# Topic 5 Notes

## 5.1 Advanced Mobile Phone System

Advanced Mobile Phone System (AMPS) is an analog mobile phone system standard developed by Bell Labs, and officially introduced in the Americas in 1978, Israel in 1986, and Australia in 1987. It was the primary analog mobile phone system in North America (and other locales) through the 1980s and into the 2000s. As of February 18, 2008, carriers in the United States were no longer required to support AMPS and companies such as AT&T and Verizon have discontinued this service permanently. AMPS was discontinued in Australia in September 2000.

AMPS is a first-generation cellular technology that uses separate frequencies, or "channels", for each conversation. It therefore required considerable bandwidth for a large number of users. In general terms, AMPS was very similar to the older "0G" Improved Mobile Telephone Service, but used considerably more computing power in order to select frequencies, hand off conversations to PSTN lines, and handle billing and call setup.

What really separated AMPS from older systems is the "back end" call setup functionality. In AMPS, the cell centers could flexibly assign channels to handsets based on signal strength, allowing the same frequency to be re-used in various locations without interference. This allowed a larger number of phones to be supported over a geographical area. AMPS pioneers fathered the term "cellular" because of its use of small hexagonal "cells" within a system.

It suffered from some weaknesses when compared to today's digital technologies. Since it was an analog standard, it is very susceptible to static and noise and has no protection from eavesdropping using a scanner. In the 1990s, "cloning" was an epidemic that cost the industry millions of dollars. An eavesdropper with specialized equipment could intercept a handset's ESN (Electronic Serial Number) and MIN (Mobile Identification Number, aka the telephone number). An Electronic Serial Number is a packet of data which is sent by the handset to the cellular system for billing purposes, effectively identifying that phone on the network. The system then allows or disallows calls and or features based on its customer file. If an ESN/MIN Pair is intercepted, it could then be cloned onto a different phone and used in other areas for making calls without paying.

Cell phone cloning became possible with off-the-shelf technology in the 1990s. Three key items were needed. The first was a radio receiver, such as the Icom PCR-1000, that could tune into the Reverse Channel, which is the frequency that the phones transmit data to the tower on. The second item was PC with a sound card and a software program called Banpaia, and the third item was a phone that could easily be used for cloning, such as the Oki 900. By tuning the radio to the proper frequency, it would receive the signal transmitted by the cell phone to be cloned, containing the phone's ESN/MIN Pair. This signal would be fed into the sound card audio input of the PC, and Banpaia would decode the ESN/MIN pair from this signal and display it on the screen. The person could then input that data into the Oki 900 phone and reboot it, after which the phone network could not distinguish the Oki from the original phone whose signal had been received. This gave the cloner, through the Oki phone, the ability to use the mobile phone service of the legitimate subscriber whose phone was cloned just as if that phone had been physically stolen instead, except that the subscriber was not without his or her phone and was not aware that the phone had been cloned—at least until that subscriber received his or her next bill.

The problem became so large that some carriers required the use of a PIN before making calls. Eventually, the cellular companies initiated a system called RF Fingerprinting, where it could determine subtle differences in the signal of one phone from another and shut down some cloned phones. Some legitimate customers had problems with this though if they made certain changes to their own phone, such as replacing the battery and/or antenna. The Oki 900 was the ultimate tool of cell phone hackers because it could listen in to AMPS phone calls right out of the box with no hardware modifications.

### 5.1.1 Digital - Advanced Mobile Phone System (D-AMPS)

The first digital version of AMPS, also using the 800 MHz spectrum. Still used (though not widely) in certain countries including Bolivia, Brazil, Canada, El Salvador, Israel, Malaysia, Myanmar, Panama, Russia, Ukraine, Uzbekistan, and Vietnam.

### Personal communications network

Personal communications network (PCN) is the European digital cellular mobile telephone network, developed in accordance with GSM standards. The PCN system was first initiated by Lord Young, UK Secretary of State for Trade and Industry, in 1988. The main characteristics of PCN are as follows:

- i. Operating frequency – 1.7–1.88 GHz (1710–1785 MHz and 1805–1880 MHz).
- ii. Uses 30 GHz or up for microwave back bone system.
- iii. Covers both small cells and large cells.
- iv. Coverage inside and outside buildings.
- v. Hand over.
- vi. Cell delivery.
- vii. Portable hand set.
- viii. User intelligent network.

PCN uses the DCS-1800 systems, which is similar to GSM, but up converts the frequency to 1.7–1.88 GHz, therefore the network structure, the signal structure and the transmission characteristics are similar between PCN and GSM, but operational frequencies are different.

## 5.2 GSM

GSM (Global System for Mobile communication) is a digital mobile telephony system that is widely used in Europe and other parts of the world. GSM uses a variation of time division technologies (TDMA, GSM, and CDMA). GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHz or 1800 MHz frequency band.

Mobile services based on GSM technology were first launched in Finland in 1991. Today, more than 690 mobile networks provide GSM services across 213 countries and GSM represents 82.4% of all global mobile connections. According to GSM World, there are now more than 2 billion GSM mobile phone users worldwide. GSM World references China as "the largest single GSM market, with more than 370 million users, followed by Russia with 145 million, India with 83 million and the USA with 78 million users."

GSM, together with other technologies, is part of the evolution of wireless mobile telecommunications that includes High-Speed Circuit-Switched Data (HSCSD), General Packet Radio System (GPRS), Enhanced Data GSM Environment (EDGE), and Universal Mobile Telecommunications Service (UMTS).

### 5.2.1 History of GSM

During the early 1980s, analog cellular telephone systems were experiencing rapid growth in Europe, particularly in Scandinavia and the United Kingdom, but also in France and Germany. Each country developed its own system, which was incompatible with everyone else's in equipment and operation. This was an undesirable situation, because not only was the mobile equipment limited to operation within national boundaries, which in a unified Europe were increasingly unimportant, but there was also a very limited market for each type of equipment, so economies of scale and the subsequent savings could not be realized.

The Europeans realized this early on, and in 1982 the Conference of European Posts and Telegraphs (CEPT) formed a study group called the Groupe Spécial Mobile (GSM) to study and develop a pan-European public land mobile system. The proposed system had to meet certain criteria:

i. Good subjective speech quality
ii. Low terminal and service cost
iii. Support for international roaming
iv. Ability to support handheld terminals
v. Support for range of new services and facilities
vi. Spectral efficiency
vii. ISDN compatibility

In 1989, GSM responsibility was transferred to the European Telecommunication Standards Institute (ETSI), and phase I of the GSM specifications were published in 1990. Commercial service was started in mid-1991, and by 1993 there were 36 GSM networks in 22 countries. Although standardized in Europe, GSM is not only a European standard. Over 200 GSM networks (including DCS1800 and PCS1900) are operational in 110 countries around the world. In the beginning of 1994, there were 1.3 million subscribers worldwide, which had grown to more than 55 million by October 1997. With North America making a delayed entry into the GSM field with a derivative of GSM called PCS1900, GSM systems exist on every continent, and the acronym GSM now aptly stands for Global System for Mobile communications.

The developers of GSM chose an unproven (at the time) digital system, as opposed to the then standard analog cellular systems like AMPS in the United States and TACS in the United Kingdom. They had faith that advancements in compression algorithms and digital signal processors would allow the fulfillment of the original criteria and the continual improvement of the system in terms of quality and cost. The over 8000 pages of GSM recommendations try to allow flexibility and competitive innovation among suppliers, but provide enough standardization to guarantee proper interworking between the components of the system. This is done by providing functional and interface descriptions for each of the functional entities defined in the system.

### 5.2.2 Services provided by GSM

From the beginning, the planners of GSM wanted ISDN compatibility in terms of the services offered and the control signalling used. However, radio transmission limitations, in terms of bandwidth and cost, do not allow the standard ISDN B-channel bit rate of 64 kbps to be practically achieved.

Using the ITU-T definitions, telecommunication services can be divided into bearer services, teleservices, and supplementary services. The most basic teleservice supported by GSM is telephony. As with all other communications, speech is digitally encoded and transmitted through the GSM network as a digital stream. There is also an emergency service, where the nearest emergency-service provider is notified by dialing three digits (similar to 911).

A variety of data services is offered. GSM users can send and receive data, at rates up to 9600 bps, to users on POTS (Plain Old Telephone Service), ISDN, Packet Switched Public Data Networks, and Circuit Switched Public Data Networks using a variety of access methods and protocols, such as X.25 or X.32. Since GSM is a digital network, a modem is not required between the user and GSM network, although an audio modem is required inside the GSM network to interwork with POTS.

Other data services include Group 3 facsimile, as described in ITU-T recommendation T.30, which is supported by use of an appropriate fax adaptor. A unique feature of GSM, not found in older analog systems, is the Short Message Service (SMS). SMS is a bidirectional service for short alphanumeric (up to 160 bytes) messages. Messages are transported in a store-and-forward fashion. For point-to-point SMS, a message can be sent to another subscriber to the service, and an acknowledgement of receipt is provided to the sender. SMS can also be used in a cellbroadcast mode, for sending messages such as traffic updates or news updates. Messages can also be stored in the SIM card for later retrieval .

Supplementary services are provided on top of teleservices or bearer services. In the current (Phase I) specifications, they include several forms of call forward (such as call forwarding when the mobile subscriber is unreachable by the network), and call barring of outgoing or incoming calls, for example when roaming in another country. Many additional supplementary services will be provided in the Phase 2 specifications, such as caller identification, call waiting, multiparty conversations.

### 5.2.3 Architecture of the GSM network

A GSM network is composed of several functional entities, whose functions and interfaces are specified. Figure below shows the layout of a generic GSM network. The GSM network can be divided into three broad parts. The Mobile Station is carried by the subscriber. The Base Station Subsystem controls the radio link with the Mobile Station. The Network Subsystem, the main part of which is the Mobile services Switching Center (MSC), performs the switching of calls between the mobile users, and between mobile and fixed network users. The MSC also handles the mobility management operations. Not shown is the Operations and Maintenance Center, which oversees the proper operation and setup of the network. The Mobile Station and the Base Station Subsystem communicate across the Um interface, also known as the air interface or radio link. The Base Station Subsystem communicates with the Mobile services Switching Center across the A interface.

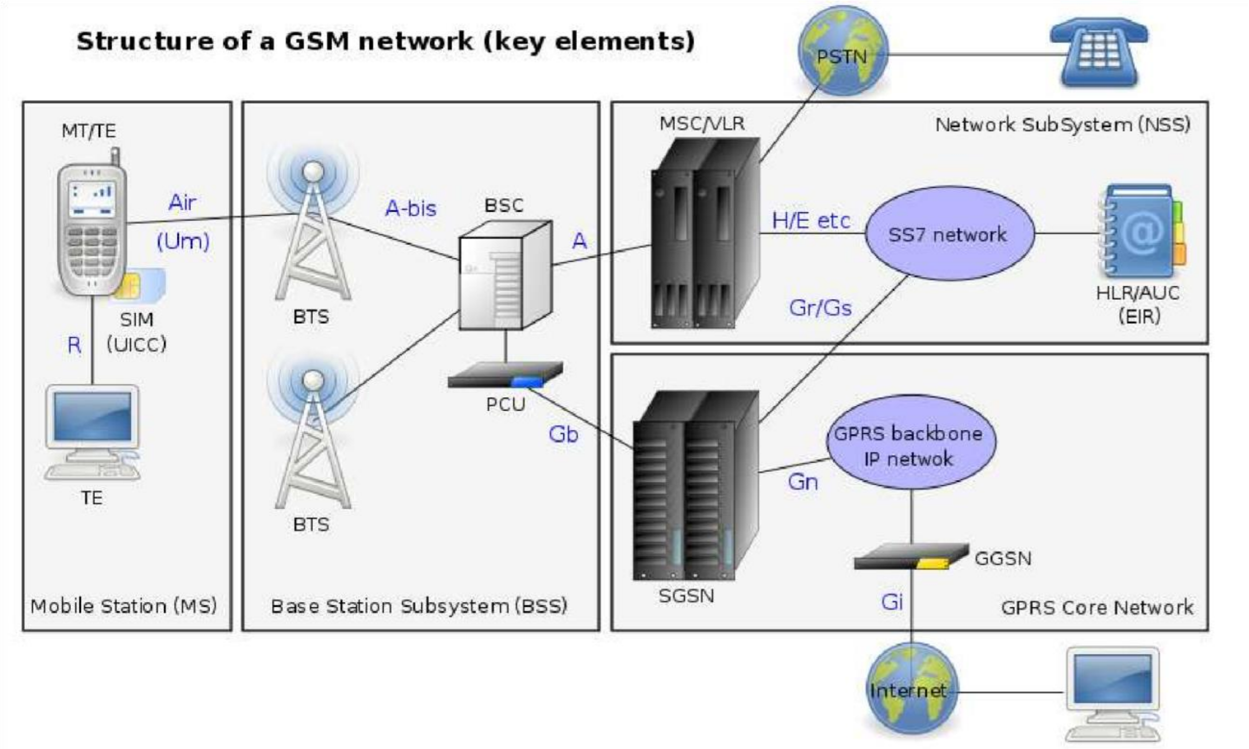

*Fig 5.1: GSM structure*

***Mobile Station***

The mobile station (MS) consists of the mobile equipment (the terminal) and a smart card called the Subscriber Identity Module (SIM). The SIM provides personal mobility, so that the user can have access to subscribed services irrespective of a specific terminal. By inserting the SIM card into another GSM terminal, the user is able to receive calls at that terminal, make calls from that terminal, and receive other subscribed services.

The mobile equipment is uniquely identified by the International Mobile Equipment Identity (IMEI). The SIM card contains the International Mobile Subscriber Identity (IMSI) used to identify the subscriber to the system, a secret key for authentication, and other information. The IMEI and the IMSI are independent, thereby allowing personal mobility. The SIM card may be protected against unauthorized use by a password or personal identity number.

***Base Station Subsystem***

The Base Station Subsystem is composed of two parts, the Base Transceiver Station (BTS) and the Base Station Controller (BSC). These communicate across the standardized Abis interface, allowing (as in the rest of the system) operation between components made by different suppliers.

The Base Transceiver Station houses the radio tranceivers that define a cell and handles the radio-link protocols with the Mobile Station. In a large urban area, there will potentially be a large number of BTSs deployed, thus the requirements for a BTS are ruggedness, reliability, portability, and minimum cost.

The Base Station Controller manages the radio resources for one or more BTSs. It handles radio channel setup, frequency hopping, and handovers, as described below. The BSC is the connection between the mobile station and the Mobile service Switching Center (MSC).

***Network Subsystem***

The central component of the Network Subsystem is the Mobile services Switching Center (MSC). It acts like a normal switching node of the PSTN or ISDN, and additionally provides all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber. These services are provided in conjunction with several functional entities, which together form the Network Subsystem. The MSC provides the connection to the fixed networks (such as the PSTN or ISDN). Signaling between functional entities in the Network Subsystem uses Signaling System Number 7 (SS7), used for trunk signaling in ISDN and widely used in current public networks.

The Home Location Register (HLR) and Visitor Location Register (VLR), together with the MSC, provide the call-routing and roaming capabilities of GSM. The HLR contains all the administrative information of each subscriber registered in the corresponding GSM network, along with the current location of the mobile. The location of the mobile is typically in the form of the signaling address of the VLR associated with the mobile station. The actual routing procedure will be described later. There is logically one HLR per GSM network, although it may be implemented as a distributed database.

The Visitor Location Register (VLR) contains selected administrative information from the HLR, necessary for call control and provision of the subscribed services, for each mobile currently located in the geographical area controlled by the VLR. Although each functional entity can be implemented as an independent unit, all manufacturers of switching equipment to date implement the VLR together with the MSC, so that the geographical area controlled by the MSC corresponds to that controlled by the VLR, thus simplifying the signalling required. Note that the MSC contains no information about particular mobile stations --- this information is stored in the location registers.

The other two registers are used for authentication and security purposes. The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment on the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI). An IMEI is marked as invalid if it has been reported stolen or is not type approved. The Authentication Center (AuC) is a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and encryption over the radio channel.

**Revision question**

1. What is GSM?
2. How does GSM facilitate mobile communication?
3. What are the components in a GSM network?
4. How does DAMPS operate?