IQRA NATIONAL UNIVERSITY

Department of Computer Science

Wireless network

Name. : Ali Muqadas

ID. : 13131

Submitted to: Sir Ghassa Husain

Assignment: **Final paper**

Question 1

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

The five ways of increasing the capacity of cellular system are

- Adding new channels
- Frequency borrowing
- Cell splitting
- Cell sectoring
- Microcells

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

3G (500-700 Kbps) (2004-2005):

3G has Multimedia services support along with streaming are more popular. In 3G, Universal access and portability across different device types are made possible. (Telephones, PDA's, etc.)

4G (100-300 Mbps) (Present):

Speeds for 4G are further increased to keep up with data access demand used by various services. High definition streaming is now supported in 4G. New phones with HD capabilities surface. Portability is increased further. World-wide roaming is not a distant dream.

5G (Probably Gigabits) (Probably 2020):

Currently there is no 5G technology deployed but under testing. When this becomes available it will provide very high speeds to the consumers. It would also provide efficient use of available bandwidth as has been seen through development of each new technology.

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

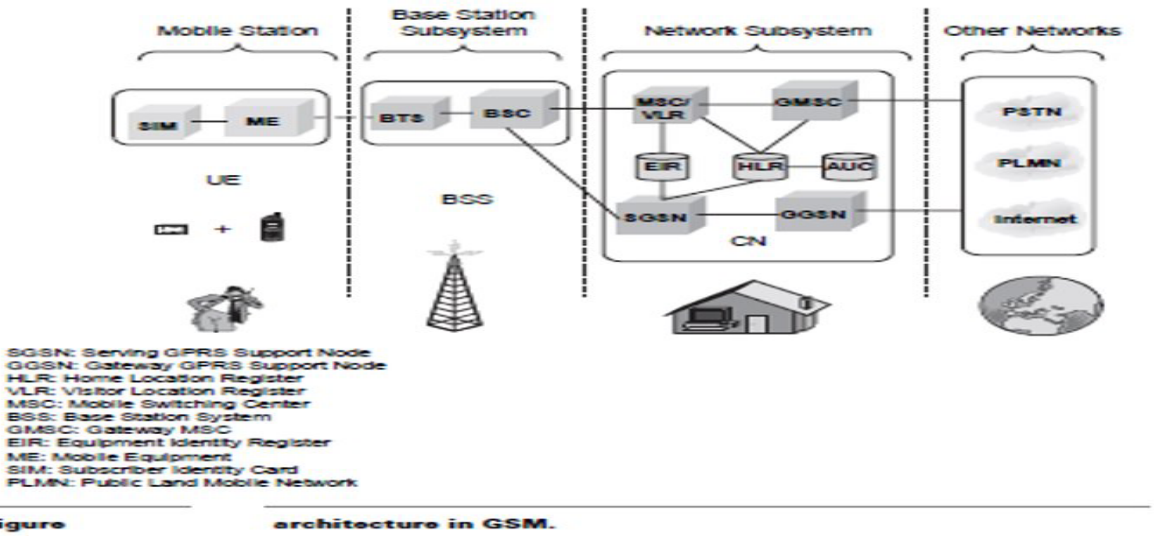


Figure architecture in GSM.

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?**

0.58 Erlangs

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

Reliability

While 100% reliability beats 99%, and 99% is good most of the time, 99% is frightening in many applications. Sure, it is easy to design a pace maker or blood pressure monitor with modern wireless IoT wireless capabilities, but nobody thinks 99% is acceptable in every location and under every circumstance. This hold back many valuable applications unless (or until) firms find ways to address it.

Security

While lax security is not a problem for boxes of razor blades shipped across the country that is not acceptable for something like an autonomous vehicle. If you don't think so, I can show you scores of rogue programmers just waiting to hold your automobile for ransom. Again, this will hold back many valuable applications.

Privacy protection. While privacy rules pose few issues for the temperature gauges on an oil pipeline, not so for devices that read activity at home. For example, just recently a vibrator company got in trouble for sending a little too much data back to the company that designed the product. It is funny, but symptomatic of a much bigger issue.

System design

Real time integration of massive data is already feasible, but those types of applications have many potential points of failure. After all, the integration of Waze with Google Maps already integrates huge numbers of low-bandwidth signals into an application that many can access. It may be irritating when it is inaccurate, but you can survive without it if the network goes down. But there lies the rub. Nobody is suggesting we integrate airplane traffic with digital weather data, and have the computers do all the routing and land the aircraft. We still need humans because the systems are flawed. To be sure, there are some things we can improve.

Question 2

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

Mobile IP was established to allow computers to keep internet connectivity while moving from one Internet connection point to another.

Primarily Mobile IP contains 3 basic capabilities

- Discovery
- Registration
- Tunnelling

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?

Types of Destination Address

There are two different types of destination addresses that can be allocated to a mobile node while it is attached to a foreign network.

They are:

- Home address
- Care-of address

h) What is tunnelling?

Force a packet to go to a specific point in the network.

- Path taken is different from the regular routing
- Achieved by adding an extra IP header to the packet with a new destination address.
- Similar to putting a letter in another envelope
- Preferable to using IP source routing option

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

- Wireless Application Environment (WAE)

This layer is of most interest to content developers because it contains among other things, device specifications, and the content development programming languages, WML, and WMLScript.

- Session Layer

Wireless Session Protocol (WSP). Unlike HTTP, WSP has been designed by the WAP Forum to provide fast connection suspension and reconnection.

- Transaction Layer

Wireless Transaction Protocol (WTP). The WTP runs on top of a datagram service, such as User Datagram Protocol (UDP) and is part of the standard suite of TCP/IP protocols used to provide a simplified protocol suitable for low bandwidth wireless stations.

- Security Layer

Wireless Transport Layer Security (WTLS). WTLS incorporates security features that are based upon the established Transport Layer Security (TLS) protocol standard. It includes data integrity checks, privacy, service denial, and authentication services.

- Transport Layer

Wireless Datagram Protocol (WDP). The WDP allows WAP to be bearer-independent by adapting the transport layer of the underlying bearer. The WDP presents a consistent data format to the higher layers of the WAP protocol stack, thereby offering the advantage of bearer independence to application developers.

Question 3

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

In IEEE 802 terms, the OSI data link layer is divided into two sublayers: logical link control (LLC) and media access control (MAC).

The data link layer functions allocated to the LLC sublayer are:

- Link establishment and termination
- Frame traffic control
- Frame sequencing
- Frame acknowledgment

The data link layer functions allocated to the MAC sublayer are:

- Frame delimiting
- Frame error checking
- Media access management

The low-level protocol standards defined by IEEE project 802 include 802.3 CSMA/CD, 802.4 token bus, and 802.5 token ring. These standards differ at the physical layer and media access control sublayer, but are compatible at the logical link control sublayer.

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

802.11 — applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).

802.11a — an extension to 802.11 that applies to wireless LANs and provides up to 54-Mbps in the 5GHz band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS.

802.11b (also referred to as 802.11 High Rate or Wi-Fi) — an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1-Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.

802.11e — a wireless draft standard that defines the Quality of Service (QoS) support for LANs, and is an enhancement to the 802.11a and 802.11b wireless LAN (WLAN) specifications. 802.11e adds QoS features and multimedia support to the existing IEEE 802.11b and IEEE 802.11a wireless standards, while maintaining full backward compatibility with these standards.

802.11g — applies to wireless LANs and is used for transmission over short distances at up to 54-Mbps in the 2.4 GHz bands.

802.11n — 802.11n builds upon previous 802.11 standards by adding multiple-input multiple-output (MIMO). The additional transmitter and receiver antennas allow for increased data throughput through spatial multiplexing and increased range by exploiting the spatial diversity through coding schemes like Alamouti coding. The real speed would be 100 Mbit/s (even 250 Mbit/s in PHY level), and so up to 4-5 times faster than 802.11g.

802.11ac — 802.11ac builds upon previous 802.11 standards, particularly the 802.11n standard, to deliver data rates of 433Mbps per spatial stream, or 1.3Gbps in a three-antenna (three stream) design. The 802.11ac specification operates only in the 5 GHz frequency range and features support for wider channels (80MHz and 160MHz) and beamforming capabilities by default to help achieve its higher wireless speeds.

802.11ac Wave 2 — 802.11ac Wave 2 is an update for the original 802.11ac spec that uses MU-MIMO technology and other advancements to help increase theoretical maximum wireless speeds for the spec to 6.93 Gbps.

802.11ad — 802.11ad is a wireless specification under development that will operate in the 60GHz frequency band and offer much higher transfer rates than previous 802.11 specs, with a theoretical maximum transfer rate of up to 7Gbps (Gigabits per second).

802.11ah— Also known as Wi-Fi HaLow, 802.11ah is the first Wi-Fi specification to operate in frequency bands below one gigahertz (900 MHz), and it has a range of nearly twice that of other Wi-Fi technologies. It's also able to penetrate walls and other barriers considerably better than previous Wi-Fi standards.

802.11r - 802.11r, also called Fast Basic Service Set (BSS) Transition, supports VoWi-Fi handoff between access points to enable VoIP roaming on a Wi-Fi network with 802.1X authentication.

802.1X — Not to be confused with 802.11x (which is the term used to describe the family of 802.11 standards) 802.1X is an IEEE standard for port-based Network Access Control that allows network administrators to restricted use of IEEE 802 LAN service access points to secure communication between authenticated and authorized devices.

Question 4

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

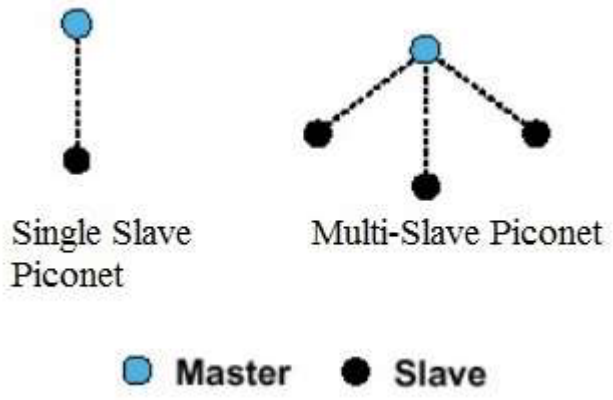
Bluetooth Low Energy (Bluetooth LE, BLE, formerly marketed as Bluetooth Smart is a wireless personal area network technology designed and marketed by the Bluetooth Special Interest Group aimed at novel applications in the healthcare, fitness, beacons, security, and home entertainment industries .Compared to Classic Bluetooth, Bluetooth

Low Energy is intended to provide considerably reduced power consumption and cost while maintaining a similar communication range.

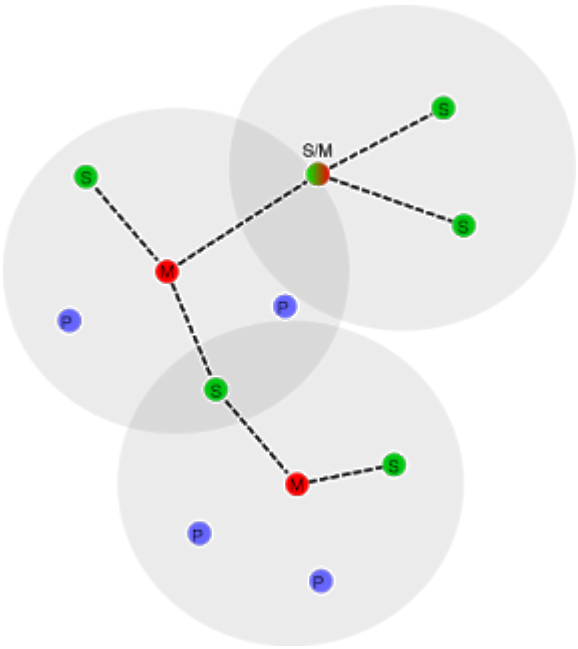
Mobile operating systems including iOS, Android, Windows Phone and BlackBerry, as well as mac OS, Linux, Windows 8 and Windows 10, natively support Bluetooth Low Energy. The Bluetooth SIG predicts that by 2018 more than 90 percent of Bluetooth-enabled smartphones will support Bluetooth Low Energy.

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

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.



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.



c) Define L2CAP data packet format?

The Logical Link Control and Adaptation Layer Protocol (L2CAP) is layered over the Baseband Protocol and resides in the data link layer. L2CAP provides connection-oriented and connectionless data services to upper layer protocols with protocol multiplexing capability, segmentation and reassembly operation, and group abstractions. L2CAP permits higher level protocols and applications to transmit and receive L2CAP data packets up to 64 kilobytes in length.
