PENN

Ch 2.3.3 GSM

- **In the early 80's the European community decided to work together to define a cellular system that would permit full roaming in all countries and give the network providers freedom to provide diverse services and allow for variations in charging and rates. At the time each country had its own network and users could not roam. In contrast to the US which had a national standard: AMPS that provided national coverage and full roaming features.**

- **By the late 80's the Europeans had a specification for a system that was to use a hybrid FDMA/TDMA air interface and the Signalling System Number 7 for the communications infrastructure.**

- **The GSM (Global System for Mobile Communications) standard is comprehensive, defining the full air interface between mobiles and the BS. However it also prescribes open interfaces between network infrastructure elements allowing equipment vendors room for**

PENN

innovations and also giving network operators flexibility in equipment procurement.

- It was decided early on that it would be purely digital, and that the old analog systems would be phased out (as opposed to operating in dual mode). GSM started off using very few channels in the spectrum, and over the years more and more channels were added as the old analog systems were retired.

- The initial GSM specification included improved voice services, data services at rates up to 9.6Kbps and short message service (transmission of 160 alphanumeric characters).

PENN

- **2.3.3.1 System Architecture**

- **GSM right from the beginning was strongly influenced by the migration of the wireline PSTN to ISDN. It therefore uses the same signalling scheme and interface nomenclature of ISDN.**

- **Because of its modular architecture with standardized interfaces between network elements/segments, operators can mix-and-match any vendor's equipment. An operator can purchase the MSC from one vendor, the BS from another and the databases from a third! In contrast, for the NA standards, the vendors have not only specified the air interface but also specified proprietary interfaces between the network elements.**

- **2.3.3.1.1 Network Elements:**

  - The **mobile station** (i.e., the mobile terminal) comes in different types distinguished by its transmission power capabilities for use in different environments. It is split in two parts: one which contains the h/w and s/w specific to the radio interface and another which contains the subscriber specific data (**subscriber**

PENN

identity module (SIM)). This latter part is removable, it comes in two flavors: one a credit sized card and the other a small chip. The former is larger but easier to install than the latter. This feature allows a user to only carry the SIM along and install it in a terminal at the destination (leased, rented, borrowed, etc.). All of the subscribers data is contained in the SIM related to services, identity, preferences, etc. A terminal without a SIM can only make emergency calls.

- **Base station system (BSS)**: consists of two parts: the **BS transceiver (BST)** and the **BS controller (BSC)**.
  - The **BST** consists of all the receivers and transmitters to communicate with the mobiles over the air interface. It combines/multiplexes the signalling and speech channels over the air interface and separates them out over the wireline interface to the BSC. A BST can be configured as omnidirectional or sectored. Each BST will consist of several transceivers each one responsible for an RF carrier. The transmission power is dependent upon the cell size.
  - The **BSC** is connected on one side to several BSTs and on the other to the MSC. It is responsible for frequency administration, it manages the radio interface and the handover process.

PENN

2.3.3.1.2 Numbering and Identification

- In a GSM system there are several types of number/IDs associated with a mobile station. Each serves a specific purpose.
  - **Mobile subscriber ISDN number (MSISDN)**: the number dialed to reach a GSM subscriber. The MSISDN will determine which gateway MSC (GMSC) to use. At the GMSC, the MSISDN is mapped onto a HLR which is queried to get the latest data related to the called mobile. The HLR provides the mobile station roaming number (MSRN). This is used by the GMSC to get to the MSC of the current location of the mobile. The MSISDN consists of: country code (CC) used by PSTN, national destination code (NDC) and subscriber number (SN). The NDC can be either the network of the suscriber or the geographical area of the subscriber's home system (in the US NDCs are the telephone area codes).
- **Int'l mobile subscriber identity (IMSI)**: a unique number associated with a subscriber. It resides in the SIM. It consists of 3 parts:
  - **The mobile country code (MCC)** which is a three digit code (different from the country code that is used in the PSTN network and of variable length). It is administered by the ITU.

PENN

- The **mobile network code (MNC)** consisting of 2 digits. It has no geographical meaning. Uniquely identifies a network.
- The **mobile station identification number (MSIN)** consisting of 10 digits which identifies a mobile subscriber inside a network.

- **Temporary mobile subscriber identity (TMSI)**: To protect the identity of a subscriber, the network will give a mobile station a temporary network ID so that is does not transmit its IMSI over the air interface until it is ‘‘secured’’.
- **Location Areas (LA)**: GSM also makes use of location area identifiers. Cells are grouped together in an LA (several LAs to a MNC, each LA has a code (LAC)) and each time a mobile enters a new LA (different LAC), it sends an update message. The smaller the LAs the more update messages. LAs are used to group cells for mobility management and to reduce the number of paging messages used to locate a subscriber.

PENN

2.3.3.2 The Compressed Speech Stream

- The vocoder produces 260 bits of speech every 20msecs. This translates into 13Kbps.
- The 260 bits are split into three groups: class 1_a bits (50), class 1 bits (132) and class 2 bits (78). The former two are error protected, the latter is not. The coded bits come to 378 bits and these are interleaved over 8 slots with the unprotected class 2 bits. The output consists of 456 bits in 8 groups of 57 bits each. The resultant bit rate is 22.8Kbps.

PENN

2.3.3.3 The Radio Channel

- GSM uses **200KHz** carriers. The frame duration is 4.62msecs and contains **8 time slots**.
- The reverse channel is **retarded by 3 slots** with regard to the forward channel.
- Frames in GSM are grouped into **multiframes** which consist of **26 frames**. As GSM uses the ISDN access procedures, the frame structure has to map onto an integral number of ISDN speech samples (1 multiframe = 960 speech samles).
- A **full rate** channel occupies 1 time slot in 24 out of the 26 slots in the multi-frame. The **SAACH** occupies 1 slot in the other two frames.
- GSM also allows for **half rate** channels, they occupy 12 slots out of a multi-frame and a 1 slot SAACH is associated with it.
- The GSM transmission rate is 270.833 Kbps (or the bit width is 3.69microsecs). Most logical channels use the same slot structure for tranmission.
- In GSM, most of the slots contain a **training sequence** that is used by an adaptive equalizer (that must be capable of handling 16microsec delay spread). 8 different training sequeces are used with low mutual cross correlation. The network operator assigns a different one to neighboring cells for identification purposes.

PENN

- Each slot (577microsecs) carries 144 bits of data.
- In GSM both terminals and BSs **turn off powe**r when not transmitting.
- GSM can use **slow frequency hopping (FH)**. The data is carried in a different carrier each time slot. This is done to enhance the performance of the channel. When one channel is bad, then only a short burst of data will be affected as the next burst(s) will be on other channels. (Note this FH is not used for spreading as in CDMA!)
- GSM supports many different types of terminals, each with different maximum transmitted power. The range is from 20W (vehicle mounted) to 0.8W.

PENN

2.3.3.1.2.1 Logical Channels

- The control channels have been classified as: **broadcast channel**, **common control channels** and **dedicated control channel**. In addition there are traffic channels and the SAACHs that are muxed on the carrier.
- In GSM the forward and reverse links have **similar structure** as compared to IS-136 and IS-95 which have very different channels in both directions.
- The **broadcast** and **common control channels** are used for synchronization, exchange of system information and setting up calls. They occupy **slot "0"** in a frame and cycle throuhg every 51 frame times. If the control channel needs more capacity it can use slots 2,4, or 6 too in the same carrier.
- The different **broadcast** and **common control channels** are:
  - **Frequency correction channel (FCCH)**: it only transmits 148 0s. Used by the terminals to adjust their frequency to that of the BS. Once a terminal has locked into the BS frequency, it can count the number of slots to the sync channel (SCH)). It always comes 8 slot times(one frame) after the FCCH .
  - **Synchronization Channel (SCH)**: It has a different structure than the other channels as it carries a long training sequence (64bit) that is the same in each cell. The SCH also carries the BS identity, and the present frame number

PENN

(position within the hypeframe). The data field is used to carry 25bit messages. The data is error protected.

- **Broadcast control channel (BCCH)**:used by BSs to convery information to all the terminals regarding the system parameters, access parameters, control channel configuration, etc. Only sends one message every 51 frame control multiframe.
- **Paging and Access Grant channel (PCH and AGCH)**: used by BSs to notify the mobiles of incoming calls (PCH) or to direct them to stand-alone dedicated control channels (SDCCH). GSM also supports the sleep mode so terminals are directed to listen to a group of paging messages every so often. The paging channel distribution is sent to all terminals over the BCCH.
- **Random Access Channel (RACH)**: used by mobiles to originate call, initiate short message transfer, respond to pages, and register. All of the common control channels in the reverse direction are used as RACH. Mobile access the channel at random and wait for an ACK. If none is received before a timer expires it tries again after a random wait time. If an ACK comes back it directs a mobile to a SDCCH for further communication. Transmissions on the RACH use shortened bursts so that the bits do not spill over into a neighboring time slot. The BS uses the arrival time of the RACH

PENN

msg. to compute the correct timing for subsequent transmissions. RACH messages contain long training sequences and a random number to distinguish transmissions from different mobiles. Theis 5 bit random number is used in the ACK along with the slot number.

- **Stand-alone dedicated control channel (SDCCH)** is a two way channel assigned to a mobile for efficient exchange of control information. It occupies 4 slots in a control multiframe. It has associated with it a SAACH that consists of 2 time slots every multiframe.
- **Traffic channels**: like IS-136, GSM supports both full rate and 1/2 rate channels. Every time slot carries 144 bits of data. The full rate channel has a transmission rate of 22.8Kbps. The GSM speech coder outputs 260bits every frame time. These are error protected to produce 456bits that are transmitted over 4 frames (8 blocks of 57 bits, 2 blocks per frame (114bits)).
- **Slow associated control channel (SAACH)**: is assigned to every traffic channel and SDCCH.
- **Fast associated control channel (FAACH)**: is used for faster msg. transfer. The FAACH takes over the data fields of a slot. To show that it is FAACH data and not speech data, it flips the polarity of the FLAG bit associated with the data filed that it has taken over.

PENN

2.3.3.3 Authentication and Security

- A 128 bit random number is sent to the mobile. This is used as input to an encryption algorithm referred to as "A3" which uses a secret key K_i stored in the SIM card.. The output consists of a 32 bit signed response (SRES). Another encryption alg. is used "A8" to calculate a 64 bit encrypting (ciphering) key, K_c from the SRES and K
- The terminal sends SRES to the BS which also uses the same random number and alg. and key to produce SRES. If the received and the calculated **SRES are the same** then the subscriber will become authorized.
- The data is **encrypted** using a 114 bit mask that is EXORed with the data in each time slot. The mask is calculated using another alg. "A5" and the inputs are the 64 bit ciphering key K_c and the current 22-bit frame number. The BS does the same operation. As the alg. uses the **current** frame number, we notice that the mask changes from frame to frame!

PENN

2.3.3.4 Handoffs

- Like the NA systems, it uses **mobile assisted hand-off (MAHO)**. Signal strength measurements are sent to the BS from the mobile. The MSC decides when to do a handoff and it informs the new BS and the mobile. When a mobile switches to a new BS it sends a series of shortened bursts to adjust its timing (giving the bS time to calculate it and send it) and allow the new BS to synchronize its receiver to the arrival time of the messages.