

Global System for Mobile Communication (GSM)

Beulah A.
AP/CSE

Introduction

- The primary goal of GSM to provide a mobile phone system that allows users to roam throughout the environment and provides voice services.
- GSM → 2G system.
- GSM operates in 900 MHz or in 1800 MHz.
- Some countries (USA and Canada) operates in 850 MHz and 1900 MHz.
- Rarely used frequency bands 400MHz and 450 MHz (Scandinavia)
- 900MHz → Uplink(890-915MHz), Downlink(935-960MHz)

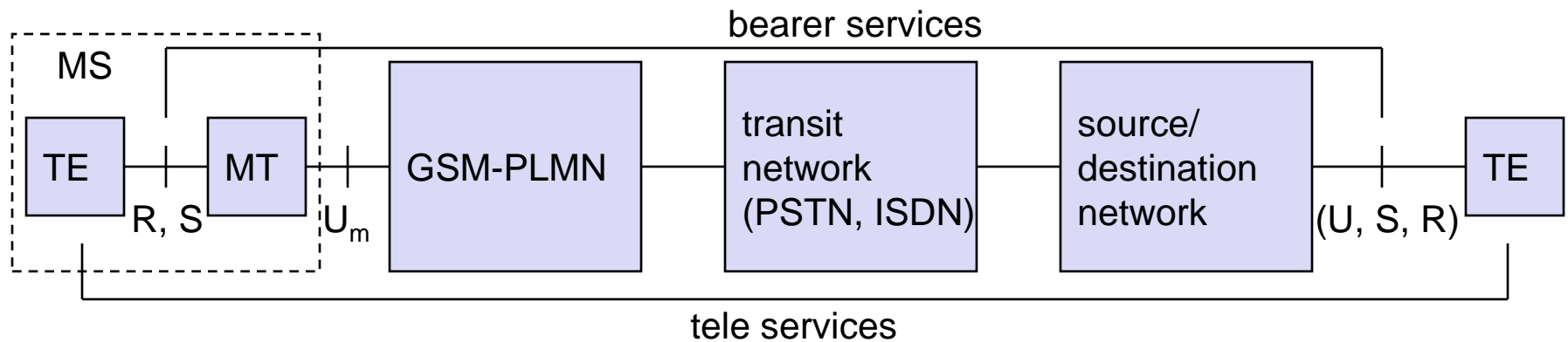
GSM Frequency Bands

Type	Channels	Uplink [MHz]	Downlink [MHz]
GSM 850	128-251	824-849	869-894
GSM 900 classical extended	0-124, 955-1023 124 channels +49 channels	876-915 890-915 880-915	921-960 935-960 925-960
GSM 1800	512-885	1710-1785	1805-1880
GSM 1900	512-810	1850-1910	1930-1990
GSM-R exclusive	955-1024, 0-124 69 channels	876-915 876-880	921-960 921-925

GSM SERVICES

GSM Services

- Three service domains
 - Bearer Services
 - Teleservices
 - Supplementary Services



Bearer Services

- Send/Receive data to/from remote phones/computers
- Therefore it is known as Data services
- Provides transparent transmission between GSM and other Networks like PSTN, ISDN etc
- PSTN (public switched telephone network)
- ISDN(Integrated Services Digital Network)
- Bearer services are implemented on lower 3 layers of OSI/ISO
- Data rate 9.6 kbps

Bearer Services

- Synchronous and asynchronous modes of transmission
- Transparent Bearer Service
 - Use the functions of Physical Layer to transmit data.
 - Forward Error Correction (FEC) is used to increase transmission quality.
 - FEC → Codes redundancy into the data stream and helps to reconstruct the original data in case of transmission errors
 - Data Rates → 2.4, 4.8 or 9.6 kbps
- Non-Transparent Bearer Service
 - Use protocols of layers 2 and 3 to implement error correction and Flow control
 - Use the transparent bearer services, in addition to Radio Link Protocol (RLP).
 - This comprises mechanism of HDLC
 - Data Rates → 1.2, 2.4, 4.8 or 9.6 kbps

Teleservices

- GSM mainly focuses on voice oriented Tele services through mobile phones.
- All these basic services have to obey cellular functions, security measurements etc.
- Offered services
 - Mobile Telephony
Primary goal of GSM was to enable mobile telephony offering the traditional bandwidth of 3.1 kHz
 - Emergency number
Common number throughout Europe (112); mandatory for all service providers; free of charge; connection with the highest priority (preemption of other connections possible)
Well known emergency number in the world today alongside **911** and **999**
India police **100** , **Medical 102,1298,108,112** Fire **101** Emergency management **2611**

Teleservices

- Additional services
 - Non-Voice-Teleservices
 - **Voice mailbox** (implemented in the fixed network supporting the mobile terminals)
 - **Short Message Service (SMS)**
Alphanumeric data transmission to/from the mobile terminal (160 characters) using the signaling channel, thus allowing simultaneous use of basic services and SMS
 - **Enhanced Message Service (EMS)**
Offers a larger text message (760 characters)
 - **Multimedia Message Service (MMS)**
Transmission of large pictures, short video clips etc.

Supplementary services

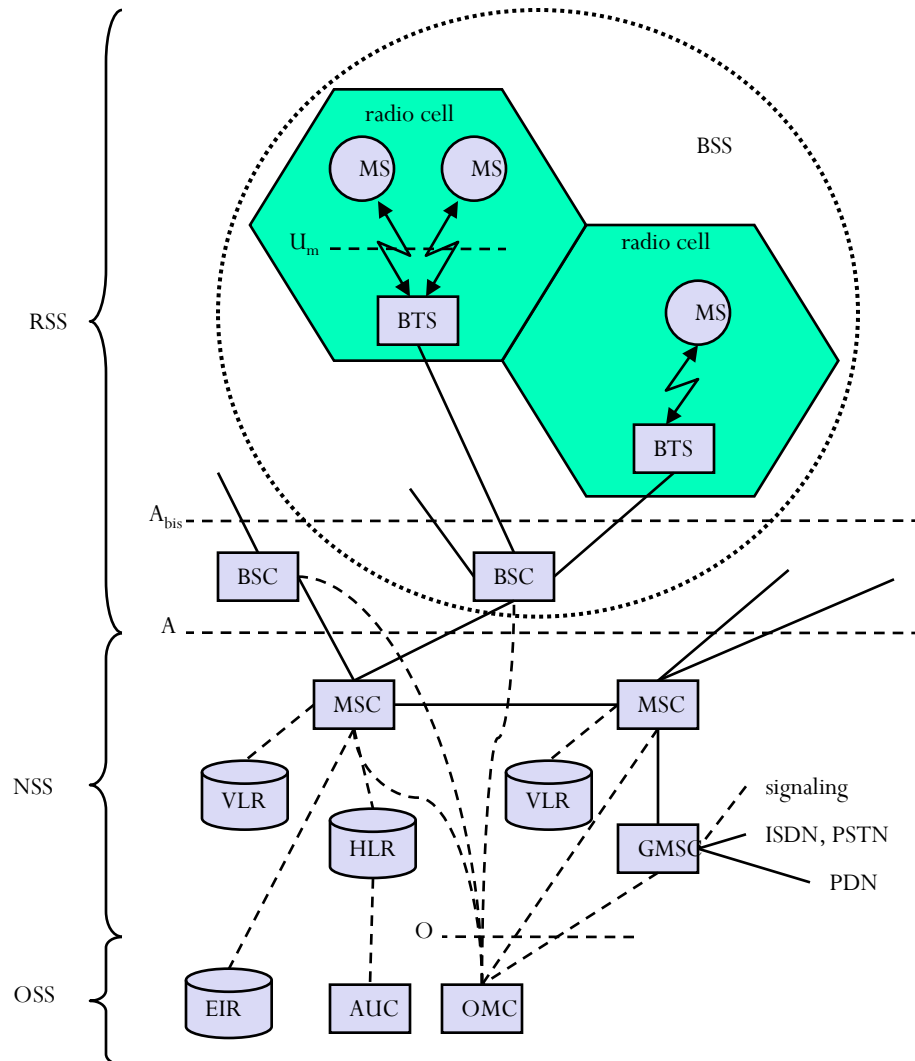
- GSM offers Supplementary services
- May differ between different service providers, countries and protocol versions
- Important services
 - User Identification
 - Call redirection
 - Forwarding of ongoing calls
 - Closed user group
 - Multiparty communication(Conferencing with up to 7 participants)

GSM ARCHITECTURE

System Architecture of GSM

- GSM consists of 3 Subsystems
 - RSS (Radio SubSystem):
 - Covers all radio aspects
 - NSS (Network and Switching Subsystem):
 - Call forwarding, handover, switching
 - OSS (Operation SubSystem):
 - Management of the network

GSM: Elements and Interfaces



- BSS (Base Station Subsystem)
- BTS (Base Transceiver Station): sender and receiver
- BSC (Base Station Controller): controlling several transceivers
- MSC (Mobile Station Controller)
- HLR (Home Location Register)
- VLR (Visitor Location Register)
- GMSC (Gateway Mobile Station Controller)
- EIR (Equipment Identity Register)
- AuC (Authentication Centre)
- OMC (Operation and Maintenance Centre)
- Interfaces
 - U_m : radio interface
 - A_{bis} : standardized, open interface with 16 kbps user channels
 - A : standardized, open interface with 64 kbps user channels

Radio SubSystem

- Components
 - MS (Mobile Station)
 - BSS (Base Station Subsystem):
 - BTS (Base Transceiver Station)
 - BSC (Base Station Controller)

Mobile Station

- A mobile station (MS) has different types of interfaces
 - Display, loudspeaker, microphone and programmable soft keys
 - Connection with computer modems(USB), Bluetooth.
- Many vendor specific functions and components such as cameras, fingerprint sensors, calendars, address books, games, and Internet browsers.

Mobile Station

- SIM (Subscriber Identity Module):
 - Personalization of the mobile terminal, stores user parameters
 - Stores all user specific data that is relevant to GSM(protected memory, flash memory)
 - Without a SIM only emergency calls are possible.
 - Contains
 - PIN (Personal Identity Number)
 - To unlock MS. Using wrong PIN 3 times will lock the SIM.
 - PUK (PIN unblocking key)
 - Authentication key K_i
 - International Mobile Subscriber Identity (IMSI)

Mobile Station

- International Mobile Equipment Identity (IMEI)
 - Device specific mechanisms Ex. For Theft protection use the device specific IMEI
 - It is usually found printed inside the battery compartment of the phone.
 - It can also be displayed on the screen of the phone by entering *#06# into the keypad on most phones.
- International Mobile Subscriber Identity (IMSI)
 - is a unique identification associated with all GSM network mobile phone users. It is stored as a 64 bit field in the SIM inside the phone and is sent by the phone to the network
 - An IMSI is usually presented as a 15 digit long number, but can be shorter .

Base Station Subsystem (BSS)

- Each BSS is controlled by a BSC (Base Station Controller)
- Functions of BSS
 - Maintaining Radio connection to MS
 - Coding/ Decoding of voice
 - Rate adaptation from /to the wireless network part

Base Transceiver Station

- Comprises of
 - Radio components including sender, receiver, antenna
- BTS connected to MS via U_m interface
- BTS connected to BSC via A_{bis}
- U_m interface Contains all the mechanisms necessary for wireless transmission (TDMA, FDMA)
- A GSM cell can measure between 100m to 35km depending on the environment (buildings, open source, mountains etc)

Base Station Controller

- Manages several BTSs.
- Handles
 - Switching between BTSs
 - Controlling BTSs
 - Managing of network resources
 - Multiplexes the radio signals and transmit to MSC

Network and Switching Subsystem

- NSS is the main component of the public mobile network GSM
 - switching, mobility management, interconnection to other networks, system control
- Components
 - MSC (Mobile Station Controller)
 - HLR (Home Location Register)
 - VLR (Visitor Location Register)
 - GMSC (Gateway Mobile Station Controller)

Mobile Services Switching Center

- High performance digital ISDN switches
- Setup connections to other MSCs and to the BSCs via the A interface.
- Forms the backbone of the GSM network.
 - Switching functions
 - Connection Setup
 - Connection Release
 - Call Handoff
 - Call forwarding
 - Conference calls
- GMSC → Gateway MSC

Home Location Register

- Central master database
- Comprise static information such as MSISDN and IMSI
- MSISDN
 - Mobile subscriber ISDN number(Phone number)
 - Services → Call forwarding, Roaming, GPRS etc.
 - The MSISDN together with IMSI are two important numbers used for identifying a mobile subscriber.
 - The latter identifies the SIM, i.e. the card inserted in to the mobile phone, while the former is used for routing calls to the subscriber.
- Contains Dynamic information such as LA ie current Location area and MSRN (Mobile subscriber Roaming Number)
- When MS leaves current LA, the information in the HLR is updated.
- HLRs can manage data for several million customers.

Visitor Location Register

- Dynamic database which stores information needed for the MS in the current LA. Such as IMSI, MSISDN, HLR address.
- When a new MS comes into an LA the VLR is responsible for copying all information for this user from HLR.
- This hierarchy avoids frequent HLR updates.

Operation SubSystem

- The OSS (Operation Subsystem) enables centralized operation, management, and maintenance of all GSM subsystems
- Authentication Center (AUC)
 - Protects intruders targeting the air interface.
 - AUC stores information concerned with security features such as user authentication and encryption.
- Equipment Identity Register (EIR)
 - Registers GSM mobile stations and user rights
 - Stolen or malfunctioning mobile stations can be locked and sometimes even localized
- Operation and Maintenance Center (OMC)
 - Different control capabilities for the radio subsystem and the network subsystem
 - Traffic monitoring, status reports of network entities,, subscriber management, security management, accounting, billing

GSM SECURITY

Security

- GSM offers security services with the help of Confidential information stored in
 - The AuC
 - The individual SIM
- AuC contains
 - The algorithms for authentication and generates the values needed for user authentication
 - The keys for encryption
- SIM stores
 - Personal data
 - Secret data.
 - These are protected with the help of PIN

Security Services

- Access control and Authentication
 - Authentication of a valid user for the SIM.
 - The user needs a secret PIN to access the SIM
 - Subscriber Authentication has to be done.
- Confidentiality
 - User data is encrypted
 - After authentication, BTS and MS apply encryption to voice, data, and Signal.
 - Confidentiality exists only between MS and BTS.
- Anonymity
 - User identifiers are not used over the air.
 - TMSI (newly assigned by the VLR) is transmitted after each location update
 - VLR can change the TMSI at any time.

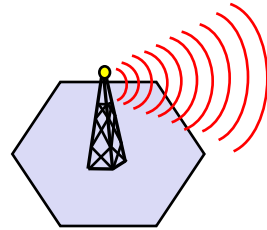
Security Services

- 3 Algorithms
- Algorithm A3 is used for authentication
- Algorithm A5 for Encryption
- Algorithm A8 for the generation of a Cipher Key.

Authentication

- The user should be authenticated, before using any service from the network.
- Authentication is based on SIM
- SIM contains
 - Authentication key K_i
 - User Identification IMSI
 - Algorithm A3 → algorithm used for authentication.
- Authentication uses a challenge-response method.

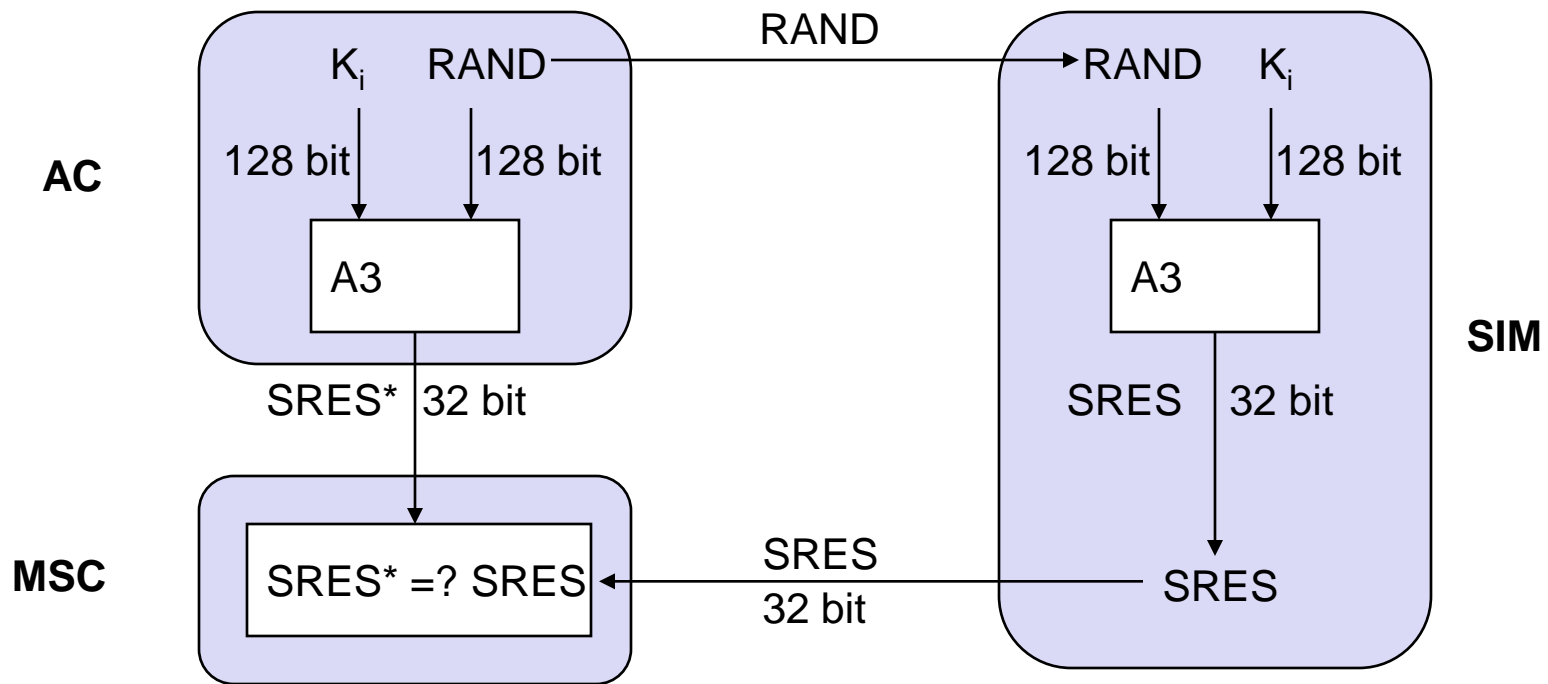
Authentication



mobile network



SIM



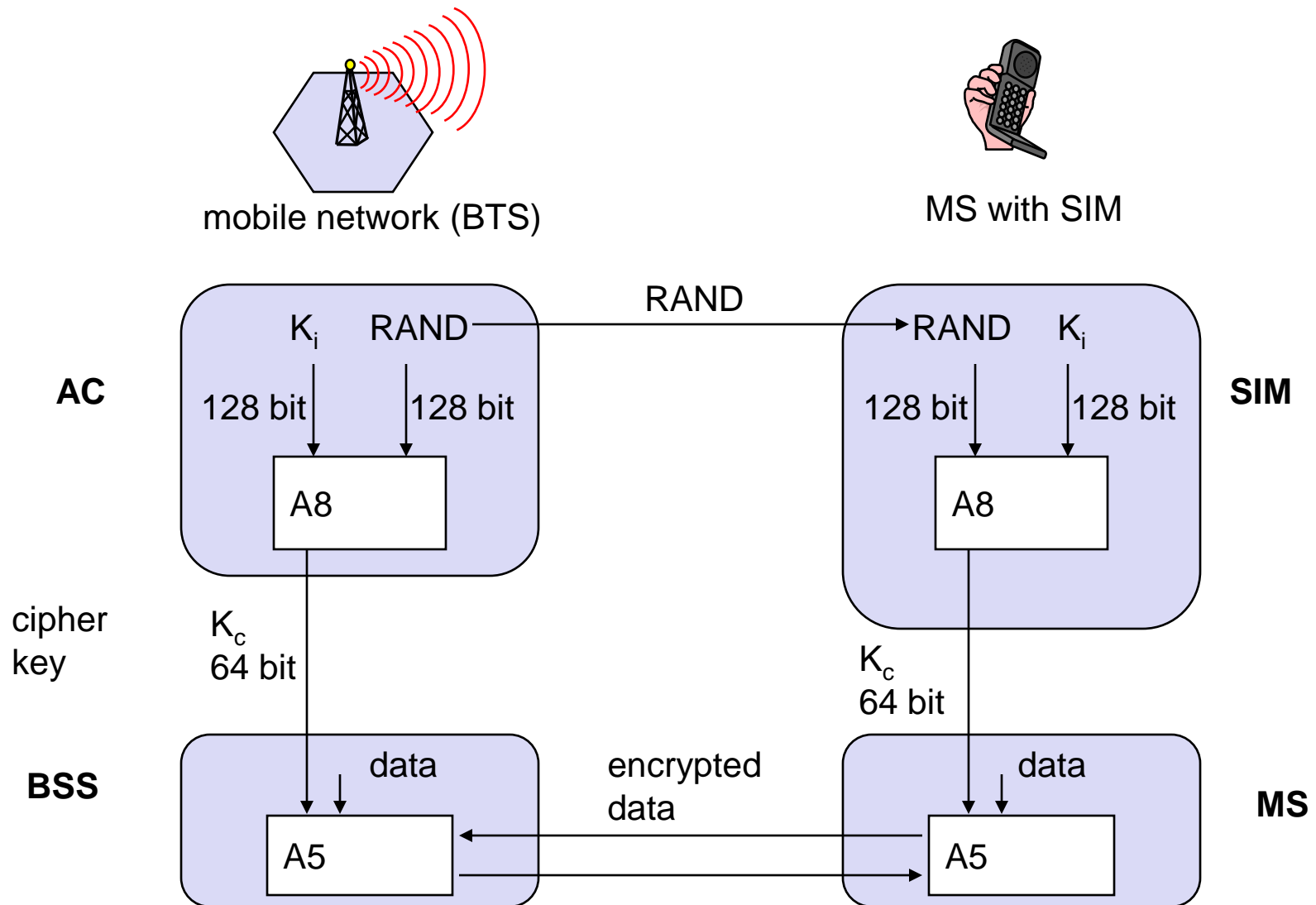
K_i : individual subscriber authentication key

SRES: signed response

Encryption

- User data are encrypted
- MS and BTS uses k_c (cipher key) for encryption
- K_c is generated using the authentication key k_i and a random value by applying the algorithm A8

Encryption



Summary

- GSM Services
 - Bearer service
 - Teleservice
 - Supplementary service
- GSM Architecture
 - RSS
 - NSS
 - OSS
- GSM Security

Test your understanding

- Identify the main reason as to why a mobile handset is compact and lightweight and yet provides a large number of features such as roaming, camera, audio and video play, record internet etc., while traditional landline phone handsets are bulky and provide only limited features.

Reference

- Jochen H. Schller, “Mobile Communications”, Second Edition, Pearson Education, New Delhi, 2007.