Cellular Networks
Theoretical Laboratory Session

WIRELESS COMMUNICATIONS 371-1-1903
SPRING 2020

Part 1 – General Theoretical Information

Cellular network generations

A cellular network or mobile network is a communication network where the last link is wireless. The network is distributed over land areas called "cells", each served by at least one fixed-location transceiver, but more normally, three cell sites or base transceiver stations. These base stations provide the cell with the network coverage which can be used for transmission of voice, data, and other types of content. A cell typically uses a different set of frequencies from neighboring cells, to avoid interference and provide guaranteed service quality within each cell.

When joined together, these cells provide radio coverage over a wide geographic area. This enables a large number of portable transceivers (e.g., mobile phones, tablets and laptops equipped with mobile broadband modems, pagers, etc.) to communicate with each other and with fixed transceivers and telephones anywhere in the network, via base stations, even if some of the transceivers are moving through more than one cell during transmission.

In the early 1980s, **1G** was introduced as voice-only communication via "brick phones". Later in 1991, the development of **2G** introduced Short Message Service (SMS) and Multimedia Messaging Service (MMS) capabilities, allowing picture messages to be sent and received between phones. In 1998, **3G** was introduced to provide faster data-transmission speeds to support video calling and internet access. **4G** was released in 2008 to support more demanding services such as gaming services, HD mobile TV, video conferencing, and 3D TV. **5G** technology has been planned for the upcoming future.

1G devices used the analog technology for the communication which includes the communication on certain frequency band (FDMA – Frequency Division Multiple Access). The conversation was a full duplex meaning both the persons can talk & listen at a time. Device was equipped with direct dialing hence operator help was no more required to connect to a call. The system was able to handle the billing, roaming and call setup functionality. Text messaging was also possible in this generation with some sophisticated devices. Since the whole technology was based on the analog system noise introduction into the signal during communication was a disadvantage. In the current days this generation's system & devices are no more used.

2G cellular networks were commercially launched on the GSM standard in 1991.

Three primary benefits of 2G networks over their predecessors were that:

1. phone conversations were digitally encrypted.
2. significantly more efficient use of the radio frequency spectrum enabling more users per frequency band.
3. Data services for mobile, starting with SMS text messages.

2G technologies enabled the various networks to provide the services such as text messages, picture messages, and MMS (multimedia messages). All text messages sent over 2G are digitally encrypted, allowing the transfer of data in such a way that only the intended receiver can receive and read it.

After 2G was launched, the previous mobile wireless network systems were retroactively dubbed 1G. While radio signals on 1G networks are analog, radio signals on 2G networks are digital. Both systems use digital signaling to connect the radio towers (which listen to the devices) to the rest of the mobile system.

With General Packet Radio Service (GPRS), 2G offers a theoretical maximum transfer speed of 40 kbit/s. With EDGE (Enhanced Data Rates for GSM Evolution), there is a theoretical maximum transfer speed of 384 kbit/s.

The most common 2G technology was the time division multiple access (TDMA)-based GSM, originally from Europe but used in most of the world outside North America.

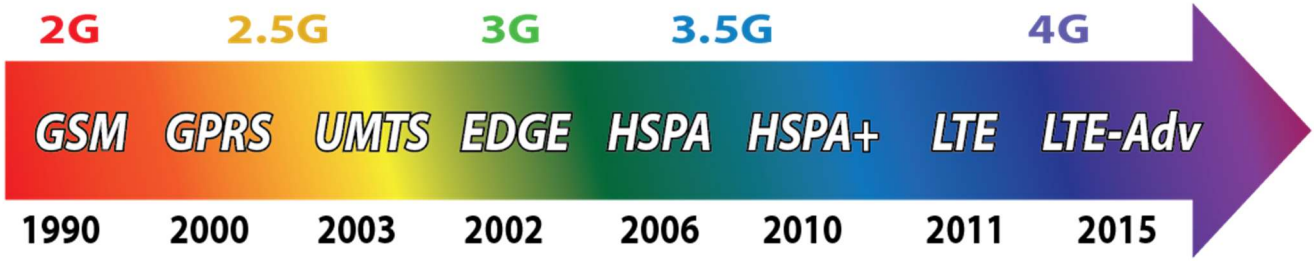
3G is the upgrade for 2G and 2.5G GPRS networks, for faster data transfer speed. This is based on a set of standards used for mobile devices and mobile telecommunications use services and networks that comply with the International Mobile Telecommunications-2000 (IMT-2000) specifications by the International Telecommunication Union. 3G finds application in wireless voice telephony, mobile Internet access, fixed wireless Internet access, video calls and mobile TV.

3G telecommunication networks support services that provide an information transfer rate of at least 144 kbit/s. Later 3G releases, often denoted 3.5G and 3.75G, also provide mobile broadband access of several Mbit/s to smartphones and mobile modems in laptop computers. This ensures it can be applied to wireless voice telephony, mobile Internet access, fixed wireless Internet access, video calls and mobile TV technologies.

4G system must provide capabilities defined by ITU in IMT Advanced. Potential and current applications include amended mobile web access, IP telephony, gaming services, high-definition mobile TV, video conferencing, and 3D television.

The first-release Long Term Evolution (LTE) standard was commercially deployed in 2009 and has since been deployed throughout most parts of the world. It has, however, been debated whether first-release versions should be considered 4G LTE.

5G is the fifth generation cellular network technology. The industry association 3GPP defines any system using "5G NR" (5G New Radio) software as "5G", a definition that came into general use by late 2018. Others may reserve the term for systems that meet the requirements of the ITU IMT-2020. 3GPP will submit their 5G NR to the ITU. It follows 2G, 3G and 4G and their respective associated technologies (such as GSM, UMTS, LTE, LTE Advanced Pro and others).

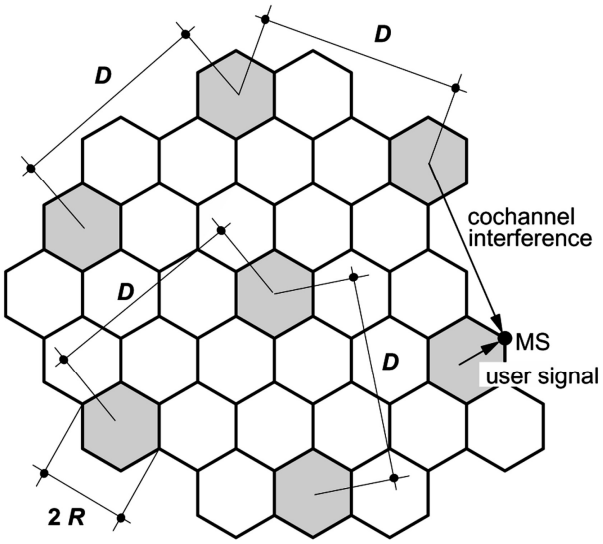


We will discuss the 4G and 5G cellular networks in the upcoming sessions in further details.

Cellular principle

Owing to the very limited frequency bands, a mobile radio network only has a relatively small number of speech channels available. For example, the GSM system has an allocation of 25 MHz bandwidth in the 900 MHz frequency range, which amounts to a maximum of 125 frequency channels each with a carrier bandwidth of 200 kHz. Within an eightfold time multiplex for each carrier, a maximum of 1000 channels can be realized. This number is further reduced by

guardbands in the frequency spectrum and the overhead required for signaling. In order to be able to serve several hundreds of thousands or millions of subscribers in spite of this limitation, frequencies must be spatially reused, i.e. deployed repeatedly in a geographic area. In this way, services can be offered with a cost-effective subscriber density and acceptable blocking probability.



Model of a cellular network with frequency reuse.

The frequency reuse distance D can be derived geometrically from the hexagon model depending on k and the cell radius R:

$$D = R\sqrt{3K}$$

Resources

https://en.wikipedia.org/wiki/Cellular_network
https://en.wikipedia.org/wiki/History_of_mobile_phones
https://en.wikipedia.org/wiki/1G
https://en.wikipedia.org/wiki/2G
https://en.wikipedia.org/wiki/3G
https://en.wikipedia.org/wiki/4G
https://en.wikipedia.org/wiki/5G
http://myphonefactor.in/2012/02/mobile-generations/

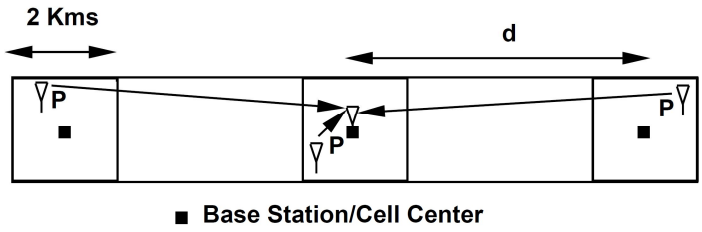
Theoretical Questions

1. What is the reason 1G networks used FDMA? Explain.

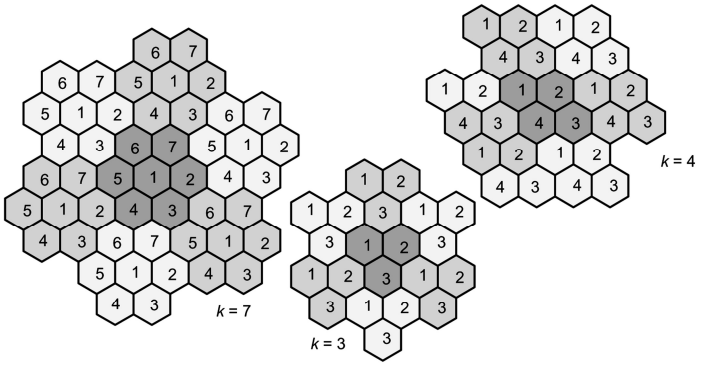
2. Does TDMA and FDMA contradict? (can we use them together?) Explain its benefits.

3. What loss elements effects the cell coverage area and range? Explain why.

4. Consider a cellular system operating at 900 MHz where propagation follows **free space path loss** with variations from **log normal shadowing** with σ = 6dB. Suppose that for acceptable voice quality a signal-to-noise power ratio of 15 dB is required at the mobile. Assume the base station transmits at 1 W and its antenna has a 3 dB gain. There is no antenna gain at the mobile and the receiver noise in the bandwidth of interest is -10dBm. Find the maximum cell size so that a mobile on the cell boundary will have acceptable voice quality 90% of the time.

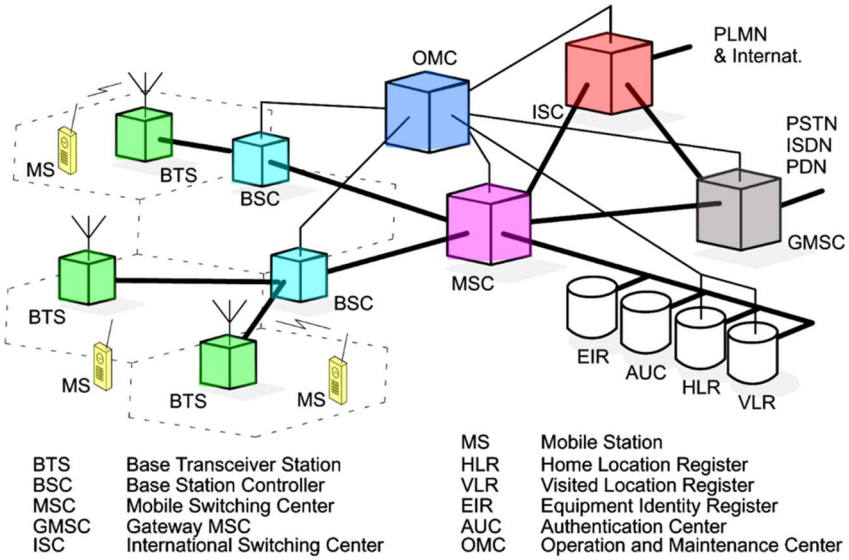


5. The following are frequency reuse and cluster formations (each number is a frequency). Is it possible to construct a K=5 cluster? Is K=9 possible? Can you find a formula for frequency reuse cluster formations? Explain.



Part 2 – GSM

System architecture



The fundamental components of a GSM network are shown in the figure above. A user carries a Mobile Station (MS), which can communicate over the air with a base station, called Base Transceiver Station (BTS) in GSM. The BTS contains transmitter and receiver equipment, such as antennas and amplifiers, as well as a few components for signal and protocol processing. For example, error protection coding is performed in the BTS, and the link-level protocol for signaling on the radio path is terminated here. In order to keep the base stations small, the essential control and protocol intelligence resides in the Base Station Controller (BSC). It contains, for example, protocol functions for radio channel allocation, channel setup and management of handovers. Typically, several BTSs are controlled by one BSC. In practice, the BTS and BSC are connected by fixed lines or point-to-point radio links. BTS and BSC together form the radio access network.

The combined traffic of the users is routed through a switch, called the Mobile Switching Center (MSC). It performs all of the switching functions of a switching node in a fixed telephone network, e.g., in an Integrated Services Digital Network (ISDN). This includes path search, data forwarding and service feature processing. The main difference between an ISDN switch and an MSC is that the MSC also has to consider the allocation and administration of radio resources and the mobility of the users. The MSC therefore has to provide additional functions for location registration of users and for the handover of a connection in the case of changing from cell to cell. A cellular network can have several MSCs with each being responsible for a part of the network (e.g., a city or metropolitan area). Calls originating from or terminating in the fixed network are handled by a dedicated Gateway MSC (GMSC). The interworking of a cellular network and a fixed network (e.g., PSTN, ISDN) is performed by the Interworking Function (IWF). It is needed to map the protocols of the cellular network onto those of the respective fixed network. Connections to other mobile or international networks are typically routed over the International Switching Center (ISC) of the respective country. A GSM network also contains several types of databases. The Home Location Register (HLR) and the Visited Location Register (VLR) store the current location of a mobile user. This is needed since the network must know the current cell of a user to establish a call to the correct base station. In addition, these registers store the profiles of users, which are required for charging and billing and other administrative issues. Two further databases perform security functions: The Authentication Center (AUC) stores security-related data such as keys used for authentication and encryption; The Equipment Identity Register (EIR) registers equipment data rather than subscriber data.

The network management is organized from a central place, the Operation and Maintenance Center (OMC). Its functions include the administration of subscribers, terminals, charging data, network configuration, operation, performance monitoring and network maintenance.

In summary, a GSM network can be divided into three subnetworks: the radio access network, the core network and the management network. These subnetworks are called subsystems in the GSM standard. The respective three subsystems are called the Base Station Subsystem (BSS), the Network Switching Subsystem (NSS) and the Operation and Maintenance Subsystem (OMSS). Figure 3.2 summarizes the hierarchical relationship between the network components MSC, BSC and BTS. The entire network is divided into MSC regions. Each of these is composed of at least one Location Area (LA), which in turn consists of several cell groups. Each cell group is assigned to a BSC. For each LA there exists at least one BSC, but cells of one BSC may belong to different LAs. The exact partitioning of the network area with respect to LAs, BSCs and MSCs is not, however, uniquely determined and is left to the network operator who thus has many possibilities for optimization.

Resources

GSM - Architecture, Protocols and Services, 3rd Edition, 2009, Jörg Eberspächer, Hans-Joerg Vögel, Christian Bettstetter, Christian Hartmann, 978-0470030707

Theoretical Questions

6. Alice (Yes, the same Alice) from wonderland wishes to call Bob (via mobile) who is currently in Springwood Minimum Security Prison. Describe the path that the call data is traveling from Alice to Bob, GSM wise. Elaborate as much as possible.

7. How does the GSM network know who Alice and Bob are? How does it know their location in order to route the call?

Air interface – physical layer (Base Station ⇔ Mobile Station)

The GSM physical layer, which resides on the first of the seven layers of the OSI, contains very complex functions. The physical channels are defined here by a TDMA scheme. On top of the physical channels, a series of logical channels are defined, which are transmitted in the time slots of the physical channels. Logical channels perform a multiplicity of functions, such as payload transport, signaling, broadcast of general system information, synchronization and channel assignment.

Logical channels

On Layer 1 of the OSI Model, GSM defines a series of logical channels, which are made available either in an unassigned random access mode or in a dedicated mode assigned to a specific user. Logical channels are divided into two categories: traffic channels and signaling (control) channels.

Traffic channels - The Traffic Channels (TCHs) are used for the transmission of user payload data (speech, data). They do not carry any control information of Layer 3. Communication over a TCH can be circuit-switched or packet-switched.

Following ISDN terminology, the GSM traffic channels are also designated as **Bm** channel (mobile B channel) or **Lm** channel (lower-rate mobile channel, with half the bit rate).

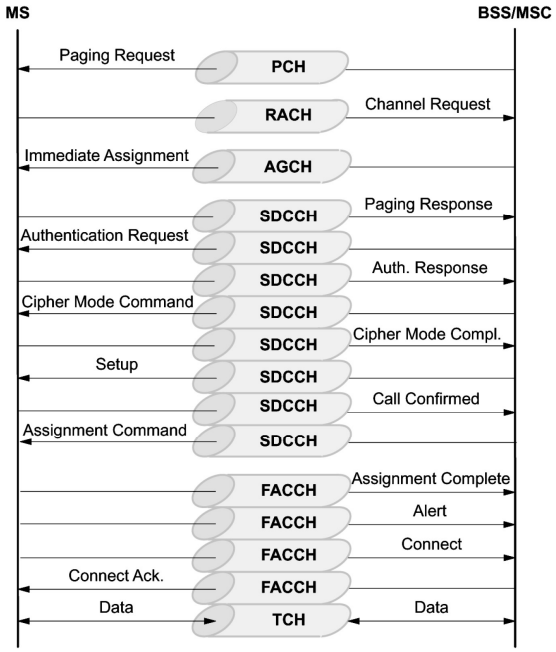
Signaling channels - The control and management of a cellular network demands a very high signaling effort. Even when there is no active connection, signaling information (for example, location update information) is permanently transmitted over the air interface. The GSM signaling channels offer a continuous, packet-oriented signaling service to MSs in order to enable them to send and receive messages at any time over the air interface to the BTS. Following ISDN terminology, the GSM signaling channels are also called **Dm** channels (mobile D channel). They are further divided into Broadcast Channel (BCH), Common Control Channel (CCCH) and Dedicated Control Channel (DCCH).

Group		Channel	Function	Direction
Traffic channel	TCH	TCH/F, Bm	Full-rate TCH	MS ↔ BSS
		TCH/H, Lm	Half-rate TCH	MS ↔ BSS
Signaling channels (Dm)	BCH	BCCH	Broadcast control	MS ← BSS
		FCCH	Frequency correction	MS ← BSS
		SCH	Synchronization	MS ← BSS
	CCCH	RACH	Random access	MS → BSS
		AGCH	Access grant	MS ← BSS
		PCH	Paging	MS ← BSS
		NCH	Notification	MS ← BSS
	DCCH	SDCCH	Stand-alone dedicated control	MS ↔ BSS
		SACCH	Slow associated control	MS ↔ BSS
		FACCH	Fast associated control	MS ↔ BSS

Channel type	Net data throughput (kbit/s)	Block length (bits)	Block distance (ms)
TCH (full-rate speech)	13.0	182 + 78	20
TCH (half-rate speech)	5.6	95 + 17	20
TCH (data, 14.4 kbit/s)	14.5	290	20
TCH (data, 9.6 kbit/s)	12.0	60	5
TCH (data, 4.8 kbit/s)	6.0	60	10
TCH (data, up to 2.4 kbit/s)	3.6	72	10
FACCH full rate	9.2	184	20
FACCH half rate	4.6	184	40
SDCCH	598/765	184	3060/13
SACCH (with TCH)	115/300	168 + 16	480
SACCH (with SDCCH)	299/765	168 + 16	6120/13
BCCH	598/765	184	3060/13
AGCH	$n \times 598/765$	184	3060/13
NCH	$m \times 598/765$	184	3060/13
PCH	$p \times 598/765$	184	3060/13
RACH	$r \times 27/765$	8	3060/13
CBCH	598/765	184	3060/13

Example: connection setup for incoming call

In the following figure it is illustrated how the various logical channels are used in principle. The MS is called via the **Paging Channe**l (PCH) and requests a signaling channel on the **Random Access Channel** (RACH). It obtains the **Stand-alone Dedicated Control Channel** (SDCCH) through an *IMMEDIATE ASSIGNMENT* message on the **Access Grant Channel** (AGCH). Then follow authentication, start of ciphering and start of setup over the **Stand-alone Dedicated Control Channel** (SDCCH). An *ASSIGNMENT COMMAND* message gives the traffic channel to the MS, which acknowledges its receipt on the **Fast Associated Control Channel** (FACCH) of this traffic channel. The FACCH is also used to continue the connection setup.



Physical channels

Physical channels transport the logical channels via the air interface. We first describe the GSM modulation technique, followed by the multiplexing structure: GSM is a multicarrier TDMA system, i.e. it employees a combination of FDMA and TDMA for multiple access. This section also covers the explanation of the radio bursts. Finally, the (optional) frequency hopping technique, which has been standardized to reduce interference.

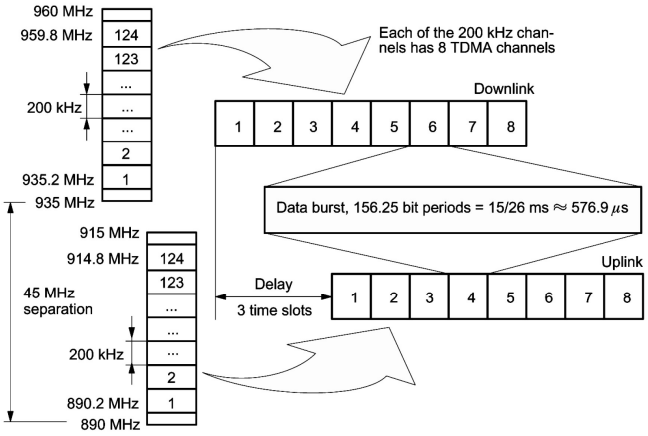
Modulation

The modulation technique used on the radio channel is Gaussian Minimum Shift Keying (GMSK). GMSK belongs to a family of continuous-phase modulation procedures, which have the special advantages of a narrow transmitter power spectrum with low adjacent channel interference, on the one hand, and a constant amplitude envelope, on the other hand, which allows use of simple amplifiers in the transmitters without special linearity requirements (class C amplifiers). Such amplifiers are especially inexpensive to manufacture, have high degree of efficiency and therefore allow longer operation on a battery charge

Multiple access, duplexing and bursts

At the physical layer (OSI Layer 1), GSM uses a combination of FDMA and TDMA for multiple access. Two frequency bands 45 MHz apart have been reserved for GSM operation: 890–915

MHz for transmission from the MS, i.e. **uplink**, and 935–960 MHz for transmission from the base station, i.e. **downlink**. Each of these bands of 25 MHz width is divided into 124 single carrier channels of 200 kHz width. This variant of FDMA is also called Multi-Carrier (MC). In each of the uplink/downlink bands there remains a guardband of 200 kHz. Each Radio Frequency Channel (RFCH) is uniquely numbered, and a pair of channels with the same number form a duplex channel with a duplex distance of 45 MHz.



A subset of the frequency channels, the Cell Allocation (CA), is allocated to a base station, i.e. to a cell. One of the frequency channels of the CA is used for broadcasting the synchronization data (FCCH and SCH) and the BCCH. Another subset of the cell allocation is allocated to a MS, the Mobile Allocation (MA). The MA is used among others for the optional frequency hopping procedure. Countries or areas which allow more than one mobile network to operate in the same area of the spectrum must have a licensing agency which distributes the available frequency number space, in order to avoid collisions and to allow the network operators to perform independent network planning.

Resources

GSM - Architecture, Protocols and Services, 3rd Edition, 2009, Jörg Eberspächer, Hans-Joerg Vögel, Christian Bettstetter, Christian Hartmann, 978-0470030707

Theoretical Questions

8. Why is there a separation of channels (Traffic channels and Control channels) in GSM? Hint: what if during a call, the mobile needs to tell the base station to amplify the transmission?

9. There are 124 FDMA channels of 200 kHz each with 8 TDMA time slots. How many users can obtain GSM service from a single base station? What is the maximal data capacity of a single band with GMSK modulation (GMSK has a gross data rate of 270.83 Kbits/s per carrier frequency)?

10. Why does broadcasting synchronization data needed? Hint: TDMA and FDMA.

Part 2 – DIY GSM sniffer

- Start in QT GUI mode. Set the sample rate to 2Msamples/sec.
- Create Ranges and Variables:
    - "Frequency" - Create a QT GUI Range from 925MHz to 2GHz with 200KHz steps and a default value of 950MHz. This will set the Carrier frequency.
    - "Gain" - Create a QT GUI Range from 0dB to 70dB with 0.5dB steps and a default value of 50dB. This will set the receiver gain.
    - "PPM" - Create a QT GUI Range from -150ppm to 150ppm with 1ppm steps and a default value of 0ppm. This will set the frequency shift in part per million (ppm).
    - Create a Variable named "Shiftoff" with the value of 400,000.
    - Create a Variable named "OSR" with the value of 4.
    - Create a Variable named "pi" with the value 3.141592654.
- Add an SDR source – "osmocom" source is an SDR source that enables you the advantages of a software api independent of the radio equipment.

  Set the source parameters:
    - Ch0 Frequency (Hz): *Frequency-Shiftoff* (the place the "Frequency" QT GUI Range you created and decrease/minus the Variable "Shift off")
    - CH0 RF Gain (dB): place the "Gain" QT GUI Range
    - Ch0 Bandwidth (Hz): *250KHz + abs(Shiftoff)*
- Add "Rotator" and set its phase increment to: *-2*pi*Shiftoff/samp_rate.* Connect it to the osmocom source out port.
- Add a "QT GUI Frequency Sink" and under the General tab set its FFT Size to 4096, Center Frequency (Hz) to "Frequency", Bandwidth (Hz) to "samp_rate", Average to Low, Update Period to 0.001 and GUI Hint to "1,0". Under the config tab, change the Control Panel to Yes.

  Connect it to the Rotator out port.
- Add a "GSM Input Adaptor" and set its ppm to "PPM", fc to "Frequency", OSR to "OSR" and Sample_rate_in to "samp_rate"

  Connect its input port to the Rotator's output port.
- Add a "GSM Receiver" and connect its input port to the GSM Input Adaptor's output port.
- Add a "GSM Clock Offset Control" and set its fc to "Frequency" and OSR to "OSR".

Connect its measurements input port to the GSM Receiver's measurements output port. Connect its output ctrl port to the GSM Input Adaptor's input ctrl port.

- Add a Stand-alone Dedicated Control Channel symbol demapper - "SDCCH/8 Demapper" and connect its bursts input port to the C0 output port of the GSM Receiver.

- Add a "Decryption" and set its Kc session key to [] (empty). Connect its bursts input port to the SDCCH/8 Demapper burts output port.

- Add a "Control channels decoder" and connect its bursts input port to the Decryption bursts output port.

- Add a "Socket PDU" and set it Type as a UDP Client with Host address 127.0.0.1 and Port 4729. Connect its pdus input port to the Control channels decoder msgs output port.

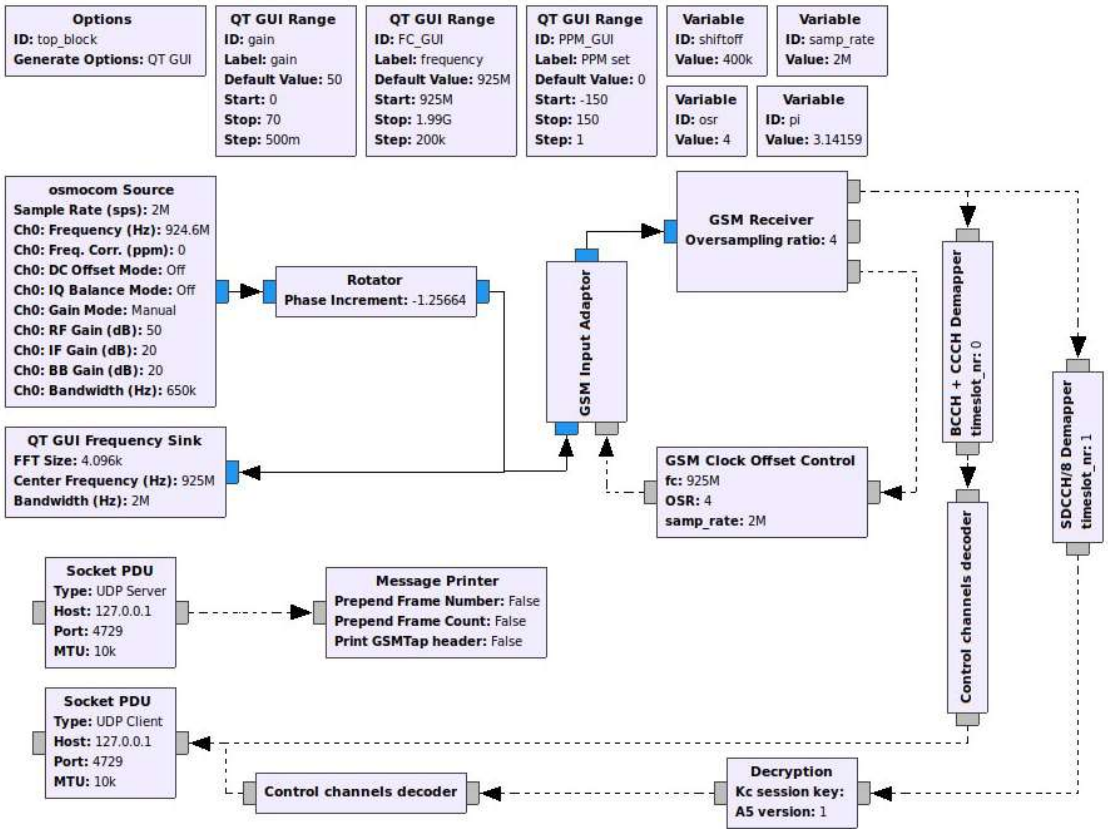
- Add another "Socket PDU" and set it Type as a UDP Server with Host address 127.0.0.1 and Port 4729. Leave it unconnected.

- Add a "BCCH + CCCH Demapper" and connect its bursts input port to the C0 output port of the GSM Receiver.

- Add another "Control channels decoder" and connect its bursts input port to the BCCH + CCCH Demapper bursts output port. Connect its msgs output port to the client Socket PDU pdus input port.

- Add a "Message Printer" and connect its msgs input port to the server Socket PDU pdus output port.

If constructed correctly your code should look like this:



In the practical session to come, we will use this GSM receiver to intercept messages from a cellular network and analyze their content. Make sure your code is correct.

Good luck!

References

- GSM - Architecture, Protocols and Services, 3rd Edition, 2009, Jörg Eberspächer, Hans-Joerg Vögel, Christian Bettstetter, Christian Hartmann, 978-0470030707
- Wireless communications, Andrea Goldsmith, Stanford University, California, 2005, 9780511841224