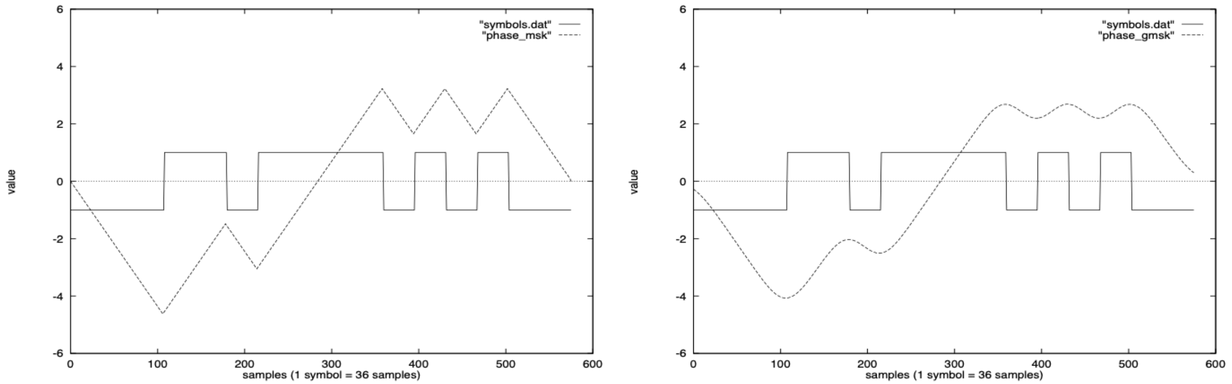


Figure 1: Symbols and phase (in radians) of MSK and GMSK signal vs samples

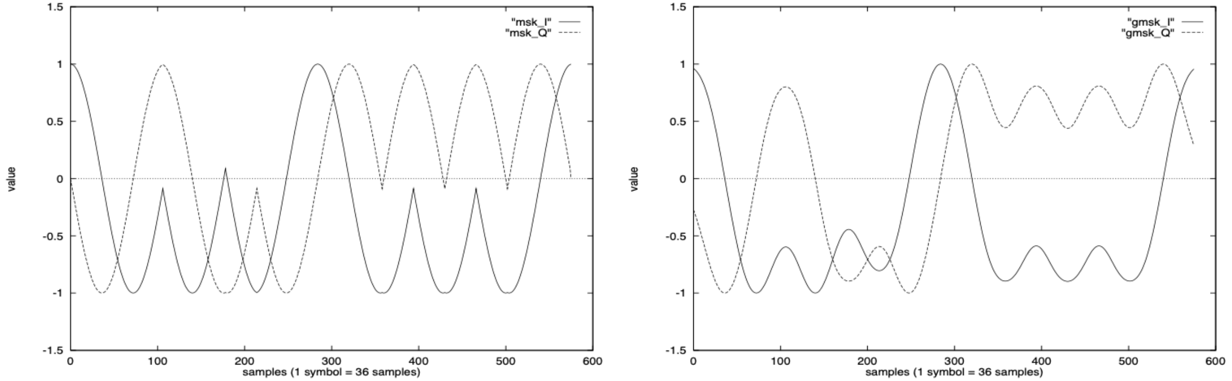


Figure 2: Baseband (I,Q) MSK and GMSK signals vs samples for fsT=36

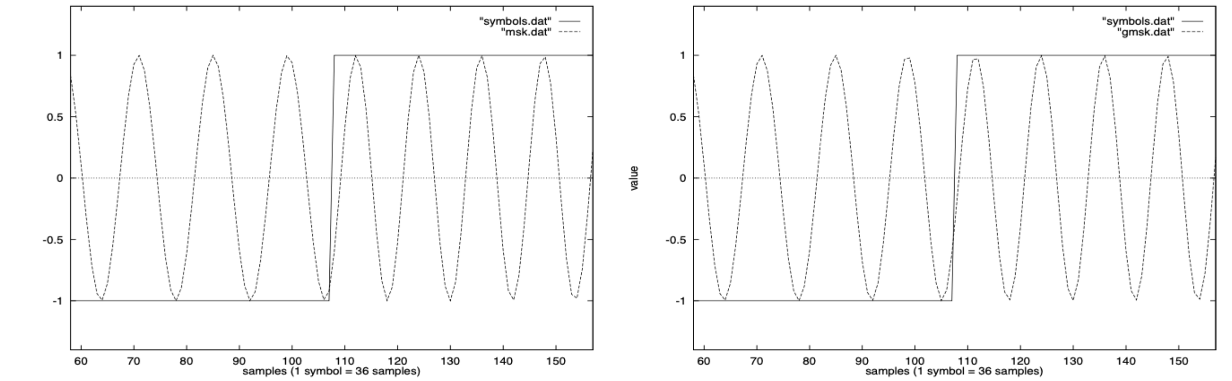
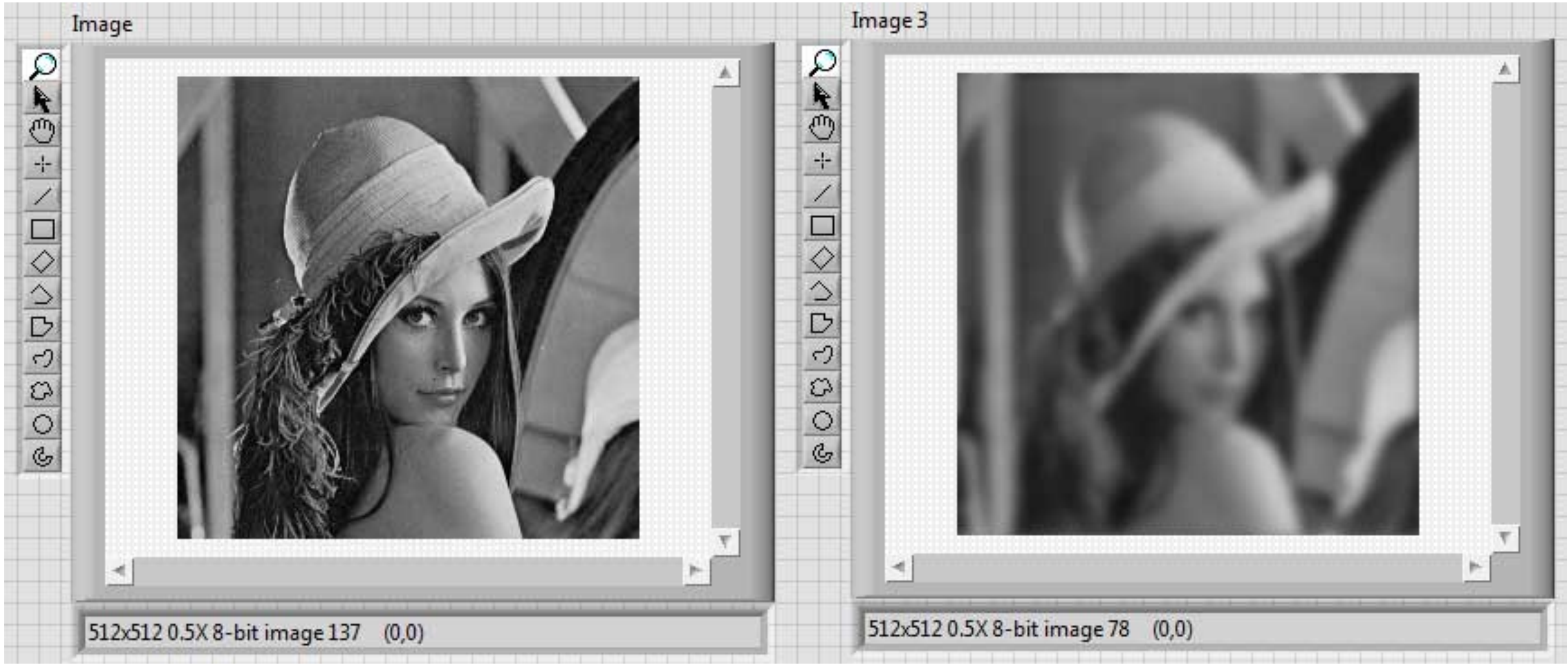


Figure 3: MSK and GMSK signal vs samples for fsT=36

Gaussian filter



What are the steps?

1. ~~Switch on the mobile (& infrastructure)~~
2. ~~Select a frequency band to receive & send~~
3. ~~Pick a way to send and receive digital bits~~
4. Define how we are going to organize the bits for multiple users
5. Listen to synchronize and get system information
6. Pick a time to send
7. Wait for a response (try again)
8. Get a control channel assigned
9. Ask to make a call
10. Authenticate
11. Get voice channel and talk
12. … (location update, release call, handover, etc …)

2G system specification

SPECIFICATION SUMMARY FOR GSM CELLULAR SYSTEM

Multiple access technology	FDMA / TDMA
Duplex technique	FDD
Uplink frequency band	890 - 915 MHz (basic 900 MHz band only)
Downlink frequency band	933 -960 MHz (basic 900 MHz band only)
Channel spacing	200 kHz
Modulation	GMSK
Speech coding	Various - original was RPE-LTP/13
Speech channels per RF channel	8
Channel data rate	270.833 kbps
Frame duration	4.615 ms

Multiple Acccess = Sending multiple signals at the same time

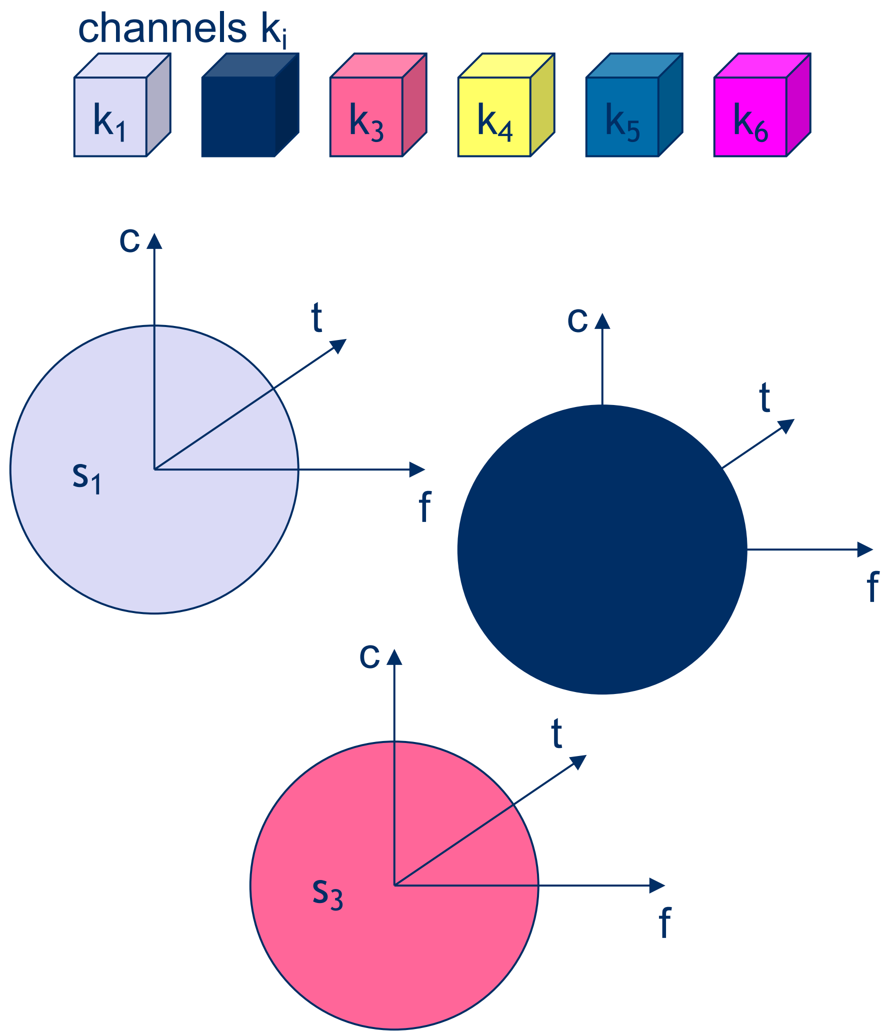
Multiplexing in 5 dimensions

- space (s)
- time (t)
- frequency (f)
- code (c)
  - Only used in 3G/UMTS, and in some random access channels
- polarisation (p)
  - Not used (for this purpose) in wireless

- **Goal: multiple use of a shared medium with minimum or no interference (think about use of highway, or in the pub).**

Space Division Multiplexing

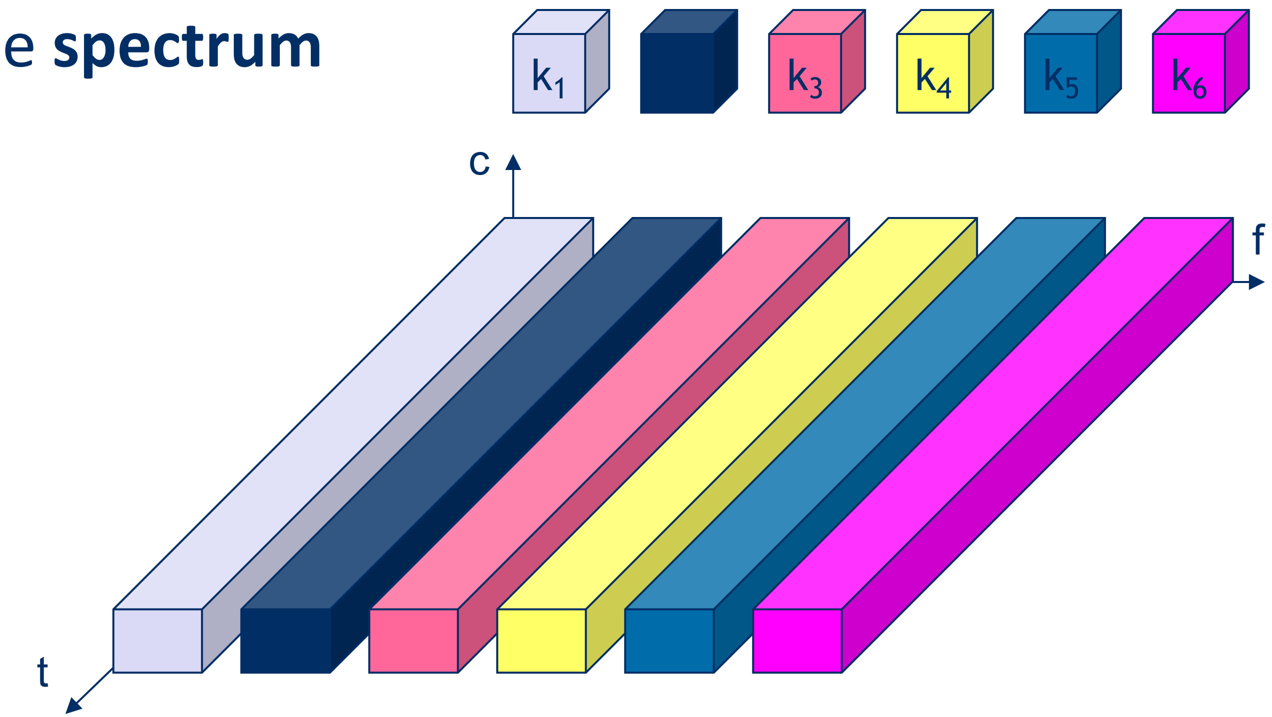
- SDM used in old analog telephone system: each subscriber is given a **separate pair of copper wires** to the LEX
- In **wireless transmission:** a separate sender for each communication channel with a wide enough distance between senders (e.g. in FM radio stations: transmission range is limited to region and many radios around the world use the same frequency without interference). In cellular, cells are a first implementation. Directional antennas can also be an implementation.



Frequency Division Multiplexing

Note: also used between operators (different chunks of 25MHz)

- **Separation** of the available spectrum into **smaller frequency bands**
- A channel gets a certain band of the **spectrum** for the **whole time**
- **Advantages:**
  - no dynamic coordination necessary
  - works also for analog signals
- **Disadvantages:**
  - waste of bandwidth if the traffic is distributed unevenly
  - inflexible
  - guard spaces to avoid frequency band overlapping



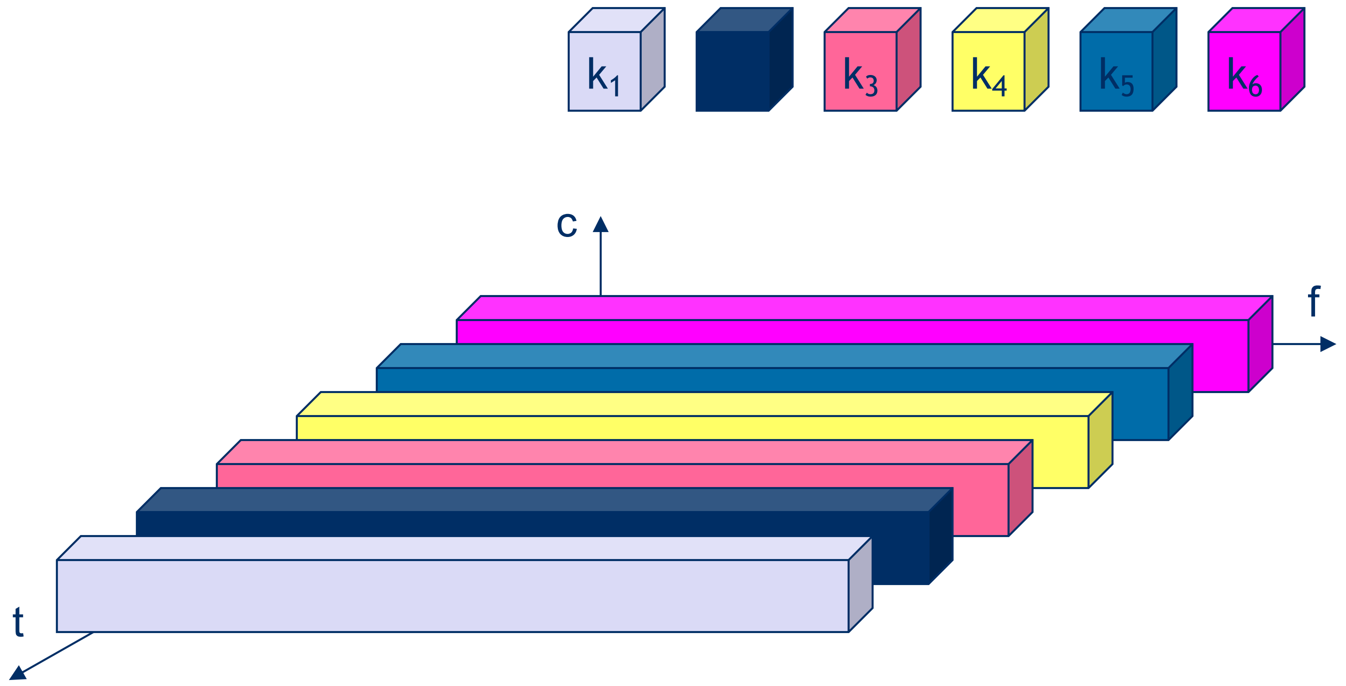
University of Antwerp
Faculty of Science

Time Division Multiplexing

- **A channel gets the whole spectrum for a certain amount of time**

- **Advantages:**
  - only one carrier in the medium at any time
  - throughput high even for many users

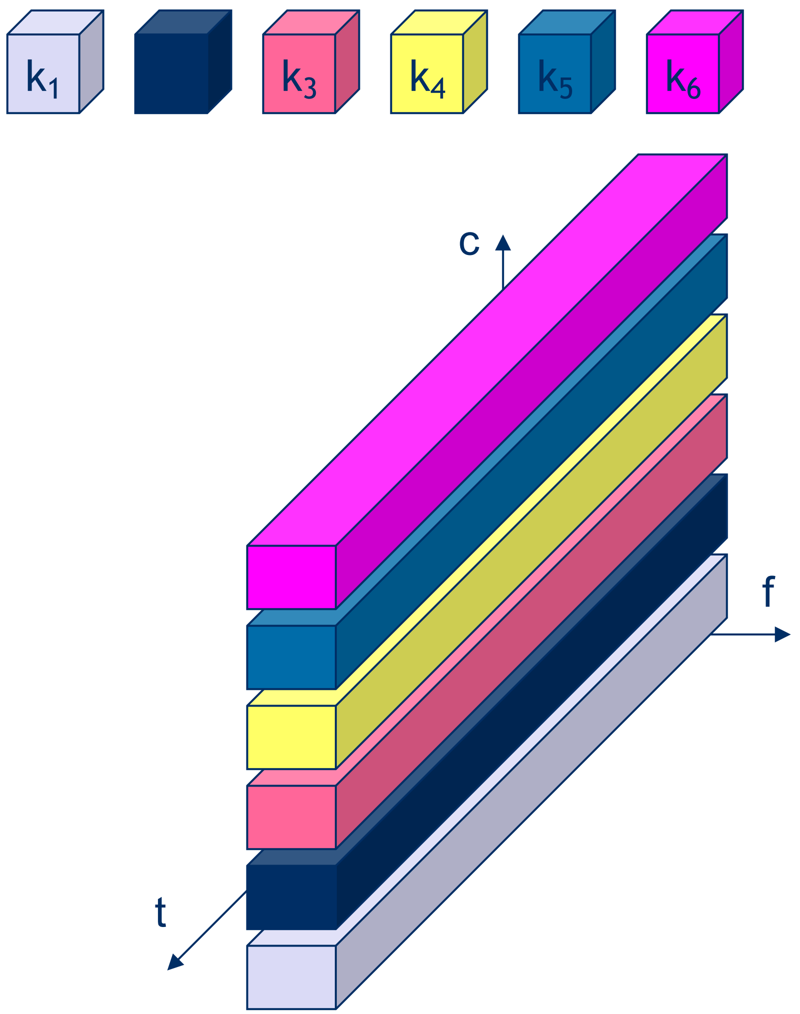
- **Disadvantages:**
  - precise synchronization necessary
  - guard time needed



Code Division Multiplexing

- **Each channel has a unique code**
  - Used in (only) 3G
- **All channels** use the **same spectrum** at the **same time**

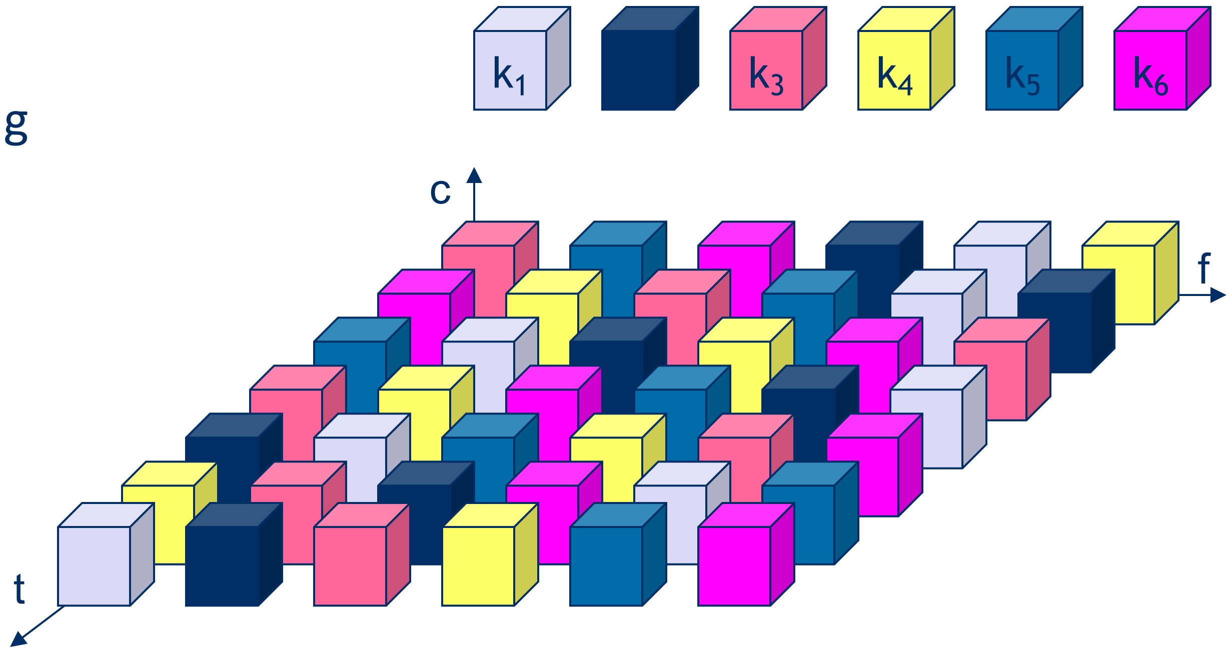
- **Advantages:**
  - bandwidth efficient
  - no coordination and synchronization necessary
  - good protection against interference and tapping
- **Disadvantages:**
  - lower user data rates
  - more complex signal regeneration
  - cell breathing
- Implemented using **spread spectrum** technology



Time and Frequency Multiplexing

- **Combination** of both methods
- A channel gets a **certain frequency band** for a **certain amount of time**
- Examples: **GSM, 4G, 5G**

- **Advantages:**
  - better protection against tapping
  - protection against frequency selective interference
  - higher data rates compared to code multiplex
- **Disadvantage:**
  - precise coordination required
  - guard bands and times



What are the steps?

1. ~~Switch on the mobile (& infrastructure)~~
2. ~~Select a frequency band to receive & send~~
3. ~~Pick a way to send and receive digital bits~~
4. Define how we are going to organize the bits for multiple users
5. Listen to synchronize and get system information
6. Pick a time to send
7. Wait for a response (try again)
8. Get a control channel assigned
9. Ask to make a call
10. Authenticate
11. Get voice channel and talk
12. … (location update, release call, handover, etc …)

2G system specification

SPECIFICATION SUMMARY FOR GSM CELLULAR SYSTEM

Multiple access technology	FDMA / TDMA
Duplex technique	FDD
Uplink frequency band	890 - 915 MHz (basic 900 MHz band only)
Downlink frequency band	933 -960 MHz (basic 900 MHz band only)
Channel spacing	200 kHz
Modulation	GMSK
Speech coding	Various - original was RPE-LTP/13
Speech channels per RF channel	8
Channel data rate	270.833 kbps
Frame duration	4.615 ms

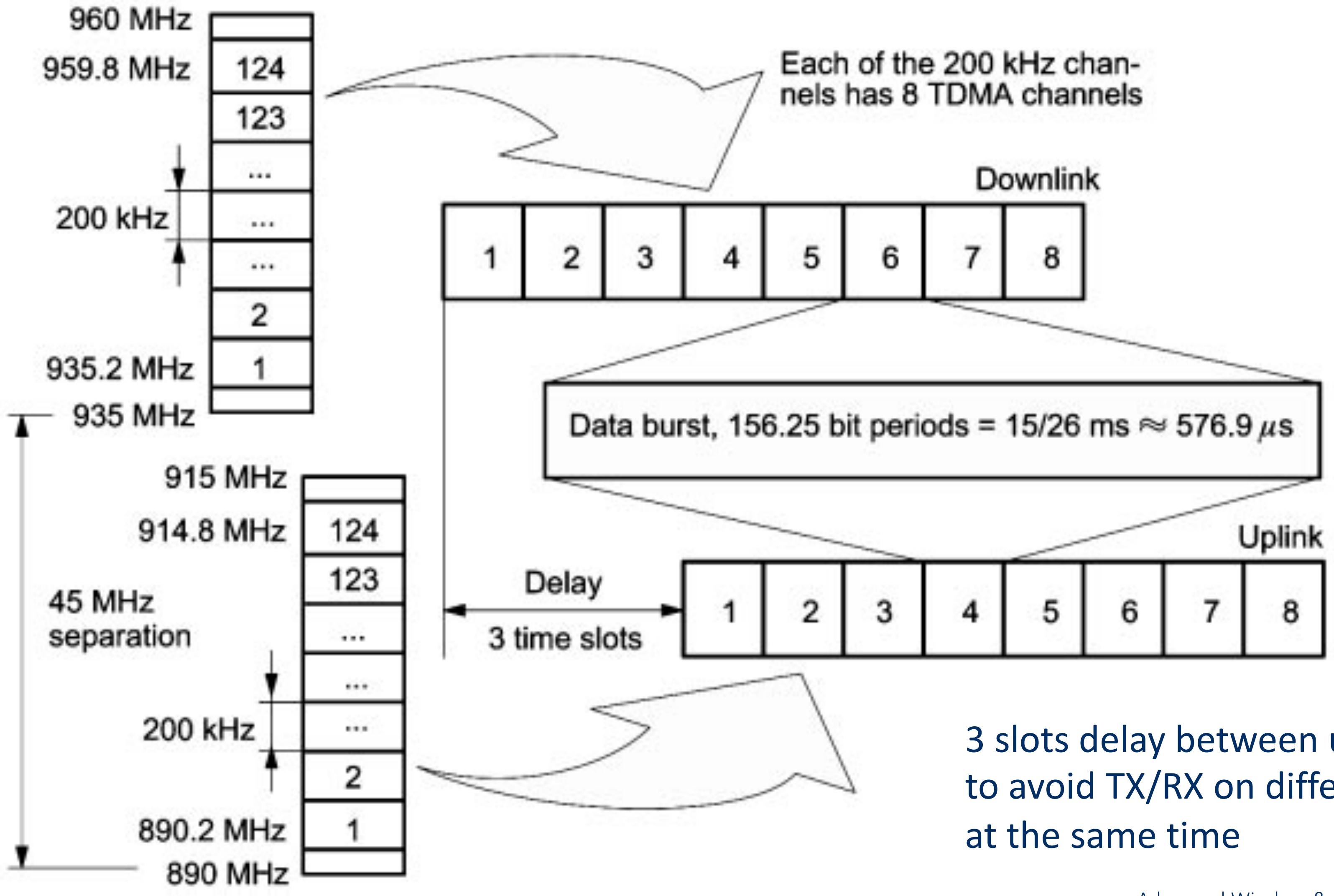
2G Multiple Access Control Scheme

- **Multiple Access in GSM : combination of**
  - Frequency Division Multiple Access (FDMA)
  - Time Division Multiple Access (TDMA)
  - Frequency hopping
- **Unit of transmission:** burst (+/- 148 bits)
- Burst is sent in Frequency/Time window
  - called a slot, with duration Burst Period
  - frequencies : every 200 kHz
  - time : every 15/26ms (~ 0.577ms)

GSM slot structure

Downlink

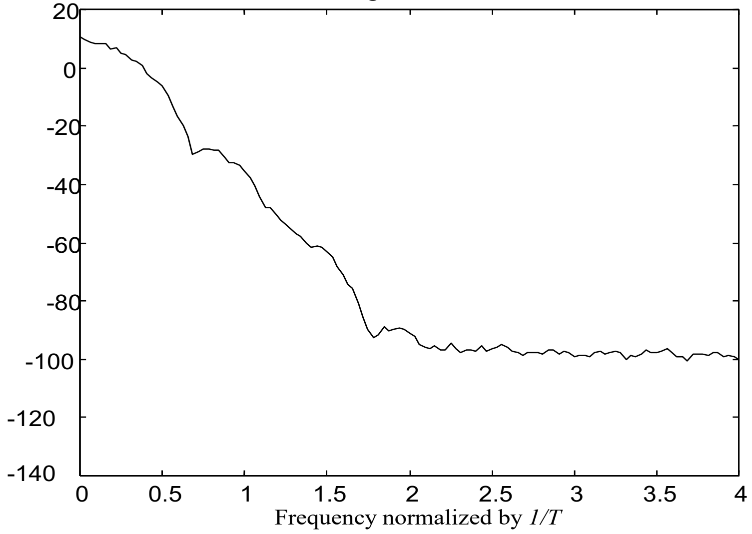
Uplink



3 slots delay between up- and downlink to avoid TX/RX on different frequencies at the same time

Capacity and link spectral efficiency

Power spectral density of the complex envelope of GMSK, *BT=0.3, fe=8, T=1.*
Logarithmic scale

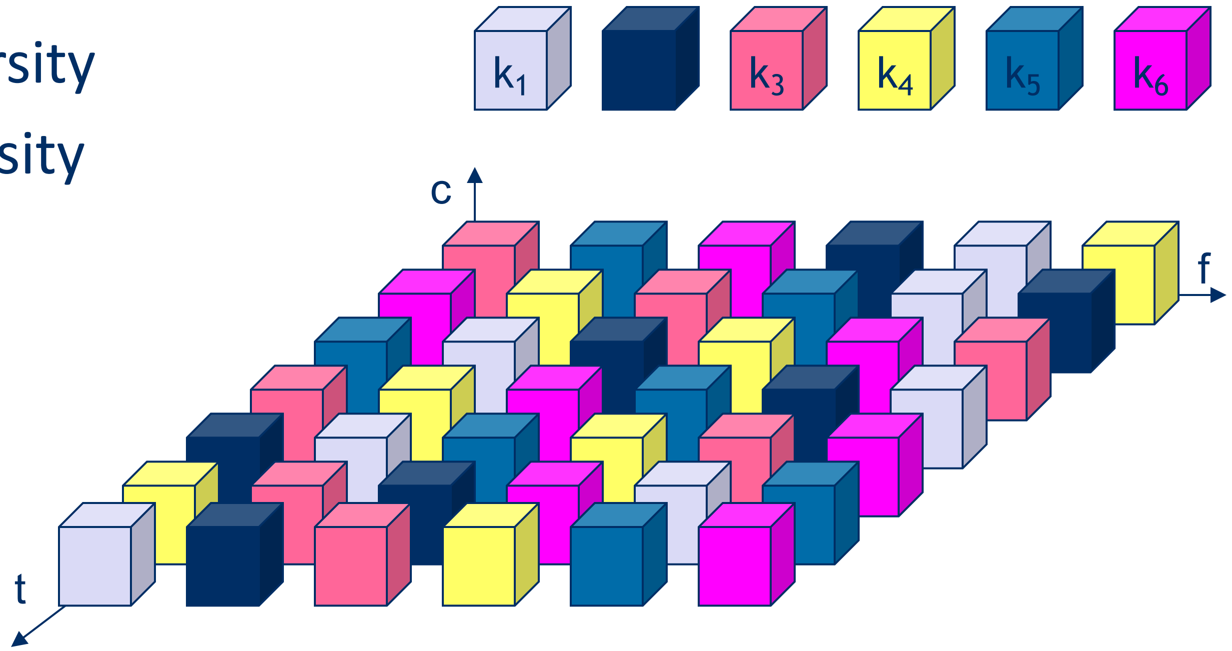


- **200 kHz** channel spacing
- **270.833 kbps** is the **max. bit rate** that avoids inter-symbol-interference
  - 148 bits per burst
- Typically, **25MHz of spectrum** divided in **125 channels** of which 124 are used
- Best possible SE = 124*270.833kbps / 25 MHz = **1.34 bits/Hz**
  - But: coding, overhead, … 148 bits in a 577µs window = 257 kbps => **1.28 bits/Hz**
  - Application note: speech after coding is 13kbps/channel => **0.52 bits/Hz**

Compare with 4G, 5G MIMO: up to 30 bits/Hz

Application to GSM

- **How concurrent users can we handle?**
  - …
- **Frequency can change during call:**
  - frequency selectivity/diversity
  - interferer mitigation/diversity



University of Antwerp
Faculty of Science

GSM frame hierarchy

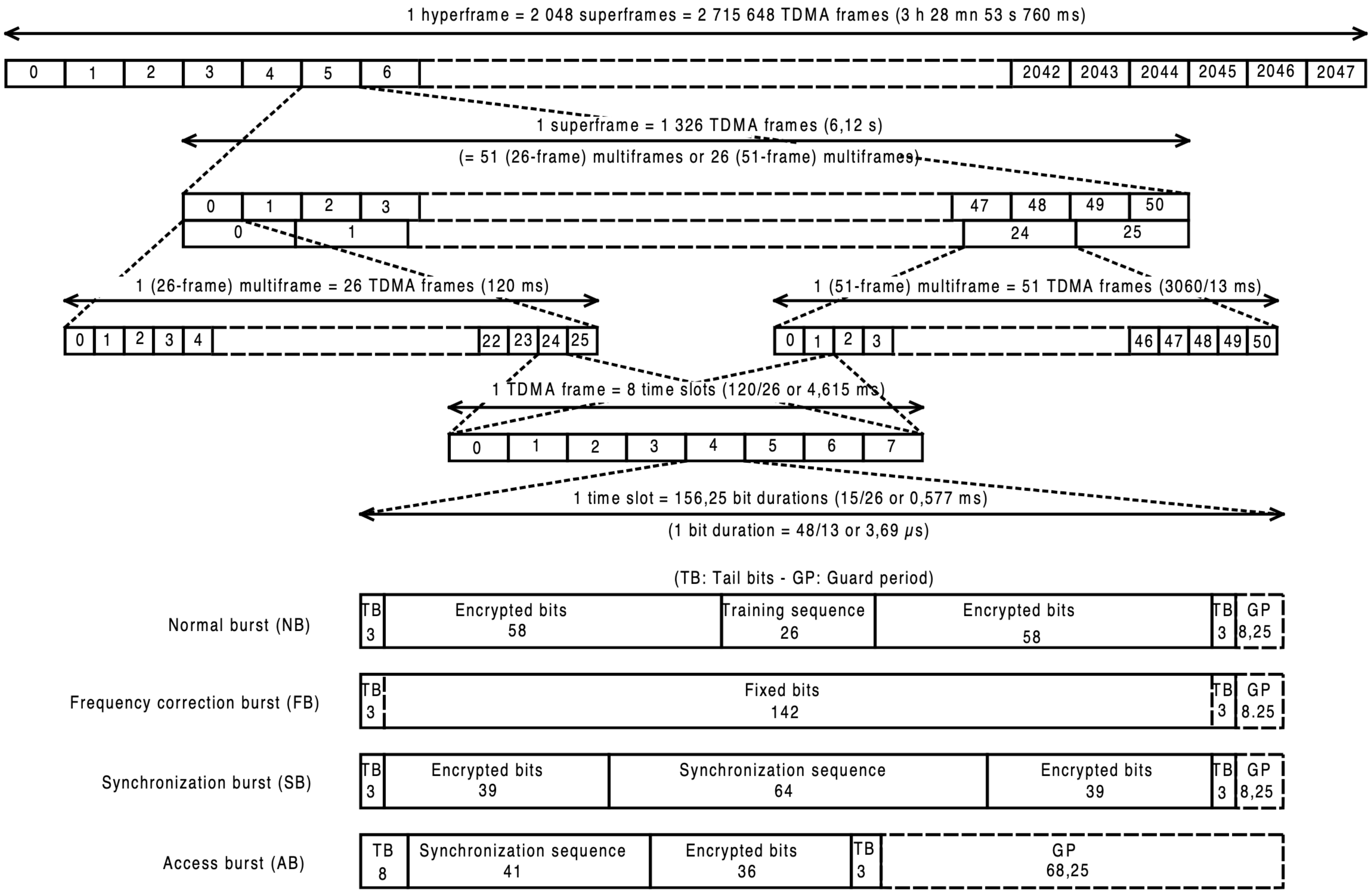
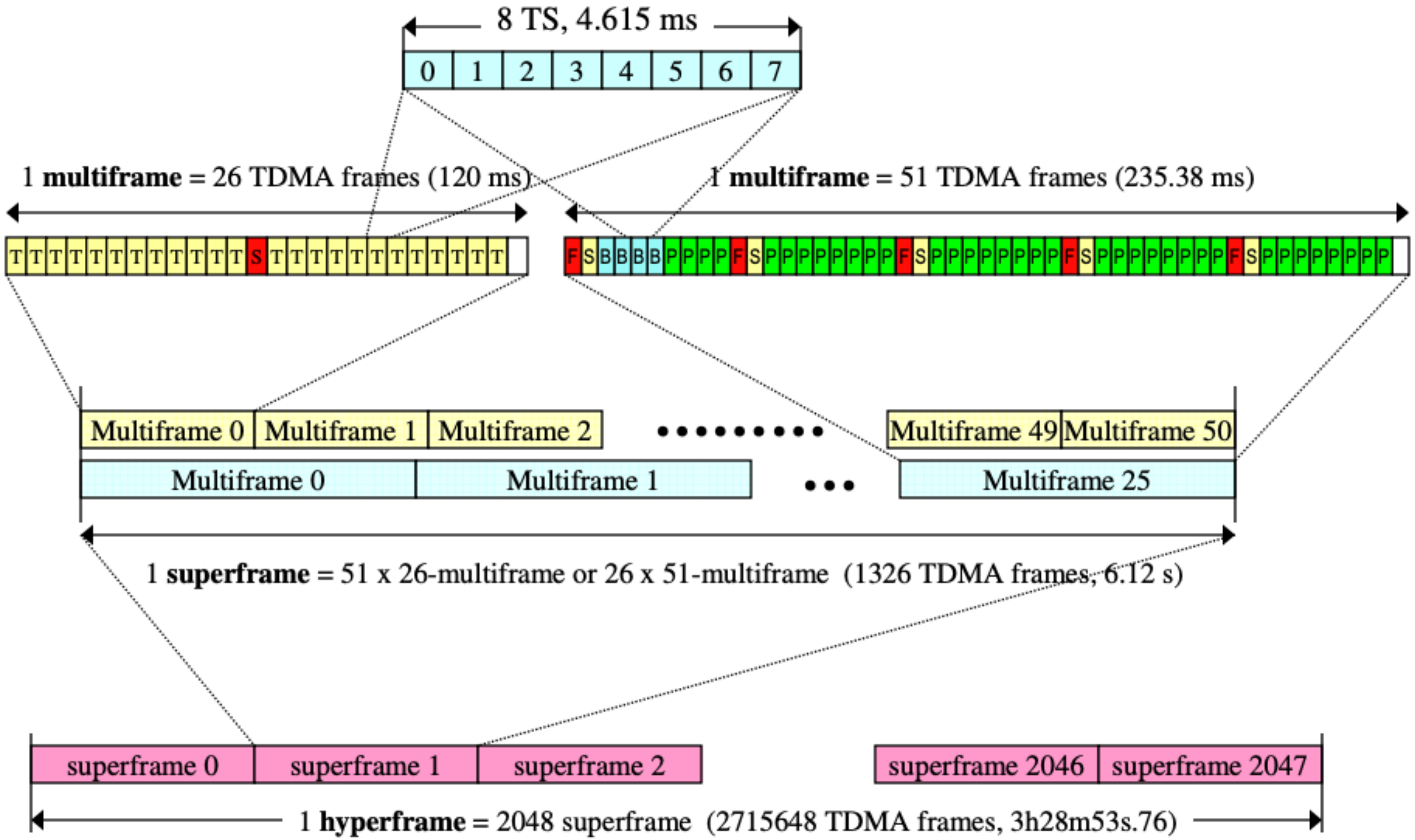
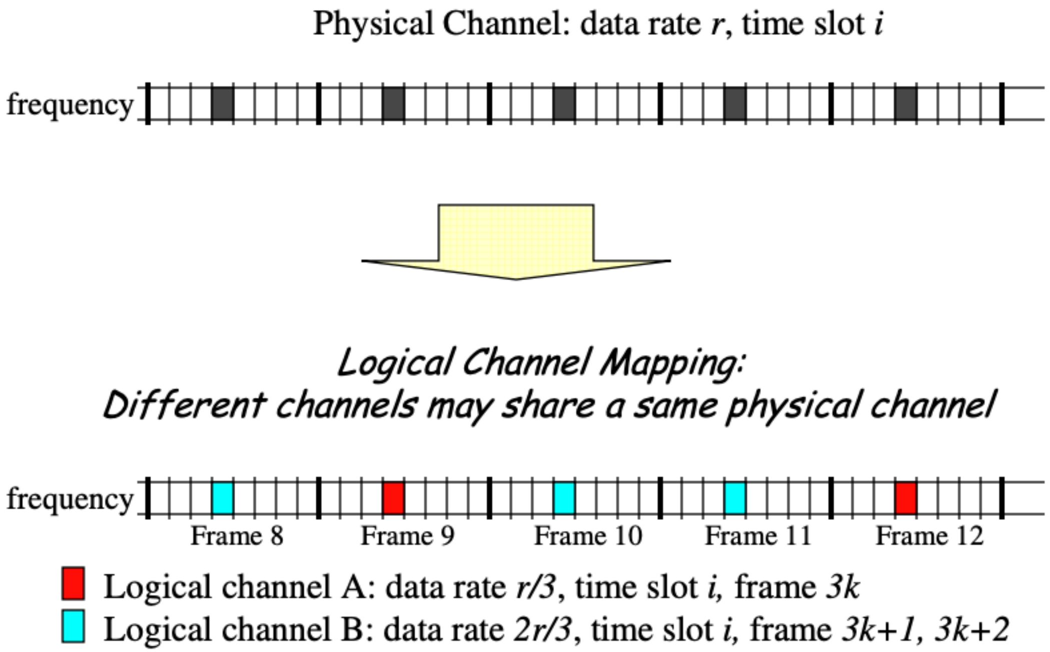


Figure 1: Time frames time slots and bursts

GSM frame hierarchy



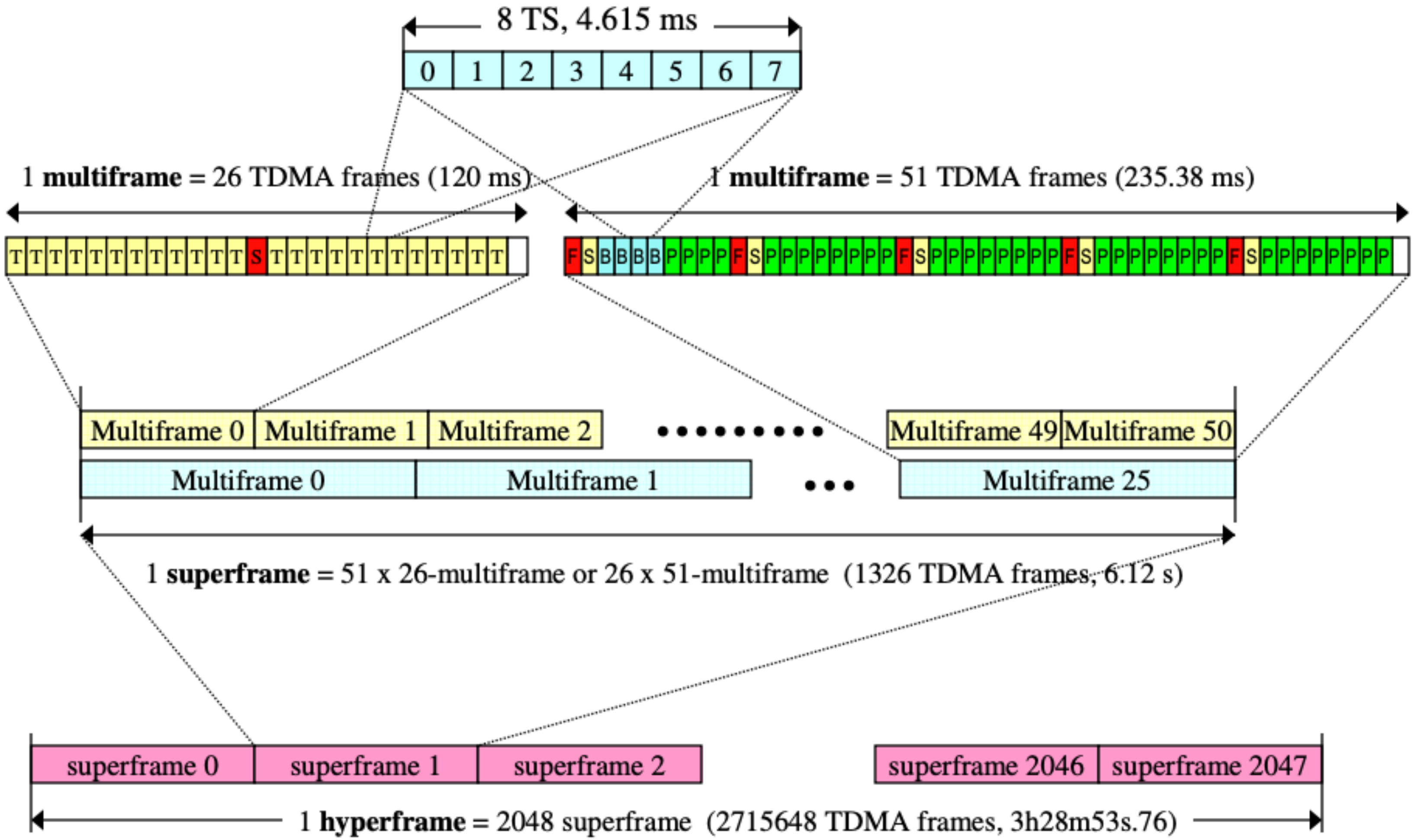
Physical and logical channels



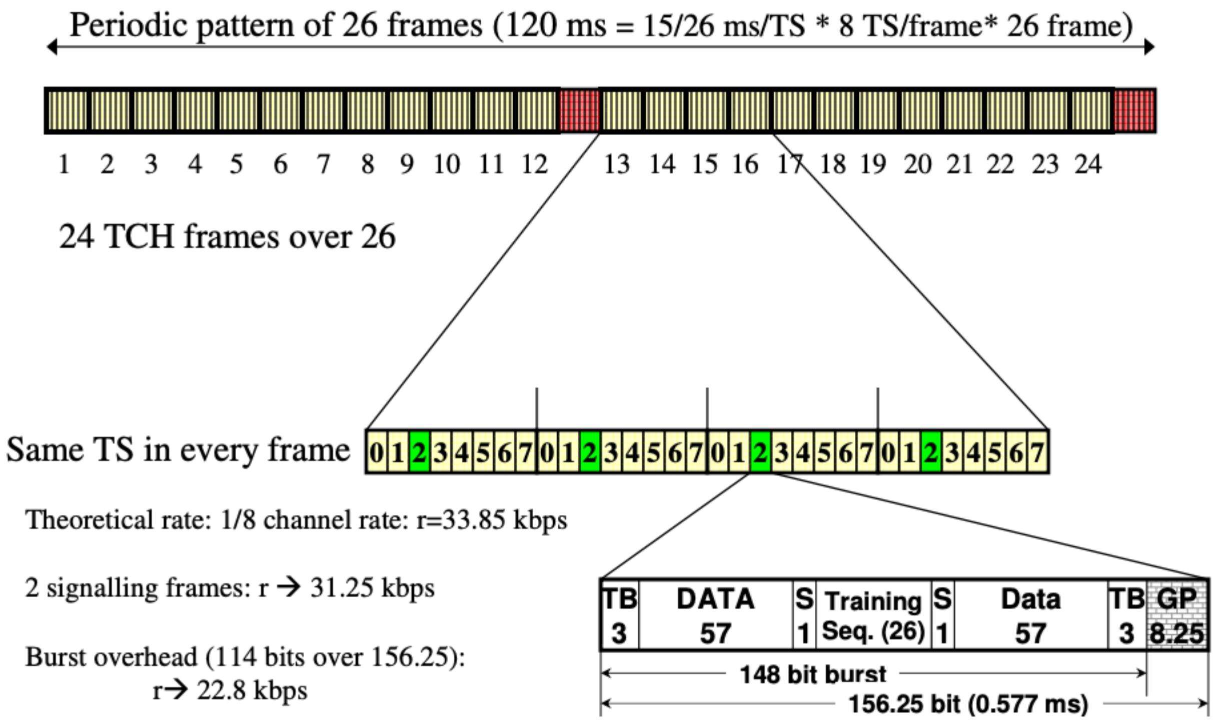
Logical channels

Traffic channel (TCH)	**TCH/F**	TCH full rate	MS←→BSS
	TCH/H	TCH half Rate	MS←→BSS
Broadcast channel	**BCCH**	Broadcast control	BSS→MS
(same information to all MS in a cell)	**FCCH**	Frequency Correction	BSS→MS
	SCH	Synchronization	BSS→MS
Common Control channel (CCCH)	**RACH**	Random Access	MS→BSS
(point to multipoint channels)	**AGCH**	Access Grant	BSS→MS
(used for access management)	**PCH**	Paging	BSS→MS
Dedicated Control channel (DCCH)	**SDCCH**	Stand-alone Dedicated control	MS←→BSS
(point-to-point signalling channels)	**SACCH**	Slow associated control	MS←→BSS
(dedicated to a specific MS)	**FACCH**	Fast associated control	MS←→BSS

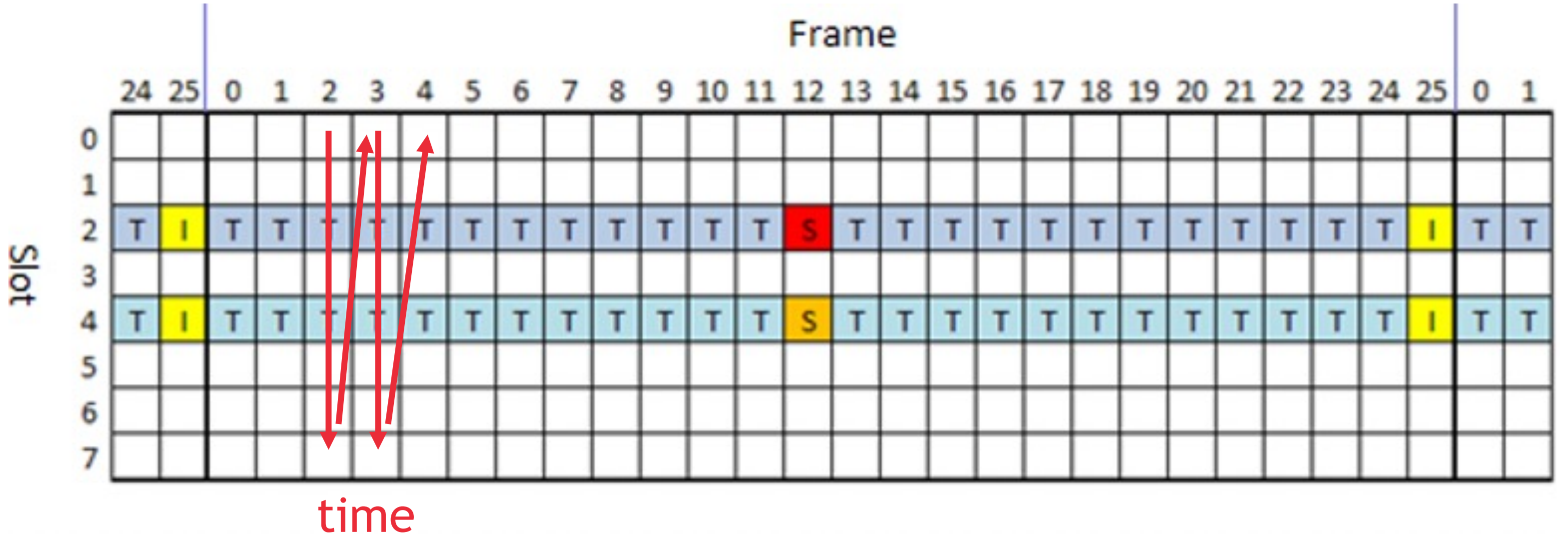
GSM frame hierarchy



Traffic channels

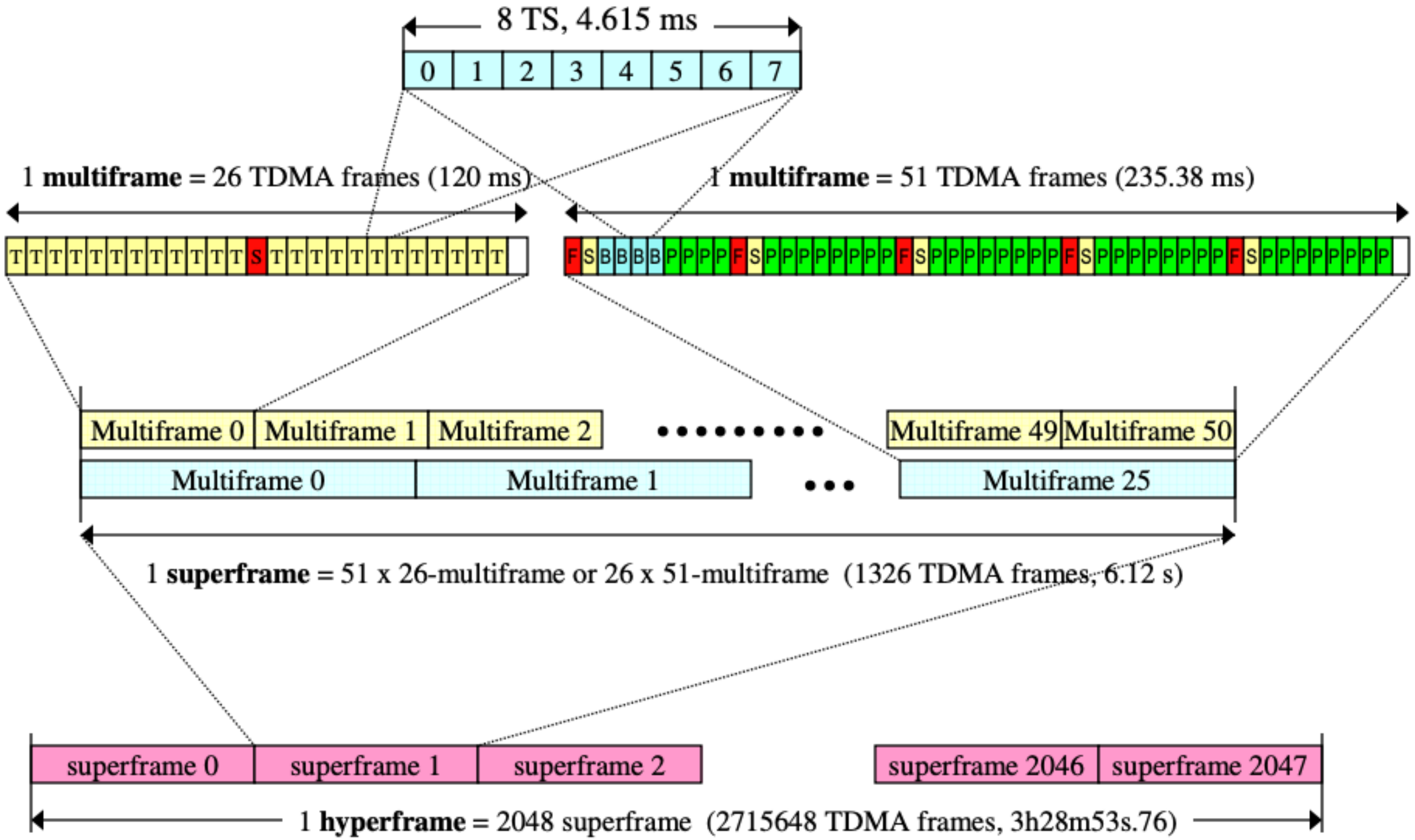


How to visualize this: at one frequency



8 physical channels
Each having multiple logical ones.

GSM frame hierarchy

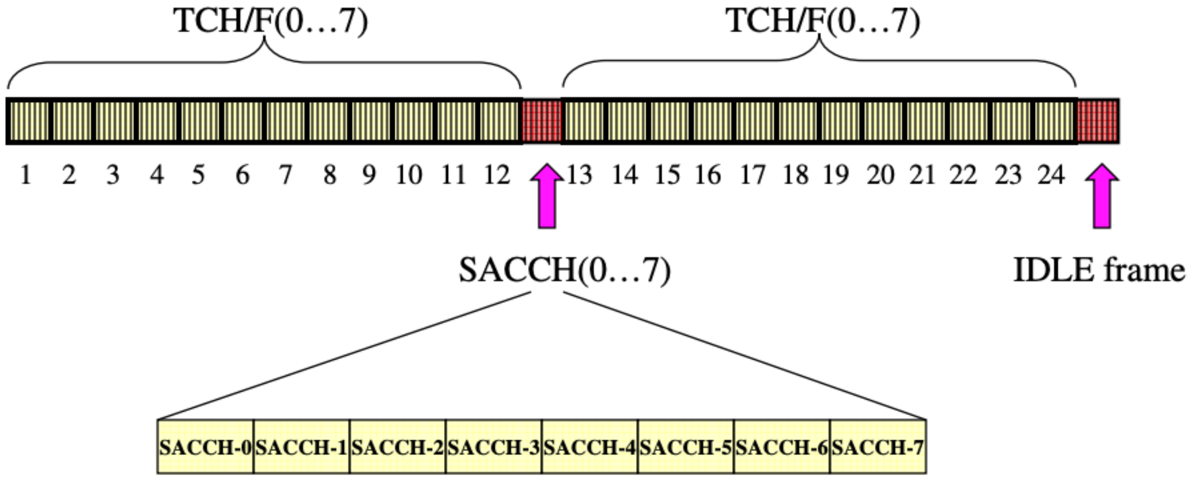


Control for a user during traffic: SACCH

➔ **Always associated to instaurated call on TCH (TCH + SACCH = TACH)**

  ➔ On the same Time Slot

➔ **Periodic (order of ½ second) time-scale information for radio link control**



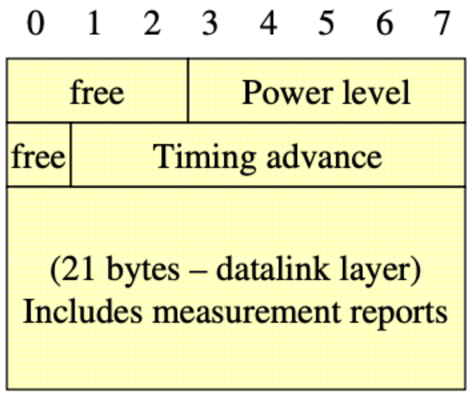
1 SACCH burst (per TCH) every 26 frames (120 ms)

SACCH?

➔ **184 bits = 23 bytes**

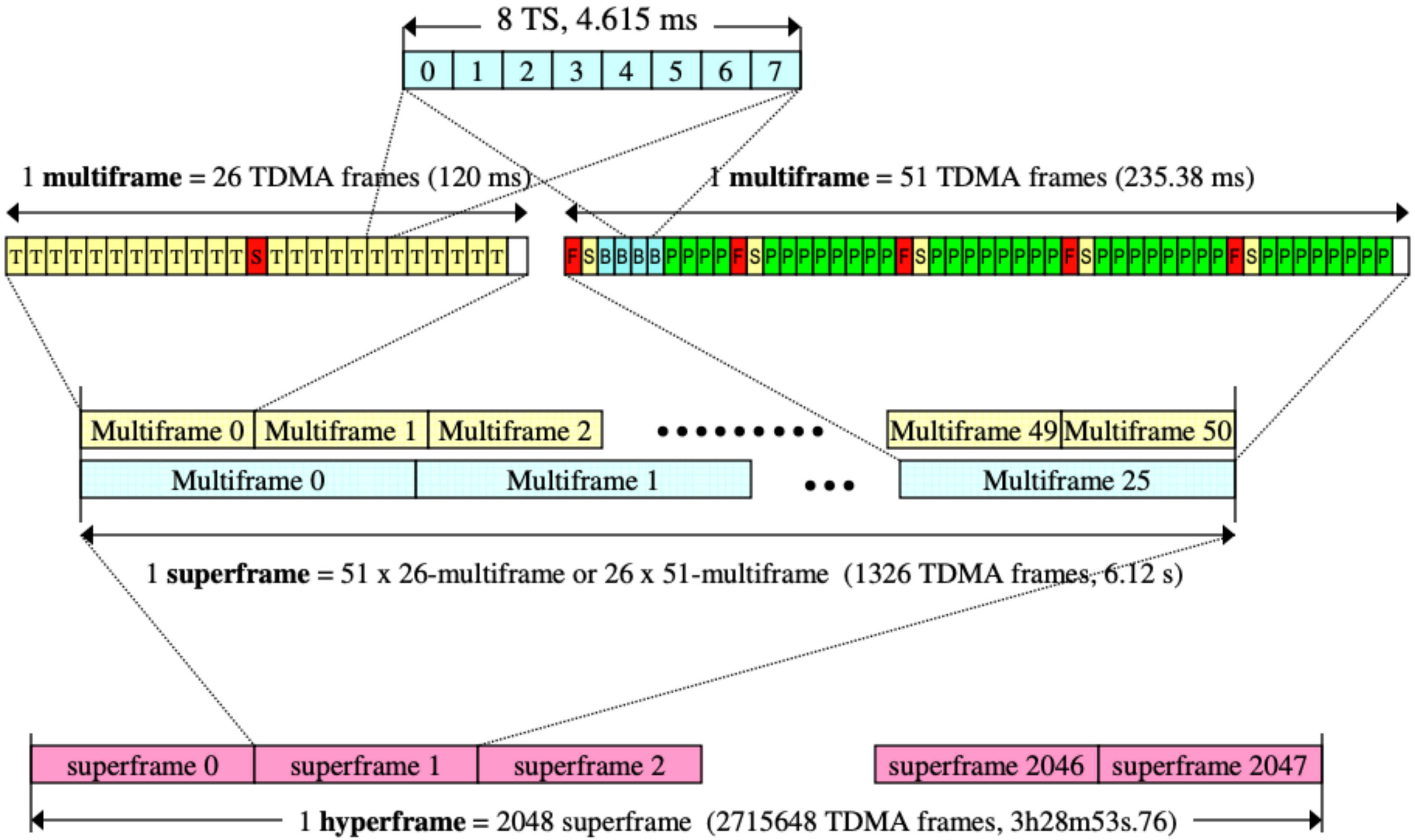
➔ **Power level**
➔ **Timing advance**
➔ **Measurement reports for link quality**
➔ **Measurement reports for handover management**

➔ **When available space: SMS**
⇨ When call in progress!



- **Power level**
  - Some MS/UE are farther, some are closer
- **Timing advance**
  - Some MS/UE are farther, some are closer
- **Measurement reports**
  - “this is what I see”
- **SMS**

GSM frame hierarchy

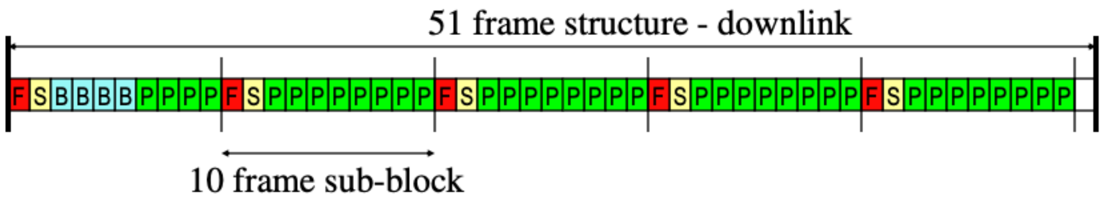


Logical channels

Traffic channel (TCH)	**TCH/F**	TCH full rate	MS←→BSS
	TCH/H	TCH half Rate	MS←→BSS
Broadcast channel	**BCCH**	Broadcast control	BSS→MS
(same information to all MS in a cell)	**FCCH**	Frequency Correction	BSS→MS
	SCH	Synchronization	BSS→MS
Common Control channel (CCCH)	**RACH**	Random Access	MS→BSS
(point to multipoint channels)	**AGCH**	Access Grant	BSS→MS
(used for access management)	**PCH**	Paging	BSS→MS
Dedicated Control channel (DCCH)	**SDCCH**	Stand-alone Dedicated control	MS←→BSS
(point-to-point signalling channels)	**SACCH**	Slow associated control	MS←→BSS
(dedicated to a specific MS)	**FACCH**	Fast associated control	MS←→BSS

Broadcast channel

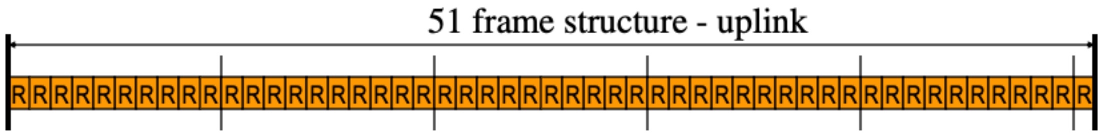
- ➔ **51 frame structure vs 26**
  - ⇨ 235.38 ms period (vs 120 ms)
- ➔ **Sub-blocks with 10 frames**
  - ⇨ Starting with Frequency Correction Channel (FCCH)
  - ⇨ Immediately followed by Synchronization Channel (SCH)
- ➔ **Other frames** **(numbered from #0 to #50):**
  - ⇨ #50 idle
  - ⇨ #2,3,4,5 BCCH
  - ⇨ Remaining: Paging (PCH) / Access Grant (AGCH) [=PAGCH]



Where is it placed?

➔ **On Downlink**

⇨ Corresponding uplink dedicated to Random Access Channel



➔ **On one frequency per cell (beacon)**

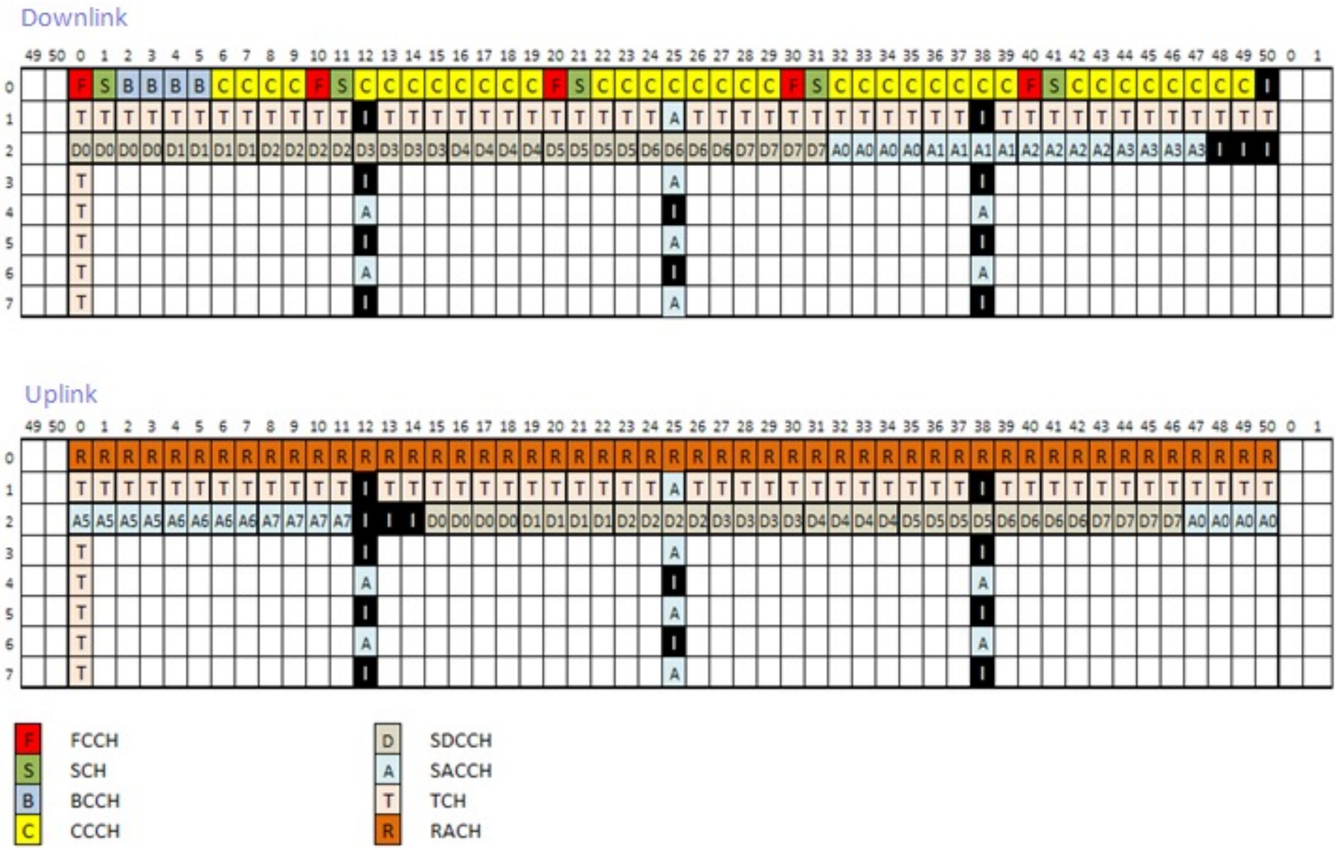
➔ **MUST BE on Time Slot #0**

➔ **Other Time slots may be used by TCH**

Provided that:

- All empty slots are filled with DUMMY bursts
- Downlink power control must be disabled

What does this look like, in reality



5 main bursts

Normal

3 start bits	58 bits of encrypted data	26 training bits	58 bits of encrypted data	3 stop bits	8.25 bits guard period

FCCH burst

3 start bits	142 fixed bits of all zeroes	3 stop bits	8.25 bits guard period

SCH burst

3 start bits	39 bits of encrypted data	64 bits of training	39 bits of encrypted data	3 stop bits	8.25 bits guard period

RACH burst

8 start bits	41 bits of synchronization	36 bits of encrypted data	3 stop bits	68.25 bit extended guard period

Dummy burst

3 start bits	58 mixed bits	26 training bits	58 mixed bits	3 stop bits	8.25 bits guard period

Data Link not just for multiplexing …

- **Data link layer improves the quality of physical layer**
  - error detection and error correction
    - parity check
    - longitudinal check
    - cyclic redundancy check
  - flow control
    - Stop-and-Wait
    - Sliding window
    - Stop-and-Wait ARQ (Automatic repeat request)
    - Go-back-N ARQ
    - Selective-reject ARQ

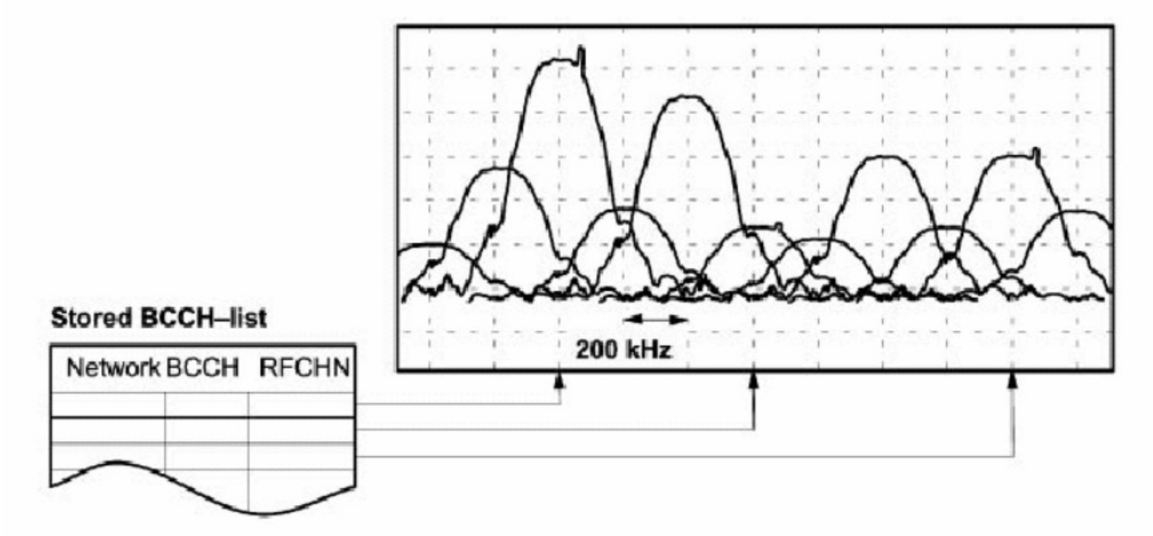
Error detection & correction

- **ISBN**
  - The two most common errors in handling an ISBN (e.g. when typing it or writing it down) are a single altered digit or the transposition of adjacent digits. It can be proven mathematically that all pairs of valid ISBN-10s differ in at least two digits. It can also be proven that there are no pairs of valid ISBN-10s with eight identical digits and two transposed digits.
- **Credit card (Luhn's)**
  - The Luhn algorithm will detect all single-digit errors, as well as almost all transpositions of adjacent digits. It will not, however, detect transposition of the two-digit sequence 09 to 90 (or vice versa). It will detect most of the possible twin errors (it will not detect 22 ↔️ 55, 33 ↔️ 66 or 44 ↔️ 77).

What are the steps?

1. ~~Switch on the mobile (& infrastructure)~~
2. ~~Select a frequency band to receive & send~~
3. ~~Pick a way to send and receive digital bits~~
4. ~~Define how we are going to organize the bits for multiple users~~
5. Listen to synchronize and get system information
6. Pick a time to send
7. Wait for a response (try again)
8. Get a control channel assigned
9. Ask to make a call
10. Authenticate
11. Get voice channel and talk
12. … (location update, release call, handover, etc …)

Listening to the broadcast channel

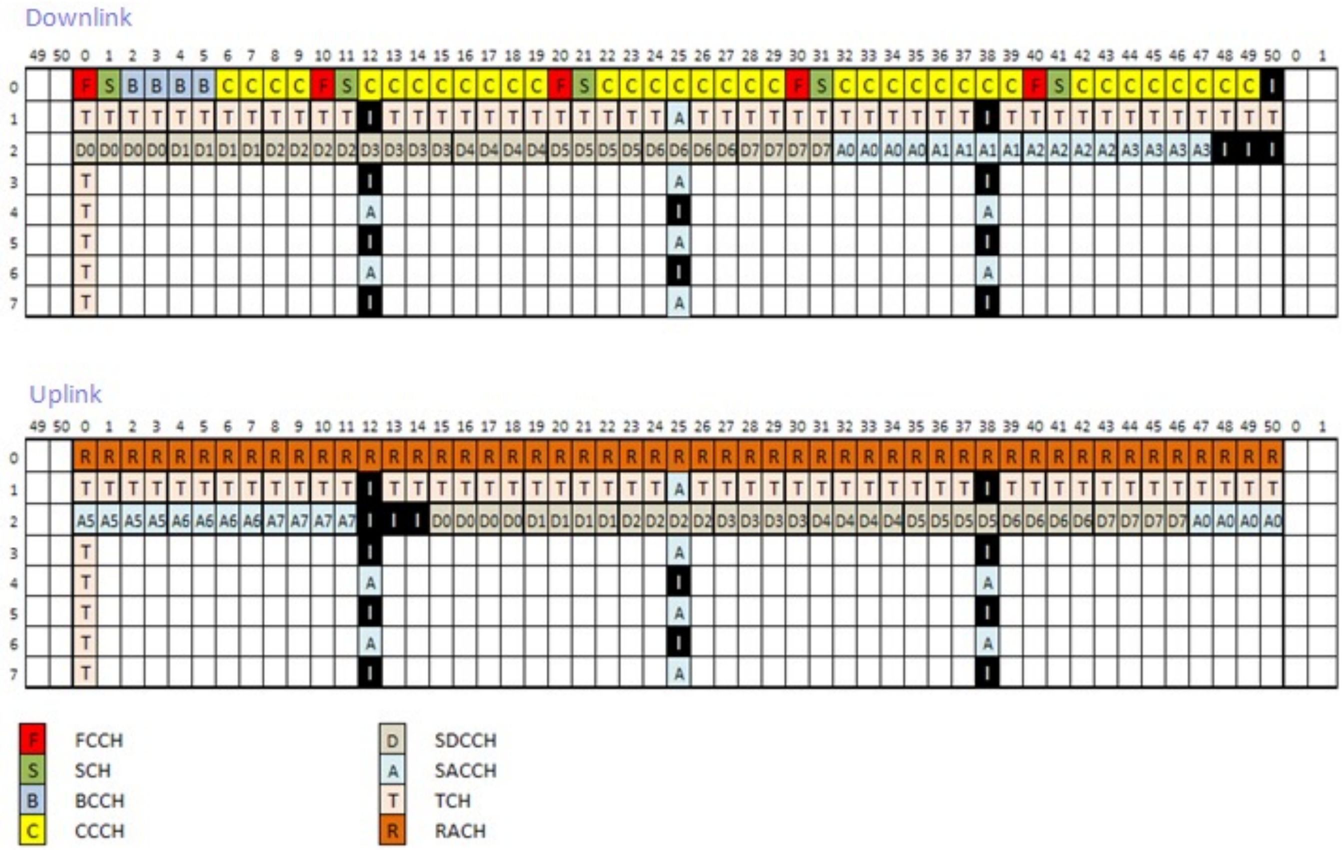


First operation when MS turned ON: spectrum analysis
(either on list of up to 32 Radio Frequency Channel Numbers of current network)
(or on whole 124 carriers spectrum)

Tune to the right frequency

- **MS will listen to strongest beacon for a pure sine wave (FCCH)**
  - Coarse bit synchronization
  - Oscillator correction
- **Then, we use the SCH burst**
  - Fine tuning of synchronization
  - Specialized sequences
- **Now we can read BCCH**
  - Parameters of the cell like RACH backoff, power, allowed, list of carriers, other BCCH, neighbors

What does this look like, in reality

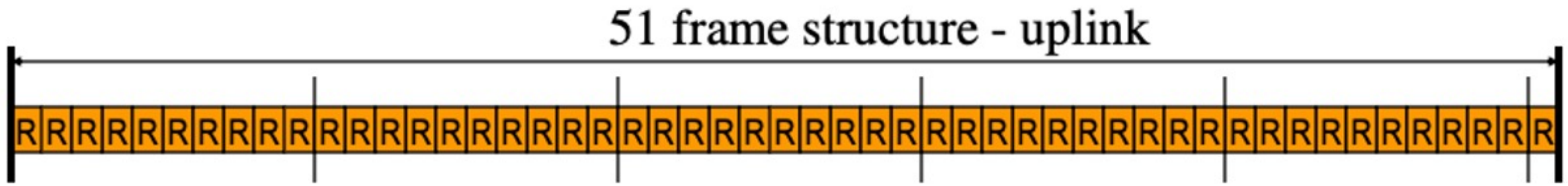


What are the steps?

1. ~~Switch on the mobile (& infrastructure)~~
2. ~~Select a frequency band to receive & send~~
3. ~~Pick a way to send and receive digital bits~~
4. ~~Define how we are going to organize the bits for multiple users~~
5. ~~Listen to synchronize and get system information~~
6. Pick a time to send
7. Wait for a response (try again)
8. Get a control channel assigned
9. Ask to make a call
10. Authenticate
11. Get voice channel and talk
12. … (location update, release call, handover, etc …)

Medium Access Control (MAC)

- **Medium Access Control (MAC) :**
  - mechanism to share the access to a common medium
- **Assumptions for further studies:**
  - N independent stations sharing common channel
  - collision when frames are sent simultaneous
  - slotted or unslotted access system
  - with or without carrier sensing
  - centralized or distributed control



Types of MAC Protocols (2)

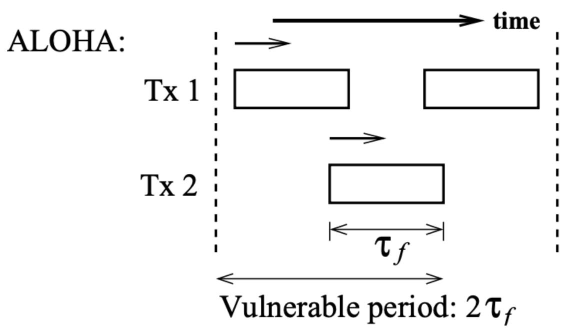
- **Random Access Protocols**
  - Transmission is random among stations
  - More than one station can transmit packets at the same time, hence, collisions are possible
  - Each station transmits at the full rate of the medium
  - In case of a collision, each node has to retransmit the packet.
  - Examples:
    - ALOHA
    - CSMA (Carrier Sensing Multiple Access) protocols

Types of MAC Protocols (3)

- **Taking-Turns Protocols**
  - Nodes take turns to transmit their packets
  - Example: polling protocol
    - One of the nodes is designated as master node
    - The master node polls each of the nodes in a round-robin fashion
  - No collisions

ALOHA Protocol : definition

- **ALOHA**
  - packet radio network (Univ. Hawaii, 1970)
  - used in many systems (e.g. GSM)
- **Operation of ALOHA**
  - station transmits when frame is available
  - station is able to check if a collision occurs
  - If a collision occurs, the station waits for a random time before sending again the frame (this waiting time is non-deterministic)



Refresher (1)

FREQUENCY

- The number of crests that pass a given point within one second is described as the frequency of the wave. One wave—or cycle—per second is called a Hertz (Hz), after Heinrich Hertz who established the existence of radio waves. A wave with two cycles that pass a point in one second has a frequency of 2 Hz.

WAVELENGTH

- Electromagnetic waves have crests and troughs similar to those of ocean waves. The distance between crests is the wavelength. The shortest wavelengths are just fractions of the size of an atom, while the longest wavelengths scientists currently study can be larger than the diameter of our planet!

ENERGY

- An electromagnetic wave can also be described in terms of its energy—in units of measure called electron volts (eV). An electron volt is the amount of kinetic energy needed to move an electron through one volt potential. Moving along the spectrum from long to short wavelengths, energy increases as the wavelength shortens. Consider a jump rope with its ends being pulled up and down. More energy is needed to make the rope have more waves.

Refresher (2)

- **bandwidth**—the range of a channel's limits; the broader the bandwidth, the faster data can be sent
- **bits per second (bps)**—a single on-off pulse of data; eight bits are equivalent to one byte
- **frequency**—the number of cycles per unit of time; frequency is measured in hertz (Hz)
- **kilo (k)**—kilo is the designation for 1,000; the abbreviation kbps represents 1,000 bits per second
- **megahertz (MHz)**—1,000,000 hertz (cycles per second)
- **milliseconds (ms)**—one-thousandth of a second
- **watt (W)**—a measure of power of a transmitter

$$\Delta P_{dB} = 10\log_{10}\frac{P_2}{P_1} = 20\log_{10}\frac{A_2}{A_1}$$

$$P_{dBm} = 10\log_{10}\frac{P}{1\text{mW}}$$

$$c = v_{light} = 300.000 \text{ km/s}$$
$$= 300 \text{ km/ms} = \frac{\lambda}{f}$$

- **frequency band**—The frequency range specified for GSM is 1,850 to 1,990 MHz (mobile station to base station).
- **duplex distance**—The duplex distance is 80 MHz. Duplex distance is the distance between the uplink and downlink frequencies. A channel has two frequencies, 80 MHz apart.
- **channel separation**—The separation between adjacent carrier frequencies. In GSM, this is 200 kHz.
- **modulation**—Modulation is the process of sending a signal by changing the characteristics of a carrier frequency. This is done in GSM via Gaussian minimum shift keying (GMSK).
- **transmission rate**—GSM is a digital system with an over-the-air bit rate of 270 kbps.
- **access method**—GSM utilizes the time division multiple access (TDMA) concept. TDMA is a technique in which several different calls may share the same carrier. Each call is assigned a particular time slot.
- **speech coder**—GSM uses linear predictive coding (LPC). The purpose of LPC is to reduce the bit rate. The LPC provides parameters for a filter that mimics the vocal tract. The signal passes through this filter, leaving behind a residual signal. Speech is encoded at 13 kbps.