Unit-I

Brief History of Mobile Computing

- Mobile Computing = Computing + Mobility + Connectivity
  - 1993 Apple: Newton Message Pad, First hand-held computer, Display rotated 90, 180, or 270 degrees, depending on device orientation,Device ran the Newton operating system,Used handwriting recognition powered by Calligrapher handwriting recognition engine.
  - 1996 US Robotics Palm Pilot,The Palm Pilot was called a PDA (Personal Digital Assistant)
- 1999 BlackBerry First Blackberry device was a two-way pager.
  - 2002 The commonly known Convergent BlackBerry supported push email, mobile telephone, text messaging, Internet faxing, Web browsing and other wireless services.
- 2003 BlackBerry Quark first device with integrated email and phone, iPhone
  - 1980s Objective-C language created by Cox and Love at their software company Stepstone
  - 2007 First integrated smart phone; iPhone apps written in Objective C language
  - 2014 Swift language released for writing iPhone apps. Swift has been characterized as Objective-C without the C.
  - 2019 Currently there are close to 1 billion iPhone and iPad devices in use.
- **Google and Android**
  - 1998 Google was founded by graduate students at Stanford.
  - 2003 Android was founded by Rubin and Miner in Palo Alto, California.
  - 2005 Google buys Android.
  - 2007 Android operating system released. Based on the Linux kernel.
  - 2007 Open Handset Alliance formed. A consortium of 84 companies joined to develop Android as an open and free mobile platform. Members include Dell, Google, Intel, Motorola, Nvidia, Qualcom, Sony, Sprint, T-Mobile. The member companies agreed to produce compatible devices.
  - 2008 First Android Device was T-mobile G1, complete with fold out QUERTY keyboard.
  - 2011 Apple sues Android device manufacturer Samsung, for patent infringment. This resulted in a 1 billion dollar settlement, which was reduced on appeal. The court battle was finally settled in 2018.
  - 2019 Currently there are more than 2 billion Android devices in use, more than more than 4,000 different devices, and more than 400 different manufacturers.

Mobile Computing

Mobile Computing is a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link. The main concept involves −

- Mobile communication
- Mobile hardware
- Mobile software

Mobile communication

The mobile communication in this case, refers to the infrastructure put in place to ensure that seamless and reliable communication goes on. These would include devices such as protocols, services, bandwidth, and portals necessary to facilitate and support the stated services. The data format is also defined at this stage. This ensures that there is no collision with other existing systems which offer the same service.

Since the media is unguided/unbounded, the overlaying infrastructure is basically radio wave-oriented. That is, the signals are carried over the air to intended devices that are capable of receiving and sending similar kinds of signals.

Mobile Hardware

Mobile hardware includes mobile devices or device components that receive or access the service of mobility. They would range from portable laptops, smartphones, tablet Pc's, Personal Digital Assistants.

These devices will have a receptor medium that is capable of sensing and receiving signals. These devices are configured to operate in full- duplex, whereby they are capable of sending and receiving signals at the same time. They don't have to wait until one device has finished communicating for the other device to initiate communications.

Above mentioned devices use an existing and established network to operate on. In most cases, it would be a wireless network.

Mobile software

Mobile software is the actual program that runs on the mobile hardware. It deals with the characteristics and requirements of mobile applications. This is the engine of the mobile device. In other terms, it is the operating system of the appliance. It's the essential component that operates the mobile device.

Since portability is the main factor, this type of computing ensures that users are not tied or pinned to a single physical location, but are able to operate from anywhere. It incorporates all aspects of wireless communications.

Threat and Security Issues in Mobile Computing

General Security Issues

There are mainly five fundamental goals of security used in the information system to deal with security issues. They are:

Confidentiality

This is used to prevent unauthorized users from gaining access to any particular user's critical and confidential information.

Integrity

This is used to ensure that any type of unauthorized modification, destruction or creation of information cannot be done.

Availability

The availability is used to ensure that authorized users get the required access whenever they need it.

Legitimate

This is used to ensure that only authorized, and legitimate users have access to the services.

Accountability

Accountability is used to ensure that the users will be responsible for their security-related activities by arranging the users and their activities in a linked form. We have to achieve these goals according to the security policy used by the service providers.

Wireless Security Issues

Wireless security issues are considered as the primary security issues of mobile computing. These are related to wireless networks. These issues occur when the hackers intercept the radio signals. Most wireless networks are dependent on other private networks, which are managed by others, so after these issues, the users have less control of security procedures. These security issues are:

Denial of Service (DOS) attacks

The denial of services or DOS attacks is one of the most common attacks of all kinds of networks and especially in a wireless network. It prevents users from using network services because the attacker sends a large amount of unnecessary data or connection requests to the communication server. It causes a slow network, and therefore the users cannot get benefitted from using its service.

Traffic Analysis

Traffic analysis is used to identify and monitor communication between users. In this process, the service provider listens the traffic flowing in the wireless channel to access the private information of users affected by the attacker.

Eavesdropping

It specifies that the attacker can log on to the wireless network and access sensitive data if the wireless network was not secure enough. This can also be done if the information is not encrypted.

Session Interception and Messages Modification

It specifies that the attacker can intercept the session and modify the transmitted data in this session. This scenario is called "man in the middle." It inserts the attacker's host between the sender and receiver host.

Spoofing

In this security issue, the attacker impersonates him as an authorized account of another user and tries to access the sensitive data and unauthorized services.

Captured and Retransmitted Messages

In this security issue, the attacker can get some of the network services by getting unauthorized access. After capturing the message, he/she can reply to it with some modifications to the same destination or another.

Device Security Issues

Mobile devices are very prone to new types of security attacks and fraud issues. These issues are not only because of the mobile devices' vulnerability but also because of the sensitive data that the mobile devices have stored. These security issues and threats such as Virus, Spyware and Trojan may damage or destroy the mobile devices and steal the information stored on them. A virus is a part of malicious software or spyware that tends to gather information about the user without his/her knowledge.

Following is a list of some mobile computing security issues we face using mobile devices:

Push Attacks

In the push attack, the attacker creates a malicious code at the user's mobile device by hacking it and then he/she may spread it to affect other elements of the network.

Pull Attacks

The pull attack is a type of attack where the attacker controls the device and handles it in his/her way. He can decide which emails they want to receive. In this attack, the user can decide about the obtained data by the device itself.

Forced De-authentication

In this security issue, the attackers convince the mobile end-point or the mobile user to drop its connection and re-connection to get a new signal. Within this process, they insert their device between the mobile device and the network and steal the information or do the fraud.

Multi-protocol Communication

The multi-protocol communication provides the ability of many mobile devices to operate using multiple protocols. For example, a cellular provider's network protocol. Most of the protocols have some security loopholes, which help the attacker to exploit this weakness and access to the device.

Mobility

This security issue may occur because of the mobility of the users and the mobile devices. You may face these security threats due to a user's location, so you must replicate the user profiles at different locations to allow roaming via different places without any concern regarding access to personal and sensitive data in any place and at any time. This repetition of sensitive data on different sites can increase seethe chances of security threats.

Disconnections

These types of security issues occur when mobile devices go to different places. It occurs in the form of frequent disconnections caused by external parties resulting in the handoff.

Personnel security issues or insider attacks

These are the non-technical attacks. They are occurred due to the lack of awareness of security policies. Due to this reason, many times, security breaches occur. Even though corporate has standard policies for mobile device security, many employees don't understand its risks. It is found in a study that most of the security risks and threats (almost 72%) occur because of careless employees than hackers (28%). It shows the importance of implementing a strong combination of technology and security awareness within an organization.

How to handle security issues?

The biggest issue in mobile computing is the credential verification of users. Because the users share the username and passwords, it may become a significant threat to security. Due to this sensitive issue, most companies are very reluctant to implement mobile computing. Some recommendations can be followed by companies or mobile users to keep their mobile devices and the data stored in the devices secure.

The company should hire qualified personnel.

- You should install security hardware and software.
- You should ensure that the data stored in the mobile devices are encrypted and audited.
- Educate the users on proper mobile computing ethics and security issues.
- You must ensure that the mobile devices are configured with a power-on authentication to prevent unauthorized access if lost or stolen.
- You must ensure that anti-virus software is installed on mobile devices.
- Make sure that the firewall client is installed on mobile devices.
- Make your mobile devices encrypted with a strong password.
- Encrypt your data stored in the secondary storage devices such as Memory Sticks, Data card, removable USB etc.
- Ensure that the Bluetooth, Wi-Fi, etc. enabled mobile devices are turned off when you are not using them.
- Make periodic backups of your mobile devices on a data server.

Characteristics of Mobile Computing

1. Portability - The Ability to move a device within a learning environment or to different environments with ease.

2. Social Interactivity - The ability to share data and collaboration between users.

3. Context Sensitivity - The ability to gather and respond to real or simulated data unique to a current location, environment, or time.

4. Connectivity - The ability to be digitally connected for the purpose of communication of data in any environment.

5. Individual - The ability to use the technology to provide scaffolding on difficult activities and lesson customization for individual learners.

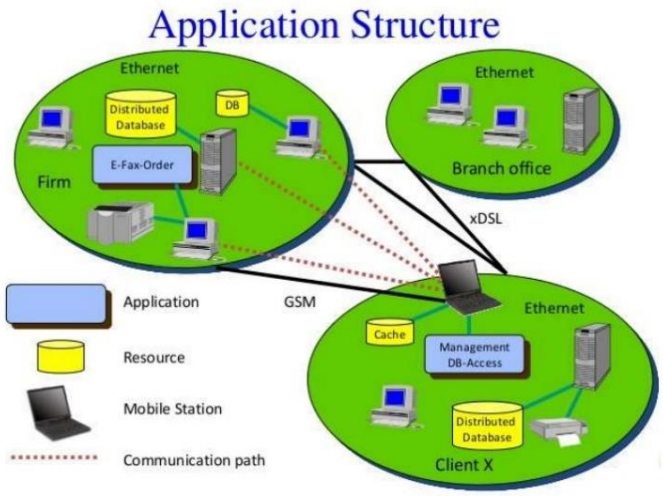
6. Small Size - Mobile devices are also known as handhelds, palmtops and smart phones due to their roughly phone-like dimensions. A typical mobile device will fit in the average adult's hand or pocket. Some mobile devices may fold or slide from a compact, portable mode to a slightly larger size, revealing built-in keyboards or larger screens. Mobile devices make use of touch screens and small keypads to receive input, maintaining their small size and independence from external interface devices. The standard form of a mobile device allows the user to operate it with one hand, holding the device in the palm or fingers while executing its functions with the thumb.

Netbooks and small tablet computers are sometimes mistaken for true mobile devices, based on their similarity in form and function, but if the device's size prohibits one-handed operation or hinders portability, then it cannot be considered a true mobile device.

7. Wireless Communication - Mobile devices are typically capable of communication with other similar devices, with stationary computers and systems, with networks and portable phones. Base mobile devices are capable of accessing the Internet through Bluetooth or Wi-Fi networks, and many models are equipped to access cell phone and wireless data networks as well. Email and texting are standard ways of communicating with mobile devices, although many are also capable of telephony, and some specialized mobile devices, such as RFID and barcode.

Structure of Mobile Computing Application

Programming languages are used for mobile system software. Operating system functions to run the software components onto the hardware. Middleware components deployment. Layered structure arrangement of mobile computing components is used. Protocols and layers are used for transmission and reception.



Programming Languages

The following are the programming languages used for Mobile Computing applications are:

- Java - J2SE.
- J2ME (Java2 Micro edition)
- JavaCard (Java for smart card)
- The Java enterprise edition (J2EE) used for web and enterprise server based applications of mobile services
- C and C++
- Visual C++
- Visual Basic

Operating System

Symbian OS, Window CE, Mac OS are the operating systems used in Mobile computing applications. It offers the user to run an application without considering the hardware specifications and functionalities. It provides functions which are used for scheduling the multiple tasks in a system.

It provides the functions required for the synchronization of multiple tasks in the system. It uses multiple threads synchronization and priority allocation. Management functions (such as creation, activation, deletion, suspension, and delay) are used for tasks and memory. It provides Interfaces for communication between software components at the application layer, middleware layers, and hardware devices.

It facilitates the execution of software components on diversified hardware. It provides Configurable libraries for the GUI (graphic user interface) in the device. It provides User application‘s GUIs, VUI (voice user interface) components, and phone API. It provides the device drivers for the keyboard, display, USB, and other devices.

Middleware

Software components that link the application components with the network-distributed components. It is used to discover the nearby device such as Bluetooth. It is used to discover the nearby hot spot for achieving device synchronization with the server or an enterprise server. It is used for retrieving data (which may be in Oracle or DB2) from a network database. It is used for service discovery at network. It is used for adaptation of the application to the platform and service availability.

Architecture of Mobile Computing Applications

Client/server architecture (and its variants) is often adopted for this kind of applications. However we have to take into consideration some specific aspects related to the mobile devices (clients), and their connectivity with servers.

Clients

There are many mobile device types, including RIM (Remote Infrastructure Management) devices, cellular telephones, PDAs, Tablet, PCs, and Laptop PCs. These mobile devices can typically operate as thin clients or fat clients, or they can be developed so that they can host web pages.

Thin Clients

Thin clients have no custom application code and completely rely on the server for their functionality. They do not depend as heavily on the mobile device‘s operating system or the mobile device type as fat clients. Thin clients typically use widely available web and Wireless Application Protocol (WAP) browsers to display the application content pages.

Fat Clients

A **thick client** (sometimes called a **fat client**) is a form of **client**-server architecture. Specifically, it is a networked **computer** system with most resources installed locally, rather than distributed over a network.

Fat clients typically have one to three layers of application code on them and can operate independently from a server for some period of time. Typically, fat clients are most useful in situations where communication between a client and server cannot be guaranteed.

For example, a fat client application may be able to accept user input and store data in a local database until connectivity with the server is re-established and the data can be moved to the server.

Frequency Scarcity Problem

If we use dedicated RF loop for every subscriber, we need larger bandwidth to serve even a limited number of subscribers in a single city.

Example

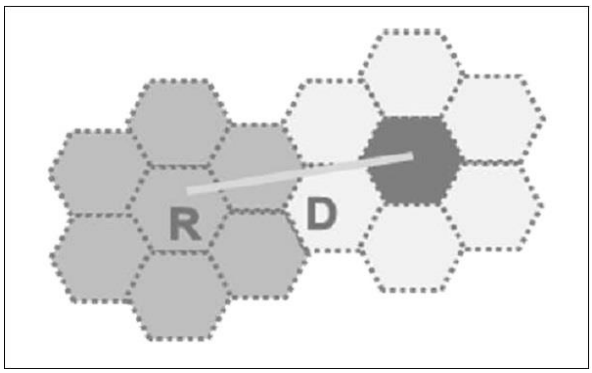
A single RF loop requires 50 kHz B/W; then for one lakh subscribers will need 1,00,000 x 50 kHz = 5 GHz.

To overcome this B/W problem, subscribers have to share the RF (radio frequency) channels on need basis, instead of dedicated RF loops. This can be achieved by using multiple access methods FDMA(Frequency Division Multiple Access), TDMA(Time-division multiple access), or CDMA(Code-division multiple access). Even then the number of RF channels required to serve the subscribers, works out to be impracticable.

Cellular Approach

With limited frequency resource, cellular principle can serve thousands of subscribers at an affordable cost. In a cellular network, total area is subdivided into smaller areas called "cells". Each cell can cover a limited number of mobile subscribers within its boundaries. Each cell can have a base station with a number of RF channels.

Frequencies used in a given cell area will be simultaneously reused at a different cell which is geographically separated. For example, a typical seven-cell pattern can be considered.



Total available frequency resources are divided into seven parts, each part consisting of a number of radio channels and allocated to a cell site. In a group of 7 cells, available frequency spectrum is consumed totally. The same seven sets of frequency can be used after certain distance.

The group of cells where the available frequency spectrum is totally consumed is called a cluster of cells.

Two cells having the same number in the adjacent cluster, use the same set of RF channels and hence are termed as "Co-channel cells". The distance between the cells using the same frequency should be sufficient to keep the co-channel (co-chl) interference to an acceptable level. Hence, the cellular systems are limited by Co-channel interference.

Hence a cellular principle enables the following.

- More efficient usage of available limited RF source.
- Manufacturing of every piece of subscriber's terminal within a region with the same set of channels so that any mobile can be used anywhere within the region.

Shape of Cells

For analytical purposes a "Hexagon" cell is preferred due to the following reasons.

- A hexagon layout requires fewer cells to cover a given area. Hence, it envisages fewer base stations and minimum capital investment.
- Other geometrical shapes cannot effectively do this. For example, if circular shaped cells are there, then there will be overlapping of cells.
- Also for a given area, among square, triangle and hexagon, radius of a hexagon will be the maximum which is needed for weaker mobiles.

In reality cells are not hexagonal but irregular in shape, determined by factors like propagation of radio waves over the terrain, obstacles, and other geographical constraints. Complex computer programs are required to divide an area into cells. One such program is "Tornado" from Siemens.

Operating Environment

Due to mobility, the radio signals between a base station and mobile terminals undergo a variety of alterations as they travel from transmitter to receiver, even within the same cell. These changes are due to −

- Physical separation of transmitter and receiver.
- Physical environment of the path i.e. terrain, buildings, and other obstacles.

Slow Fading

- In free space conditions (or) LOS, RF signal propagation constant is considered as two i.e. r = 2. This is applicable for static radio systems.
- In mobile environment, these variations are appreciable and normally 'r' is taken as 3 to 4.

Rayleigh Fading

The direct line of sight in mobile environment, between base station and the mobile is not ensured and the signal received at the receiver is the sum of a number of signals reaching through different paths (multipath). Multipath propagation of RF waves is due to the reflection of RF energy from a hill, building, truck, or aero plane etc.; the reflected energy undergoes a phase change also.

If there are 180 out-of phase with direct path signals, they tend to cancel out each other. So the multipath signals tend to reduce the signal strength. Depending upon the location of the transmitter and receiver and various reflecting obstacles along the path length, signal fluctuates. The fluctuations occur fast and it is known as "Rayleigh fading".

In addition, multipath propagation leads to “pulse widening” and “Inter symbol Interference”.

Doppler Effect

Due to the mobility of the subscriber, a change occurs in the frequency of the received RF signals. Cellular mobile systems use following techniques to counter these problems.

- Channel coding
- Interleaving
- Equalization
- Rake receivers
- Slow frequency hopping
- Antennae diversity

Co-Channel Interference and Cell Separation

We assume a cellular system having a cell radius “R” and Co-channel distance “D” and the cluster size “N”. Since the cell size is fixed, co-channel interference will be independent of power.

Co-chl interference is a function of Q = D/R.

Q = Co-chl interference reduction factor.

Higher value of “Q” means less interference.

Lower value of “Q” means high interference.

“Q” is also related to cluster size (N) as Q = 3N

Qh = 3N = D/R

For different values of N, q is −

N = 1 3 4 7 9 12 Q = 1.73 3 3.46 4.58 5.20 6.00

Higher values of “q”

- Reduces co-channel interference,
- Leads to higher value of “N” more cells/cluster,
- Less number of channels/cells,
- Less traffic handling capacity.

Lower values of “q”

- Increases co-channel interference.
- Leads to lower value of “n” fewer cells / cluster.
- More number of channels / cells.
- More traffic handling capacity.

Generally, N = 4, 7, 12.

C/I Calculations and 'q'

The value of "q" also depends on C/I. "C" is the received carrier power from the desired transmitter and "I" is the co-channel interference received from all the interfering cells. For a seven-cell reuse pattern, the number of co-channel interfering cells shall be six in number.

I = m2b $\sum$ Mz1 I_m

Loss of signal is proportional to (distance) –r

R – Propagation constant.

c α R-r

R = Radius of cell.

I α 6 D-r

D= Co-channel separation distance

C/I = R – r / 6D –r = 1/6 × Dr / Rr = 1/6 (D/R) r

C/I = 1/6 q r since q = D/R and q r = 6 C/I

Q = [6 × C/I]1/r

Based upon the acceptable voice quality, the value of C/I has been found to be equal to 18 dB.

Assuming,

- A seven-cell reuse pattern
- Omni directional antennae

Value of 'q' can be typically around 4.6.

Value r is taken as 3.

This is an ideal condition, considering the distance of the mobile units from the interfering cells to be uniformly equal to 'D' in all cases. But practically mobile moves and distance 'D' reduces to 'D-R' when it reaches the boundary of the cell, and C/I drops to 14.47 dB.

Hence 'freq' reuse pattern of 7 is not meeting C/I criteria with omni directional antennae.

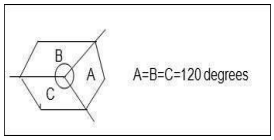
If N = 9 (or) 12,

N = 9q = 5.2C/I = 19.78 dB

N = 12q = 6.0C/I = 22.54 dB

Hence, either 9 or 12 cell pattern is to be with omni directional antennae, but traffic handling capacity is reduced. Hence they are not preferred.

In order to use N = 7 (or lower), directional antennas are used in every cell site. A cell having 3 sectors is very popular and will be like the figure shown below.



Antenna's font – back coupling phenomenon reduces number of potential interferers.

For example if N = 7.

With omni directional antennae, number of interfering cells shall be six. With directional antennae & 3 sectors the same is reduced to two. For N = 7 and three sectors, the C/I improves from 14.47 dB to 24.5 dB even in worst conditions. Then C/I meets the requirement of 18dB. For N = 7 and six sectors, the C/I improves to 29 dB.

For Urban applications, N = 4 and a three sector cell is used so that more number of carriers per cell are obtained than N = 7. Also the C/I becomes 20 dB in worst cases.

DAMPS Uses 7/21 cell pattern

GSM Uses 4/21 cell pattern

Advantages of sectoring

- Decrease co-channel interference
- Increase system capacity

Disadvantages of sectoring

- Large number of antennas at the base station.
- Increase in the number of sectors/cell reduces the trunking efficiency
- Sectoring reduces the coverage area, for a particular group of channels.
- Number of 'Hand offs' increases.

Hand Off

When the mobile unit travels along a path it crosses different cells. Each time it enters into a different cell associated with f = different frequency, control of the mobile is taken over by the other base station. This is known as 'Hand off'.

Hand off is decided based on −

- Received signal strength information if it is below a threshold value.
- Carrier to interference ratio is less than 18 dB.

Adjacent Channel Interference

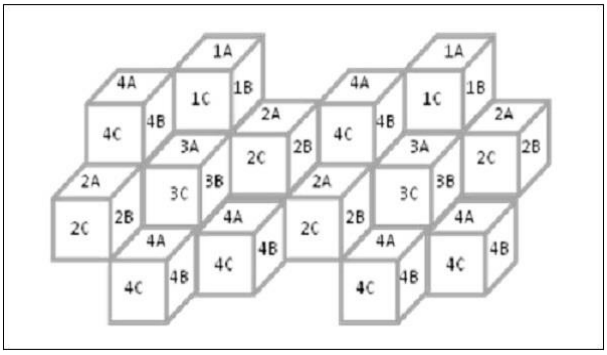
A given cell/sector uses a number of RF channels. Because of imperfect receiver filters, which allow nearby frequencies to leak into pass band, adjacent channel interference takes place.

It can be reduced by keeping the frequency separations between each RF channel in a given cell as large as possible. When the reuse factor is small, this separation may not be sufficient.

A channel separation, by selecting RF frequencies, which are more than 6 channels apart, is sufficient to keep adjacent channel interferences within limits.

For example, in GSM which follows 4/12 pattern, N = 4

Sectors = 3/cell



IA will use RF Carr. 1, 13, 25,……..

IB will use RF Carr 5, 17, 29,……

IC will use RF Carr. 9, 21, 33,…….. and so on.

Trunking

Cellular radios rely on trunking to accommodate a large number of users in a limited radio spectrum. Each user is allocated a channel on need/per call basis and on termination of the cell, the channel is returned to the common pool of RF channels.

Grade of Service (GOS)

Because of trunking, there is a likelihood that a call is blocked if all the RF channels are engaged. This is called 'Grade of Service' "GOS".

Cellular designer estimates the maximum required capacity and allocates the proper number of RF channels, in order to meet the GOS. For these calculations, 'ERLANG B' table is used.

Cell Splitting

When the number of users reaches a saturation in a start-up cell (initial design) and no more spare frequency is available, then the start-up cell is split, usually in four smaller cells and traffic increases by four and more number of subscribers can be served.

After 'n' splits, the traffic will be −

$T2 = T0 \times 42$

Power will be reduced −

$P2 = P0 – n \times 12$ db

Hence cell splitting improves the capacity and lowers the transmission power.