Contents

1. Mobile network architectures

- Access, core, differences, similarities
- Calling, data, additional services (SMS)
- Radio, radio controller, closer switching, (internet switching), packet and circuit networks connected, later: controller and radio joined, 5g virtualised, built on each other

2. Data communication in mobile networks

- Data communication based on different primary methods; GPRS/EDGE built on current voice transfer (GSM, FDMA/TDMA), UMTS improved by using WCDMA, LTE improved by using OFDMA to improve spectral usage. 5G NR uses OFDMA but with different wavelengths, numerologies etc.
- 75 kbit/200kbit, 2-10Mbit, 100-1000Mbit, 1-10Gbit. Difference in formatting scheme makes a huge difference on capacity. E.g. UMTS using WCDMA which improved on the old technologies by a huge factor, but this technology has some limitations; interference, near/far, synchronization in both UE and node. LTE improved this by using OFDMA which also added extra capability of sharing capacity. Since LTE is only packet based, it is easy to share capacity in this (also a lot of PRB instead of time slots). In 5G, extra wavelengths are added next to LTE wavelengths, which also increases capacity.
- Near/far, frequency loss, power requirements (5G BWP)

3. GPRS & EDGE

- Both packet and circuit networks. BTS with BSC, connected to SGSN and MSC. Only difference between them is in the air. Traffic mostly routed to home GGSN, even while roaming. Separate attach/detach for voice & data to handle different capabilities in UE. States are kept for each UE (idle, standby, ready). After data handshake, PDP context established. Mobility handled by UE based on error rate (3 different modes). Takes 1-2s. Both routing area changes and location area changes are told to the network (location area = other SGSN).
- FDD with each frequency giving 8 timeslots. These timeslots can either be reserved data, reserved voice or dynamic (voice most important). A lot of different multislot classes exist (how many RX, how many TX, how many added). Different encoding schemes impact bitrate but improve risk of bit errors. Time slots can also be aggregated to improve data rates (as

in HSCSD). EDGE improves this bitrate to ≈ 200kbit with modulation format, incremental redundancy and coding schemes (8-PSK instead of GMSK). Different channels for different use cases: data channels, control channels. 4 TS in 52 frame for timing advance, power control, measurements. 4 TS every 20ms = 1 block (smallest possible), 12 of these in 240ms period. For uplink: access to data channel can be requested on random access channel. In GSM, SMS treated as control, in GPRS/EDGE treated as data.
- Network operator has to plan which reselection method is used, routing/location areas, number of frequency pairs used.

4. UMTS fundamentals

- UMTS uses WCDMA so units can talk on same frequency - also allows frequency reuse between cells. Bits are encoded into "chips". How many chips per bit depends on spreading factor. This adds processing gain, so if not as much bitrate is needed, the antenna is gained. Things like multipath diversity are also no longer problems - rake receivers combat these. This makes for a robust and flexible radio access method, however it is limited by interference and needs complex power control (expensive in UE). Also cuts down on frequency planning. All in all FDD.
- Number of users depends on distance, current usage, connection requirements. More capacity can be added with more frequencies. Each UE uses some part of a spreading code tree. To handle mobility: during a call, proper handover is done. Outside of call, update area. Handover decisions made by RNC (network). Handover can be soft, softer, hard. Soft: UE has set of active connections. In DL: mobile receives frames from more cells. In UL: RNC receives from more cells and selects best. Softer handover: handover between different areas of same cell. Easily dealt with by rake receiver. Hard handover between cells, frequency bands, FDD/TDD. MSC/SGSN handle mobility states (detached, idle, connected). Mobiles also placed in RRC states: not connected, connected and ready, connected but paging needed.
- Architecture of UMTS basically the same as EDGE; RNC controls base stations, connected to SGSN and MSC, connected to each other. Core still PS or CS.

5. UMTS evolution: HSPA

- Bundles R99 codes/channels, adds 16 QAM, changes modulation/coding on the fly based on feedback from terminal. HARQ (Stop and Wait) between UE and Node B - faster than relying on transport protocol. Network decides for each 2ms timeslot which UE's receive data (random fairness). Decision based on quality, capability, resources, buffer, QoS. HSPA Evolution uses 64QAM DL, 16QAM UL for increased bit-rates, MIMO, dual band.
- UMTS bit rate up to 2Mbit, HSDPA MINIMUM 2Mbit up to 84Mbit - 5.2Mbit UL. Increases cell throughput, decreases latency. Max bitrate with 64QAM and MIMO.
- Main channel SF=16, fast scheduling from BTS, adaptive modulation, QPSK, 16QAM, 64QAM, no soft handover, HARQ. Also has signalling channel, HS-DPCCH for sending quality + ACK. DL Signalling channel: UE listens to up to four, terminal specific masking, sends coding, modulation, redundancy, ARQ information. UL Channels: E-DCH for HARQ, scheduling, retransmission. E-HICH for HARQ info. E-AGCH for enhanced access grant channel. E-DPCCH for retransmission information. Scheduling also controlled by Node B by UE request. Both scheduled and non-scheduled grants exist.
- Increases bit-rates with adaptive modulation and coding, L1 HARQ DL, L2 UL, Node B based scheduling. Also has new shared channel. No longer has fast power control. Instead of WCDMA, use timeslot based access.

6. LTE fundamentals

- Unlike older generations, the radio controller is integrated into the cell itself. There is also a direct connection to the GGSN instead of passing through SGSN - which is then renamed MME (Mobility Management Entity). The GGSN is renamed sGW. This passes to PDN-GW which has an internet connection. This means that all radio functionality is centralised in the eNode B, thereby clearly seperating control and user plane functions. The core network

consists of the sGW and pGW. The control plane consists of MME, HSS, PCRF. Services are handled by IMS (e.g. VoLTE).
- Duplexing is done with both FDD and TDD. Downlink uses OFDMA, UL uses SC-FDMA since OFDMA means more power usage in UE. 22 frequency bands are defined; sub 1, around 2-2.5. Small subcarriers allow to choose based on subcarrier performance. Each subcarrier is 15kHz from the next. Because of orthogonality, no guard band needed. Compared to 5MHz in WCDMA. Resources assigned as PRB, 12 carriers of 1ms divided into 14 symbols, 180kHz total. Each carrier has adaptive modulation and coding, QPSK, 16QAM or 64QAM. Max total system bw is 20MHz. Scheduler runs every 1ms in eNode B. The frames in a PRB also contain control, sync, and reference channels. Uplink scheduling based on request for access, random access channel available if no scheduled permission. 8 parallel L2 HARQ SAW. Also possibility for MIMO, 2x2 or 4x4.
- Bit rate depends on number of PRBs allocated, UE capability, radio link quality (coding, modulation), MIMO, overhead. E.g. with 1200 carriers (20MHz), 64QAM, 14 ksym/s, 100Mbps total - minus reference carriers. Possible to get 1200 DL with 8x8 MIMO, 64QAM. No dedicated channels exist, only common shared.

7. LTE procedures & services

- Handover is controlled by the network, assisted by measurements from UE. Based on signal strength, received power, radio quality. Intra cell mobility: timing advance. Inter cell: divided into idle and connected. In idle: cells grouped in tracking areas. When changing tracking areas, the network is notified. Reselection only happens after some time to prevent ping pong. If connected: X2 or S1 handover - X2 if eNodeB are connected with X2 interface, S1 if they are not. The user should not notice a handover since the traffic is routed in the core network to the other eNode B. Changing RAT is similar to S1 handover.
- HARQ, timing advance, paging, slow power control (no near far). Cell search: find good enough cell to camp on by 1) trying last from SIM or 2) searching all frequencies. Sync signals sent every 5ms. Random access: to establish RRC_CONNECTED. Read BCH to get available PRACH channels. Send preamble sequence on PRACH with low power. If access granted, send data on PUSCH. Network attach: search cell, contact network on random access, send attach once in RRC_CONNECTED, auth, inform capability, inform location, setup data tunnel to sGW, inform UE - UE gets IP right away.
- LTE only supports PS, so fallback on CS or use VoLTE or VoIP. SMS sent over interface between MME and MSC (GSM) called SG. Delivered over signalling RRC connections between MME and UE. Voice fallback also uses SG interface - LTE UE must attach as voice capable (MME will register UE with proper 2g/3g). Voice fallback slow because of RAT. The network also repairs itself and has automatic neighbour relations.

8. 5G fundamentals

- Can be deployed 6 different ways: SA with EPC (just 4g), SA with 5GC (with and without LTE antenna), NSA with EPC (most common), NSA with 5GC and LTE primary, NSA with 5GC and NR primary. Option 3 can be divided into 3 more; 3 (traffic split between 4G and 5G at eNodeB), 3a (traffic is split between 4G and 5G at EPC - sGW), 3x (traffic split between 4G and 5G at cell). 3a cannot support dynamic 4g/5g switching and 3 requires routing 5g through eNodeB.
- 2G: FDD only; 3G & 4G: FDD with TDD option. In 5G: TDD in new bands (3.5GHz + 26GHz). With multiple use-cases, multiple options are needed. NR DL: 1 frame(10ms) = 10 subframe(1ms) (like 4g). 1 PRB = 12 subcarriers, 14 symbols (like 4g). NR has wider frequency bands (100MHz instead of 20). Because of many subcarriers at 15kHz, subcarrier can be adjusted (numerology). UEs can switch between different bandwidth-parts to reduce energy consumption while sacrificing bandwitdth and capacity. Since network is mostly down, time division slots can be assigned dynamically. Since this also requires a lot of synchronization, signals and broadcast info sent on PBCH. Each time slot is .5ms and contains 14 symbols. Can be dynamically assigned to UL or DL. Since no frequency guard bands, UL/DL pattern must be synchronized between operators so DL does not overpower UL.
- Mid-band between 100 and 1.4GBit, mmwave 4Gbit, low-band slower. Latency in air is 8-12ms. Depends on numerology (and thereby number of carriers), modulation and coding

scheme

9. 5G procedures and operation

- 6 different deployment options with EPC or 5GC. Mostly option 3 is used. Since 5g is an upgrade to LTE, it can run on the same core and with the same antennas; option 1 is just LTE. It can also be run on only new hardware. Splitting the capacity usage between the technologies is possible with option 3 - called EN-DC (anchor at 4g - add capacity on 5g). This is done by establishing RRC_CONNECTED to eNodeB, then attach messages to MME, then establish session, then reconfigure RRC. Stand-alone architecture looks like LTE, however only functions are defined (possible to virtualise the network). This also makes stateless interaction possible. Network also sliced to contain different operations on different slices.
- Connection: request to gNB which forwards to AMF. AMF asks for identity, AUSF and UDM challenge UE. AMF and UDM discuss, then registration accept and complete to UE. Session management: UE sends PDU establishment request to AMF, creates context in UDM, assigns IP to UE. Mobility management: UE tells measurements, gNB forwards to new gNB and the core network is told of the change - looks like LTE. No tracking area updating, so reuse of registration procedure: UE is informed of identifiers. New registration procedure when camping on cell with identifier not in set. IP packets routed in backhaul with tunnelling. In case of handover, UPF changes destination in outer header; no change in inner packet or UE IP.

10. Mobile network procedures

- A handover is different in the technologies. GSM handover is mobile assisted but network controlled. In GPRS/EDGE, no contiguous data flow so no handover. Instead do cell reselection. In UMTS, handover decisions are made by RNC based on noise and signal strength. If no connection active, location area update. If active connection, soft/softer/hard handover. Soft: active set of antennas. Softer: treated as multipath, no additional resources. Hard: between frequencies or systems. In LTE & 5G: depends on the interface, but not noticeable because of late path switching. Cell reselection is also different in the technologies. In GPRS/EDGE, normally decided by UE. In LTE, mobile assisted, network controlled. In UMTS, also controlled by network by having multiple active at the same time.
- In GSM, the call is setup by examining the data in the call setup request. The BSC is alerted if it has to assign capacity for the call. UMTS is also circuit switched, so calls handled the same way. In LTE, calls are either defaulted to older standard or carried out as VoLTE using SIP. SIP is the protocol used to initiate the call. Each user has a SIP address (can be translated from phone number). In LTE implemented as IMS. Signalling from eNodeB -> sGW -> pGW -> P-CSCF -> S-CSCF or to internet. Can also handle DTMF tones. Can also work with older circuit switched. 5G is also packet based, so same technology works.
- Signalling is usually done on specific channels, e.g. the first timeslot in the first TRX of a cell. The signalling can be something like synchronization information, frequency correction, power control or timing advance.

11. Cellular networks: Principles and applications

- Since all technologies more or less use the same frequencies, the operator must decide which frequencies to use for which purposes. In cases where talkover is a problem (anything but UMTS), the frequencies used are controlled in neighbouring cells. In LTE and 5G, the eNode B's themselves communicate about how to best schedule transfer of information so as to reduce the amount of interference.
- Example technologies
- Pros of GSM: low battery usage, simple to implement, fast enough for very small purposes. Not, however, fast enough for anything but the bare minimum; to do anything actually related to traffic, a new technology is needed. EDGE is fast enough if nothing else exists, but it is not necessarily easier to implement than some of the newer technologies.