CIT 3101 Mobile Computing Lecture Notes

Bachelor of Science in Information Technology (Dedan Kimathi University of Technology)

0078

CIT 3101 MOBILE COMPUTING

COURSE OUTLINE

Facilitator: Mr. Michael Kamau, *Email*:mmicckama@gmail.com

Prerequisite: Computer Networks, Object Oriented Programming II(Java)

Main Goal	This course introduces us to the theory and practice of Mobile Computing systems. It helps us to understand the technical concerns of mobile computing environments and what mobile developers face regardless of the platform.
Objectives/ Learning outcomes	At the end of the course, students should: [1]. Acquire basic knowledge about mobile computing environment and platforms [2]. To understand mobile communication protocols and technologies [3]. To learn the standards of Mobile Communication [4]. To learn Applications of Mobile Computing [5]. Work with the J2ME and J2EE platforms

Course Content

TIME	TOPICS	REF
Week 1	**Introduction**: Overview of the various mobile computing, paradigms, devices, software and applications	
Week 2	**Fundamentals of Wireless Communication**: Introduction, Wireless transmission, Principles of Wireless Transmission.	
Week 3	Wireless mobile Networks and Mobility Management	
Week 4	Mobile Communication protocols/standards	
Week 5	CAT ONE	
Week 6	Mobile Computing Architecture and Frameworks Development Tools	
Week 7	Wireless communication Technologies in mobile computing: MobileIP	
Week 8	Wireless communication Technologies in mobile computing: CDPD and SMS	
Week 9	Mobile Communication Technologies and Services: GSM, GPRS	
Week 10	CAT TWO	
Week 11	Mobile Communication Technologies and Services: VoIP and Satellite Communication	
Week12	Wireless Application Protocol and WAP environment	
Week 13	XML: Document and Meta-Data format for mobile computing	
Week 14	Mobile and Wireless networks Security	
Week 15	FINAL EXAM	

Lectures:	3 Hours per week (2 hrs Theory and 1 hr Discussions)
Delivery methods	Lectures, group and individual assignments, interactive tutorials, presentations and demonstrations.
Learning Materials	A computer , Facilitators Notes/Handout, Projector & a Whiteboard.

Course Text Books:

1. **Mobile Computing Principles: Designing and developing mobile applications By Reza B' Far**
2. Hansmann, Merk, Nicklous, Stober, Principles of Mobile Computing.
3. Raj Kamal, Mobile Computing, Oxford University Press, 2007

Reference Textbooks:

4. Mark Beaulieu, (2002), *Wireless Internet Applications & Architectures: Building Professional Wireless Applications Worldwide,* Addison-Wesley,
5. Frank Adelstein, Sandeep K.S. Gupta ”Fundamentals of Mobile and Pervasive Computing ”,Tata McGraw-Hill
6. Ivan Stojmeniovic – Handbook of Wireless Networks and Mobile Computing
7. Andrew Tanenbaum – Computer Networks
8. Introduction to J2ME and J2EE platforms

Useful Links

1. https://www.wisdomjobs.com/e-university/mobile-computing-interview-questions.html
2. https://www.wisdomjobs.com/e-university/mobile-security-tutorial-1463.html

Methods of course assessment:

Assignments	10%
Continuous assessment test s	20%
End of semester examination	70%
Total	100%

Note: Late submissions and Plagiarized work leads to penalties and cancellations

LESSON 1

INTRODUCTION TO MOBILE TECHNOLOGY

Overview of the various mobile computing, applications and devices

Basics of mobile computing: Def: **Mobile computing refers to the use of small and portable computing devices** in wireless enabled networks that perform computation tasks.
Mobile computing describes technologies that :

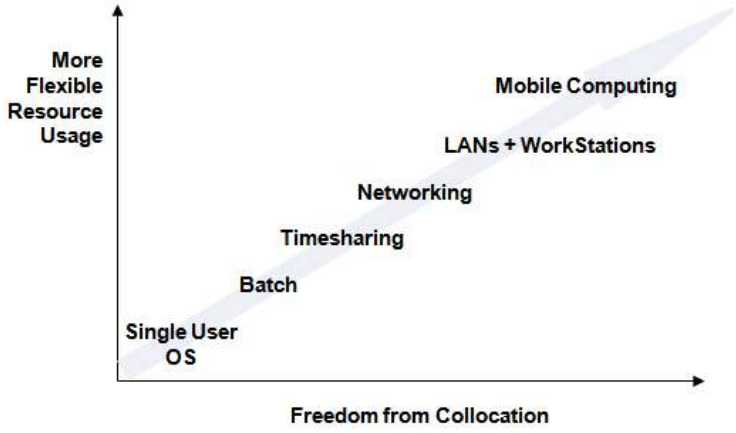
- enable people to access network services anyplace, and anytime,
- with portable and wireless computing and communication enabled devices.

Some other names:

- Pervasive computing/ Ubiquitous computing - computing everywhere
- Wireless computing

Ubiquitous computing (sometimes ubiqcomp) integrates computation into the environment, rather than having computers which are distinct objects.

Natural evolution of computing



Mobile Computing 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. It consists of the hardware devices, the software and communication parts.

Def: A **mobile device** refers to an electronic device that can move or be moved from place to place with ease. Basic components in mobile devices include:

digital camera, media players, games, wireless communication receptors, Office suites applications, customized mobile apps, internet browsing functionality & peripheral support for connection with PCs e.g USB connection

Paradigms in mobile computing

i. *Low power computing:* Mobile computing brings about a focus on energy efficiency and performance optimization that guarantees reliability just like with other computer devices.

   Mobile technologies and designs squeeze more powerful performance into ever-smaller devices which consequently boost battery life, by minimizing the peripheral components that consume power. Smaller designs also reduce heat emitted by parts and the need for cooling fans as power management functions are integrated across the entire design system.

   Mobile designs embody event-based programming whereby, when applications are not directly concerned with events, the CPU is switched off in order to conserve power.

ii. *Computing in an environment with limited resources:* High computing performance brings about the need to use a lot of resources such as memory and power. However mobile computing enables a tradeoff which ensures low power consumption, cool operation, and light weight memory consumption.

   Mobile computing designs have enabled advancement in system integration, processing innovation and idle power management.
   Mobile computing devices can work with low storage e.g. can be run in about 1 MB of memory.

iii. *Fault tolerance and persistence:* Due to the distributed nature of mobile computing design, a service breakdown in one of the node is corrected by services of other functioning nodes.

iv. *Pervasiveness/ubiquity:* Any time any place computing, unlike a desktop in an office.

v. *Varying User Interfaces:* Using a combination of interface types in mobile devices is not uncommon. Examples of some alternative interfaces are voice user interfaces, smaller displays, stylus and other pointing devices, touch-screen displays, and miniature keyboards.

Design Issues and Limitations in Mobile Computing Systems

Unlike desktops, mobile devices use special types of designs, which are scaled to the requirements of their application software, hardware, and peripherals used in them. For example ,these considerations are necessary:

1. Operating systems

2. File systems
3. Database systems
4. Programming Languages
5. Communication architecture and protocols
6. Hardware and architecture
7. Real-Time, multimedia, QoS
8. Security
9. Application requirements and design

Limitations of mobile computing

1. **Resource-poor**
   - Battery packs
   - Hardware: Memory, CPU, peripherals
   - Software – Middleware
   - low bandwidth or bandwidth fluctuation
2. **Less secure**
   - Lost or stolen
   - Devices more vulnerable, endpoint authentication harder
3. **Mobile connectivity**
   - Dynamic changes in environment: infrastructure
   - Reliability: disconnections
4. **Heterogeneous network**
   - Different devices, interfaces and protocols
5. **Need for Location awareness**
   - Locality adaptation during search and handoff

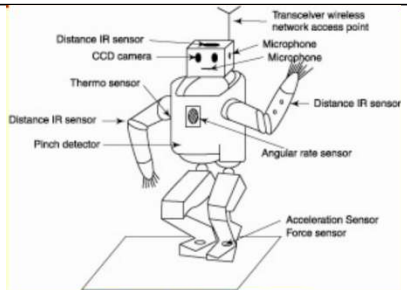
Mobile Hardware and Software

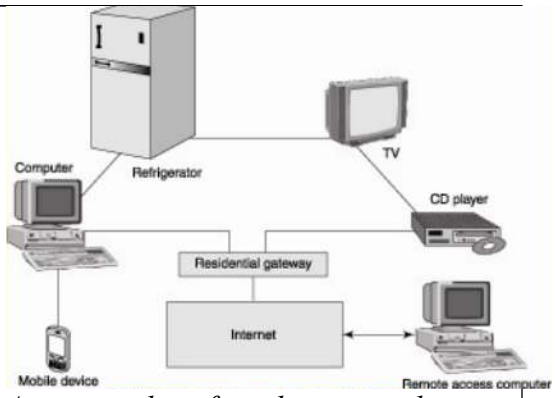
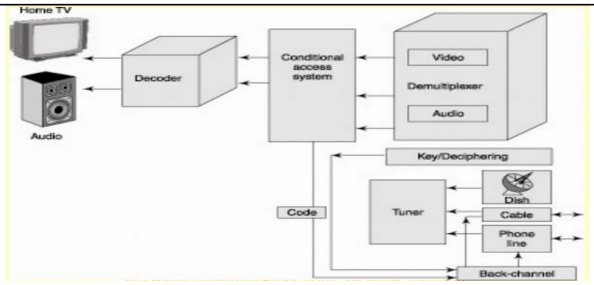
a) Mobile Devices :- These are hardware devices or device components that receive or access the services offered by mobile computing. Basic types of mobile devices range from :

Mobile Phones(smart phones), This is the main device that is best describe the aspect of mobility in mobile computing.	
Laptop computers, Though classified as a personal computers, laptops provide mobility and flexibility of use, unlike traditional desktop computers.	

Tablets, They can be categorized as mini laptops as they provide close functionalities with a laptop; even though at a smaller scale of computation and customization.	
Personal Digital Assistants(PDAs) These can be programmed for customized applications like taking notes for research during field work, reading books..etc.	

Other types of mobile devices include:

Robots In a robotic system or an industrial automation system- multiple smart sensors are embedded in it. Smart sensors consists of the sensing device, processor, memory, analog to digital converter (ADC), signal processing element, wireless or infrared receiver and transmitter.	 *Diagram of a robotic system*
Sensors - devices that sense the physical environment e.g. sensors for temperature, pressure, light, metal, smoke, and proximity to an object. Normally, a sensor sends its signals to a computer or controller i.e. wireless sensors which facilitate interaction of the mobile device with the surrounding environment. ***Actuators-*** devices that receive signals from a controller or central computer and accordingly activates a physical device, appliance, or system. A smart actuator is able to receive the commands or signals from a network, mobile device, computer, or controller and accordingly activates the physical device or system.	

Smart Appliances Home appliances and security systems can be controlled using a cell phone or computer, especially those appliances that are networked using power lines. Signals from these appliances can communicate from one appliance to another, thus forming a network. The devices can also communicate though a central server or network using very short-range wireless protocols, such as Bluetooth.	 *An example of a home appliances network*
Set-top box This is a computer-based device with data, media, and network processing capabilities, which interconnects the home TV and the broadcasting service network. Its mechanism of operation is similar to that of a mobile phone device, where the server of mobile service provider manages and administers the operation of the device.	

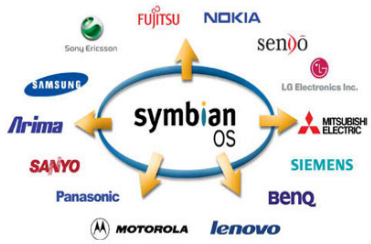
In summary, devices can be categorize into:

Mobile personal Gadjets	laptop, PDA, PocketPC, smartphones, iPad, Tablet
Home electronics:	TV, DVD player, satellite TV set-top boxes, Stereos, iPod, Gameboy/Sony psp/Nintendo DS
Location positioning devices	GPS, MAPs
Automobiles	Embedded systems
Tags	RFIDs, SmartCards
Wearable computing and sensor network	Smart watches

These devices can be characterized as either :

- Fixed and wired, or, Fixed and wireless
- Mobile and Wired ,or, Mobile and Wireless

b) Mobile software-: For the hardware to work, they need the support of mobile software ,just like computer devices. Therefore, mobile software are programs that run on the hardware; which include both the operating systems and the application software.
Mobile operating systems help to start the hardware devices and also to support the functionality of mobile apps. Major Mobile OS software include:

Palm OS, It was initially developed by **Palm**, Inc. It focused in including the functionality of touch screen on mobile devices. http://searchmobilecomputing.techtarget.com/definition/Palm-OS.	
Win CE, Windows Embedded Compact is an Microsoft product that has a hybrid kernel/OS framework. Used in windows phones. It is based on the Microsoft Windows OS which is designed for including or embedding in mobile and other space-constrained devices. It is mainly designed for real-time applications e.g. cable TV set top-boxes. https://msdn.microsoft.com/en-us/library/ms905511.aspx.	
Symbian OS, Was initially developed in Europe by Nokia as an operating system targeting mobile devices .It was initially the base support for communication in primitive mobile devices, but later was improved to support user interaction using smart phones. http://www.symbianos.org/. Symbian OS	
Android OS, The OS is open source which is mostly developed and maintained by Google. This is one of the latest and the most improved OS which runs on smart-phones, watches, cars and TVs. It comes with full user interaction and the latest mobile communication technologies.	
Linux OS for Mobile Devices, Linux can be modified easily to suit different sorts of hardware and software applications. Being an open source OS, it enables the user to customize their device to suit their specific needs.	

To do (students):

[1]. Find out other types of mobile OS e.g. those that support iPhones and other popular smart-phone brands.

[2]. State two unique features in every device and mobileOS

Applications of Mobile Computing

To do:- (Add brief notes on each of these applications)

[1]. Emergency news reporting

- Early transmission of patient data to the hospital, current status, first diagnosis
- Provide mobile infrastructure in dealing with Natural Disaster (earthquake, hurricane, fire), terrorist attacks, war, ...

[2]. Vehicles

- transmission of news, road condition, weather, music via DAB
- personal communication using GSM
- position via GPS
- local ad-hoc network with vehicles close-by to prevent accidents, guidance system, redundancy
- vehicle data (e.g., from busses, high-speed trains) can be transmitted in advance for maintenance

[3]. E-commerce

- Sales representatives are using Tablet PCs with Smart phones for presentation, transmitting/access information among office, hotel, and customer location.

[4]. Industrial
[5]. Home assistance
[6]. Office applications
[7]. Research and information management
[8]. Security
[9]. Banking and finance
[10]. Education
[11]. Taxation/dispatch
[12]. Electronic mail and web access
[13]. Communication and social networking i.e. Mobile Internet Access
[14]. Mobile Multimedia Entertainment
[15]. Medical and fitness i.e. healthcare
[16]. Personal records keeping
[17]. Weather and environment management

LESSON 2

FUNDAMENTALS OF WIRELESS COMMUNICATION

Wireless Transmission

Communication is :- a two-way transmission and reception of data streams i.e. two or more communicating devices where the transmitter sends the signals and received by receivers.

Fig( )A general signal transmission model

Commu nication issues include ad hoc infrastructure networks as well as communication properties like: **protocols, data formats and concrete technologies**.

Therefore, Mobile communication entails transmission of data to and from communicating devices, whereby at least one of the device is mobile which is remotely located.

Limitations of the Wireless Communication

1) Heterogeneity of fragmented networks
2) Frequent disconnections due to interference
3) Limited communication bandwidth
4) Limitations Imposed by Mobility e.g. need for large delay variation
5) Limitations of the Mobile Computer
6) Regulations and spectrum
7) Lower security, simpler to attack

Wireless Media: Wireless Communication uses Unguided media for transmission i.e.
This one does not require a physical conduit for data to be transmitted. Since mobile device depend on mobility, this is the most convenient form of transmission .In this form of transmission electrical signals are transmitted by converting them into electromagnetic radiation. The radiation transmitted via antennae that radiates electromagnetic signals.

Improvement from wired communication systems led to development of wireless communication medium where there is no need of a physical conduit to propagate data signals from sender to receiver, who are geographically separated. Therefore, Wireless systems operate via transmission through space, other than through physical connections.

We can sometimes call wireless communication, mobile communication as it also involves motion of transmitter and receiver. Two major issues involved in this mode of communication are:

i. Communication channel often varies with time and frequency.

ii. There is always interference between multiple service users.

Frequencies for wireless transmission

We have various signal frequency bands within the electromagnetic spectrum, whereby a frequency of a signal is measured by;

- $f=c/\lambda= (300/\lambda)$
- Frequency, f is measured in MHz
- wavelength, λ in meter
- the velocity of signal propagation, $c = 300 \times 10^6$ m/s for electromagnetic waves in air.

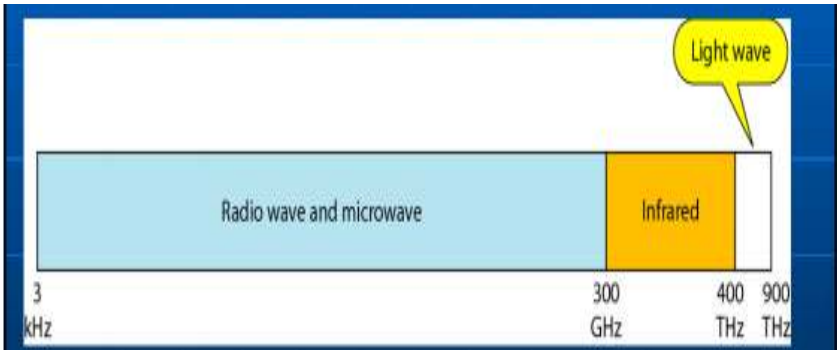


Fig: Electromagnetic spectrum for wireless communication

To do:

1) Read about ranges of Frequencies and Wavelengths allocations
2) Read About the History of Wireless Communication

Antennaes and Signal Propagation

Antennae/Wireless Receptor: An antennae is a peripheral device that transmits and receives electromagnetic signals. The forms of antennae are mainly determined by the frequency ranges they operate in and can vary from a single piece of wire to a parabolic dish.

Fig( ) forms/types of antennaes

An antenna is normally tuned to the frequency band in which the transmitting system connected to it operates. Its size is inversely proportional to the frequencies of transmitted signals.

Mobile devices are manufactured with a receptor medium that is capable of sensing and receiving network signals in full-duplex mode i.e. are capable of sending and receiving signals at the same time. To do so, they need to use an established communication network to operate

on; which is provided/supported by the various existing communication technologies i.e. wireless.

Wireless Signal: Signals are physical representation of data i.e. functions of time and location. Users of wireless communication systems can only exchange data through transmission of signals. Signals, therefore refer to voice, data, or multimedia packet streams, which are received by a receptor.

Factors that determine the quality of communication

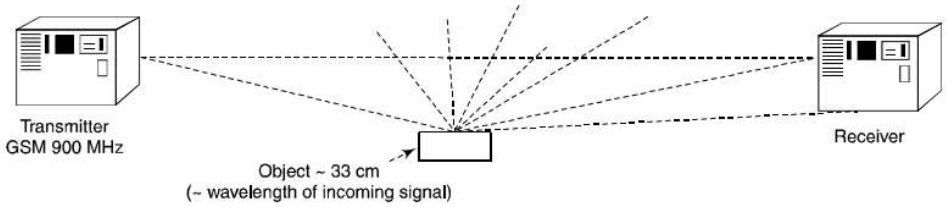
Current researches are currently focusing on developing schemes that would lead to improvement on the quality, capacity and efficiency of wireless systems.

During signal transmission, several factors can determine the quality of communication, namely:

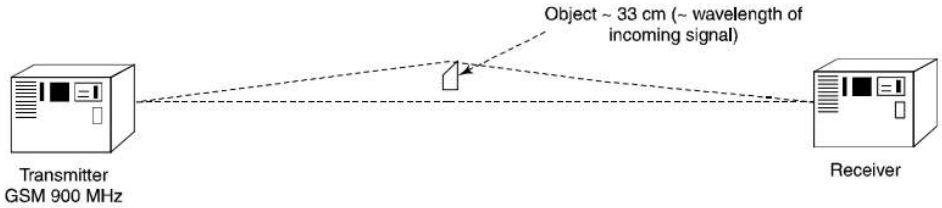
1. **Line-of-sight propagation.** This is the ideal transmission of signals, without refraction, diffraction, or scattering in between the transmitter and the receiver, but losses do occur.

2. **Attenuation.** When obstacles are greater in size than signal wavelength, the strength of the signal decreases e.g. A GSM 900 MHz ($\lambda >= 33$ cm) signal, will face attenuation in objects of size > 1 m (>> λ~33cm).

3. **Scattering.** When obstacle size is equal to or less than wavelength. This decreases signal strength greatly e.g. A GSM signal, about 33 cm in wavelength, scattered by an object of 30 cm or less makes only a small part of the scattered signal to reach the receiver.

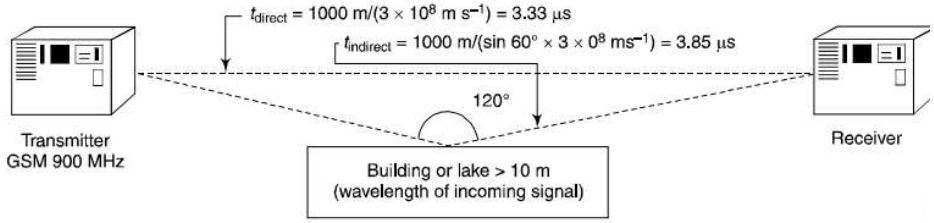


4. **Diffraction**. A signal bends from the edges of an obstacle of size equal to or less than the wavelength e.g. A GSM signal of wavelength 33 cm will diffract from an object of 33 cm or less causing it to or not to reach its destination.



5. **Reflection.** A signal may also be reflected from the surface of an obstacle, or the earth's surface e.g. A GSM 900 MHz (λ= 33 cm) signal the transmitter signal reflects from an object of size 10 m and above (much greater than λ)

The reflected signal suffers a delay in reaching its destination or a distortion of the waveforms which causes misrepresentation of information encoded in the signal.



Principles for wireless networks communication

Our focus is on three main principles namely:

a) wireless channels & Signals
b) modulation
c) multiplexing

a.) Wireless channels and Signal Transmission

Wireless medium is a much more difficult medium than wired network. The spectrum available for cellular systems is quite limited , the interference level is quite high and rapid growth is increasing the level of interference. They operate via electromagnetic radiation from transmitter to receiver. In order to get the electromagnetic field at the receiving antenna, you have to account for the reflections from nearby buildings, vehicles and bodies of land and water. Objects in line of sight between sender and receiver have to be accounted for.

The wavelength **ƛ(f)**of electromagnetic radiation at any given time is given by:

ƛ=c/f, where c=3*10^8m/s is the velocity of light

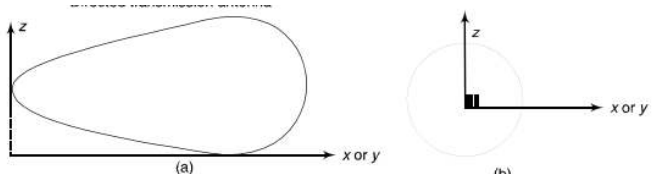
Electromagnetism alone cannot be used to characterize wireless channels in detail, but it provides an underlying nature of these channels. Mobile communication gadgets must operate under a wide variety of conditions. It makes sense to view these conditions probabilistically .

Characteristics of wireless channels

Here we look at **two** general situations:

- **Free space, fixed transmitting and receiving antennas**

Consider a fixed antenna radiating into free space. The electric and magnetic field at any given location *d* are perpendicular to each other and to the direction of propagation from the antenna.



Fig( )radiation pattern in a wireless transmission

The electric field at **d** is, in general a vector with components in the two co-ordinate directions perpendicular to the line of propagation. The electric waveform is usually a pass band waveform modulated around a carrier, and we focus on the complex positive frequency part of the waveform. The explanation for this response is that the receiving antenna only causes local changes in the electric field, and thus alters neither the delay nor the attenuation.

- **Free space, moving antenna**

Continue to assume a fixed antenna transmitting into free space, but now assume that the receiving antenna is moving with constant velocity v in the direction of increasing distance from the transmitting antenna.

The channel is characterized as a linear time-varying channel (LTV).

***Shadowing*:** Shadowing refers to the phenomena of partially blocking wireless signals when partially absorbing materials, such as walls of buildings, lies between the sending and receiving antennas. The attenuation due to shadowing is exponential in the width of a barrier that must be passed through.

Input/output models of wireless channels

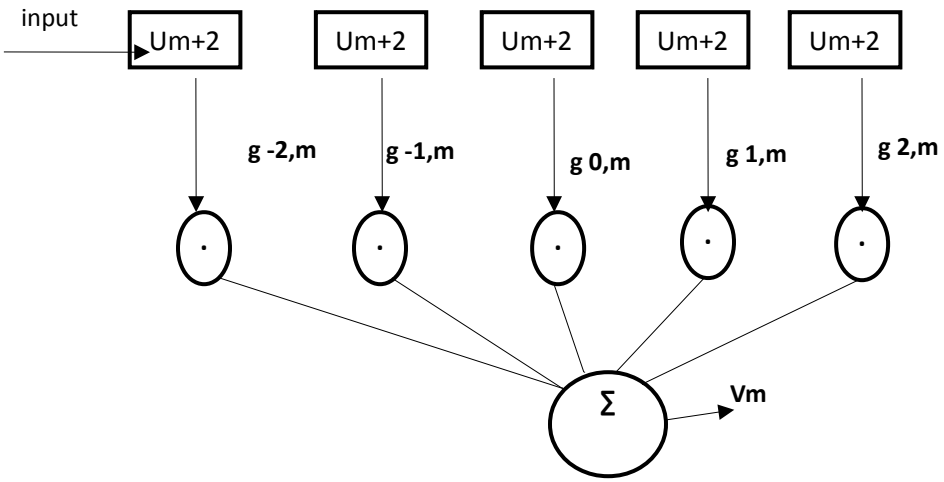
In wireless communication, it is important to focus on modeling input/output behavior of a channel, rather than individual behavior of each signal path. A wireless channel is thus viewed as consisting of an arbitrary collection of J electromagnetic paths as a more abstract input/output model. In physical situations, the important signal paths are accompanied by other insignificant and highly attenuated paths. We in most occasions are required to ignore/omit the insignificant paths.

In a real-life situation a portable receiver moving through the channel experiences a space-varying fading phenomenon. One can therefore associate an impulse response "profile" with each point in space.

2.) A discrete-time baseband model

We use the sampling theorem to convert the continuous-time baseband channel to a discrete-time channel. Using this model each impulse response can be described by a sequence of "0"s and "1"s (the path indicator sequence), where a "1" indicates presence of a path in a given bin and a

"0" represents absence of a path in that bin. To each "1" amplitude and a phase value are associated.



Fig( )A time-varying discrete time baseband channel model.

Each unit of time a new input enters the shift registers and the old values right shift. The channel taps also change, but slowly. If the k^{th} tap is unchanging with m for each k, then the channel is line-time invariant. If each tap changes slowly with m, then the channel is called slowly-time varying**.**

3) Statistical channel models

In wireless communication, physical paths are unknown at the transmitter and receiver. However so, from an input/output viewpoint, it is the tap gains that are of primary interest. Since these tap gains change with time, location, bandwidth, carrier frequency, and other parameters, a statistical characterization of the tap gains is needed in order to understand how to communicate over each of these. Here, each tap gain $\mathbf{g_{k,m}}$ is viewed as a sample value of random variable $\mathbf{G_{k,m}}$.

One reasonable point of view here is that the above models are often poor approximations for individual physical situations, but when averaged over all physical situations that a wireless system must operate over, **they make more sense.** The models provide a number of insights into communication in the presence of fading.

***Data Detection*:-**Detection for wireless channels involves measuring the channel filter taps as they evolve in time, and then using the measured values in decoding data. If the response can be measured accurately, then the detection problem becomes very similar to that of wired channels.

To achieve reliable communication, it is necessary either to have density and/or coding between faded and unfaded parts of the channel, or to use channel measurement and feedback to control the signal power in the presence of fades.

***Diversity* :-** Severe attenuation makes it impossible for the receiver to determine the transmitted signal unless some less-attenuated replica of the transmitted signal is provided to the receiver. This resource is called diversity and it is the single most important contributor to reliable wireless communications.

Diversity is used to reduce error probabilities at the receiver since it refers to rather broad set of techniques.

Multiple physical transmission paths give rise to multi-fading and diversity; the first usually causes difficulties and the second usually adds to those difficulties. In a two tap model, the path outputs are separated into two groups and the effect of each can be observed separately. With one tap model, the paths are all combined, since there are no longer independent observable sets of paths. Many wireless situations, particularly those in cellular and local area networks, contain relatively small number of significant coherent paths.

The diversity receiver can be generalized to other discrete models for wireless channels. For example the frequency band could be separated into segments separated by the coherence frequency, thus getting roughly independent fading in each and the ability to separate the outputs in each of those bands.

Another way to achieve diversity is through multiple antennas at the transmitter and receiver. Multiple antennas at the receiver allow the full received power available at one antenna to be received at each antenna, rather than splitting the power as occurs with time diversity or frequency diversity. For all these more general ways to achieve diversity, the input and output should obviously be represented by the appropriate orthonomal expansions to bring out the diversity terms.

b) Modulation

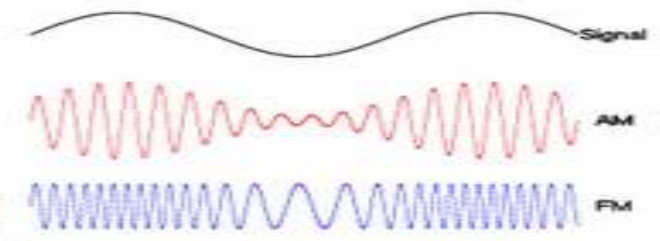
Remember that the antenna size is inversely proportional to the frequencies of transmitted signals, where Low frequency (LF) signals need vary large antennae.

Modulation is the process of varying one signal, called the carrier, according to the pattern provided by another signal (modulating signal).

The carrier usually an analog signal is selected to match the characteristics of a particular transmission system. This increases the compatibility of transmitted signal and transmission medium.

The amplitude, frequency, or phase angle of a carrier wave is varied in proportion to the variation in the amplitude, amplitude, frequency, or phase variation of the modulating wave (message signal).

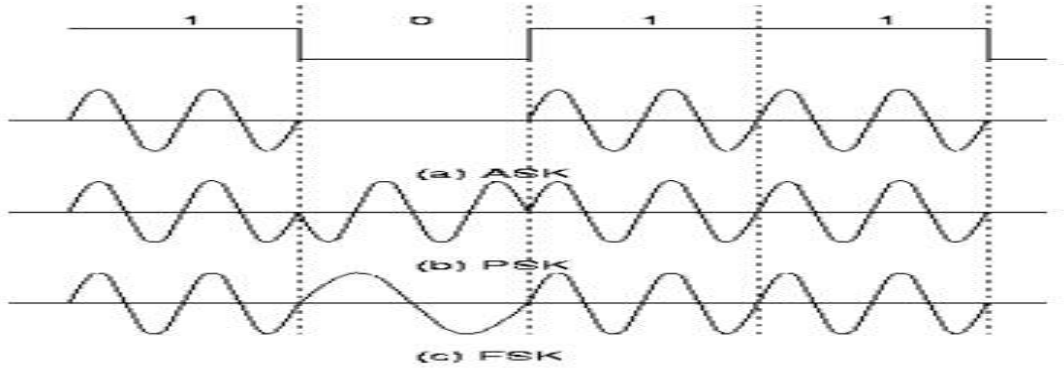
We can call modulation as the instantaneous change of amplitude or frequency i.e.



There are two forms of modulation, namely:

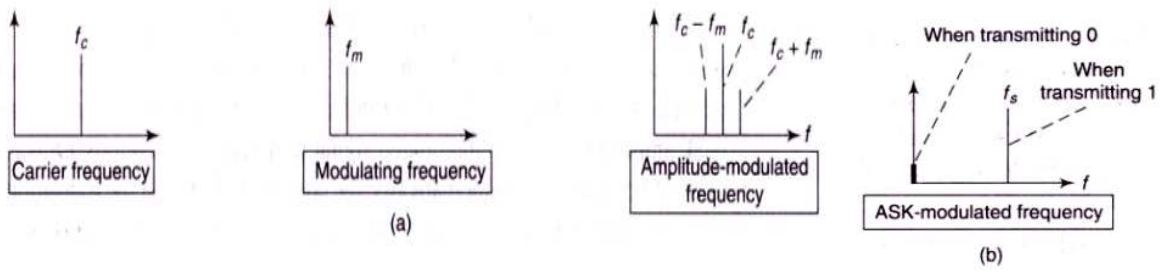
Analog modulation: It is a technique b which the frequency or a set of carrier frequencies are used for wireless transmission such that ,the peak amplitude, frequency, and phase angle varies with time in proportion to the peak amplitude of the modulating signal.

Digital modulation: Here, the amplitude, frequency, or phase angle parameters of carrier or subcarrier frequencies are varied according to the variation in the modulating signal bit (1 or 0), modulating bit-pair: (00, 01, 10 or 11) or set of 4 or more bit

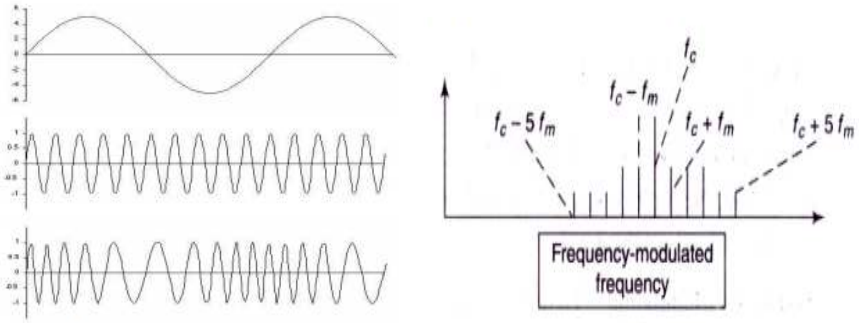


Fig( ) Demonstration of digital modulation

Amplitude shifted keying(ASK):- if as per 1 or 0, amplitude of carrier is varied.

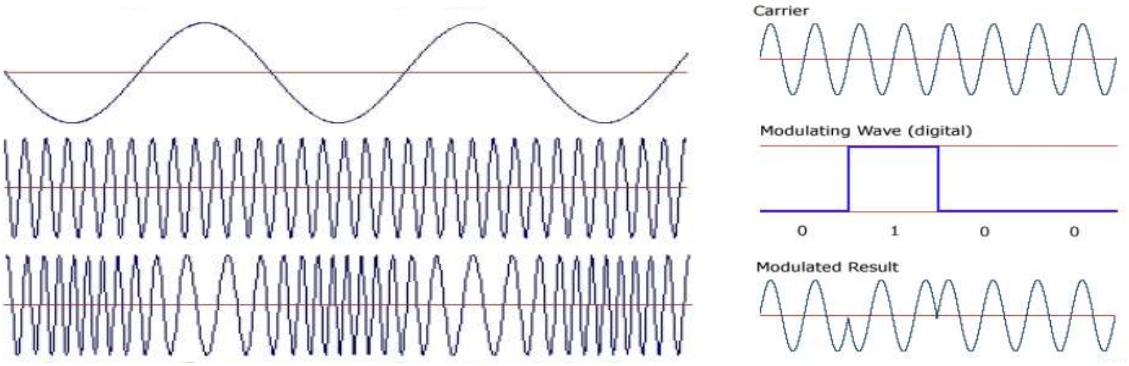


Frequency shifted keying(FSK): -if as per 1 or 0 , frequency of carrier is varied.



The transmitted signal frequency consists of many sinusoidal components of small frequencies. The transmitted signal frequency consists of a component of frequency (fc - fs) and a sinusoidal component of frequency (fc + fs).

Phase-shift keying (PSK):- Binary Phase Shifted Keying (PSK or BPSK) 0 degrees or 180 degrees if as per 1 or 0 phase angle varied.



The transmitted signal frequency consists of many sinusoidal components of small frequencies. Data is transmitted by varying or modulating the phase of the carrier wave.

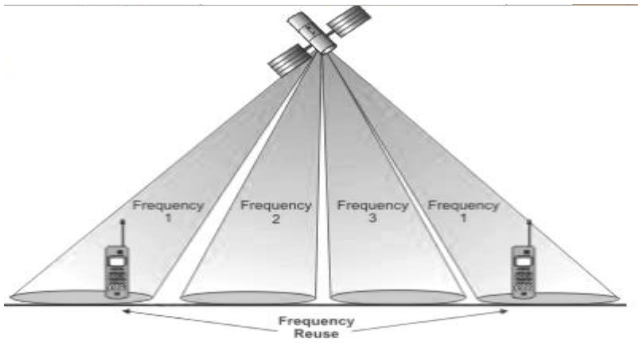
c. Multiplexing

One of the major issues faced by wireless communication is how to spread an input signals or codeword over time and frequency(within the available delay and frequency constraints).If a signal is essentially contained both within a time interval T_{coh} and a frequency interval F_{coh} „then a single fade can bring the entire signal far below the noise level. If, however the signal is spread over multiple intervals of duration T_{coh} and/or multiple bands of width F_{coh} ,then a single fade will affect only one portion of the signal. Spreading the signal over regions with relatively independent fading is called *diversity*. The parameters T_{coh} and F_{coh} tell us how much spreading in time and frequency is required for using diversity techniques.

Multiplexing :- means that different channels, users, or sources can share a common space, time, frequency, or code for transmitting data.

The basic principle used by multiplexers is a many-to-one concept whereby many inputs are combined as one link or one output from a MUX unit where a DMUX unit at the receiver reproduces the same many units at the end of the entity i.e. mutiplexing tells how many users can share the medium with minimum or no interference.
There are several types of multiplexing techniques:

Space Division Multiple Access(SDMA):- This refers to a division of the available space, where multiple sources can access the same medium at the same time.



A wireless transmitter transmits the modulated signals and accesses a space slot, and another transmitter accesses another space slot such that the signals from both can propagate in two separate spaces in the medium without affecting each other.
Used in GSM and CDMA

Example
Assume we have four groups A, B, C, and D of mobile users and four different regional space slots, R1, R2, R3, and R4.
Group A uses R1, B uses R2, C uses R3, and D uses R4 for transmitting and receiving signals to and from a base station.

Time Division Multiple Access(TDMA):- This is where different sources use different time-slices for transmission of signals. It is an access method in which multiple users, data services, or sources are allotted different time-slices to access the same channel.
The available time-slice is divided among multiple modulated-signal sources.
These sources use the same medium, set of frequencies, and same channel for transmission of data.
Example
Eight GSM radio-carriers (e.g., mobile phones) C1, C2, C3, C4, C5, C6, C7, and C8 in eight TDMA time-slices, one for each radio carrier.
Eight phones GSM devices simultaneously transmit in the same frequency band (channel)
Time-slice allotted to each 577 µs

Frequency Division Multiple Access(FDMA):- In this case, different sources use different frequency for transmission of signals.
Each device is allocated a fixed frequency
Multiple devices share the available radio spectrum by using different frequencies.

Example
GSM 900 at 890–915 MHz uplink from user to the base station and 935–960 MHz downlink . Each channel 200 kHz bandwidth.

Code Division Multiple Access(CDMA) :- This requires that different sources use different codes for transmission of signals. Multiple users are allotted different codes (sequences of symbols) to access the same channel (set of frequencies).
A symbol is a bit (0 or 1) which is transmitted after encoding and processing bits of data such as text, voice, pictures, or video.
Example
Each code is uniquely made up of n symbols which is used for transmitting a signal of frequencies fc0, fc0 + fs, fc0 + 2fs, …, fc0 + (n – 2) fs, fc0 + (n – 1) fs by the same channel.

Frequencies are also called chipping frequencies in scheme called DSSS (Direct Sequence Spread Spectrum) and hopping frequencies in FHSS (Frequency hopping Sequence Spread Spectrum.

To do: read about OFDAM

Limitations of wireless Networks

1. Typically much slower than wired networks e.g. "State of the art" wireless LAN: 54Mb/sec while Wired LAN: 10000Mb/sec+
2. Higher transmission bit error rates (BER)
3. Uncontrolled population
4. Difficult to ensure Quality of Service (QoS)
5. Asymmetric bandwidth

LESSON 3

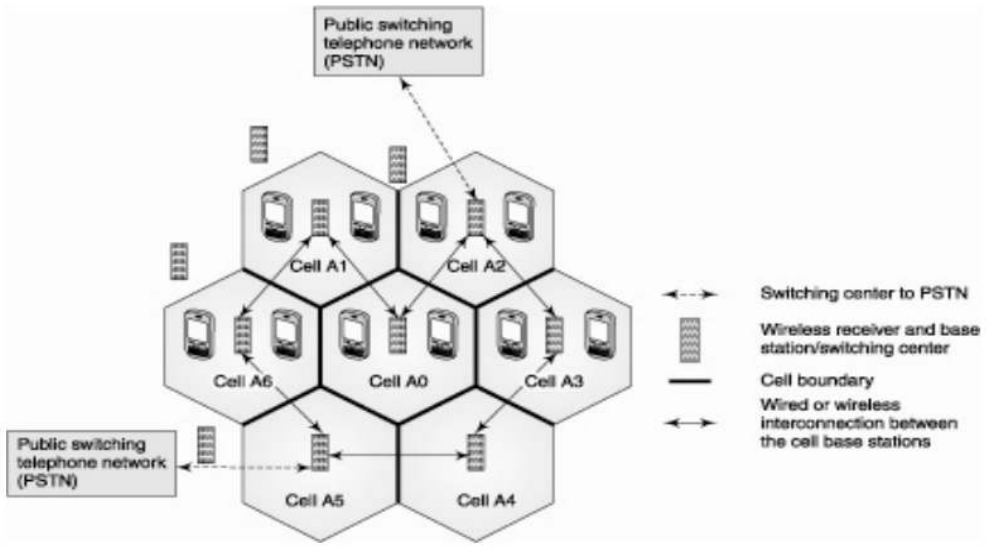
WIRELESS MOBILE NETWORKS,MOBILITY AND COMMUNICATION STANDARDS

Wireless Networks According to Distance of coverage..read about these

1. PAN: Personal Area Network
2. LAN :Local Area Network
3. MAN: Metro Area Network
4. WAN : Wide Area Network
5. Cellular Networks

Wireless Mobile /Cellular Networks

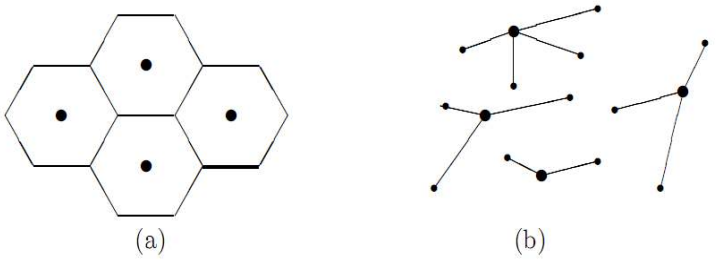
The most distinguished form of wireless communication is cellular networks. A cellular network consists of a relatively large number of subscribers with cellular/mobile phones which can be used in almost all geographical locations.



Fig( )A demonstration of cellular network/mobile wireless communication

There are also a number of fixed base stations strategically arranged to provide wireless electromagnetic communication with arbitrarily located cell phones.

The area covered by a base station is called a cell. In practice, base stations are placed somewhat irregularly, depending on the location of places such as buildings tops, hill tops and other areas with good coverage.



(a) (b)

Part (a): an oversimplified view in which each cell is hexagonal.

Part (b): a more realistic case where base stations are irregularly placed and cell phones choose the best base station

Each cell phone when it makes a call is connected via its antenna(sender-point) and electromagnetic radiation, to the base station with the best apparent communication path(channel).The base stations in a given area are connected to a mobile telephone switching office(MTSO) by high speed wire, fiber or microwave connections. The MTSO is connected to the public wired telephone network.

Thus an incoming call from a cell phone is first connected to a base station and from there to the MTSO and then to the wired network. From there, the call goes to its destination, which might be another cell phone, a computer connection or an ordinarily wired line phone. M.T.S.O plays a major role of coordinating which base station will handle a call to or from a cell phone and also when to hand off a cell phone conversation from one base station to another.

The wireless link from a base station to a cell phone is called the **dow**

nlink (or forward) channel and the link from a cell phone to a base station is called the **uplink (or reverse) channel**. There are usually many cell phones connected to a single base station.

Advantages and Disadvantages of cellular systems

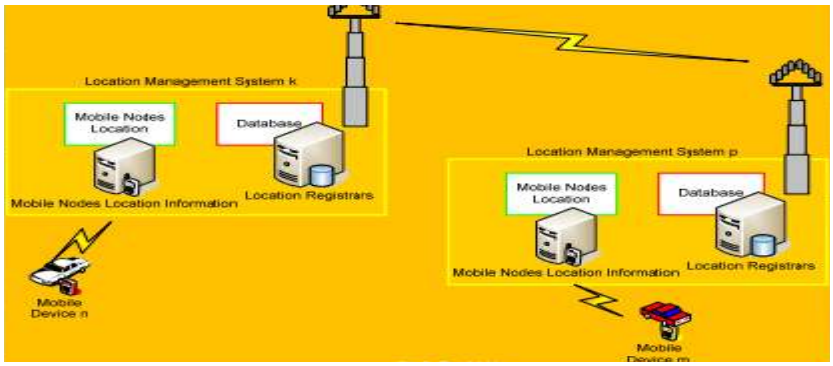
Advantages	**Disadvantages**
High capacity, Less transmission power, Local interface only, Robustness	Near-far problem that affects the signal quality, self jamming due to frequency planning, soft handoff needed

Location and Mobility Management in Cellular Systems

Location Management Principles & techniques involves:

Location Registrars (databases),whose operations include:

- Search operation
- Update operation



Task 1: **Location Management System & Operations**

Location Registrars – databases

Two operations are involved i.e.

Search	Update (Registration)
• Mobile Node m – Invoke the search operation • Mobile Node n – Current Location Unknown	• Mobile Node n – Informs the system of its current location. Frequency of update (never performed?, too frequent?)

Location Update Procedure

A mobile device inform a cellular network whenever it moves from one location area to another. Mobiles are responsible for detecting location area code.

Types

- *Periodic Location Update*: Each mobile is require to regularly report its location at a set time interval.
- *Radom Location Update*: When a mobile moves from one location area to the next while not on a call. Or A stationary mobile that selects coverage from a cell in a different location area because of signal fading

The Aspects of mobility involve two concepts:
User mobility: means that a user can have access to the same or similar telecommunication services at different places.

1) Between different communication devices
2) Between different applications

Device portability: many mechanisms in the network and inside the device have to make sure that communication is still possible while the device is moving.

1) Between different geographical locations
2) Between different networks

Mobility management strategies aim at maintaining uninterrupted (seamless) signal connectivity when a mobile device changes location from within a cell C_i or a network N_i to another cell C_j or network N_j.
Two important tasks characterize a cellular telephony network to ensure constant connectivity;

a. Infrastructure management by roaming.
b. Location management and registration management by handoff.

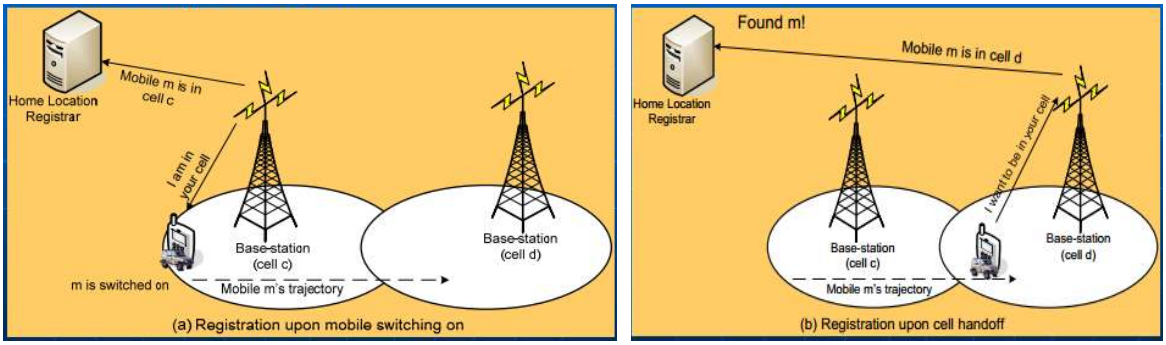
A. Infrastructure management through Roaming

For large-scale mobility, when a mobile user moves from one location to another (for example, from one country to another), the system should be informed of the user's current location. Otherwise, it is impossible to deliver the services to the mobile user.

Two basic operations in roaming management are registration (a mobile phone informs the system of its current location) and location tracking (the system locates the mobile phone). Location tracking is required when the network attempts to deliver a call to the mobile user.

B. Handoff Management

For small-scale mobility, when a mobile user is in a conversation, a radio link connects the mobile phone to a base station. If that user moves to another base station's coverage area, the radio link to the old base station is disconnected, and a radio link in the new base station is required to continue the conversation. This process is called automatic link transfer or handoff.



Handoff ensures that the mobile node remains connected while moving from one cell to another
Or to ensure that in-transit packets can be routed correctly. That is:

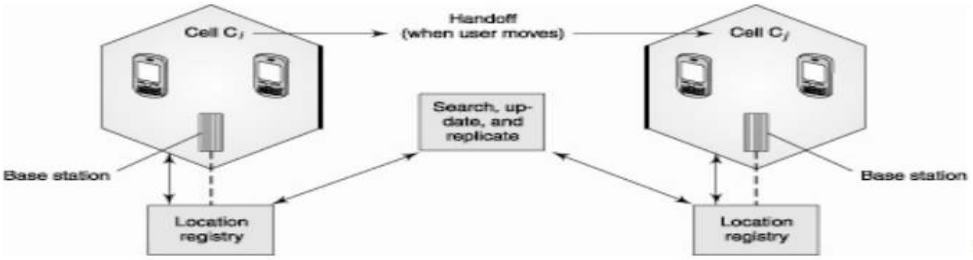
Mobile device m ↔Mobile device n

Task 1. Determine Device m's Location and Establish a Route i.e.

a. Its access point (AP) in the wireless network
b. Base stations in cellular networks

Task 2. Handoff - when m device move out of the range of current AP, it established a connection with another AP.

Task 3. The connection/data packets are routed correctly to new AP



Fig( )Handoff management

Subtasks involved during Handoff

The tasks include:

Deciding when to handoff to a new AP, Selecting a new AP from several APs in the vicinity, Acquiring resources: channels and Informing Old AP to reroute data packets; and send state information

1. *Decide when to handoff to a new AP*

When **deciding when to handoff (switch) to a new AP**, Handoff Decision can be initiated/controlled:

a. Mobile-controlled Handoff
b. Network-controlled Handoff

Decision Factors for handoff includes:

- The mobile station moves out of the range of a BTS or a certain antenna of a BTS. The received signal level decreases continuously until it falls below the minimal requirements for communication.
- The error rate may grow due to interference. All these effects may diminish the quality of the radio link.
- The wired infrastructure may decide that the traffic in one cell is too high and shift some MS to other cells with a lower load i.e. due to load balancing.

Smooth Operation:

• Code Division Multiple Access – permit smooth handoffs. Multiple base stations can be in communication before selecting a base station

2. *Select a new AP from several APs in the vicinity*

Selecting a new AP from several APs in the vicinity

Deciding Factors

- The SNR of the beacon signals from these APs.
- The anticipated region the mobile node is expected to move to.
- The availability of resource at the AP:
- Uplink & downlink channels of connection-oriented circuit-switched network

Address (such as IP) in a packet switched network

3. *Acquiring resources: channels and Informing Old AP to reroute data packets*

When **Acquiring resources,** Various Channel Allocation Schemes are involved.

4. *send state information*

This involves Informing old AP to reroute data packets; and send state information

In network-controlled handoff, the surrounding base stations measure the signal from the mobile phone, and the network initiates the handoff when the criteria are met. In mobile phone-assisted handoff , the network asks the mobile phone to measure the signal from the surrounding base stations. The network makes the handoff decision based on the report from the mobile phone.

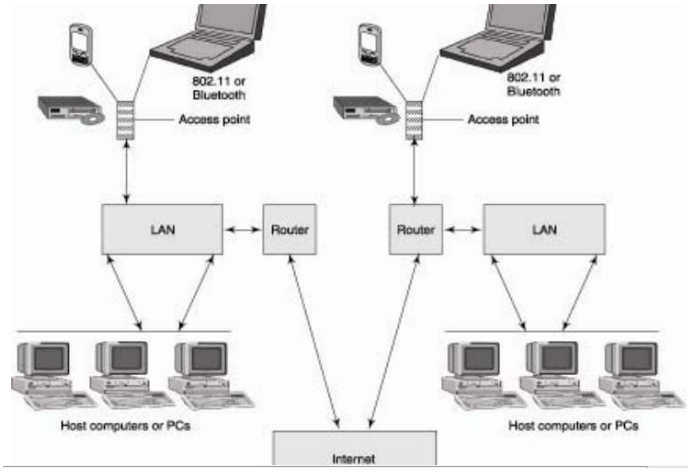
Types of Digital Cellular Systems

Mobile systems are generally classified according to how they allocate frequencies. There are three well established mutually incompatible major types of digital cellular systems.GSM system, TDM (time division modulation) and CDMA (code division multiple access).Many cell phones can switch between multiple modes as a partial solution to these incompatibility issues.

We shall revisit this later. **To do**: *read more about this*

Other types of wireless systems are broadcast systems such as:

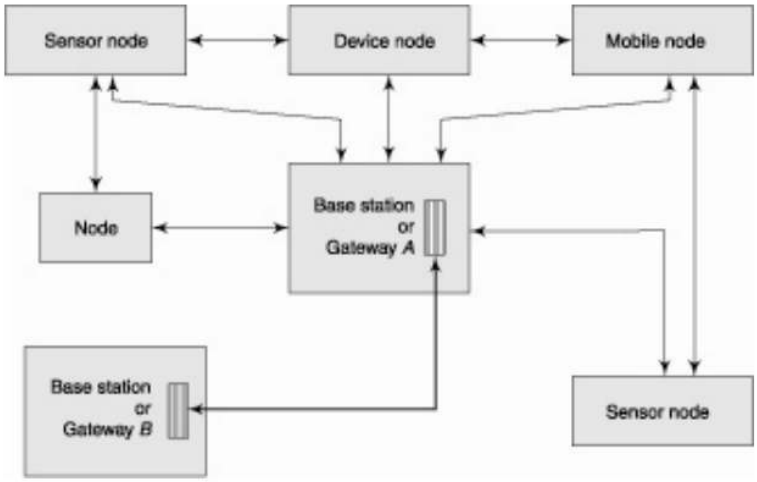
1. **Radio, TV and paging systems:-** Their difference with cellular systems is based on different data rates, size of areas covered by each broadcasting node and the frequency ranges.
2. **Wireless LANS:-** are designed for much higher data rates than cellular systems, but are somewhat similar to single cell of a cellular system. Communication through WLAN is happens through access points called hotspots e.g.



Fig( )A demonstration of WLAN

Blue tooth:- is a smaller LAN that covers a smaller cell range.

3. **Ad hoc network(s):-** is a type where networks organize themselves into links between various parts of nodes and develop routing tables using the links. They don't rely on a central base station. In ad hoc networks, nodes communicate directly or by use of a base station as a gateway i.e.



Fig( )demonstration of an ad hoc network setup

Note that this is a collection of autonomous nodes that communicate with each other by forming a multi-hop radio network in a decentralized manner. No infrastructure, no default router available and "every" node needs to be a router.

Overview of 1G,2G,2.5G and 4G Cellular communication standards

The "G" in these acronyms simply refers to the word "generation" of cellular transmission technologies. These generations are not defined by time periods, rather by types of technology. The G include:

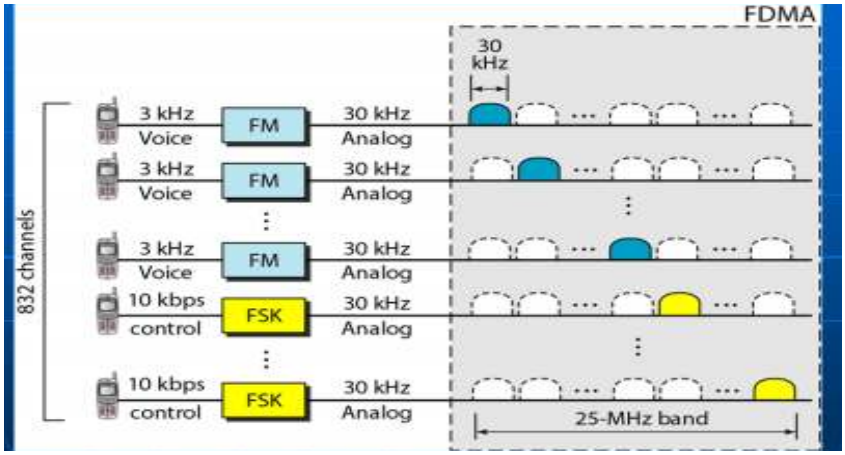
A. First Generation- 1G (1982-Bell Labs in US)

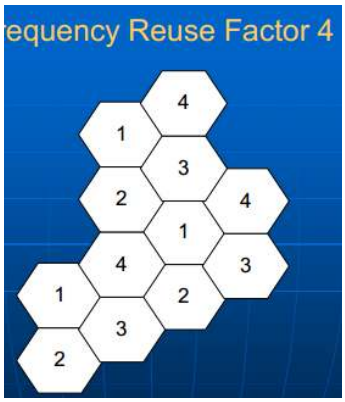
1. Advanced Mobile Phone Service (AMPS)
2. Uses Analog FDMA (Frequency Division Multiple Access)
3. No of Channels: 832 channels: 25 MHz / 30 kHz, can be shared by two providers
4. Each cell uses some set of frequencies not used by any of its neighbors i.e. Adjacent cells are assigned different frequency bands to avoid interference

E.g. ISM 800-MHz band:

- ✓ Base Station →Mobile Station: forward communication channels (824-849 MHz: 25 MHz band)
- ✓ Base Station ←Mobile Station: reverse communication channels (869-894 MHz: 25 MHz band)

- ✓ Voice channel – Frequency modulation (30 kHz)
- ✓ Control Channels - FSK (Frequency Shift Keying) – 10 kbps/30 kHz signal



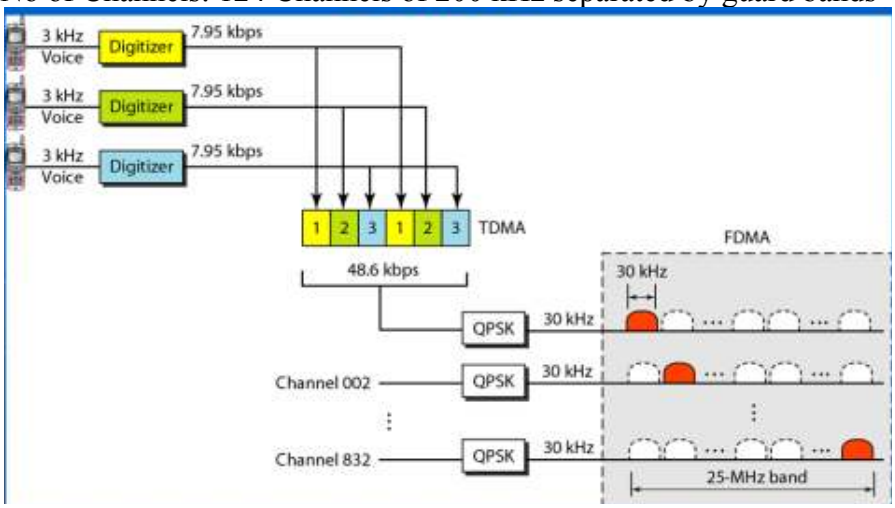


AMPS reverse communication band and Frequency reuse factor 4

B. Second Generation- 2G

1. D-AMPS (Digital Advanced Mobile Phone System)
2. In this standard, devices communicate voice as well as data signals. They have data rates of up to 14.4 kbps.
3. TDMA-FDMA/ CDMA (Code Division Multiple Access) e.g. GSM
4. Voice Signal Digitization: PCM (Pulse Code Modulation) and compression i.e. Voice channel →Digitize + Compress → digital signal
   3 kHz →PCM Digitized →7.95 kbps digital voice channel
   TDMA : 1 slot – 7.95 kbps
   E.g. of a TDMA Frame [1 2 3 1 2 3]

5. Bands: 2 bands, each band 25 MHz
6. No of Channels: 124 Channels of 200 kHz separated by guard bands



D-AMPS

B.1 2.5 G

These are enhancements for data rates up to 100 kbps.The technology came onto the market in 1988.

– extend 2G system by adding packet-switched connection

- ✓ GPRS (General Packet Radio Service; for data packet service on GSM network)
- ✓ EDGE (Enhanced Data GSM Evolution, up to 384 Kbps) - a transition to 3G by Cingular that used TDMA for 2G
- ✓ Support WAP, search, directory services, etc

C. Third Generation- 3G(2001)

1. This standard has higher data rates to support voice, data, and multimedia streams. It facilitates data rates of 2 Mbps or higher for short distances, and 384 kbps for long distance transmissions.
2. It enable transfer of video clips and faster multimedia communication.
3. These standards are used by a Combination of Technologies :
   - Audio and Video
   - VoIP
   - Still & Moving Images
   - Digital Data
   - UMTS (Unified Mobile Telephone Service): Enhanced multimedia: movie, images, music ,Internet Surfing & Video telephony, Video conferencing
4. Uses an Always connected infrastructure.
5. WCDMA (wideband CDMA). Used by most GSM cellular providers.

   CDMA2000- Code Division Multiple Access

   • Pioneered by Qualcomm

   • Used by most CDMA providers

   • Used by Verizon Wireless and Sprint

4. Fourth Generation-4G(2011)

1. This provides mobile ultra-broadband Internet access, using:
   - Mobile WiMAX standard (at first in South Korea in 2006).
   - Long Term Evolution (LTE) standard (in Oslo, Norway since 2009)

   Standard requirements:

   i. All IP, packet-switched networks
   ii. Peak data rates of up to approximately 100 Mbit/s for high mobility and up to approximately 1 Gbit/s for low mobility
   iii. Scalable channel bandwidths of 5–20 MHz, optionally up to 40 MHz.
   iv. Dynamically share and use the network resources to support more simultaneous users per cell.
   v. Smooth handovers across heterogeneous networks.
   vi. Offer high quality of service for multimedia support.

   Two main networking principles came up:

   – Orthogonal Frequency Division Multiplexing (OFDM) i.e. Spatial Multiplexing

   – Multiple-Input Multiple-Output (MIMO) i.e. Space-Time Coding

The tables below show the peak data rates for different generations of mobile networks:

2G

Speeds in kbit/s	*down and up*
GSM CSD	9.6 kbit/s
CDPD	up to 19.2 kbit/s
GSM GPRS (2.5G)	56–115 kbit/s
GSM EDGE (2.75G)	up to 237 kbit/s

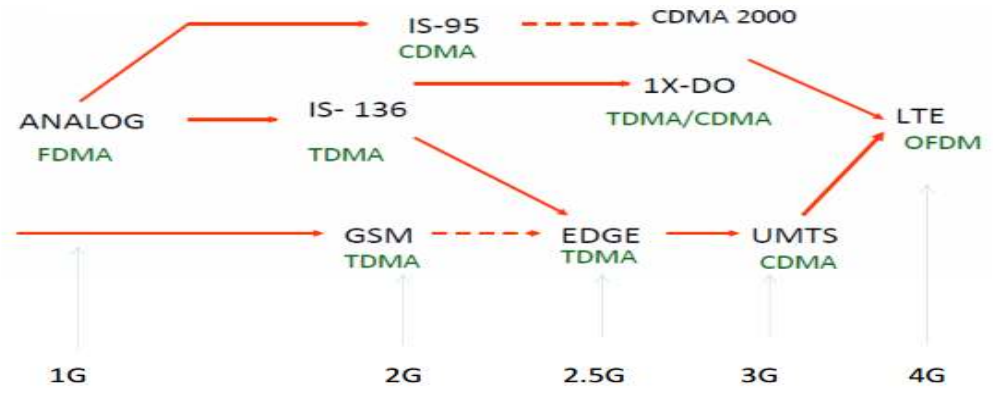
3G

Speeds in Mbit/s	*down*	*up*
UMTS W-CDMA	0.4 Mbit/s	
UMTS HSPA	14.4	5.8
UMTS TDD	16 Mbit/s	
CDMA2000 1xRTT	0.3	0.15
CDMA2000 EV-DO	2.5–4.9	0.15–1.8
SM EDGE-Evolution	1.6	0.5

4G

Speeds in Mbit/s	*down*	*up*
HSPA+	21–672	5.8–168
Mobile WiMAX (802.16)	37–365	17–376
LTE	100–300	50–75
LTE-Advanced:		
High-speed moving	100 Mbit/s	
Not moving or lower-speed moving	up to 1000 Mbit/s	
MBWA (802.20)	80 Mbit/s	

Evolution of Cellular Networks



Wireless transmission protocols

Wireless links can be used to create a wireless local loop- thought of as the "last mile" of the telecommunication network that resides between the central point of management the individual homes or business in close proximity to the central point of management .

An advantage of WLL technology is that once the wireless equipment is paid for, there are no additional costs for transport between the central point of management and the customer premises equipment.

There are several transmission protocols in wireless networks that help to achieve different application oriented tasks. Below, some of these applications are given:

A. Bluetooth(Wireless PAN)

Facilitates ad-hoc data transmission over short distances from fixed and mobile devices. Bluetooth is used to connect and exchange information between devices like PDAs, mobile phones, laptops, PCs, printers and digital cameras wirelessly.

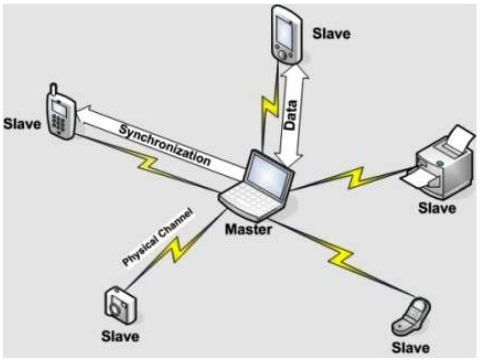


Fig:data transmission with bluetooth

Uses a radio technology called frequency hopping spread spectrum. It chops up the data being sent and transmits chunks of it on up to 79 different frequencies.In its basic mode, the modulation is Gaussian frequency shift keying (GFSK).

Characteristics

- It can achieve a gross data rate of 1 Mb/s.
- Bluetooth is primarily designed for low power consumption, within a short range (power-class-dependent: 1 meter, 10 meters, 100 meters) based on low-cost transceiver microchips in each device.
- Different multiplexing schemes e.g. frequency hopping spread spectrum

Limitation

a) Has a limited range of connectivity.
b) Suffers security vulnerabilities i.e. Issues such as DOS attacks, evesdropping, man-in-the middle attacks, message modification etc.

B. Wireless Local Area Networks (W-LAN)

IEEE 802.11 WLAN .

Uses 2Mbps user data rates (will fallback to 1Mbps in noisy conditions)

IEEE 802.11a standard provides upto 54Mbps throughput in the 5GHz band.

The DS-SS IEEE 802.11b has been called Wi-Fi.

Wi-Fi networks have limited range. A typical Wi-Fi home router using 802.11b or 802.11g with a stock antenna might have a range of 32 m (120 ft) indoors and 95 m (300 ft) outdoors.Range also varies with frequency band.

IEEE 802.11g uses Complementary Code Keying Orthogonal Frequency Division Multiplexing (CCK-OFDM) standards .

Characteristics

- Direct communication within a specific range.
- Low power for battery use.
- Transparency concerning applications and location awareness.
- Provides a robust transmission technology with a global seamless operation.

Limitations

- Suffers from security vulnerabilities

C. WiMax(World Interoperability for Microwave Access)-Wireless MAN

Provides upto 70 Mb/sec symmetric broadband speed without the need for cables. The technology is based on the IEEE 802.16 standard (also called WirelessMAN)

WiMAX can provide broadband wireless access (BWA) up to 50 km for fixed stations, and 5 - 15 km for mobile stations.

The 802.16 specification applies across a wide range of the RF spectrum, and WiMAX could function on any frequency below 66 GHz (higher frequencies would decrease the range of a Base Station to a few hundred meters in an urban environment).

characteristics

a) support for multi-path: The technology offers Orthogonal Frequency Division Multiplexing (OFDM) based pysical layer, to provide configuration for multipath.
b) Broadband access:
c) High speed data rate: upto 70 mbps.
d) scalability: can support an arbitrary number of devices.
e) reliability: offers modulation and error correction to reduce the BER.

D. Microwave/radio

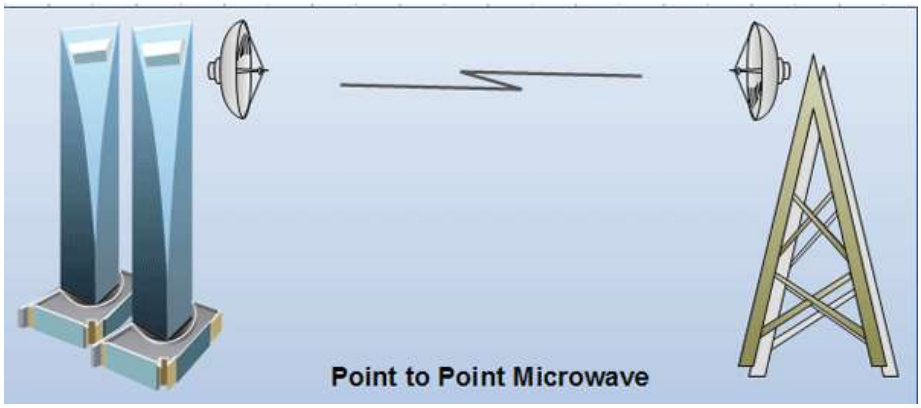
Microwave transmission is the transmission of information or energy by electromagnetic waves whose wavelengths are measured in small numbers of centimetre.

This is a form of radio transmission that use Ultra-high frequencies developed out of experiments with radar (radio detecting and ranging) .

There are several frequency ranges assigned to microwave systems, all of which are in the Giga Hertz (GHz) range and the wavelength in the millimeter range. This very short wavelength gives rise to the term microwave. Such high frequency signals are especially susceptible to attenuation and, therefore must be amplified or repeated after a particular distance.

In order to maximize the strength of such a high frequency signal and, therefore, to increase the distance of transmission at acceptable levels, the radio beams are highly focused.

The transmit antenna is centered in a concave, reflective metal dish which serves to focus the radio beam with maximum effect on the receiving antenna, as illustrated in the Figure below.



The receiving antenna, similarly, is centered in a concave metal dish, which serves to collect the maximum amount of incoming signal.

It is a point-to-point, rather than a broadcast, transmission system. Additionally, each antenna must be within line of sight of the next antenna.

Microwave hops generally are limited to 80 km(given the curvature of the earth, and the obvious problems of transmitting through it).

Frequency Bands Maximum Antenna Separation Analog/Digital 4-6 GHz 32-48 km Analog 10-12 GHz 16-24 km Digital 18-23 GHz 8-11 km Digital.

General Properties

1) **Configuration**: Microwave radio consists of antennae centered within reflective dishes that are attached to structures such as towers or buildings. Cables connect the antennae to the actual transmit (receive) equipment.
2) **Bandwidth**: Microwave offers substantial bandwidth, often in excess of 6 Ghz.

3) **Error Performance** :Such high frequency radio is particularly susceptible to environmental interference, e.g. precipitation, haze, smog, and smoke. Generally speaking, however, microwave performs well in this regard.
4) **Distance** Microwave is distance limited(80), especially at the higher frequencies. This limitation can be mitigated through special and more complex arrays of antennae incorporating spatial diversity in order to collect more signals.

Limitations

1) **Security:** As is the case with all radio systems, microwave is inherently not secure. Security must be imposed through encryption (scrambling) of the signal.
2) **Cost**: The acquisition, deployment and rearrangement cost of microwave can be high. However, it often compares very favorably with cabled systems, which require right-of-way, trenching, conduit, splicing, etc.

Applications

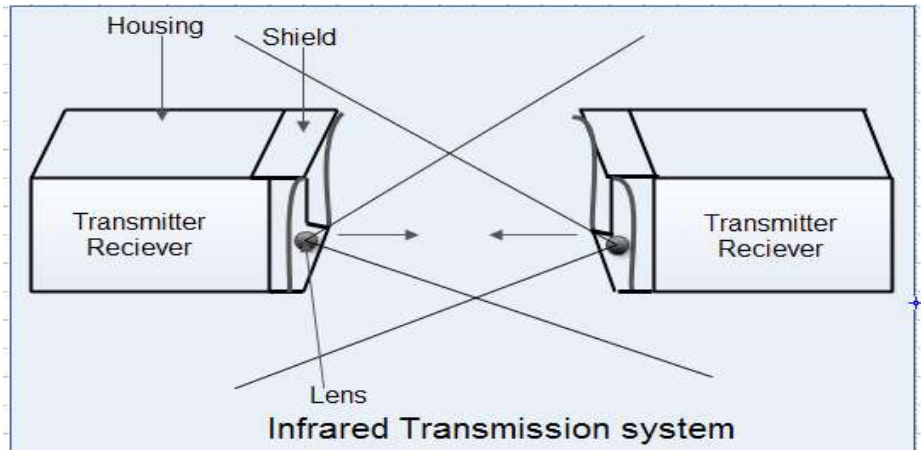
Contemporary applications include private networks, interconnection of cellular radio switches, and as an alternative to cabled systems in consideration of difficult terrain.

E. IrDA(Infra-Red Data Association)

Infrared light transmissions have existed for many years and their use having been limited to TV remote controls and wireless slide projector remote controls.

Infrared systems use the infrared light spectrum to send a focused light beam to a receiver.

A pair of lenses is used, with a focused lens employed in the transmitting device and a collecting lens in the receiving device as shown in the Figure below:.



Infrared Transmission system

Infrared is an airwave, rather than a conducted transmission system, used in short-range transmission,

They do offer substantial bandwidth, but with risks of interference.

Infrared often is an attractive alternative i.e the forward cell can reuse frequencies used in the previous cell. This helps in sharing the same frequency band. Many calls can be handled by one frequency especially where digital phones are used.

Characteristics

a) uses light as a communication medium
b) Low power consumption-receivers need little power.
c) Low bit error rate i.e. The number of received bits of a data stream that have been altered due to noise.
d) rapid deployment, especially as there are no licensing requirements as typically is the cue with microwave. Infrared offers fairly substantial bandwidth at relatively low Cost.

Limitations

1. infrared systems require line-or-sight
2. suffer from environmental interference, as do microwave system.
3. infrared is distance limited e.g. 10 M

F. RFID(Radio Frequency Identification)- Tags

RFID is a method of remotely storing and retrieving data using devices called RFID tags.

- An RFID tag is a small object, such as an adhesive sticker, that can be attached to or incorporated into a product.
- RFID tags contain antennas to enable them to receive and respond to radio-frequency queries from an RFID transceiver.
- No line-of sight required (compared to laser scanners)
- Withstand difficult environmental conditions (cold, frost etc.)

Consists of network connected devices(fixed or mobile)with an antennae that sends data commands to the tags.
The tags contain intelligent bar codes that can give a unique identity which can be electronically retrieved.Uses electromagnetic fields to automatically identify and track tags in attached objects when these objects are scanned.

Categories:

- Active RFID: battery powered, distances up to 100 m
- Passive RFID: operating power comes from the reader over the air, distances up to 6 m
- Applications:- Automated toll collection: RFIDs mounted in windshields allow commuters to drive through toll plazas without stopping

Characteristics

a) **No need for direct line of sight to activate**: Mostly, the electronic components will be protected by plastic covers.
b) **Read/Write capability**: RFID reader can communicate with the tag and alter a lot of the information allowed by the designers.
c) **Anti-collision**: If an RFID reader identifies many tags in the reader range, it can result to tag collision and reader collision. If all tags were to transmit to the readers simultaneously, then the signals would interfere with each other; rendering them ineffective. Anti-collision enables the tags to take turns in transmitting to the reader; hence maintains high integrity.

G. Zigbee

ZigBee is the specification for a suite of high level communication protocols using small, low-power digital radios based on the IEEE 802.15 standard.
Efficient for wireless personal area networks (WPANs), such as wireless headphones connecting with cell phones via short-range radio.

ZigBee is targeted at radio-frequency (RF) applications that require a low data rate, long battery life, and secure networking.
ZigBee operates in the industrial, scientific and medical (ISM) radio bands; 868 MHz in Europe, 915 MHz in countries such as USA and Australia, and 2.4 GHz in most worldwide.

H. Sensor Networks

Comprises of a group of tiny devices and wireless infrastructure that monitors and records conditions in an environment.
The sensor network connects to the internet ,WAN or LAN, so that the data collected can be transmitted to back-end systems of applications.

Characteristics

a) power efficiency: This sustains efficiency in the networks ability to handle mobile nodes and changeable parts.
b) Scalability: The network can gro in terms of the number of nodes attached to the infrastructure without causing an excessive overhead.
c) Reliability and flexibility :Sensor networks can withstand harsh conditions, or can adapt to changes in the the environmental conditions, architectural designs and topology.
d) Resilience: they are able to cope with node failures in the network due to their distributed nature.

LESSON 4

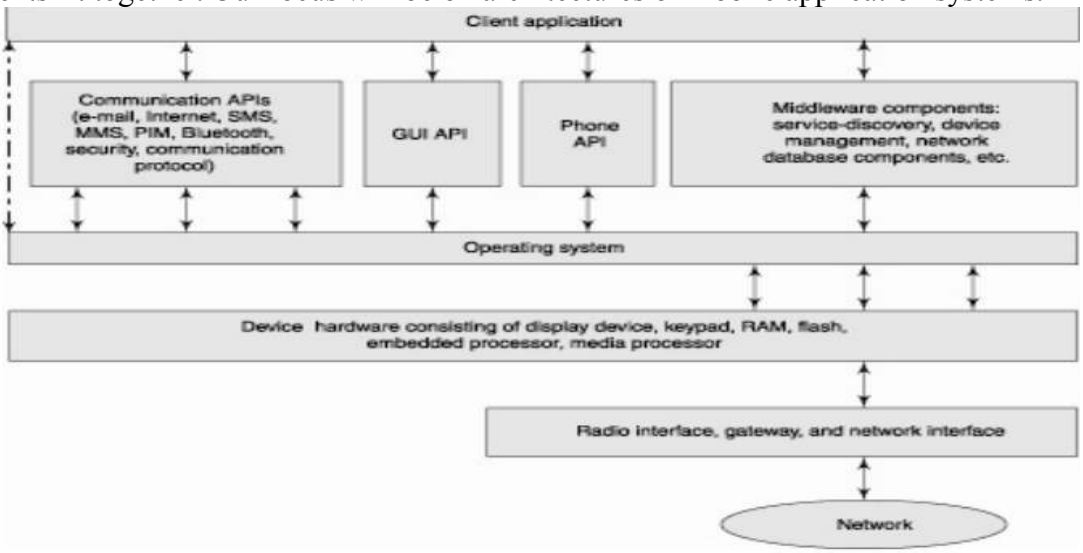
MOBILE COMPUTING ENVIRONMENT ARCHITECTURE AND TOOLS

This refers to the infrastructure which ensures that seamless and reliable communication goes on. These include devices , protocols, services, bandwidth, and portals necessary to facilitate and support the stated services.

Here we are going to look at some very high-level architectures, and discuss how we should use them in building our mobile applications.

Mobile Application/Software Architecture

In general, software architecture is a particularly high-level abstraction of the system and how its components fit together. Our focus will be on architectures of mobile application systems.



Our discussion is limited to issues concerning the design and implementation of mobile applications. In this discussion, we will limit our discussion to software architectures at the application layer and avoid discussions of network topologies, hardware, and other layers of computing systems that reside at layers beneath the application layer. Below is a general framework for android applications:

Then, we will look at the effects of the mobile condition and the dimensions of mobility on the architecture of a computing system.

Mobile Network-Based Architectural Frameworks and Development Tools

Now, let us take a look at a few of the most popular network-based application architectures that have emerged as the prevalent mobile architectures. Because access must be granted to the same application ubiquitously through any device and interface means that mobile applications are inherently distributed network-based systems. Therefore mobile architectures are inherently network based computing architectures.

Network-based architectures are a subset of distributed computing architectures and include the following:

A) Centralized/Mainframe Architecture : In a centralized/mainframe architecture, all of the intelligence of the computing system resides within a central host.

At the edge of the network, remote terminals provide nothing more than a dumb interface to the central host. Mainframe architectures are often accessed by a variety of systems such as PCs and other systems; nevertheless, they are fully centralized as no part of the task that they fulfill can be distributed to the systems that access them.

Every computing function including data storage, logical computations, and rendering of the user interface is done on the central server. Typically, the terminals at the edge of the network are used simply to display the prepared content to be displayed at the central server. The systems that access them are there for one reason: to allow the user to interface with them.

A fully centralized framework,

Applies:	**Do not apply:**
• QOS • Limiter power supply • Active transactions • Location awareness	• Platform proliferation • Limited device capabilities • Support for variety of user interfaces

Examples include: Call centers, ATM, grocery store cash registers, air-traffic control terminals, Battle field systems among other mission-critical-type systems.

Many of today's existing mobile computing systems are fully centralized systems. *For example*, many grocery stores use hand-held mobile scanners to keep track of inventory connected to a central host. However, centralized mobile applications are very costly and typically very inflexible. Most of these types of applications can only be implemented when the financial benefits of using the system exceed the total cost of devices, the centralized hardware, and the software.

B) Client–Server Architectures: In a client–server model, there are two distinct programs residing on separate machines. One program is said to be the "client" of the other. The other program is said to "serve" the client and, therefore, is the "server." In an abstract sense, there is

one server for one or more clients. Client–server architectures provided a feasible means of distributing applications and computing in a network.

In the client–server architecture, the client can do more than just being a hardware interface with no computing power.

A fully client server framework,

Applies:	Do not apply:
• The abilities of the client to interface with the user of the system. • Location awareness. • Better handling of server downtime i.e. the client can give the user a message that tells the user why the server is not accessible (e.g., the server is not responding or cannot be found) • Support for variety of user interfaces	• Centralized QOS

Over time, in an evolutionary manner, variations of the client–server architecture have arisen. These variations are created by the breakdown of the types of responsibilities assigned to the client and the server.

Modern databases were one of the first real commercial examples of the server in the client–server architecture .The primary task of databases, as servers, is to store data, but they can also hold business logic. This logic can be implicit in the form of the structure and content of the data or explicit in the form of stored procedures and queries. Typically, a database program runs on one computer and is accessed through some database connectivity protocol such as ODBC (Open Database Connectivity) or JDBC (Java Database Connectivity) by the clients. The clients may use the server to store data and retrieve data using stored procedures or other mechanisms.

C) N-Tier Architectures:

N-tier architectures try to further apply the principle of separation of concerns to the client–server model by separating the concerns into a set of n layers.

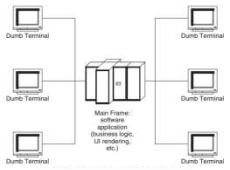
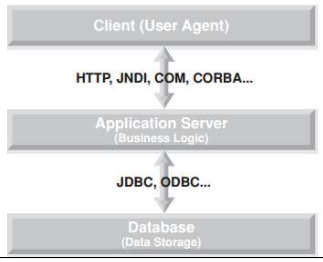
E.g. A 3-tier architecture separates the concern of business logic computations from the rest of the application. The database did the storage of the data and the “application server” took care of the computation of the business logic that needed to be accessed by the clients. In the 3-tier architecture, the application server is the client to the database server and the user interface application, or whatever renders the user interface components, is the client to the application server. This chaining of components in a client-to-server manner is essentially the evolutionary step in the N-tier architectures over the simple 2-tier client–server models.

A fully n-tier framework,

Applies:	Do not apply:

• Better scalability • More reliability properties	• Centralized QOS

Differences

Fully Centralized	N-Tier Client-Server
	
• Have custom-designed clients • Embedded in nature • Designed to do only one thing	N-Tier -Any Number of Tiers – No Limits e.g. 3-Tier

N-Tier Architectures and the World Wide Web

Today, a large portion of the infrastructure of the WWW, arguably the most successful model of distributed computing, is based on 2-tier and 3-tier architectures.

The Web is essentially a client–server system where the clients and servers communicate through HTTP (Hyper-Text Transfer Protocol). The clients are browsers that interpret user interface instructions in HTML (Hyper-Text Markup Language) and other client-side scripting languages such as JavaScript for rendering a graphical user interface.

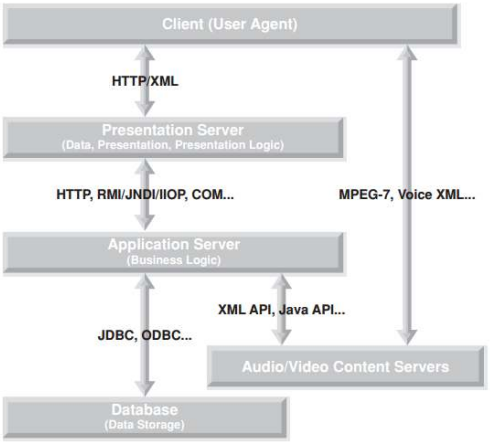
The servers are so-called Web servers that serve the requests of the clients coming in through HTTP with responses that contain HTML. Though there are other types of content that can be served by the Web server, the most popular is HTML. The format of content is often referred to as the MIME (Multimedia Internet Mail Extensions) type of the content. Regardless of the format of the content, content can be grouped into two families: static(content that does not change at the time of the request from the client or because of the request from the client) and dynamic(content is generated at run time and is based on information specific to the instance of the client, the request, or the session).

For most typical Web systems, the concerns are storage, business logic, and presentation of data to the client. This yields $n=3$ for the N-tier architecture. The important thing to note about N-tier architectures is that they favor centralization over decentralization. Because the clients of N-tier systems, such as Web browsers, can communicate with each other, doing logical operations or storing data at the client either is very cumbersome or creates big problems. The strength of N-tier architectures lies in their ability to separate concerns at a central node in the network, thereby allowing for scalability and reliability.

D) N > 3 for Mobile Applications: The first-generation Internet-enabled mobile systems had many of the properties of the mobile systems that we have talked about: The user interfaces varied, the QOS was unreliable, etc. This was not what the 3-tier systems of the Web were designed for.

The 3-tier systems of the Web were designed to produce one type of user interface for one group of browsers. As long as the browser could understand HTML and JavaScript, the user interface was fairly easy to render. As the Web evolved, the Web-browsers also began to use a variety of plug-ins, such as Macromedia Flash, that would prohibit use of content in a resource-starved mobile environment.

The majority of mobile commercial solutions in the market today focus on data-driven mobile solutions with N-tier architectures. A simple version of such N-tier architecture (N=4) may be seen in the figure below:



N=4 tier architecture

The "wireless Web" is a problem that has been tackled by numerous vendors, each with its own version of the presentation server, promising to "wireless-enable" the Web. Presentation servers have allowed the N-tier architecture to evolve further to address the diversification of devices. Nevertheless, N-tier architectures remain in the client–server family. The clients still cannot communicate with each other directly.

E) Peer-to-Peer Architectures: N-tier client–server architectures, with all of their benefits, do not address several dimensions of mobility. N-tier architectures, for example, require that the user be connected to the network because the servers are somewhere else on the network. If one client has the data that another client needs, there is no way for them to discover each other and exchange the information.

Peer-to-peer (P2P) application architectures allow any participant of the network to communicate with any and all of the other participants provided those participants adhere to the rules of the network-based application architecture.

P2P application infrastructures satisfy the problems presented by the dimensions of mobility much better than do client–server and centralized architectures.

P2P architectures do not require connectivity to a server or centralized host; therefore, if a network participant, or peer, needs a piece of information, there may be a variety of other peers that can satisfy its need.

Because P2P architectures rely on the computing power available at the edge of the network (closer to the place where the actual user of the system is) they can deal better with specialization of content to the required user interface.

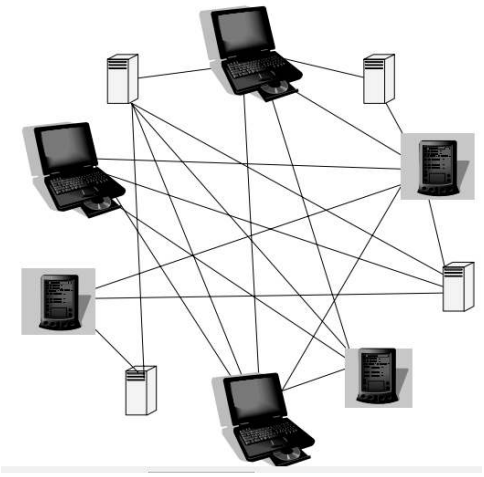


Fig: peer-to-peer network

F) Mobile Agent Architectures: Mobile agent–based software systems are a drastic departure from centralized, client–server, and N-tier systems. Mobile agents have the following properties:

- They are programs that encapsulate data and code, which may be dispatched from a client computer and transported to a remote server for execution.
- They execute asynchronously and autonomously.

The term mobile agent s refers software components that can move from server to server in the network while keeping the state of the application intact. Mobile agents manage their own life cycles based on the logic programmed into them.

Because of their autonomy and their ability to move from one environment to another, mobile agents seem particularly promising for building mobile applications.

Selection of the Frameworks and Tools

1) Thin-Client-Server

- Browser that loads markup code (Web-model)
- No concern about environment
- Server-side structure

2) Thick-Client Wireless Client-Server

- Client -custom application
- Using the client as a means of storing data for the offline business logic
- Does not need to be centralized
- Having thick clients is more difficult due to: Restricted resources & Deployment and provision problem

The platforms that allow thick-client development for mobile devices address this in two ways:

a. Some provide an operating system or a virtual machine that provides the application programmers with a platform that lessens the number of permutations for writing code.
b. Hardware manufacturers, such as Qualcomm and Texas Instruments, provide programming environments directly on top of the hardware. Operating system:- Windows CE, Symbian . Virtual Machine :- J2ME

Stand-alone Applications

They do not need networking components. Needs of synchronization with some external system periodically

Connectivity Platform	Stand-alone	Networked	
		Wired	Wireless
Mobile Platforms			WAP
	Symbian		
	BREW		
	Java /Android		
	.NET		

Table: Some mobile development products

LESSON 5

WIRELESS COMMUNICATION TECHNOLOGIES IN MOBILE COMPUTING

This lesson we try to give an introduction to some of the most pervasive technologies to give us a good understanding of the limitations and capabilities of the infrastructure that our mobile applications will be using for communication.

a) Mobile IP

Current versions of the Internet Protocol (IP) assume that the point at which a computer attaches to the Internet or a network is fixed and its IP address identifies the network to which it is attached. Datagrams are sent to a computer based on the location information contained in the IP address.

If a mobile computer, or **mobile node**, moves to a new network while keeping its IP address unchanged, its address does not reflect the new point of attachment. Consequently, existing routing protocols cannot route datagrams to the mobile node correctly.

Mobile IP solves this problem by allowing the mobile node to use two IP addresses: a fixed **home address** and a **care-of address** that changes at each new point of attachment. Mobile IP enables a computer to roam freely on the Internet or an organization's network while still maintaining the same home address. Consequently, computing activities are not disrupted when the user changes the computer's point of attachment to the Internet or an organization's network. Instead, the network is updated with the new location of the mobile node. The mobile device can change its location to a foreign network and still access and communicate with and through the mobile computer's home network.

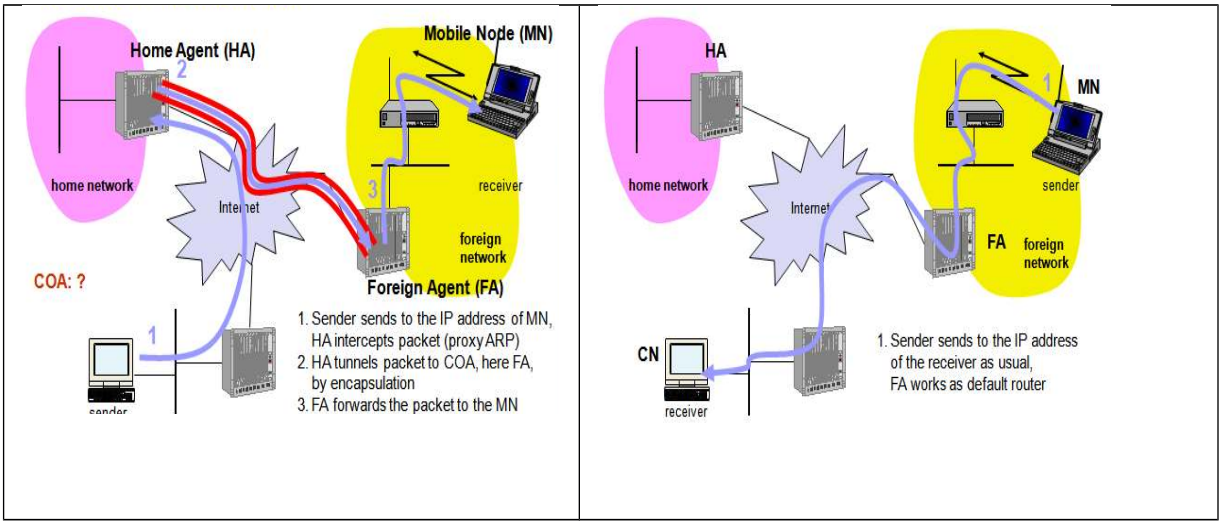
Mobile IP is most often found in wireless WAN environments where users need to carry their mobile devices across multiple LANs with different IP addresses.

Mobile IP protocol Architecture/Topology

Mobile IP is designed to allow mobile device users to move from one network to another while maintaining their permanent IP address.
The following terminologies characterize a mobile IP environment:
Home Network: A network, possibly virtual, having a network prefix matching that of a mobile node's home address.
Home Address: An IP address that is assigned for an extended period of time to a mobile node. It remains unchanged regardless of where the node is attached to the Internet.
Foreign network:
Care-of Address: The termination point of a tunnel toward a mobile node, for datagrams forwarded to the mobile node while it is away from home.
Link Layer Address: The address used to identify an endpoint of some communication over a physical link. A facility or medium over which nodes can communicate at the link layer.
Link: Typically, the link layer address is an interface's media access control (MAC) address.

Mobility Binding: The association of a home address with a care-of address, along with

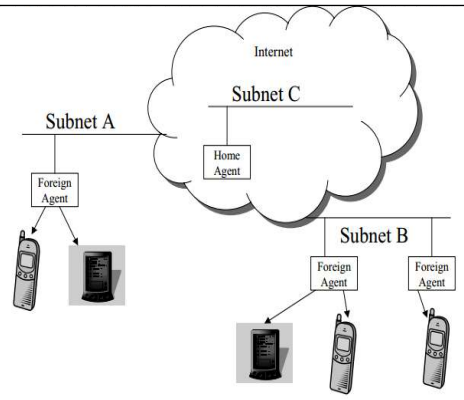
the remaining lifetime of that association.
Virtual Network: A network with no physical instantiation beyond a router (with a physical network interface on another network).



Fig() Mobile IP architecture

The illustrations depict the use of wireless transceivers to transmit the datagrams to the mobile node. Also, all datagrams between the Internet host and the mobile node use the mobile node's home address regardless of whether the mobile node is on a home or foreign network. The care-of address is used only for communication with mobility agents and is never seen by the Internet host.

Mobile IP introduces the following new functional entities:



Mobile IP system components

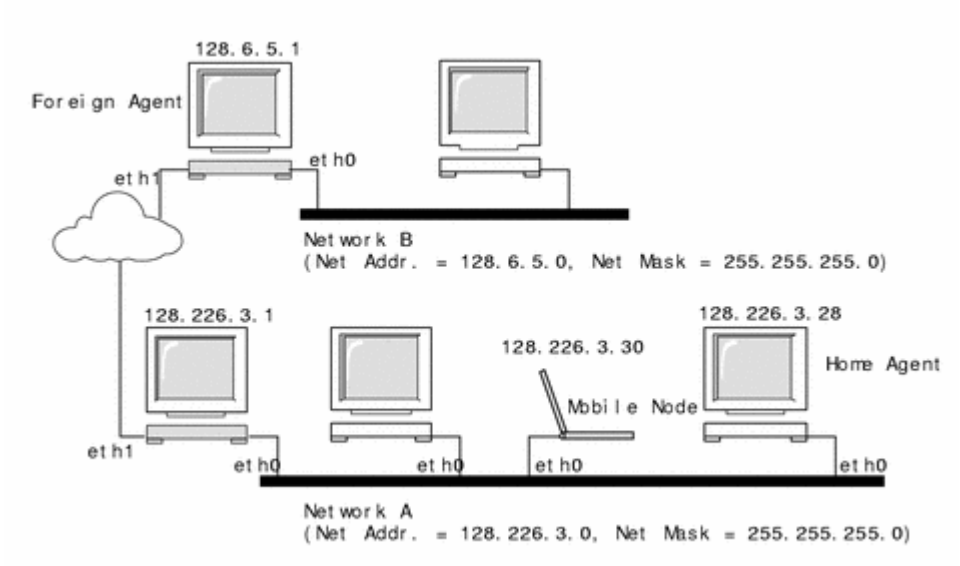
- **Mobile Node (MN)**–Host or router that changes its point of attachment from one network to another. It can also be the mobile device connected to the network through some sort of connectivity, most probably wireless.
- **Home Agent (HA)**–Router on a mobile node's home network that intercepts datagrams destined for the mobile node, and delivers them through the care-of address. The home agent also maintains current location information for the mobile node.
- **Foreign Agent (FA)**–Router on a mobile node's visited network that provides routing services to the mobile node while the mobile node is registered.

Using the Mobile IP topology, the following scenario shows how a datagram moves from one point to another within the Mobile IP framework:

1. The Internet host sends a datagram to the mobile node using the mobile node's home address i.e. normal IP routing process.
2. If the mobile node is on its home network, the datagram is delivered through the normal IP process to the mobile node. Otherwise, the home agent picks up the datagram.
3. If the mobile node is on a foreign network, the home agent forwards the datagram to the foreign agent.
4. The foreign agent delivers the datagram to the mobile node in the foreign network.
5. Datagrams from the mobile node to the Internet host are sent using normal IP routing procedures. If the mobile node is on a foreign network, the packets are delivered to the foreign agent. The foreign agent forwards the datagram to the Internet host.

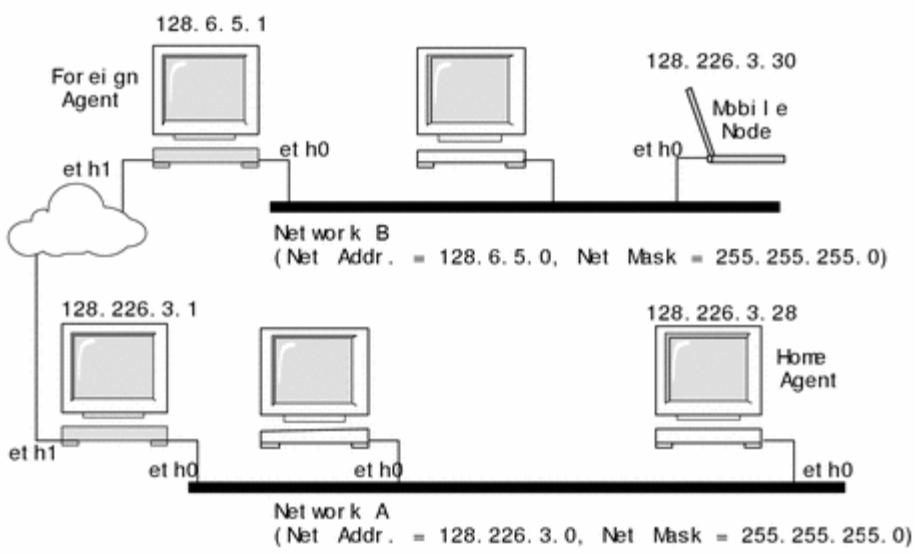
Mobile IP provides two basic functions: *agent discovery and registration*. During agent discovery, home agents and foreign agents may advertise their availability on each link for which they provide service. A newly arrived mobile node can send a solicitation on the link to learn if any prospective agents are present. When the mobile node is away from home, it registers its care-of address with its home agent during the registration phase.

The following illustration shows a mobile node residing on its home network, Network A, before the mobile node moves to a foreign network, Network B. Both networks support Mobile IP. The mobile node is always associated with its home network by its permanent IP address, `128.226.3.30`. Though Network A has a home agent, datagrams destined for the mobile node are delivered through the normal IP process.



Fig( ) mobile node residing on a home network

The next illustration shows the mobile node moving to a foreign network, Network B. Datagrams destined for the mobile node are intercepted by the home agent on the home network, Network A, encapsulated, and sent to the foreign agent on Network B. Upon receiving the encapsulated datagram, the foreign agent strips off the outer header and delivers the datagram to the mobile node visiting Network B.



Fig( )A mobile node moving into a foreign network

The care-of address might belong to a foreign agent, or might be acquired by the mobile node through Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol (PPP). In the latter case, a mobile node is said to have a co-located care-of address.

The mobile node uses a special **registration** process to keep its home agent informed about its current location. Whenever a mobile node moves from its home network to a foreign network, or from one foreign network to another, it chooses a foreign agent on the new network and uses it to forward a registration message to its home agent.

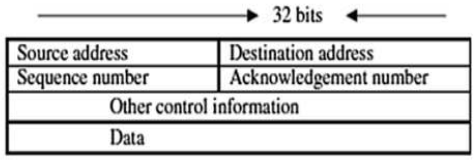
Mobility agents (home agents and foreign agents) advertise their presence using **agent advertisement** messages. A mobile node can optionally solicit an agent advertisement message from any locally attached mobility agents through an **agent solicitation** message. A mobile node receives these agent advertisements and determines whether they are on its home network or a foreign network.

When the mobile node detects that it is located on its home network, it operates without mobility services. If returning to its home network from being registered elsewhere, the mobile node **deregisters** with its home agent.

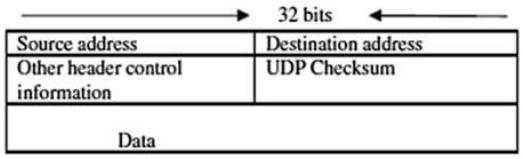
Mobile IP is being designed to be in line with mobility solutions offered based on IPv6, but because most of the infrastructure of the Internet only supports IPv4 at this time, backward compatibility to IPv4 is a requirement.

IPV4

IP Version 4, which is the current, most implemented version of IP, assumes that a node's IP address uniquely identifies the node's point of attachment to the Internet.



TCP Data packet structure



UDP Data packet structure

IPV6

Provides enhancements over IPV4.It is designed to accommodate higher speeds and the mix of graphic and video data. The driving force was the need for more addresses due to growth of the Internet.

IPv6 includes 128-bit source and destination address fields.

IPv6 includes many features for streamlining mobility support that are missing in IP Version 4 (current version), including stateless address auto-configuration and neighbor discovery.

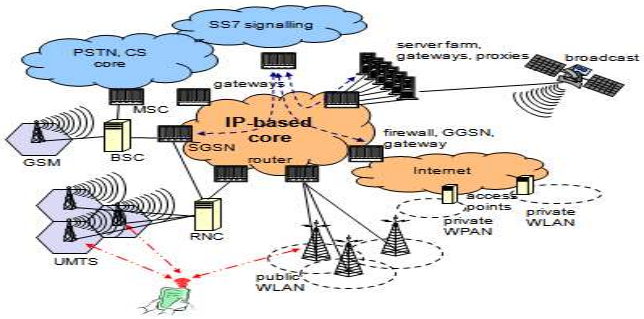
Major differences between IPV6 and IPV4,and application in mobile computing

1) **IPV6 provides support for what is known in Mobile IPv4 as "route optimization"** .It is now built in as a fundamental part of the protocol, rather than being added on as an optional set of extensions that may not be supported by all nodes as in Mobile IPv4.

   Support is also integrated into Mobile Ipv4 and into IPv6 itself. This allows for mobile nodes and mobile IP to coexist efficiently with routers that perform "ingress filtering" . A mobile node now uses its care-of address as the source address in the IP header of packets it sends, allowing the packets to pass normally through ingress filtering routers.

2) **The use of the care-of address as the source address in each packet's IP header also simplifies routing of multicast packets sent by a mobile node.** With Mobile IPv4, the mobile node had to tunnel multicast packets to its home agent in order to transparently use its home address as the source of the multicast packets. With Mobile IPv6, the use of the home address option allows the home address to be used but still be compatible with multicast routing that is based in part on the packet's source address.
3) **No need to deploy special routers as "foreign agents," as in Mobile IPv4**. In Mobile IPv6, mobile nodes make use of **IPv6 features, such as neighbor discovery and address auto-configuration** , to operate in any location away from home without any special support required from its local router.
4) **Mobile IPv6 utilizes IP Security (IPsec) for all security requirements** (sender authentication, data integrity protection, and replay protection) for binding updates (which serve the role of both registration and route optimization in Mobile IPv4).

5) The **movement detection mechanism in Mobile IPv6 provides bidirectional confirmation of a mobile node's ability to communicate with its default router in its current location** (packets that the router sends are reaching the mobile node, and packets that the mobile node sends are reaching the router).
6) **Most packets sent to a mobile node while away from home in Mobile IPv6 are sent using an IPv6 routing header rather than IP encapsulation**, whereas Mobile IPv4 must use encapsulation for all packets.
7) The **dynamic home agent address discovery mechanism in Mobile IPv6 uses IPv6 anycast and returns a single reply to the mobile node**, rather than the corresponding Mobile IPv4 mechanism that used IPv4 directed broadcast and returned a separate reply from each home agent on the mobile node's home link.
8) **Mobile IPv6 defines an advertisement interval option on router advertisements** (equivalent to agent advertisements in Mobile IPv4), allowing a mobile node to decide for itself how many router advertisements (agent advertisements) it is willing to miss before declaring its current router unreachable.



Fig() IP-based generation Network

b) Cellular Digital Packet Data(CDPD)

This refers to packet data over cellular networks i.e. IP packet service over mobile networks. The data network overlay on analog cellular telephone system. The service schedules data packets to unused voice channels.

Overlaid on existing analog cellular systems specifically, Advance Mobile Phone Service-(AMPS) share their infrastructure equipments on a non-interfering basis. AMPS is unsuited for packet data due to long call setup times .
Basically, CDPD transmits packet data over idle cellular channels, and mechanisms called **channel sniffing and channel hopping** are used to autonomously switch the CDPD stream to another channel when the current channel is about to be assigned for voice usage.

CDPD does not communicate with the underlined cellular network. However, its takes advantage of its knowledge of the channel assignment algorithm of the cellular cell, and predicts the channels available for CDPD use.

The CDPD handover is mobile controlled. CDPD user mobility is supported by Mobile Network Location Protocol.
CDPD is used primarily for

1) Law enforcement
2) Handheld/laptop IP access
3) Providing main competition by offering “Wireless Web” phones

Design Goals

1) Low speed, high latency data service. It was Primarily intended for paging and email.
2) Provides broadcast and multiple-access service.
3) Dynamically shared media, always online.
4) Share channels with AMPS allocation
5) Transparency to existing AMPS service.

Channel Scanning/sniffing, CDPD uses unused AMPS channels,usually there are several available.
Each 30KHz channel = 19.2kbps up and down
Channel scanning is done in steps below:

1) Check signal levels from nearby cells, using a list of reference channels distributed by the CDPD infrastructure to find levels.
2) Select cell with best signal. If non-critical and no cell is significantly better than current, no handoff is done (hysteresis)Scan RF channels in cell for CDPD. Stop when an acceptable channel is found.

CDPD channel hopping, can be implemented in two ways:

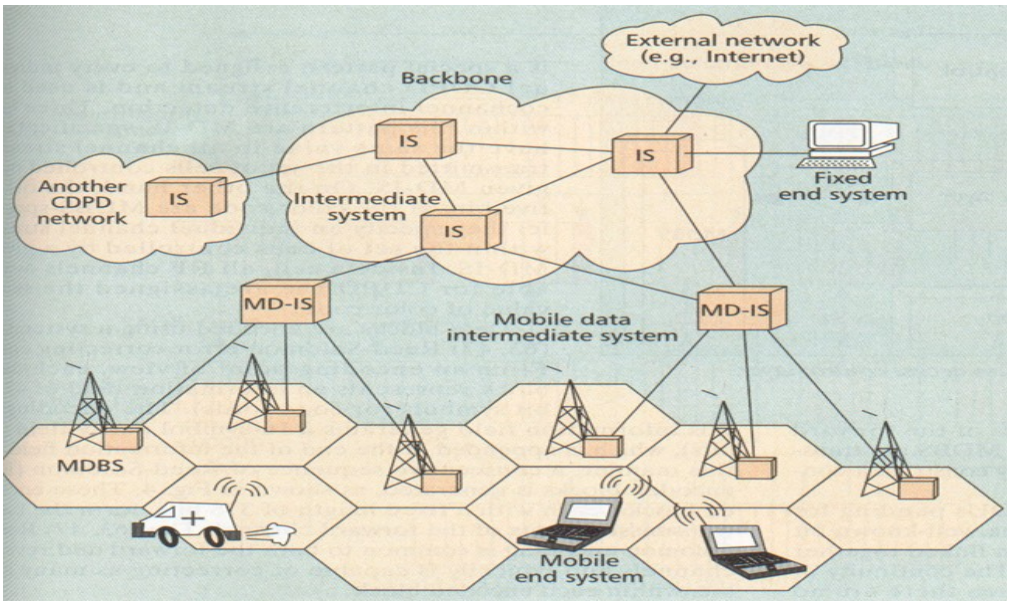
***Forced*:** AMPS must be vacated within 40ms of allocation for voice use.
Planned: Regular hops prevent AMPS system from identifying channel as unusable.

Handoff in CDPD

a) Critical handoffs: The system must choose new channel if;
   - High error rate is observed or BS signal lost. Received signal strength below a threshold.
   - Base station does not receive data from mobile nodes.

b) Noncritical handoffs : happen when;
   - Channel rescan interval expires.
   - Signal strength changes significantly

The CDPD Network infrastructure/Architecture



A.) The **Intermediate System(IS)**: routes to corporate and value added networks like the internet.

B.)MD-IS provides MOBILE routing for data streams using MNLP (Mobile Network Location Protocol).

- ***Mobile home function***- like home agent processing in Mobile IP or Home Location Register (HLR) function in cellular networks. It uses encapsulation to forward packets to MD-IS in the visited region.
- ***Mobile Serving Function***: like foreign agent processing in Mobile IP or Visitor Location Register (VLR) function in cellular networks; it performs registration/authentication/authorization/accounting.

Therefore Mobile Data Intermediate System(MD-IS): is used for mobility management. It works together with the Intermediate System(IS).

C.) The **Mobile Data Base Station(MD-BS):** is collocated with cellular MTSO-the cellular voice equipment which manages cells/air interfaces.

It controls radio interface responsible for radio channel allocation and radio media access.

- Relay Frequency(RF) Channel Pair:
- Forward link from BS to multiple ESs
- Reverse link from multiple ESs to BS

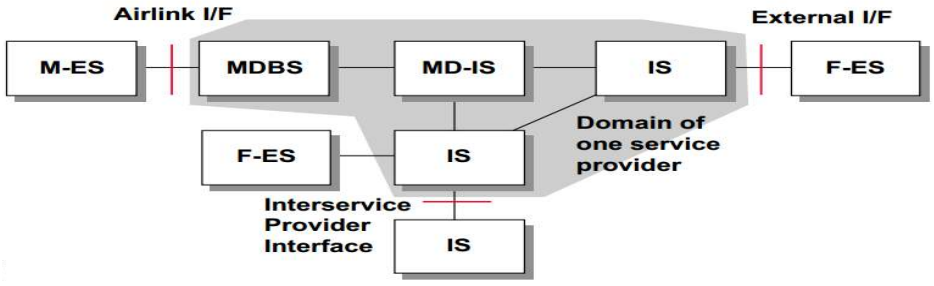
CDPD channels must be able to hop to new frequencies as demanded by the voice services

C.) Mobile End Station(M-ES): is the terminal e.g. a smart phone or a laptop. CDPD network tracks the location of ES and routes them message data-grams. The ES address does NOT imply location; but the current sub-network "point of attachment" determines this e.g. using IP.

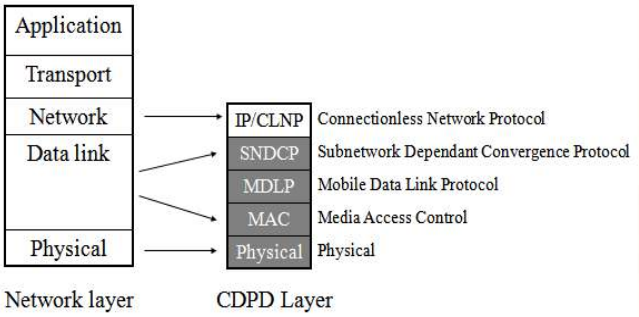
ES are associated with the CDPD network's routing domain, not the user's corporate home network.

A Fixed End Systems (F-ES) i.e. Fixed location, traditional routing can be used

Internal F-ES: provided by service provider, considered to be inside the security firewall,which helps in authentication, authorization, network management, accounting e.g. for domain name services, location services, etc.
External F-ES: external to CDPD, must operate over the external network interface.



CDPD Layering and Protocols

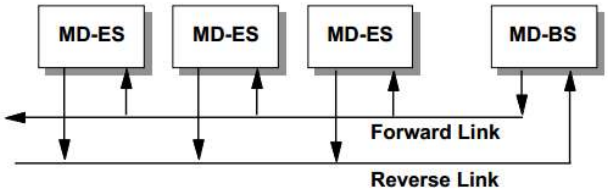


1.) Physical Layer Gaussian Minimum Shift Keying modulation, which compromises between channel bandwidth and decoder complexity.
Raw data rate = 19.2 Kbps per channel.
It is restricted to using pair of analog or digital TDMA cellular voice frequency pairs for each physical CDPD channel.

Functions

a) Tune to specified pair of RF channels
b) Transmit/receive bits
c) Set power levels
d) Measure signal strengths
e) Suspend/resume monitoring of RF channels in M-ES to conserve battery power

2.) Data Link Layer- (MAC Layer)
It arbitrate access to shared medium between M-ES and MD-BS.
Frame recognition, frame delimiting, error detection/ correction.



Forward link: scheduled by BS, signals channel idle/busy
Reverse link: contention access with back-off

During the forward channel: Data packets "broadcast" from BS to ES.
During the reverse channel: M-ES will back off and retry whenever it senses decode failure flag on the forward channel.

5.) Network Layer- Mobile Data Link Protocol (MDLP)
Provides Point (MD-IS) to multipoint (M-ES), connection-oriented, fully sequenced, acknowledged transfers.

Functions:

a) One or more logical data link connections on a channel stream.
b) Sequence control
c) Transmission/format/operational error detection and recovery—retransmits missing blocks
d) Flow control
e) Sleep function for power conservation
f) Dynamic address assignment (Temporary Equipment ID--TEI)

5.) Network Layer- Sub-network Dependent Convergence Protocol (SNDCP)
It is a connectionless mode sub-network service

Functions:

a) Mapping of data primitives
b) Segmentation/reassembly of Network packets Data Units(NPDUs).
c) Compression/elimination of redundant protocol control information
d) Encryption/decryption
e) Network layer to data link layer multiplexing .

5.) Network Layer - (IP Connectionaless Network Protocol)
Mobile Network Registration .
It is connectionless, exchanges configuration information between M-ES and MD-IS:

- Network Entity Identifier (NEI)
- Subnet Point of Attachment (SNPA)

Functions:

a) Registration/deregistration of NEIs with MD-IS
b) Authentication of M-ES and its NEI
c) Admission of M-ES to services offered by MD-IS

Mobile Home Function includes: Location Directory , redirection and forwarding
Servcing Function: Registration Directory, readdress "decapsulation" service.

Network Layer Mobility for CDPD vs. Mobile IP

CDPD	Mobile IP
Home Agent/home function: Using a Location Directory	**Home Agent:** Using a configuration and Registration Table.
No need for mobility binding	Mobility Binding: binding between a mobile host and its attachment agent, registration lifetime, id number, etc.
Attachment Agent: Registration Directory	**Attachment Agent:** Configuration and Registration Table

c) SMS

SMS is the delivery of alphanumeric messages to mobile phones over wireless networks. SMS is not inherently a wireless communication technology. It is a value-added service designed to run on long-range wireless networks.

To many 1G and 2G data networks, it is the only or the most important form of data communication. SMS messages can be sent from a mobile device or from an SMSC (Short Messaging Service Center), routed by an SMSC, and arrive at a suitable destination as an SMS message, an e-mail, or some other form of electronic message.

Two things make SMS fundamentally different from the other data access technologies:

- It can be delivered whether or not there is an ongoing voice call and,
- it is an asynchronous messaging system that allows for flexibility in the temporal behavior of the network and related delivery attributes.

SMS does not require usage of one type of wireless network over the other; it can be implemented over whatever network is available. However, to date, it is primarily implemented on TDMA and CDMA networks.

The figure below shows the basic architecture of a telecommunication infrastructure that can deliver SMS messages.

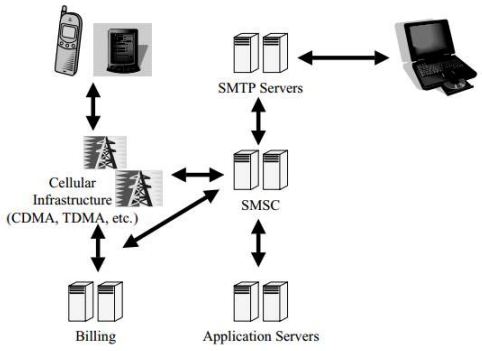


Fig: Basic system diagram for an SMS-enabled system

Most carriers, for security reasons, do not offer third-party connectivity to their SMSC or any connected part of the infrastructure of an SMS system. Unfortunately, this means that the only way for a programmer to write an SMS application is to interface with the carrier's SMTP servers that are then connected to the SMSC.

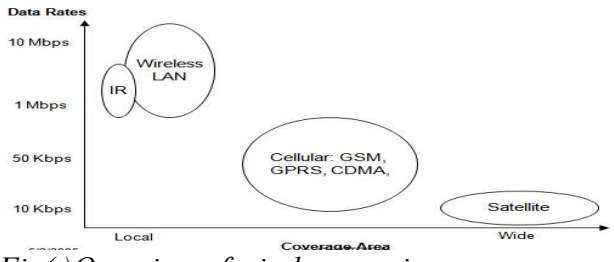
Carriers either create an alias at some domain (user@carrierdomain.com) or the phone number is used (7145555555@carrierdomain.com). In other words, creating an SMS message, as far as we are concerned, is the same as creating an e-mail. On the other hand, With SMS-enabled devices (typically mobile phones and PDAs), you simply compose your short message and address it to the phone number of the recipient and off it goes.

One interesting thing about SMS is that, because of its pervasiveness, it is occasionally used as a text-based application-layer transport protocol. In other words, we can build a mobile application that resides on the device, in one of the environments we have looked at such as J2ME and Windows CE, and use SMS to send and receive messages from some other node on the network.

LESSON 6

MOBILE COMMUNICATION TECHNOLOGIES AND SERVICES

In this lesson, we look at various wireless technologies that are most relevant to mobile computing. Particularly of interest are those in the long range family(we discussed short range in wireless communication protocols). We will look at the various aspects of these technologies individually in this section.



Fig( )Overview of wireless services

1) GSM

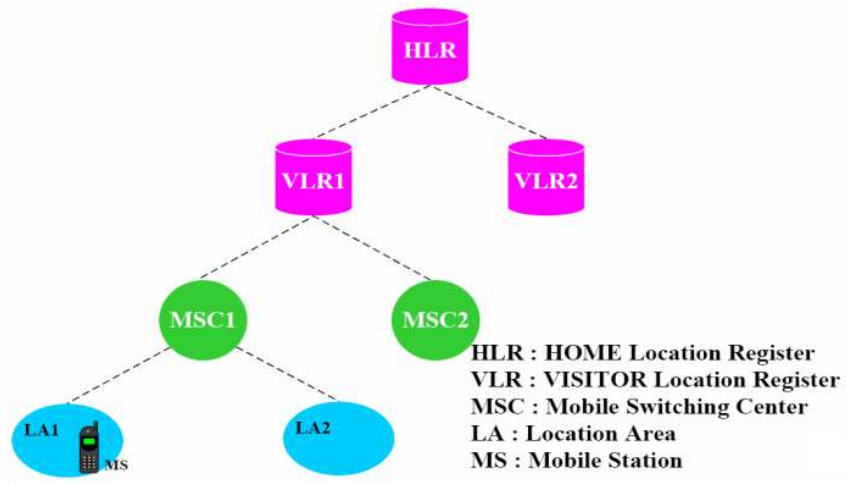
This refers to as Global System for Mobile(GSM) communication and was developed by the Groupe Spéciale Mobile (GSM) which was founded in Europe in 1982.

As a mobile communication standard GSM communication uses cellular networks. The GSM standard (is a 2G standard)operates in the frequency ranges of 900, 1800, and 1900 MHz.

GSM enabled phones enable easy international roaming in GSM networks. GSM is a cellular network, which means that mobile phones connect to it by searching for cells in the immediate vicinity.

Topology

GSM networks track the locations of the mobile subscribers so that incoming calls can be delivered to the subscribers i.e.



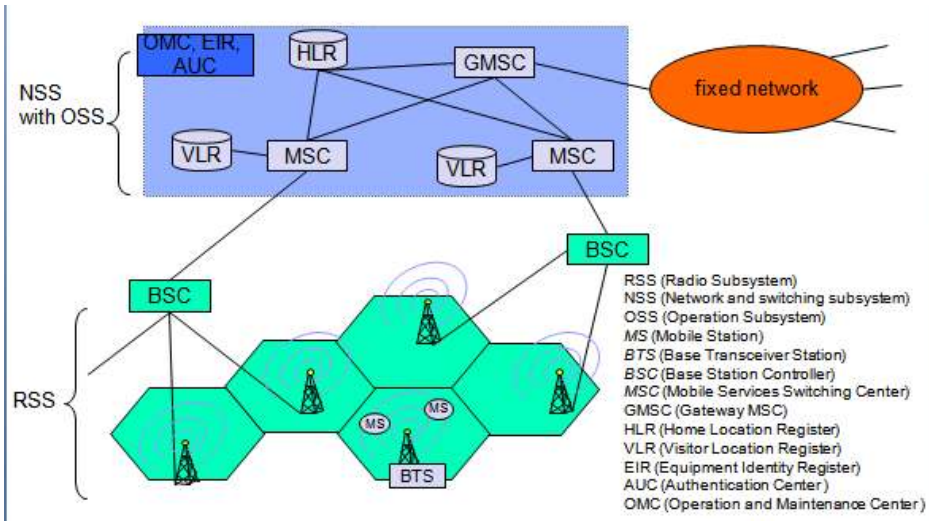
Localization And Calling In Gsm

Worldwide localization of users and roaming are the main service provided by the GSM network system. The system always knows where a user currently is, and the same phone number is valid worldwide. For providing this service GSM updates the user location periodically. The HLR always contains information about the current location. VLR responsible for the MS informs the HLR about location changes. As soon as an MS moves into the new location area (range of new VLR), the HLR sends all user information needed to the new VLR.

To locate an MS and to address the MS, following numbers are needed:

- Mobile station international ISDN number (MSISDN).
- International mobile subscriber identity (IMSI).
- Temporary mobile subscriber identity (TMSI).
- Mobile station7 roaming number (MSRN).

GSM architecture Overview



A mobile service area is partitioned into several location area (LAs) or registration areas.
A LA consists of a group of base transceiver stations(BTSs/BSC) that communicate with the MSs over radio links.

Location update procedure(registration)

BTSs periodically broadcast the corresponding LA address to the MSs. When an MS receives an LA address different from the one stored in its memory, it sends a registration message to the network.

In GSM, registration or location update occurs when an MS moves from one LA to another.

HLR is a database that stores all the relevant subscriber data including mobile subscriber ISDN number , details of subscription permissions such as call forwarding,
roaming, etc., subscriber's ISMI, user's location area, user's current VLR and MSC status.

VLR- dynamic real-time database that stores both permanent and temporary subscriber data which is required for communication between the MSs in the coverage area of the MSC associated with that VLR

GSM services

GSM services constitute a group of capabilities that the service provider offers to the subscribers, which are divided into three categories namely;

a) **Bearer services:** Those that give the subscriber the capacity required to transmit appropriate signals between certain access points i.e. user-network interfaces
b) **Teleservices:** Services which provide the subscriber with necessary capabilities including terminal equipment functions to communicate with other subscribers.
They include: Telephonic-voice at full data rate (13.4 kbps), Fax, SMS, Emergency number 112 for emergency calls.
c) **Supplementary services**: They are services which modify or supplement basic telecommunications services. They are offered together or in association with basic

telecommunications services. They include:1) Caller line forwarding (redirection), caller line identification,2)Line identification to the caller.3)Closed user group formation ,4)Multiparty groupings (e.g., in an enterprise),5)Call holding, call waiting, and barring calls from specified numbers or group,6) Restricted provisioning of certain services to the users ,7) Internet and email access granted on special requests from users & 8)Providing information regarding call charges, remaining phone account balance, etc.

Objectives of the GSM service

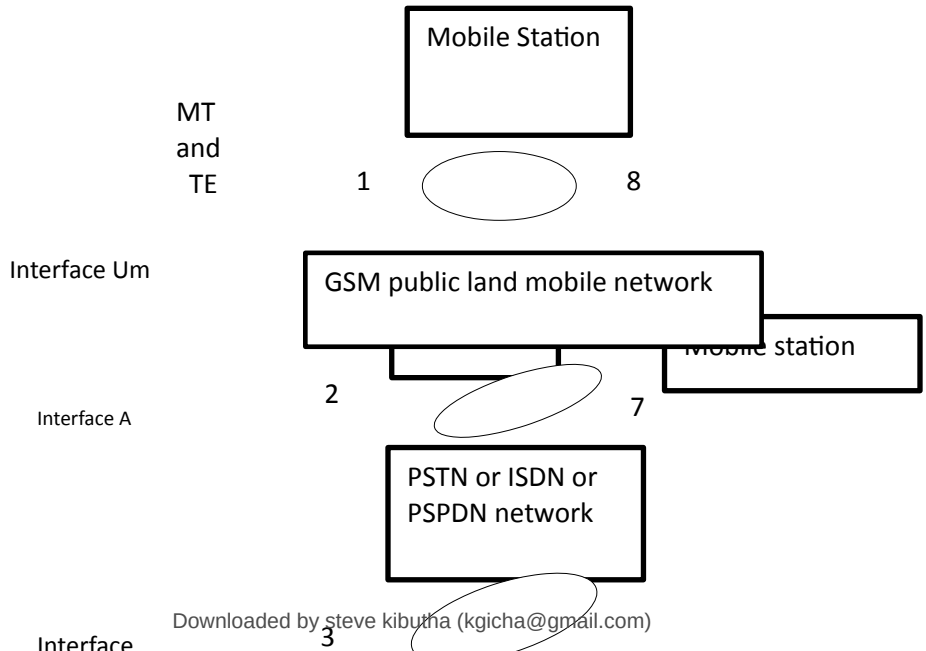
The GSM system offers the opportunity for a subscriber to roam freely through countries where a GSM infrastructure is operational.

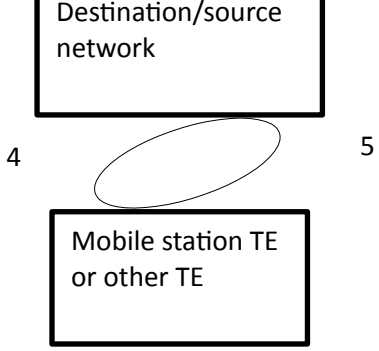
GSM depends upon existing wireline networks to route the calls between mobile subscribers. Generally, the following are the objectives of a GSM network with respect to subscribers' services:

a) Provide voice and non-voice services, that are compatible with those offered by existing networks.
b) To introduce a mobile radio system that is compatible with ISDN.
c) To give access to the GSM network for a mobile subscriber in a country that operates the GSM system.
d) To provide facilities for automatic roaming i.e. locating, and updating of mobile subscribers.
e) To provide for efficient use of the frequency spectrum.

GSM Infrastructure Connection

It is established between two Terminal Equipments(TE) i.e. the source and the destination.
The destination TE may or may not belong to a GSM network.
A mobile terminal acts as an interface between a communications network (for example, interface between the GSM public land mobile network) and terminal, TE ─the source or destination of the service.
The TE is used by a caller to connect and talk (communicate) and MT for mobile communication.
Connection depends on the source–destination network which may be a GSM, PSTN (public switched telephone network), ISDN (integrated services digital network), PSPDN (public switched public data network), or any other network carrying the data to the end-point TE.





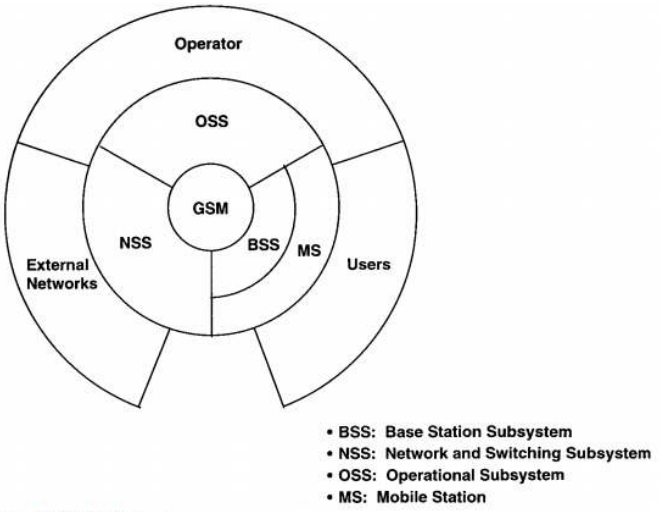
connection between two terminal equipments or mobile terminals

- A caller TE transmits through interface 1 to a GSM public land /mobile network
- Through 2 to a PSTN network
- Through 3 to a source–destination network
- Through 4 to a terminal or mobile station TE
- In place of the PSTN network, there may be an ISDN or PSPDN network
- The connected TE communicates back by transmitting through interfaces 5, 6, 7, and 8

Four sets of interfaces (1, 8), (2, 7), (3, 6), and (4, 5). There is a transceiver in each set
The symbol Um(user mobile interface) conventionally denotes the interface (1, 8)
Symbol A denotes a mobile network interface (2, 7) to a PSTN or other wired network

GSM Subsystems

A series of functions are required to support the services and facilities in the GSM.
The basic subsystems of the GSM architecture are:



In GSM, interaction between the subsystems can be grouped in two main parts:

1) **Operational**. External networks to/from NSS to/from BSS to/from MS to/from subscriber
2) **Control**. OSS to/from service provider

The operational processes provides transmission paths and establishes them. The MS, BSS, and NSS form the operational part of the GSM system.

The control processes interacts with the traffic-handling activity of the operational part by monitoring and modifying it to maintain or improve its functions.

Base Station Subsystem (BSS): BSS provides and manages transmission paths between the MSs and the NSS. It manages the radio interface between MSs and the rest of the GSM system.

Network and Switching Subsystem (NSS): The NSS has the responsibility of managing communications and connecting MSs to the relevant networks or other MSs.

It consists of a number of mobile services switching centres (MSC),which uses the home location register(HLR) and the visitor location register(VLR).

Operational Subsystem (OSS): The OSS provides means for a service provider to control and manage the GSM system.

Mobile Station(MS): It is a hardware and software to transmit and receive GSM data, and a user terminal (TE) through which the user receives and sends the data.

The MS consists of the physical equipment used by the subscriber to access telecommunication services.

Understanding a Mobile Station

Basically, an MS can be divided into two parts:(1) the hardware and software to support radio and human interface functions.(2) terminal/user-specific data in the form of a smart card called subscriber identity module(SIM), which can effectively be considered a sort of logical terminal. The SIM card plugs into the first part of the MS and remains in for the duration of use. Without the SIM card, the MS is not associated with any user and cannot make or receive calls (except possibly an emergency call if the network allows). The SIM card is issued by the mobile service provider after subscription, while the first part of the MS would be available at retail shops to buy.

MS identity

An MS has a number of identities including:

1. **International Mobile Equipment Identity (IMEI), i.e *#06#**

The **IMEI** uniquely identifies the MS equipment. It is assigned by the equipment manufacturer. The IMEI contains 15 digits and carries:

- The Type Approval Code (TAC)—6 digits
- The Final Assembly Code (FAC)—2 digits
- The serial number (SN)— 6 digits
- A Spare (SP)—1 digit

2. **International Mobile Subscriber Identity (IMSI),**

The **IMSI** is stored in the SIM. The SIM card contains all the subscriber-related information stored on the user's side of the radio interface.
The IMSI is assigned to an MS at subscription time. It uniquely identifies a given MS. The IMSI will be transmitted over the radio interface only if necessary.
The IMSI contains 15 digits and includes:

- Mobile Country Code (MCC)—3 digits (home country)
- Mobile Network Code (MNC)—2 digits (home GSM PLMN)
- Mobile Subscriber Identification (MSIN)
- National Mobile Subscriber Identity (NMSI)

The **SIM** carries the following information:

- Authentication Key (128-bit authentication key provided by the service provider)
- Subscriber information e.g. Personal Identity Number(PIN)
- Access control class e.g. Pin Unlocking Key(PUK)
- Additional GSM services
- Location Area Identity (LAI)
- (International Subscriber Identification(IMSI) and Domain Name(ISDN) number.

GSM offers users with good voice quality, call privacy, and network security.
The SIM cards provide the security mechanism for GSM.
SIM cards are like credit cards and identify the user to the GSM network. They can be used with any GSM handset, providing phone access, ensuring delivery of appropriate services to that user and automatically billing the subscriber's network usage back to the home network.

2) General Packet Radio Service(GPRS)

General Packet Radio Service (GPRS) is a Mobile Data Service accessible to GSM mobile phones users. This service is packet-switched and several number of users can divide the same transmission channel for transmitting the data. It is a speed enhanced data transmission service designed for GSM systems. It is often described as "2.5G".

GPRS is also known as GSM-IP (Global-System Mobile Communications Internet Protocol) as it keeps the users of this system online, allows to make voice calls, and access internet on-the-go. Even Time-Division Multiple Access (TDMA) users benefit from this system as it provides packet radio access.

GPRS supersedes the wired connections, as this system has simplified access to the packet data networks like the internet. The packet radio principle is employed by GPRS to transport user data packets in a structure way between GSM mobile stations and external packet data networks. These packets can be directly routed to the packet switched networks from the GPRS mobile stations.

GPRS employs the GSM physical layer which connects mobile stations for voice-data transmission to the Internet where packet data networks have at higher data rate.

Objectives of GPRS

GPRS is the first step toward an end-to-end wireless infrastructure and has the following goals:

1. Open architecture
2. Consistent IP services
3. Same infrastructure i.e. integrated telephony and Internet infrastructure
4. Service innovation independent of infrastructure

Key Features of GPRS

The following key features describe wireless packet data:

- **The always online feature -** Removes the dial-up process, making applications only one click away.
- **An upgrade to existing systems -** Operators do not have to replace their equipment; rather, GPRS is added on top of the existing infrastructure.
- **was an integral part of future 3G systems -** GPRS is the packet data core network for 3G systems EDGE and WCDMA.
- **Packet switching**: Packets of data at any given instant can take multiple (time slots or channels) ; Depending on the idle slots at that instance. The receiver assembles the packets into the original sequence in the data. GPRS is packet-switched which means that multiple users share the same transmission channel, only transmitting when they have data to send.
- GPRS **provides moderate speed data transfer**, by allocating unused cell bandwidth to transmit data.

Usually, GPRS data is billed per kilobytes of information transceived. In 3G mobile systems like UMTS (Universal Mobile Telecommunication System), voice and data services will be mixed in a normal communication.

Benefits of GPRS

- **Higher Data Rate:** In the typical GSM mobile, setup alone is a lengthy process and equally, rates for data permission are restrained to 9.6 kbit/s. The session establishment time offered while GPRS is in practice is lower than one second and ISDN-line data rates are up to many 10 kbit/s.
- **Easy Billing:** GPRS packet transmission offers a more user-friendly billing than that offered by circuit switched services. In circuit switched services, billing is based on the duration of the connection. This is unsuitable for applications with bursty traffic, since the user must pay for the entire airtime, even for idle periods when no packets are sent . In GPRS billing can be based on the amount of transmitted data. The advantage for the user is that he or she can be "online" over a long period of time but will be billed based on the transmitted data volume.

Services offered by GPRS

GPRS has opened a wide range of unique services to the mobile wireless subscriber. Below are some of the characteristics of the services offered:

a) **Mobility -** ability to maintain constant voice and data communications while on the move.
b) **Immediacy -** Allows subscribers to obtain connectivity when needed, regardless of location and without a lengthy login session.
c) **Localization -** Allows subscribers to obtain information relevant to their current location.

Using the above three characteristics varied possible applications were developed to offer to the mobile subscribers, which in general, can be divided into two high-level categories: Corporation and Consumer

These two levels further include:

- **Communications -** E-mail, fax, unified messaging and intranet/internet access, etc.
- **Value-added services -** Information services and games, etc.
- **E-commerce -** Retail, ticket purchasing, banking and financial trading, etc.
- **Location-based applications -** Navigation, traffic conditions, and location finder, etc.
- **Vertical applications -** Freight delivery, fleet management and sales-force automation.
- **Advertising -** Advertising may be location sensitive. For example, a user entering a mall can receive advertisements specific to the stores in that mall.

GPRS Architecture

GPRS architecture works on the same procedure like GSM network, but, has additional entities that allow packet data transmission. Along with the packet data transport the GSM network accommodates multiple users to share the same air interface resources concurrently.

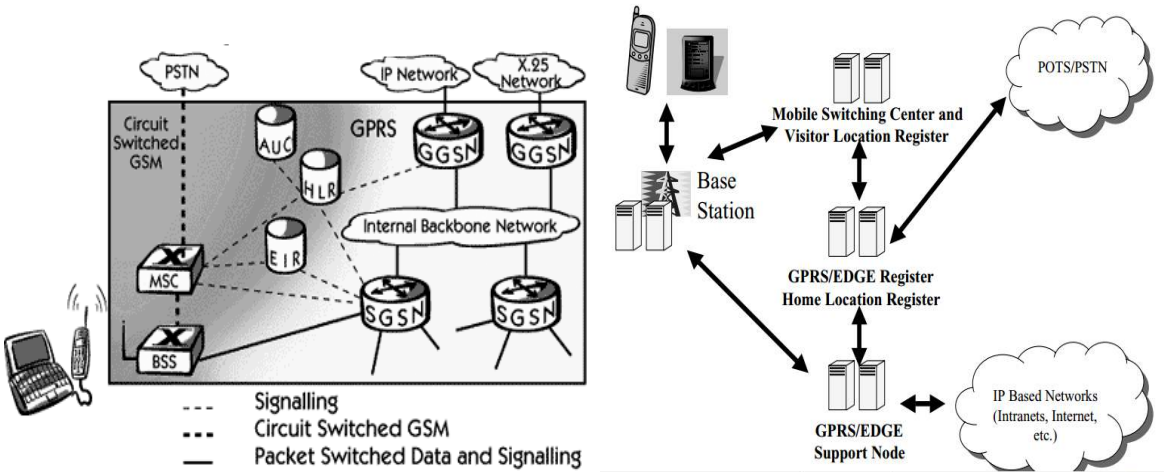
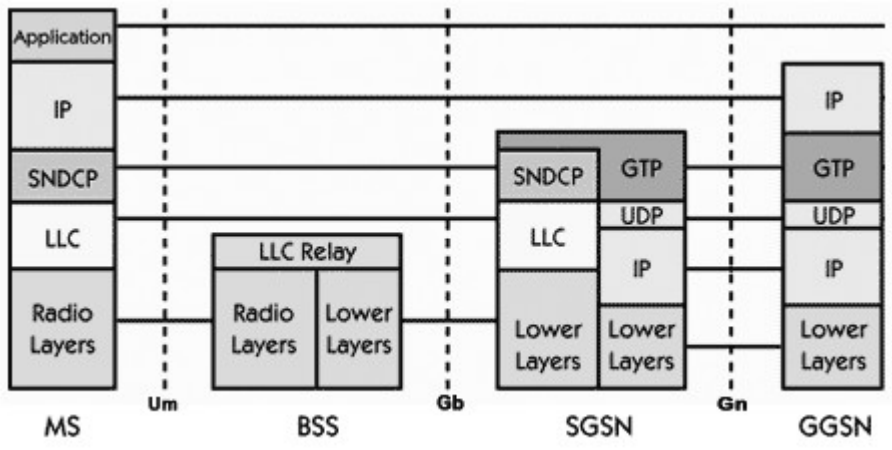


Fig: GPRS system Architecture diagram

GPRS attempts to reuse the existing GSM network elements as much as possible, but to effectively build a packet-based mobile cellular network, some new network elements, interfaces, and protocols for handling packet traffic are required. Therefore, GPRS requires modifications to numerous GSM network elements as summarized below:

GSM Network Element	Modification or Upgrade Required for GPRS.
Mobile Station (MS)	New Mobile Station is required to access GPRS services, and will be backward compatible with GSM for voice calls.
BTS	A software upgrade is required in the existing Base Transceiver Station(BTS).
BSC	The Base Station Controller (BSC) requires a software upgrade and the installation of new hardware called the packet control unit (PCU),which directs the data traffic to the GPRS network.
GPRS Support Nodes (GSNs)	The deployment of GPRS requires the installation of new core network elements called the Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN).
Databases (HLR, VLR, etc.)	All the databases involved in the network will require software upgrades to handle the new call models and functions introduced by GPRS.

GPRS Protocols



The process that takes place in the application looks like a normal IP sub-network for the users both inside and outside the network. The application communicates via **standard IP**, that is carried through the GPRS network and out through the gateway of GPRS. The packets that are mobile between the GGSN and the SGSN use the GPRS tunneling protocol(), this way the IP addresses located on the external side of the GPRS network do not have to deal with the internal backbone. UDP and IP are run by **GTP**.

Sub-Network Dependent Convergence Protocol (SNDCP) and **Logical Link Control (LLC)** combination is used in between the SGSN and the MS. The SNDCP flattens data to reduce the load on the radio channel. A safe logical link by encrypting packets is provided by LLC and the same LLC link is used as long as a mobile is under a single SGSN.

In case, the mobile moves to a new routing area that lies under a different SGSN; then, the old LLC link is removed and a new link is established with the new Serving GSN X.25. Services are provided by running X.25 on top of TCP/IP in the internal backbone.

3) Voice over IP (VoIP)

It refers to Internet Telephony or the technique of transporting voice over IP networks.

Adding voice to packet networks generates many challenges including:

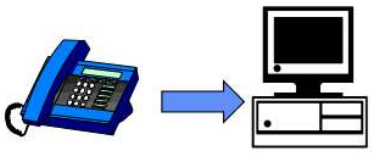
- interoperability
- packet loss
- delay
- scalability
- reliability
- quality

The underlying network must meet strict performance criteria including: minimizing call rejections, network latency, packet loss and disconnects.

Call control (signaling) must make the telephone calling process transparent so that the callers need not know the technology involved.

In VoIP, the system management, security and accounting are consolidated with PSTN OSSs.

This set the standards development and the design of terminals and gateways and the rolling out of services on a global scale.

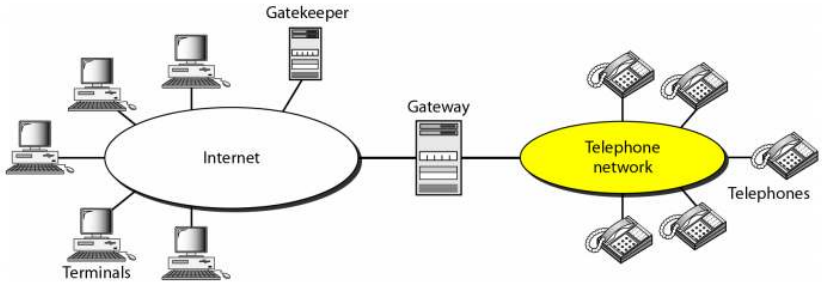


Architecture

The simplest IP telephone system uses two basic components:

IP telephone: end device allowing humans to place and receive calls.

Media Gateway Controller: providing overall control and coordination between IP phones; allowing a caller to locate a callee (e.g. call forwarding)



VoIP protocols

There are currently four families of VoIP protocols:

1) Session Initiation Protocol(SIP) which is used for call control. The call control protocols establish, modify and release connections.
2) Session Description Protocol(SDP) that is used to describe the "media" session inside of SIP and other protocols.
3) Real Time Streaming Protocol(RTSP) used to set up streaming sessions e.g. performing signaling Compression- a solution for compressing messages generated by application protocols such as SIP and RTSP.
4) Multiplexing protocol for circuit-based multimedia communications system. Packet-based multimedia communications systems.
5) Media Gateway Control Protocol(H248/MEGACO).

How Transmission Happens

SIP defines three main elements that comprise a signaling system:

User Agent: IP phone or applications

Location servers: store information about a user's location or IP address

Support servers which include:

- *Proxy Server*: forwards requests from user agents to another location.
- *Redirect Server*: provides an alternate called party's location for the user agent to contact.
- *Registrar Server:* receives user's registration requests and updates the database that location server consults.

SIP Operates at the Application Layer.

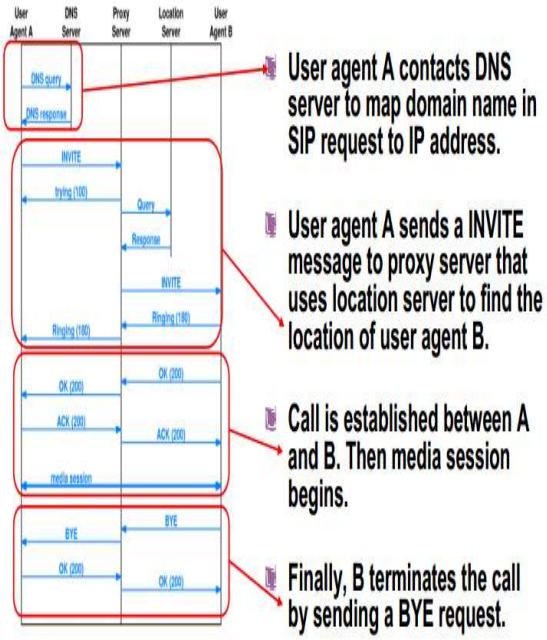
It encompasses all aspects of signaling, e.g. location of called party, ringing a phone, accepting a call, and terminating a call.

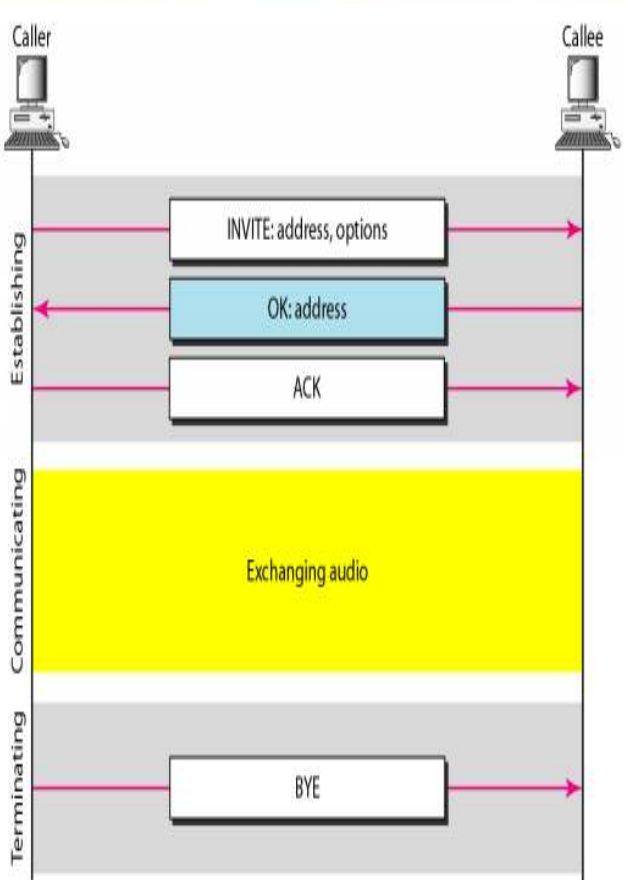
Provides services such as call forwarding.

Relies on multicast for conference calls.

Allows two sides to negotiate capabilities and choose the media and parameters to be used.

SIP URI is similar to an email address. (With prefix "sip:") E.g. sip:bob@somewhere.com

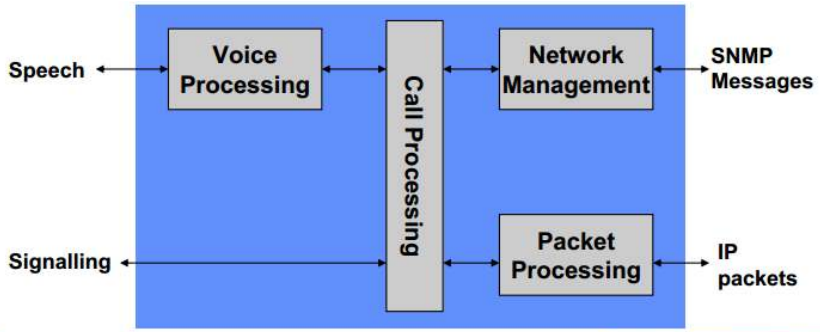




A example of a SIP Session

There are three basic SIP message formats:

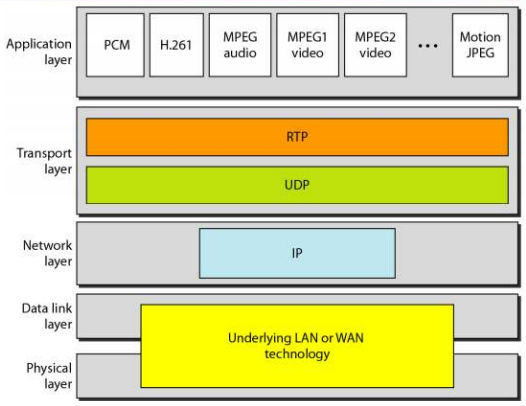
The following picture shows the functional components of terminals that use the H.323 standards:



RTP - Real-time Transport Protocol:- A real time end to end protocol utilizes existing transport layers for data that has real time properties. Takes the bit stream generated by the media encoder breaking it into packets, sending the packets over the network and recovering the bit stream at the receiver.

It plays a key role in Internet telephony since it is the component that moves the actual voice among the participants.

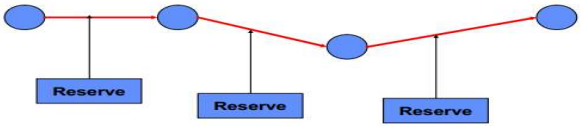
Signalling protocols provide the parameters for RTP transport.



Note: TCP, is not suitable for interactive multimedia traffic because we cannot allow retransmission of packets. UDP is more suitable than TCP for interactive traffic. However, we

need the services of RTP, another transport layer protocol, to make up for the deficiencies of UDP.

RSVP Protocol: - It is a general purpose signaling protocol that allows network resources to be reserved for a connectionless data stream, based on receiver controlled requests.



Applications of VoIP

1) Internet aware telephones: Enhancement of ordinary telephones to serve as an Internet access device as well as ordinary telephony. Directory services could be accomplished via the Internet.
2) PSTN Gateways: PC based telephone accessing a public network by calling a gateway at a point close to the destination to minimize long distance charges.
3) Remote access from branch or home: Small office could gain access to corporate voice, data and fax.
4) Voice calls from a mobile PC via the Internet.
5) Internet call centers.

4) Satellite Networks

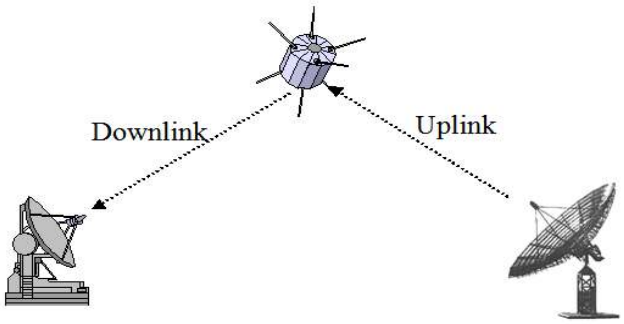
Satellites are specifically made for telecommunication purpose. They are used for mobile applications such as communication to ships, vehicles, planes, hand -held terminals and for TV and radio broadcasting. They are responsible for providing these services to an assigned region (area) on the earth.

- Like cellular systems, except that the base stations (i.e., satellites) move as will mobile devices.
- Satellite coverage attractive for areas of world not well served by existing terrestrial infrastructure: ocean areas, developing countries

A satellite works most efficiently when the transmissions are focused within a desired area. When the area is focused, then the emissions don " t go outside that designated area and thus minimizing the interference to the other systems i.e. more efficient spectrum usage.

Satellites should be designed by keeping in mind its usability for short and long term effects throughout its life time.

The earth station should be in a position to control the satellite if it drifts from its orbit or if it is subjected to any kind of drag from the external forces.



Small rocket boosters on each satellite keep them flying in the correct path. The satellites have a lifetime of about 10 years until all their fuel runs out.

In a communications satellite, the equipment which provides the connecting link between the satellite's transmit and receive antennas is referred to as the **transponder**.

A transponder is capable of :

a) Receiving uplinked radio signals from earth satellite transmission stations (antennas).
b) Amplifying received radio signals
c) Sorting the input signals and directing the output signals through input/output signal multiplexers to the proper downlink antennas for retransmission to earth satellite receiving stations (antennas).

Types of Satellites

There are 2 kinds of manmade satellites in the sky above:

1. One that ORBITS the earth once or twice a day e.g. space shuttle, the international space station and the Global Positioning System(GPS)
2. A communications satellite which is PARKED in a STATIONARY position 35,900 km above the equator of the STATIONARY earth.

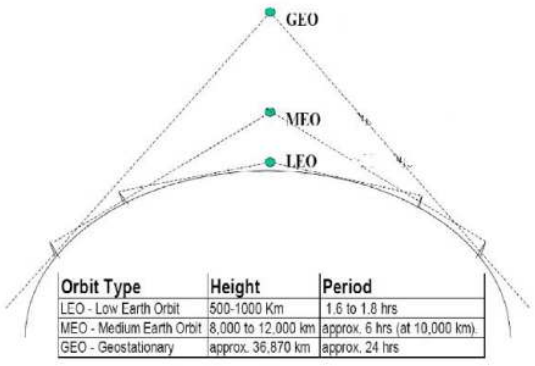
In general, satellites can be grouped in three categories:

- **LEO:** Low Earth Orbit satellites have a small area of coverage. They are positioned in an orbit approximately 3000km from the surface of the earth. They complete one orbit every 90 minutes. The large majority of satellites are in low earth orbit. The satellite in LEO orbit is visible to a point on the earth for a very short time.
- **MEO:** Medium Earth Orbit satellites have orbital altitudes between 3,000 and 30,000 km. They are commonly used in navigation systems such as GPS
- **GEO:** Geosynchronous (Geostationary) Earth Orbit satellites are positioned over the equator. The orbital altitude is around 30,000 -40,000 km There is only one geostationary orbit possible around the earth, lying on the earth's equatorial plane.

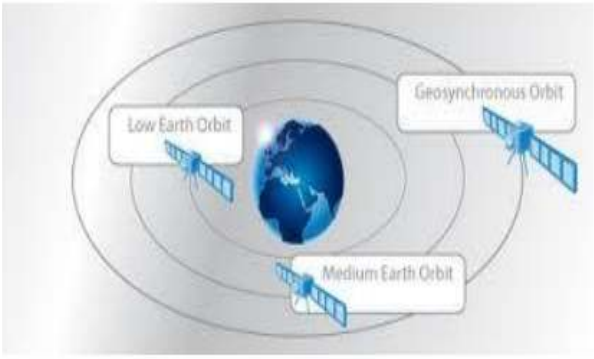
While satellites are in no danger of bumping in to one another yet, they must be spaced around the circle so that their frequencies do not interfere with the functioning of their nearest neighbors.

The satellite orbit at the same speed as the rotational speed of the earth on its axis. They complete one orbit every 24 hours. This causes the satellite to appear stationary with respect to a point on the earth, allowing one satellite to provide continual coverage to a given area on the earth's surface

One GEO satellite can cover approximately 1/3 of the world's surface. They are commonly used in communication systems



Orbit Type	Height	Period
LEO - Low Earth Orbit	500-1000 Km	1.6 to 1.8 hrs
MEO - Medium Earth Orbit	8,000 to 12,000 km	approx. 6 hrs (at 10,000 km)
GEO - Geostationary	approx. 36,870 km	approx. 24 hrs



LEO,MEO and GEO range

Some **General applications of Satellites** include: Weather Forecasting, Radio and TV Broadcast, Military Satellites, Navigation Satellites, Connecting Remote Area , Global Mobile Communication etc

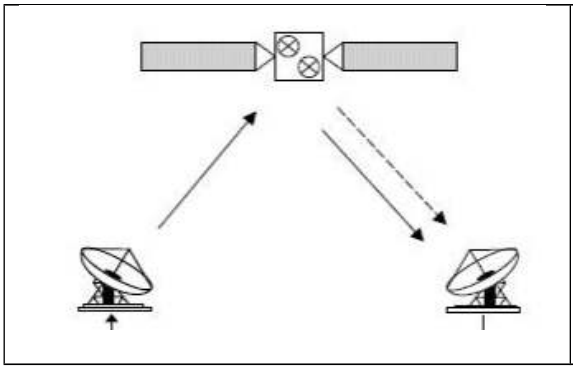
Satellite Access

Communications satellites are used to carry telephone, video, and data signals, and can use both analog and digital modulation techniques.

- **Modulation:** Modification of a carrier's parameters (amplitude, frequency, phase, or a code) in dependence on the symbol to be sent.
  Modulation modifies an RF Carrier signal so that it contains input signal information like : Amplitude, Frequency, Phase and Polarization.
  The Modulation Techniques employed include:(1)BPSK - Binary Phase Shift Keying,(2) QPSK - Quadriphased Phase Shift Keying,(3)FSK - Frequency Shift Keying,(4)MFSK - Multiple FSK and (4)DPSK - Differential Phase Shift Keying.
- **Multiplexing:** The task of multiplexing is to assign space, time, frequency, and code to each communication channel with a minimum of interference and a maximum of medium utilization. Multiple Access Strategies include; FDMA , TDMA or CDMA
- **Communication channel:** Electromagnetic (EM) radiation/ EM waves generated by a satellite device can be detected by another located at some distance away.

By controlling certain aspects of the radiation (through modulation), useful information can be embedded in the EM waves and transmitted from one device to another.

A communication link refers to an association of sender(s) and receiver(s) that want to exchange data, using one of several constellations of a carrier's parameters defined by the used modulation scheme.



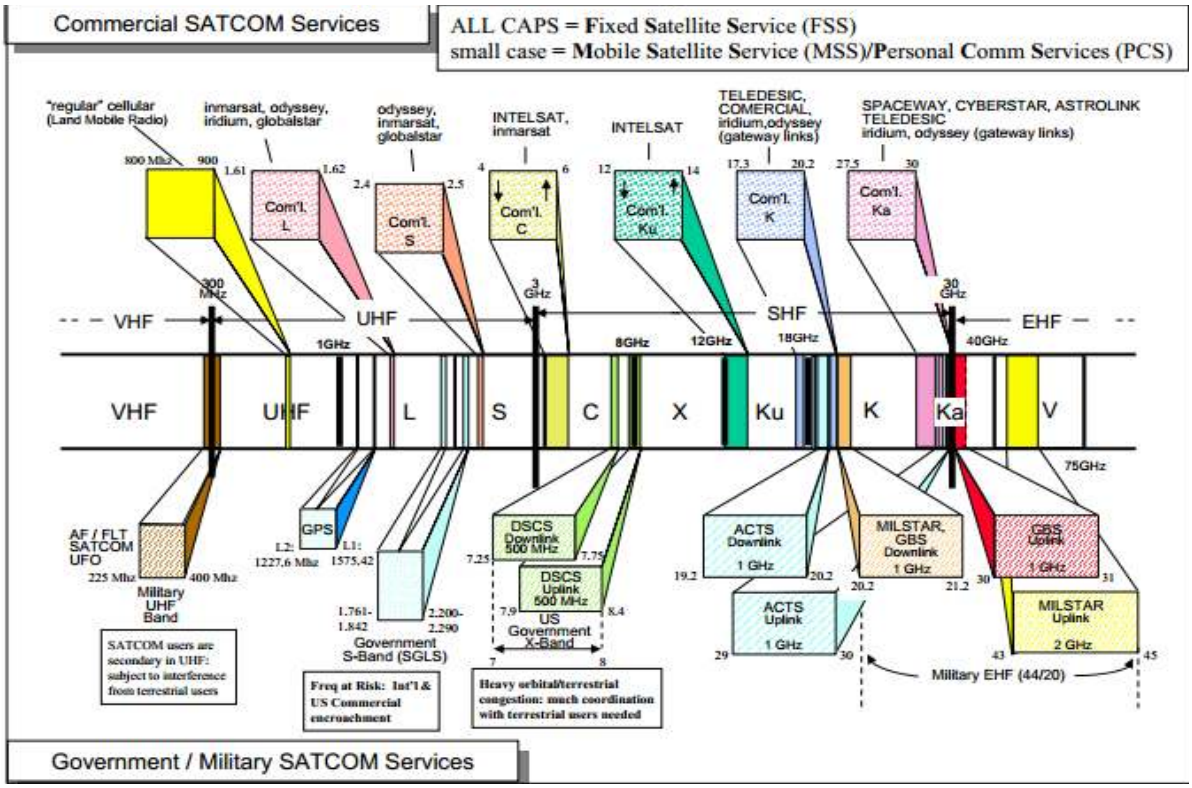
Link Design Process

First define requirements for each link. To design Each Link;

- ✓ Select frequency
- ✓ Select modulation & coding scheme
- ✓ Apply antenna size & beam width constraints
- ✓ Estimate atmospheric, rain attenuation
- ✓ Estimate received noise, interference power
- ✓ Calculate required antenna gain & transmitter power

System Noise which is external to signal receptors includes; Galactic noise, Clouds, rain in path, Solar noise , Man-made noise, Nearby objects, Satellite structure **and Attenuation**(The atmosphere absorbs some frequencies during communication. Clouds and rain reduces signal availability.)

Frequencies Usage



Factors which determine Frequency selection

1) Spectrum availability and FCC allocation

2) Relay/Ground Station frequency
3) Antenna size
4) Atmospheric/Rain attenuation
5) Noise temperature
6) Modulation and coding

The receiver antennas can be: Parabolic dish,Helix, Horn Phased Arrays;- Multiple beams or Hopping beams

Analog vs. Digital Transmission

In analog transmission (e.g. television broadcast) by satellite, the baseband video signal and one or two audio subcarriers constitute a composite video signal. Digital data are digitized analog signals, which may conveniently share a channel, allowing a link to carry a varying mix of voice and data traffic.

Digital modulation is obviously the modulation of choice for transmitting. Digital signals from different channels are interleaved for transmission through time division multiplexing (TDM) , and can carry any type of traffic.

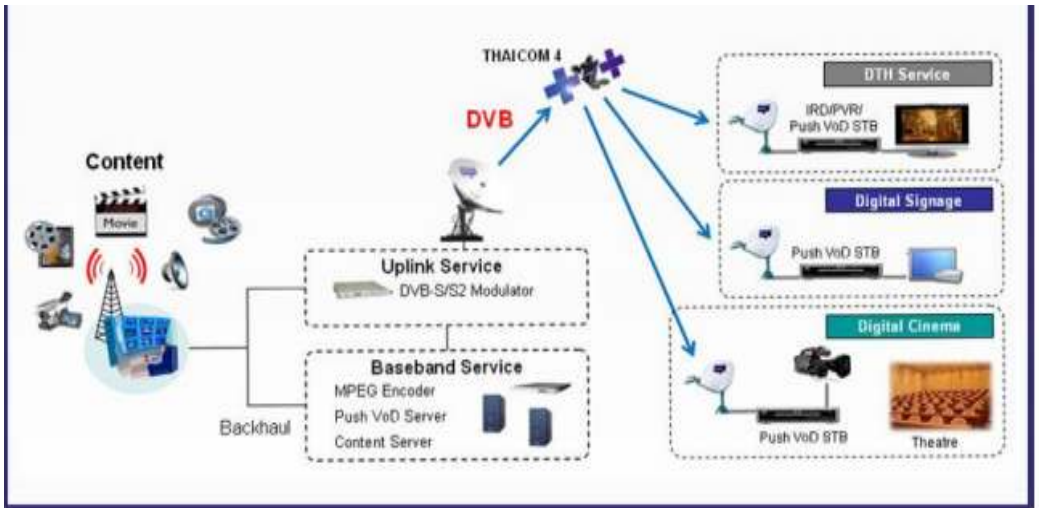
We compare at two levels:

a) Data—continuous (audio) vs. discrete (text)
b) Signaling—continuously varying electromagnetic wave vs. sequence of voltage pulses.

Advantages of Digital Communication

1) Less distortion and interference
2) Easy to regenerate
3) Low error rates results to high data integrity.
4) Multiple streams can be easily multiplexed into a single stream hence large channel capacities with digital communication system.
5) Security. It is easy to apply encryption to digital data.
6) Drift free, miniature, low power hardware
7) Better integration if all signals are in one form. Can integrate voice, video and digital data.

Example: **Digital Video Broadcasting (DVB):** Digital Video Broadcasting (DVB) has become the synonym for digital television and for data broadcasting world -wide.



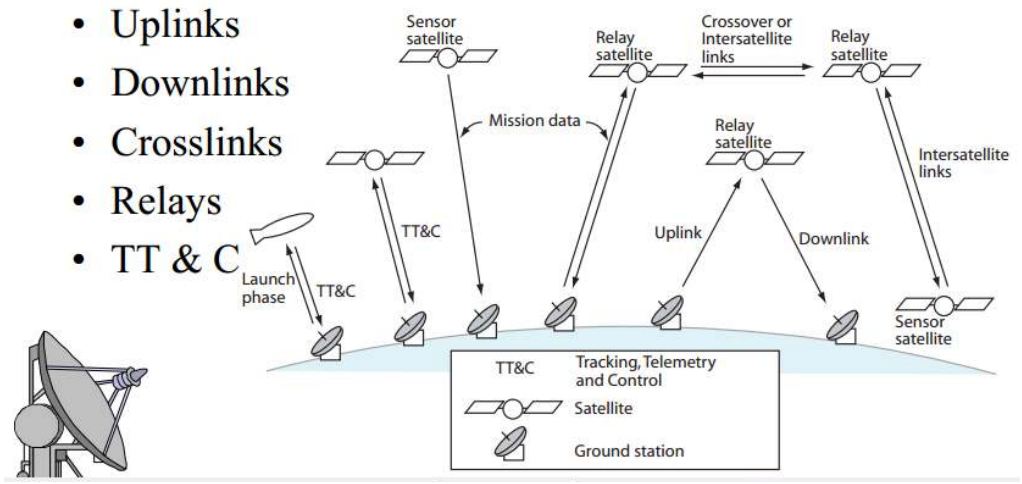
Digital Video Broadcasting systems

The transmission from the BS in the downlink can be heard by each and every mobile user in the cell, and is referred as **broadcasting**. Transmission from the mobile users in the uplink to the BS is many-to-one, and is referred to as **multiple access**. Multiple access schemes allow many users to share simultaneously a finite amount of radio spectrum resources. They should not result in severe degradation in the performance of the system as compared to a single user scenario. Approaches that can be broadly grouped into two categories: narrowband and wideband.

Satellite Communications Architecture

The communications architecture consists of satellites and ground stations interconnected with communications links. A satellite communications system can be broadly divided into two segments—a **ground segment and a space segment**.

A. Space Segment — Satellites orbiting the earth: The space segment will obviously include the satellites, but it also includes the ground facilities needed to keep the satellites operational, these being referred to as the tracking, telemetry, and command (TT&C) facilities. In many networks it is common practice to employ a ground station solely for the purpose of TT&C.



A satellite's design includes;

- Onboard Processing
- Autonomous Satellite Control
- Network Management

The control segment tracks the satellites and then provides them with corrected orbital and time information. The control segment consists of five unmanned monitor stations and one Master Control Station. The five unmanned stations monitor GPS satellite signals and then send that information to the Master Control Station where anomalies are corrected and sent back to the GPS satellites through ground antennas.

Defined by Function **a satellite's system function** can be used for;

- Tracking, Telemetry & Command
- Data Collection
- Data Relay

Telemetry:- Voltages, currents, temperatures, accelerations, valve and relay states
Commanding:- Low data rate, 2.) Store, verify, execute or execute on time,3.) Programmable control

Some examples of the existing TT&C Systems:- 1.)AFSCN (SGLS) - AF Satellite Control Network (Space Ground Link System). 2.)NASA DSN - Deep Space Network.3.) Intelsat/ COMSAT 4.) TDRS - Tracking and Data Relay Satellite

B. Earth Segment : The earth segment of a satellite communications system consists of the transmit and receive earth stations e.g. home TV receive-only (TVRO) systems and terminal stations used for international communications networks.
Also included in the earth segment are those stations which are on ships at sea, and commercial and military land and aeronautical mobile stations.

The function of an earth station is to receive information from or transmit information to, the satellite network .

The design of earth station configuration depends upon many factors and its location. These factors include:

- Type of services
- Frequency bands used
- Function of the transmitter
- Function of the receiver
- Antenna characteristics

The location of an earth station can be; *In land, On a ship at sea or Onboard aircraft*

Any earth station consists of four major subsystems: ***Transmitter, Receiver , Antenna & Tracking equipment***

Two other important subsystems are: Terrestrial interface equipment & Power supply

The functional elements of a basic digital earth station are shown in the below figure:

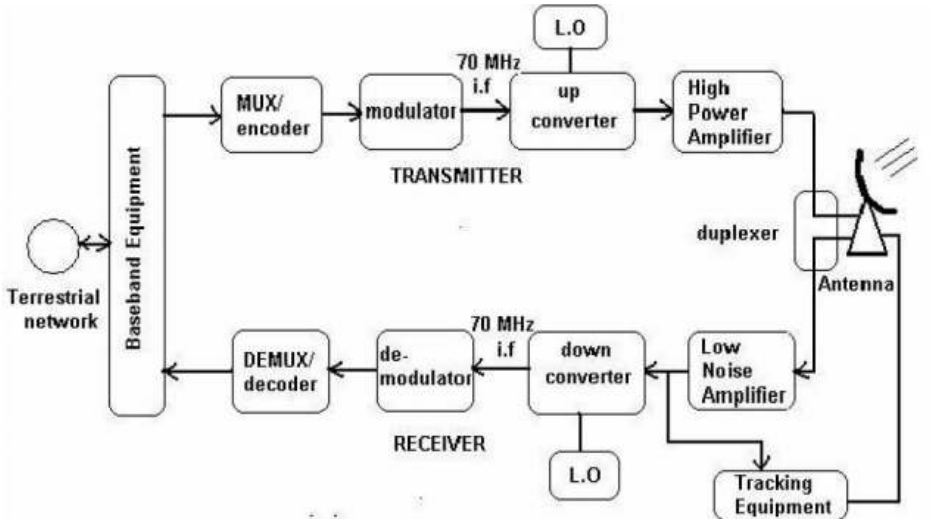


Fig: Satellite Transmitter-Receiver diagram

Earth Station Tracking System:- Tracking is essential when the satellite drift, as seen by an earth station antenna is a significant fraction of an earth station's antenna beam width.

Antenna System:- The antenna system consist of:

a) Feed System: The feed along with the reflector is the radiating/receiving element of electromagnetic waves.

b) Antenna Reflector: Mostly parabolic reflectors are used as the main antenna for the earth stations because of the high gain available from the reflector and the ability of focusing a parallel beam into a point at the focus where the feed, i.e., the receiving/radiating element is located .

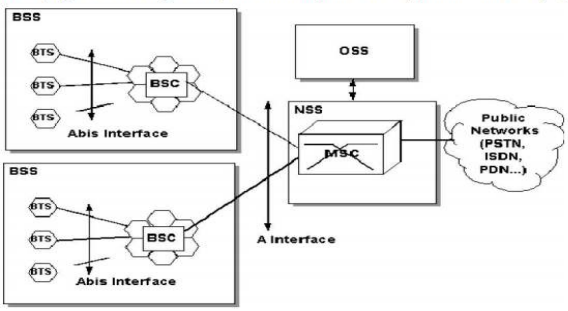
c) Antenna Mount: Type of antenna mount is determined mainly by the coverage requirement and tracking requirements of the antenna systems.

d) Antenna tracking System: An earth station's tracking system is required to perform some of the functions such as, i)Satellite acquisition, ii)Automatic tracking, iii)Manual tracking and iv)Program tracking.

Mobile Satellite services

(1) GSM : GSM allows cellular communications systems to move beyond the limitations posed by the older analog systems. By using digital encoding techniques, more users can share the same frequencies than had been available in the analog systems.

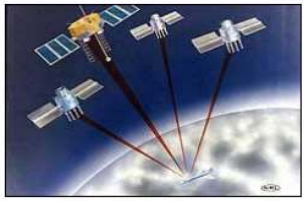
While the frequencies and link characteristics of these systems differ from the standard GSM air interface, all of these systems must deal with users roaming from one cell (or satellite beam) to another, and bridge services to public communication networks including the Public Switched Telephone Network (PSTN), and public data networks (PDN) .



GSM uses General Packet Radio Service (GPRS) for data transmissions like browsing the web.

(2) Global Positioning System (GPS): The Global Positioning System (GPS) is a satellite based navigation system that can be used to locate positions anywhere on earth.

Designed and operated by the U.S. Department of Defense, it consists of satellites, control and monitor stations, and receivers. GPS receivers take information transmitted from the satellites and uses triangulation to calculate a user's exact location.



GPS is used on incidents in a variety of ways, such as:

- To determine position locations; for example, you need to radio a helicopter pilot the coordinates of your position location so the pilot can pick you up.
- To navigate from one location to another.
- To create digitized maps.
- To determine distance between two points or how far you are from another location.

How GPS Determines a Position:

Anyone can buy a receiver and track their exact location by using a GPS receiver. The GPS receiver uses the following information to determine a position :

- **Precise location of satellites:** When a GPS receiver is first turned on, it downloads orbit information from all the satellites called an almanac. This process, the first time, can take as long as 12 minutes; but once this information is downloaded, it is stored in the receiver's memory for future use.
- **Distance from each satellite:** The GPS receiver calculates the distance from each satellite to the receiver by using the distance formula: distance = velocity x time.
- **Triangulation to determine position:** The receiver determines position by using triangulation. When it receives signals from at least three satellites the receiver should be able to calculate its approximate position (a 2D position). The receiver needs at least four or more satellites to calculate a more accurate 3D position.

E.g. Satellite Navigation System in Flights management

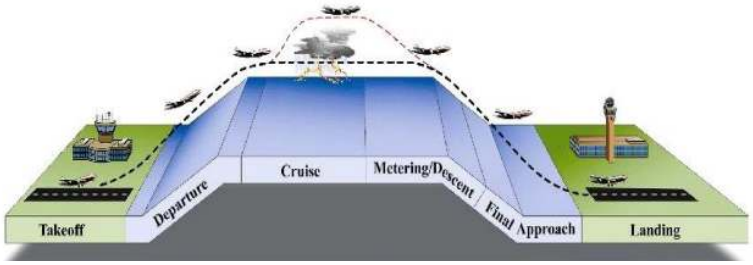


Fig: LEO, MEO and GEO orbits

Benefits:

- Enhanced Safety
- Increased Capacity
- Reduced Delays

(3) Direct Broadcast satellites (DBS): Satellites provide broadcast transmissions in the fullest sense of the word, because antenna footprints can be made to cover large areas of the earth.

The idea of using satellites to provide direct transmissions into the home has been around for many years, and the services pro- vided are known generally as direct broadcast satellite (DBS) services.

Broadcast services include audio, television, and Internet services.

(4) Satellite-email services: The addition of Internet Access enables a satellite to act as an Internet Service Provider (ISP) capable of offering users a tailor -made Internet connection.

With Internet services added to our range of terrestrial networks, you don't need to subscribe to a third party for Internet access.

Satellite Internet generally relies on three primary components:

- a satellite in geostationary orbit ,
- a number of ground stations known as gateways that relay Internet data to and from the satellite via radio waves (microwave), and
- a VSAT (very-small aperture terminal) dish antenna with a transceiver, located at the subscriber's premises.

Other components of a satellite Internet system include a modem at the user end which links the user's network with the transceiver, and a centralized network operations center (NOC) for monitoring the entire system.

LESSON 7

WIRELESS APPLICATION PROTOCOL(WAP) AND WAP ENVIRONMENT

Limitations of Internet for wireless applications:	**Mobile software development considerations**
• Low bandwidth • High latency • Limited connection stability	• Input device may be harder to manipulate • Sound may be limited • Storage/processing ability could be slower • Small display size, since display is limited • Create apps with limited memory • Create apps with limited processing power

Wireless Application Protocol(WAP)

WAP (Wireless Application Protocol) is a specification for a set of communication protocols to standardize the way that wireless devices, such as cellular phones and radio transceivers, can be used for Internet access, to provide services including: e-mail, the World Wide Web, newsgroups, and instant messaging.

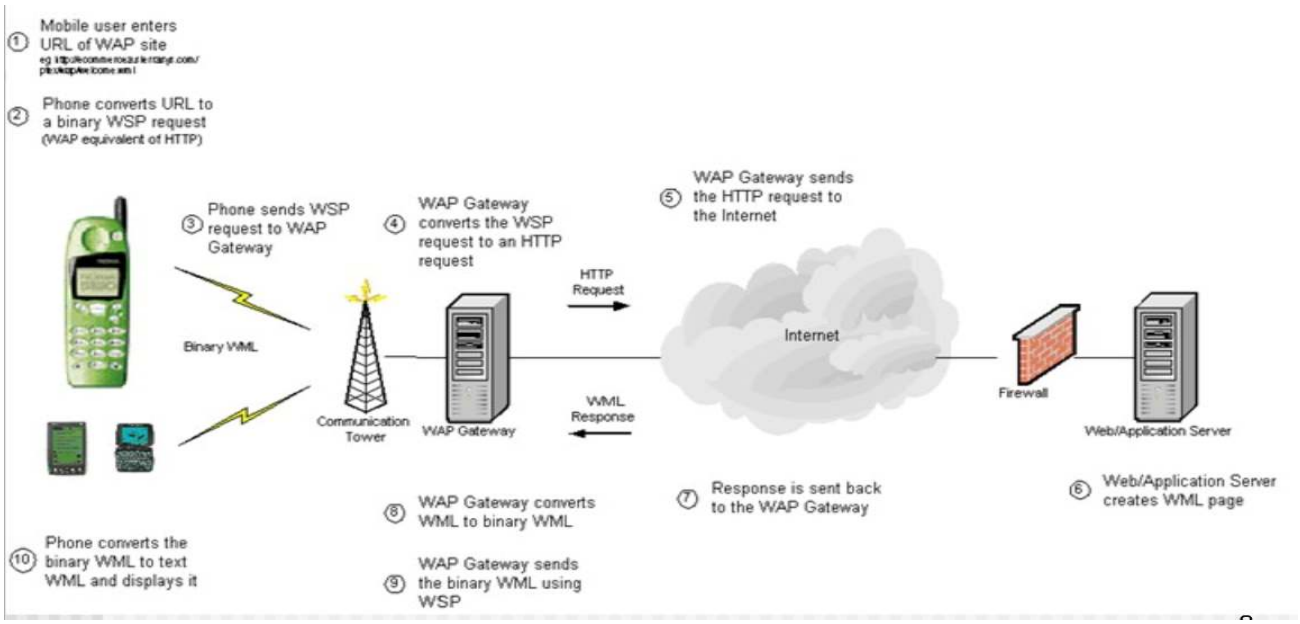
Wireless application protocol (WAP) is a communications protocol that is used for wireless data access through most mobile wireless networks.

WAP enhances wireless specification interoperability and facilitates instant connectivity between interactive wireless devices (such as mobile phones) and the Internet. WAP functions in an open application environment and may be created on any type of OS.

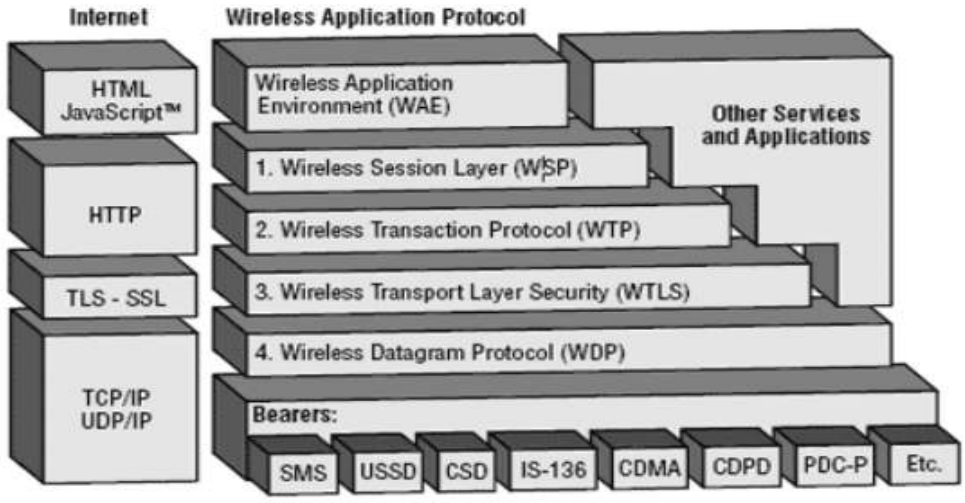
The WAP architecture

WAP Infrastructure consists of:

a. Mobile client
b. A public land mobile network like GSM, etc
c. A public telephony network
d. A WAP gateway
    i. Protocol conversion
    ii. Content encoding
e. An IP network
f. A WAP application server



Just like the internet, WAP is designed in a layered fashion, so that it can be extensible, flexible, and scalable. As a result, the WAP protocol stack is divided into five layers as shown in the diagram below:

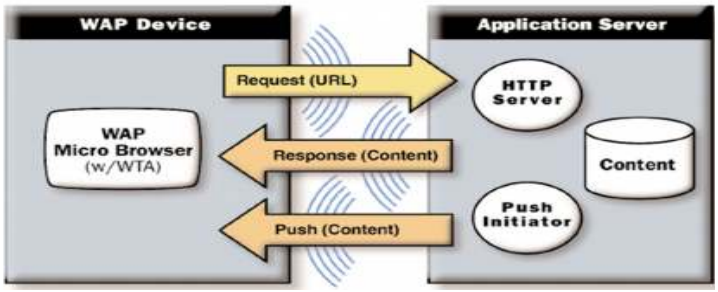


1. **Application Layer(Wireless Application Environment):-** This layer is of most interest to content developers because it contains among other things, device specifications, and the content development programming languages, WML, and WMLScript.
2. **Session Layer(Wireless Session Protocol) :-** Unlike HTTP, WSP has been designed to provide fast connection, suspension and reconnection.
3. **Transaction Layer (Wireless Transaction Protocol):-** 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.

4. **Security Layer(Wireless Transport Layer Security):-** 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.
5. **Transport Layer(Wireless Datagram Protocol):-** 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.

   In the WAP architecture, each of the above layers provides a well-defined interface to the layer above it. Meaning that the internal workings of any layer are transparent or invisible to the layers above it.

   The layered architecture allows other applications and services to utilize the features provided by the WAP stack as well; thus making it possible to use the WAP-stack for services and applications that currently are not specified by WAP.



The WAP programming Model

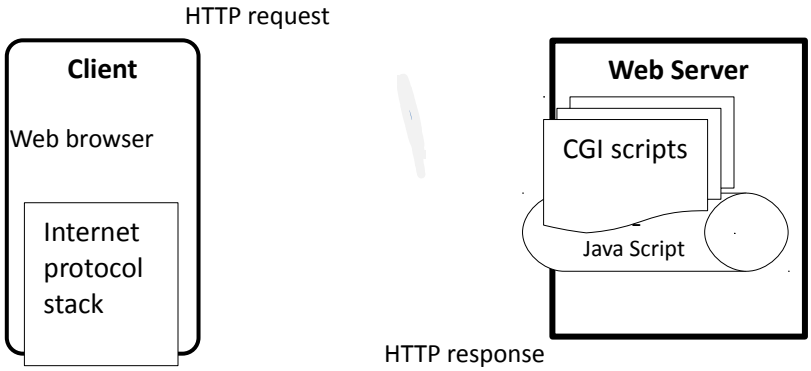
WAP Model

WAP is a sub system of the internet model. We begin by examining the internet model.

The Internet model

Internet model makes it possible for a client to reach services on a large number of origin servers, each addressed by a unique Uniform Resource Locator (URL).

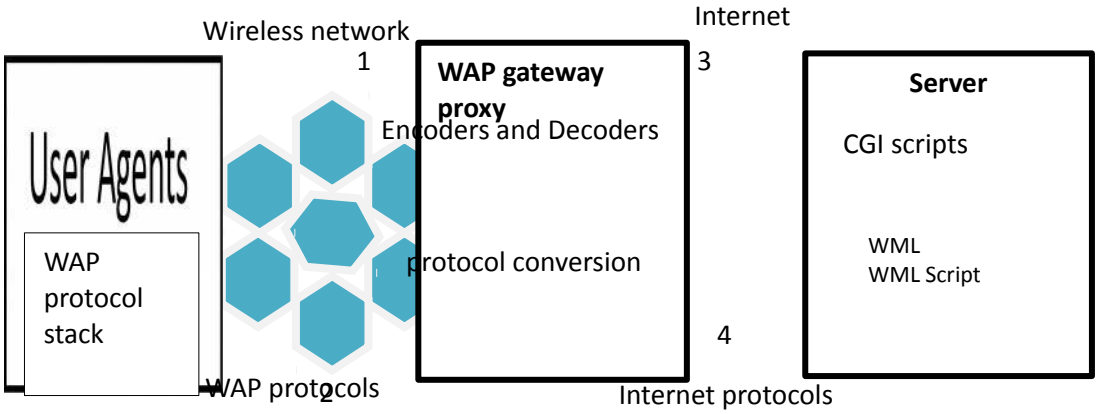
On the web, hype-text markup language(HTML) provides the content developer with a means to describe the appearance of a service in a flat document structure i.e. a webpage. If more advanced features like procedural logic are needed, then scripting languages such as JavaScript or VB Script may be utilized.



The content available at the web server may be static or dynamic. Static content is produced once and not changed or updated very often e.g. a standard presentation, while Dynamic content is needed when the information provided by the service changes more often like news, stock quotes, and account information. Technologies such as Active Server Pages (ASP), Common Gateway Interface (CGI), and Servlets allow content to be generated dynamically.

The WAP Environment/Model

This is similar to the internet model, apart from an additional layer called the WAP gateway.
WAP Gateway is a proxy or the entity that connects the wireless domain with the Internet.
The request that is sent from the wireless client to the WAP Gateway/Proxy uses the Wireless Session Protocol WSP-which is a binary version of HTTP.
A markup language - the Wireless Markup Language (WML) has been adapted to develop optimized WAP applications. In order to save valuable bandwidth in the wireless network, WML can be encoded into a compact binary format. Encoding WML is one of the tasks performed by the WAP Gateway/Proxy.

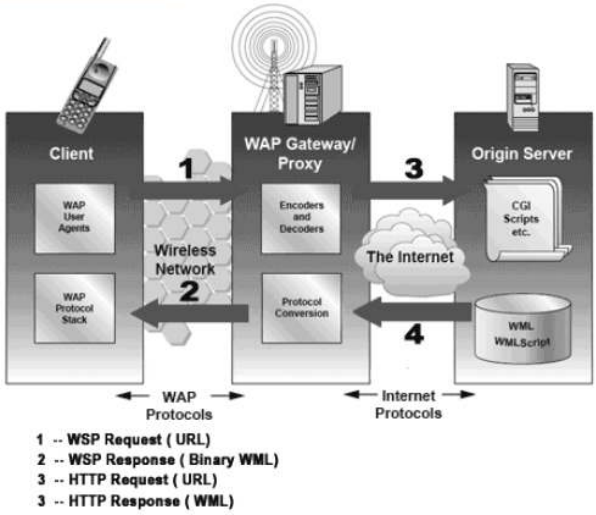


1. WSP request(URL)
2. WSP response(Binary WML)
3. Http request(URL)
4. Http response(WML)

How WAP Model Works

1. A user selects an option on their mobile device that has a URL with Wireless Markup language WML content assigned to it.
2. The phone sends the URL request via the phone network to a WAP gateway using the binary encoded WSP protocol.
3. The gateway translates this WAP request into a conventional HTTP request for the specified URL and sends it over to the Internet.
4. The appropriate Web server picks up the HTTP request and processes the request just as it would any other request. If the URL refers to a static WML file, the server delivers it. If a CGI script is requested, it is processed and the content returned as usual.

5. The Web server adds the HTTP header to the WML content and returns it to the gateway.
6. The WAP gateway compiles the WML into binary form and then sends the WML response back to the mobile device.
7. The phone receives the WML via the WSP protocol.
8. The micro-browser processes the WML and displays the content on the screen.



a) WAP hardware and websites
b) WAP Gateway/Proxy is the entity that connects the wireless domain with the Internet.

c) The WAP client software uses, a markup language - the Wireless Markup Language (WML) has been adapted to develop optimized WAP applications.
d) In order to save valuable bandwidth in the wireless network, WML can be encoded into a compact binary format. Encoding WML is one of the tasks performed by the WAP Gateway/Proxy.

Key features of WAP

Some of the key features offered by WAP include:

1. **A programming model similar to the Internet's:**
2. **Wireless Markup Language WML:** WML is a markup language used for authoring WAP services, fulfilling the same purpose as HTML does on the Web. In contrast to HTML, WML is designed to fit small handheld devices.
3. **WMLScript:** WMLScript can be used to enhance the functionality of a service, just as Java script can be utilized in HTML. It makes it possible to add procedural logic and computational functions to WAPbased services just like Java Script in HTML.
4. **Wireless Telephony Application Interface (WTAI):** The WTAI is an application framework for telephony services. WTAI user agents are able to make calls and edit the phone book by calling special WMLScript functions or by accessing special URLs.

If one writes WML decks containing names of people and their phone numbers, you may add them to your phone book or call them right away just by clicking the appropriate hyperlink on the screen.

5. **Optimized protocol stack:** The protocols used in WAP are based on well-known Internet protocols, such as HTTP and Transmission Control Protocol TCP, but they have been optimized to address the constraints of a wireless environment, such as low bandwidth and high latency.

WAP - Core Services

Some examples of useful mobile services are in the following fields:

1) **Banking**: Accessing account statements., Paying bills, Transferring money between accounts.
2) **Finance**: Retrieving stock and share prices, Buying and selling stocks and shares, Looking up interest rates, Looking up currency exchange rates.
3) **Shopping**: Buying everyday commodities, Browsing and buying books.
4) **Ticketing**: Booking or buying airline tickets,Booking theatre tickets.
5) **Entertainment:** Retrieving restaurant details, Playing interactive games.
6) **Weather:** Retrieving local weather forecasts, Looking up weather at other locations.
7) **E- Messaging:** Voice mail, Unified Messaging & Enhanced support of legacy SMS services.

Examples of WAP applications include:

- 123Jump http : / / www. 123jump. com A selection of stock data and news, all via WAP.
- 2PL World-Wide Hotel Guide http : / / wap. 2pl. com A worldwide hotel guide accessible in multiple languages via a WAP-enabled device.
- AEGEE-Eindhoven http : / / wappy. to / aegee / A Europe-wide students association, whose goal is to allow all students to integrate and learn about each others cultures.
- Ajaxo http : / / www. ajaxo. com A WAP service for Wireless Stock Trading from any WAP-enabled device.
- Amazon.com Bookshop http : / / www. amazon. com / phone / Amazon.com has launched this WAP portal HDML − based for browsing books.
- Traffic Maps http : / / www. webraska. com / A French service that monitors and shows the latest in traffic news via maps

LESSON 8

XML: THE DOCUMENT AND METADATA FORMAT FOR MOBILE COMPUTING

WML

WML which is most commonly known as Wireless Markup Language is a meta-language that has originated from the XML and perform the function of implementing the wireless application protocol specifications such as in the devices that require mobile communication and connectivity.

WML (wireless markup language) allows Web developers to design pages specifically for micro-browsers. WML allows the text pages of the website to become accessible and viewable on the mobile phones over a cellular and wireless network.

WML is considered a part of Wireless Application Protocols that works above the standard data link protocols. It provides proper programming and tool facilities and completes the set of network communication programs that are supportive of the usual internet protocols. This type of language is open source and is available for everyone to use and benefit. Anyone who has some knowledge of the HTML can take full advantage of this language and write a presentation layer using the code.

It spells out the data format which ensures that there is no collision with other existing systems like HTML, which offer the same services.

WML is an XML language used to specify content and user interface for WAP devices like PDA and Mobile Phones.

WML takes care of the small screen and the low bandwidth of transmission. WAP sites are written in WML, while web sites are written in HTML. WML files have the extension ".wml", though they are very similar to HTML i.e. they both use tags and are written in plain text format.

XML

Extensible Markup Language(XML) is a markup language that uses a set of additional items called markups to create a document of hierarchical structure. It is called extensible because it allows the author of the document to define the markup elements by their own. We can develop documents containing structured information i.e. XML contains content (e.g. text, images etc.) and along with that it also contains some information or hints about what role that content plays.

XML is often used for distributing data over the Internet...*READ pg 123 about its history.*

XML separates the Web page content from its format, allowing the Web browser to display the contents of a Web page in a form appropriate for the display device. For example, a smart phone,

a PDA, and a notebook computer all could display the same XML page or use different formats or sections of the XML page.

Characteristics

1. XML was designed to store and transport data.

2. XML was designed to be both human- and machine-readable.

Advantages of xml

1. Since xml supports UNICODE, all most all the human readable written languages can be communicated using xml.
2. It can be used to render data structure, i.e. records and lists and trees.
3. XML is self-documenting, i.e. it contains data and description about the data.
4. XML is used both on and offline for storing and processing data.
5. XML follows international standards.
6. XML allows validation of the document using XSD or Schematron. These are types of the schema for validating xml documents. The tree-like structure of xml is suitable for almost all the types of documents.
7. Being platform independent, it has lots benefits. Like it is not very prone to technological changes. Even though changes are made in DTD or schema, it is easier to keep forward or backward compatibility available.

Difference between xml and wml

XML	WML
Extensible Markup Language	Wireless Markup Language
A meta language that allows the user to define their customized expressions to perform many purposes on computers.	Performs the function of implementing the wireless application protocol specifications such as in the devices that require mobile communication and connectivity.
Creates data that is sent on the internet from one place to the other in the original format.	The language used to create pages that get displayed in a WAP browser.
XML is inspired by the HTML coding platform	WML has originated from the XML and follows the same protocol.
XML does not perform any task on its own but just transfers information in packets from one place to the other over the internet.	WML performs the task of converting the text to a readable format on the mobile devices.

WAP applications Design Considerations

While designing a WAP site, you must ensure that you keep things simple and easy to use.

Keep in mind that there are no standard micro browser behaviors and that the data link may be relatively slow, at around 10Kbps.

The following are general design tips that you should keep in mind when designing a service:

1. Keep the WML decks and images to less than 1.5KB.
2. Keep the text brief and meaningful, and as far as possible try to pre-code options to minimize the rather painful experience of user data entry.
3. Keep the URLs brief and easy to recall.
4. Minimize menu levels to prevent users from getting lost and the system from slowing down.
5. Use standard layout tags such as <big> and <b>, and logically structure your information.
6. Don't go overboard with the use of graphics, as many target devices may not support them.

WML - ENVIRONMENT

To develop WAP applications, you will need the following:

1. A WAP enabled Web Server: You can enable your Apache or Microsoft IIS to serve all the WAP client request.
2. A WAP Gateway Simulator: This is required to interact to your WAP server.
3. A WAP Phone Simulator: This is required to test your WAP Pages and to show all the WAP pages.

You can write your WAP pages using the following languages:

- Wireless Markup Language (WML) to develop WAP application.
- WML Script to enhance the functionality of WAP application.

Installing WAP Phone Simulator. If you have WAP enabled phone, then you do not need to install this simulator. But while doing development, it is more convenient and economic to use a simulator.

XML and Mobile Applications

Mobile applications relate to XML in the following two ways:

1.*Mobile applications should understand and be able to manipulate XML content*. As content on the Internet, and other networks, moves in an XML format, it is very desirable that a given mobile application can handle XML. How the XML is handled is of particular interest to that application. Although the task of parsing and interpreting the XML can be done on the mobile device itself, or some proxy such as an application server that processes all content for the device, issues such as performance become of paramount concern.

2.*Mobile applications use XML to facilitate their implementations*. For example, XML documents can be used by mobile applications to exchange data; configuration of a device or a server may be encapsulated in an XML file; some protocols such as WAP use XML as the means for presentation. There are countless places where mobile applications and related frameworks can use XML internally.

Whether the mobile application is handling XML content or using XML internally, it must be able to construct XML documents, to parse them, and to take actions based on the contents of the XML documents. When it comes to parsing XML, there are two widespread methods: DOM and SAX....*read this pg 126-160*

Key XML Technologies for Mobile Computing....read more about these

1. **Extensible Hypertext Markup Language(XHTML) and WML**
2. **Voice Extensible Markup Language(VXML)**
   - Designed for voice user interfaces. It allows specification of a command-based voice dialog through a markup language
3. **XForms**
   - XForms allows us to build user interfaces with a focus on the interactions and data exchanges between the user and the user interface as opposed to specific types of user interface.
4. **Call Control Extensible Markup Language(CCXML)**
   - Application of XML for managing voice calls. It focuses on routing the calls and connecting calls (in contrast to VXML). It is based on Java Telephony APIs (JTAPI)
5. **XML Pipeline**
   - It specifies how to process various XML resources. It specifies the flow of processing instructions that are applied to one or more given documents residing on the host . It specifies the flow of processing instructions that are applied to a variety of XML documents, residing at a variety of hosts
6. **WAP Binary Extensible Markup Language(WBXML)**
   - Defines a way to represent XML in 0's and 1's instead of text
7. **Synthetic Speech Markup Language(SSML)**
   - It is used for the infrastructure of the voice user interface
8. **Resource Description Framework(RDF)**
   Created specifically:
   - to allow discovery of various resources, indexing them and, creation of resources that are made up of other RDF resources by simply nesting the RDF descriptions

   RDF is part of Semantic Web

LESSON 9

MOBILE AND WIRELESS NETWORKS SECURITY

Mobile/Cellular Security

Security is always one of the biggest concerns when designing any application, but particularly distributed applications. Distributed applications operate over networks, involve multiple users, and have many other properties that make them more vulnerable to security breaches.

Most mobile application or mobile platforms do not exist in isolation. Therefore, the bigger picture is that most mobile applications are really distributed applications being used by mobile users on mobile devices.

We need security for two reasons:

a. to keep out those malicious parties who are trying to get access to things that they are not allowed to access and,
b. to ensure that information and system access are not inadvertently given to parties not actively seeking a system breach.

We can use the OSI model and its taxonomy to group the various types of security concerns for mobile applications. We will start from the top and work our way down:

a. **Application Layer Security**: This the most important layer for securing our mobile application. As software application developers, practically speaking, we have the most control at this layer i.e. we decide whatever security features we need to implement. At this same layer, a networked application that uses HTTP for communication may include usage of encrypted communication using techniques such as DS3 or a similar technology as well as authentication for whatever other computing system is communicating with our application.
b. **Presentation Layer and Session Layer Security**: SSL is by far the most popular and the one for which nearly all platforms provide support e.g. in WAP, the security mechanism of WTLS provides the SSL implementation for the WAP protocol. SSL is implemented by writing the SSL specification as a library for your operating system or trying to implement it on an end-to-end system. Additionally, there has been discussion among mobile device vendors in providing hardware-based solutions for SSL to provide a more efficient method for secure communications.
c. **Transport Layer and Network Layer Security (IPSec):** These layers are, respectively, the home of TCP and IP (as well as other equivalent protocols). Whereas SSL assures that all communications are secure, IPSec assures that the nodes that are communicating are not malicious and masquerading as nodes that they are not. IPSec also provides more low-level encryption and allows us to do "*IP Tunneling*." IPSec is particularly important in the infrastructure that supports the mobile application.

d. **Data Link Layer Security**: This is where things like MAC (Medium Access Control) addresses belong. It is tough to cause a security breach through the data link layer because it is typically hardware implemented. It is much more difficult to get significant malicious programs such as viruses onto the hardware to begin with.
e. **Physical Layer Security**: The biggest differences between security implementations of mobile systems and stationary systems are a by-product of the fact that mobile systems are typically connected to the network through a wireless connection.

Wired systems, whether fiber-optic cables, coaxial cable, or twisted-pair wires, limit access to the bits and bytes traveling across the communication channels that they provide inside their physical medium. However, bits and bytes are all over the space between two wireless nodes waiting to be read as there is no limiting "conduit" in the case of wireless communication.

Not only that, but intrusion detection is enormously more difficult in wireless systems where signal attenuations, phase shifts, and other phenomena are part of the physical condition of the network and cannot be used reliably to indicate security breaches.

Security issues in Mobile Computing

Considering this taxonomy of security issues based on the OSI model, the dimensions of mobility, and the mobile condition of the mobile user leads us to the following security issues that are unique from any of those concerns experienced by stationary applications:

1) Secure authentication and authorization of nodes,
2) Secure communications between the authenticated and authorized nodes of the network over a wireless connection (at various OSI layers using the correspondingly appropriate techniques such as SSL at the presentation/session layers),
3) Secure deployment of an application on the target device,
4) Secure storage and retrieval of information on the mobile device,
5) Securing information collected or provided by the mobile application infrastructure (e.g., location information),
6) Securing any conversion of content required for supporting multimodal applications,
7) Securing synchronization and exchange of information among different channels in a multichannel communication environment,
8) Defending against the fraudulent usage of the wireless service, and
9) Defending against various Denial of Service attacks that may interrupt service to the network users (mobile application users in our case) or make other security breaches possible.

Mobility and its impact to mobile security

In addition to these concerns, once again, we bring up the dimensions of mobility i.e. the dimensions of mobility are the fundamental bases for those difference we see between mobile applications and stationary applications.

Dimensions of mobility to see the differences in requirements, design, and implementations of security between mobile and stationary applications. In other words, we need to consider the following:

1) *How do security concerns change when the location of the device and application are changing, when the application is using location information in its internal logic?* The location information must be provided not only securely but also privately.
2) *Is security compromised by the QOS?* For example, some systems do not appropriately secure dropped packets. QOS is a dimension of mobility largely because of the intermittent connectivity of the mobile user but also because the connectivity may be provided through a wireless network.
   Is Security is almost always dependent on device capabilities as it takes device resources to encrypt/decrypt data.? For example, the size of the encryption key may need to be smaller for some devices than others as they may not have the processing power to encrypt and decrypt the data in a timely manner.

3) *Does the mode of operating a mobile application affect the security of other applications?* Obviously, not every application or transaction within the same application requires the same amount of security. The key is to make sure that the security of those transactions that must be secure is never compromised regardless of the device mode of operation.
4) *Do the use of various interfaces interfere with the security of other applications?* Various user interfaces require different types of security. For example, it may be fine to display some secure and private information to the user on the GUI application as he or she may be able to hide it from the surroundings, but the same is not true in the case of a VUI; we do not want to play a text-to-speech clip of the user's bank account balance or, at the very least, we want to give the user the choice to hear or view his or her balance. Voice itself can also be used to test liveliness as well as authentication. Another critical issue is to provide proper security for intermodal and inter-channel communications.
5) *Is there a mechanisms to control security issues arising from different mobile devices in the dynamic market?* The problem of device proliferation, coupled with the distributed nature of mobile applications, magnifies the scalability problem of implementing security. Each user may have many different mobile devices. For example, a typical user may have a mobile device in his or her automobile (telematic device), a cell phone, a PDA, a laptop, and possibly a tablet PC, each of which may connect to the network thorough a distinct channel or set of channels and have its own set of security needs and requirements.
6) *How does the aspect of interactivity affect the use of mobile applications*? Actively interacting with the user presents us with more privacy problems then security problems. Whereas we can use the user's response to the initial transaction for authorization, we

must be able to authenticate the user prior to sending out that initial message. Sending the initial interaction or pushed message to the wrong user in itself is a security flaw.

7) Other concerns: The mobile condition of the user introduces the following new concerns which include:
    - Mobile devices are more susceptible to theft and loss than stationary devices.
    - With mobile users, there is a range of environments to consider in a security policy i.e. with or without a VPN (Virtual Private Network), users may connect to the network directly, through a corporate Internet service provider, or through their own Internet service provider, thereby using a variety of different security guidelines established by different organizations.
    - The rapid development of mobile technology to meet higher user expectations has led to security being seen as too much work in a compressed timeline.
    - Many mobile devices use SIM cards. Securing the configuration and reconfiguration of these SIM cards in itself is a security issue i.e. SIM configuration change can lead to a change of behavior or intention on the part of the device.

Having discussed all of these various concerns and how we can categorize them for mobile applications, we must take a further step, before all others, in designing a secure system i.e. we must determine the threat levels. This is perhaps the single most neglected step in most systems i.e. once a solution works, we have a tendency to use that solution for all sorts of problems, whether or not the solution is a good fit.

Without the proper threat recognition in which the various levels of threat, sources of threat, and the cost of security are addressed, trying to solve the security problems of a system, whether mobile or not, becomes a haphazard series of jumps between isolated symptoms instead of a systematic solution to the roots of security problems.
In the case of mobile applications, what you need to keep in mind while determining the threat levels are the following:

- Mobile applications are a superset of their stationary counterpart. Therefore, you must take into account all of those concerns of stationary applications.
- Consider the new security concerns introduced by the various dimensions of mobility and the very distributed nature of mobile applications.
- Consider the appropriateness of the level of security concern for each part of the mobile application. It is easy to overestimate or underestimate the level of security required for a particular transaction. The requirements-gathering process is critical here. Also, different parts of the application may require different security levels.

Security in Wireless Networks

A general problem with wireless communication is that the data can simply be plucked right out of the air. Because the medium of communication is space itself, the data being communicated is more accessible. Unlike wired communication, there are no conduits nor physical barriers: The bits and bytes are everywhere out in space to be picked up by all listeners, legitimate or otherwise.

Generally speaking, we are not only concerned with securely establishing communication channels and securing the transmission over the channel.

To do(optional) *:Read more about security in various wireless network technologies such as Bluetooth, LANs, GSM, and TDMA. Also discuss how security is enforced in ADHOC networking technologies pg 760-769*

Future of wireless and mobile networks

1) Shift industrial paradigm from piecewise solutions to end-to-end information systems

2) Improved radio technology and antennas

    - smart antennas, beam forming, multiple-input multiple-output (MIMO) 802.11N
    - dynamic spectrum allocation

3) Core network convergence

    - IP-based, quality of service, mobile IP

4) Ad-hoc technologies

    - spontaneous communication, power saving, redundancy

5) Simple and open service platform

    - intelligence at the edge, not in the network (as with IN)
    - more service providers, not network operators only

****