MOTHER TERESA WOMEN'S UNIVERSITY

DIRECTORATE OF DISTANCE EDUCATION

KODAIKANAL – 624 102

M.Sc COMPUTER SCIENCE

(P.G)

MATERIAL FOR MOBILE COMPUTING

SUBJECT CODE

Compiled by Dr. K.Kavitha

MOBILE COMPUTING

UNIT I

Introduction : Mobility of Bits and Bytes – Wireless The beginning – Mobile computing – Dialog Control – Networks –Middleware and Gateways – Applications and Services – Developing Mobile Computing Applications – Security in Mobile Computing – Standards – Why is it necessary – Standard Bodies –Players in the wireless space. Mobile Computing Architecture: history of computers - History of Internet – Internet the Ubiquitous Network – Architecture for mobile computing- Three – tier Architecture – Design Considerations for mobile computing- mobile computing through Internet – Making existing applications mobile-enabled.

UNIT II

Mobile computing through Telephony: Evolution of Telephony – Multiple Access Procedures – mobile computing through telephone-developing an IVR application – voice XML – Telephony Application Programming Interface. Emerging Technologies: Introduction – Bluetooth – radio Frequency Identification – wireless broadband-mobile IP – Internet Protocol version 6 -Java card.

UNIT III

Global System for Mobile Communications: Global system for Mobile communications – GSM Architecture – GSM Entities –call routing in GSM –PLMN Interfaces-GSM address and identifiers-Network aspects in GSM-GSM Frequency Allocation –Authentication and Security. General PacketRadio Service: Introduction-GPRS and packet Data Network – GPRS Network operations-Data Services in GPRS-Application for GPRS-Limitations of GPRS-Billing and charging in GPRS.

UNIT IV

Wireless Application Protocol: Introduction –WAP-MMS-GPRS applications. CDMA and 3G. Introduction – Speed spectrum technology-IS95-CDMA versus GSM-Wireless Data-Third Generation Networks-Application on 3G.

UNIT V

Wireless LAN: Introduction –wireless LAN advantages-IEEE802.11 standards-wireless LAN architecture-mobility in wirelessLAN –deploying wireless LAN-Mobile adhoc Networks and sensor Networks – Wireless LAN Security-WIFI versus 3G-Internet networks-SS#7 signaling-IN Conceptual Model-softswitch-programmable networks-technologies and Interfaces for IN

Books Prescribed:

1.Mobile Computing Technology applications and Service creation, Asoke K Talukder, Roopa R Yavagal, Tata McGraw-Hill publishing company New Delhi 2007.

Reference Books

1.Mobile Communication- Jochen Schiller 2nd edition Pearson 2003.

UNIT I

INTRODUCTION

MOBILE COMPUTING Mobile computing can be defined as a computing environment over physical mobility. The user of mobile computing environment will be able to access data, information or other logical objects from any device in any network while on the move. The computing environment is mobile and moves along with the user. This is similar to the telephone number of a GSM (GLOBAL SYSTEM FOR MOBILE COMMUNICATION) phone, which moves with the phone. The offline (local) and real time (remote) computing environment will move with the user. In real time mode user will be able to use all his remote data and service online.

Nomadic Computing: The computing environment is nomadic and moves along with the mobile user. This is true for both local and remote services.

Pervasive Computing: A computing environment, which is pervasive in nature and can be made available in any environment.

Ubiquitous Computing: A disappearing (nobody will notice its presence) every place computing environment. User will be able to use both local and remote services.

Mobility refers to our ability to move freely. **Mobility** training is a series of movements and exercises that can help alleviate restriction within the muscular, skeletal and nervous systems that may limit our **mobility**.

Mobility of Bits and Bytes

In the last two centuries, mobility has been redefined. Both physical and virtual objects are now

Mobile. – Mobility of physical objects relate to movement of matters,-whereas movements of virtual objects relate to movements of bits and bytes.

Wireless The beginning

Today, the wireless communication market has grown rapidly. Communication technologies have become an integral part of human"s daily life. In this section, the wireless communication technologies have evolved from the first to third generation and are moving towards to Fourth Generation (4G) as illustrated in table 1.1. The table 1.1 summarizes the development of wireless communications from First Generation (1G), Second Generation (2G) and Third Generation (3G), offering the properties of each generation by comparing the driving technology, representative standard, radio frequency, bandwidth, multi-address technique, core networks and service type.

Generation	1G	2G	2.5G	3G
Driving technology	Analogue signal processing	Digital signal processing	Packet switching	Intelligent signal processing
Representative standard	AMPS, TACS	GSM, I-Mode	GPRS, TDMA, HSCSD, EDGE	IMT-2000 (UMTS, WCDMA, CDMA2000
Radio frequency	400M – 800M	800M – 900M, 1800M –	800M – 900M, 1800M –	2G
Bandwidth	2.4K – 30K	9.6K – 14.4K	171K – 384K	2M – 5M
Multi-address	FDMA	TDMA, CDMA	TDMA, CDMA	CDMA
Core network	Telecom networks	Telecom networks	Telecom networks	Telecom networks,
Service type	Voice	Voice, short message service	Data service	Voice, data, some

Mobile computing

Mobile Computing describes the application of small, portable, wireless computing and communication devices, which is used when mobile is changing its location. It requires wireless network to support outdoor mobility and handover from one network to another network. Challenges of the mobile computing are mobility context aware applications, naming and locating, routing data and messages, reliability in the presence of disconnection, data management, transaction models, security and seamless mobility.

Dialog Control

In any communication there are two types of user dialogues. These are long session – oriented transactions and short transaction. Going through a monolithic document page by page can be considered as a session-oriented transaction. Going to a particular page directly through an index can be considered as a short transaction. Selection of the transaction mode will depend on the type of advice we use. A session may be helpful in case of services offered through computers with large screens and mouse. For devices with limited input/output like SMS for instance, short transactions may be desired.

Let us consider an example of bank balance enquiry over the internet. In case of internet banking through desktop computer, the user has to go through the following minimum dialogues:

1.Enter the URL of the bank site.

2. Enter the account number/password and login into the application.

3.Select the balance enquiry dialogue and see the balance,

4.Logout from the internet banking.

The dialog above is an example of session oriented transaction. Using short transaction, the same objective can be met through one single dialogue. In short transaction user sends a SMS message, say ‘mybal’ to the system and receives the information on balance. The application services all the 5 dialogue steps as one dialogue. In this case many steps like authentication, selection of transactions need to be performed in smarter ways.

Networks

Mobile computing will use different types of networks. These can be fixed telephone networks, GSM, GPRS, ATM, Frame Relay, ISDN, CDMA, CDPD, DSL, Dial-up,WiFi, 802.11, Bluetooth,Ethernet,Broadband,etc.,

Wireline Networks

Wireline networks will be linked by **network** devices, such as repeaters, hubs, switches, bridges, and routers, and joined by physical pipe, such as electronic and fiber cable. Wireless **networks** will be connected by many antennas or WiFi or WiMAX devices.

Wireless Networks

Wireless networks are computer **networks** that are not connected by cables of any kind. The use of a **wireless network** enables enterprises to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations.

Adhoc Networks

An **ad hoc network** is a **network** that is composed of individual devices communicating with each other directly. The term implies spontaneous or impromptu construction because these **networks** often bypass the gatekeeping hardware or central access point such as a router.

Bearers

Bearer service. In telecommunications, **Bearer** Service or data service is a service that allows transmission of information signals between **network** interfaces. ... The **bearer** services include the following: Rate adapted sub-rate information like circuit switched asynchronous and synchronous duplex data, 300-9600 bits.

Middleware and Gateways

- Any software layered between a user application and operating system can be termed as middleware.
- Middleware examples are
  - communication middleware,
  - object oriented middleware,
  - message oriented middleware,
  - transaction processing middleware,

- database middleware,
- behavior management middleware,
- RPC middleware
- etc.

There are some middleware components like behavior management middleware, which can be a layer between the client device and the application. In mobile computing context we need different types of middleware components and gateways at different layers of the architecture.

- These are:
  1. Communication middleware
  2. Transaction processing middleware
  3. Behavior management middleware
  4. Communication gateways.

Communication middleware

- The application will communicate with different nodes and services through different communication middleware.
- Different connectors for different services will fall in this category.
- Examples could be TN3270 for IBM mainframe services, or Javamail connector for IMAP or POP3 services.

Transaction processing middleware

- In many cases a service will offer session oriented dialogue (SoD).
- For a session we need to maintain a state over the stateless Internet.
- This is done through an application server.
- The user may be using a device, which demands a short transaction whereas the service at the backend offers a SoD.
- In such cases a separate middleware component will be required to convert a SoD to a short transaction.
- Management of the Web components will be handled by this middleware as well.

Behavior Management Middleware

- For different devices we need different types of rendering.
- We can have applications, which are developed specially for different types of rendering.
- For example, we can have one application for Web, another for WAP, and a different one for SMS.
- On the contrary, we may choose to have a middleware, which will manage entire device specific rendering at the run time.
- This middleware will identify the device properly and handle all the behavior related stuff independent of the application.
- The system may be required to have some context awareness.
- All these will be handled by behavior management middleware.

Communication Gateways

- Between the device and the middleware there will be network of networks.
- Gateways are deployed when there are different transport bearers or networks with dissimilar protocols.
- For example, we need an IVR (Interactive Voice Response) gateway to interface voice with a computer, or an WAP gateway to access internet over a mobile phone.

- The following diagram (Figure) depicts a schematic diagram of services in a mobile computing environment where services from enterprise to a vending machine can be used from different devices.

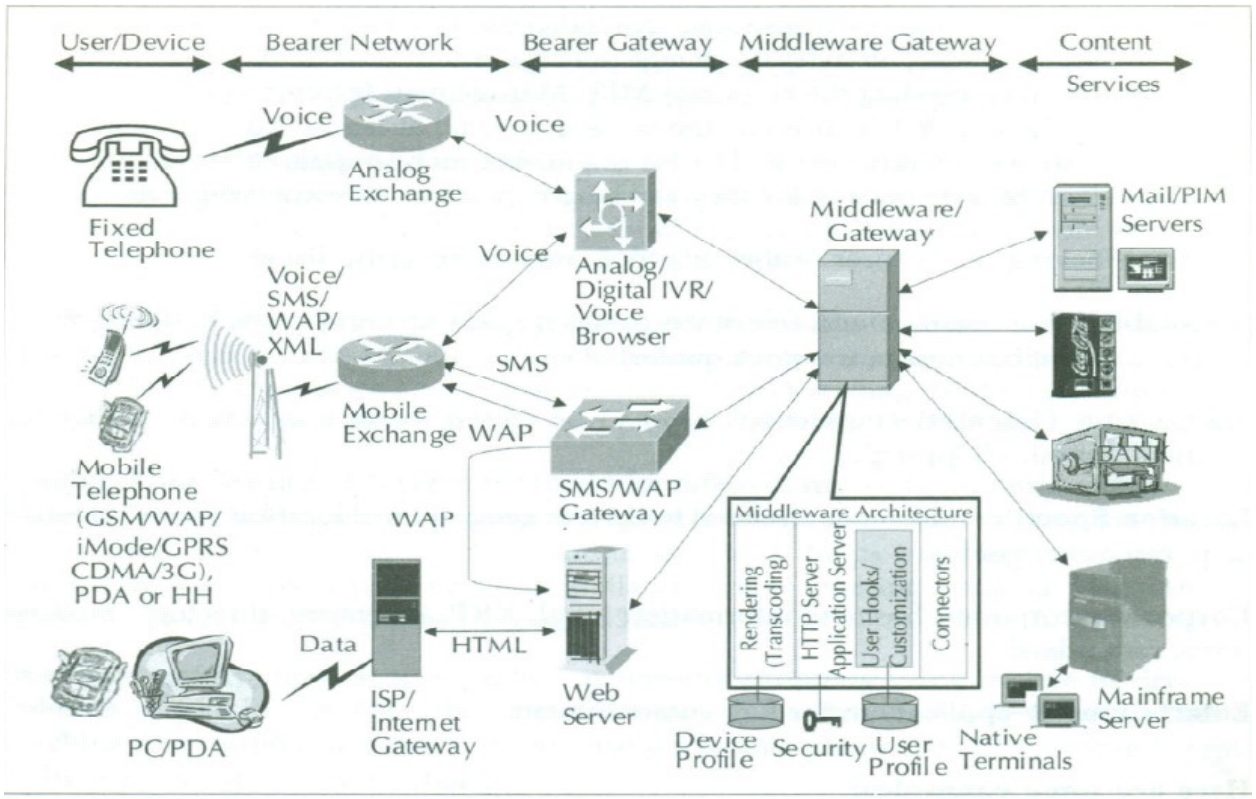


Figure: Systematic Representation of mobile computing environment

Applications and Services

Data and information, through mobile computing services are required by all people regardless of the fact that they are mobile are not. Mobile users will include people like mobile executives, sales people, service engineers, road warriors, farmers in the field, milkman, newspaper boy, courier or pizza delivery boy. Logically everybody is a mobile user in some respect I some part of the lifestyle. For people, who are stationary, mobile computing is necessary in the office hours. For example we may need to do a bank transaction from home at night or respond to an urgent mail while at home. There are many applications and services for the mobile computing space. These application or services run on origin server. These are also known as content server.

Contents will primarily be lifestyle specific. An individual has different lifestyles in different social environment. Also, lifestyles do change during the course of the day. One individual can be an executive needing the corporate MIS application during the

day. While at home the same individual at leisure can use applications for youth lifestyle or entertainment. The list of possible mobile application can never be complete. From lifestyle perspective they can be grouped in to different categories like.

Personal – belongs to the user(Wallet, life-tool, medical records, diary)

Perishable-time sensitive and relevance passes quickly(breaking news weather, sports, business news, stock quotes).

Location specific-information related to current geographical location(street direction map, restaurant guide).

Corporate-corporate business information(mail, ERP, inventory, directory, business alerts, reminders)

Entertainment-applications for fun, entertainment.

Developing Mobile Computing Applications

Any portal system today supports user mobility. If I have an internet mail account like Hotmail or yahoo. I can access my mail from anywhere. I need a desktop or laptop computer to access my mailbox. I may not be able to access the same mail through some other device like a fixed phone. There are a number of factors that make mobile computing different from desktop computing. As a result of mobility the attributes associated with devices, network and users are constantly changing.

New mobile application:

Let us assume that in a bank, some new applications need to be built for e-commerce. The banks wants to offer banking through voice and web. Assuming that the bank already has a computerized system in place, the bank will develop two new applications. One will handle the telephone interface through interactive voice response and the other through Web. At a later point in time, if the banks decides to offer SMS and WAP, they will develop two new applications to support SMS and WAP interfaces

respectively. To protect the investment and quick adaptation, the bank decide to use transaction processing middle ware and RPC middleware. All these are possible only if it is a fresh applications development.

Making Legacy Application Mobile

Characteristics

1.The application has moved into the sustenance phase in the software development life cycle.

2.An application which cannot be modified. This could be due to unavailability of the original development platforms, unavailability of original source code of unavailability of expertise to make necessary changes.

3. Products and packaged software where enterprises does not have any control. This could be due to high cost of ownership for new upgrade or the vendor does not have any plan to suppor the new requirement.

Security in Mobile Computing

Mobile security is the protection of smartphones, tablets, laptops and other portable computing devices, and the networks they connect to, from threats and vulnerabilities associated with wireless computing. Mobile security is also known as wireless security.

Securing mobile devices has become increasingly important in recent years as the numbers of the devices in operation and the uses to which they are put have expanded dramatically. The problem is compounded within the enterprise as the ongoing trend toward IT consumerization is resulting in more and more employee-owned devices connecting to the corporate network.

SearchSecurity.com's 2012 enterprise mobile security survey polled 487 IT security professionals and IT managers. The survey found the following top five mobile security concerns:

1. Device loss was the top concern. If an employee leaves a tablet or smartphone in a taxi cab or at a restaurant, for example, sensitive data, such as customer information or

corporate intellectual property, can be put at risk. According to Marcus Carey, a security researcher at Boston-based compliance auditing firm Rapid7 Inc., such incidents have been behind many high-profile data breaches.

2. Application security was the second-ranking concern. One problem is mobile apps that request too many privileges, which allows them to access various data sources on the device. According to Domingo Guerra, president and co-founder of San Francisco-based Appthority Inc., many mobile apps -- especially free ones -- are built with ties to advertising networks, which makes contacts, browsing history and geolocation data extremely valuable to application developers. As Guerra put it, "Developers want to monetize, consumers want free apps and then ad networks will pay developers to get all of that juicy data from their users." According to survey respondents, leaked corporate contacts, calendar items and even the location of certain executives could put the company at a competitive disadvantage.Another concern is malicious or Trojan-infected applications that are designed to look like they perform normally, but secretly upload sensitive data to a remote server.

3. Device data leakage was the third-ranking mobile security issue. Nearly all of the chief concerns identified in the mobile security survey, from data loss and theft to malicious applications and mobile malware, are sources of data leakage. While most corporate access privileges on mobile devices remain limited to calendar items and email, new mobile business applications can tap into a variety of sources, if the enterprise accepts the risks, said mobile security expert Lisa Phifer. Increased corporate data on devices increases the draw of cybercriminals who can target both the device and the back-end systems they tap into with mobile malware, Phifer said. "If you're going to put sensitive business applications on those devices, then you would want to start taking that threat seriously."

4. Malware attacks were the fourth-ranking mobile security concern. A new report from Finland-based antivirus vendor F-Secure Corp. found the vast majority of mobile malware to be SMS Trojans, designed to charge device owners premium text messages. Experts say Android devices face the biggest threat, but other platforms can

attract financially motivated cybercriminals if they adopt Near Field Communications and other mobile payment technologies. An F-Secure analysis of more than 5,000 malicious Android files found that 81% of mobile malware can be classified as Trojans, followed by monitoring tools (10.1%) and malicious applications (5.1%).

5. Device theft was fifth on the list of top concerns. Smartphone theft is a common problem for owners of highly coveted smartphones such as the iPhone or high-end Android devices. The danger of corporate data, such as account credentials and access to email, falling into the hands of a tech-savvy thief, makes the issue a major threat to the IT security pros who took the survey.

Standards- Why is it necessary

Standards provide people and organizations with a basis for mutual understanding, and are used as tools to facilitate communication, measurement, commerce and manufacturing. Standards are everywhere and play an important role in the economy, by: facilitating business interaction.

Standards form the fundamental building blocks for product development by establishing consistent protocols that can be universally understood and adopted. This helps fuel compatibility and interoperability and simplifies product development, and speeds time-to-market. Standards also make it easier to understand and compare competing products. As standards are globally adopted and applied in many markets, they also fuel international trade.

It is only through the use of standards that the requirements of interconnectivity and interoperability can be assured. It is only through the application of standards that the credibility of new products and new markets can be verified. In summary standards fuel the development and implementation of technologies that influence and transform the way we live, work and communicate.

Standard Bodies

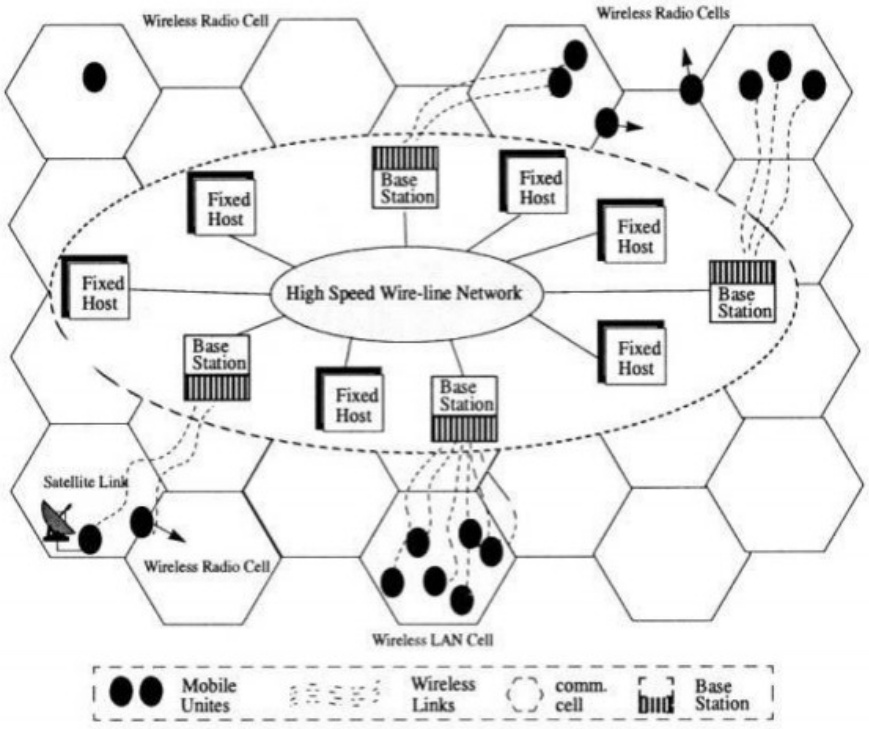
The international organization for standardization is a world wide federation of national standards bodies from more than 140 countries one from each country. ISO is a non governmental organization established in 1947. The mission of ISO is to promote the development of standardization and related activities in the world with a view to facilitation the international exchange of good and services.

Players in the wireless space.

In a wireless network there are many stake holders, These are

1. Regulatory authorities
2. The operator or the service provider.
3. The user or the subscriber
4. Equipment vendors
5. Research organization

Mobile Computing Architecture:



Steps

Some of the fixed hosts are special computers equipped with wireless interfaces, and are known as base (radio) stations (BS). They are also known as mobile support stations (MSS). Base stations, which are placed in the center of cellular coverage areas, act as access points between the mobile computers and the fixed network. Mobile computers can be in one of three states.

- The first state places a mobile computer within a cell and capable of communicating.
- The second state places the mobile computer out of range of any service cell and not capable of communication.
- The third state places a mobile computer in a cell, communicating, but just ready to cross a cell boundary.

History of computers

The first counting device was used by the primitive people. They used sticks, stones and bones as counting tools. As human mind and technology improved with time more computing devices were developed.

Abacus

The history of computer begins with the birth of abacus which is believed to be the first computer. It is said that Chinese invented Abacus around 4,000 years ago.It was a wooden rack which has metal rods with beads mounted on them. The beads were moved by the abacus operator according to some rules to perform arithmetic calculations. Abacus is still used in some countries like China, Russia and Japan.

Napier's Bones

It was a manually-operated calculating device which was invented by John Napier (1550-1617) of Merchiston. In this calculating tool, he used 9 different ivory strips or bones marked with numbers to multiply and divide. So, the tool became known as "Napier's Bones. It was also the first machine to use the decimal point.

Stepped Reckoner or Leibnitz wheel

It was developed by a German mathematician-philosopher Gottfried Wilhelm Leibnitz in 1673. He improved Pascal's invention to develop this machine. It was a digital mechanical calculator which was called the stepped reckoner as instead of gears it was made of fluted drums.

Difference Engine

In the early 1820s, it was designed by Charles Babbage who is known as "Father of Modern Computer". It was a mechanical computer which could perform simple calculations. It was a steam driven calculating machine designed to solve tables of numbers like logarithm tables.

Analytical Engine

This calculating machine was also developed by Charles Babbage in 1830. It was a mechanical computer that used punch-cards as input. It was capable of solving any mathematical problem and storing information as a permanent memory.

History of Internet

Advanced Research Project Agency(ARPA) was formed to fund Science and Technology projects and position USA as a leader in technology. Internet represents one of the best examples of the benefits of sustained investment on research and development through ARPA. Beginning with the early research in packet switching, the government, industry and academia have been partners in evolving and deploying the exciting Internet technology. People in almost all parts of life starting from education, IT, telecommunication, business, and society at large have felt the influence of this pervasive information infrastructure.

Packet switching networks such as the NPL network, ARPANET, Merit Network, CYCLADES, and Telenet, were developed in the late 1960s and early 1970s using a variety of communications protocols. Donald Davies first demonstrated packet

switching in 1967 at the National Physics Laboratory (NPL) in the UK, which became a testbed for UK research for almost two decades. The ARPANET project led to the development of protocols for internetworking, in which multiple separate networks could be joined into a network of networks.

In the early 1980s the NSF funded the establishment for national supercomputing centers at several universities, and provided interconnectivity in 1986 with the NSFNET project, which also created network access to the supercomputer sites in the United States from research and education organizations. Commercial Internet service providers (ISPs) began to emerge in the very late 1980s. The ARPANET was decommissioned in 1990.

Internet the Ubiquitous Network

Ubiquitous networking is the underlying combination of wired and wireless technologies that support communications among the various systems involved.Some current smart speaker systems feature voice-activated digital assistants that can interface with the internet, answer questions and control home automation hubs

Mobile computing devices have changed the way we look at computing. Laptops and personal digital assistants (PDAs) have unchained us from our desktop computers. A group of researchers at AT&T Laboratories Cambridge are preparing to put a new spin on mobile computing. In addition to taking the hardware with you, they are designing a ubiquitous networking system that allows your program applications to follow you wherever you go.

By using a small radio transmitter and a building full of special sensors, your desktop can be anywhere you are, not just at your workstation. At the press of a button, the computer closest to you in any room becomes your computer for as long as you need it. In addition to computers, the Cambridge researchers have designed the systemto work for other devices, including phones and digital cameras.

Ubiquitous network is a context-aware network of computing devices which are connected at any place, anytime and with any object. Ubiquitous network allows all users to access and exchange information of any kind freely at any time, from anywhere, and from any appliance through the use of broadband and mobile access. Combines optical communication, mobile and consumer electronics into one network.

Three – tier Architecture

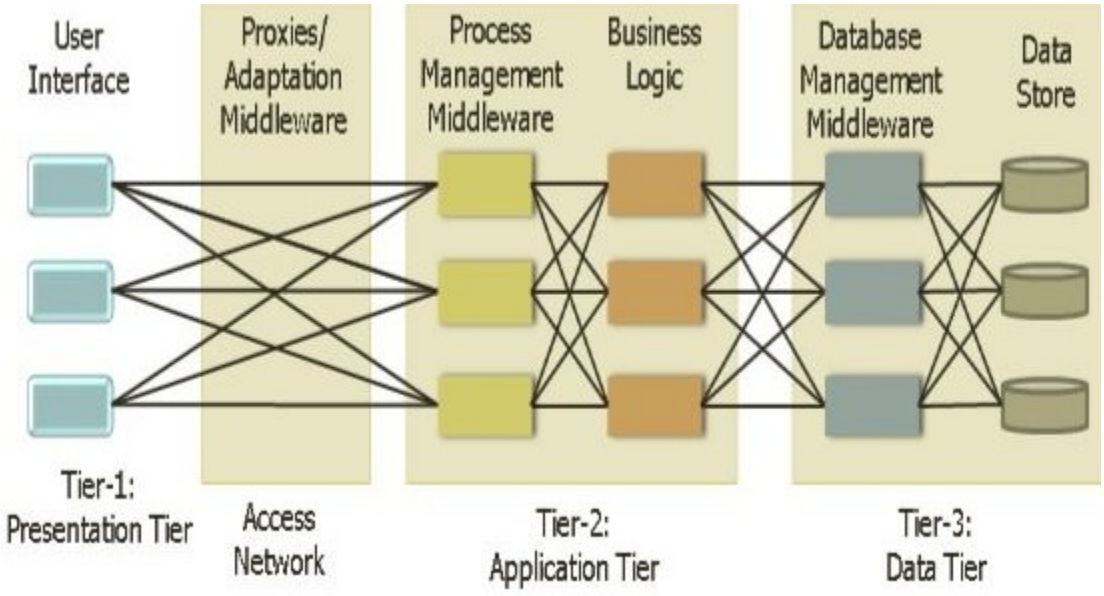


Figure: 3-tier architecture for mobile computing

A 3-tier architecture is an application program that is organized into three major parts, comprising of:

- *The data access layer tier at the bottom,*
- *The application tier (business logic) in the middle and*
- *The client tier (presentation) at the top.*

Each tier is distributed to a different place or places in a network. These tiers do not necessarily correspond to physical locations on various computers on a network, but rather to logical layers of the application.

1. Presentation Layer (UI):

- This layer presents data to the user and optionally permits data manipulation and data entry, also this layer requests the data form Business layer.
- This layer accomplished through use of Dynamic HTML and client-side data sources and data cursors.

2. Business Logic Layer:

- The business logic acts as the server for client requests from workstations. It acts according Business rules fetch or insert data through the Data Layer.
- In turn, it determines what data is needed (and where it is located) and acts as a client in relation to a third tier of programming that might be located on a local or mainframe computer.
- Because these middle-tier components are not tied to a specific client, they can be used by all applications and can be moved to different locations, as response time and other rules require.

3. Data Access Layer:

- The third tier of the 3-tier system is made up of the DBMS that provides all the data for the above two layers.
- This is the actual DBMS access layer.
- Avoiding dependencies on the storage mechanisms allows for updates or changes without the application tier clients being affected by or even aware of the change.

Design Considerations for mobile computing

Following guidelines to ensure that your application meets your requirements and platforms efficiently in scenarios common to mobile computing through Internet –Making existing applications mobile-enabled.

a)Decide If you build a rich client, a thin web client, or Rich internet application
b)Dteremine the device types you will support.
c)Design considering occasionally connected limited bandwidth scenario when required.
d)Design a UI appropriate for mobile devices, taking into platform constraint.
e)Design a layered architecture appropriate for mobile devices that improves reuse and maintainability.

Mobile computing through internet

For mobile and ubiquitous computing, the access network, it could range from infrared, Bluetooth, WiFi, GSM,GPRS,IS-95, CDMA etc., For wired, it is expected to be some kind of LAN. In case of wired network the bandwidth is higher, stable and the device is likely to a workstation with a large memory and display. Also, such devices are not constrained by the limited battery power.

When the user-facing device is a wired device, the complexity and challenges are far less. However, some of the constraints for wireless can still apply in the case of wired

devices and networks. Therefore, from the mobile computing client point of view, consideration for wired device will be the same as a wireless client.

Making Existing Applications Mobile Enabled

There are many applications that are now being used with the intranet or the corporate networks,

that need to be made ubiquitous. These are different productivity tools like e-mail or messaging applications, workflow systems etc., will also fall within this category. These applications need to be made ubiquitous and mobile computing capable. There are many ways by which this can be achieved.

1.Enhance existing application take the current application. Enhance the application to support mobile computing.

2.Rent an application from an ASP there are many organizations who develop ubiquitous application and rent the same at a fee.

3. Write a new application develop a new application to meet the new business requirement of the mobile computing.

4.Buy a packaged solution there are many companies who are offering packaged solutions for various business areas starting from manufacturing to sales and marketing. Buy and install one of these which will also address the mobile computing needs of the enterprise.

5.Bridge the gap through middleware use different middleware technique to face lift and mobile computing enable the existing application.

One of these techniques or any combinations can be used to make an application ubiquitous. If the enterprise has a source code for the application, enhancement of the existing application may be a choice. Buying a package or renting a solution from an ASP can also be preferred path for some business situations.

Many of these applications might have been developed in-house, but may not be in a position to be enhanced. Some might have been purchased as products. A product developed by outside agency cannot be enhanced or changed as desired. In many of such situations, mobile computing enabling can be done through middleware. The

combination of communication middleware and application middleware can be used to make an application mobile.

UNIT II

MOBILE COMPUTING THROUGH TELEPHONY

The 60s and 70s saw a variety of commercial car services – the earliest weighed 90-100 pounds

- These services operated using high power transmissions
- The concept of low power transmission in hexagonal cells was introduced in 1947
- The electronics were advanced enough by the 60s to pull it off, but there was no method for handoffs from one cell to the next

Evolution of Telephony

That problem was solved with the first functioning cell system and first real cell phone call in 1973. The phone, which weighed about six pounds, was developed by Martin Cooper of Motorola • Bell Labs and Motorola were the main competitors in the US. Bell Labs did most of the work developing the cell technology, but Motorola was ahead in phone development

- But they both lost out to Japan and Northern Europe. Service began in Tokyo in 1979 and Nordic Mobile Telephone was founded in Norway, Sweden, Finland, and Denmark the same year

Tests began in the Baltimore/DC area in 1981

- The first commercial service began in 1983 with the advent of the legendary Motorola DynaTAC 8000X

- In 1984 Bell Labs perfected the modern system of cellular telephony that we use today
- Thus began first generation analog cellular telephony (1G), though we didn't call it that at the time

Multiple Access Procedures **Multiple Access Procedures**

The radio channel is a communication medium shared by many subscribers in one cell. Mobile stations compete with one another for the frequency resource to transmit their information streams. Without any other measures to control simultaneous access of several users, collisions can occur (multiple access problem). Since collisions are very undesirable for a connection-oriented communication like mobile telephony, the individual subscribers/mobile stations must be assigned dedicated channels on demand. In order to divide the available physical resources of a mobile system, i.e. the frequency bands, into voice channels, special multiple access procedures are used which are presented in the following (Figure).

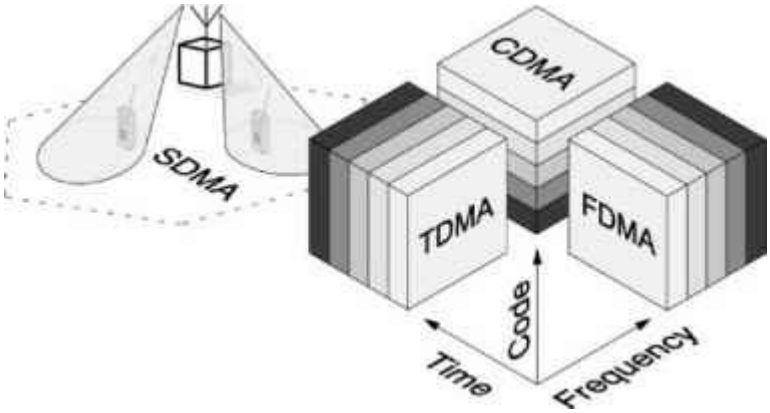


Figure : Multiple access procedures

Frequency Division Multiple Access (FDMA)

Frequency Division Multiple Access (FDMA) is one of the most common multiple access procedures. The frequency band is divided into channels of equal bandwidth such that each conversation is carried on a different frequency (Figure). Best suited to analog mobile radio, FDMA systems include the C-Netz in Germany, TACS in the UK, and AMPS in the USA. In the C-Netz, two frequency bands of 4.44 MHz each are subdivided into 222 individual communication channels at 20 kHz bandwidth. The effort in the base station to realize a frequency division multiple access system is very high.

Even though the required hardware components are relatively simple, each channel needs its own transceiving unit. Furthermore, the tolerance requirements for the high-frequency networks and the linearity of the amplifiers in the transmitter stages of the base station are quite high, since a large number of channels need to be amplified and transmitted together [15,54]. One also needs a duplexing unit with filters for the transmitter and receiver units to enable full-duplex operation, which makes it nearly impossible to build small, compact mobile stations, since the required narrowband filters can hardly be realized with integrated circuits.

Figure: Channels of an FDMA system (schematic)

Time Division Multiple Access (TDMA)

Time Division Multiple Access (TDMA) is a more expensive technique, for it needs a highly accurate synchronization between transmitter and receiver. The TDMA technique is used in digital mobile radio systems. The individual mobile stations are cyclically assigned a frequency for exclusive use only for the duration of a time slot. Furthermore, in most cases the whole system bandwidth for a time slot is not assigned to one station, but the system frequency range is subdivided into subbands, and TDMA is used for multiple access to each subband. The subbands are known as carrier frequencies, and the mobile systems using this technique are designated as multicarrier systems (not to be confused with multicarrier modulation). The pan-European digital system GSM employs such a combination of FDMA and TDMA; it is a multicarrier TDMA system. A frequency range of 25 MHz holds 124 single channels (carrier frequencies) of 200 kHz bandwidth each, with each of these frequency channels containing again 8 TDMA conversation channels.

Thus the sequence of time slots assigned to a mobile station represents the physical channels of a TDMA system. In each time slot, the mobile station transmits a data burst. The period assigned to a time slot for a mobile station thus also determines the number of TDMA channels on a carrier frequency. The time slots of one period are combined into a so-called TDMA frame. Figure shows five channels in a TDMA system with a period of four time slots and three carrier frequencies.The TDMA signal transmitted on a carrier frequency in general requires more bandwidth than an FDMA signal, since because of multiple time use, the gross data rate has to be correspondingly higher. For example, GSM systems employ a gross data rate (modulation data rate) of 271 kbit/ s on a subband of 200 kHz, which amounts to 33.9 kbit/ s for each of the eight time slots.

In addition, there are also frequency-selective co-channel interferences, which can contribute to the deterioration of the transmission quality. In a TDMA system, this leads to the phenomenon that the channel can be very good during one time slot, and very bad during the next time slot when some bursts are strongly interfered with. On the other hand, a TDMA system offers very good opportunities to

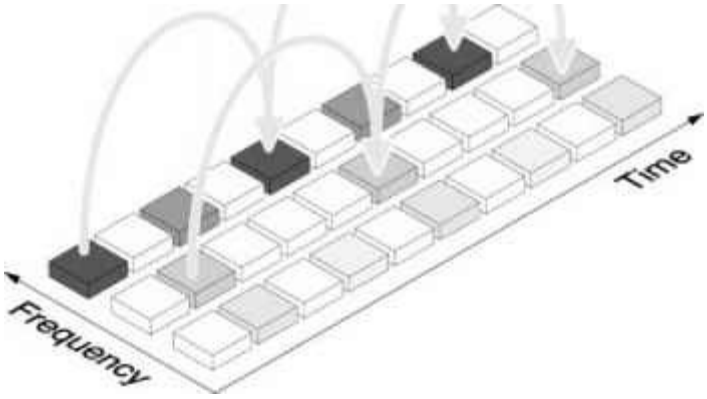


Figure : TDMA channels on multiple carrier frequencies

attack and drastically reduce such frequency-selective interference by introducing a frequency hopping technique. With this technique, each burst of a TDMA channel is transmitted on a different frequency (Figure).

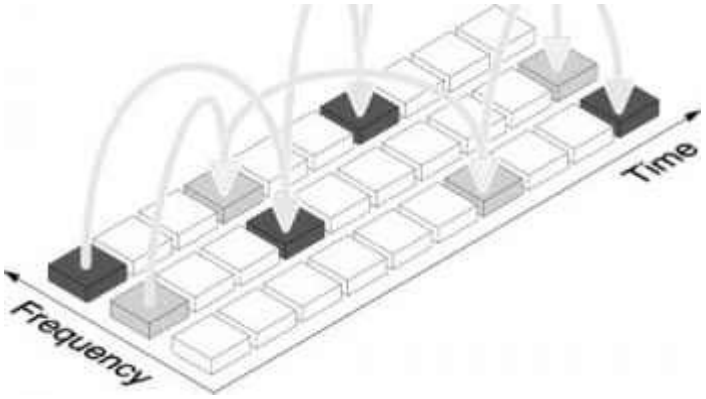


Figure : TDMA with use of frequency hopping technique

In this technique, selective interference on one frequency at worst hits only every ith time slot, if there are i frequencies available for hopping. Thus the signal transmitted by a frequency hopping technique uses frequency diversity. Of course, the hopping sequences must be orthogonal, i.e. one must ascertain that two stations transmitting in the same time slot do not use the same frequency. Since the duration of a hopping period is long compared to the duration of a symbol, this technique is called slow frequency hopping. With fast frequency hopping, the hopping period is shorter than a time slot and is of the order of a single symbol duration or even less. This technique then belongs already to the spread spectrum techniques of the family of code division multiple access techniques, Frequency Hopping CDMA (FH-CDMA).

As mentioned above, for TDM access, a precise synchronization between mobile and base station is necessary. This synchronization becomes even more complex through the mobility of the subscribers, because they can stay at varying distances from the base station and their signals thus incur varying propagation times. First, the basic problem is to determine the exact moment when to transmit. This is typically achieved by using one of the signals as a time reference, like the signal from the base station (Figure). On receiving the TDMA frame from the base station, the mobile can synchronize and transmit time slot synchronously with an additional time offset (e.g. three time slots in Figure).

Another problem is the propagation time of the signals, so far ignored. It also depends on the variable distance of the mobile station from the base. These propagation times are the reason why the signals on the uplink arrive not frame-synchronized at the base, but with variable delays. If these delays are not compensated, collisions of adjacent time slots can occur (Figure). In principle, the mobile stations must therefore advance the time-offset between reception and transmission, i.e. the start of sending, so much that the signals arrive frame-synchronous at the base station.

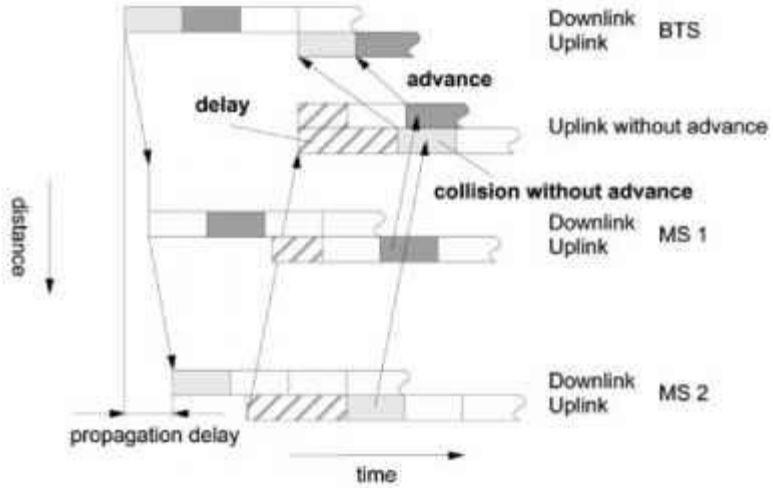


Figure : Differences in propagation delays and synchronization in TDMA systems

Code Division Multiple Access (CDMA)

Systems with Code Division Multiple Access (CDMA) are broadband systems, in which each subscriber uses the whole system bandwidth (similar to TDMA) for the complete duration of the connection (similar to FDMA). Furthermore, usage is not exclusive, i.e. all the subscribers in a cell use the same frequency band simultaneously. To separate the signals, the subscribers are assigned orthogonal codes. The basis of CDMA is a band-spreading or spread spectrum technique. The signal of one subscriber is spread spectrally over a multiple of its original bandwidth. Typically, spreading factors are between 10 and 1000; they generate a broadband signal for transmission from the narrowband signal, and this is less sensitive to frequency-selective interference and disturbances. Furthermore, the spectral power density is decreased by band spreading, and communication is even possible below the noise threshold.

Direct Sequence CDMA

A common spread-spectrum procedure is the direct sequence technique (Figure). In it the data sequence is multiplied directly - before modulation - with a spreading sequence to generate the band-spread signal. The bit rate of the spreading signal, the so-called chip rate, is obtained by multiplying the bit rate of the data signal by the spreading factor, which generates the desired broadening of the signal spectrum. Ideally, the spreading sequences are completely orthogonal bit sequences ("codes") with disappearing cross-correlation functions. Since such completely orthogonal sequences cannot be realized, practical systems use bit sequences from pseudo noise (PN) generators to spread the band. For dispreading, the signal is again multiplied with the spreading sequence at the receiver, which ideally recovers the data sequence in its original form.

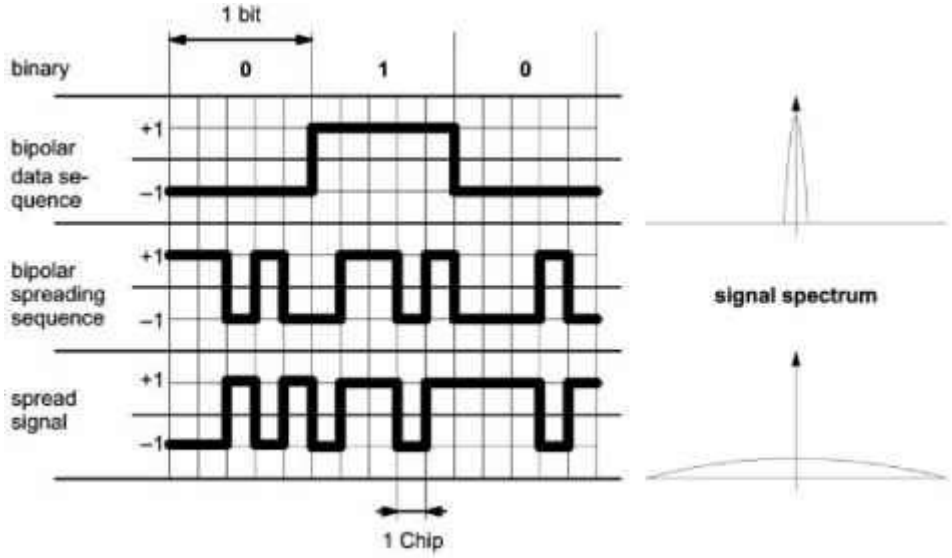


Figure : Principle of spread spectrum technique for direct sequence CDMA

Thus one can realize a code-based multiple access system. If an orthogonal family of spreading sequences is available, each subscriber can be assigned his or her own unique spreading sequence. Because of the disappearing cross-correlation of the spreading sequences, the signals of the individual subscribers can be separated in spite of being transmitted in the same frequency band at the same time.

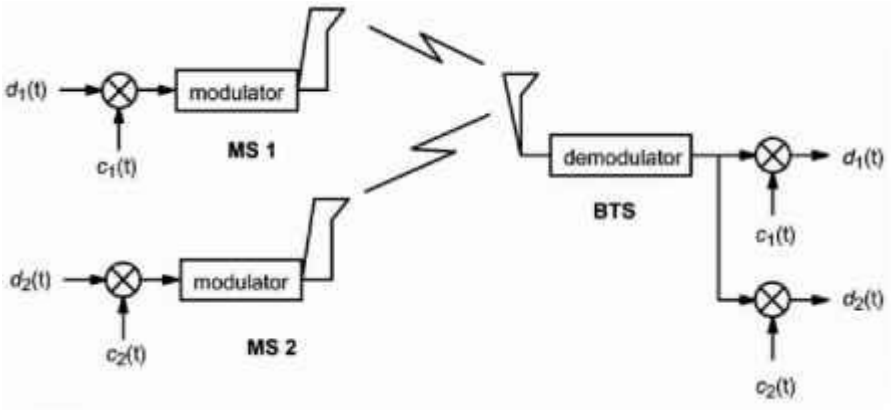


Figure : Simplified scheme of code division multiple access (uplink)

In a simplified way, this is done by multiplying the received summation signal with the respective code sequence (Figure). Thus, if direct sequence spreading is used, the procedure is called Direct Sequence Code Division Multiple Access (DS-CDMA).

Frequency Hopping CDMA

Another possibility for spreading the band is the use of a fast frequency hopping technique. If one changes the frequency several times during one transmitted data symbol, a similar spreading effect occurs as in case of the direct sequence procedure. If the frequency hopping sequence is again controlled by orthogonal code sequences, another multiple access system can be realized, the Frequency Hopping CDMA (FH-CDMA).

Space Division Multiple Access (SDMA)

An essential property of the mobile radio channel is multipath propagation, which leads to frequency-selective fading phenomena. Furthermore, multipath propagation is the cause of another significant property of the mobile radio channel, the spatial fanning out of signals. This causes the received signal to be a summation signal, which is not only determined by the Line of Sight (LOS) connection but also by an undetermined number of individual paths caused by refractions, infractions, and reflections. In principle, the directions of incidence of these multipath components could therefore be distributed arbitrarily at the receiver.

Especially on the uplink from the mobile station to the base station, there is, however, in most cases a main direction of incidence (usually LOS), about which the angles of incidence of the individual signal components are scattered in a relatively narrow range. Frequently, the essential signal portion at the receiver is distributed only over an angle of a few tens of degrees. This is because base stations are installed wherever possible as free-standing units, and there are no interference centers in the immediate neighborhood.

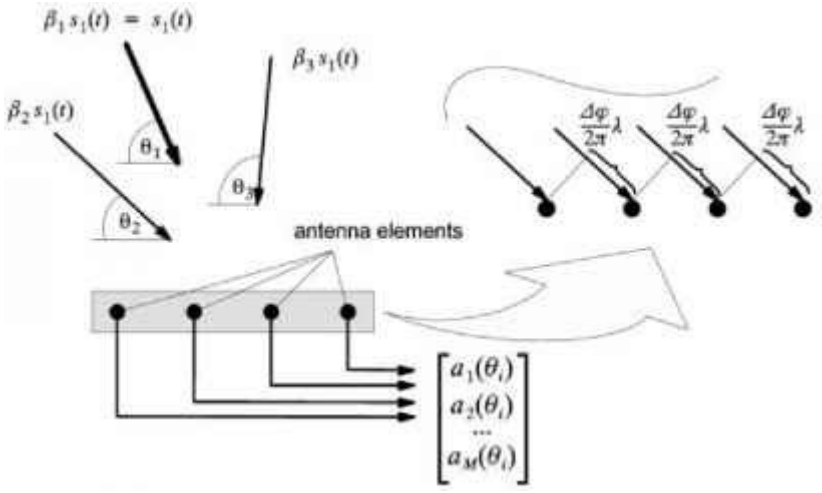


Figure Multipath signal at an antenna array

This directional selectivity of the mobile radio channel, which exists in spite of multipath propagation, can be exploited by using array antennas. Antenna arrays generate a directional characteristic by controlling the phases of the signals from the individual antenna elements. This allows the receiver to adjust the antenna selectively to the main direction of incidence of the received signal, and conversely to transmit selectively in one direction. This principle can be illustrated easily with a simple model (Figure).

The directional characteristics of the array antenna can be controlled adaptively such that a signal is only received or transmitted in exactly the spatial segment where a certain mobile station is currently staying. On the one hand, one can thus reduce co-channel interference in other cells, and on the other hand, the sensitivity against interference can be reduced in the current cell. Furthermore, because of the spatial separation, physical channels in a cell can be reused, and the lobes of the antenna diagram can adaptively follow the movement of mobile stations. In this case, yet another

multiple access technique (Figure 2.13) is defined and known as Space Division Multiple Access (SDMA).

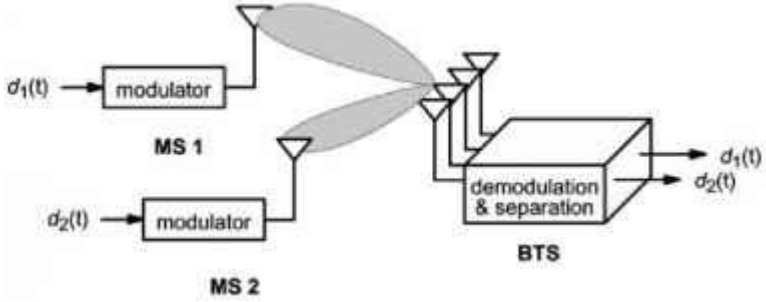


Figure : Schematic representation of spatial multiple access (uplink)

SDMA systems are currently the subject of intensive research. The SDMA technique can be combined with each of the other multiple access techniques (FDMA, TDMA, CDMA). This enables intracellular spatial channel reuse, which again increases the network capacity. This is especially attractive for existing networks which can use an intelligent implementation of SDMA by selectively upgrading base stations with array antennas, appropriate signal processing, and respective control protocols.

Mobile computing through telephone

One of the early examples of mobile computing was accessing applications and services through voice interface. This technology was generally referred to as computer telephony interface. Different banks around the world were offering telephone banking for quite sometime using this technology. In a telephone banking application, the user calls a number and then does his banking transaction through a fixed telephone. In this application the telephone does many functions of a bank teller. Input to this system is a telephone keyboard and output is a synthesized voice. These applications can be used from anywhere in the world. The only issue in this case is the cost of a call.

The telephone companies soon came up with a brilliant idea to solve this problem of multiple numbers by offering 800 services using Intelligent Networks technology. This also commonly known as TOLL Free numbers. In this technology only one number like 1-800-2MYBANK is published. The number is not attached to any specific exchange or

any specific city. When a subscriber calls this number an optimal routing is done and the call is connected to the nearest service center.

To make this type of mobile computing work through voice interfaces, we use interactive voice response. In USA and Japan IVRs are commonly known as Voice Response Unit. The technical name for this technology is Computer Telephony. IVR software can be hosted on a Windows-NT, Linus, or other computers with the voice cards. There are many companies who manufacture voice cards; however, one of the most popular card vendors is from Inter/Dialogic. IVR works as the gateway between a voice based telephone system and a computer system. Multiple telephonelines are connected to the voice card through appropriate telecom interfaces. When a caller dials the IVR number , a ring tone is received by the voice card with in the IVR. The voice card answers the call and establishes a connection between the caller and the IVR application.

Developing an IVR application

Like any other application development, computer telephony/IVR application development also requires definition of the user interface. The user interface in IVR application is called the call flow. In a call flow we define how the call will be managed. Let us take a simple example of ticket booking in a theatre. In this application, the user dials a service number and enters a phone number. The operator calls the user back and accepts the booking request. The extra step of call back is done for security reason.

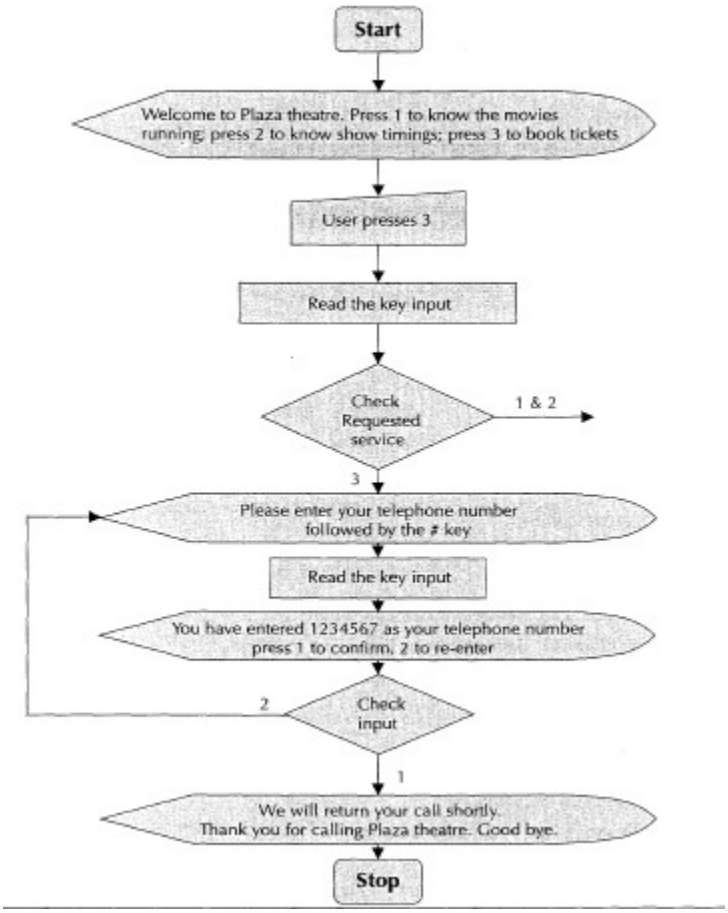


Figure: Call flow for a theatre ticket booking

Voice XML

In mobile computing through telephone, the IVR is connected to the server through client/server architecture. It is also possible to host the IVR and the application on the same system. Today internet is used in addition to client/server interface between the IVR and the server. This increase the flexibility in the whole mobile computing architecture. Http is used for voice portals as well. In the case of a voice portal, a user uses an internet site through voice interface. For all these advanced features, VoiceXML has been introduced. Recent IVRs are equipped with DSP and are capable or recognizing voice. The output is synthesized voice through TTS(Text to speech).

The voice eXtensible Markup Language is an XML based markup language for creating

distributed voice applications. VoiceXML is designed for creating audio dialogs that feature synthesized speech, digitized audio, recognition of spoken voice and DTMF key input. Using VoiceXML, we can create web-based voice applications that users can access through telephone.

Voice XML supports dialog that feature:

- Spoken input
- DTMF(telephone key) input
- Recording of spoken input
- Synthesized speech output.
- Recorded audio output
- Dialog flow control
- Scoping of input.

Telephony Application Programming Interface.

TAPI(Telephony Application Programming Interface and Speech Application Programming Interface) are two standards that can be used when developing voice telephony applications. Using TAPI, programmers can take advantage of different telephone systems, including ordinary PSTN,ISDN and PBX(Private Branch Exchange) without having to understand all their details. Use of these API will save the programmer the pain of trying to program hardware directly. Through TAPI and SAPI a program can talk over telephones or video phones to people or phone connected resources. Through TAPI one will be able to:

- Simple user interfaces to setup calls. This can be calling someone by clicking on their picture or other images.
- Use simple graphical interface to set up a conference call and then attend the call at the scheduled time.
- See who yor’re talking to.
- Attach voice greeting with an email. This will allow the receiver to listen to this greeting while opening the email.

- Set groups and security measures such that a service can receive phone calls from certain numbers
- Send and receive faxes
- Same set of TAPI APIs are available in many smart phones.

Emerging Technologies:

Introduction

Bluetooth is a technology in the personal area network. RFID is emerging as a leading technology in the logistics, manufacturing, and retail industry.

Bluetooth

Bluetooth is a wireless technology standard for exchanging data between fixed and mobile devices over short distances using short-wavelength UHF radio waves in the industrial, scientific and medical radio bands, from 2.400 to 2.485 GHz, and building personal area networks (PANs). It was originally conceived as a wireless alternative to RS-232 data cables.

Bluetooth is managed by the Bluetooth Special Interest Group (SIG), which has more than 35,000 member companies in the areas of telecommunication, computing, networking, and consumer electronics. The IEEE standardized Bluetooth as **IEEE 802.15.1**, but no longer maintains the standard. The Bluetooth SIG oversees development of the specification, manages the qualification program, and protects the trademarks. A manufacturer must meet Bluetooth SIG standards to market it as a Bluetooth device. A network of patents apply to the technology, which are licensed to individual qualifying devices. As of 2009, Bluetooth integrated circuit chips ship approximately 920 million units annually.

A master BR/EDR Bluetooth device can communicate with a maximum of seven devices in a piconet (an ad-hoc computer network using Bluetooth technology), though not all devices reach this maximum. The devices can switch roles, by agreement, and the slave can become the master (for example, a headset initiating a connection to a

phone necessarily begins as master—as an initiator of the connection—but may subsequently operate as the slave).

The Bluetooth Core Specification provides for the connection of two or more piconets to form a scatternet, in which certain devices simultaneously play the master role in one piconet and the slave role in another.At any given time, data can be transferred between the master and one other device (except for the little-used broadcast mode). The master chooses which slave device to address; typically, it switches rapidly from one device to another in a round-robin fashion. Since it is the master that chooses which slave to address, whereas a slave is (in theory) supposed to listen in each receive slot, being a master is a lighter burden than being a slave. Being a master of seven slaves is possible; being a slave of more than one master is possible. The specification is vague as to required behavior in scatternets.

Radio Frequency Identification

Radio-frequency identification (**RFID**) uses electromagnetic fields to automatically identify and track tags attached to objects. The tags contain electronically stored information. Passive tags collect energy from a nearby RFID reader's interrogating radio waves. Active tags have a local power source (such as a battery) and may operate hundreds of meters from the RFID reader. Unlike a barcode, the tags don't need to be within the line of sight of the reader, so it may be embedded in the tracked object. RFID is one method of automatic identification and data capture (AIDC).

RFID tags are used in many industries. For example, an RFID tag attached to an automobile during production can be used to track its progress through the assembly line; RFID-tagged pharmaceuticals can be tracked through warehouses; and implanting RFID microchips in livestock and pets enables positive identification of animals.Since RFID tags can be attached to cash, clothing, and possessions, or implanted in animals and people, the possibility of reading personally-linked information without consent has raised serious privacy concerns. These concerns resulted in standard specifications development addressing privacy and security issues. ISO/IEC 18000 and ISO/IEC

29167 use on-chip cryptography methods for untraceability, tag and reader authentication, and over-the-air privacy. ISO/IEC 20248 specifies a digital signature data structure for RFID and barcodes providing data, source and read method authenticity. This work is done within ISO/IEC JTC 1/SC 31 Automatic identification and data capture techniques. Tags can also be used in shops to expedite checkout, and to prevent theft by customers and employees.

Wireless broadband

Wireless technologies are proliferating in a major way in to the first-mile or last-mile subscriber access, as opposed to twisted-pair local loop. These technologies are generally referred to as Wireless local loop. Wireless local loop is also known as fixed wireless system .the world is moving towards a convergence of voice, data and video.

IEEE 802.6 is a standard governed by the ANSI for Metropolitan Area Networks (**MAN**). It is an improvement of an older standard (also created by ANSI) which used the Fiber distributed data interface (FDDI) network structure. The **IEEE 802.6** standard uses the Distributed Queue Dual Bus (DQDB) network form.

- IEEE 802.16 air interface for fixed broadband wireless access systems, also called wireless MAN or wireless local loop, has protocol stack:
    - It provides multimegabits wireless services for voice, Internet, movies on demand, etc.
- Physical layer operates in 10 to 66 GHz range, and base has multiple antennas, each pointing at a separate sector.

  For close-in subscribers, 64QAM is used, so typical 25 MHz spectrum offers 150 Mbps; for medium-distance subscribers, 16QAM is used; and for distant subscribers QPSK is used
- Data link layer consists of three sublayers

  – Security sublayer manages encryption, decryption, and key management, crucial for privacy and security

– Service-specific convergence replaces logical link control, providing seamlessly interface for network layer that may have both datagram protocols and ATM

MAC Sublayer Protocol

802.16 MAC sublayer is completely connection oriented to provide quality-of-service guarantees for telephony and multimedia, and MAC frames occupy integral number of physical layer time slots Each frame is composed of subframes, and the first two are downstream and upstream maps

– These two maps tell what is in which time slot and which time slots are free.

– Downstream map also contains system parameters to inform new users as they come on-line • Downstream channel: base simply decides what to put in which subframe

• Upstream channel: there are competing subscribers and its allocation is tied to class of service

– Constant bit rate: dedicate certain time slots to each connection and bandwidth is fixed through the connection, providing typical telephone channel service

– Real-time variable bit rate: for compressed multimedia and other soft real-time applications in which bandwidth needed each instant may vary Base polls subscriber at fixed interval to ask how much bandwidth is needed this time.

– Non-real-time variable bit rate: for non-real-time heavy transmissions such as large file transfers Base polls subscribers often at non rigidly defined intervals to see who needs this service.

– Best-efforts: no polling and subscriber contends for bandwidth with others.

Requests for bandwidth are done in time slots marked in upstream map as available for contention.

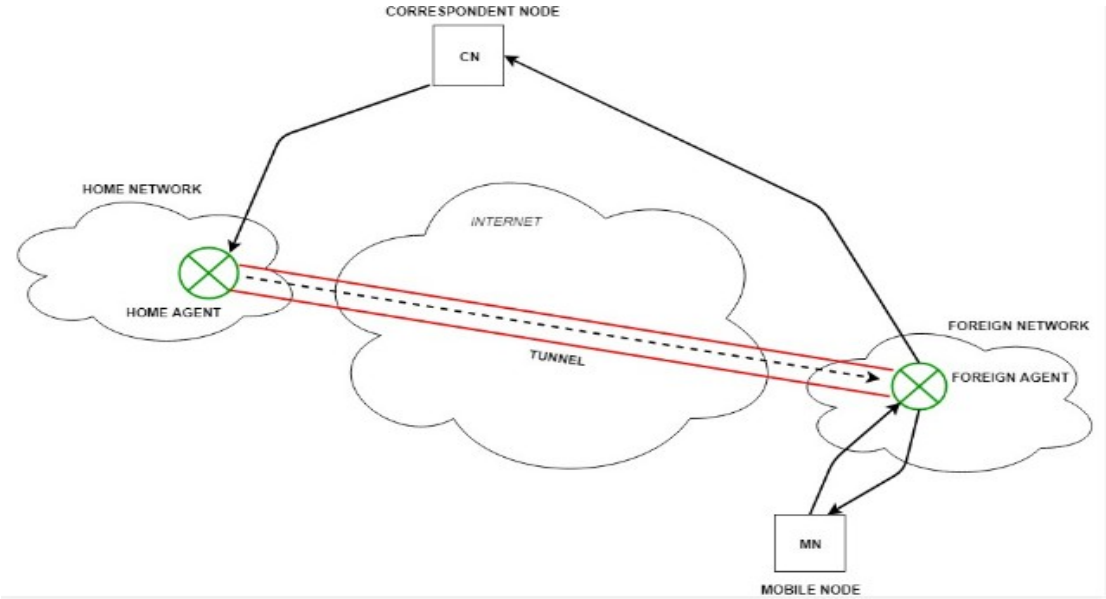
Successful request will be noted in next downstream map, and unsuccessful subscriber has to wait a random period of time before try again

Mobile IP

Mobile IP is a communication protocol (created by extending Internet Protocol, IP) that allows the users to move from one network to another with the same IP address. It ensures that the communication will continue without user's sessions or connections being dropped.

Terminologies:

- **Mobile Node (MN):**
  It is the hand-held communication device that the user caries e.g. Cell phone.
- **Home Network:**
  It is a network to which the mobile node originally belongs to as per its assigned IP address (home address).
- **Home Agent (HA):**
  It is a router in home network to which the mobile node was originally connected
- **Home Address:**
  It is the permanent IP address assigned to the mobile node (within its home network).
- **Foreign Network:**
  It is the current network to which the mobile node is visiting (away from its home network).
- **Foreign Agent (FA):**
  It is a router in foreign network to which mobile node is currently connected. The packets from the home agent are sent to the foreign agent which delivers it to the mobile node.
- **Correspondent Node (CN):**
  It is a device on the internet communicating to the mobile node.
- **Care of Address (COA):**
  It is the temporary address used by a mobile node while it is moving away from its home network.



Working:

Correspondent node sends the data to the mobile node. Data packets contains correspondent node's address (Source) and home address (Destination). Packets reaches to the home agent. But now mobile mode is not in the home network, it has moved into the foreign network. Foreign agent sends the care-of-address to the home agent to which all the packets should be sent. Now, a tunnel will be established between the home agent and the foreign agent by the process of tunneling.

Tunneling establishes a virtual pipe for the packets available between a tunnel entry and an endpoint. It is the process of sending a packet via a tunnel and it is achieved by a mechanism called encapsulation.

Now, home agent encapsulates the data packets into new packets in which the source address is the home address and destination is the care-of-address and sends it through the tunnel to the foreign agent. Foreign agent, on other side of the tunnel receives the data packets, decapsulates them and sends them to the mobile node. Mobile node in response to the data packets received, sends a reply in response to foreign agent. Foreign agent directly sends the reply to the correspondent node.

Key Mechanisms in Mobile IP:

Agent Discovery:

Agents advertise their presence by periodically broadcasting their agent advertisement messages. The mobile node receiving the agent advertisement messages observes whether the message is from its own home agent and determines whether it is in the home network or foreign network.

Agent Registration

Mobile node after discovering the foreign agent, sends registration request (RREQ) to the foreign agent. Foreign agent in turn, sends the registration request to the home agent with the care-of-address. Home agent sends registration reply (RREP) to the foreign agent. Then it forwards the registration reply to the mobile node and completes the process of registration.

Tunneling:

It establishes a virtual pipe for the packets available between a tunnel entry and an endpoint. It is the process of sending a packet via a tunnel and it is achieved by a mechanism called encapsulation. It takes place to forward an IP datagram from the home agent to the care-of-address. Whenever home agent receives a packet from correspondent node, it encapsulates the packet with source address as home address and destination as care-of-address.

Route Optimization in Mobile IP

The route optimization adds a conceptual data structure, the binding cache, to the correspondent node. The binding cache contains bindings for mobile node's home address and its current care-of-address. Every time the home agent receives a IP datagram that is destined to a mobile node currently away from the home network, it sends a binding update to the correspondent node to update the information in the

correspondent node's binding cache. After this the correspondent node can directly tunnel packets to the mobile node.

Internet Protocol version 6 - Java card.

IP v6 was developed by Internet Engineering Task Force (IETF) to deal with the problem of IP v4 exhaustion. IP v6 is 128-bits address having an address space of 2^128, which is way bigger than IPv4. In IPv6 we use Colon-Hexa representation. There are 8 groups and each group represents 2 Bytes.

In IPv6 representation, we have three addressing methods :

- Unicast
- Multicast
- Anycast

Unicast Address: Unicast Address identifies a single network interface. A packet sent to unicast address is delivered to the interface identified by that address.

Multicast Address: Multicast Address is used by multiple hosts, called as Group, acquires a multicast destination address. These hosts need not be geographically together. If any packet is sent to this multicast address, it will be distributed to all interfaces corresponding to that multicast address.

Anycast Address: Anycast Address is assigned to a group of interfaces. Any packet sent to anycast address will be delivered to only one member interface (mostly nearest host possible).

UNIT III

GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

- GSM stands for **G**lobal **S**ystem for **M**obile Communication. It is a digital cellular technology used for transmitting mobile voice and data services.
- The concept of GSM emerged from a cell-based mobile radio system at Bell Laboratories in the early 1970s.
- GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard.
- GSM is the most widely accepted standard in telecommunications and it is implemented globally.
- GSM is a circuit-switched system that divides each 200 kHz channel into eight 25 kHz time-slots. GSM operates on the mobile communication bands 900 MHz and 1800 MHz in most parts of the world. In the US, GSM operates in the bands 850 MHz and 1900 MHz.
- GSM owns a market share of more than 70 percent of the world's digital cellular subscribers.
- GSM makes use of narrowband Time Division Multiple Access (TDMA) technique for transmitting signals.
- GSM was developed using digital technology. It has an ability to carry 64 kbps to 120 Mbps of data rates.
- Presently GSM supports more than one billion mobile subscribers in more than 210 countries throughout the world.
- GSM provides basic to advanced voice and data services including roaming service. Roaming is the ability to use your GSM phone number in another GSM network.

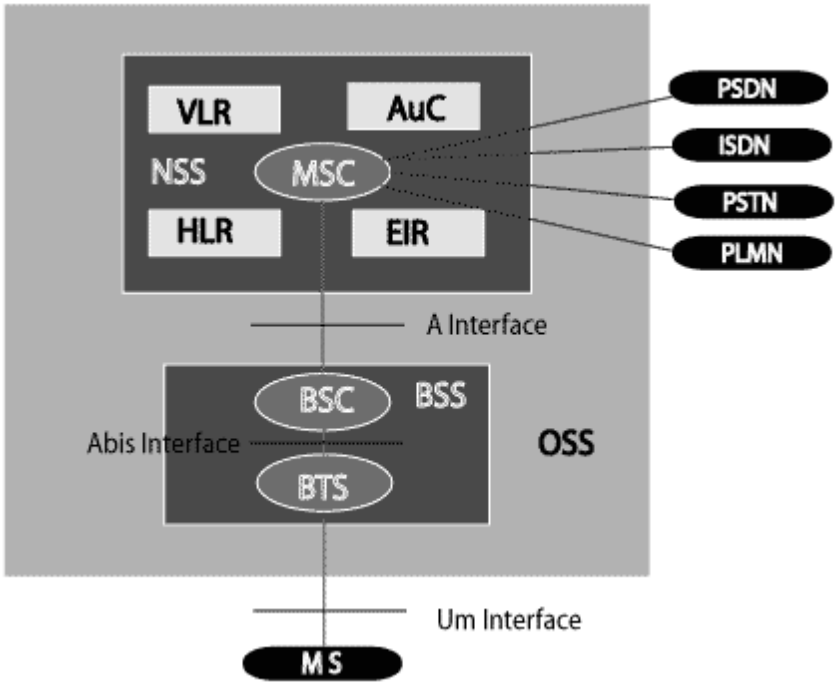
GSM digitizes and compresses data, then sends it down through a channel with two other streams of user data, each in its own timeslot.

GSM Architecture

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

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

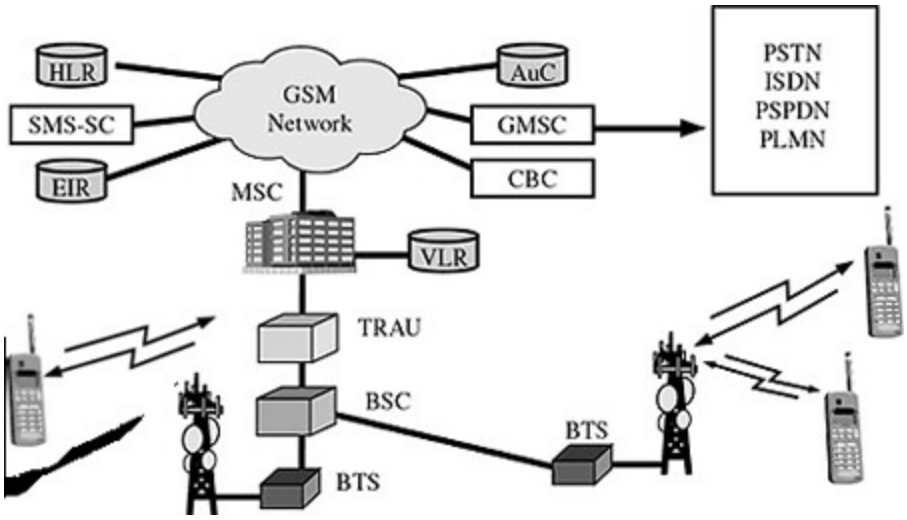
Given below is a simple pictorial view of the GSM architecture.



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

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

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



The MS and the BSS communicate across the Um interface. It is also known as the *air interface* or the *radio link*. The BSS communicates with the Network Service Switching (NSS) center across the *A* interface.

GSM network areas

In a GSM network, the following areas are defined:

- **Cell** : Cell is the basic service area; one BTS covers one cell. Each cell is given a Cell Global Identity (CGI), a number that uniquely identifies the cell.
- **Location Area** : A group of cells form a Location Area (LA). This is the area that is paged when a subscriber gets an incoming call. Each LA is assigned a Location Area Identity (LAI). Each LA is served by one or more BSCs.
- **MSC/VLR Service Area** : The area covered by one MSC is called the MSC/VLR service area.
- **PLMN** : The area covered by one network operator is called the Public Land Mobile Network (PLMN). A PLMN can contain one or more MSCs.

GSM Entities

The GSM technical specifications define different entities that form the GMS network by defining their functions and interface requirements. The GSM network can be divided in to four main groups.

The mobile station. - This includes the mobile equipment and the subscriber identify module

The Base station subsystem. - This includes the base transceiver station and the base station controller.

The network and switching substystem. – This includes mobile switching center. Home location register, visitor location register, Equipment identity register, and the Authentication Center.

The operation and support subsystem- This includes the operation and maintenance center.

Mobile Station

Mobile station is the technical name of the mobile or the cellular phone. In early days mobile phones were a little bulky and were sometimes installed in cars like other equipment's. Even the handheld terminals were quite big. Though the phones have become smaller and lighter, they are still called mobile station. Mobile station consists of two main elements. The mobile equipment or the mobile device. In otherwords, this is the phone without the SIM card. The subscriber identity module. These are different types of terminals distinguished principally by their power and application. The handheld GSM terminals have experienced the highest evolution. The weight and volume of these terminals are continuously decreasing.

Base Station subsystem

The BSS connects the mobile station and the NSS(Network and Switching Subsystem). It is in charge of the transmission and reception for the last mile. The BSS can be divided into two parts.

The Base Transceiver station corresponds to the transceivers and antennas used in each cell othe network. In a large urban area, a large number of BTSs are potentially

deployed. A BTS is usually placed in the center of a cell. Its transmitting power defines the size of a cell.

The Base Station controller is the connection between the BTS and mobile service switching center. The BSC manages the radio resources for one or more BTSs. It handles handovers, radio channel setup, control of radio frequency power levels of the BTSs, exchange function, and the frequency hopping.

Network and switching subsystem

The central component of the network subsystem in the mobile switching center. It does multiple functions.

- It acts like a normal switching node for mobile subscribers of the same network.
- It acts like a normal switching node for the PSTN fixed telephone
- It acts like a normal switching node for ISDN
- It provides all the functionality needed to handle a mobile subscriber such a registration, authentication, locating updating, handovers and call routing.
- It includes databases needed in order to store information to manage the mobility of a roaming subscriber.

Call routing in GSM

Human interface is analog. However, the advancement in digital technology makes it very convenient to handle information in digital fashion. In GSM there are many complex technologies used between the human analog interface in the mobile and the digital network.

Digitizer and source coding.

The user speech is digitized at 8 Khz sampling rate using Regular Pulse Excited – Linear Predictive coder(RPEC-LPC) with a long term predictor loop where information from previous samples is used to predict the current sample. Each sample is then represented in signed 13-bit linear PCM value. The digitized data is passed to the coder with frames of 160 samples where encoder compresses these 160 samples in to 260

bits. GSM frames resulting in one second of speech compresed into 1625 bytes and achieving a rate of 13 Kbits/sec

Channel Coding

This introduces redundancy into the data for error detection and possible error correction where the gross bit rate after channel coding is 22.8kbps. These 456 bits are divided into eight 57-bit blocks and the result is interleaved amongst eight successive time slot bursts for protection against burst transmission errors. Interleaving this step rearranges a group of bits in a particular way to improve the performance of the error correction mechanisms. The interleaving decreases the possibility of losing whole bursts during the transmission by dispersing the errors.

Ciphering

This encrypts blocks of user data using a symmetric key shared by the mobile station and the BTS. **Burst formatting**

It adds some binary information the ciphered block for use in synchronization and equalization of the received data.

Modulation

This techniques chosen for the GSM system is the Gaussian Minimum shift keying where binary data is converted back into analog signal to fit the frequency and the time requirements for the multiple access rules. This signal is then radiated as radio wave over the air.

Multipath and equalization

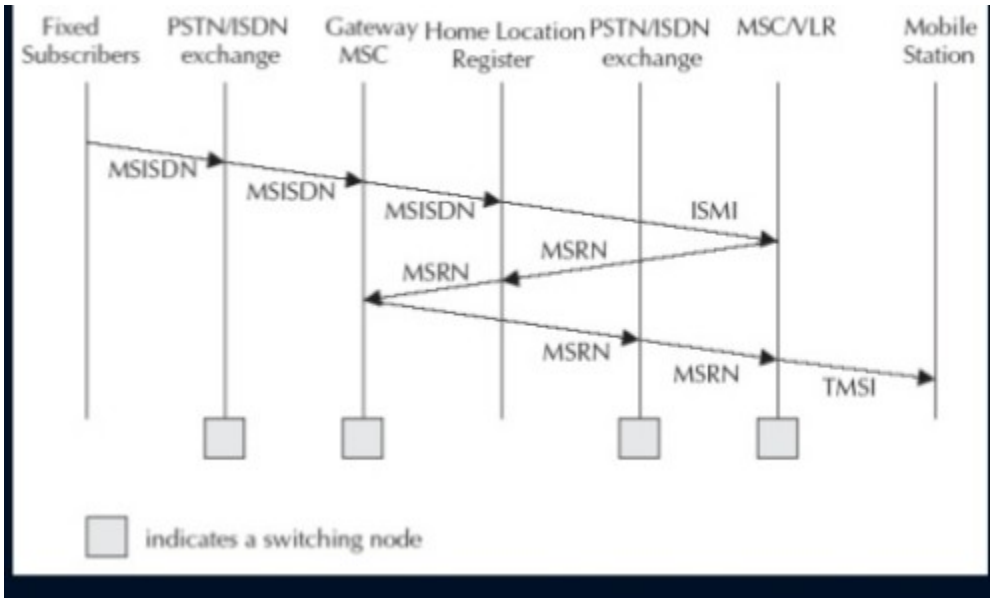
An equalizer is in charge of extracting the right signal from the received signal while estimating the channel impulse response of the GSM system and then it constructs an inverse filter/ The received signal is then passed through the inverse filter

Synchronization

For successful operation of a mobile radio system, time and frequency synchronization are needed. Frequency synchronization is necessary so that the transmitter and receiver frequency match while time synchronization is necessary to identify the frame boundary and the bits within the frame.

Call Routing

- The call first goes to the local PSTN exchange where PSTN exchange looks at the routing table and determines that it is a call to a mobile networks.
- PSTN forwards the call to the Gateway MSC of the mobile network.
- MSC enquires the HLR to determine the status of the subscriber. It will decide whether the call is to be routed or not. If MSC finds that the call can be processed, it will find out the address of the VLR where the mobile is expected to be present
- If VLR is that of a different PLMN, it will forward the call to the foreign PLMN through the Gateway MSC. If the VLR is in the home network, it will determine the Location area.
- Within the LA, it will page and locate the phone and connect the call.



PLMN Interfaces

A public land mobile network (PLMN) is any wireless communications system intended for use by terrestrial subscribers in vehicles or on foot. Such a system can stand alone, but often it is interconnected with a fixed system such as the public switched telephone network (PSTN). The most familiar example of a PLMN end user is a person with a cell phone. However, mobile and portable Internet use is also becoming common.

The ideal PLMN provides mobile and portable users with a level of service comparable to that of subscribers in a fixed network. This can be a special challenge in regions where the terrain is irregular, where base station sites are hard to find and maintain, and in urban environments where there are numerous obstructions such as buildings, and myriad sources of radio-frequency (RF) radiation that can cause noise and interference. Most systems today use digital technology rather than the older analog methods. This transition has resulted in improved communications coverage and reliability, but as anyone who regularly uses a cellular telephone knows, perfection has yet to be achieved.

A PLMN requires special security measures because a wireless system is inherently more susceptible to eavesdropping and unauthorized use than a hard-wired system. Smart cards containing user data, encryption/decryption, and biometric verification schemes can minimize this problem.

GSM address and identifiers

GSM treats the users and the equipment in different ways. Phone numbers, subscribers, and equipment identifiers are some of the known ones. There are many other identifiers that have been well-defined, which are required for the subscriber's mobility management and for addressing the remaining network elements. Vital addresses and identifiers that are used in GSM are addressed below.

International Mobile Station Equipment Identity (IMEI)

The International Mobile Station Equipment Identity (IMEI) looks more like a serial number which distinctively identifies a mobile station internationally. This is allocated

by the equipment manufacturer and registered by the network operator, who stores it in the Equipment Identity Register (EIR). By means of IMEI, one recognizes obsolete, stolen, or non-functional equipment.

Following are the parts of IMEI:

- **Type Approval Code (TAC)** : 6 decimal places, centrally assigned.
- **Final Assembly Code (FAC)** : 6 decimal places, assigned by the manufacturer.
- **Serial Number (SNR)** : 6 decimal places, assigned by the manufacturer.
- **Spare (SP)** : 1 decimal place.

Thus, IMEI = TAC + FAC + SNR + SP. It uniquely characterizes a mobile station and gives clues about the manufacturer and the date of manufacturing.

International Mobile Subscriber Identity (IMSI)

Every registered user has an original International Mobile Subscriber Identity (IMSI) with a valid IMEI stored in their Subscriber Identity Module (SIM).

IMSI comprises of the following parts:

- **Mobile Country Code (MCC)** : 3 decimal places, internationally standardized.
- **Mobile Network Code (MNC)** : 2 decimal places, for unique identification of mobile network within the country.
- **Mobile Subscriber Identification Number (MSIN)** : Maximum 10 decimal places, identification number of the subscriber in the home mobile network.

Mobile Subscriber ISDN Number (MSISDN)

The authentic telephone number of a mobile station is the Mobile Subscriber ISDN Number (MSISDN). Based on the SIM, a mobile station can have many MSISDNs, as each subscriber is assigned with a separate MSISDN to their SIM respectively.

Listed below is the structure followed by MSISDN categories, as they are defined based on international ISDN number plan:

- **Country Code (CC)** : Up to 3 decimal places.
- **National Destination Code (NDC)** : Typically 2-3 decimal places.
- **Subscriber Number (SN)** : Maximum 10 decimal places.

Mobile Station Roaming Number (MSRN)

Mobile Station Roaming Number (MSRN) is an interim location dependent ISDN number, assigned to a mobile station by a regionally responsible Visitor Location Register (VLA). Using MSRN, the incoming calls are channeled to the MS.

The MSRN has the same structure as the MSISDN.

- **Country Code (CC)** : of the visited network.
- **National Destination Code (NDC)** : of the visited network.
- **Subscriber Number (SN)** : in the current mobile network.

Location Area Identity (LAI)

Within a PLMN, a Location Area identifies its own authentic Location Area Identity (LAI). The LAI hierarchy is based on international standard and structured in a unique format as mentioned below:

- **Country Code (CC)** : 3 decimal places.
- **Mobile Network Code (MNC)** : 2 decimal places.
- **Location Area Code (LAC)** : maximum 5 decimal places or maximum twice 8 bits coded in hexadecimal (LAC < FFFF).

Temporary Mobile Subscriber Identity (TMSI)

Temporary Mobile Subscriber Identity (TMSI) can be assigned by the VLR, which is responsible for the current location of a subscriber. The TMSI needs to have only local significance in the area handled by the VLR. This is stored on the network side only in the VLR and is not passed to the Home Location Register (HLR).

Together with the current location area, the TMSI identifies a subscriber uniquely. It can contain up to 4 × 8 bits.

Local Mobile Subscriber Identity (LMSI)

Each mobile station can be assigned with a Local Mobile Subscriber Identity (LMSI), which is an original key, by the VLR. This key can be used as the auxiliary searching key for each mobile station within its region. It can also help accelerate the database

access. An LMSI is assigned if the mobile station is registered with the VLR and sent to the HLR. LMSI comprises of four octets (4x8 bits).

Cell Identifier (CI)

Using a Cell Identifier (CI) (maximum 2 × 8) bits, the individual cells that are within an LA can be recognized. When the Global Cell Identity (LAI + CI) calls are combined, then it is uniquely defined.

Network aspects in GSM

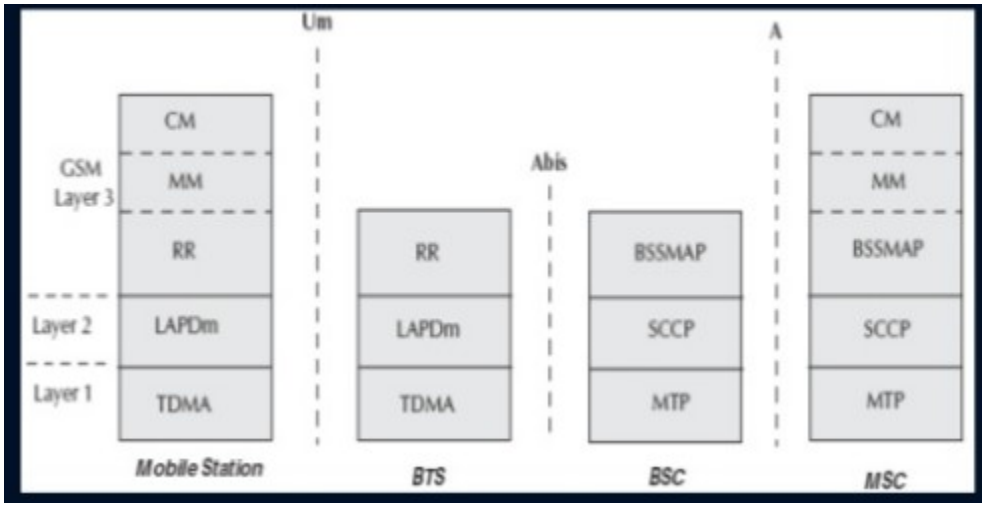


Figure Signaling protocol structure in GSM

MS Protocols

Based on the interface, the GSM signaling protocol is assembled into three general layers:

- **Layer 1** : The physical layer. It uses the channel structures over the air interface.
- **Layer 2** : The data-link layer. Across the Um interface, the data-link layer is a modified version of the Link access protocol for the D channel (LAP-D) protocol used in ISDN, called Link access protocol on the Dm channel (LAP-Dm). Across the A interface, the Message Transfer Part (MTP), Layer 2 of SS7 is used.
- **Layer 3** : GSM signalling protocol's third layer is divided into three sublayers:
    - Radio Resource Management (RR), - It controls the set-up maintenance and termination of radio and fixed channels including handovers.

- Mobility Management (MM), and – It manages the location updating and registration procedures as well as security and authenticaton
- Connection Management (CM)- it handles general call control and manages supplementary services and the short message service.

Mobility management

Mobility management is a functionality that facilitates mobile device operations in Universal Mobile Telecommunications System (UMTS) or Global System for Mobile Communications (GSM) networks. Mobility management is used to trace physical user and subscriber locations to provide mobile phone services, like calls and Short Message Service (SMS).

GSM Frequency Allocation

Each way the bandwidth for the GSM system is 25 MHz which provides 125 carriers uplink/downlink each having a bandwidth of 200 Khz. ARFCN denote a forward and reverse channel pair which is separated in frequency by 45 MHz.Practically a guard band of 100 kHZ is provided at the upper and lower end of the GSM 900 MHz spectrum and only 124 channels are implemented.

GSM uses TDMA and FDMA one or more carrier frequencies are assigned to each base station and each of these carrier frequencies is then divided in time using a TDMA scheme where fundamental unit is called a burst period lasting approximately 0.577ms. Eight burst periods are grouped into a TDMA frame of approximately 4.615ms which forms the basic unit for the definition of logical channels. One physical channel is one burst period per TDMA frame while, normally channels are defined by the number and position of their corresponding burst periods.

Authentication and Security.

Authentication In GSM

1. The security procedures in GSM are aimed at protecting the network against unauthorized access and protecting the privacy of mobile subscriber against eavesdropping,

2. Eavesdropping on subscriber communication is prevented by ciphering the information.
3. To protect identity and location of the subscriber the appropriate signalling channels are ciphered and Temporary Subscriber Identity (TMSI) instead of IMSI is used over the radio path.
4. At the time of initiating a service, the mobile terminal is powered on the subscriber may be required to enter 4-8 digits Password Identification Number (PIN) to validate the ownership of the SIM.
5. At the time of service provisioning the IMSI, the individual subscriber authentication key (Ki), the authentication algorithm (A3), the cipher key generation algorithm (A8) and the encryption algorithm (A5) are programmed into the SIM by GSM operator.
6. The A3 ciphering algorithm is used to authenticate each mobile by verifying the user password within the SIM with the cryptographic key at the MSC. The A5 ciphering algorithm is used for encryption. It provides scrambling for 114 coded bits sent in each TS. The A8 is used for ciphering key.
7. The IMSI and the secret authentication key (Ki) are specific to each mobile station, the authentication algorithm A3 and A8 are different for different networks and operators encryption algorithm A5 is unique and needs to be used across all GSM network operators.
8. The authentication centre is responsible for all security aspects and its function is closely linked with HLR.
9. The secret authentication key (Ki) is not known to mobile user and is the property of service provider, the home system of the mobile station (MS) generates the random number say Rand which is 126 bit number. This random number is sent to MS. The MS uses A3 algorithm to authenticate the user. The algorithm A3 uses Ki and Rand number to generate a signed result called s_RES. MS sends s_RES to home system of MS.
10. In the home system authentication contains Ki and it also uses the same authentication algorithm A3 to authenticate the valid user. The A3 algorithm use Ki and Rand generated by home system to generate a signed result

called 〖(s〗_RES). The s_RES generated by MS and authentication centre are compared. If both s_RES are identical only then the user is valid and access is granted otherwise not.

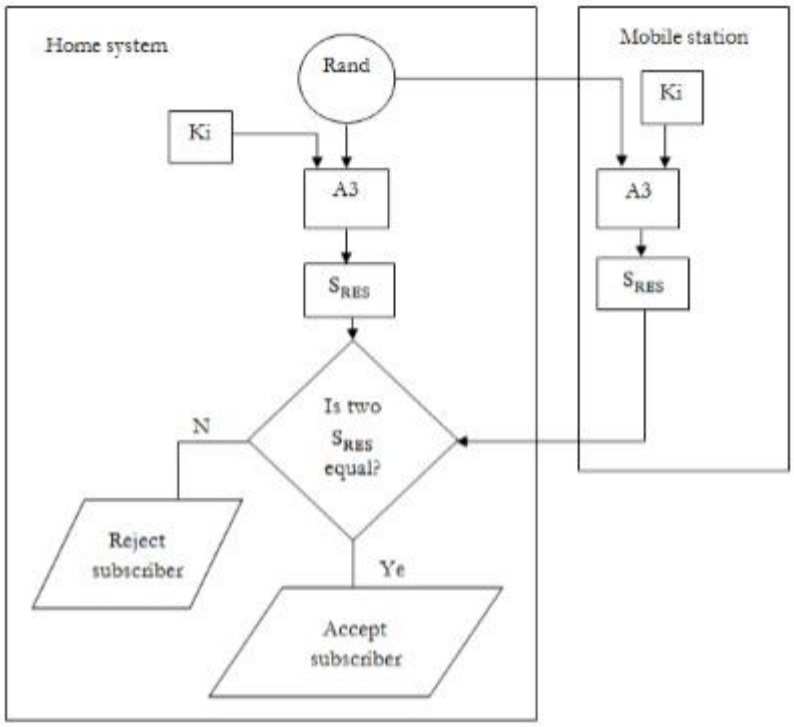


Fig: Authentication in GSM

Security in GSM

GSM allows three-band phones to be used seamlessly in more than 160 countries. In GSM, security is implemented in three entities:

1) Subscriber identity module (SIM) contains authentication key Ki (64-bit), ciphering key (Kc) generating algorithm, and authentication algorithm. SIM is a single chip computer containing the operating system (OS), the file system, and applications. SIM is protected by a PIN and owned by an operator. SIM applications can be written with a SIM tool kit.

2) GSM handset contains ciphering algorithm.

3) Network uses algorithms and IDs that are stored in the authentication center.

Degree of security in GSM is higher basic security mechanisms are:

a) Access control and authentication :It prevents access by unregistered users.

b) Encryption: It prevents unauthorized listening.

c) Confidentiality: It prevents subscriber's location discloser.

General Packet Radio Service:

Introduction

General Packet Radio Services (GPRS) is a packet-based wireless communication service that promises data rates from 56 up to 114 Kbps and continuous connection to the Internet for mobile phone and computer users. The higher data rates allow users to take part in video conferences and interact with multimedia Web sites and similar applications using mobile handheld devices as well as notebook computers. GPRS is based on Global System for Mobile (GSM) communication and complements existing services such circuit-switched cellular phone connections and the Short Message Service (SMS).

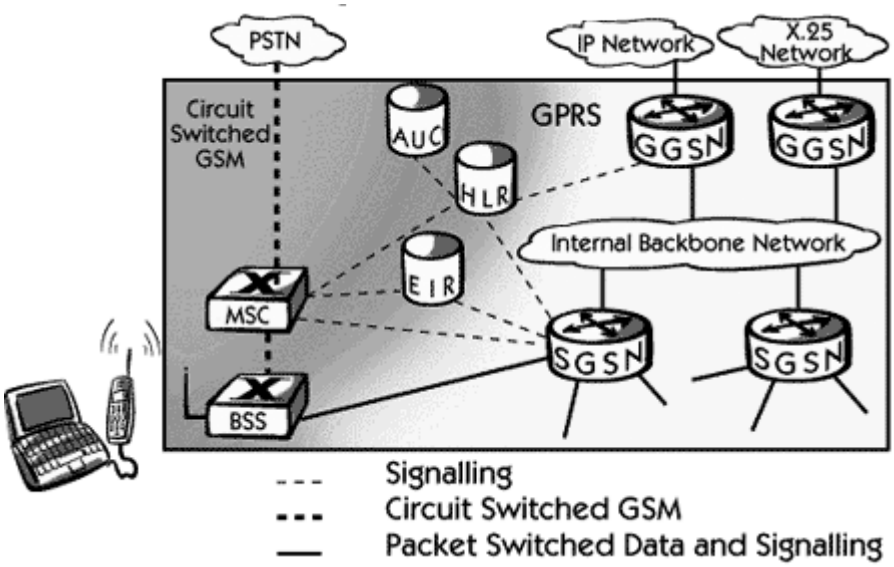
In theory, GPRS packet-based services cost users less than circuit-switched services since communication channels are being used on a shared-use, as-packets-are-needed basis rather than dedicated to only one user at a time. It is also easier to make applications available to mobile users because the faster data rate means that middleware currently needed to adapt applications to the slower speed of wireless systems are no longer be needed. As GPRS has become more widely available, along with other 2.5G and 3G services, mobile users of virtual private networks (VPNs) have been able to access the private network continuously over wireless rather than through a rooted dial-up connection.

GPRS also complements Bluetooth, a standard for replacing wired connections between devices with wireless radio connections. In addition to the Internet Protocol (IP), GPRS supports X.25, a packet-based protocol that is used mainly in Europe. GPRS is an evolutionary step toward Enhanced Data GSM Environment (EDGE) and Universal Mobile Telephone Service (UMTS).

GPRS and packet Data Network

GPRS architecture works on the same procedure like GSM network, but, has additional entities that allow packet data transmission. This data network overlaps a second-generation GSM network providing packet data transport at the rates from 9.6 to 171 kbps. Along with the packet data transport the GSM network accommodates multiple users to share the same air interface resources concurrently.

Following is the GPRS 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. These new terminals 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). The PCU directs the data traffic to the GPRS network and can be a separate hardware element associated with the BSC.
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 Mobile Stations

New Mobile Stations (MS) are required to use GPRS services because existing GSM phones do not handle the enhanced air interface or packet data. A variety of MS can exist, including a high-speed version of current phones to support high-speed data access, a new PDA device with an embedded GSM phone, and PC cards for laptop computers. These mobile stations are backward compatible for making voice calls using GSM.

GPRS Base Station Subsystem

Each BSC requires the installation of one or more Packet Control Units (PCUs) and a software upgrade. The PCU provides a physical and logical data interface to the Base Station Subsystem (BSS) for packet data traffic. The BTS can also require a software upgrade but typically does not require hardware enhancements.

When either voice or data traffic is originated at the subscriber mobile, it is transported over the air interface to the BTS, and from the BTS to the BSC in the same way as a standard GSM call. However, at the output of the BSC, the traffic is separated; voice is

sent to the Mobile Switching Center (MSC) per standard GSM, and data is sent to a new device called the SGSN via the PCU over a Frame Relay interface.

GPRS Support Nodes

Following two new components, called Gateway GPRS Support Nodes (GSNs) and, Serving GPRS Support Node (SGSN) are added:

Gateway GPRS Support Node (GGSN)

The Gateway GPRS Support Node acts as an interface and a router to external networks. It contains routing information for GPRS mobiles, which is used to tunnel packets through the IP based internal backbone to the correct Serving GPRS Support Node. The GGSN also collects charging information connected to the use of the external data networks and can act as a packet filter for incoming traffic.

Serving GPRS Support Node (SGSN)

The Serving GPRS Support Node is responsible for authentication of GPRS mobiles, registration of mobiles in the network, mobility management, and collecting information on charging for the use of the air interface.

Internal Backbone

The internal backbone is an IP based network used to carry packets between different GSNs. Tunneling is used between SGSNs and GGSNs, so the internal backbone does not need any information about domains outside the GPRS network. Signaling from a GSN to a MSC, HLR or EIR is done using SS7.

Routing Area

GPRS introduces the concept of a Routing Area. This concept is similar to Location Area in GSM, except that it generally contains fewer cells. Because routing areas are smaller than location areas, less radio resources are used While broadcasting a page message.

GPRS Network operations

Session Management

In order to send and receive data, the MS shall activate the packet data address (IP address) that it wants to use. This operation lets the corresponding GGSN know the MS, and then interworking with external data networks can start.

PDP context consists of PDP type, PDP address(optional), QoS parameters (optional), access point name, etc. The optional means that when activating a context, these are optional; when context is active, they have some negotiated or subscribed value.GPRS uses the concept of non-anonymous and anonymous PDP contexts.

The non-anonymous PDP context means that:

1. MS must have a subscription for this operation
2. Network verifies that no unauthorized PDP context activation is done
3. Network knows who holds each PDP context
4. No limitations on mobility (MS may move freely in the network)

The anonymous PDP context means that:

1. No subscription is needed, no need to attach first
2. Network does not know who uses PDP context
3. Limited mobility (only within limited area)

The user may have several subscribed contexts which are used to access to external data networks. Any of the contexts can be activated or deactivated independently. When context is activated, user can send and receive data packets from MS to fixed network, from fixed network to MS, or form MS to MS. When a context is not activated, the network drops the packets.

There are two kinds of activation, Anonymous PDP context activation and Non-anonymous PDP context activation. Here only Non-anonymous PDP context activation is given (with defined address), see Figure

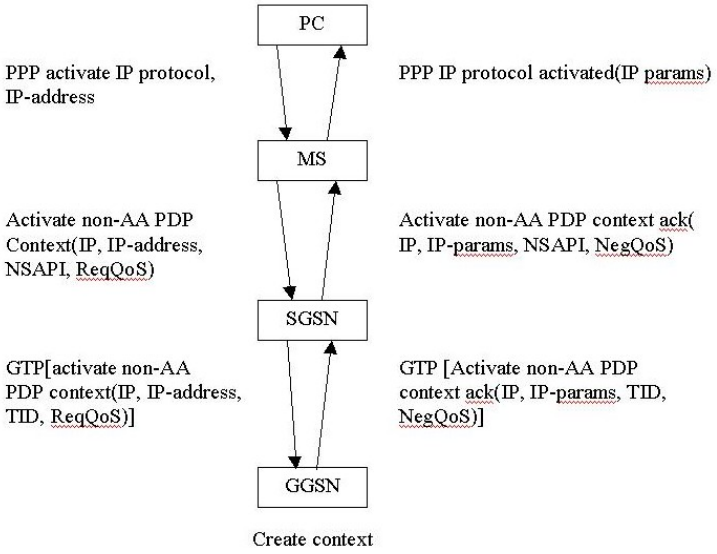


Figure :non-anonymous PDF context activation address defined

The main procedures are:

1. MS informs the network that it wants to activate this PDP context
2. SGSN checks that MS is allowed to activate the context. Also SGSN fills/defines missing (=optional) parameters
3. SGSN selects GGSN to be used
4. QoS negotiation: MS requests some QoS level (or default); SGSN may downgrade the QoS (if it can not handle that high); GGSN may downgrade even further

In order to communicate with network, the MS shall activate one or more PDP contexts. Once the MS has been attached to the network, the PDP context can be negotiated with the SGSN. If access is permitted, the SGSN informs the GGSN to update the context for the MS. The GGSN context includes the address of the SGSN that is currently serving the MS and tunneling information. The PDP context activation is completed by an acknowledgement from the network to the MS.

Routing(Data Transmission)

The data transmission can be Mobile oriented data transmission, Mobile terminated data transmission, and Mobile originated and terminated data transmission.In the case

of a mobile-originated transmission (cf. Figure), the SGSN encapsulates the incoming packets from MS and routes them to the appropriate GGSN, where they are forwarded to the correct PDN. Inside PDN, PDN-specific routing procedures are applied to send the packets to the corresponding host.

Packets coming from a corresponding host are routed the GGSN through the PDN based on the examination of the destination address. The GGSN checks the routing context associated with this destination address and determines the serving SSGN

address and tunneling information.

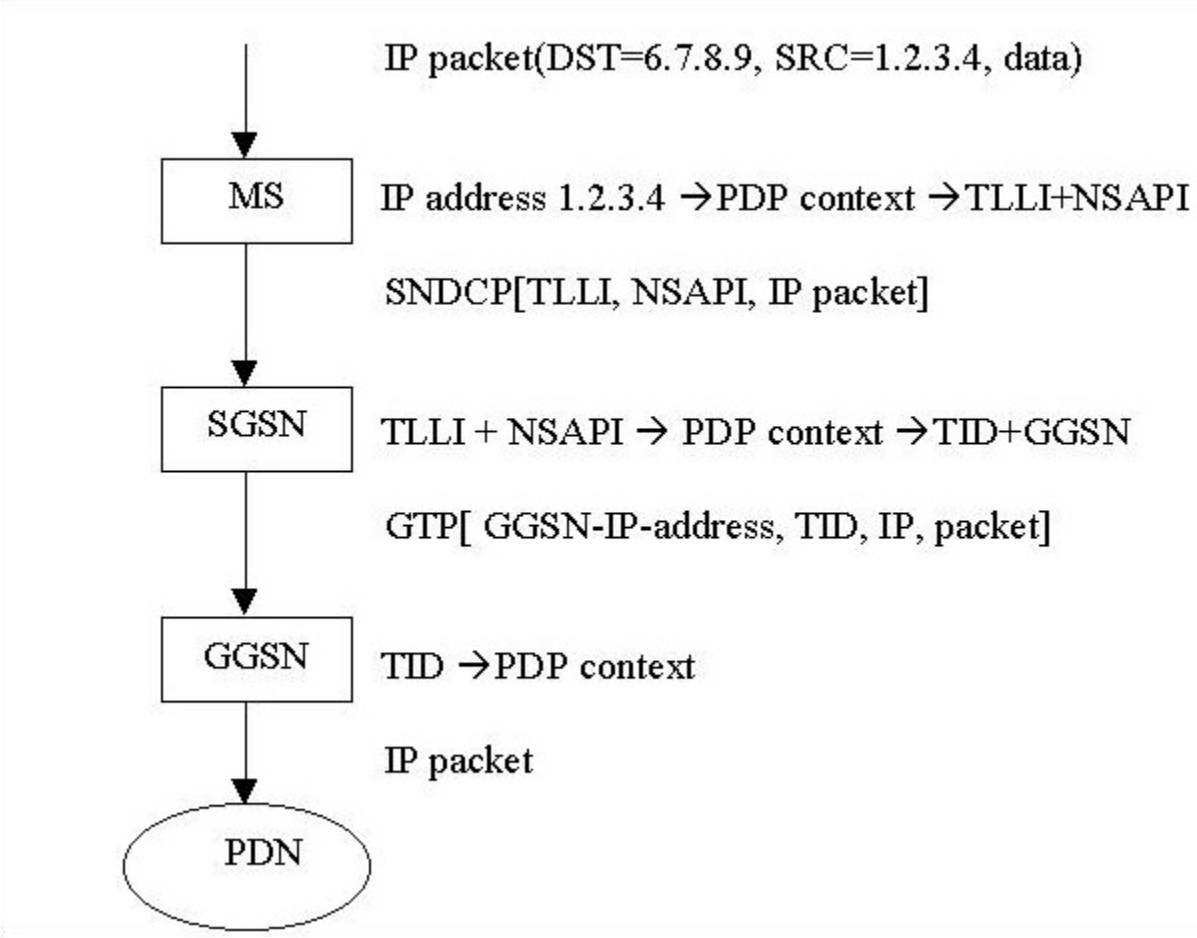


Figure: Mobile originated data transfer.

Mobility management

Mobility management [1], [4], [6] is also needed in GPRS. There are three activities related to mobility management, that is attach, detach, and location update. Attach

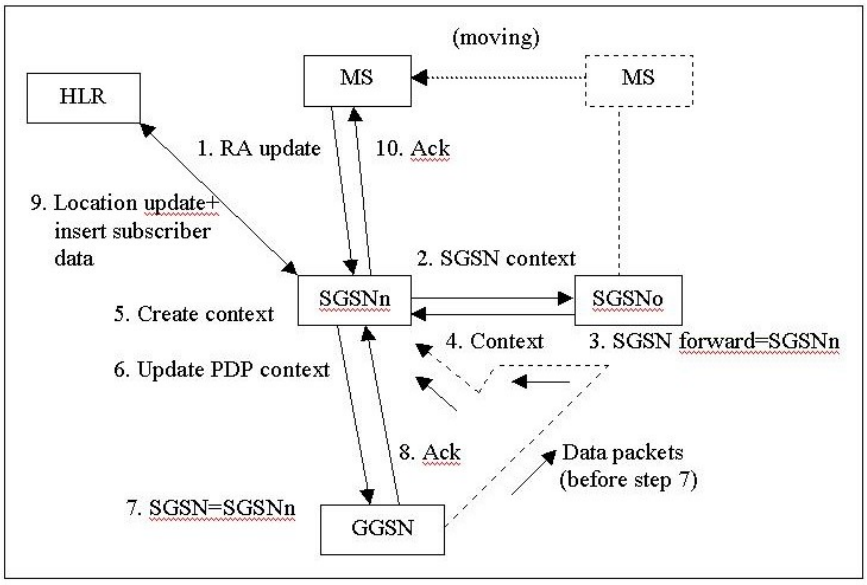
means entering/joining the system. Detach means leaving the system. Location update includes routing area (RA) update and cell update.Before an MS is able to send data to a corresponding host, it has to attach to the GPRS system. During the attachment procedure, the GPRS shall do the following things:

1. Inform the network for the MS's request to be active
2. Network check the MS's identity and initiate ciphering mode for data communication
3. If SGSN does not already have the MS&#65533;s subscription info, download the information from HLR to SGSN
4. Update MSC/VLR
5. Signal between the MS and SGSN

As a result of this attachment, a logical link control context, including a temporary logical link identity (TLLI), is established between the MS and SGSN.

A cell update is performed implicitly on the logical link control level. In cell update, the following information needs to be updated:

1. Specific cell update message
2. Any valid signaling message
3. Any user data sent uplink



When MS changes RA, the GPRS needs to update routing area (cf. Figure). The MS sends a routing update request containing the cell identity and the identity of the

previous routing area (RA) to the SGSNn. If the RA is served by the same SGSN, the location information is updated and an acknowledge is sent back to the MS. There is no need to inform the GGSN, because the SGSN and tunneling information are not changed.

However if the previous RA is served by another SGSN, the GGSN must be informed. The GGSN address and tunneling information can be requested from the previous SGSNo. Simultaneously, the SGSNo is requested to transmit the undelivered data packets to the new SGSN. Afterwards, the information context of the MS is deleted from the memory of the SGSNo. As soon as the address and tunneling information is received from the SGSNo, the new SGSN address and tunneling information is delivered to GGSN.

GPRS Applications

GPRS supports standard data network protocol (TCP/IP, X.25) based applications , such as www, ftp, telnet, email, video, audio for wireless PCs or mobile offices. There are also GPRS specific protocol based applications, e.g. point-to-point application (Toll road system, UIC train control system, etc.) and point-to-multipoint application (weather info, road traffic info, news, fleet management).

Recently, an important industry trend is remote access, a new technology, referred to as a virtual private network (VPN). With this new technology, companies will be able to let their remote workers wirelessly access to corporate resources and stay in touch with their work teams.

Quality of Service (QoS)

A QoSparameter is associated with each service request primitive received at an Network Service Access Point (NSAP). This is a set of parameters that collectively specify the performance of the network service that the network service user expects the network provider in relation this request. In addition, QoS is also used to specify the

optional services to be used with this request. The QoS may vary from one network to another.

GPRS supports Quality of Service. The QoS profile attributes in GPRS are:

1. *Precedence class*---indicates the importance of the packet with regard to discarding it in case of problems and degradation of QoS when necessary)
2. *Reliability class*---specifies the mode of operation for various error detection and recovery protocols, how securely the data should be delived.
3. *Delay class*---the transfer delay includes the uplink radio channel access or downlink radio channel scheduling delay, the radio channel transit delay, and GPRS network transit delay
4. *Peak throughput class* --- define the maximum allowed transfer rate
5. *Mean throughput class* --- define long term average transfer rate

In GPRS, the default QoS profile is defined in HLR. The SGSN and GGSN control QoS in GPRS, but mainly in the SGSN.One of the problems of GPRS is relatively low bandwidth and the lack of capability to perform packet multiplexing between LLC packets with different QoS requirement of same PDP context. Another problem is regarding the packets discarding when the MS moves from one BSS to another.

Limitations of GPRS

There are some limitations with GPRS which can be summarized as:

Limited Cell Capacity for All Users: Only limited radio resources can be deployed for different uses. Both Voice and GPRS calls use the same network resources.

Speed Lower in Reality: Achieving the theoretical maximum GPRS data transmission speed of 172.2 kbps would require a single user taking over all eight time slots without any error protection.

Support of GPRS Mobile Terminate Connection for a mobile server not supported: As of date, a GPRS terminal can only act as a client device. There are many services for which server has to be mobile.

The data rate supported by GPRS is slower than the data rate of the latest wireless standards like LTE, LTE-advanced, etc.,

• We cannot troubleshoot the error in case any issue appears in front of us.
• The problem of congestion also occurs in GPRS which means that if multiple users of GPRS are utilizing the services of GPRS in the same area at the same time, then slower data connection there.

Billing and charging in GPRS.

As packet data is introduced into mobile systems, the question of how to bill for the services arises. Always online and paying by the minute does not sound all that appealing. Here, we describe the possibilities but it totally depends on different service providers, how they want to charge their customers.

The SGSN and GGSN register all possible aspects of a GPRS user's behavior and generate billing information accordingly. This information is gathered in so-called Charging Data Records (CDR) and is delivered to a billing gateway.

The GPRS service charging can be based on the following parameters:

- **Volume -** The amount of bytes transferred, i.e., downloaded and uploaded.
- **Duration -** The duration of a PDP context session.
- **Time -** Date, time of day, and day of the week (enabling lower tariffs at offpeak hours).
- **Final destination -** A subscriber could be charged for access to the specific network, such as through a proxy server.
- **Location -** The current location of the subscriber.
- **Quality of Service -** Pay more for higher network priority.
- **SMS -** The SGSN will produce specific CDRs for SMS.
- **Served IMSI/subscriber -** Different subscriber classes (different tariffs for frequent users, businesses, or private users).
- **Reverse charging -** The receiving subscriber is not charged for the received data; instead, the sending party is charged.
- **Free of charge -** Specified data to be free of charge.
- **Flat rate -** A fixed monthly fee.

- **Bearer service -** Charging based on different bearer services (for an operator who has several networks, such as GSM900 and GSM1800, and who wants to promote usage of one of the networks). Or, perhaps the bearer service would be good for areas where it would be cheaper for the operator to offer services from a wireless LAN rather than from the GSM network.

UNIT IV
WIRELESS APPLICATION PROTOCOL

Introduction

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

WAP (Wireless Application Protocol) is a specification for a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access, including e-mail, the World Wide Web, newsgroups, and instant messaging. While Internet access has been possible in the past, different manufacturers have used different technologies. In the future, devices and service systems that use WAP will be able to interoperate.

The WAP layers are:

- Wireless Application Environment (WAE)
- Wireless Session Layer (WSL)
- Wireless Transport Layer Security (WTLS)
- Wireless Transport Layer (WTP)

The WAP was conceived by four companies: Ericsson, Motorola, Nokia, and Unwired Planet (now Phone.com). The Wireless Markup Language (WML) is used to create pages that can be delivered using WAP.There are other approaches to an industry standard besides WAP, including i-Mode.

MMS

Multimedia Messaging Service (MMS) is a communications technology developed by 3GPP (Third Generation Partnership Project) that was developed to enable the transmission of multimedia content via text message.
An extension to the Short Message Service (SMS) protocol, MMS defines a way to send and receive, almost instantaneously, wireless messages that include images, audio, and video clips in addition to text.

A common application of MMS messaging is picture messaging, which is the use of phone cameras to take photos for immediate delivery to a mobile recipient. Other possibilities include animations and graphic presentations of stock quotes, sports news and weather reports.

How MMS works

The process of sending and receiving a MMS message in a typical phone-to-phone MMS transaction works this way:

- The sending phone triggers a data connection that provides TCP/IP network connectivity, typically over GPRS (General Packet Radio Service).
- The sending phone performs an HTTP POST to a Multimedia Messaging Service Center (MMSC) of the MMS message encoding in the MMS Encapsulation Protocol as defined by the Open Mobile Alliance. The encoded MMS message includes all of the content of the MMS message, along with header information that includes a list of intended recipients for the message. (The HTTP POST will be routed through a proxy server in most environments. Some devices will use WP-HTTP (Wireless Profiled HTTP) and TCP through a WAP 2.0 proxy server, while other devices will use the Wireless Session Protocol through a conventional Wireless Application Protocol [WAP] proxy server/gateway.)
- The MMSC receives the submitted MMS message and validates the sender of the message.
- The MMSC stores the content of the MMS message, making it available as a URL link that's dynamically generated.

- The MMSC generates an MMS notification message, which is sent via WAP Push over SMS to the recipient(s) of the message. This MMS notification message contains a URL pointer to the dynamically generated MMS content.
- The recipient receives the MMS notification message and then initiates a data connection that provides TCP/IP network connectivity (usually over GPRS).
- The recipient phone performs an HTTP (or Wireless Session Protocol) GET to retrieve the MMS message content URL from the MMSC.

Best practice for MMS

To optimize MMS messages for the best user experience, use the following best practices:

- Ensure the image layout is vertical as most mobile devices display vertically.
- Use JPEG format for images.
- File size of images should not exceed 420 KB.
- The best dimensions for images are 327 pixels (height) and 400 pixels (width).
- The resolution of the image should be 72 pixels.
- Remember the subject line is 64 characters.
- Keep additional text to fewer than 500 words for better readability.
- Use GIF format for animated images.
- GIF format file size should be under 600 KB.

GPRS applications.

A number of unique services are given to the wireless mobile subscriber by GPRS. Some of them provides increased value services to the users. Following are the some characteristics:

Mobility – GPRS provides uninterrupted data and voice connectivity while on the move.

Immediacy – Whenever needed, the connectivity is established. Not to worry about the location you are in and the login session.

Localization – GPRS gives you information relevant to their current location on the facilities they can get from.

Number of applications are developed using the above characteristics and provided to the users. All the applications are segregated to two high-level categories:

- Corporation
- Consumer

Above two levels even include:

Communications – Fax, E-mail, unified messaging and intranet/internet access, etc.

Value-added services – Apps that provide Information services and other games, etc.

E-commerce – Retail applications like Flipkart, purchasing tickets using Paytm, banking apps and financial trading, etc.

Location-based applications – Applications that provide navigation, update traffic conditions, airline/rail schedules and location finder, etc.

Vertical applications - Delivery, fleet management and automating sales-force.

Advertising – Using location based applications, advertising makes it easier for local retailers.

Apart from the above applications, we have non-voice services as well like MMS, SMS along with voice calls. After GPRS came into existence, Closed User Group (CUG) term used in common. Other services that are in plan to implement are Call Forwarding Unconditional (CFU), and Call Forwarding on Mobile subscriber Not Reachable (CFNRc).

CDMA and 3G.

Introduction

Stands for "Code Division Multiple Access." CDMA is a wireless transmission technology that was developed during World War II by the English allies to avoid having their transmissions jammed. After the war ended, Qualcomm patented the technology and made it commercially available as a digital cellular technology. Now CDMA is a popular communications method used by many cell phone companies.

Unlike the GSM and TDMA technologies, CDMA transmits over the entire frequency range available. It does not assign a specific frequency to each user on the communications network. This method, called multiplexing, is what made the transmissions difficult to jam during World War II. Because CDMA does not limit each user's frequency range, there is more bandwidth available. This allows more users to communicate on the same network at one time than if each user was allotted a specific frequency range.

Because CDMA is a digital technology, analog audio signals must be digitized before being transmitted on the network. CDMA is used by 2G and 3G wireless communications and typically operates in the frequency range of 800 MHz to 1.9 GHz.

3G is the third generation of wireless technologies. It comes with enhancements over previous wireless technologies, like high-speed transmission, advanced multimedia access, and global roaming.
3G is mostly used with mobile phones and handsets as a means to connect the phone to the internet or other IP networks in order to make voice and video calls, to download and upload data, and to surf the Web.
The 3G standard, although it still serves as a fallback for some cellular providers, has largely been superseded by the 4G standard, which itself is being eclipsed by 5G services.

Speed spectrum technology

Spread spectrum is a technique used for transmitting radio or telecommunications signals. The term refers to the practice of spreading the transmitted signal to occupy the frequency spectrum available for transmission.

IS95

IS-95 was the first CDMA mobile phone system to gain widespread use and it is found widely in North America. Its brand name is cdmaOne and the initial specification for the

system was IS95A, but its performance was later upgraded under IS-95B. It is this later specification that is synonymous with cdmaOne. Apart from voice the mobile phone system is also able to carry data at rates up to 14.4 kbps for IS-95A and 115 kbps for IS-95B.

IS95 / cdmaOnewas the first cellular telecommunications system to use the CDMA - code division multiple access system. Previous systems had used FDMA - frequency division multiple access or TDMA - time division multiple access. With IS-95 being a second generation - 2G system and all the later 3G systems using CDMA as their access system, this meant that IS95 / cdmaOne was a pioneering system.

CDMA versus GSM

GSM (Global System for Mobile Communication) and **CDMA** (Code Division Multiple Access) are two dominant technologies for mobile communication. These two technologies differ in the way calls and data travel over the mobile phone networks take place. On comparing both the technologies GSM has some limitation when the call quality is concerned but still has more flexibility and an easy implementation relative to the CDMA technology. The major difference between the two lies in terms of the technology they use, security factors, their global reach and the data transfer speeds.

1. Technology

The CDMA is based on spread spectrum technology which makes the optimal use of available bandwidth. It allows each user to transmit over the entire frequency spectrum all the time. On the other hand GSM operates on the wedge spectrum called a carrier. This carrier is divided into a number of time slots and each user is assigned a different time slot so that until the ongoing call is finished, no other subscriber can have access to this. GSM uses both Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA) for user and cell separation. TDMA provides multiuser access by chopping up the channel into different time slices and FDMA provides multiuser access by separating the used frequencies.

2. Security

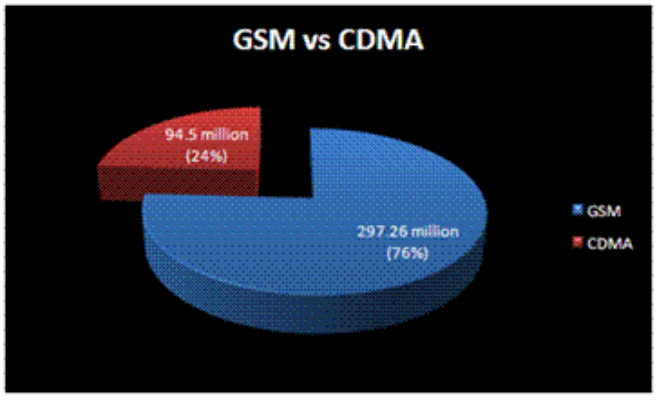
More security is provided in **CDMA technology as compared with the GSM technology** as encryption is inbuilt in the CDMA. A unique code is provided to every user and all the conversation between two users are encoded ensuring a greater level of security for CDMA users. The signal cannot be detected easily in CDMA as compared to the signals of GSM, which are concentrated in the narrow bandwidth. Therefore, the CDMA phone calls are more secure than the GSM calls. In terms of encryption the GSM technology has to be upgraded so as to make it operate more securely.

3. Spectrum Frequencies

The CDMA network operates in the frequency spectrum of CDMA 850 MHz and 1900 MHz while the GSM network operates in the frequency spectrum of GSM 850 MHz and 1900 MHz.

4. Global Reach

GSM is in use over 80% of the world's mobile networks in over 210 countries as compared to CDMA. CDMA is almost exclusively used in United States and some parts of Canada and Japan. As the European Union permissions GSM use, so CDMA is not supported in Europe. In North America, especially in rural areas, more coverage is offered by CDMA as compared to GSM. As GSM is an international standard, so it's better to use GSM in international roaming. GSM is in use by 76% of users as compared to CDMA which is in use by 24% users.



5. Data Transfer Rate

CDMA has faster data rate as compared to GSM as EVDO data transfer technology is used in CDMA which offers a maximum download speed of 2 mbps. EVDO ready mobile phones are required to use this technology. GSM uses EDGE data transfer technology that has a maximum download speed of 384 kbps which is slower as compared to CDMA. For browsing the web, to watch videos and to download music, CDMA is better choice as compared to GSM. So CDMA is known to cover more area with fewer towers.

6. Radiation Exposure

GSM phones emit continuous wave pulses, so there is a large need to reduce the exposures to electromagnetic fields focused on cell phones with “continuous wave pulses”. On the other hand CDMA cell phones do not produce these pulses. GSM phones emit about 28 times more radiation on average as compared to CDMA phones. Moreover, GSM phones are more biologically reactive as compared to CDMA.

Wireless Data

The transmission of data over the air. Wireless data includes all Internet-based communications, and although voice can be carried via the Internet protocol (voice over IP), the term excludes voice transmission that is paid by minutes of usage to a carrier. Wireless data generally refers to transmission to and from a mobile device; however, "fixed wireless" applications transmit data over the air between stationary objects.

Third Generation Networks

3rd Generation Mobile Telecommunications (3G), is a set of standards that came about as a result of the International Telecommunication Union’s (ITU) initiative known as IMT-2000 (International Mobile Telecommunications-2000). 3G systems are expected to deliver quality multimedia to mobile devices by way of faster and easier wireless communications as well as “anytime, anywhere” services. This term is also known as 3rd generation mobile telecommunications.

Application on 3G.

The expanded capabilities of wireless networks and devices will open new avenues for applications. With 3G networks, we will see greater emphasis on laptop remote access into corporate applications. In this way, middleware for anything other than custom applications will start to become less relevant in the enterprise.

In addition to important developments in network and device capabilities, IT executives should keep their eye on the following hot topics that should expand the applications framework in 2006.

Location-based services

LBS will be an area for value-added corporate applications this year. More than 50 percent of all phones being sold to companies have GPS chips, and accuracy levels continue to improve. A number of carriers have built an extensive partner network to deliver location-enabled applications that are delivering ROI daily in the enterprise market. We are increasingly seeing integrated products that combine LBS with in-office software to link assignment, dispatch, notification and tracking.

Enterprises should think about LBS in two ways: as a unique capability for specific vertical segments, such as fleets and transportation; and as a value-added capability within existing applications. In the U.S., for example, mobile carrier Sprint has partnered with IBM and Microsoft to deliver a Web services capability for location, where APIs are included in the application framework.

Packaged applications

In 2006 there will be a number of packaged applications in the areas of salesforce and field-force automation, offered directly by the wireless operators. One driving force is the reduced need to optimize certain functions for mobile using expensive and complex middleware, because of significantly improved wireless network and device capabilities. Additionally, small and midsize businesses are looking for plug-and-play software for certain functions, and believe that applications such as salesforce automation can be implemented without a great deal of customization.

Device management

Device management is becoming the new front in mobile security. As high-end devices proliferate, sensitive corporate information can get into the wrong hands if a phone is lost or stolen. More-advanced devices are also increasingly vulnerable to spam and viruses. There are millions of enterprise workers carrying around high-end mobile devices containing sensitive corporate information, and enterprises historically have not done a good job of tracking these devices as assets.

There is a rapidly expanding array of products for device management. A sound framework for mobile device management includes both policies, such as extending WLAN policies to the WAN, and technology - everything from firewalls; VPNs; anti-spam, anti-spyware and anti-virus programs; intrusion detection; mobile-asset tracking; device lockdown; and so on.

New business models

Enterprise decision makers might consider managed services as an approach for certain elements of their mobile-solution sets. Device management provides a good case in point. The good news is that there is a broad range of device management products available today. The bad news is that the product ecosystem is disparate and fragmented. As a result, many IT executives are not dealing with the device management problem directly and effectively. Managed services is an approach that is gaining popularity. For example, the lead product in Sprint's Managed Mobility Services program addresses device management.

UNIT V

WIRELESS LAN

Introduction

A wireless LAN (or WLAN, for wireless local area network, sometimes referred to as LAWN, for local area wireless network) is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection. The IEEE 802.11 groups of standards specify the technologies for wireless LANs. 802.11 standards use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing and include an encryption method, the Wired Equivalent Privacy algorithm.High-bandwidth allocation for wireless will make possible a relatively low-cost wiring of classrooms in the United States. A similar frequency allocation has been made in Europe. Hospitals and businesses are also expected to install wireless LAN systems where existing LANs are not already in place.Using technology from the Symbionics Networks, Ltd., a wireless LAN adapter can be made to fit on a Personal Computer Memory Card Industry Association (PCMCIA) card for a laptop or notebook computer.

Wireless LAN advantages

- Flexibility: within radio coverage, nodes can communicate without further restriction.
- Radio waves can penetrate walls.
- Planning: wireless ad hoc networks allow for communication without planning. Wired networks need wiring plans
- Robustness: wireless networks can survive disasters, if the wireless devices survive people can still communicate.
- It is a reliable type of communication
- As WLAN reduces physical wires so it is a flexible way of communication
- WLAN also reduces the cost of ownership
- It is easier to add or remove workstation
- It provides high data rate due to small area coverage
- You can also move workstation while maintaining the connectivity

- For propagation, the light of sight is not required
- The direction of connectivity can be anywhere i.e. you can connect devices in any direction unless it is in the range of access point
- Easy installation and you need don't need extra cables for installation
- WLAN can be useful in disasters situation e.g. earthquake and fire. People can still communicate through the wireless network during a disaster
- It is economical because of the small area access
- If there are any building or trees then still wireless connection works

IEEE802.11 standards

802.11 and *802.11x* refers to a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997.

There are several specifications in the *802.11* family:

- **802.11** — applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).
- **802.11a** — an extension to 802.11 that applies to wireless LANs and provides up to 54-Mbps in the 5GHz band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS.
- **802.11b** (also referred to as 802.11 High Rate or Wi-Fi) — an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1-Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.
- **802.11e** — a wireless draft standard that defines the ***Q**uality **o**f **S**ervice* (QoS) support for LANs, and is an enhancement to the 802.11a and 802.11b wireless LAN (WLAN) specifications. 802.11e adds QoS features and multimedia support to the

existing IEEE 802.11b and IEEE 802.11a wireless standards, while maintaining full backward compatibility with these standards.

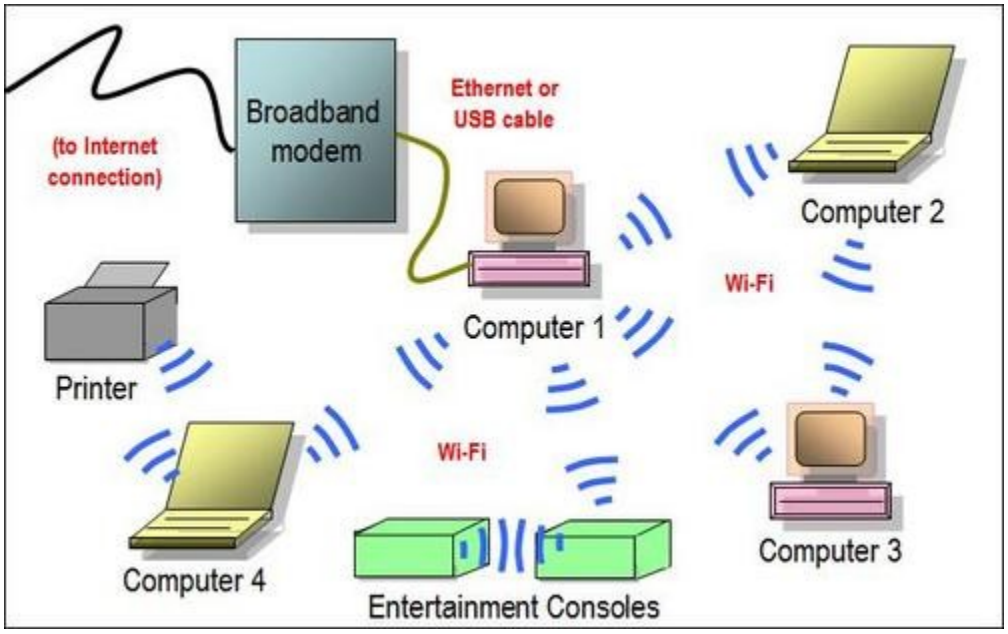
- **802.11g** — applies to wireless LANs and is used for transmission over short distances at up to 54-Mbps in the 2.4 GHz bands.
- **802.11n** — 802.11n builds upon previous 802.11 standards by adding ***m****ultiple-****i****nput* ***m****ultiple-****o****utput* (MIMO). The additional transmitter and receiver antennas allow for increased data throughput through spatial multiplexing and increased range by exploiting the spatial diversity through coding schemes like Alamouti coding. The real speed would be 100 Mbit/s (even 250 Mbit/s in PHY level), and so up to 4-5 times faster than 802.11g.
- **802.11ac** — 802.11ac builds upon previous 802.11 standards, particularly the 802.11n standard, to deliver data rates of 433Mbps per spatial stream, or 1.3Gbps in a three-antenna (three stream) design. The 802.11ac specification operates only in the 5 GHz frequency range and features support for wider channels (80MHz and 160MHz) and beamforming capabilities by default to help achieve its higher wireless speeds.
- **802.11ac Wave 2** — 802.11ac Wave 2 is an update for the original 802.11ac spec that uses MU-MIMO technology and other advancements to help increase theoretical maximum wireless speeds for the spec to 6.93 Gbps.
- **802.11ad** — 802.11ad is a wireless specification under development that will operate in the 60GHz frequency band and offer much higher transfer rates than previous 802.11 specs, with a theoretical maximum transfer rate of up to 7Gbps (Gigabits per second).
- **802.11ah**— Also known as Wi-Fi HaLow, 802.11ah is the first Wi-Fi specification to operate in frequency bands below one gigahertz (900 MHz), and it has a range of nearly twice that of other Wi-Fi technologies. It's also able to penetrate walls and other barriers considerably better than previous Wi-Fi standards.
- **802.11r** - 802.11r, also called *Fast* ***B****asic* ***S****ervice* ***S****et* (BSS) Transition, supports VoWi-Fi handoff between access points to enable VoIP roaming on a Wi-Fi network with 802.1X authentication.
- **802.1X** — Not to be confused with 802.11x (which is the term used to describe the family of 802.11 standards) 802.1X is an IEEE standard for port-based Network

Access Control that allows network administrators to restricted use of IEEE 802 LAN service access points to secure communication between authenticated and authorized devices.

Wireless LAN architecture

In planning the wireless network, we will have to determine which wireless network architecture to adopt in the network environment. There are two architectures available, namely **standalone** and **centrally coordinated** wireless network.

Standalone architecture (Ad hoc mode)



By using ad hoc mode, all devices in the wireless network are directly communicating with each other in peer to peer communication mode. No access point (routers/switches) is required for communication between devices.

For setting up ad hoc mode, we need to manually configure the wireless adaptors of all devices to be at ad hoc mode instead of infrastructure mode, and all adaptors must use the same channel name and same SSID for making the connection active.

Ad hoc mode is most suitable for small group of devices and all of these devices must be physically present in close proximity with each other. The performance of network

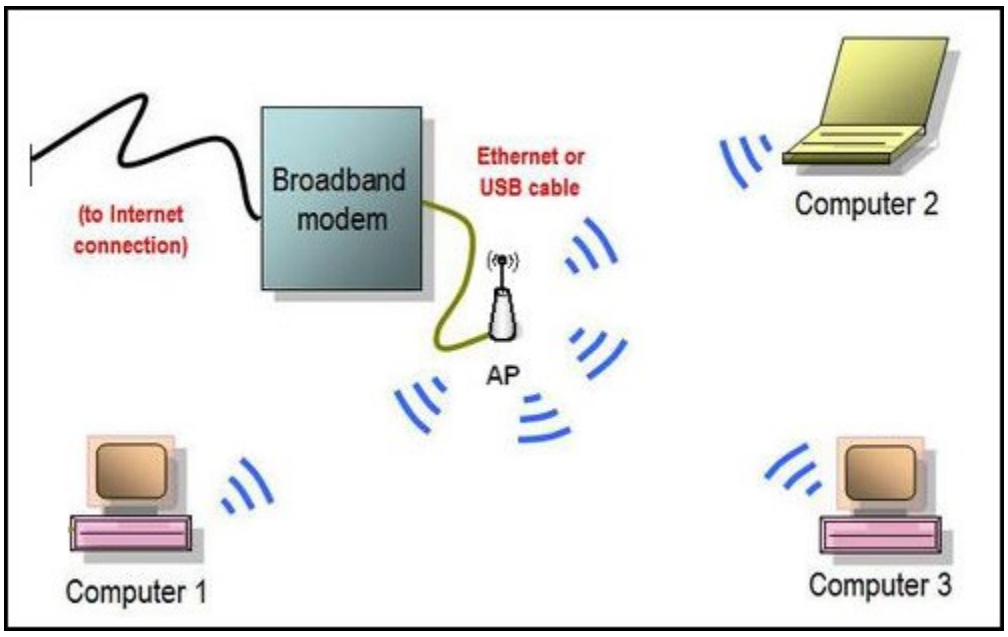
suffers while the number of devices grows. Disconnections of random device may occur frequently and also, ad hoc mode can be a tough job for network administrator to manage the network. Ad hoc mode has another limitation is that, ad hoc mode networks cannot bridge to wired local area network and also cannot access internet if without the installation of special gateways.

However, Ad hoc mode works fine in small environment. Because ad hoc mode does not need any extra access point (routers/switches), therefore it reduces the cost. Ad hoc can be very useful as a backup option for time being if network based on centrally coordinated wireless network (infrastructure mode) and access points are malfunctioning.

An ad hoc mode uses the integrated functionality of each adaptor to enable wireless services and security authentication. The characteristics of an Ad hoc wireless network are listed as below:

• All access points in the network operate independently and has own configuration file.
• Access point is responsible for the encryption and decryption.
• The network configuration is static and does not respond to changing network conditions.

Centrally Coordinated Architecture (Infrastructure mode)



The other architecture in wireless network is centrally coordinated (infrastructure mode). All devices are connected to wireless network with the help of Access Point (AP). Wireless APs are usually routers or switches which are connected to internet by broadband modem.

Infrastructure mode deployments are more suitable for larger organizations or facility. This kind of deployment helps to simplify network management, and allows the facility to address operational concerns. And resiliency is also assured while more users can get connected to the network subsequently.The infrastructure mode provides improved security, ease of management, and much more scalability and stability. However, the infrastructure mode incurs extra cost in deploying access points such as routers or switches.

An infrastructure mode wireless network has the characteristics as below:

- The wireless centralized controller coordinates the activity of access point.
- The controller is able to monitor and control the wireless network by automatically reconfiguring the access point parameters in order to maintain the health of the network.

- The wireless network can be easily expanded or reduced by adding or removing access points and the network can be reconfigured by the controller based on the changes in RF footprint.
- Tasks such as user authentication, fault tolerance, control of configuration, policy enforcement and expansion of network are done by the wireless network controller.
- Redundant access points can be deployed in separate locations to maintain control in the event of an access point or switch failure.

Mobility in wireless LAN

When a station wants to access an existing BSS, the station need to get synchronization information from the AP.

The station can get this information by one of two means:

Passive Scanning: In this case the station just waits to receive a Beacon Frame from the AP,

Active Scanning: In this case the station tries to locate an Acces Point by transmitting Probe Request Frames and waits for Probe Response from the AP.

The Authentication Process

Once a wireless station has located an AP anddecides to join its BSs, it goes through the authentication process. This is interchange of authentication information between the AP and the station, where the WLAN device proves its identity.

The Association Process

Once the station is authenticated, it then starts the association process which is the exchange of information about the stations and BSS capabilities, and which allows the DSS to know about the current position of the station. A station is capable of transmitting and receiving data frames only after the association process is completed.

Roaming

Roaming is the process of moving from one cell to another without losing connection. This function is similar to the cellular phones handover, with two main differences

1. On a packet-based LAN system, the transition from cell to cell may be performed between packet transmissions, as opposed to telephony where the transition may occur during a phone conversation.
2. On a voice system, a temporary disconnection during handoff does not affect the conversation. However, in a packet – based environment it significantly reduces performance because retransmission is performed by the upper layer protocols.

Deploying wireless LAN

Network Design

The first step in designing a wireless network is to identifying the areas that need to be covered the number of users and the types of devices they will use. From these requirements we need to determine how many access point are required and where they must be placed. The goal is to ensure adequate RF coverage to users. AP placement is typically determined using a combination of the theoretical principles and a thorough site survey. Site survey is necessary to determine the required coverage, number density and location of APs.

AP Transmission Power

The transmission power of most Aps ranges from 1 mw upto 100 mw. Transmission power affects the effective range of the radio signal. The higher the transmission power, the longer the range of the signal. Higher power settings are appropriate in many large enterprise installations with cube wall offices and a lot of open space. Lower settings are appropriate in environments such as test labs or small offices where the longer range is not required. Because lowering the transmission power reduces the range of an AP, lower power settings can also enable the wireless network to provide higher aggregate throughput. At lower power settings, more Aps can be installed to serve a particular area than is possible at higher power levels.

Mobile adhoc Networks and sensor Networks

A mobile ad-hoc network (MANET) consists of mobile hosts equipped with wireless communication devices. The transmission of a mobile host is received by all hosts within its transmission range due to the broadcast nature of wireless communication and omni-directional antennae. If two wireless hosts are out of their transmission ranges in the ad hoc networks, other mobile hosts located between them can forward their messages, which effectively builds connected networks among the mobile hosts in the deployed area. Due to the mobility of wireless hosts, each host needs to be equipped with the capability of an autonomous system, or a routing function without any statically established infrastructure or centralized administration. The mobile hosts can move arbitrarily and can be turned on or off without notifying other hosts. The mobility and autonomy introduces a dynamic topology of the networks not only because end-hosts are transient but also because intermediate hosts on a communication path are transient.

Characteristics

- Operating without a central coordinator
- Multi-hop radio relaying
- Frequent link breakage due to mobile nodes
- Constraint resources (bandwidth, computing power, battery lifetime, etc.)
- Instant deployment

Applications

- Military applications
- Collaborative computing
- Emergency rescue
- Mesh networks
- Wireless sensor networks
- Multi-hop cellular networks
- Wireless Community Network

Major Issues and Challenges

- Hidden terminal problem
- Exposed terminal problem

- Channel efficiency
- Access delay and fairness
- Differential service
- Realistic mobility modeling
- power-aware routing
- Constructing virtual backbone
- Distinguish contention, packet drop, and noise errors
- Security
- Efficient multicasting

Wireless LAN Security:

WIFI versus 3G

Typically, **Wi-Fi** connections are more **secure** for transferring data between a router **and** a computing device, **and** they experience fewer technical difficulties. While **3G network** connections are generally **secure** while data is in transit, they experience more interference **and** connection failures than **Wi-Fi** connections.

Imagine you want to send a picture of your new toy car to your friend. This picture is **data** and it has some size in MB, say 3 Mega Bytes. If you are at home and using your laptop to share this picture then you will use internet through your Wi-Fi router. Here **Wi-Fi** is the technology that lets you connect to internet wirelessly provided you have internet connection at home.

Internet exists as a group of inter connected computer networks, that means the data from your laptop has to reach your friends house hence this connection between you and your friend is established by internet.

Mobile service providers let us access the same internet using **3G/4G connection** from our phones or tablets. Since its a mobile service it lets us access internet from any place provided the service is available.

Internet networks and Internetworking:

Internet networks-SS#7 signaling

Signaling System 7 (SS7) is an international telecommunications standard that defines how network elements in a public switched telephone network (PSTN) exchange information over a digital signaling network. Nodes in an SS7 network are called signaling points.

SS7 consists of a set of reserved or dedicated channels known as signaling links. There are three kinds of network points signaling points: Service Switching Points (SSPs), Signal Transfer Points (STPs), and Service Control Points (SCPs). SSPs originate or terminate a call and communicate on the SS7 network with SCPs to determine how to route a call or set up and manage some special feature. Traffic on the SS7 network is routed by packet switches called STPs. SCPs and STPs are usually mated so that service can continue if one network point fails.

SS7 uses out-of-band signaling, which means that signaling (control) information travels on a separate, dedicated 56 or 64 Kbps channel rather than within the same channel as the telephone call. Historically, the signaling for a telephone call has used the same voice circuit that the telephone call traveled on (this is known as in-band signaling). Using SS7, telephone calls can be set up more efficiently and special services such as call forwarding and wireless roaming service are easier to add and manage.

SS7 is used for these and other services:

- Setting up and managing the connection for a call
- Tearing down the connection when the call is complete
- Billing

- Managing call forwarding, calling party name and number display, three-way calling, and other Intelligent Network (IN) services
- Toll-free (800 and 888) and toll (900) calls
- Wireless as well as wireline call service including mobile telephone subscriber authentication, personal communication service (PCS), and roaming

SS7 messages contain such information as:

The route to network point 587 is crowded. Use this route only for calls of priority 2 or higher.Subscriber so-and-so is a valid wireless subscriber. Continue with setting up the call.

IN Conceptual Model

A conceptual model is a representation of a system, made of the composition of concepts which are used to help people know, understand, or simulate a subject the model represents. It is also a set of concepts. Some models are physical objects; for example, a toy model which may be assembled, and may be made to work like the object it represents.

The term conceptual model may be used to refer to models which are formed after a conceptualization or generalization process. Conceptual models are often abstractions of things in the real world whether physical or social. Semantic studies are relevant to various stages of concept formation. Semantics is basically about concepts, the meaning that thinking beings give to various elements of their experience.

Conceptual models (models that are conceptual) range in type from the more concrete, such as the mental image of a familiar physical object, to the formal generality and abstractness of mathematical models which do not appear to the mind as an image. Conceptual models also range in terms of the scope of the subject matter that they are taken to represent. A model may, for instance, represent a single thing (e.g. the Statue of Liberty), whole classes of things (e.g. the electron), and even very vast domains of subject matter such as the physical universe. The variety and scope of conceptual

models is due to the variety of purposes had by the people using them. Conceptual modeling is the activity of formally describing some aspects of the physical and social world around us for the purposes of understanding and communication.

Softswitch

Softswitch is a central device in a telecommunications network which connects telephone calls from one phone line to another, across a telecommunication network or the public Internet, entirely by means of software running on a general-purpose system.

A softswitch can be used to control calls and process media on circuit switched **Time-Division Multiplex (TDM)** network infrastructure, packet switched **Internet Protocol (IP)** infrastructure, or a combination of the two. Many network operators use a softswitch with both TDM and IP capability as an essential transitional element as they go through the process of **IP network transformation**.

A softswitch (short for **software switch**) uses software on standard hardware to control phone calls, whereas older switching equipment uses dedicated, purpose-built switching hardware. In TDM network infrastructure, dedicated hardware is still required for physical TDM connections. However, in an all-IP network infrastructure using only VoIP calls, a softswitch can be virtualized entirely and run on any general-purpose hardware with Ethernet connections as part of an NFV deployment.

A softswitch combines two elements: a **call agent** or **call feature server** for call control, routing and signalling, and a **mediagateway** or **access gateway** for processing media streams. These two elements can be co-located on a single piece of hardware, or located on separate hardware where one call agent or call feature server can control one or more gateways.

The softswitch concept only applies to Next Generation Network (NGN) architecture or older networks. This does not apply in the IP Multimedia Subsystem (IMS) architecture,

where the concept of a softswitch doesn't exist. In an IMS network, a Media Gateway Control Function (MGCF) or Access Gateway Control Function (AGCF) controls the gateways and the two components are not conceptually aggregated into one.

Programmable networks

A programmable network is one in which the behavior of network devices and flow control is handled by software that operates independently from network hardware. A truly programmable network will allow a network engineer to re-program a network infrastructure instead of having to re-build it manually.
Programmable networking has several benefits over traditional networking:

- Reduced long-term costs.
- Ability for applications to maintain information about device capabilities.
- Ability for networks to respond to application status and resource requirements.
- Better allocation of bandwidth and resources.
- Packet prioritization for traffic shaping.
- Improved operational flexibility and enhanced transparency.
- Support for emerging privacy and security technologies.

Network programmability is central to software-defined networking (SDN). Currently, the most popular specification for creating a software-defined network is a protocol called Open Flow, which lets network administrators remotely control routing tables. With OpenFlow, the packet-moving decisions are centralized, so that the network can be programmed independently of the individual switches and data center gear.

The term programmable network is used by some vendors as a synonym for software-defined networking. In its infancy, SDN was often referred to as the "Cisco killer" because it allows network engineers to support a switching fabric across multi-vendor

commodity hardware and use software to shape traffic from a centralized control console without having to touch individual switches.

Cisco, however, has adopted the term programmable networking to describe its own vision for the future of networking -- a future that goes beyond separating the control and forwarding planes to actually permitting programming up and down the network stack. To that end, Cisco says it will address demand for programmable networks in three ways. First, it will offer software-defined networking and OpenFlow for some users. Second, Cisco will support virtual network overlays like LISP and VXLAN, to bridge the physical and virtual worlds. Third, Cisco will introduce a software development kit (SDK) that makes all of its routers and switches programmable through a universal API.

Technologies and Interfaces for IN

Intelligent Network (IN) is a telephone network architecture originated by Bell Communications Research (Bellcore) in which the service logic for a call is located separately from the switching facilities, allowing services to be added or changed without having to redesign switching equipment. According to Bell Atlantic, IN is a "service-specific" architecture. That is, a certain portion of a dialed phone number, such as 800 or 900, triggers a request for a specific service. A later version of IN called Advanced Intelligent Network (AIN) introduces the idea of a "service-independent" architecture in which a given part of a telephone number can interpreted differently by different services depending on factors such as time of day, caller identity, and type of call. AIN makes it easy to add new services without having to install new phone equipment.

Bellcore called its network IN/1. It included this model:

- The customer's telephone
- The switching system (starting with the switch a call is handled by first, usually at a telephone company central office (CO)
- A database called a service control point (SCP) that defines the possible services and their logic

- A service management system (SMS).

PARLAY

Parlay X was a set of standard Web service APIs for the telephone network (fixed and mobile). It is defunct and now replaced by OneAPI, which is the current valid standard from the GSM association for Telecom third party API.

It enables software developers to use the capabilities of an underlying network. The APIs are deliberately high level abstractions and designed to be simple to use. An application developer can, for example, invoke a single Web Service request to get the location of a mobile device or initiate a telephone call.

The Parlay X Web services are defined jointly by ETSI, the Parlay Group, and the Third Generation Partnership Project (3GPP). OMA has done the maintenance of the specifications for 3GPP release 8.

The APIs are defined using Web Service technology: interfaces are defined using WSDL 1.1 and conform with Web Services Interoperability (WS-I Basic Profile).