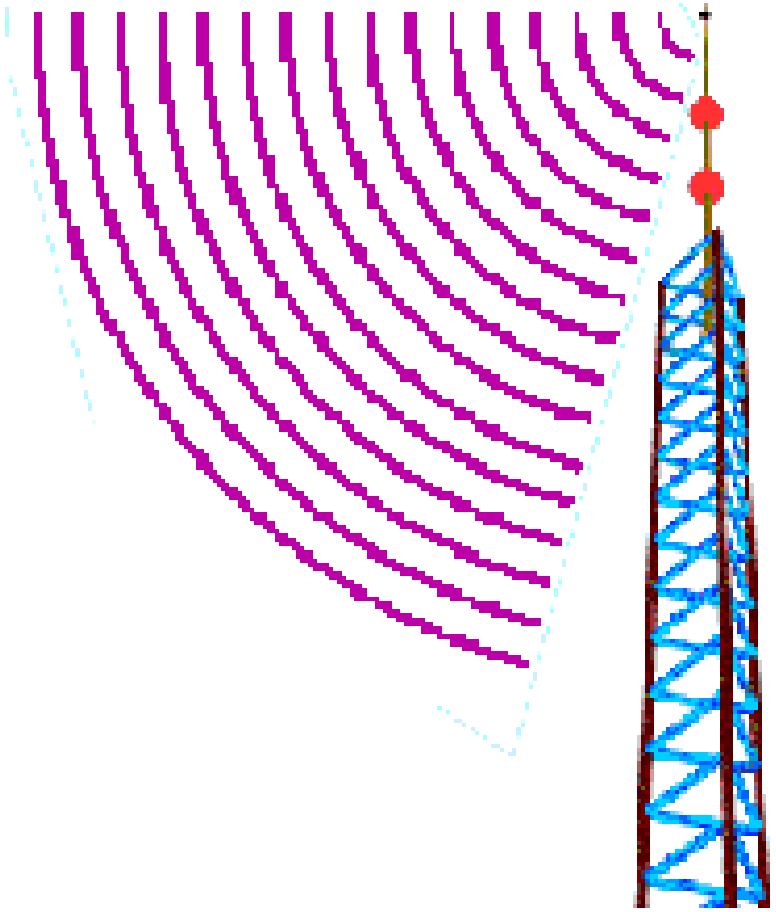
Cellular Wireless Networks



EMİNE DUMLU

Outline

- Introduction to Cellular Wireless Network
- Generation Of Cellular Network
- Features of Cellular Systems
- Cellular Technologies
- Used Protocols
- Advantages of Cellular Networks

Cellular Wireless Network

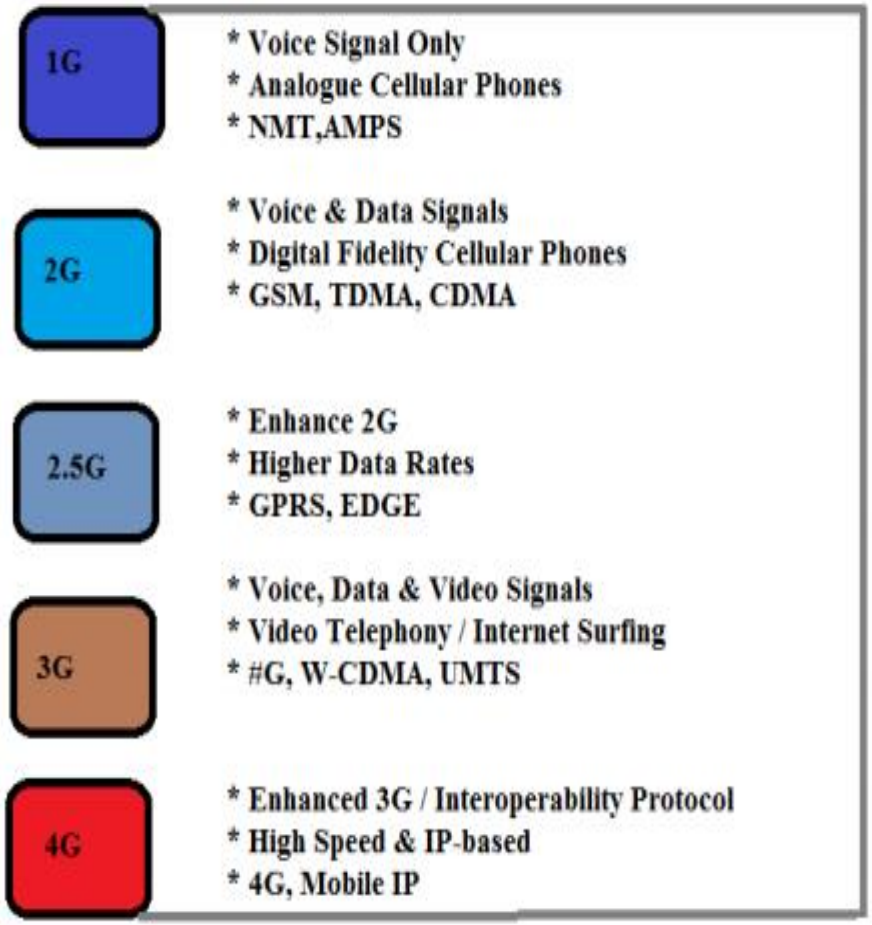
- A **cellular network** or **mobile network** is a communication network where the last link is wireless.
- Cellular technology is the basis for mobile wireless communications and supports users in locations that are not easily served by wired networks.
- The technology is developed for mobile radio telephone to replace high power transmitter/receiver systems.
- Cellular networks use lower power, shorter range and more transmitters for data transmission.

Cellular Network

- Cellular networks are called such because of the fact that a geographical area is divided up into cells, each cell being serviced by one or more radio transceivers (transmitter/ receiver) known as a cell site or base station.
- Base station provides the cell with the network coverage which can be used for transmission of voice, data and others.
- A cell might use a different set of frequencies from neighboring cells, to avoid interference and provide guaranteed service quality within each cell.
- Communication in a cellular network is full duplex.
- Full duplex communication is attained by sending and receiving messages on two different frequencies.

Generation of Cellular Network

- Cellular networks were certainly the first and so far most successful commercial application of wireless networks.
- The evolution of cellular communications network is commonly known by 1G, 2G, 3G and 4G.Cellular Networks have been around since the 1980s



1G Cellular Networks

- First generation (1G) networks were the first cellular networks introduced in the 1980s.
- 1st generation cellular networks are purely analog cellular systems.
- They were only capable of transmitting voice at speeds of about 9.6 kbps max
- 1G systems had some limitations such as no support for encryption, poor sound quality and inefficient use of the spectrum due to their analog nature.

2G Cellular Networks

- Second generation cellular networks also known as personal communication services (PCS).
- Introduced the concept of digital modulation meaning that voice was converted into digital code, and then into analog (radio) signals.
- Being digital, they overcame certain limitations of 1G systems.
- They consist of digital traffic channels, perform encyption, error detection & correction: Very clear voice reception
- Users share channels dynamically via Time division multiple access or code division multiple access (CDMA)

2G Cellular Networks

- Various 2G technologies have been deployed around the world:
  - Code Division Multiple Access (CDMA): it is the primary technology in the USA.
    - good security
    - Frequency-diversity:Frequency-dependent transmission impairments (noise bursts, selective fading) have less effect
  - Global System for mobile communication (GSM): developed in Europe
  - Personal Digital Cellular: deployed in Japan

2G and 2.5G

- Some of the data services which are part of the 2.5G extension are
  - ***Short Messaging Service (SMS):*** Transfer of messages between cell phones. It uses standard protocols to allow fixed line or mobile phone devices to exchange short text messages
  - ***High-Speed Circuit-Switched Data (HSCSD):*** This was done by GSM, which runs at speeds of 115 kbps. This technique cannot support large bursts of data. HSCSD was not widely implemented as GPRS is more popular.

2G and 2.5G

- ***General Packet Radio Service (GPRS):*** It is a packet oriented data service for 2G and 3G cellular network. This technique can support large data transfers.

- ***Enhanced Data Rates for GSM Evolution (EDGE):*** It is a digital mobile phone technology that allows improved data transmission rates as backward compatible extension of GSM.

Third Generation: 3G Cellular Networks

- 3G is the next generation wireless cellular network whose aim is to provide a world wide standard and a common frequency band for mobile networking.
- Objective to provide fairly high-speed wireless communications to support multimedia, data, and video in addition to voice
- This is digital with high speed data transfer
- Ex: UMTS in Europe. It is being developed as an evolution of GSM and therefore based on the GPRS .

Third Generation: 3G Cellular

- Data transmission rates can be asymmetric or symmetrical
- It provides support for circuit switched and packet switched data services
- Technology is digital using time division multiple access or code division multiple access

4G Cellular

- **4G** is the fourth generation of wireless mobile telecommunications technology, succeeding 3G.
- Some of the 4G services talked about are incorporating quality of service (QoS) and Mobility.
- 4G also use the IPV6 address scheme.
- MU-MIMO (Multiple User MIMO) Antenna used in 4G cellular networks.

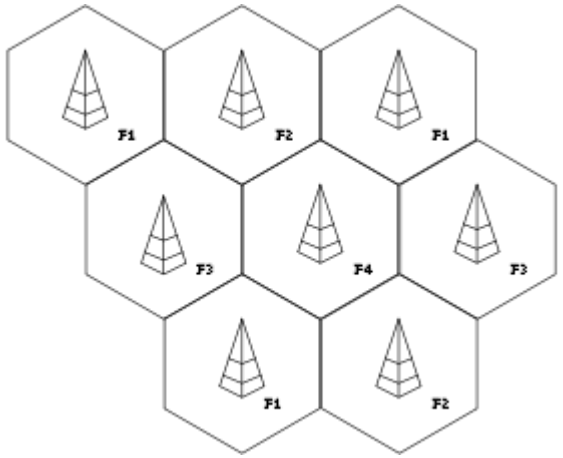
	1st	2nd	3rd	4th
Name	Analog Cellular (1970s)	Digital Cellular, PCS (1980s~)	IMT-2000 (2000~)	(Beyond IMT-2000) (2005~)
Core Network	Circuit-based Analog (PSTN)	Circuit-based Digital (GSM,IS-95)	IP-based (GPRS, Mobile-IP)	All-IP-based
Air Network	FDMA	FDMA+TDMA, CDMA	WCDMA, cdma2000	Smart Antenna
Frequency (MHz)	900	900, 1800MHz	2000MHz	5~60GHz

Features of Cellular Systems

- The features of cellular systems are as follows;
  - Offer very high capacity in a limited spectrum.
  - Reuse of radio channel in different cells.
  - Enable a fixed number of channels to serve an arbitrarily large number of users by reusing the channel throughout the coverage region.
  - Communication is always between mobile and base station (not directly between mobiles).
  - Each cellular base station is allocated a group of radio channels within a small geographic area called a cell.
  - Neighboring cells are assigned different channel groups.
  - Frequency reuse or frequency planning.

Cellular Geometries

- The general view of cells in cellular network.
- The shape of cells can be either square or hexagon

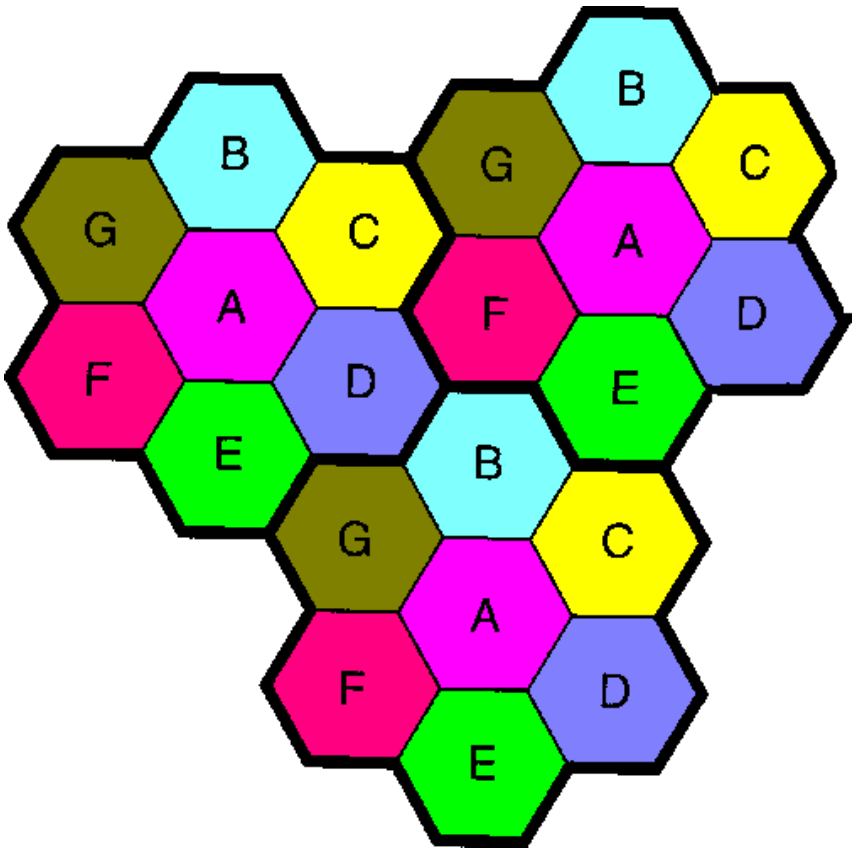


Frequency Reuse

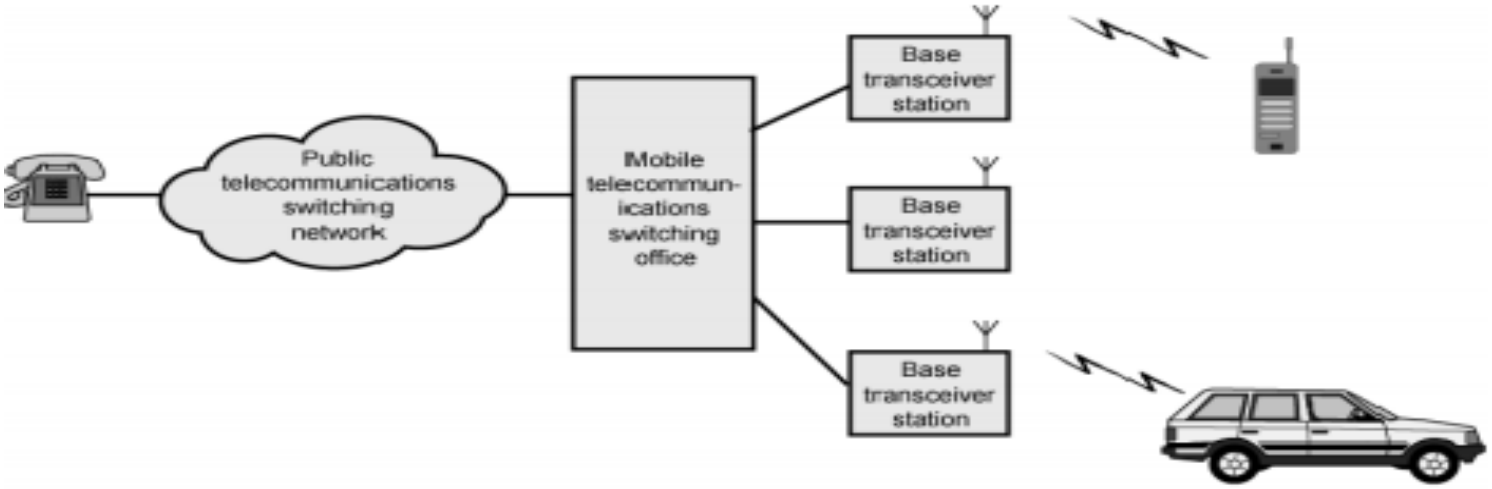
- A cell might use a different set of frequencies from neighboring cells, to avoid interference and provide guaranteed service quality within each cell.
- The key characteristic of a cellular network is the ability to re-use frequencies to increase both coverage and capacity.
- Frequency reusing is the concept of using the same radio frequencies within a given area, that are separated by considerable distance, with minimal interference, to establish communication.
- Frequency reuse offers the following benefits:
  - Allow communications within cell on given frequency
  - Allow re-use of frequencies in nearby cells
  - Use same frequency for multiple conversations

Frequency Reuse

- Each colour/letter uses the same frequency band



How does it work?



- The network architecture is very similar for most cellular systems.
- A cellular network consists of both land and radio based sections.
- Such a network is commonly referred to as a PLMN - public land mobile network

How Does it Work?

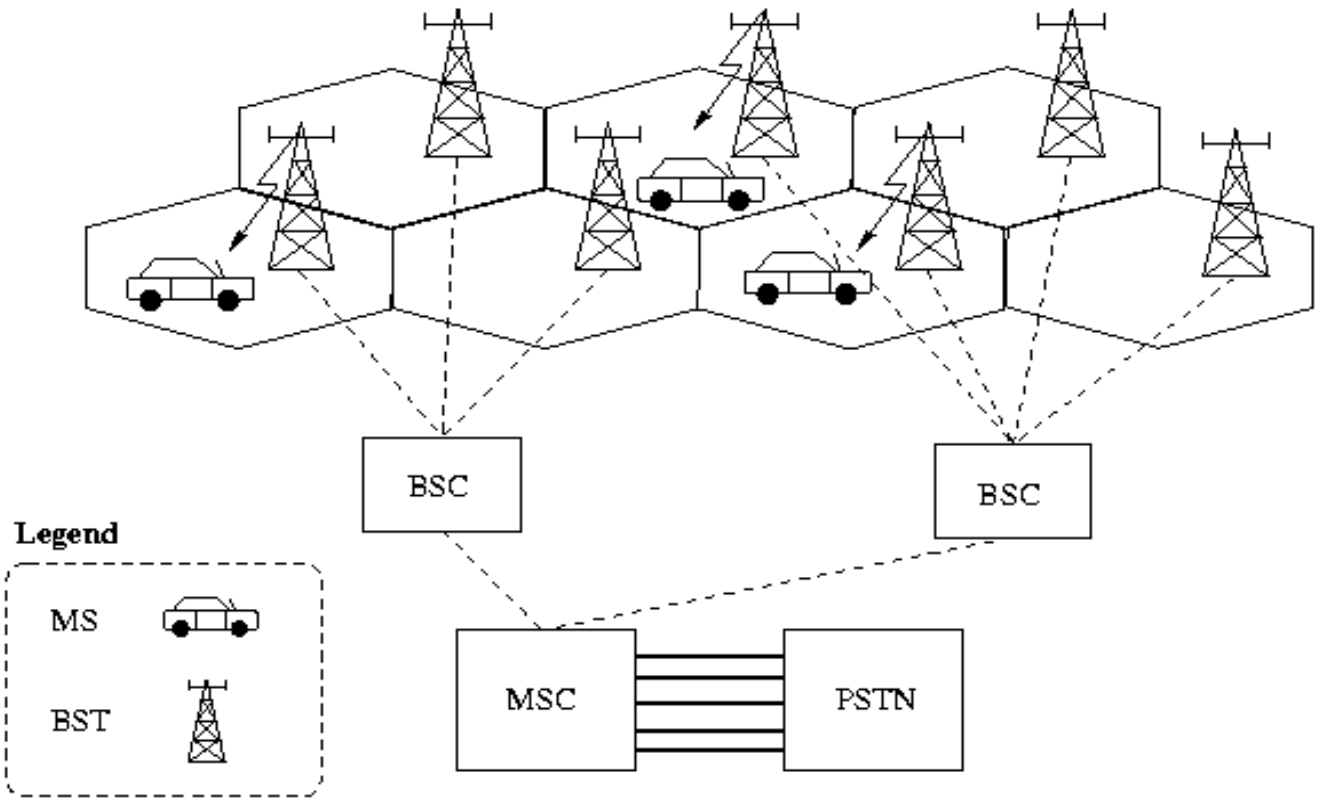


Figure 1: A cellular System

Cellular Network Architecture

- ***Mobile station (MS)*** - Device used to communicate over the cellular network.
- ***Base station tranceiver (BST)*** - Transmitter/ receiver used to transmit/ receive signals over the radio interface section of the network.
- ***Base station controller (BSC)*** - Controls communication between a group of BST's and a single MSC.
- ***Mobile switching centre (MSC)*** - The heart of the network, sets up and maintains calls made over the network.
- ***Public switched telephone network (PSTN)*** - The land based section of the network.

Cell Signal Encoding

- To distinguish signals from several different transmitters;
  - Time division Multiple Access (TDMA):
  - Frequency Division Multiple Access (FDMA)
  - Code Division Multiple Access
  - Orthogonal Frequency Division Multiple Access were developed.

Cell Signal Encoding

- With TDMA, the transmitting and receiving time slots used by different users in each cell are different from each other.
- With FDMA, the transmitting and receiving frequencies used by different users in each cell are different from each other.
- The principle of CDMA is more complex, but achieves the same result; the distributed transceivers can select one cell and listen to it.

Cellular Technologies

- There are a number of different digital cellular technologies, including:
  - Global System for Mobile Communications(GSM)
  - General Packet Radio Service (GPRS)
  - CDMA
  - Evolution-Data Optimized (EV-DO)
  - Enhanced Data Rates for GSM Evolution (EDGE)
  - Universal Mobile Telecommunications System (UMTS)
  - Digital Enhanced Cordless Telecommunications (DECT)
  - Integrated Digital Enhanced Network (iDEN)

Used Protocols

- A simple way to understand protocol stacks is to divide them in three different layers:
  - the physical layer,
  - the data link layer,
  - the network layer.

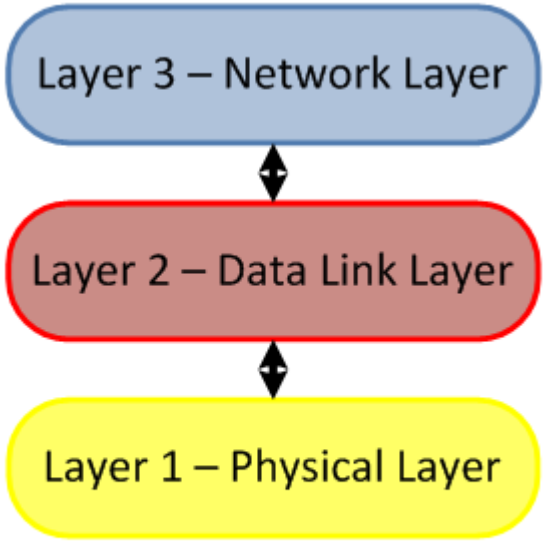


Figure 1: Protocol stack layers

The Physical Layer

- It consists, in electrical engineering terms, of the transmission and reception hardware as well the software controlling it.
  - GSM: Uses GMSK modulation, encoding 1 bit per symbol.
  - GSM/EDGE: Uses PSK8 modulation, 3 bits per symbol.
  - LTE: Uses OFDM or OFDMA modulation and includes potential multiple-input multiple-output (MIMO) features.

The Data Link Layer

- The data link layer enables the different network entities to transfer data between themselves through the physical layer.

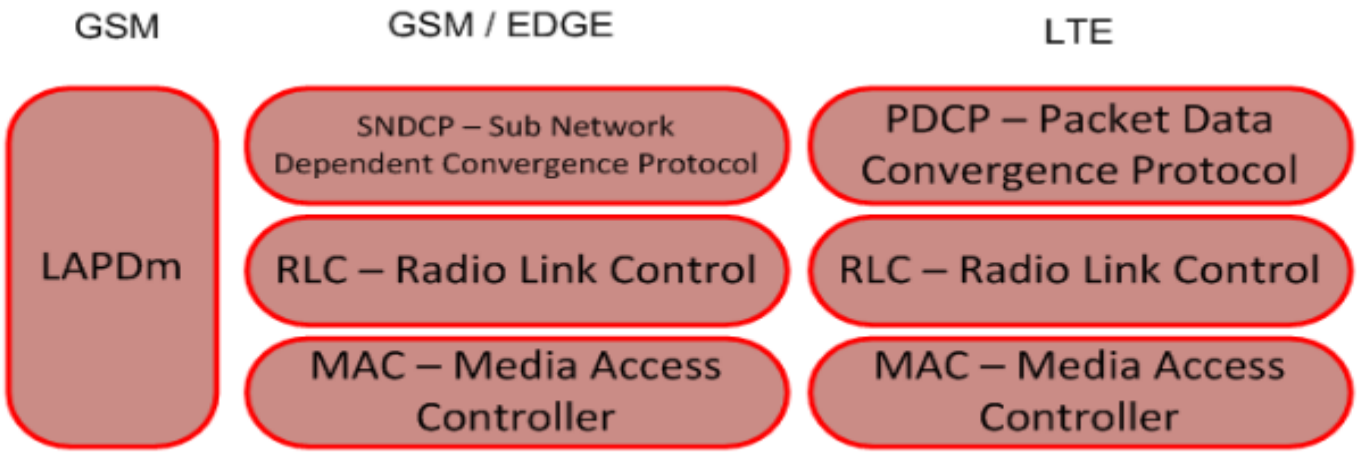


Figure 2: Data link layer (layer 2) comparision

The Data Link Layer

- The MAC sub-layer handles the mapping between the logical and transport channels, linking the RLC to the physical layer.
- Logical channels define what type of data is transported whereas transport channels define how data is transported.

The Data Link Layer:

- ***Radio Link Protocol*** *(Link Layer Protocol)* proposed a point-to-point automatic repeat request (ARQ) for radio channels.Used between Base Station and Device.
- A RLP detects packet losses and performs retransmissions to bring packet loss. A packet is retransmitted only if the transmitter is sure that it was not received.
- This makes the protocol very efficient.
- Feedback packets from the receiver together with sequence number of packets and a send sequence number at the transmitter are used to determine whether the packet was received or not.

The Data Link Layer : RLC

- In the basic protocol, the channel may be forced to be idle during periods when all retransmissions have been completed. Cellular networks such as GSM and CDMA use different variations of RLP.
- In UMTS and in LTE, the protocol is called RLC (Radio Link Control).
- The RLC sub-layer handles the transfer of user data through the logical channel connection with the MAC.

The Network Layer

- The network layer's function is the interconnection of nodes within a network.

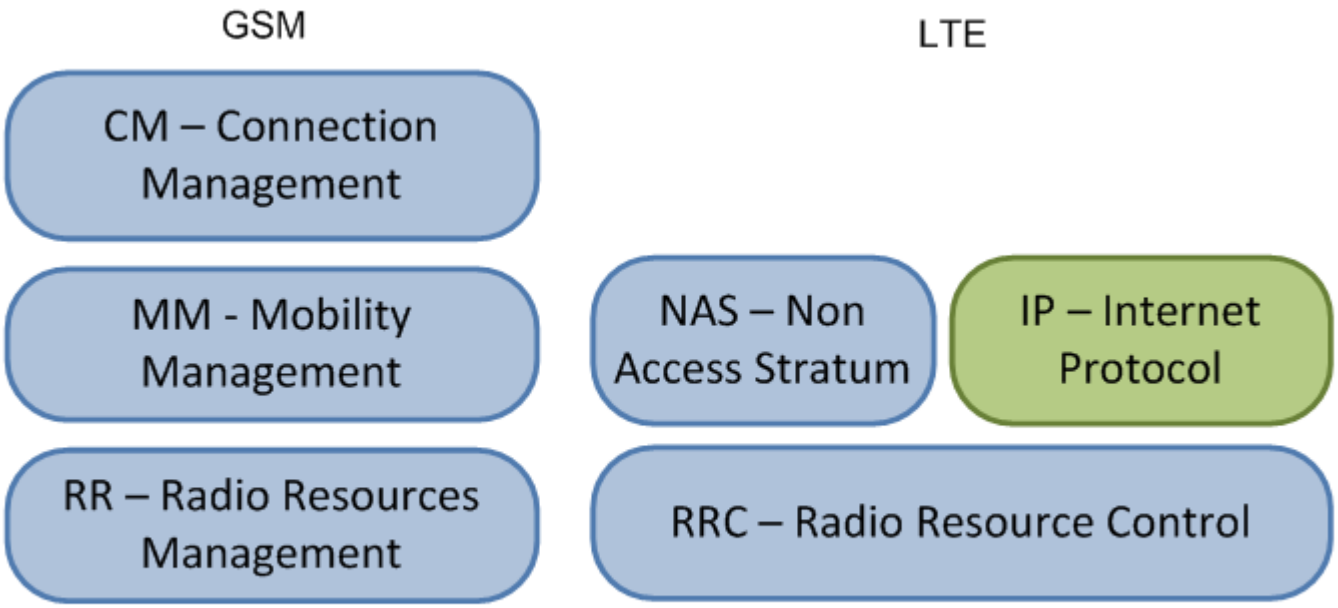


Figure 4: Network layer (layer 3) comparision

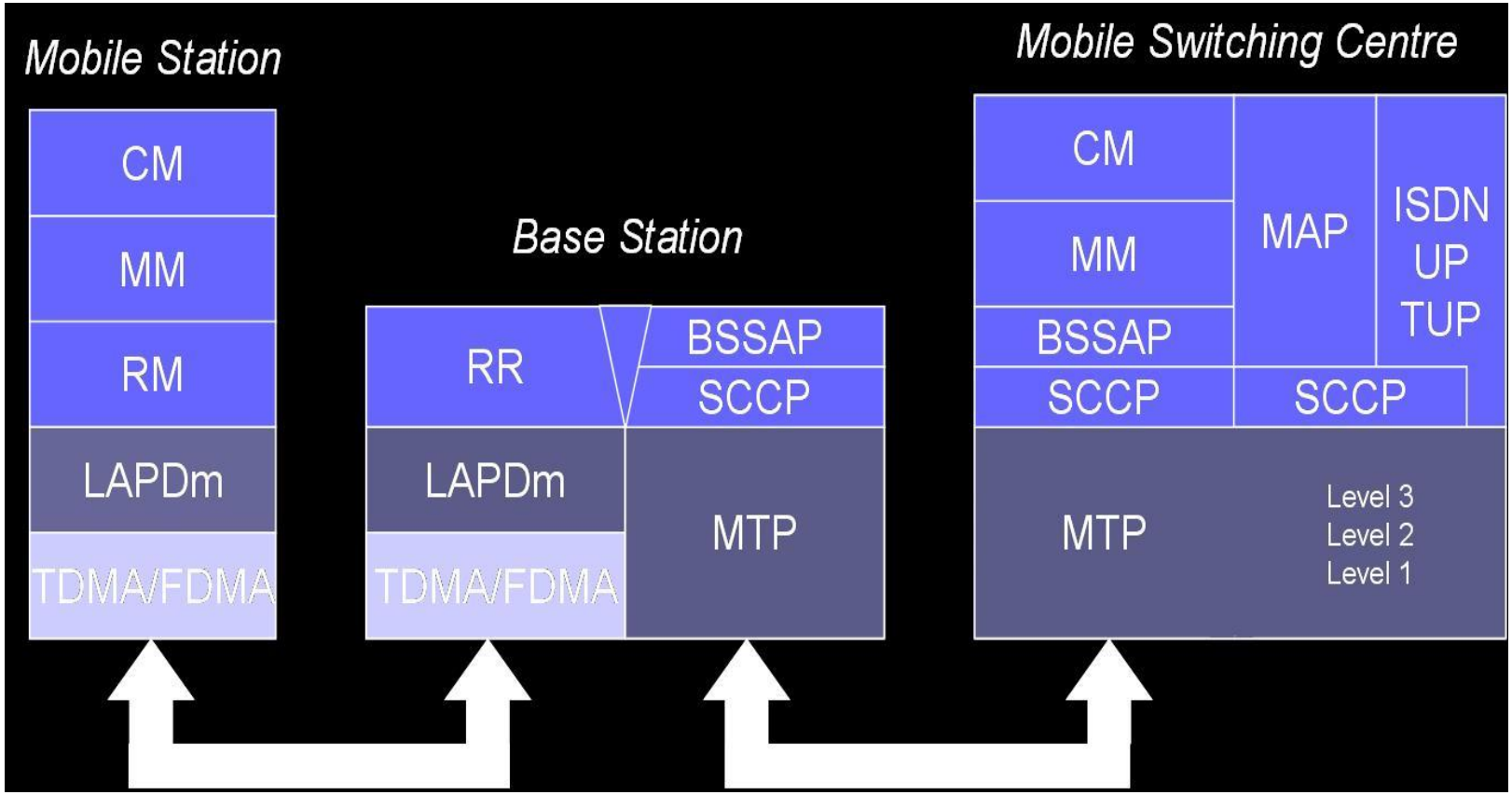
The Network Layer

- The GSM network layer is divided in three sub layers:
  - Radio resources management (RRM)
  - Mobility management (MM)
  - Connection management (CM)
- The LTE network layer is divided in two sub layers:
  - Radio resource control (RRC): Handles the point-to-point connections to the user equipment.
  - Non-access stratum (NAS): Handles the communications sessions within the network. It's in charge of mobility management and user identification.

The GSM

- The Global System for Mobile communications (GSM) is the most widely adopted 2G technology in the world.
- In GSM, there are five main functions:
  - Transmission.
  - Radio Resources management (RR).
  - Mobility Management (MM).
  - Communication Management (CM).
  - Operation, Administration and Maintenance

GSM Protocol



GSM Protocol - MS

- The GSM protocol stacks correspond to that of the OSI reference model in that layers 1 and 2 correspond to the physical and link layers as defined by the OSI model.
- Based on the interface, the GSM signaling protocol is assembled into three general layers:
  - ***Layer 1*** : The physical layer. It uses the channel structures over the air interface. The information is transmitted over the wireless link using a combination of FDMA and TDMA.
  - ***Layer 2*** The link layer. provides a link between the networking layers above it, and the physical layer below it. t provides error detection and correction of packets received from the physical layer.

GSM Protocol - MS

- **Layer 3** : GSM protocol's third layer is divided into three sublayers:
  - ***Radio Resource Management (RM):*** The general purpose of Radio Resource procedures is to establish, maintain and release RR connections that allow a point-to-point dialogue between the network and a Mobile Station.
  - ***Mobility Management (MM):*** handles connection establishment, maintenance.
  - ***Connection Management (CM):*** controls call-related and call-independent supplementary services as well as SMS. The call control (CC) protocol is one of the protocols of the Connection Management (CM) sublayer. Every mobile station must support the call

GSM Protocol – BSS Protocols

- The responsibility of the RR layer is to manage the RR-session, the time when a mobile is in a dedicated mode, and the radio channels including the allocation of dedicated channels.
- The MSC side of the base station features both message and data link layers.
- The Base Substation System Application Part (BSSAP) provides channel switching, radio resource management and internetworking functions.
- The Message Transfer Part (MTP) and Signalling Connection Control Part (SCCP) together implement the data link layer as well as layer 3 transport functions to allow the transfer of call control, mobility management and SMS data.

GSM Signalling - MSC

- The mobile switching centre is in effect the interface between the BSS and the rest of the mobile network. The signalling from here takes the form of the International Telecommunications Union (ITU) Signalling System No. 7 (SS7).
- This is the only part of the GSM infrastructure capable of packet and circuit switching; GPRS allows packet switching but is actually independent of GSM.

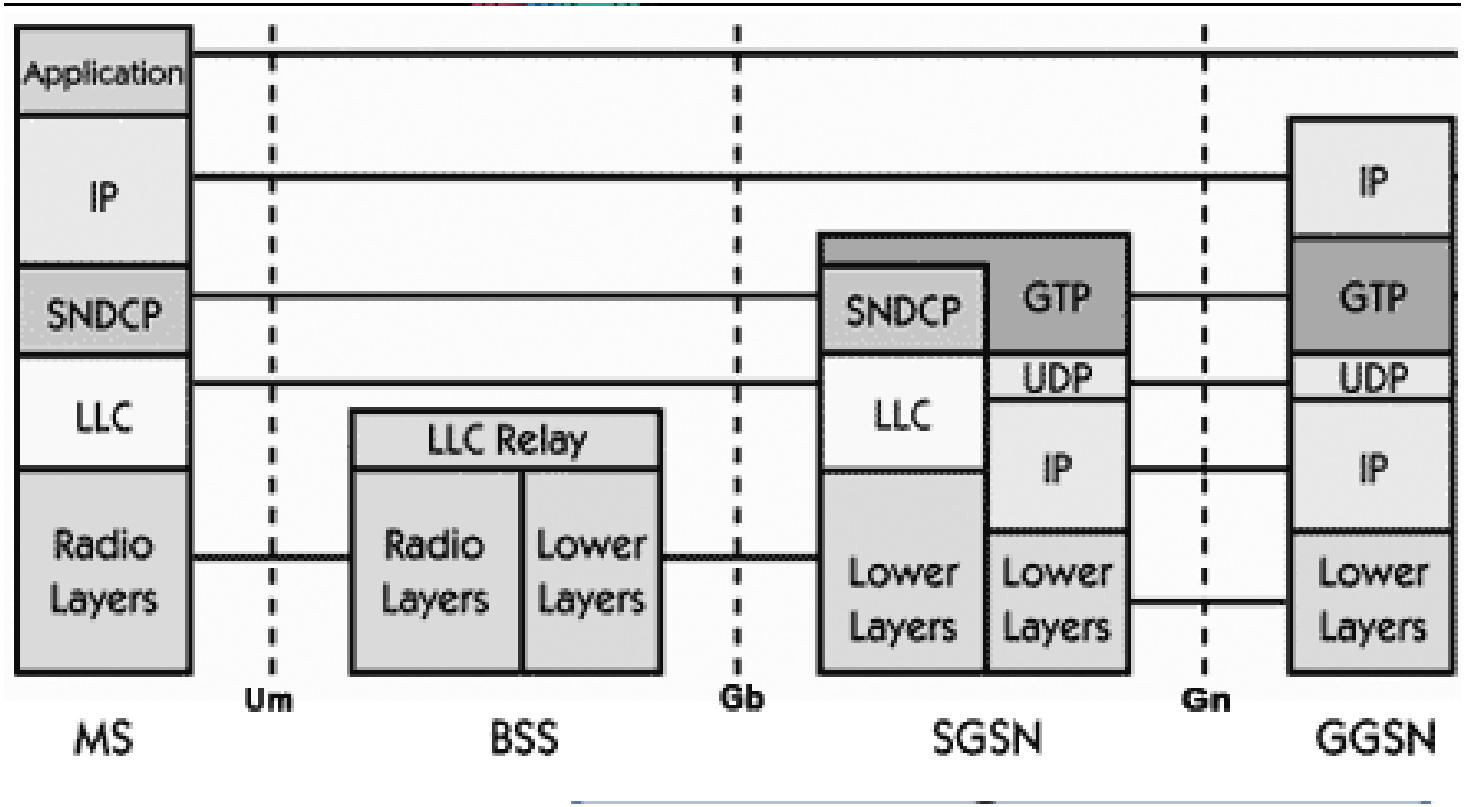
GSM Signalling – MSC - SCCP

- ***The Signalling Connection Control Part*** (SCCP), together with MTP, correspond to the lower three layers of the OSI model.
- SCCP allows for connection-oriented and connectionless services for data transfer. It is reliable and independent of the underlying hardware and transparent to users.

Signalling System No.7 - MTP

- The Message Transfer Partis split into three sublayers;
  - **Level 3:** provides congestion control, signalling management, message discrimination (priority), distribution and routing much like the network layer in OSI.
  - **Level 2:** provides a reliable, sequenced delivery of packets over level 1 connections, like the OSI data link layer
  - **Level 1:** defines characteristics of the digital signalling link and is equivalent to the OSI physical layer.

GPRS Protocol Stack

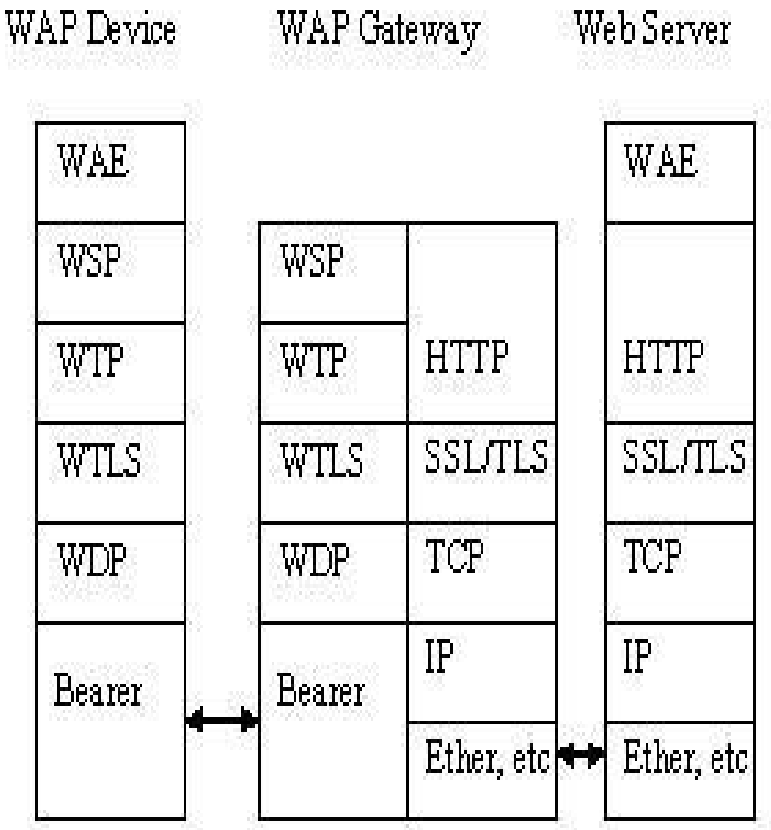


Security Issues in Cellular Networks

- There are several security issues that have to be taken into consideration when deploying a cellular infrastructure.
  - Authentication: Cellular networks have a large number of subscribers, and each has to be authenticated to ensure the right people are using the network.
  - Integrity: With services such as SMS, chat and file transfer it is important that the data arrives without any modifications.
  - Confidentiality: With the increased use of cellular phones in sensitive communication, there is a need for a secure channel in order to transmit information.
  - Device Security: If a device is lost or stolen, it needs to be protected from unauthorized use so that potential sensitive information such as emails, documents, phone numbers etc. cannot be accessed.

Wireless Application Protocol (WAP):

- Since one of the most important services provided by 3G systems is access to the Internet, it is important to understand the security mechanisms of the protocol used to access the Internet.
- WAP is an open specification which enables mobile users to access the Internet.
- This protocol is independent of the underlying network e.g. WCDMA, CMDA 2000



Wap Protocol Stack

WAP

- Wireless Application Environment (WAE): This provides an environment for running web applications or other WAP applications.
- Wireless Session Protocol (WSP): This is similar to the HTTP protocol and provides data transmissions with small sizes so that WAP1 clients can process the data with less complexity.
- Wireless Transaction Protocol (WTP): This is responsible for providing reliability.
- Wireless Transport Layer Security (WTLS): This is responsible for providing security features such as authentication, confidentiality, integrity etc. between a WAP1 client and the WAP gateway.
- Wireless Datagram Protocol (WDP): This provides the underlying transport service.

WAP

- Hypertext Transfer Protocol (HTTP): A standard protocol used to transmit web pages.
- Transport Layer Security (TLS): This layer provides security features such as authentication, confidentiality, integrity etc. In WAP1, this is between the WAP1 gateway and the server. In WAP2 this is between the WAP2 client and the server.
- Transport Control Protocol (TCP): Standard transport protocol used to provide reliability over IP.
- Internet Protocol (IP): Protocol used to route data in a network.
- Bearer Protocol: This is the lowest level protocol and can be any wireless technique such as GSM, CDMA etc.

The List of Cellular Data Communication Protocols

- BSMAP
- BSSLAP
- BSSAP
- DLCI
- BSSAPLE
- BSSMAP
- BTSM
- CC
- DTAP (CDMA)
- DTAP (GSM)
- MM
- MMS
- RR

Advantages of Cellular Networks

- Cellular networks use "small" cells with low powered transceivers instead of one large area with a high powered transceiver.
- Using cellular networks increases overall call handling capacity.
- Avoids central point of failure.
- Allows dynamic distribution of capacity based on demand.
- Less interference with other wireless communications
- Cellular radio network infrastructures are growing at a tremendous rate.
- Cellular networks are becoming high speed data networks.

THANK YOU…

ÖNEMLİ

Bu projeler lisansüstü öğrencilerinin hazırladığı çalışmalar olup tüm sorumluluk hazırlayan öğrencilere aittir. Öğrenciler hazırladığı projeye göre not almışlardır.