Cellular Base Station Technology

Harald Welte laforge@gnumonks.org

osmocom.org / sysmocom.de

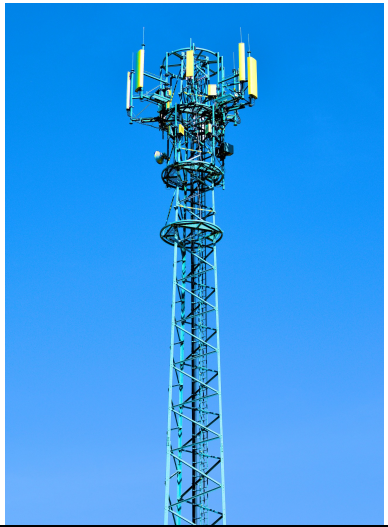
September 2019, CCCB Datengarten

Outline

About the speaker

- Free Software + OSHW developer for more than 20 years
- Used to work on the Linux kernel from 1999-2009
- By coincidence among the first people enforcing the GNU GPL in court
- Since 2009 developing FOSS in cellular communications (Osmocom)
- Living and working in Berlin, Germany.

What is a Cellular Base station?



- transmits and receives signals from/to mobile phones
- converts wireless signals to wired signals
- sits between the *air interface* and *back-haul*
- is the most visible part of cellular networks

The 3GPP Specification point-of-view: 2G

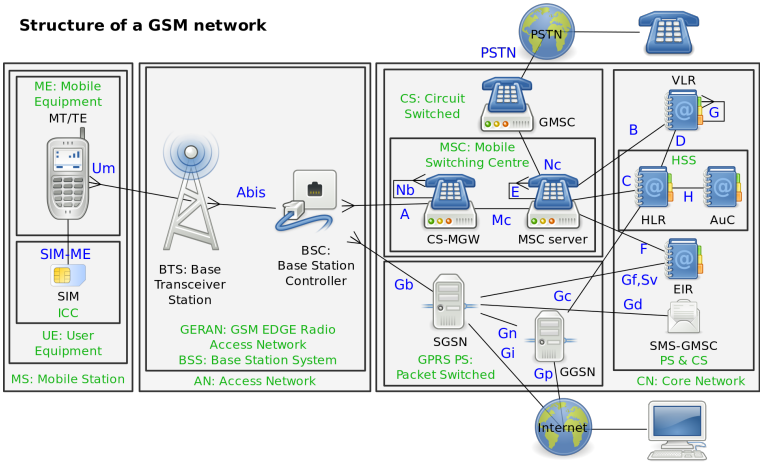


Image credits: tsaitgaist via Wikipedia

The 3GPP Specification point-of-view: 3G

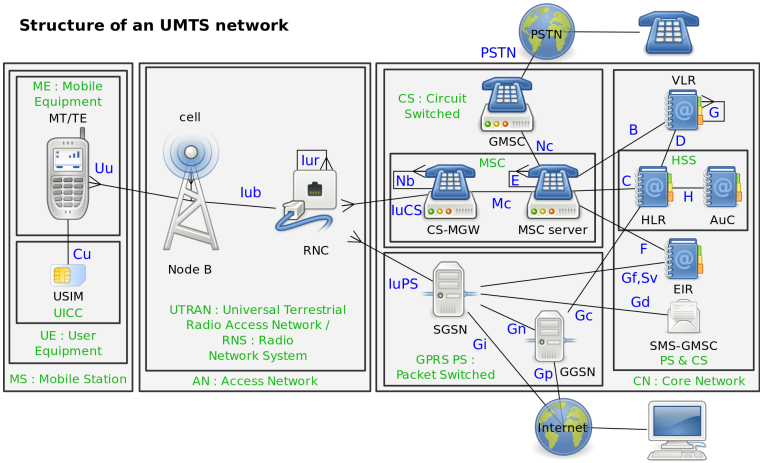


Image credits: tsaitgaist via Wikipedia

The 3GPP Specification point-of-view

What do we learn from this?

The 3GPP Specification point-of-view

What do we learn from this?

- The telecom world loves acronyms

The 3GPP Specification point-of-view

What do we learn from this?

- The telecom world loves acronyms
- Specifications deal with functional / logical network elements
- Cellular network contains lots of elements
- Today, we only want to look at real-world base stations

Terminology across cellular generations

Generation	Name	Base Station	Back-haul	Next element
2G	GSM/GPRS	BTS	Abis	BSC
3G	UMTS	NodeB	Iub	RNC
4G	LTE	eNodeB	S1	MME + SGW
5G	NR	gNodeB	N2 + N3	AMF + UPF

Site vs. Cell

Site A single tower and associated equipment

- could in theory be omnidirectional
- in reality almost always sectorized
- classic setup is three-sector site (120 degree per sector)

Cell A logical cell in one cellular network generation

- typically illuminated by one (set of) antenna

- Result: Single site often has 9 cells
- three sectors for each of 2G, 3G and 4G

Components of a cellular base station

- Tower/Pole (civil engineering part)
- Antenna
- Coaxial Cable
- Actual Base Station Electronics
- Back-haul connection to the rest of the network
- Power Supply / Environment (Fans, AC, UPS, ...)

Simplified Rx/Tx chain

- Simplified Receiver chain:

- Simplified Transmitter chain:

Reality is more complex in many cases (circulator, active predistortion, rx diversity, ...)

Even more Simplified Rx/Tx chain

- Even more simplified Receiver chain:

- Even more simplified Transmitter chain:

Classic Cell Site (year 2000)

The traditional way of building cell sites:

- (multiple) large racks full of equipment
- installed in [air conditioned] shelters
- all active electronics on ground level
- long lines of coaxial cable up the tower
- only passive element (antenna) up tower
- half of transmitted power lost in cable

Image: Timur V. Voronkov via Wikimedia Commons (CC-BY-SA)

Slightly less Classic Cell Site

The fist step of logical evolution:

- equipment becomes smaller (partial rack)
- no strict need for large shelter anymore
- all active electronics on ground level
- long lines of coaxial cable up the tower
- only passive element (antenna) up tower
- half of transmitted power lost in cable

Equipment gets smaller, less power hungry and dissipates less heat Image: Peter Schmidt @33dBm

Coaxial Cables...

Why don't we like long coaxial cables

- good cabling is 1/2" to 1" in diameter and costs a lot
- installation is more like plumbing than cabling
- looses lots of energy over length of tower; compensated by
  - downlink: more PA; waste of energy; causs more heat dissipation
  - uplink: tower-mounted amplifier (TMA)
- higher frequencies have even more losses (and we went from 900 MHz to 1800 MHz to 2100 MHz to 2600 MHz)
- more bands mean more coaxial cables in parallel

Towards Remote Radio Heads

So why not do he logical thing and ...

Towards Remote Radio Heads

So why not do he logical thing and ...

- Generate the RF closer to the antenna?

Answer:

- Requires much more compact radios
- Requires passive cooling
- Difficult installation (heavy)
- Environmental protection (sun, rain, temperature cycles)
- Hard to service / replace

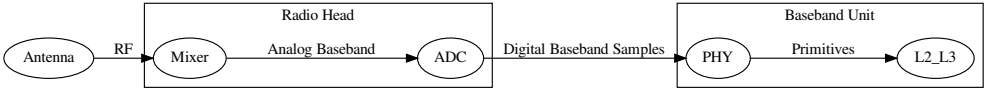
(Remote) Radio Heads

Solution: Instead of moving all equipment up the tower,

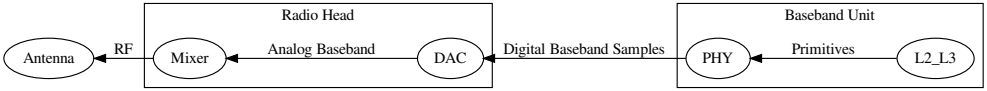
- Move only the Analog parts of the chain up
- Transport digital samples up/down the tower
- Base Station split in two parts:
  - Baseband processing (*digital unit*)
  - Radio processing (*radio unit*)

Base Station split with Radio Heads

- Incredibly Simplified Receiver chain:



- Incredibly Simplified Transmitter chain:



Cell Sites with (Remote) Radio Heads

Cell Sites with (Remote) Radio Heads

Cell Sites with (Remote) Radio Heads

Image: Peter Schmidt @33dBm

New term: front-haul

- *back-haul* is the connection between cell and core
- *front-haul* is the newly-introduced term for the link between radio head and baseband unit
- physical medium
  - typically fiber-optic
  - copper only if radio next to baseband unit
- physical layer
  - OBSAI (Open Base Station Architecture Initiative)
    - Started in 2002 by Hyundai, LG, Nokia, Samsung, ZTE
    - Mostly obsolete now
  - CPRI (Common Public Radio Interface)
    - Ericsson, Huawei, NEC, Alcatel-Lucent
    - more adoption particularly in recent years
  - eCPRI showing up on the horizon

from fiber-based front-haul to C-RAN

As digital baseband samples are transmitted over fiber optics

- can cover distances way above height of the tower
- single-mode transceivers allow for dozens of kilometers
- allows for cell sites without any shelter or rack
- leads to some people proclaiming *cloud-RAN* or *centralized RAN*
  - don't distribute baseband compute power in the field
  - bring all your baseband samples into the cloud
  - perform CPU-intensive baseband function in data center
- bit rates are high. A single LTE 2x2 MIMO carrier at 20MHz needs 2Gbps CPRI bandwidth
  - site with 3 sectors and multiple carriers exceeds 10Gbps
- latency constraints are biggest limiting factor

Antennas

- You learned some antenna basics
- You think about an omnidirectional dipole
- Almost no cellular base station antenna is like that
- Complexity of those antennas has grown significantly

Vertical polarization vs. X-Pol

- Nominally, cellular signals are emitted in vertical polarization
- Industry has moved to two radiators at +45 / -45 degrees polarization
- This apparently gives polarization gain, as signals reflected (by buildings) don't arrive in vertical polarization
- Isolation between radiators typically 20..30dB, allowing use cases like
  - operating two transmitters without combiner
  - operating Rx + Tx without duplexer
  - diversity reception within one antenna (polarization diversity)

Single-Band vs. Multiple Bands

- So you rolled out a GSM network in 900 MHz
  - then added more GSM on 1800 MHz
  - then added 3G on 2100 MHz, ...
- Do you add one new set of three sector antennas per band?
  - space and weight constraints on tower
  - they may affect each others' radiation pattersn
- Industry responds with multi-band antennas

Electrical Tilt

- For RF planning, you want to determine where your cell physically ends
- Tilting antennas downwards means RF signals emitted eventually will hit the ground
- Adjusting the network by climing up the tower and mechanically adjusting tilt is cumbersome
- Industry responds with *Electrical Tilt*
- Rods are controlled by motors leading to *Remote Electrical Tilt (RET)*

MIMO

- MIMO means Multiple-In / Multiple-Out
- uses spatial diversity to establish multiple signals between different antennas
- 2x2 MIMO is standard with LTE today
- 5G / New Radio specified for massive MIMO (32-64 antennas in base station!)

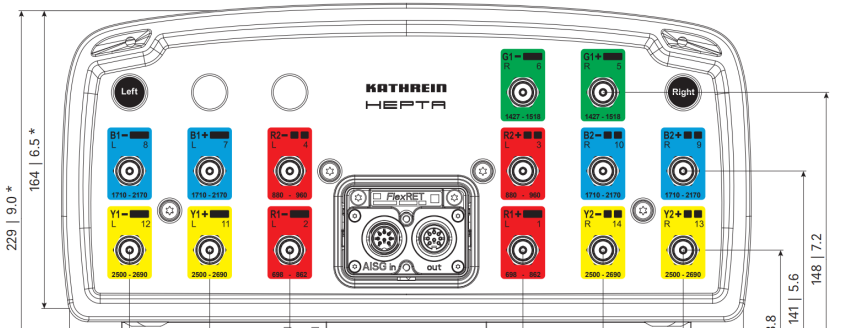
Antennas with many ports

Where will it end?

14-Port Antenna

KATHREIN

Layout of interface:



Further integration

- the radio head has moved up the tower
- coaxial cables are shorter than ever
- ... but we have more and more of them
- So what do we do?

Further integration

- the radio head has moved up the tower
- coaxial cables are shorter than ever
- ... but we have more and more of them
- So what do we do?
- Integrate radio head inside antenna!

Antenna Integrated Radio

- Systems like *Nokia RAS* / *Ericsson AIR*
- Radio heads completely integrated with antenna
- no coaxial cable at all
- CPRI over fiber directly into the antenna
- Everything Great? New problems
  - enormous weight not suitable everywhere
  - complicated measurements (field technicians)

Classic 2G back-haul

- 2G (GSM) was specified while ISDN was hot
- back-haul of GSM BTS is done via E1/T1 (ISDN PRI)
- E1 has 30 usable timeslots of 64kBps each
  - use one for signaling (A-bis RSL + OML)
  - use one quarter (16kBps) sub-slot for each voice call
- While GSM is still deployed today, 3GPP never specified any other transport
- Every vendor came up with their own proprietary kludge on how to carry Abis over IP

Classic 3G back-haul

- 3G (UMTS) was specified when ATM was the next hot thing
- back-haul of NodeB is done via ATM
- in reality, often Inverse ATM Multiplex (ATM over 4xE1 ISDN)
- 3GPP at least later adapted specs for IP based transport
  - Every 20ms voice codec frame split over three different UDP packets. yay!

4G back-haul

- 4G is first 3GPP cellular technology transported over IP from day one
- Therefore, no exotic physical layers
- Ethernet in most cases
- Problem: Where do we get clock from?
  - ISDN/E1/ATM always provided clock reference
  - Ethernet doesn't provide clock reference

IP-based back-haul and base station clocking

- cellular base stations need super stable clock reference
  - requirement of 30 ppb is almost 1000 times more accurate than crystal
  - even ovenized crystals (OCXOs) not long-term stable enough
- in the post-ISDN/PDH/SDH days, pick your poison:
  - go for a GPS-DO and create a single point of failure, or
  - use Synchronous Ethernet and loose the advantage of low-cost COTS Ethernet Switches, or
  - use IEEE PTP and hope your switches don't introduce too much jitter, or
  - let your base stations hammer your NTP server and pray

Base Station Electronics: Baseband

- Typically some multi-core DSP
  - e.g. TI Keystone2 (eight 64bit 1.2GHz DSPs)
  - built-in coprocessors (FFT, crypto, Turbo Decoder, Viterbi)
  - built-in CPRI/OBSAI Controller
  - four ARM Cortex A-15 for L2/L3 processing
- Often also FPGAs + vendor-specific ASICs
  - Ericsson big on ASICs
  - proprietary ASICs/SoCs with 10.5 billion transistors
  - that's comparable to Apple A12X / Huawei Kirin 990!

Base Station Electronics: Radiohead

- Some RFIC (typically ADI)
  - ADC + DAC
  - up/downconversion (mixer)
  - on-chip filters
- Power Amplifier
  - typically 2 stages of drivers + final PA
- Circulator
  - protect PA from power reflected back from antenna
- Cavity Duplexer

Digital [Adaptive] Pre-distortion

- Ensure Linear PA even for high-PAPR signals

Base Station Software

- Don't expect too many familiar things here
- decades of proprietary development by large corporations
- Enea OSE (Operating System Embedded) popular with Ericsson + Nokia
  - proprietary microkernel with custom-everything including filesystems
- vxworks found in some equipment like Huawei radioheads
- Linux found mostly only in small cells, inheriting software from femtocells

Further Reading

- http://cpri.info/
- FlexiWCDMA teardown: https://www.youtube.com/watch?v=d5xT4p9FXIw
- Ericsson RBS6000 teardown: https://www.youtube.com/watch?v=q0127zY3voE

Thanks

Thanks for your attention.
You have a General Public License to ask questions now :)