Name: Hassan Mudassir

ID:13003

Course: Wireless Network

Question 1:

A) List five ways of increasing the capacity of a cellular system?

Ans) 1) Cell splitting:

Cell splitting is the process of sub dividing a congested cell into smaller cells, each with its own base station and corresponding reduction in antenna height and transmitted power. Cell splitting increases capacity of a cellular system since it increases number of times that channels are reused.

2) Adding new channels:

Typically, when a system is set up in a region, not all of the channels are used, and growth and expansion can be managed in an orderly fashion by adding new channels.

3) Microcell zone concept:

The increased number of hands off, increase load on the switching and control link because of sectoring. A solution to this problem is given by microcell zone concept.

4) Cell sectoring:

In cell sectoring a single omnidirectional antenna at base station is replaced by several directional antennas, each radiating within a specified sector.

5) Frequency borrowing:

In the simplest case, frequencies are taken from adjacent cells by congested cells. The frequencies can also be assigned to cells dynamically.

B) Briefly differentiate between 3G, 4G & 5G Cellular Networks?

Ans) 3G:

Introduced in year: 2001

Technology: WCDMA

Access system: CDMA

Switching type: Packet switching except for air interference

Internet service: Broadband

Bandwidth: 25 MHz

Advantage: High Security, International Roaming

Applications: Video conferencing, mobile TV, GPS

4G:

Introduced in year: 2009

Technology: LTE, WiMAX

Access system: CDMA

Switching type: Packet Switching

Internet service: Ultra Broadband

Bandwidth: 100 MHz

Advantage: Speed, High speed handoffs, global mobility

Applications: High speed applications, Mobile TV, wearable devices

5G:

Introduced in year: 2018

Technology: MIMO, mm Waves

Access system: OFDM, BDMA

Switching type: Packet switching

Internet service: Wireless World Wide Web

Bandwidth: 30 GHz to 300GHz

Advantage: Extremely high speeds, Low Latency

Applications: High Resolution video streaming, remote control of vehicles, robots and medical procedures

---

C) Briefly explain Overall GSM Architecture with the help of diagram?

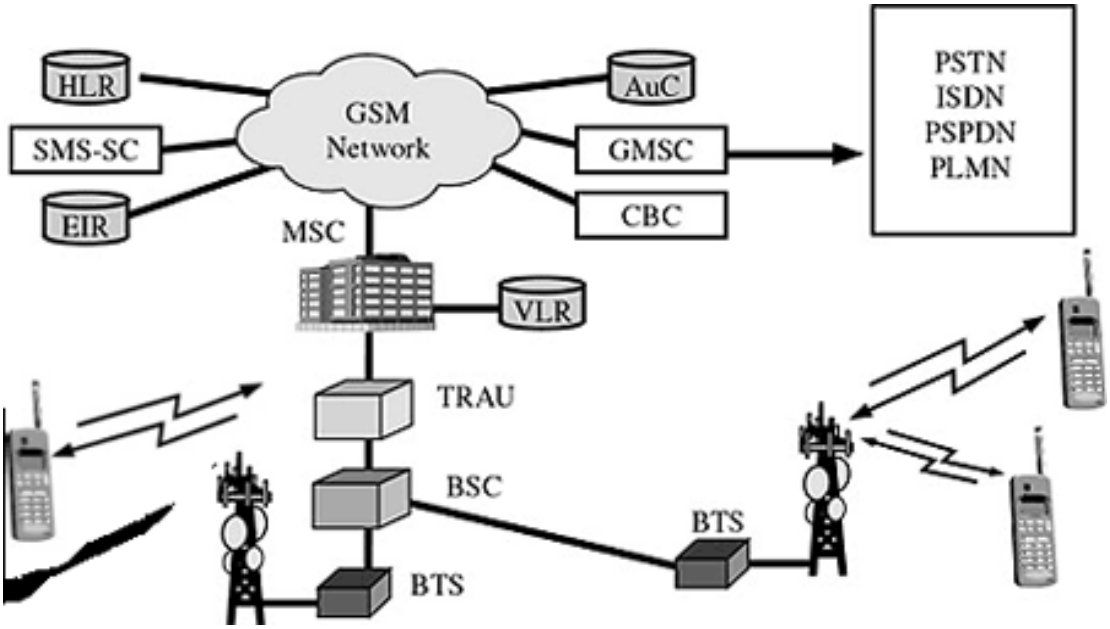
Ans) A GSM network comprises of many functional units. These functions and interfaces are explained in this chapter. The GSM network can be broadly divided into:

- The Mobile Station (MS)
- The Base Station Subsystem (BSS)
- The Network Switching Subsystem (NSS)
- The Operation Support Subsystem (OSS)

The additional components of the GSM architecture comprise of databases and messaging systems functions:

- Home Location Register (HLR)
- Visitor Location Register (VLR)
- Equipment Identity Register (EIR)
- Authentication Center (AuC)
- SMS Serving Center (SMS SC)
- Gateway MSC (GMSC)
- Chargeback Center (CBC)
- Transcoder and Adaptation Unit (TRAU)

The following diagram shows the GSM network along with the added elements:



D) A telephony connection has duration of 35 minutes. This is the only connection made by this caller during the course of an hour. How much is the amount of traffic, in Erlangs, of this connection?

Ans) $A = \lfloor h = 1 * (35/60) = 0.583$ Erlangs

E) What are the current and future cellular network issues and challenges?

Ans) Current Issues and challenges:

Traffic Volume Growth. Around the world cellular networks are seeing between 60% to 120% annual growth in data volumes. The problem with that kind of growth is that as soon as any upgrade is made to a part of the network it is consumed by the growth. This kind of growth means constant choke points in the network and problems encountered by customers.

WiFi Offload Not Effective. For years cellular networks have talked about offloading data to WiFi. But the industry estimates are that only between 5% and 15% of data through cellphones is being handled by WiFi. This figure does not include usage in homes and offices where the phone user elects to use their own local network, but rather is the traffic that is offloaded when users are outside of their base environment. Finding ways to increasing WiFi offload would lower the pressure on mobile networks.

Traffic has Moved Indoors. An astounding 75% of mobile network traffic originates from inside buildings. Historically mobile traffic came predominantly from automobiles and people outside, but the move indoors looks like a permanent new phenomenon driven by video and data usage.

Still Too Many Failures. There are still a lot of dropped voice calls, and 80% of them are caused by mobility failures, meaning a failure of the network to handle a customer on the move. 50% of dropped data sessions are due to capacity issues.

Cellular providers are looking for the capacity to more dynamically assign radio resources on the fly at different times of the day. It’s been shown that there are software techniques that can optimize the local network and can reduce failures by as much as 25%.

CHALLENGES TO FUTURE MOBILE NETWORKS

We can divide the challenges of future mobile networks into following categories:

• Efficient utilization of network resources in CHN environment.

• Technological independent network access, end to end connection and seamless handover.

• Maintaining the certain level of QoS (Quality of Service) for user applications.

• Cooperative network management.

• An intelligent billing policy.

Question 2:

F) List and briefly define the capabilities provided by Mobile IP?

Ans: Mobile IP includes three basic capabilities:

- **Discovery.** A mobile node uses a discovery procedure to identify prospective home agents and foreign agents.
- **Registration.** A mobile node uses an authenticated registration procedure to inform its home agent of its care-of address.
- **Tunneling.** Tunneling is used to forward IP datagrams from a home address to a care-of address.

G) What are the two different types of destination addresses that can be assigned to a mobile node while it is attached to a foreign network?

Ans: The destination care-of address can either be that of a foreign agent, or it can be a co-located address that is associated physically with the node.

H) What is tunneling?

Ans: Tunneling:

Tunneling is a process in which an IP datagram is encapsulated with an outer IP header so as to be transmitted across the Internet using the destination address and parameters of the outer header.

I) Briefly explain WAE, WSP, WTP, WTLS, WDP & WCMP Protocols in WAP Protocol Stack?

Ans) WAE – WIRELESS APPLICATION ENVIRONMENT

The Wireless Application Environment (WAE) defines the following functions:

Wireless Markup Language (WML).

WML is an XML-based markup language for the visual display of WAP-based contents. Once HTML and WML will converge into XML, many compatibility problems, during conversion from HTML to WML, will cease to exist.

WML Script.

A script language, very similar to JavaScript.

Wireless Telephony Application (WTA, WTAI).

Telephony services and Programming interfaces.

Content formats.

These are specifications for data formats, including images, telephone directories, calendar information, and so on.

The WAE corresponds to the application layer in the OSI model.

WSP – WIRELESS SESSION PROTOCOL

The Wireless Session Protocol (WSP) implements an interface for connection-oriented and connectionless session services. The connection-oriented session service operates using the protocol of the transaction layer. However, the connectionless session service uses a secure or non-secure datagram service.

WSP offers the following basic functions:

- Functions and semantics of HTTP/1.1, using a compact coding scheme
- Pausing and resuming sessions
- A general facility for reliable and unreliable data push
- Negotiation of protocol functions

WTP – WIRELESS TRANSACTION PROTOCOL

The Wireless Transaction Protocol (WTP) is a transaction-oriented protocol, executed using a datagram service. WTP offers the following functions:

Three classes of transaction services

(a) Unreliable one-way requests

(b) Reliable one-way requests

(c) Reliable two-way request/response transactions

Optional user-to-user reliability feature.

The WTP user triggers confirmation for each received message.

Optional out-of-band data for confirmations.

Protocol Data Unit (PDU) chaining and delayed confirmation.

In order to reduce the number of sent messages

Asynchronous transactions

WTLS – WIRELESS TRANSACTION LAYER SECURITY

The WTLS layer implements a security protocol based on the TLS (Transport Layer Security) industry standard. WTLS is intended for use with the WAP transport protocols and has the following features:

Data integrity – WTLS ensures that the data sent between the terminal and an application server is in no way altered or damaged.

Confidentiality – WTLS ensures that the data sent between the terminal and an application server remains confidential and cannot be understood by any other participant who may have intercepted the data stream.

Authentication – WTLS ensures the authenticity of the terminal and of the application server.

Denial-of-service protection – Wireless Transaction Layer Security (WTLS) contains features that will recognize and reject data that has been repeated or not verified successfully. WTLS hinders many typical denial-of-service attacks and protects the upper protocol layers. Though, this is not a perfect solution.

WDP – WIRELESS DATAGRAM PROTOCOL

The WDP layer operates on various bearers that depend on the used network type. WDP offers a consistent interface for the upper layers, so that communications occurs transparently using one of the available bearer services. Therefore, the transport layer is adapted to the specific functions of the underlying bearer.

WCMP – WIRELESS CONTROL MESSAGE PROTOCOL

The Wireless Control Message Protocol defines the error reporting mechanism for WDP datagrams as well as the protocol elements that can be used for diagnosis and informational purposes (for example, WCMP echo request and response). WCMP is determined depending on the bearer used. In IP-based networks, WCMP functions are implemented using the Internet Control Message Protocol (ICMP).

Question 3:

a) **List and briefly define the IEEE 802 protocol layers**

Ans)

- **Logical link control (LLC):**

Provides an interface to higher layers and perform flow and error control.

- **Medium access control (MAC):**

Provides addressing for physical attachment points to the LAN and provides medium access.

- **Physical:**

Defines the topology, transmission medium, and signaling.

B) Briefly differentiate between IEEE 802.11 n, o, p, r, s, t, u, v standards and their services?

Ans) **IEEE 802.11n-2009**: commonly shortened to 802.11n, is a wireless-networking standard that uses multiple antennas to increase data rates. The Wi-Fi Alliance has also retroactively labelled the technology for the standard as Wi-Fi 4. It standardized support for multiple-input multiple-output, frame aggregation, and security improvements, among other features, and can be used in the 2.4 GHz or 5 GHz frequency bands.

The purpose of the standard is to improve network throughput over the two previous standards—802.11a and 802.11g—with a significant increase in the maximum net data rate from 54 Mbit/s to 72 Mbit/s with a single spatial stream in a 20 MHz channel, and 600 Mbit/s (slightly higher gross bit rate including for example error-correction codes, and slightly lower maximum throughput) with the use of four spatial streams at a channel width of 40 MHz

IEEE 802.11p is an approved amendment to the IEEE 802.11 standard to add wireless access in vehicular environments (WAVE), a vehicular communication

system. It defines enhancements to 802.11 (the basis of products marketed as Wi-Fi) required to support Intelligent Transportation Systems (ITS) applications. This includes data exchange between high-speed vehicles and between the vehicles and the roadside infrastructure, so called V2X communication, in the licensed ITS band of 5.9 GHz (5.85–5.925 GHz). IEEE 1609 is a higher layer standard based on the IEEE 802.11p

IEEE 802.11r-2008 or **fast BSS transition** (**FT**), also called fast roaming, is an amendment to the IEEE 802.11 standard to permit continuous connectivity aboard wireless devices in motion, with fast and secure handoffs from one base station to another managed in a seamless manner. It was published on July 15, 2008. IEEE 802.11r-2008 was rolled up into 802.11-2012

IEEE 802.11s is Wireless LAN standard and an IEEE 802.11 amendment for mesh networking, defining how wireless devices can interconnect to create a WLAN mesh network, which may be used for relatively fixed (not mobile) topologies and wireless ad hoc networks. The IEEE 802.11s working group draws upon volunteers from university and industry to provide specifications and possible design solutions for wireless mesh networking. As a standard, the document was iterated and revised many times prior to finalization.

IEEE 802.11:

In July 2004, the IEEE formed the IEEE 802.11T Task Group to develop a test specification document, "Recommended Practice for the Evaluation of 802.11 Wireless Performance," expected to be completed in January 2008. By forming the task group, the IEEE has acknowledged the need to provide users with an objective means of evaluating functionality and performance of 802.11 products.

The 802.11T document defines test metrics in the context of use cases. The three principal-use cases are data, latency sensitive and streaming media.

IEEE 802.11u-2011 is an amendment to the IEEE 802.11-2007 standard to add features that improve interworking with external networks.

802.11 is a family of IEEE technical standards for mobile communication devices such as laptop computers or multi-mode phones to join a wireless local area

network (WLAN) widely used in the home, public hotspots and commercial establishments.

The IEEE 802.11u standard was published on February 25, 2011.

802.11v is the Wireless Network Management standard for the IEEE 802.11 family of standards. 802.11v allows client devices to exchange information about the network topology, including information about the RF environment, making each client network aware, facilitating overall improvement of the wireless network.

802.11v describes enhancements to wireless network management, such as:

- Network assisted Power Savings - Helps clients to improve battery life by enabling them to sleep longer. For example, mobile devices use a certain amount of idle period to ensure that they remain connected to access points and therefore consume more power when performing the following tasks in a wireless network.
- Network assisted Roaming - Enables the WLAN to send messages to associated clients, for better APs to associate with clients. This is useful for both load balancing and in directing poorly connected clients.

Question 4:

a) **Throw some light on Bluetooth Low Energy (BLE) wireless technology?**

Ans) Bluetooth Low Energy

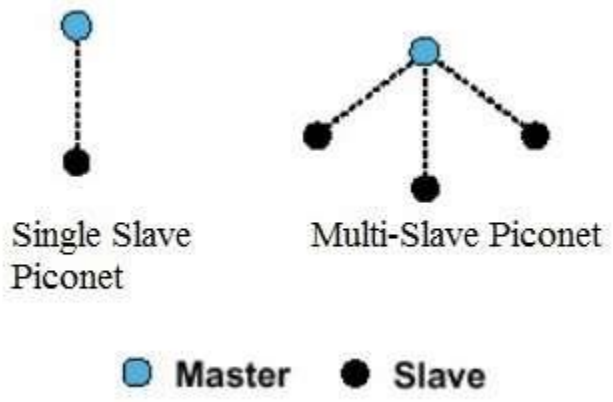
Bluetooth Low Energy is the intelligent, power-friendly version of Bluetooth wireless technology. It is already playing a significant role in transforming smart gadgets to smarter gadgets by making them compact, affordable, and less complex.

Bluetooth Low Energy, also marketed as Bluetooth Smart, started as part of the Bluetooth 4.0 Core Specification. Initially designed by Nokia as Wibree before being adopted by the Bluetooth Special Interest Group (SIG), its initial focus was to provide a radio standard with the lowest possible power consumption, specifically optimized for low cost, low bandwidth, low power, and low complexity.

B) Briefly differentiate between Piconets and Scatternets? Explain with the help of diagrams:

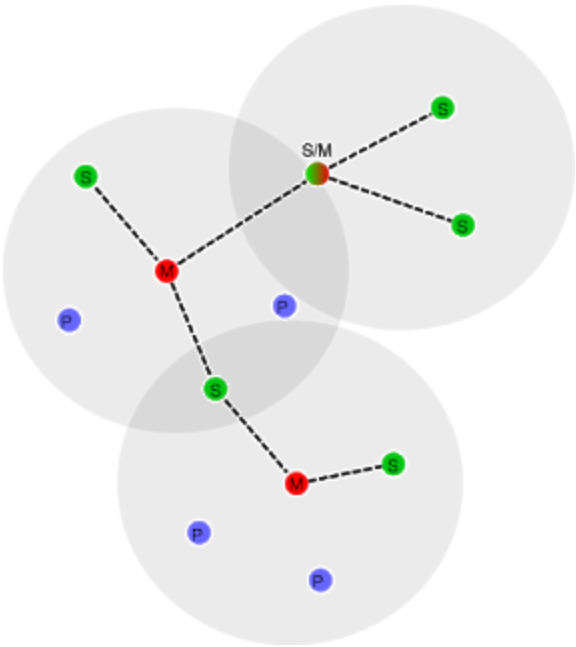
Ans) Piconet:

A piconet is the type of connection that is formed between two or more Bluetooth-enabled devices such as modern cell phones or PDAs. Bluetooth enabled devices are "peer units" in that they are able to act as either master or slave. However, when a piconet is formed between two or more devices, one device takes the role of 'master', and all other devices assume a 'slave' role for synchronization reasons. Piconets have a 7 member address space (3 bits, with zero reserved for broadcast), which limits the maximum size of a piconet to 8 devices, i.e. 1 master and 7 slaves.



Scatternet:

A scatternet is a number of interconnected piconets that supports communication between more than 8 devices. Scatternets can be formed when a member of one piconet (either the master or one of the slaves) elects to participate as a slave in a second, separate piconet. The device participating in both piconets can relay data between members of both ad hoc networks. However, the basic bluetooth protocol does not support this relaying - the host software of each device would need to manage it. Using this approach, it is possible to join together numerous piconets into a large scatternet, and to expand the physical size of the network beyond Bluetooth's limited range.



Scatternet (master=red, slave=green, parking=blue)

C) Define L2CAP data packet format?

Ans) Logical Link Control and Adaptation Protocol (L2CAP):

L2CAP is packet-based but follows a communication model based on channels. A channel represents a data flow between L2CAP entities in remote devices. Channels may be connection-oriented or connectionless. All packet fields use Little Endian byte order.
