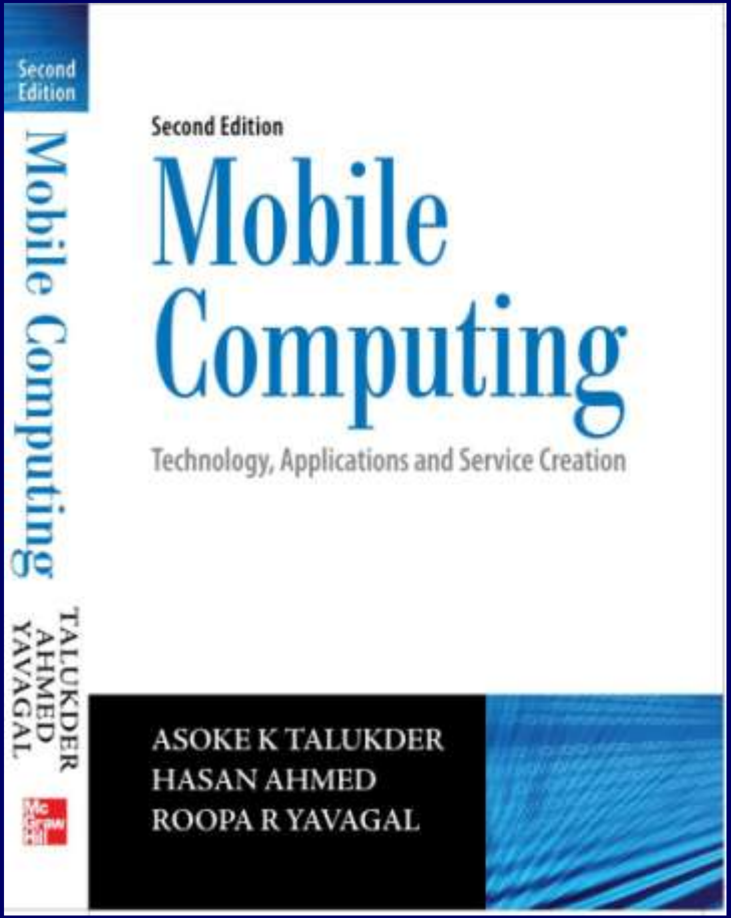


Second Edition

Second Edition

Mobile Computing

Technology, Applications and Service Creation

ASOKE K TALUKDER
HASAN AHMED
ROOPA R YAVAGAL

Mobile Computing

TALUKDER
AHMED
YAVAGAL

Mobile Computing

Chapter 5

GSM

Asoke K Talukder

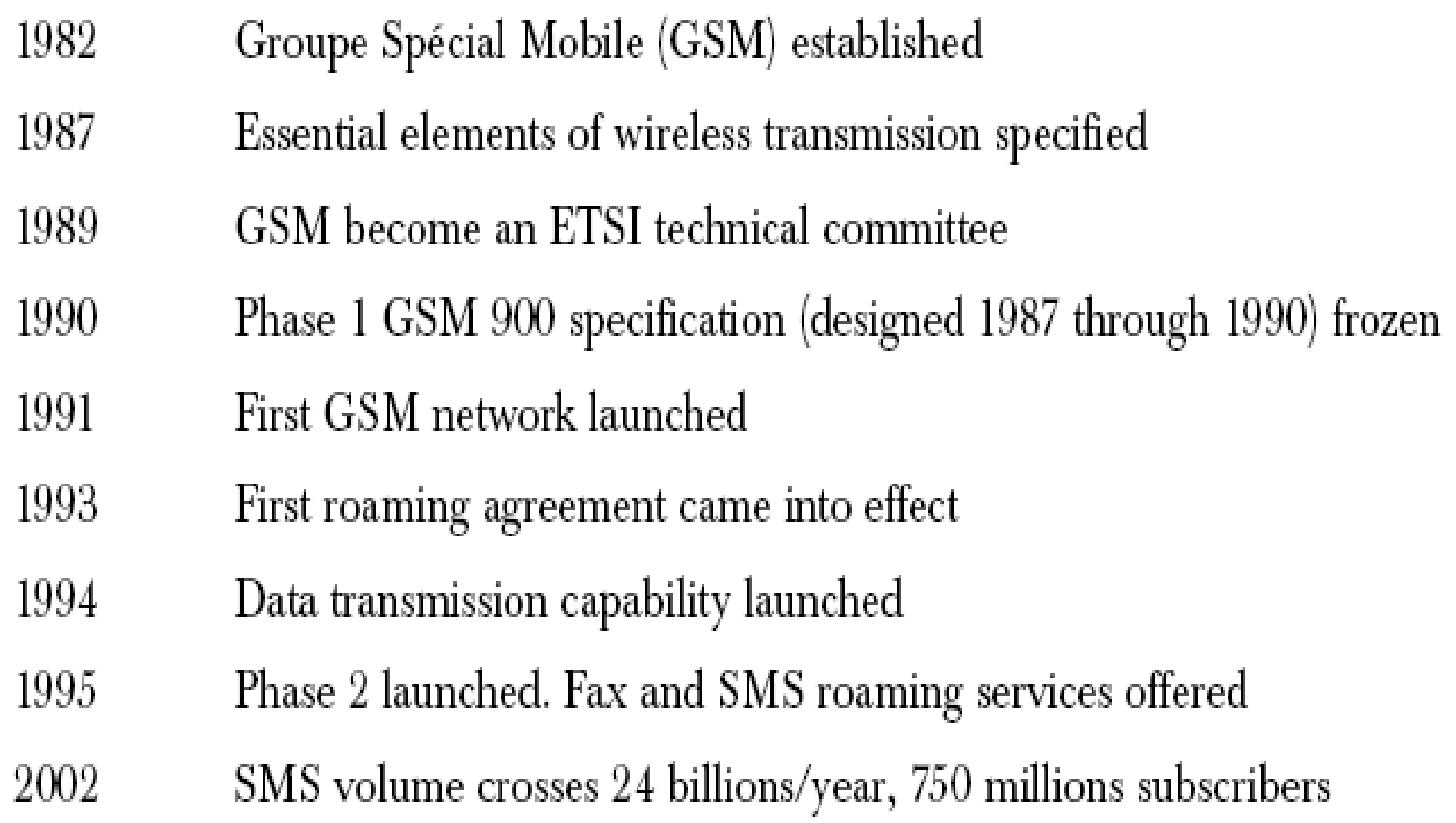
Hasan Ahmed

Global System for Mobile Communications

- Originally GSM stood for Groupe Speciale Mobile
- GSM to meet the following business objectives

1. Support for international roaming
2. Good speech quality
3. Ability to support handheld terminals
4. Low terminal and service cost
5. Spectral efficiency
6. Support for a range of new services and facilities
7. ISDN compatibility

GSM Timeline



1982	Groupe Spécial Mobile (GSM) established
1987	Essential elements of wireless transmission specified
1989	GSM become an ETSI technical committee
1990	Phase 1 GSM 900 specification (designed 1987 through 1990) frozen
1991	First GSM network launched
1993	First roaming agreement came into effect
1994	Data transmission capability launched
1995	Phase 2 launched. Fax and SMS roaming services offered
2002	SMS volume crosses 24 billions/year, 750 millions subscribers

Use of TDMA and FDMA in GSM

❑ Uses a combination of FDMA (Frequency Division Multiple Access) and TDMA (Time Division Multiple Access)

❑ Allocation of 50 MHz (890–915 MHz and 935–960 MHz) bandwidth in the 900 MHz frequency band and using FDMA further divided into 124 (125 channels, 1 not used) channels each with a carrier bandwidth of 200 KHz

❑ Using TDMA, each of the above mentioned channels is then further divided into 8 time slots

❑ So, with the combination of FDMA and TDMA, a maximum of992 channels for transmit and receive can be realized

Frequency reuse in GSM

- To serve hundreds of thousands of users, the frequency must be reused and this is done through cells.

- The area to be covered is subdivided into radio zones or cells. Though in reality these cells could be of any shape, for convenient modeling purposes these are modeled as hexagons. Base stations are positioned at the center of these cells.

- Each cell *i* receives a subset of frequencies *fbi* from the total set assigned to the respective mobile network. To avoid any type of co-channel interference, two neighboring cells never use the same frequencies.

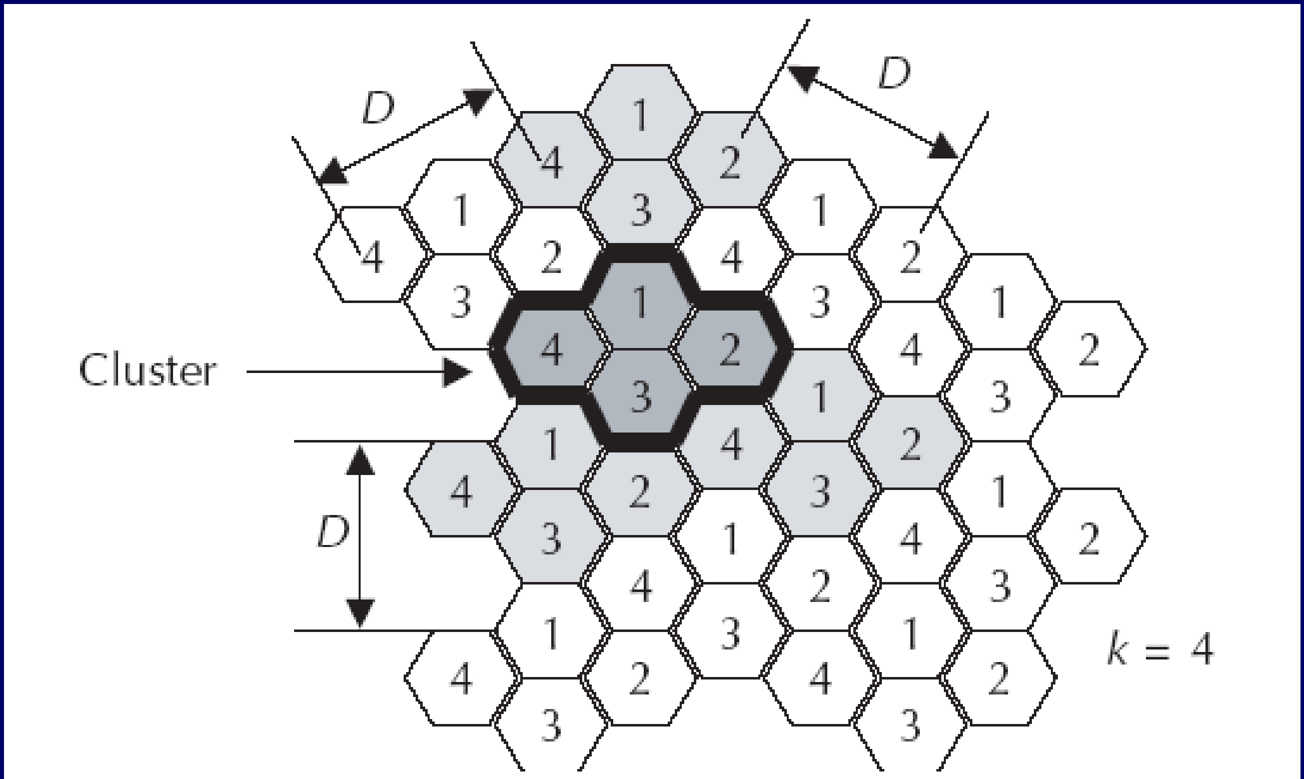
Frequency reuse in GSM

❑ Only at a distance of *D* (known as frequency reuse distance), the same frequency from the set *fbi* can be reused. Cells with distance *D* from cell *i*, can be assigned one or all the frequencies from the set *fbi* belonging to cell *i*.

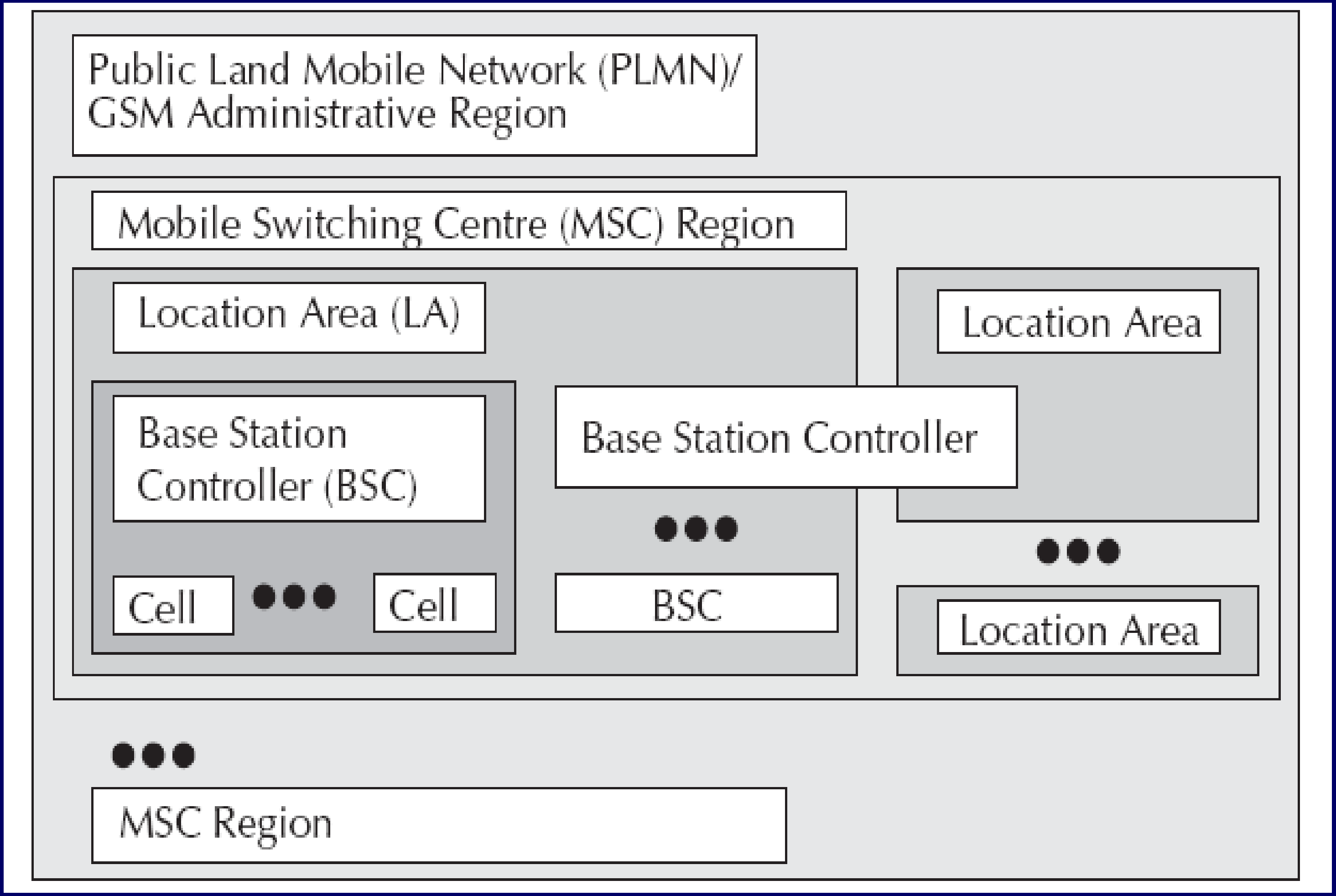
❑ When moving from one cell to another during an ongoing conversation, an automatic channel change occurs. This phenomenon is called handover. Handover maintains an active speech and data connection over cell boundaries.

❑ The regular repetition of frequencies in cells result in a clustering of cells. The clusters generated in this way can consume the whole frequency band. The size of a cluster is defined by *k*, the number of cells in the cluster. This also defines the frequency reuse distance *D*. The figure in next slide shows an example of cluster size of 4.

Cell clusters in GSM



GSM System Hierarchy



Public Land Mobile Network (PLMN)/
GSM Administrative Region

Mobile Switching Centre (MSC) Region

Location Area (LA)

Base Station
Controller (BSC)

Cell ●●● Cell

Base Station Controller

●●●

BSC

Location Area

●●●

Location Area

●●●

MSC Region

GSM System Hierarchy

- Consists at the minimum one administrative region assigned to one MSC (Mobile Switching Centre)

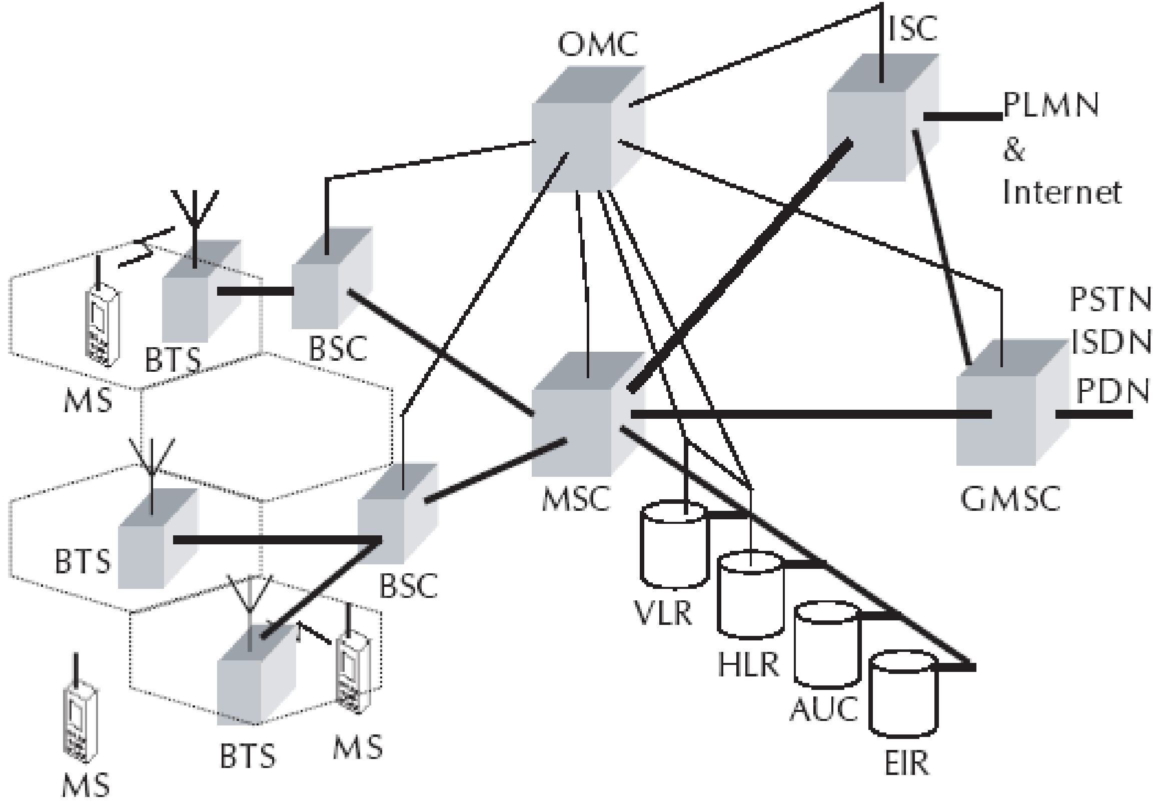
- Administrative region is commonly known as PLMN (Public Land Mobile Network)

- Each administrative region is subdivided into one or many Location Area (LA)

- One LA consists of many cell groups and each cell group is assigned to one BSC (Base Station Controller)

- For each LA, there will be at least one BSC while cells in one BSC can belong to different LAs

GSM Architecture



BTS	Base Transceiver Station
BSC	Base Station Controller
MSC	Mobile Switching Center
GMSC	Gateway MSC
ISC	International Switching Center

MS	Mobile Station
HLR	Home Location Register
VLR	Visitor Location Register
AUC	Authentication Center
EIR	Equipment Identity Register
OMC	Operation and Maintenance Center

GSM Architecture

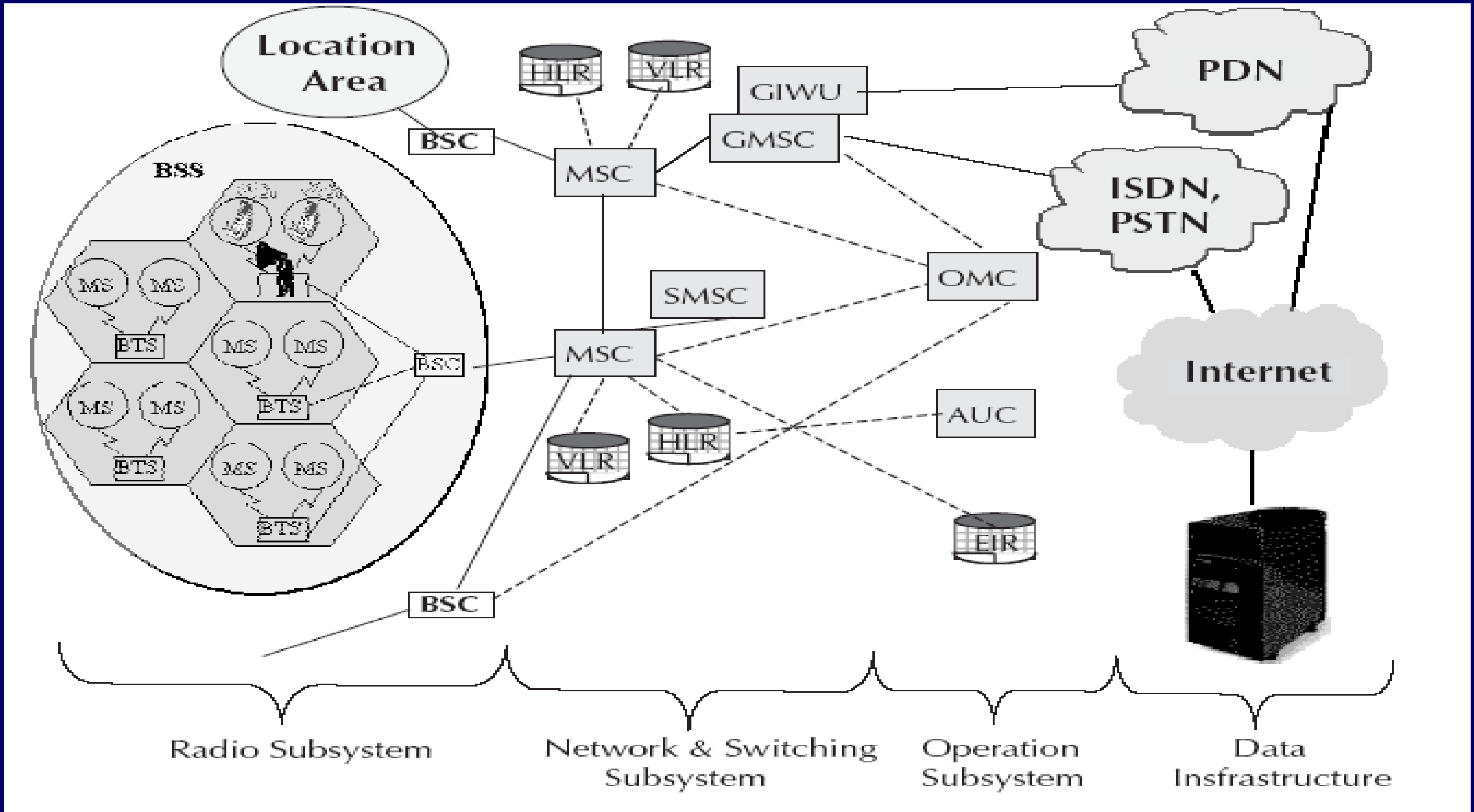
❑ Cells are formed by the radio areas covered by a BTS (Base Transceiver Station)

❑ Several BTSs are controlled by one BSC

❑ Traffic from the MS (Mobile Station) is routed through MSC

❑ Calls originating from or terminating in a fixed network or other mobile networks is handled by the GMSC (Gateway MSC)

Operational Architecture of GSM



BTS	Base Transceiver Station	ISDN	Integrated System Digital Network
BSC	Base Station Controller	HLR	Home Location Register
MSC	Mobile Switching Center	VLR	Visitor Location Register
GMSC	Gateway MSC	AUC	Authentication Center
SC	Service Center/SMS Controller	EIR	Equipment Identity Register
GIWU	Gateway Interworking Unit	OMC	Operation and Maintenance Center
PDN	Public Data Network	PSTN	Public Switched Telephone Network
MS	Mobile Station		

Home Location Register (HLR) in GSM

- ❑ It contains the following information:

1. Authentication information like International Mobile Subscriber Identity (IMSI)
2. Identification information like name, address, etc. of the subscriber
3. Identification information like Mobile Subscriber ISDN (MSISDN) etc.
4. Billing information like prepaid or postpaid
5. Operator selected denial of service to a subscriber

Home Location Register (HLR) in GSM

6. Handling of supplementary services like for CFU (Call Forwarding Unconditional), CFB (Call Forwarding Busy), CFNR (Call Forwarding Not Reachable) or CFNA (Call Forwarding Not Answered)
7. Storage of SMS Service Center (SC) number in case the mobile is not connectable so that whenever the mobile is connectable, a paging signal is sent to the SC
8. Provisioning information like whether long distance and international calls allowed or not
9. Provisioning information like whether roaming is enabled or not

Home Location Register (HLR) in GSM

10. Information related to auxiliary services like Voice mail, data, fax services, etc.
11. Information related to auxiliary services like CLI (Caller Line Identification), etc.
12. Information related to supplementary services for call routing. In GSM network, one can customize the personal profile to the extent that while the subscriber is roaming in a foreign PLMN, incoming calls can be barred. Also, outgoing international calls can be barred, etc.
13. Some variable information like pointer to the VLR, location area of the subscriber, Power OFF status of the handset, etc.

Entities in GSM

- The Mobile Station (MS) - This includes the Mobile Equipment (ME) and the Subscriber Identity Module (SIM).

- The Base Station Subsystem (BSS) - This includes the Base Transceiver Station (BTS) and the Base Station Controller (BSC).

- The Network and Switching Subsystem (NSS) - This includes Mobile Switching Center (MSC), Home Location Register (HLR), Visitor Location Register (VLR), Equipment Identity Register (EIR), and the Authentication Center (AUC).

- The Operation and Support Subsystem (OSS) - This includes the Operation and Maintenance Center (OMC).

Mobile Station

❑ Mobile Station (MS) consists of two main elements: mobile equipment or mobile device (that is the phone without the SIM card) and Subscriber Identity Module (SIM)

❑ Terminals distinguished principally by their power and application

❑ SIM is installed in every GSM phone and identifies the terminal

❑ SIM cards used in GSM phones are smart processor cards with a processor and a small memory

❑ SIM card contains the International Mobile Subscriber Identity (IMSI) used to identify the subscriber to the system, a secret key for authentication, and other security information

Base Station Subsystem

❑ Base Station Subsystem (BSS) connects the Mobile Station and the Network and Switching Subsystem (NSS)

❑ In charge of the transmission and reception for the last mile

❑ BSS can be divided into two parts: Base Transceiver Station (BTS) or Base Station and Base Station Controller (BSC)

❑ Base Transceiver Station corresponds to the transceivers and antennas used in each cell of the network

❑ BTS is usually placed in the center of a cell and its transmitting power defines the size of a cell

Base Station Subsystem

❑ BTS houses the radio transmitter and the receivers that define a cell and handles the radio-link protocols with the Mobile Station while handling between one and sixteen transceivers depending on the density of users in the cell

❑ Base Station Controller is the connection between the BTS and the Mobile service Switching Center (MSC) and manages the radio resources for one or more BTSs

❑ BSC handles handovers, radio-channel setup, control of radio frequency power levels of the BTSs, exchange function, and the frequency hopping

Network and Switching Subsystem

- ❑ Central component of the Network Subsystem is the Mobile Switching Center (MSC)
- ❑ Signaling between functional entities in the Network Subsystem uses Signaling System Number 7 (SS7)
- ❑ MSC together with Home Location Register (HLR) and Visitor Location Register (VLR) databases, provide the call-routing and roaming capabilities of GSM
- ❑ MSC does the following functions:

1. It acts like a normal switching node for mobile subscribers of the same network (connection between mobile phone to mobile phone within the same network)

Network and Switching Subsystem

2. It acts like a normal switching node for the PSTN fixed telephone (connection between mobile phone to fixed phone)

3. It acts like a normal switching node for ISDN

4. It provides all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, handovers and call routing

5. It includes databases needed in order to store information to manage the mobility of a roaming subscriber

Network Switching Subsystem

❑ MSC together with Home Location Register (HLR) and Visitor Location Register (VLR) databases, provide the call-routing and roaming capabilities of GSM

❑ HLR contains all the administrative information of each subscriber registered in the corresponding GSM network

❑ Location of the mobile is typically in the form of the signaling address of the VLR associated with the mobile station

❑ HLR is always fixed and stored in the home network, whereas the VLR logically moves with the subscriber

❑ VLR is similar to a cache, whereas HLR is the persistent storage

Network and Switching Subsystem

❑ VLR contains selected administrative information borrowed from the HLR, necessary for call control and provisioning of the subscribed services

❑ When a subscriber enters the covering area of a new MSC, the VLR associated with this MSC can request information about the new subscriber from its corresponding HLR in the home network

❑ There is a component called Gateway MSC (GMSC) that is associated with the MSC

Network and Switching Subsystem

❑ GMSC is the interface between the mobile cellular network and the PSTN and also is in charge of routing calls from the fixed network towards a GSM user and vice versa

❑ GMSC is often implemented in the same node as the MSC

❑ GIWU (GSM Inter Working Unit) corresponds to an interface to various networks for data communications

Operation and Support Subsystem

❑ Operations and Support Subsystem (OSS) controls and monitors the GSM system

❑ OSS is connected to the different components of the NSS and to the BSC and also in charge of controlling the traffic load of the BSS

❑ Equipment Identity Register (EIR) rests with OSS

❑ EIR is a database that contains a list of all valid mobile equipment within the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI)

❑ EIR contains a list of IMEIs of all valid terminals

Operation and Support Subsystem

- ❑ An IMEI is marked as invalid if it has been reported stolen or is not type approved

- ❑ The EIR allows the MSC to forbid calls from this stolen or unauthorized terminals

- ❑ Authentication Center (AUC) is responsible for the authentication of a subscriber

- ❑ AUC is a protected database and stores a copy of the secret key stored in each subscriber’s SIM card

Short Message Service

❑ Short Message Service (SMS) is one of the most popular services within GSM

❑ SMS is a data service and allows a user to enter text message up to 160 characters in length when 7 bit English characters are used

❑ SMS is a proactive bearer and is an ‘always on’ network

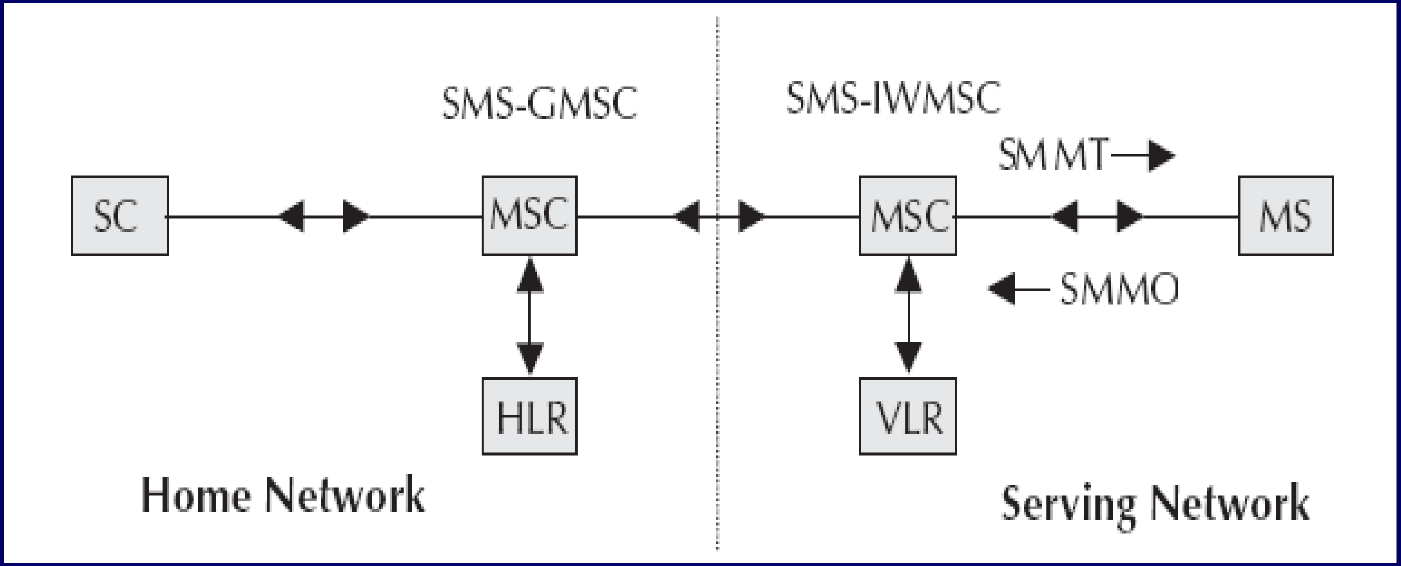
❑ Message center is referred to as Service Centre (SC) or SMS Controller (SMSC)

❑ SMSC is a system within the core GSM network which works as the store and forward system for SMS messages

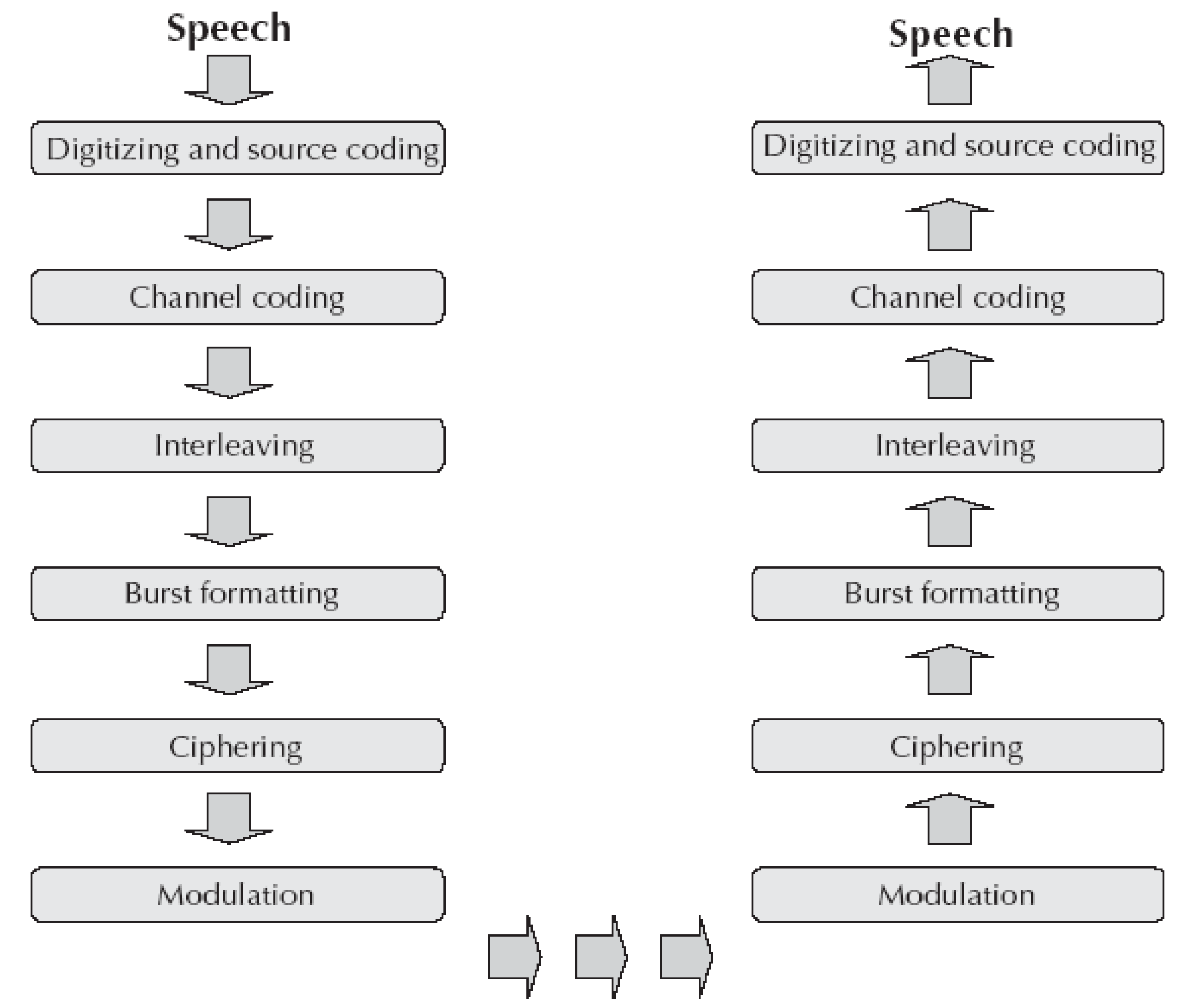
SMS

- Two types of SMS: SMMT (Short Message Mobile Terminated Point-to-Point) and SMMO (Short Message Mobile Originated Point-to-Point)
- SMMT is an incoming short message from the network and is terminated in the MS (phone or Mobile Station)
- SMMO is an outgoing message originated in the MS, and forwarded to the network for delivery
- For an outgoing message, the SMS is sent from the phone to SC via the VLR and the Inter Working MSC (IWMSC)
- For incoming message, the path is from SC to the MS via the HLR and the Gateway MSC (GMSC)

SMS Transfer



From speech to radio waves



From speech to radio waves

- ❑ Digitizer and source coding: The user speech is digitized at 8 KHz sampling rate using Regular Pulse Excited–Linear Predictive Coder (RPE–LPC) with a Long Term Predictor loop where information from previous samples is used to predict the current sample. Each sample is then represented in signed 13-bit linear PCM value. This digitized data is passed to the coder with frames of 160 samples where encoder compresses these 160 samples into 260-bits GSM frames resulting in one second of speech compressed into 1625 bytes and achieving a rate of 13 Kbits/sec.

From speech to radio waves

❑ Channel coding: This introduces redundancy into the data for error detection and possible error correction where the gross bit rate after channel coding is 22.8 kbps (or 456 bits every 20 ms). These 456 bits are divided into eight 57-bit blocks and the result is interleaved amongst eight successive time slot bursts for protection against burst transmission errors.

❑ Interleaving: This step rearranges a group of bits in a particular way to improve the performance of the error-correction mechanisms. The interleaving decreases the possibility of losing whole bursts during the transmission by dispersing the errors.

❑ Ciphering: This encrypts blocks of user data using a symmetric key shared by the mobile station and the BTS.

From speech to radio waves

❑ Burst formatting: It adds some binary information to the ciphered block for use in synchronization and equalization of the received data.

❑ Modulation: The modulation technique chosen for the GSM system is the Gaussian Minimum Shift Keying (GMSK) where binary data is converted back into analog signal to fit the frequency and time requirements for the multiple access rules. This signal is then radiated as radio wave over the air.

❑ Multipath and equalization: An equaliser is in charge of extracting the ‘right’ signal from the received signal while estimating the channel impulse response of the GSM system and then it constructs an inverse filter. The received signal is then passed through the inverse filter.

From speech to radio waves

❑ Synchronization: For successful operation of a mobile radio system, time and frequency synchronization are needed. Frequency synchronization is necessary so that the transmitter and receiver frequency match (in FDMA) while Time synchronization is necessary to identify the frame boundary and the bits within the frame (in TDMA).

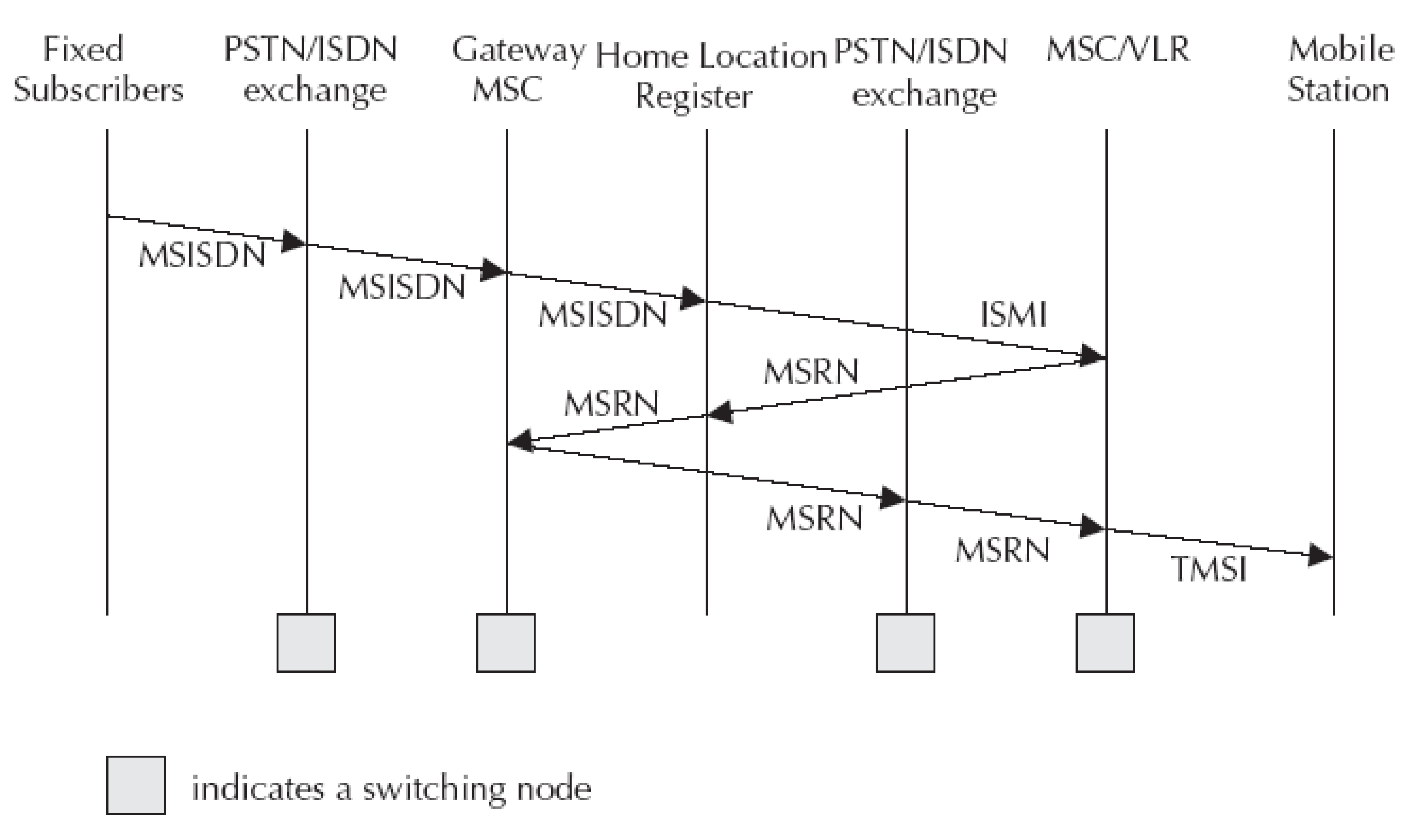
❑ To avoid collisions of burst transmitted by MS with the adjacent timeslot such collisions, the Timing Advance technique is used where frame is advanced in time so that this offsets the delay due to greater distance. Using this technique and the triangulation of the intersection cell sites, the location of a mobile station can be determined from within the network.

Call Routing

- The directory number dialed to reach a mobile subscriber is called the Mobile Subscriber ISDN (MSISDN) which is defined by the E.164 numbering plan and includes a country code and a National Destination Code, which identifies the subscriber’s operator. The first few digits of the remaining subscriber number may identify the subscriber’s HLR within the home PLMN

- For example, the MSISDN number of a subscriber in Bangalore associated with Airtel network is +919845XYYYYY which is a unique number and understood from anywhere in the world. Here, + means prefix for international dialing, 91 is the country code for India and 45 is the network operator’s code (Airtel in this case). X is the level number managed by the network operator ranging from 0 to 9 while YYYYY is the subscriber code which , too, is managed by the operator.

Call Routing



Call Routing

❑ The call first goes to the local PSTN exchange where PSTN exchange looks at the routing table and determines that it is a call to a mobile network.

❑ PSTN forwards the call to the Gateway MSC (GMSC) of the mobile network.

❑ MSC enquires the HLR to determine the status of the subscriber. It will decide whether the call is to be routed or not. If MSC finds that the call can be processed, it will find out the address of the VLR where the mobile is expected to be present.

Call Routing

❑ If VLR is that of a different PLMN, it will forward the call to the foreign PLMN through the Gateway MSC. If the VLR is in the home network, it will determine the Location Area (LA).

❑ Within the LA, it will page and locate the phone and connect the call.

PLMN Interfaces

❑ Basic configuration of a GSM network contains a central HLR and a central VLR where HLR contains all security, provisioning and subscriber related information and VLR stores the location information and other transient data.

❑ MSC needs subscriber parameter for successful call set-up.

❑ Any data related to user call (connection, teardown etc.) are processed with SS7 protocol for signaling using ISUP (ISDN User Part) stack between network nodes.

❑ For mobile specific signaling, a protocol stack called MAP (Mobile Application Part) is used over the SS7 network which does all database transactions and handover/roaming transactions between the MSC.

GSM Addresses and Identifiers

- International Mobile Station Equipment Identity (IMEI): Every mobile equipment in this world has a unique identifier which is called IMEI. IMEI is allocated by the equipment manufacturer and registered by the network operator in the Equipment Identity Register (EIR).

- International Mobile Subscriber Identity (IMSI): When registered with a GSM operator, each subscriber is assigned a unique identifier called IMSI which is stored in the SIM card and secured by the operator. IMSI consists of several parts: 3 decimal digits of Mobile Country Code (MCC), 2 decimal digits of Mobile Network Code (MNC) and a maximum of 10 decimal digits of Mobile Subscriber Identification Number (MSIN) which is a unique number of the subscriber within the home network.

GSM Addresses and Identifiers

❑ Mobile Subscriber ISDN Number (MSISDN): The MSISDN number is the real telephone number as is known to the external world. MSISDN number is public information whereas IMSI is private to the operator. IMSI can be multiple such as when a subscriber opts for fax and data, he is assigned a total of three numbers: one for voice call, one for fax call and another for data call. MSISDN follows the international ISDN (Integrated Systems Data Network) numbering plan.

❑ ISDN has Country Code (CC) of 1 to 3 decimal digits, National Destination Code (NDC) of 2 to 3 decimal digits and Subscriber Number (SN) of maximum 10 decimal digits.

GSM Addresses and Identifiers

- ❑ Location Area Identity: Each LA in a PLMN has its own identifier called Location Area Identifier (LAI) which is structured hierarchically and unique. LAI consists of 3 digits of CC, 2 digits of Mobile Network Code and maximum of 5 digits of Location Area Code.

- ❑ Mobile Station Roaming Number (MSRN): When a subscriber is roaming in another network, a temporary ISDN number is assigned to the subscriber called MSRN. MSRN is assigned by the local VLR in charge of the mobile station and follows the structure of MSISDN.

GSM Addresses and Identifiers

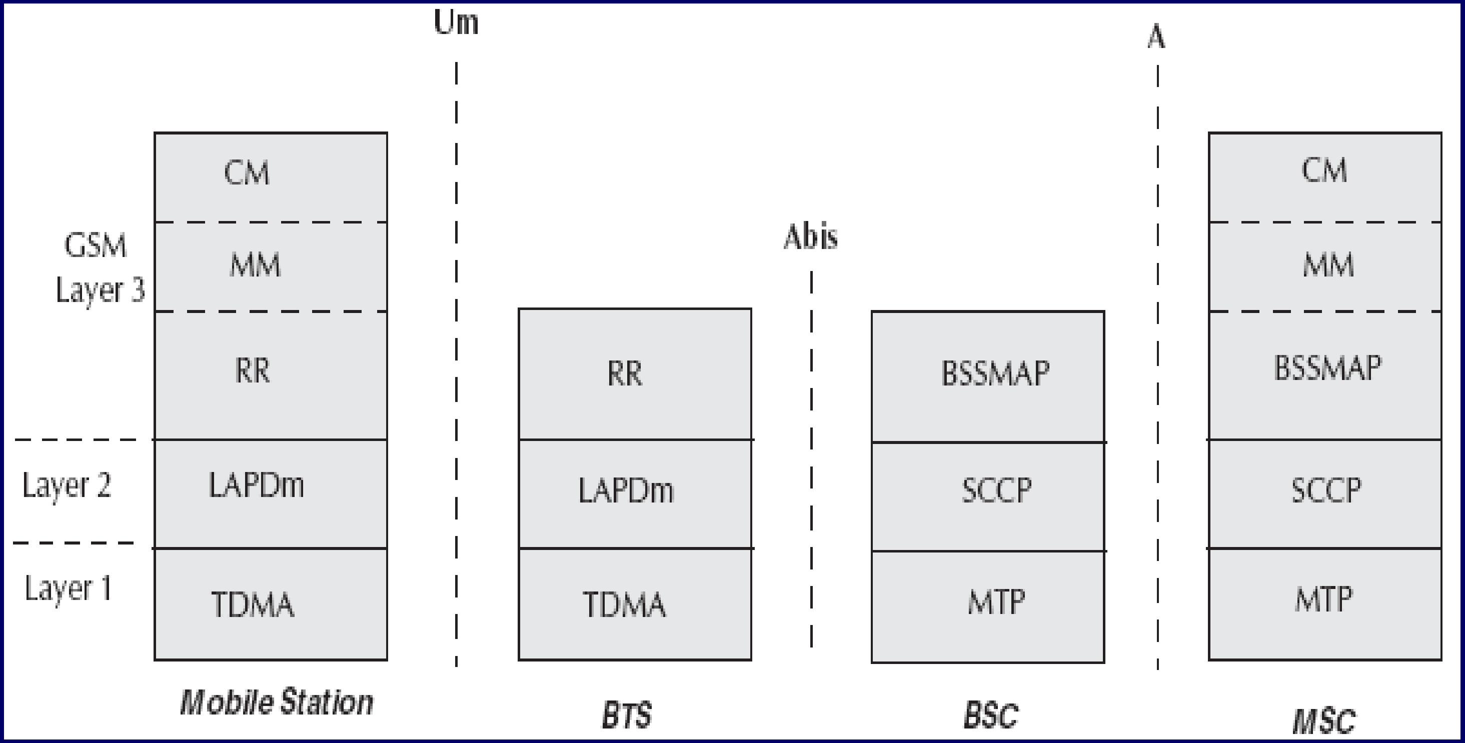
❑ Temporary Mobile Subscriber Identity (TMSI): TMSI is a temporary identifier assigned by the serving VLR used in place of the IMSI for identification and addressing of the mobile station. Together with the current location area, a TMSI allows a subscriber to be identified uniquely.

❑ Local Mobile Subscriber Identity (LMSI): LMSI is assigned by the VLR and stored in the HLR and is used as a searching key for faster database access within the VLR.

❑ Cell Identifier: Within a LA, every cell has a unique Cell Identifier (CI) and together with a LAI, a cell can be identified uniquely through Global Cell Identity (LAI & CI).

❑ MSCs and Location Registers (HLR & VLR) are addressed with ISDN numbers while they may use a Signaling Point Code (SPC) within a PLMN.

Network aspects in GSM



Signaling protocol structure in GSM

Network aspects in GSM

- Layer 1 is the physical layer which uses the channel structures over the air interface.

- Layer 2 is the data link layer and across the Um interface, the data link layer is a modified version of the LAPD protocol used in ISDN or X.25, called LAPDm.

- Across the A interface, the Message Transfer Part layer 2 of Signaling System Number 7 is used.

Network aspects in GSM

- Layer 3 of the GSM signaling protocol is itself divided into three sub-layers:

1. Radio Resources Management: It controls the set-up, maintenance and termination of radio and fixed channels, including handovers.
2. Mobility Management: It manages the location updating and registration procedures as well as security and authentication.
3. Connection Management: It handles general call control and manages Supplementary Services and the Short Message Service.

Handover

- The procedure of change of resources is called handover when the user is mobile while the call is in progress.
- There are four different types of handover in the GSM system, which involve transferring a call between:

1. Channels (time slots) in the same cell
2. Cells (Base Transceiver Stations) under the control of the same Base Station Controller (BSC)
3. Cells under the control of different BSCs but belonging to the same Mobile Switching Center (MSC)
4. Cells under the control of different MSCs

Handover

❑ First two types of handover, called internal handovers, involve only one Base Station Controller (BSC). To save signaling bandwidth, they are managed by the BSC without involving the Mobile services Switching Center (MSC), except to notify it at the completion of the handover.

❑ Last two types of handover, called external handovers, are handled by the MSC.

Mobility Management

- ❑ Mobility Management (MM) function handles the procedures that arise from the mobility of the subscriber and is in charge of all the aspects related to the mobility of the user, especially the roaming, the location management, and the security/authentication of the subscriber.

- ❑ First location update procedure is called the IMSI attach procedure where the MS indicates its IMSI to the network whereas when a mobile station is powered off, it performs an IMSI detach procedure in order to tell the network that it is no longer connected.

Mobility Management

❑ A location update message is sent to the new MSC/VLR which records the location area information and then sends the location information to the subscriber’s HLR.

❑ If the mobile station is authenticated and authorized in the new MSC/VLR, the subscriber’s HLR cancels the registration of the mobile station with the old MSC/VLR.

❑ Location update is also performed periodically and if after the updating time period, the mobile station has not registered, it is then deregistered.

Mobility Management

- When there is an incoming call for a subscriber, the mobile phone needs to be located and a channel needs to be allocated and the call connected.

- A powered-on mobile is informed of an incoming call by a paging message sent over the paging channel of the cells within the current location area while location updating procedures and subsequent call routing use MSC, HLR and VLR.

- If the subscriber is entitled to service, HLR sends a subset of the subscriber information needed for call control to the new MSC/VLR and sends a message to the old MSC/VLR to cancel the old registration.

Mobility Management

❑ An incoming mobile terminating call is directed to the Gateway MSC (GMSC) function which, as a switch, interrogates the subscriber's HLR to obtain routing information and thus contains a table linking MSISDNs to their corresponding HLRs.

❑ The routing information that is returned to the GMSC is the Mobile Station Roaming Number (MSRN).

❑ MSRNs are related to the geographical numbering plan and not visible to subscribers.

Mobility Management

- Generally, GMSC queries the called subscriber’s HLR for an MSRN.

- HLR stores only the SS7 address of the subscriber’s current VLR while VLR temporarily allocates an MSRN from its pool for the call.

- MSRN is returned to the HLR and back to the GMSC, which can then route the call to the new MSC. At new MSC, IMSI corresponding to the MSRN is looked up and the mobile station is paged in its current location area.

- HLR is referred for incoming call whereas VLR is referred for outgoing call.

GSM Frequency Allocation

❑ Normally, GSM uses 900 MHz band wherein 890-915 MHz is allocated for the uplink (mobile station to base station) and 935–960 MHz is allocated for the downlink (base station to mobile station). Each way the bandwidth for the GSM system is 25 MHz which provides 125 carriers uplink/downlink each having a bandwidth of 200 kHz.

❑ ARFCN (Absolute Radio Frequency Channel Numbers) denote a forward and reverse channel pair which is separated in frequency by 45 MHz.

❑ Practically, a guard band of 100 kHz is provided at the upper and lower end of the GSM 900 MHz spectrum and only 124 (duplex) channels are implemented.

GSM Frequency Allocation

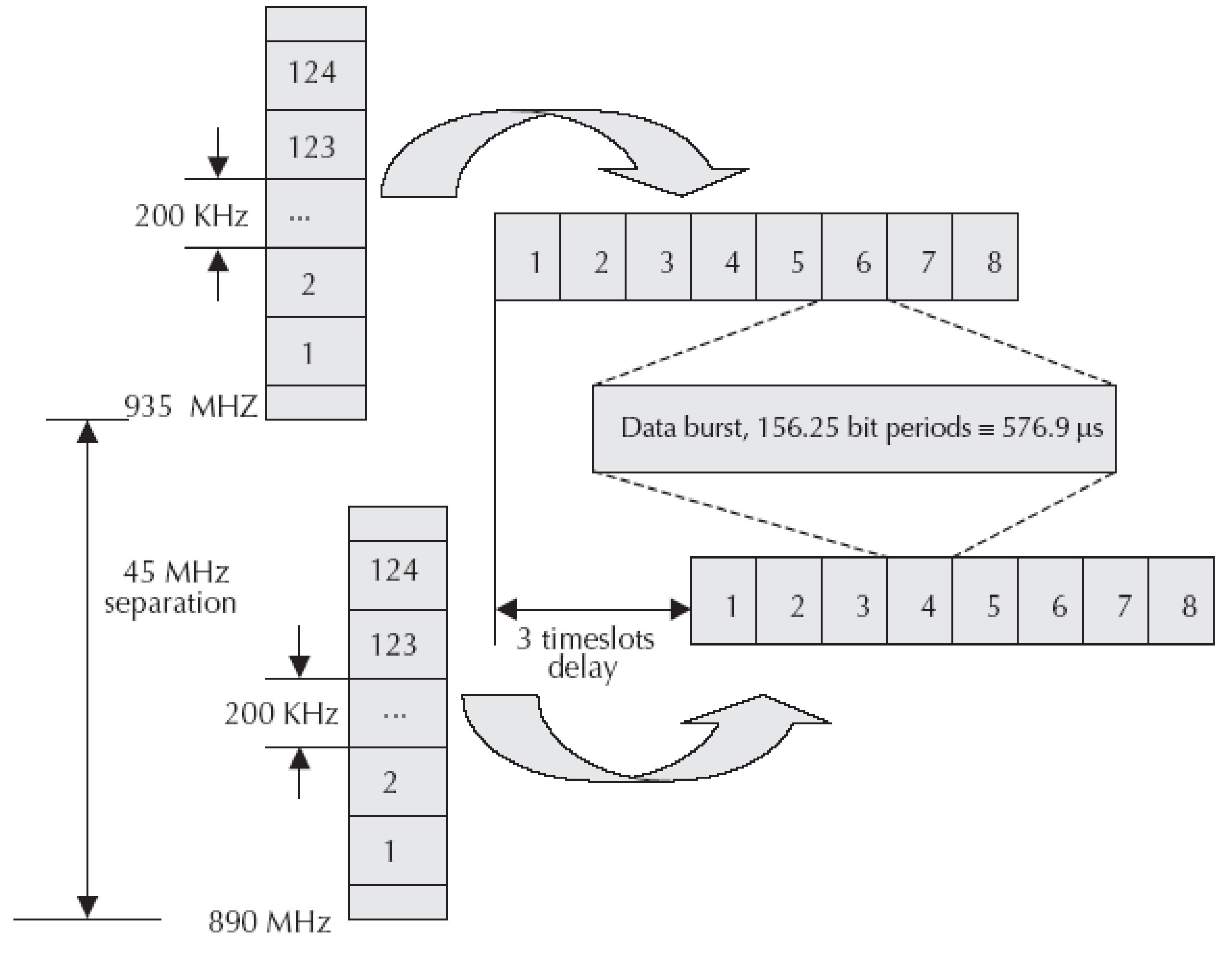
❑ GSM uses a combination of Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA) encoding.

❑ One or more carrier frequencies are assigned to each base station and each of these carrier frequencies is then divided in time using a TDMA scheme where fundamental unit is called a burst period lasting approximately 0.577 ms.

❑ Eight burst periods are grouped into a TDMA frame of approximately 4.615 ms which forms the basic unit for the definition of logical channels.

❑ One physical channel is one burst period per TDMA frame while, normally, channels are defined by the number and position of their corresponding burst periods.

GSM Frequency Allocation



Carrier frequencies and TDMA frames

Authentication and Security

- Authentication involves two functional entities - the SIM card in the mobile phone and the Authentication Center (AUC).

- Following authentication by algorithm A3, a key is generated for encryption.

- An algorithm A8 is used to generate the key while a different algorithm called A5 is used for both ciphering and deciphering procedures for signaling, voice and data.

- So, SS7 signal, voice, data, and SMS within GSM networks are ciphered over the wireless radio interface.

A3 Algorithm

- During authentication, MSC challenges the MS with a random number (RAND).

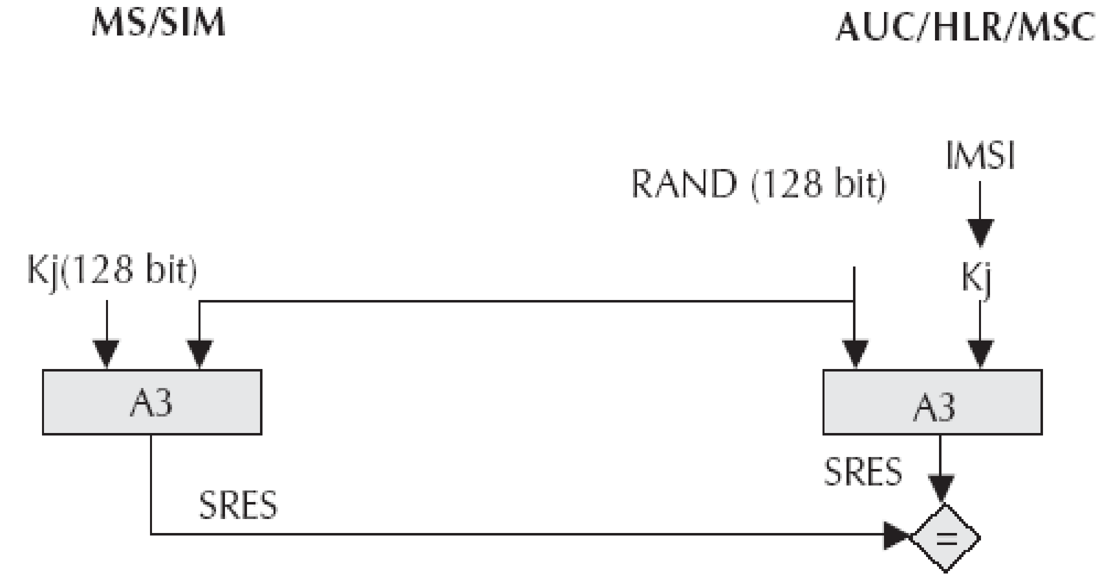
- SIM card uses this RAND received from the MSC and a secret key Kj stored within the SIM as input. Both the RAND and the Kj secret are 128 bits long. Using the A3 algorithm with RAND and Kj as input a 32-bit output called signature response (SRES) is generated in the MS and then sent back to MSC.

- Using the same set of algorithms, the AUC also generates a SRES. The SRES from MS and the SRES generated by the AUC are compared.

- If they are the same, the MS is authenticated.

A3 Algorithm

❑ The idea is that no keys will be transacted over the air. However, if the SRES values calculated independently by the SIM and the AUC are the same, then Kj has to be same and if Kj is same, SIM card is genuine.

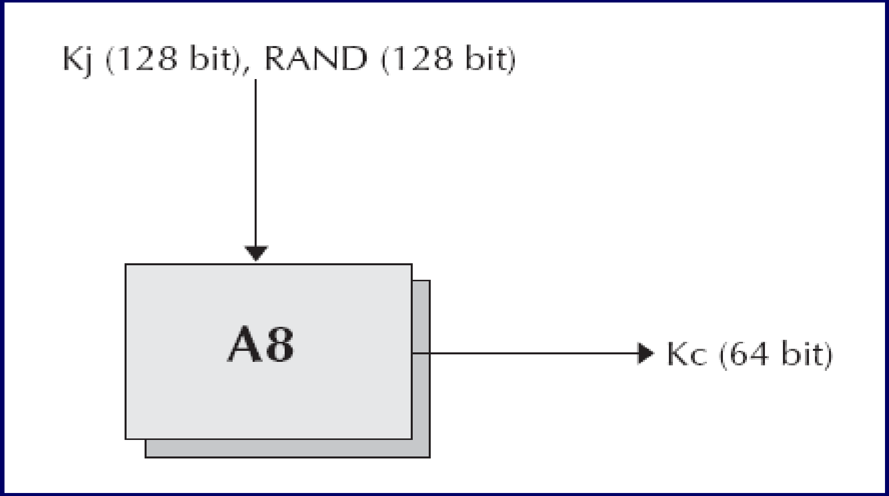


A8 Algorithm

❑ A8 algorithm is the key generation algorithm.

❑ A8 generates a session key, Kc, from the random challenge RAND (received from the MSC) and from the secret key Kj.

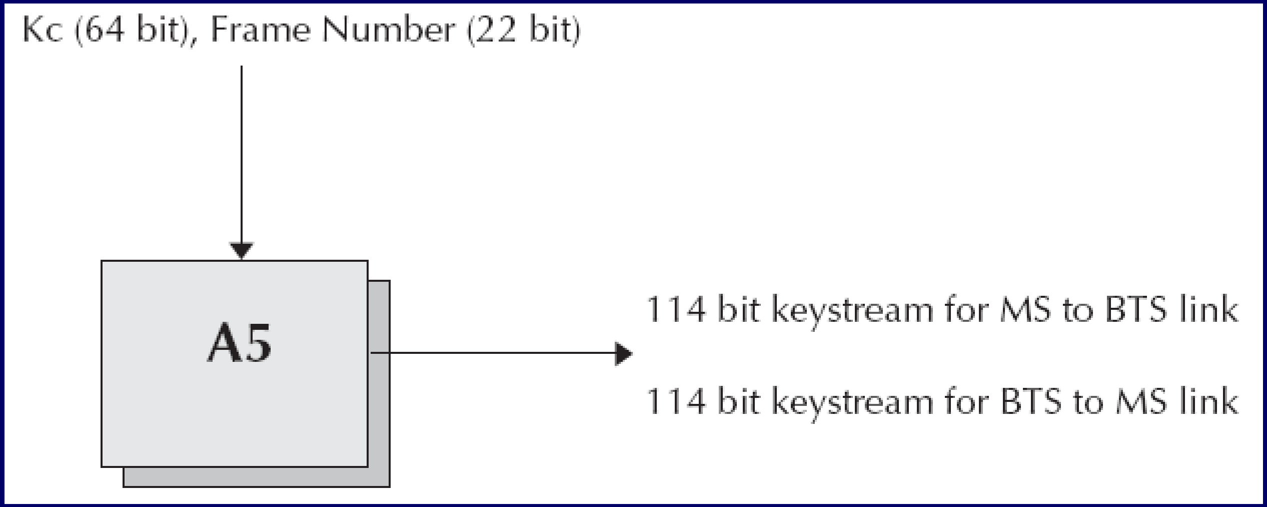
❑ Keys are generated at both the MS and the network end. The session key, Kc, is used for ciphering till the MSC decides to authenticate the MS once again.



A5 Algorithm

- ❑ A5 is the stream cipher algorithm used to encrypt over-the-air transmissions. The stream cipher is initialized all over again for every frame sent with the session key, Kc, and the number of the frame being encrypted or decrypted.

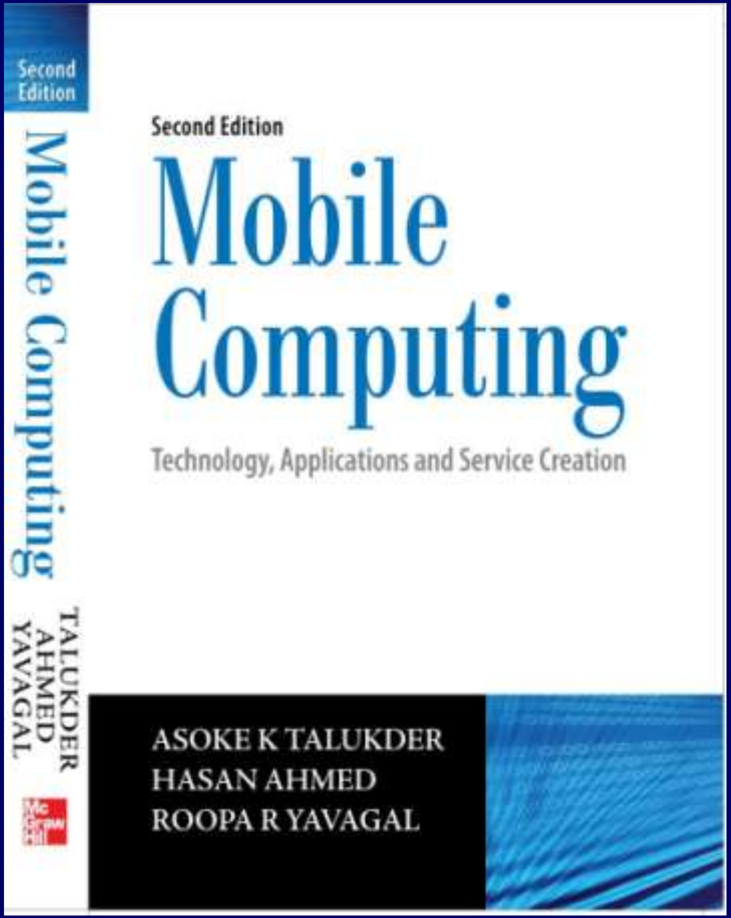
- ❑ Same Kc is used throughout the call but the 22-bit frame number changes during the call, thus, generating a unique key stream for every frame.


Kc (64 bit), Frame Number (22 bit)
A5
114 bit keystream for MS to BTS link
114 bit keystream for BTS to MS link

Next Chapter

Short Message Service

Thanks



Second Edition

Mobile Computing

Technology, Applications and Service Creation

ASOKE K TALUKDER
HASAN AHMED
ROOPA R YAVAGAL

Mobile Computing

Chapter 6

SMS

Asoke K Talukder

Hasan Ahmed

Short Message Service (SMS)

❑ Most popular data bearer/service within GSM

❑ More than one billion SMS messages interchanged everyday with a growth of more than half a billion every month on an average

❑ Runs on SS7 signaling channels, which are always present but mostly unused, be it during an active user connection or in the idle state

❑ Each short message is up to 160 characters in length when 7-bit English characters are used and 140 octets when 8-bit characters are used

Strengths of SMS

❑ Omnibus nature of SMS: SMS uses SS7 signaling channel which is available throughout the world.

❑ Stateless: SMS is session-less and stateless as every SMS message is unidirectional and independent of any context. This makes SMS the best bearer for notifications, alerts and paging.

❑ Asynchronous: SMS is completely asynchronous. In case of SMS, even if the recipient is out of service, the transmission will not be abandoned and hence, SMS can be used as message queues. SMS can be used as a transport bearer for both synchronous (transaction oriented) and asynchronous (message queue and notification) information exchange.

Strengths of SMS

❑ Self-configurable and last mile problem resistant: SMS is self-configurable and subscriber is always connected to the SMS bearer irrespective of the home and visiting network configurations.

❑ Non-repudiable: SMS message carries the Service Center (SC) and the source MSISDN as a part of the message header through which any SMS can prove beyond doubt its origin.

❑ Always connected: As SMS uses the SS7 signaling channel for its data traffic, the bearer media is always on. Users cannot switch OFF, BAR or DIVERT any SMS message. SMS message is delivered to the Mobile Station (MS) without any interruption to the ongoing call.

SMS Architecture

❑ Two types of SMS - **SM MT** (Short Message Mobile Terminated Point-to-Point) and **SM MO** (Short Message Mobile Originated Point-to-Point)

❑ SM MT is an incoming short message from the network and is terminated in the MS

❑ SM MO is an outgoing message originated in the MS and forwarded to the network for delivery

❑ For an outgoing message, the path is from MS to SC via the VLR and the IWMSC (Inter Working MSC) function of the serving MSC whereas for an incoming message the path is from SC to the MS via HLR and the GMSC (Gateway MSC) function of the home MSC

Strengths of SMS

❑ Omnibus nature of SMS: SMS uses SS7 signaling channel which is available throughout the world.

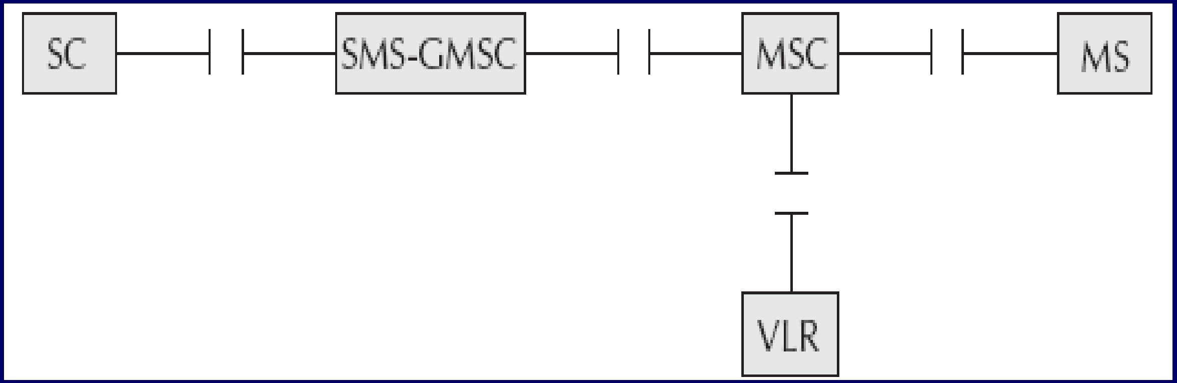
❑ Stateless: SMS is session-less and stateless as every SMS message is unidirectional and independent of any context. This makes SMS the best bearer for notifications, alerts and paging.

❑ Asynchronous: SMS is completely asynchronous. In case of SMS, even if the recipient is out of service, the transmission will not be abandoned and hence, SMS can be used as message queues. SMS can be used as a transport bearer for both synchronous (transaction oriented) and asynchronous (message queue and notification) information exchange.

Short Message Mobile Terminated (SMMT)

❑ Message is sent from SC to the MS.

❑ For the delivery of MT or incoming SMS messages, the SC of the serving network is never used which implies that a SMS message can be sent from any SC in any network to a GSM phone anywhere in the world.

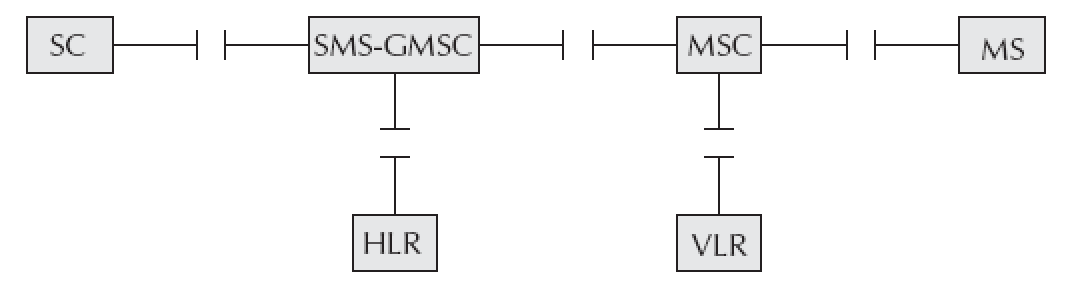


Interfaces in SMMT

Short Message Mobile Originated

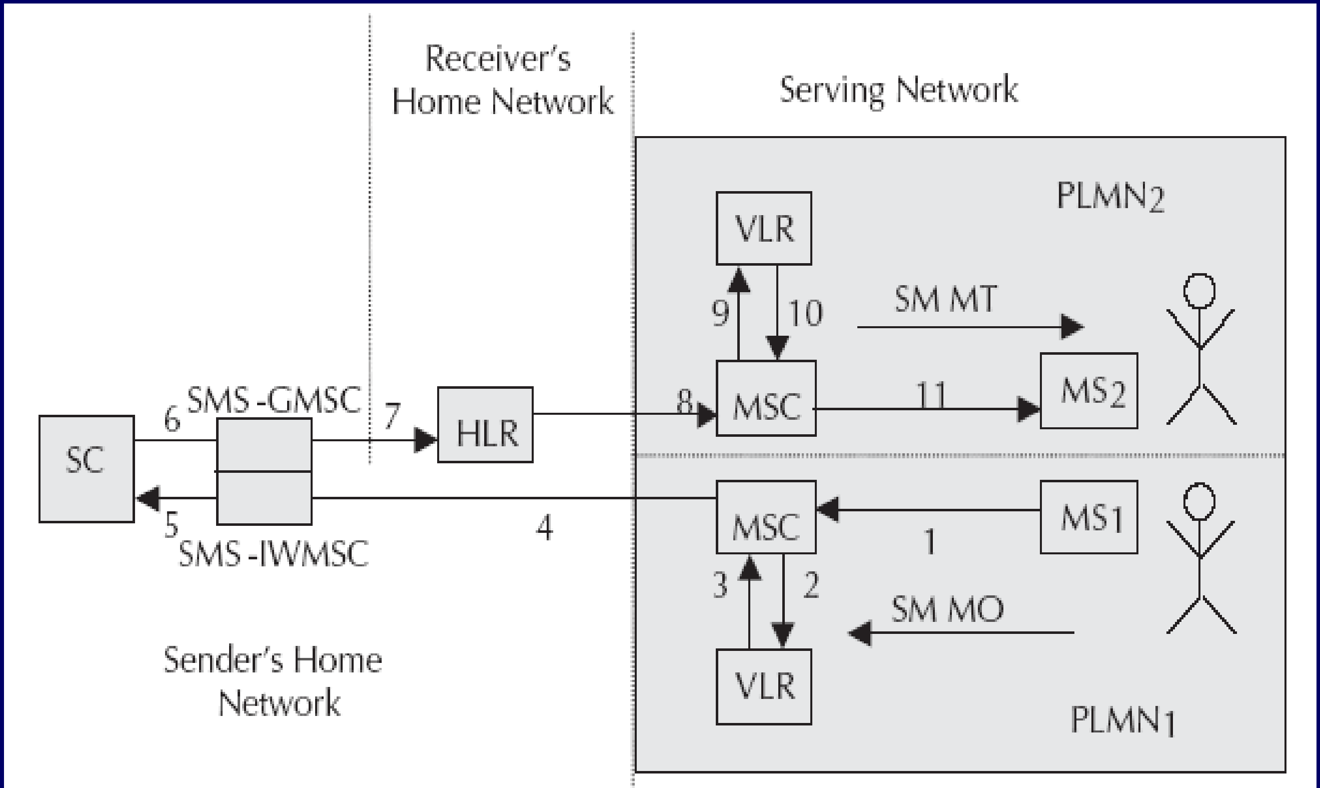
❑ For a MO message, the MSC forwards the message to the home SC.

❑ MO message works in two asynchronous phases. In the first phase, the message is sent from the MS to the home SC as a MO message. In the second phase, the message is sent from the home SC to the MS as a MT message.



Interfaces in SMMO

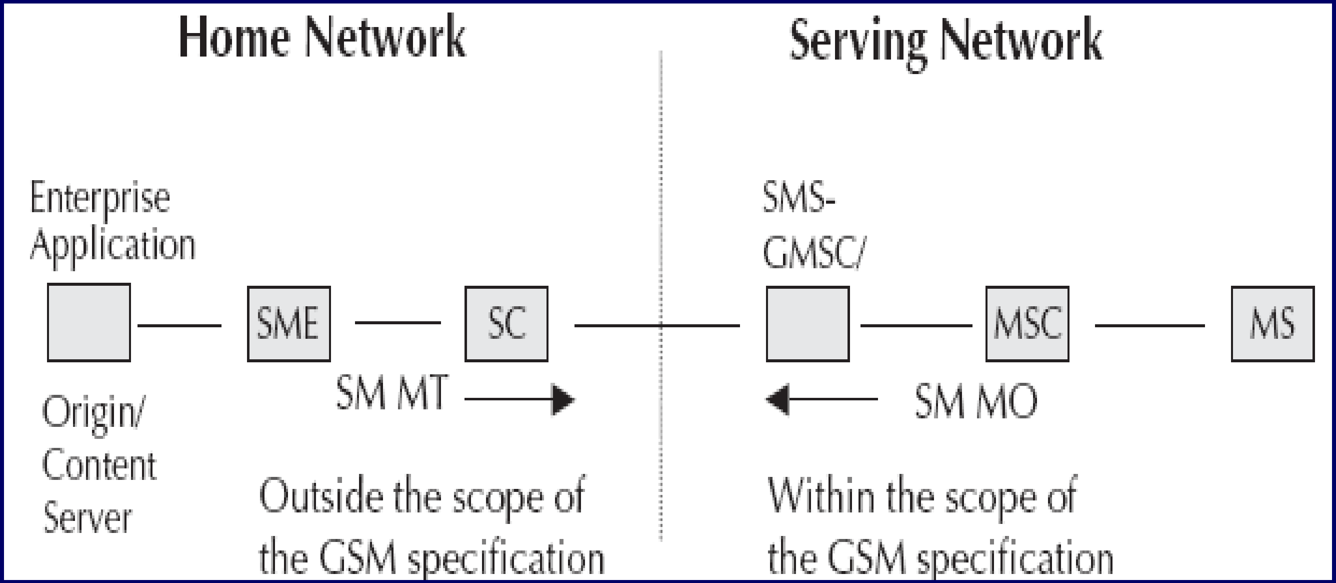
SMS Transfer



SMS as an Information Bearer

- For using SMS as an information bearer, we need to connect the services running on the Enterprise Origin server to the SC through an SME (Short Message Entity) or ESME (External Short Message Entity).
- SME in any network is generally a SMS gateway.
- With respect to SMS, a GSM subscriber is always in control of the SC in the home network irrespective of the serving network.
- If there is any SMS-based data service in the home network, it will be available in any foreign network.

SMS as an Information Bearer



Operator Centric Pull

❑ Operators offer different information on demand and entertainment services through connecting an Origin server to the SC via a SMS gateway.

❑ Such service providers are known as Mobile Virtual Network Operator(s) (MVNO).

❑ MVNOs develop different systems, services and applications to offer data services using SMS.

❑ Many enterprises use MVNOs to make their services available to mobile phone users.

Example of MVNO

❑ Let’s say few banks offer balance enquiry and other low security banking services over SMS and customers need to register for the service.

❑ During the registration, the customer needs to mention the MSISDN of the phone which will be used for a banking service.

❑ Once a user is registered for the service, he enters ‘BAL’ and sends the message to a service number (like 333) as a MO message and then SC delivers this MO message to the SMS gateway (known as SME-Short Message Entity) connected to this service number.

Example of MVNO

❑ SMS gateway then forwards this message to the enterprise application and response from the enterprise application is delivered to the MS as a MT message from the SME.

❑ Even if the subscriber is in some remote region of a foreign network within GSM coverage, he can send the same SMS to the same service number in his home network and this makes the home services available in the foreign network. Hence, operator-centric SMS pull service is completely ubiquitous.

Operator Centric Pull

- ❑ Connectivity between SME and Origin server could be anything like SOAP (Simple Object Access Protocol), direct connection through TCP socket or through HTTP.

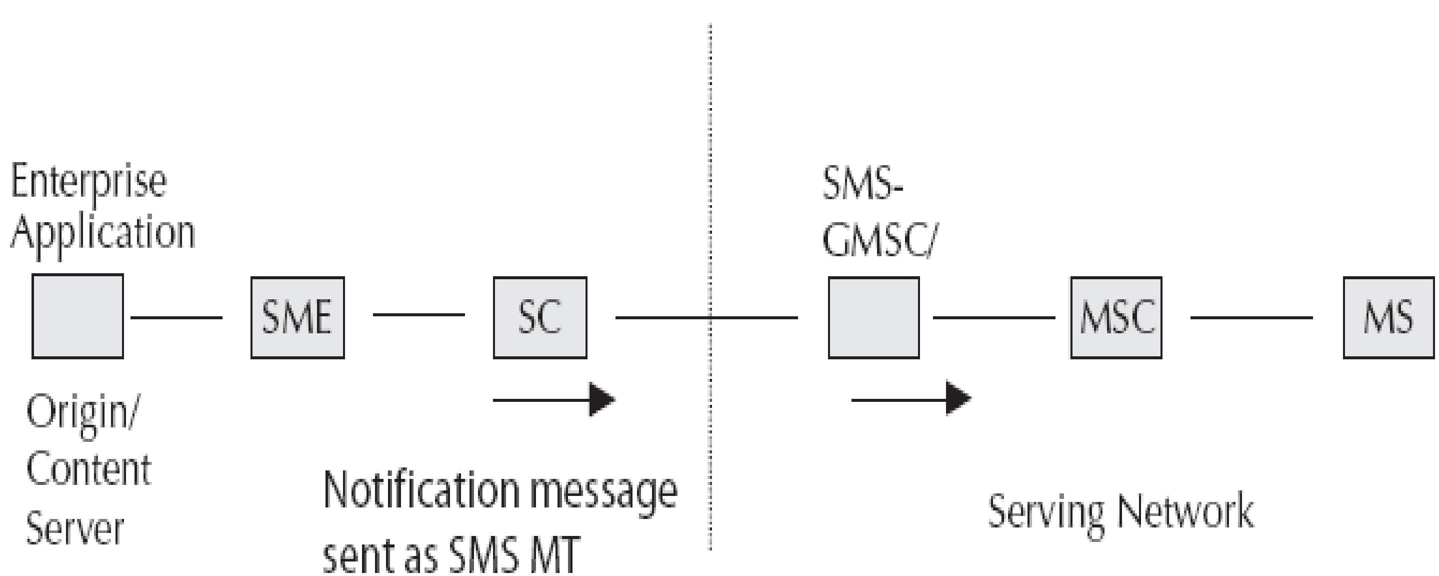
- ❑ There are applications where SMS is used in session oriented transactions as ‘SMS chat’ and ‘SMS contests’ need to remember the user context over multiple transactions.

Operator Independent Push

- Any push, which may be an alert, notification or even response from a pull message generated by an application, can be serviced by any network and delivered to any GSM phone in any network without any difficulty.

- If appropriate roaming tie-ups are in place, an enterprise can use SMS to send business alerts or proactive notifications to its customer anywhere, anytime on his phone.

Operator Independent Push



Operator Independent Pull

- For a SMS message to be routed to some enterprise SME connected to external SC, SAT is used.

- SAT application running on the SIM card changes the SC number during the transmission of the SMS and forces the SMS to recognize a different SC of a different network as its home SC.

- Here, too, SMS is sent to the SME connected to the home SC. If a SMS service is operator dependent, the cellular operator can use this to its advantage.

- Enterprises need operator independent pull as enterprises have customers around the world subscribing to different GSM networks

- Above scenario can also be achieved through Intelligent Network.

Value Added Services through SMS

❑ Value Added Services (VAS) can be defined as services, which share one or more of the following characteristics:

1. Supplementary service (not a part of basic service) but adds value to total service offering
2. Stimulates incremental demand for core services offering
3. Stands alone in terms of profitability and revenue generation potential
4. Can sometimes stand-alone operationally
5. Does not cannibalize basic service unless clearly favorable

Value Added Services through SMS

6. Can be an add-on to basic service, and as such, may be sold at a premium price
7. May provide operational and/or administrative synergy between or among other services and not merely for diversification

Value Added Services through SMS

- VAS over SMS are entertainment and information on demand which is further categorized into:

1. Static information which does not change frequently
2. Dynamic information which changes in days
3. Real-time information which changes continually

- Some of the common VAS examples are:

1. News/Stock Quotes Service
2. Session-based Chat Application
3. Email through SMS
4. Health Care Services
5. Micro-Payment Services

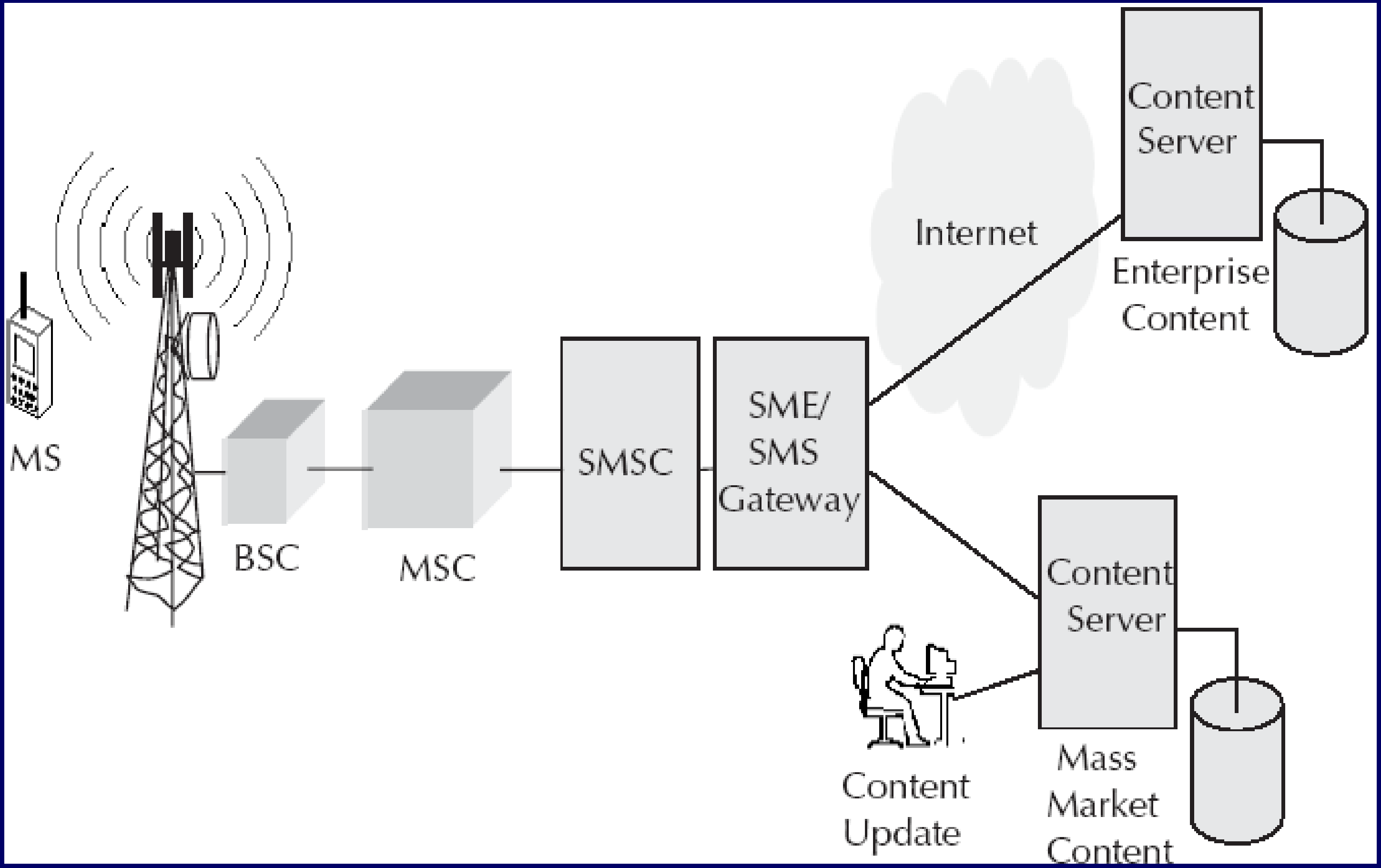
Alert services through VAS

❑ Proactive alert services can be of the two kinds – Time based and Watermark based

❑ Time based proactive alerts are sent to the mobile phone at a pre-assigned time of the day

❑ Watermark based proactive alerts are sent when some event occurs

VAS Architecture



Location based services through SMS

- Location based services could be road direction, restaurant guide, shopping alerts, etc.

- In location based services, only the information relevant to the current location of the mobile phone (or the subscriber) is provided.

- The location of a mobile phone can be determined either from the network or from the device.

- The location of a mobile phone can be determined either from the network or from the device.

- To find out the location from the device either of the following technologies are used - Cell ID (CID) based system and Global Positioning System (GPS) based system.

Cell ID based system

- CID of the current BTS is determined and then mapping of the cell identifier to the geographical location is performed.
- For CID based system, the signal strength from all the different CIDs are extracted from the device and sent to the server through a SMS.
- Location of the user is determined using the signal strength and triangulation algorithms.

GPS based system

- ❑ GPS is Global Positioning System.
- ❑ Location is determined through a GPS receiver installed within the phone.
- ❑ GPS provides facility to compute position, velocity and time of a GPS receiver.
- ❑ GPS based system is not dependent on the network operator.

Accessing the SMS bearer

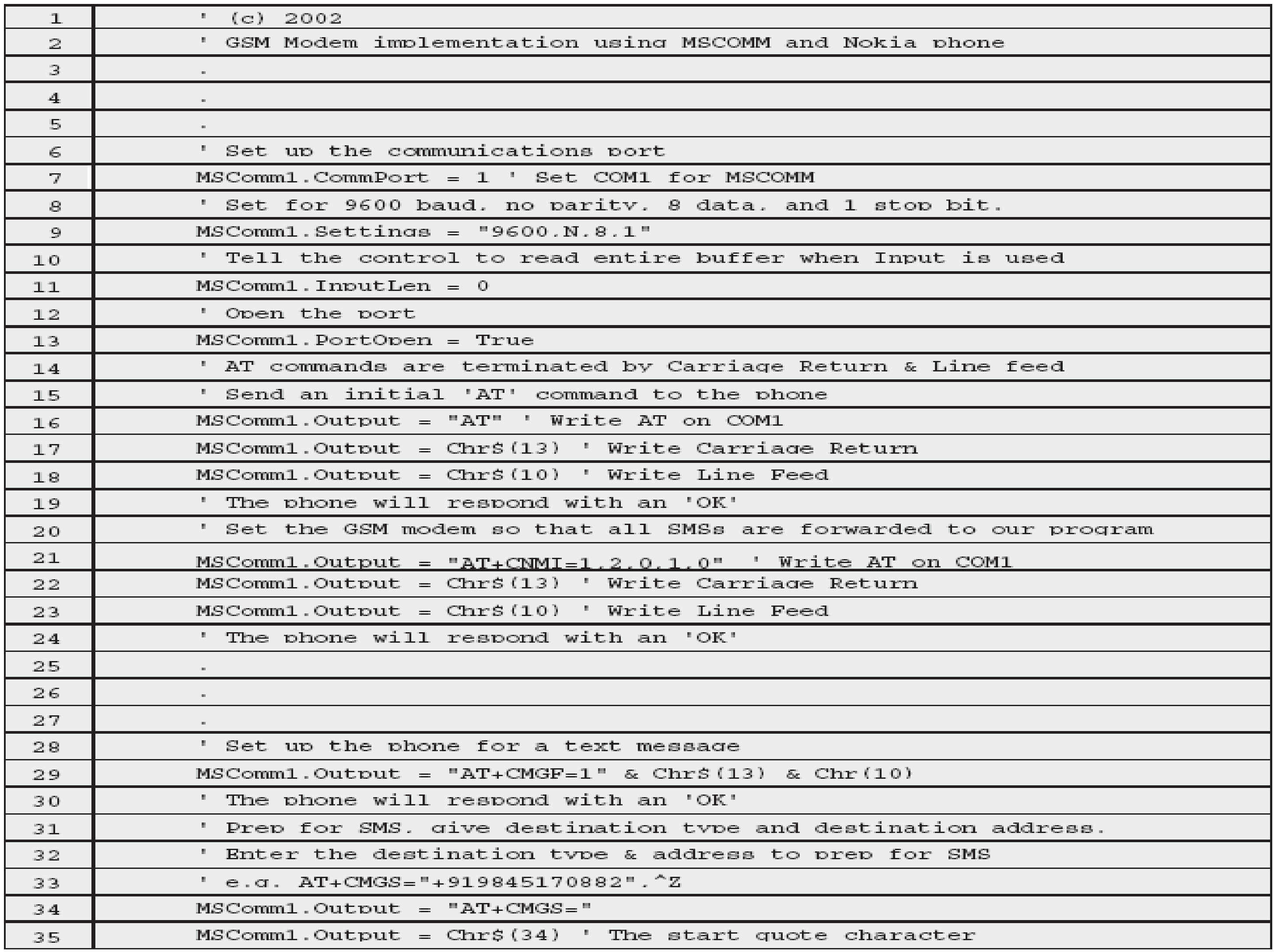
- There are two ways through which SMS bearer can be accessed:

1. Using a mobile phone as a GSM modem and connecting it to the computer
2. Using the SMSC of an operator through SMPP or similar interface

GSM Modem

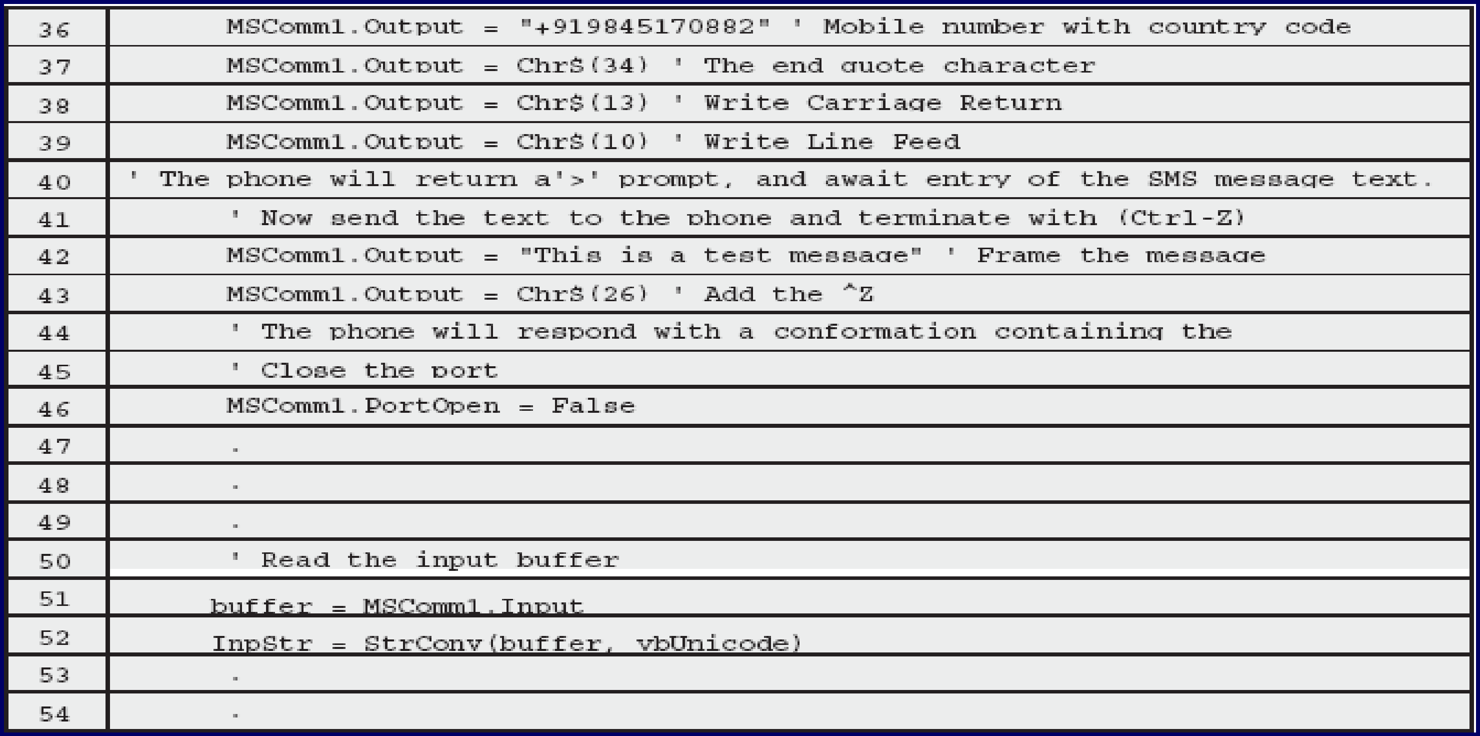
- ❑ Normal cell phone can be used as a data modem which will be in a position to access the network as a normal GSM phone.
- ❑ Once phone and computer is connected (through wired or wireless means), cell phone can be used as an external GSM modem and issue **AT** commands to transact data over the GSM/SMS bearer. AT in Hayes terminology is known as attention and are commands to the modem from the computer.
- ❑ AT commands can be for sending a SMS, reading a SMS, checking battery power, writing a phone book entry, etc.
- ❑ To read a SMS from the GSM modem, we need to ensure that the SMS is forwarded to the computer rather than the phone local store and for this CNMI commands are used.

Example code for GSM



```
' (c) 2002
' GSM Modem implementation using MSCOMM and Nokia phone
.
.
.
' Set up the communications port
MSComm1.CommPort = 1 ' Set COM1 for MSCOMM
' Set for 9600 baud, no parity, 8 data, and 1 stop bit.
MSComm1.Settings = "9600,N,8,1"
' Tell the control to read entire buffer when Input is used
MSComm1.InputLen = 0
' Open the port
MSComm1.PortOpen = True
' AT commands are terminated by Carriage Return & Line feed
' Send an initial 'AT' command to the phone
MSComm1.Output = "AT" ' Write AT on COM1
MSComm1.Output = Chr$(13) ' Write Carriage Return
MSComm1.Output = Chr$(10) ' Write Line Feed
' The phone will respond with an 'OK'
' Set the GSM modem so that all SMSs are forwarded to our program
MSComm1.Output = "AT+CNMI=1,2,0,1,0"  ' Write AT on COM1
MSComm1.Output = Chr$(13) ' Write Carriage Return
MSComm1.Output = Chr$(10) ' Write Line Feed
' The phone will respond with an 'OK'
.
.
.
' Set up the phone for a text message
MSComm1.Output = "AT+CMGF=1" & Chr$(13) & Chr(10)
' The phone will respond with an 'OK'
' Prep for SMS, give destination type and destination address.
' Enter the destination type & address to prep for SMS
' e.g. AT+CMGS="+919845170882",^Z
MSComm1.Output = "AT+CMGS="
MSComm1.Output = Chr$(34) ' The start quote character
```

Example code for GSM



```
      MSComm1.Output = "+919845170882" ' Mobile number with country code
      MSComm1.Output = Chr$(34) ' The end quote character
      MSComm1.Output = Chr$(13) ' Write Carriage Return
      MSComm1.Output = Chr$(10) ' Write Line Feed
' The phone will return a'>' prompt, and await entry of the SMS message text.
      ' Now send the text to the phone and terminate with (Ctrl-Z)
      MSComm1.Output = "This is a test message" ' Frame the message
      MSComm1.Output = Chr$(26) ' Add the ^Z
      ' The phone will respond with a conformation containing the
      ' Close the port
      MSComm1.PortOpen = False
      .
      .
      .
      ' Read the input buffer
     buffer = MSComm1.Input
     InpStr = StrConv(buffer, vbUnicode)
      .
      .
```

Example code for GSM

❑ Code is written in Visual Basic and uses Microsoftmscomm controls. The mscomm controls use the COM1 port for communication.

❑ Line 13 is for setting of the communication port and the interface between the computer and the modem.

❑ Lines 14–24 are for initialization of the GSM phone as modem.

❑ Lines 28–46 are to send a SMS.

❑ Lines 50–52 are for reading SMS from the modem.

SMPP

❑ Short Message Peer to Peer (SMPP) protocol

❑ Open, industry standard protocol designed to provide a flexible data communications interface for transfer of short message data between a Message Center (SC or SMSC) and a VAS application such as a WAP Proxy Server, Voice Mail server, E-Mail Gateway or any other Messaging Gateway

❑ SMPP client is termed a External Short Message Entity (ESME) and is connected to the SC

❑ SMPP release v3.4 presently supports Digital Cellular Network technologies which include GSM, IS-95 (CDMA), CDMA 1X/CDMA 2000, ANSI-136 (TDMA) and IDEN

SMPP

- ❑ SMPP supports a full featured set of two way messaging functions such as:

1. Transmit messages from an ESME to single or multiple destinations via the SMSC
2. An ESME may receive messages via the SMSC from other SMEs
3. Query the status of a short message stored on the SMSC
4. Cancel or replace a short message stored on the SMSC
5. Send a registered short message
6. Schedule the message delivery date and time

SMPP

7. Select the message mode such as datagram or store and forward
8. Set the delivery priority of the short message
9. Define the data-coding type of the short message
10. Set the short message validity period
11. Associate a service type with each message such as voice mail notification

SMPP

- Open message transfer protocol that enables short message entities (SMEs) outside the mobile network to interface with an SC and non-mobile entities that submit messages to, or receive messages from an SMSC are known as External Short Message Entities (ESMEs)

- The SMPP protocol defines operations and data as:

1. Set of operations for the exchange of short messages between an ESME and an SMSC

2. Data that an ESME application must exchange with an SMSC during SMPP operations

SMPP

- ❑ Subscribers to an SMS capable Cellular Network may receive short messages on a Mobile Station (MS) from one or more ESMEs
- ❑ Examples of such ESME applications can be:

1. Voice mail alerts originating from a VMS (Voice Messaging System)
2. Numeric and alphanumeric paging services
3. Informative services
4. Calls directly dialed or diverted to a message-bureau operator, who forwards the message to the SMSC, for onward delivery to a subscriber’s handset

SMPP

5. Fleet management applications that enable a central station to use the SMSC to determine the location of its service vehicles and notify the closest vehicle of a service request in their area
6. Telemetry applications
7. WAP Proxy Server

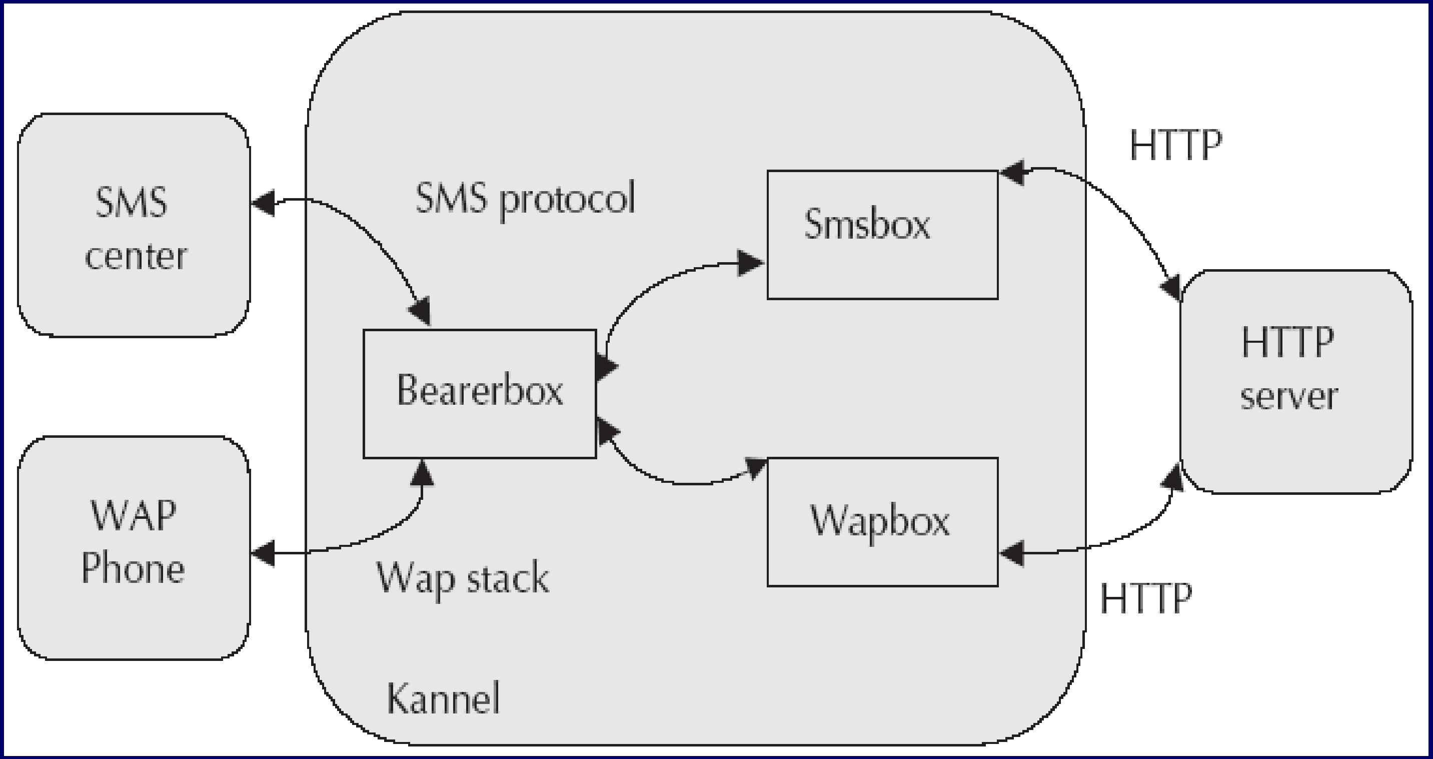
Kannel

- Open source SMS gateway
- Kannel gateway also supports WAP and MMS (Multi Media Messaging) interfaces
- Offers HTTP interface for message transfer and administrating of the gateway
- Kannel divides its various functions into different kinds of processes (figure ahead) called boxes, based on what kinds of external agents it needs to interact with
- Bearerbox implements the bearer level of SMS and as a part of this, it connects to the SMS centers
- Definitions of different TCP/IP ports, usernames, passwords, etc. are required to be defined for Bearerbox connection

Kannel

- ❑ Smsbox implements the rest of the SMS gateway functionality and as a part of this it receives textual SMS messages from the bearerbox and interprets them as service requests and responds to them in the appropriate way
- ❑ All the services are handled and managed by Smsbox
- ❑ There can be only one bearerbox, but any number of Smsboxes in a single Kannel instance
- ❑ While it is possible to have each SMS center served by a different process, it has been deemed not to give enough extra reliability or scalability to warrant the complexity
- ❑ Each box is internally multithreaded

Kannel Architecture



Pull messages in Kannel

- User enters a message with a keyword and then sends the same to a service number.
- During binding of the SMS gateway, we intimate the SC that we are listening for a service number. Therefore, all the messages sent to a service number will be routed to our SMPP gateway.
- In the Kannel configuration file, we mention that whenever there is a message with a particular keyword, it should be forwarded to a HTTP URL.
- To service the user with appropriate response, we need to know the request with all the parameters and the MSISDN number of the phone. These are transferred from Kannel gateway to the URL through %a and %p.

Pull messages in Kannel

- The response of the http request will be forwarded directly to the user by Kannel gateway.
- If the response from the content/origin server is more than 160 characters, Kannel splits the message into multiple messages.
- The max message parameter defines the limit of maximum number of messages as response. If we set the max messages to 0, no response will be sent to the user, though there could be some response coming from the HTTP request.

Push messages in Kannel

- Message is sent through HTTP interface as well and an application uses an HTTP URL to communicate with the Kannel gateway and to send SMS messages
- Kannel delivers these messages to the SC
- To offer certain level of security, Kannel allows the user authentication through user identifier and a password to access such URLs

Next Chapter

General Packet Radio Service (GPRS)

Thanks