



5104-ARUNAI ENGINEERING COLLEGE

TIRUVANNAMALAI



DEPARTMENT OF COMPUTER SCIENCE

SEMESTER-V1

CS8601- MOBILE COMPUTING

Arunai Engineering College

Unit - I

Introduction

Introduction to Mobile Computing - Applications of Mobile

Computing - Generations of Mobile Communication Technologies -

Multiplexing - Spread spectrum - MAC protocols - SDMA - TDMA -

FDMA - CDMA

Mobile Computing

Ability to compute remotely while on the move. It's possible to access information from anywhere & at any time.

It's an advanced technology



uses computing devices

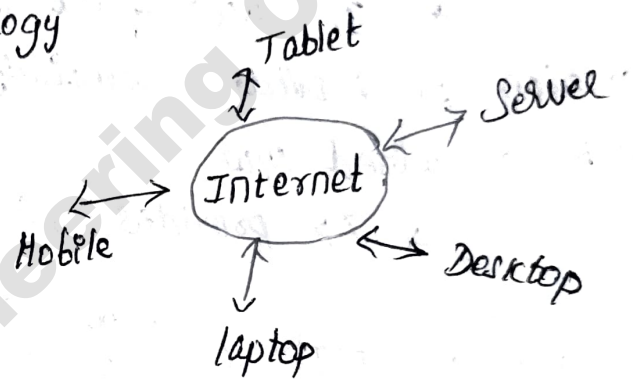


allows tr of data



with the help of wireless facility without any physical link & it

can be used at any where & anytime



Three Components

- * Mobile communication [tr & rx data over wireless] while on move
- * Mobile Hardware [portable device]
- * Mobile Software [Application]

Wireless → in which voice & data transmitted, emitted, received via microwaves.

Characteristics of Mobile Computing

1. Ubiquity - any time everywhere
2. Location awareness - Eg: GPS
3. Adaptation - able to adjust BW without disturbing user
4. Broadcast - Broadcast simultaneously to hundreds of users
5. Personalization - able to personalize the information needed by them

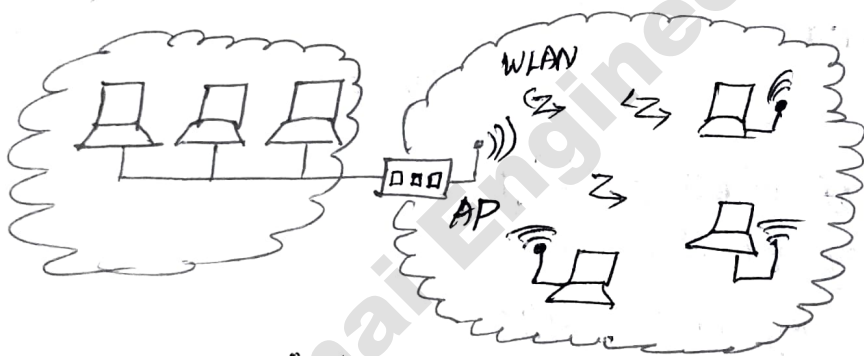
Wireless N/w :-

Types :-

1. Extension of wired N/w's :-

* It uses fixed infrastructure such as base station to provide essentially single hop wireless connection with a wired N/w.

* AP provides wireless connection to the devices.



2. Full wireless Network

* The wireless N/w without any wire is called an adhoc N/w. It don't have any fixed infrastructure.

It's based on multi hop wireless communication

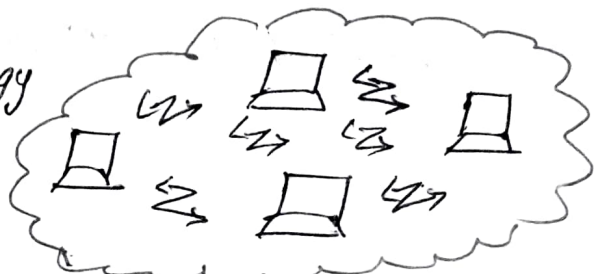
* AP requires authentication to avoid unauthorized users

Eg. bluetooth technology

Full

wireless

Adhoc N/w



Structure of Mobile Computing Application

Three tier structure of Mobile Computing application

1. presentation layer (Tier-1)

⇒ This is top most layer of Mobile Computer application.

⇒ It concerns the user interface

⇒ It facilitates user to issue requests & to present the results to them meaningfully.

Computing codes of this layer usually run on the client's computer including web browsers & client programs to give information to the user & also to collect data from the user.

[For requesting data & building query]

2. Application layer

* It makes logical decisions & performs calculation depends upon query.

* It moves data b/w pres. layer & data layer for processing requests given by user.

* It acts as engine of automobile (i/p ↓ process ↓ make) decision) fixed server.

[For processing query]

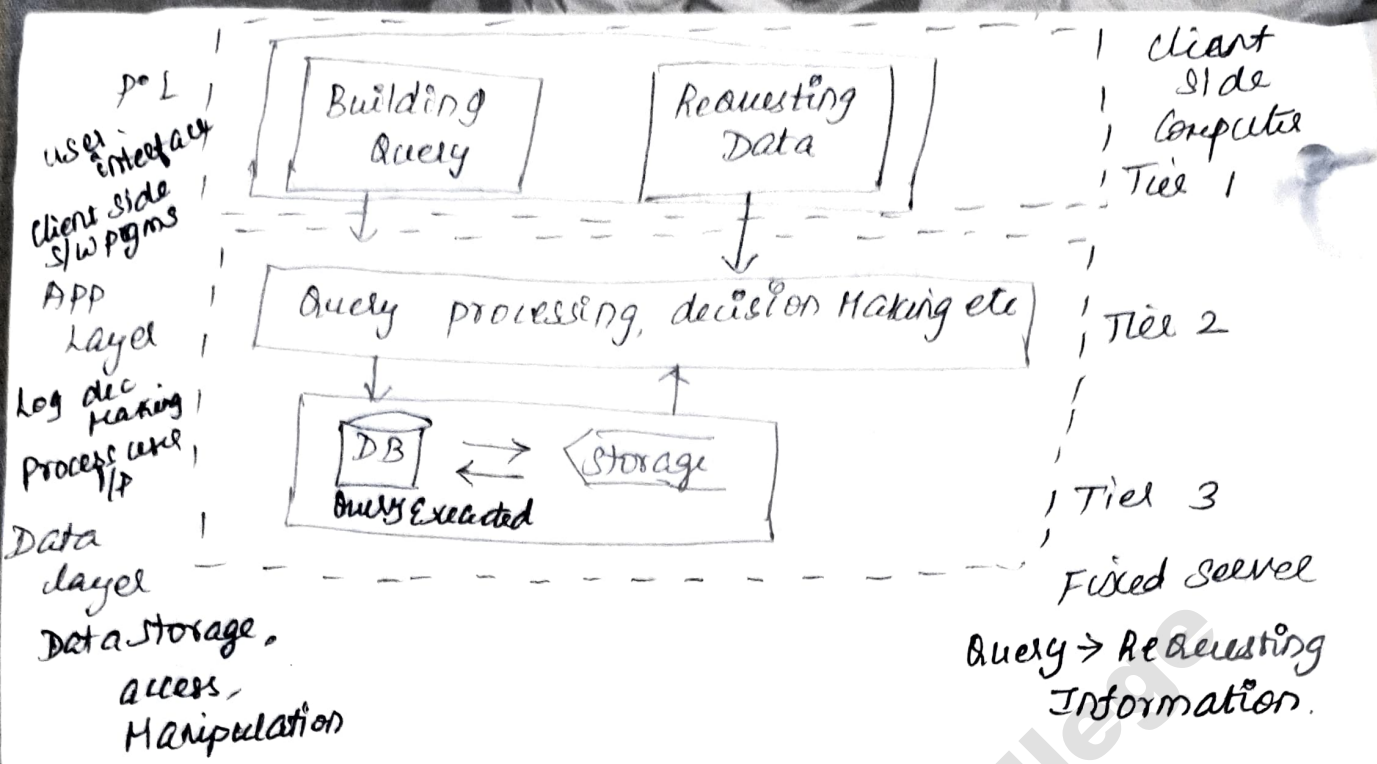
3. Data layer

* provides the basic functions with data like storing data, retrieving data & Manipulating data.

* It has Database & all the information is stored & retrieved from database.

* This layer also implemented on a server.

[For processing query]



Arunai Engineering College

Applications of Mobile Computing

1. Vehicles

- * Music, news, road conditions, weather reports & broadcast informations are received via digital audio broadcasting with 1.5 Mbit/s
- * For personal communication GSM, UHS might be available for voice & data connectivity with 384 kbit/s.
- * Current position of car determined by GPS.

2. Emergencies

- * Ambulance with high quality wireless connection to a hospital can carry vital information about injured persons to hospital
- * Necessary steps taken for particular type of accidents specialist can be consulted for early diagnosis
- * In natural disasters like hurricanes or earthquakes.

3. Business

- * Managers use mobile computers, critical presentation on to major customers. They can access latest market share information.
- * They can communicate with office about possible new offers & call meeting for discussing responds to new proposals

4. Credit card Verification

- * Point of sale terminals in shops & supermarkets, when customer use credit cards for transactions intercom required to Bank central comp & pos terminal to verify user.

5. Replacement of wired N/w

* It can be used to replace wired N/w's eg remote sensors, for theatres or in historic buildings

* It's often impossible to wire remote sensors for wireless. Via satellite can help this situation.

6. Infotainment

* provide up to date information at any appropriate location

* Another growing app lies in Entertainment & games to enable

7. Location dependent services

It's important for an app to know something about location or the user might need location information for further activities

1. Location aware services eg. points, fax in local
2. Follow on services [automatic call fwd, ^{ENV} % of actual workspace
3. Information services ^{to current location}
"PUSH" eg. Current special offers in supermarket
"PULL" eg.
4. Support services [caches, intermediate results, state information etc]
5. privacy

Limitations of Mobile Computing.

1. Resource constraints :- Battery
 2. Interference :- Radio tx can't be protected against interference against shielding & result in High loss rate for transmitted data. & ↑ bit error rates
 3. Bandwidth: tx. rates are very low for wireless devices
 4. Dynamic changes in communication environment.
⇒ Variations in signal power within a region, thus link delays & connection losses
 5. Network issues - discovery of connection service to destination & Connection stability
 6. Interoperability issues - Varying protocol standards
 7. Security constraints - Not only can portable devices be stolen more easily, but the radio interface is also prone to the dangers of eavesdropping.
 8. [Restrictions, Safety & Security, Quality of Service, Lack of infrastructure]
Wireless N/w compared to fixed N/w
- * Higher loss rate due to interference Eg:- Engines, lightning
 - * Restrictive regulations of frequencies
 - * Lower transmission rate
 - * Higher delays, higher jitter
 - * Lower security, simpler active attacking

Advantages of Mobile Computing

- * Location flexibility
- * Saves time
- * Enhanced productivity
- * Ease of Research
- * Entertainment

Generations of Mobile Communication Technologies

⇒ Mobile Communication has become more popular in last few years due to fast reform from 1G to 5G in Mobile technology.

⇒ It's due to requirement of services compatible transmission technology & very high increase in telecom customers.

1. First Generation

* 1G were the first mobile phones to be used, which was introduced in 1982 & completed in early 1990.

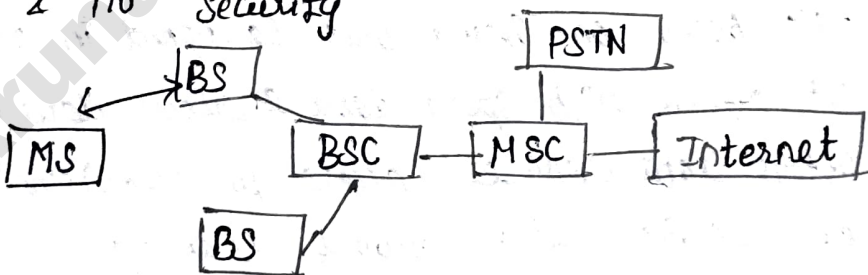
* It's used for voice services & based on technology called AMPS (Advanced mobile phone system).

* It was used FDMA & Frequency Modulated M

* Channel Capacity 30KHZ, Freq Band - 824-894MHZ

* It introduces Mobile Technologies such as MTS mobile Telephone System, Advanced Mobile Telephone System, Improved mobile Telephone Service (IMTS) & push to talk (PTT).

* It has low capacity, unreliable handoff, poor voice links & no security



2. Second Generation

* 2G based on GSM & was emerged in late 1980s

* It uses digital signals for voice tr & it provides services to deliver text & picture message at low speed in kbps

* BW ⇒ 30 to 200KHZ

2-5 G

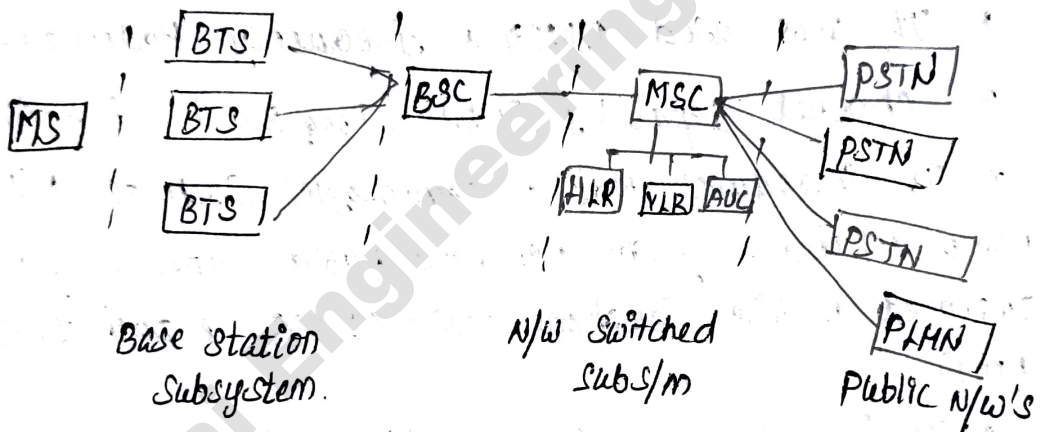
uses pkt switched & circuit switched domain
& provide data rate upto 144 kbps

Eg: GPRS, CDMA & Edge [Enhanced data rate for
General package radio service GSM Evolution]

Some

Main features of 2G & 2.5G

- * Data Speed up to 64 kbps
- * uses digital sig's
- * better Quality & Capacity
- * unable to handle complex data such as videos
- * GSM improved further led to development of advance technology b/w 2G & 3G
- * provides phone calls, send/receive e-mail, web browsing, speed 64-144 kbps, camera phones,



3. Third Generation (UMTS) for video calling

- * It's based on GSM & was launched in 2000.
- * It offers High speed data & allows data up to 4Mbps offers data services, access to television) video, new services like Global Roaming
- * Operating range of 2100MHz & BW 15-20MHz used for High speed internet service & video chatting

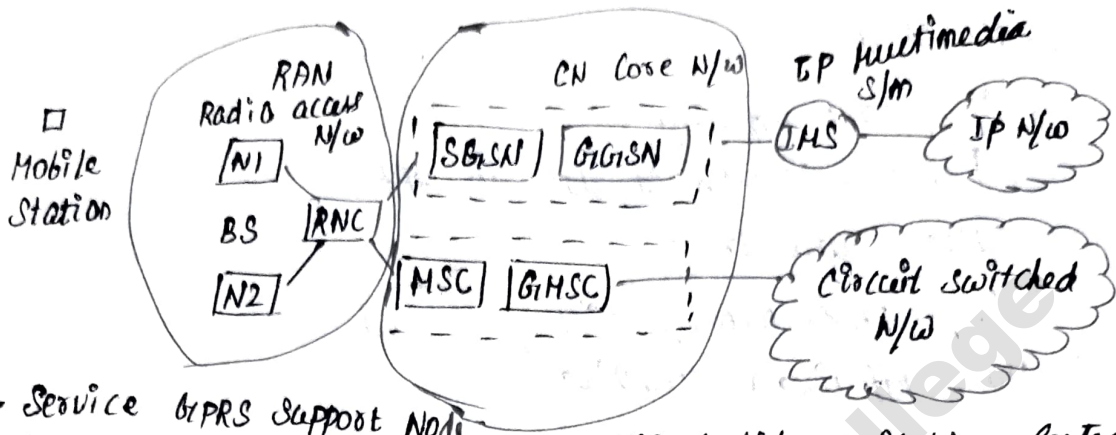
Some Main features are

- ⇒ Speed 2 Mbps
- ⇒ ↑ B.W & Data transfer rates
- ⇒ Faster Communication

- * receives large email messages
- * Expensive 3G phones etc

3G called as Universal Mobile Telecommunication System

TD-SCDMA, WCDMA \Rightarrow air interface Technology



S-GSN - Service GPRS Support Node
G-GSN - Gateway " " "

IMS - Mobile Switching Centre
G-MSC - Gateway mobile Switching Centre

4. Fourth Generation

- \Rightarrow It offers downloading speed of 100Mbps
- \Rightarrow Same feature as 3G, additionally Multi media Newspapers to watch TV pgms with more clarity & send data much faster than previous generations
- \Rightarrow Long term Evolution as 4G.

[Forthcoming Applications like

Multimedia Messaging Services MMS.
Video chat
Mobile TV,
HDTV, digital Video Broadcasting]

Some features of 4G

- * Speed 10Mbps - 1Gbps
- * High quality streaming video
- * Combination of WiFi & Wi-Max
- * High security
- * Battery use is more
- * Need Complicated Hardware

5. Fifth Generation

- * Started from late 2010s
- * better levels of connectivity & coverage
- * focuses on world wireless world wide web (WWW).
- * "Complete wireless communication with no limitations."

Some features are

- ⇒ ↑ speed & capacity
- ⇒ ↑ broadcasting of data in ~~600ps~~ Gbps
- ⇒ Faster data tx.
- ⇒ Large phone memory, dialing speed
- ⇒ More effective & attractive.

Technology	1G	2G	3G	4G	5G
Start	1970 - 1980	1990 - 2004	2004 - 2010	Now	by soon
BW	2kbps	64kbps	2Mbps	1Gbps	> 1 Gbps
Technology	Analog	digital	CDMA2000 UMTS EDGE	Wi-MAX Wi-Fi LTE	WWW
Core N/w	PSTN	PSTN	Pkt N/w	Internet	Internet
Switching	Circuit	Circuit, Packet	packet	All packet	All packet
Freq	30 kHz	1.8 GHz	1.6 - 2 GHz	2 - 8 GHz	3 - 30 GHz
Access S/m	FDMA	TDMA/ CDMA	CDMA	CDMA	OFDM / BDMA

Multiplexing [HDX - Application of Multiplexing]

* It's the process of combining multiple signals into one signal, over a shared medium, with min or no interference

* It describes how several users can share a medium with minimum or no interference

* Bands are split into channels.

Eg: Highway with several lane.

Four main ways of assigning channels

⇒ Space Division Multiplexing: allocate according to location

⇒ Time Division Multiplexing: allocate according to units of time

⇒ Frequency Division Multiplexing: " " to frequencies

⇒ Code Division Multiplexing: allocate according to access

Guard space: gaps b/w allocations. Codes.

Space division Multiplexing

SDM. All transmissions done

* This is the basis of frequency reuse

Simultaneously

* Each physical space is assigned channels

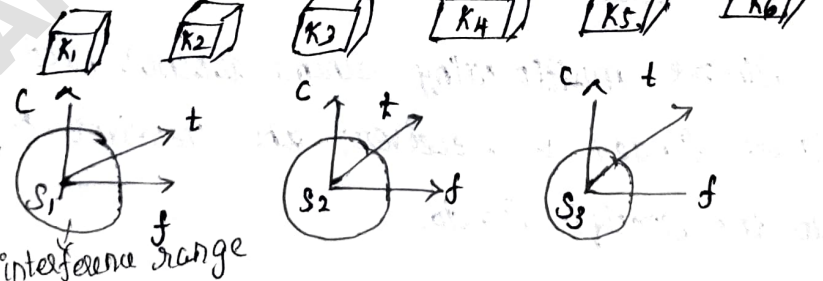
* Spaces that don't overlap can have the same channels assigned to them.

Eg: FM Radio stations in different countries.

This scheme is used at FM radio stations where

the tx range is limited to certain region, many radio stations around the world can use the same frequency without interference.

channels k_i



* It shows 6 channels k_i & introduces 3D coordinate S/M's.

* This shows the dimension of code c , time t , freq f .

* For SDM, first 3D space S_i also shown. Here space is represented via circles indicating the interference range.

* For remaining k_4 to k_6 , 3 additional spaces would be needed.

* In our highway example this (would imply that each driver had his or her own lane)

Drawback:

* Although this procedure clearly represents a wastage of space this is exactly the principle used by old analog telephone & each subscriber is given a separate pair of copper wires to the local exchange.

* In wireless tx, SDM implies a separate sender for each communication channel with a wide enough distance b/w senders

Frequency division Multiplexing [^{Diff freq Bands for Diff users} television broadcasting, Mobile or Satellite Stations]

* Separation of whole spectrum into smaller non overlapping frequency bands (guard spaces) are needed.

* A channel gets a certain band of spectrum for the whole time - receiver has to tune to the sender frequency

* Again guard spaces are needed to avoid frequency band overlapping also called adjacent channel interference.

* This scheme is used [for radio stations within the same region] where each radio station has its own frequency.

* This very simple multiplexing scheme does not need complex coordination between sender & receiver; the receiver only has to tune in to the specific sender.

Adv:-

* No dynamic coordination necessary

* works also for analog signal & digital

Disadvantages:

* While radio stations broadcast 24 hours a day, Mobile communication typically takes place for only a few minutes at a time.

* Assigning a separate frequency for each possible communication scenario would be a tremendous waste of frequency resources. (wastage of Bandwidth)

* Additionally, the fixed assignment of frequency to a sender makes the scheme very inflexible & (limits the no. of senders)

*

Time Division Multiplexing (in telephonic services) (Diff time slots for diff users)

* Here a channel K_i is given the whole bandwidth for a certain amount of time, i.e) all senders use the same frequency but at different points in time

* Again guard spaces, which now represent time gaps, have to separate the different periods when the senders use the medium. In our highway eg. this would refer to the gap between two cars

* If two tr's overlap in time, this is called co-channel interference. (In highway eg, interference b/w two cars results in an accident.)

To avoid this type of interference, precise synchronization b/w different senders is necessary.

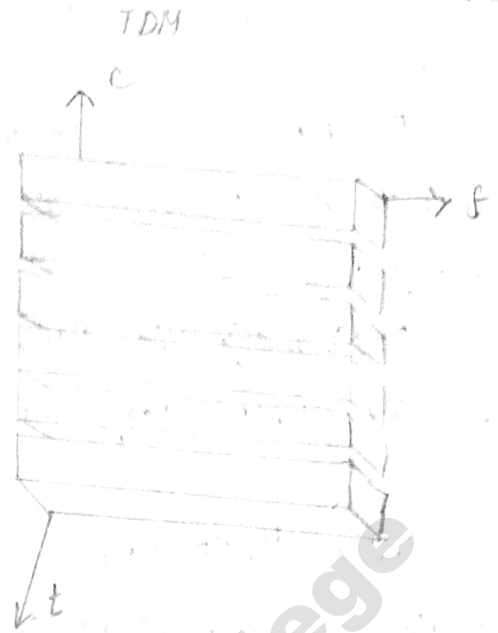
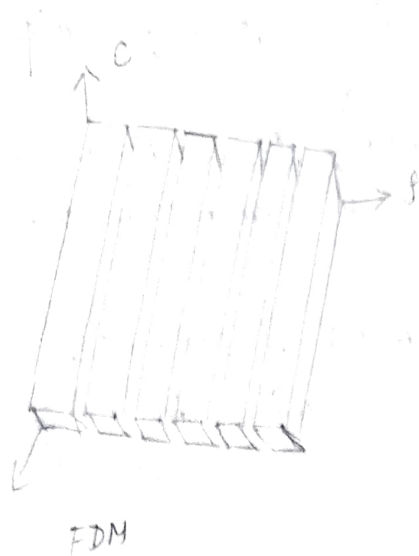
Adv:-

* Only one carrier is in the medium at any time.

* Throughput high even for many users

Dis:-

precise clock synchronization necessary



Time & freq Multiplexing

⇒ FDM & TDM can be combined i.e. a channel

⇒ [A channel gets a certain frequency band for a certain amount of time]

⇒ Now guard spaces are needed both in time & freq dimension. The channel may use this band only for a short period of time

eg: GSM.

Adv:-

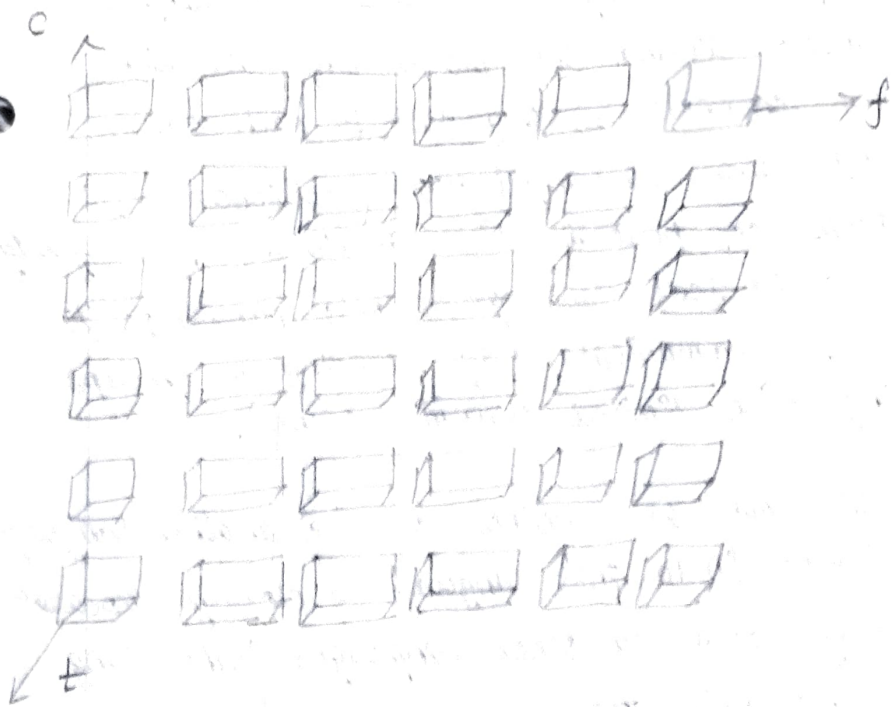
Better protection against tapping.

protection against freq selective interference.

Higher data rates

Dis:-

precise clock synchronization necessary.



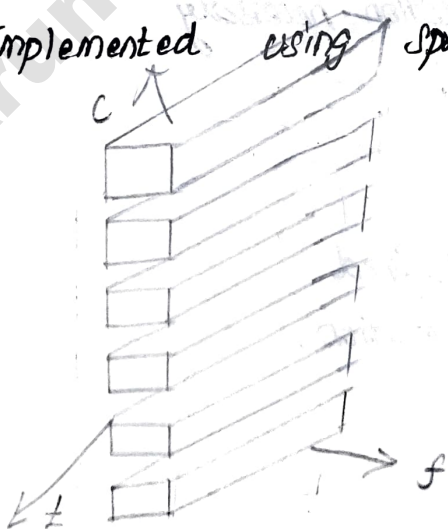
Code division Multiplexing. [

* Figure shows how [all channels n_i uses the same ^{spectrum} freq. at same time for transmission]

Separation is now achieved by assigning [each channel its own code]

" Separation is now achieved by assigning each channel its own code. guard spaces are realized by using codes with the necessary 'distance' in code space, eg. orthogonal codes.

Implemented using spread spectrum technology.



Eg of CDMA - party with many participants from different countries around the world who establish comm. channels. i.e) they talk to each other, using same freq range (approx 300-6000 Hz depends on personal voice) at same. If everybody speaks the same language, SDM is needed to be able to communicate (eg. standing in groups, talking with limited transmit power).

* But as soon as another code i.e) another language is used, one can tune in to this language & clearly separate comm in this language from all other languages. (Other lang appears as background noise). This explains why CDMA has built in security.

* If language is unknown, the signals can still be received, but they are useless.

* By using a secret code, a secure channel can be established in a hostile environment. Guard spaces are also important in this illustrative example.

Adv:-

Bandwidth Efficient.

No Coordination & Synchronization necessary

Good ^{protec against} interference & tapping.

Dis:-

Precise power control required

More complex signal regeneration.

Data tr. rate is low

AD

Spread Spectrum

1. Two stage Modulation Technique

1. Each tx information spread into N pulses referred as chips

2. Chips are tx over digital Modulator

Received Side:-


1. tx ed chips demodulated & passed through correlator that despread signal

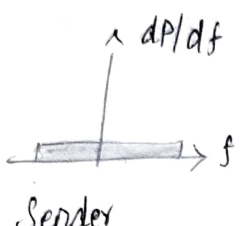
Spread Spectrum

Problem of radio tx: Frequency dependent fading can wipe out narrow band signals for duration of the interference.

Solution: [Spread the narrow band signal into broadband signal using a special code]

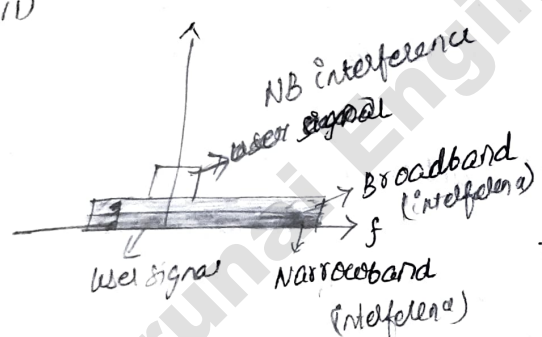
Steps Protection against narrow band interference $dp \rightarrow$ power density

(i)  shows an idealized narrowband signal from a sender or user data

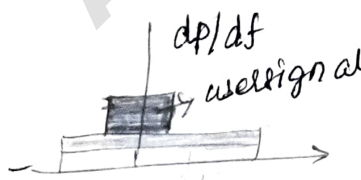
(ii)  Sender now spreads the signal in step (i)

- * Converts NB to Broadband signal.
- * energy needed to tx is same, but it is now spread over a larger freq range.

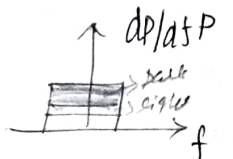
1. NB - BB
 2. Energy - same, but it is spread over larger freq
 3. Power \downarrow than original NB with
- * The power level of the spread signal can be much lower than that of the original narrow band signal without losing data.

(iii)  NB interference
user signal
Broadband (interference)
Narrowband (interference)
f

- * During transmission, narrowband & broadband interference add to the signal.
- * Sum of interference & user signal is received.

(iv)  dp/df
user signal
f

- * Receiver now knows how to despread the signal, converting spread user signal to narrowband signal again, while spreading the narrowband interference & leaving the broadband interference

(v)  dp/df
user signal
f

- * The receiver applies a BPF to cutoff frequencies left & right side of narrowband signal.

* Finally receiver can reconstruct the original data because the power level of the user signal is high (signal much stronger than remaining interfered)

Drawbacks:

- (i) Increased Complexity: of receivers that have to disspread a signal
- (ii) Large frequency band is needed due to spreading of signal

Although spread signals appear more like noise, they still raise the background noise level & may interfere with other transmission if no special precautions are taken.

Spread spectrum can be achieved in two different ways in following two sections

(i) Direct Sequence Spread Spectrum

It takes a user bit stream & perform an XOR with a so called chipping sequence

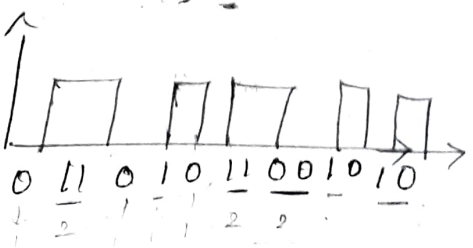
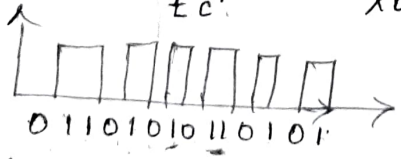
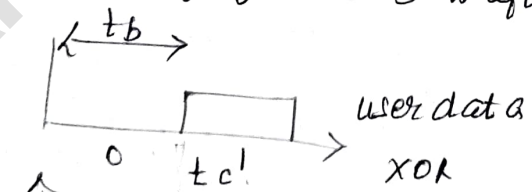
Eg:- 0110101 either its complement
 [If user bit equals 0] 1001010
 01101010110101 [If user bit equals 1]

* While each user bit has a duration t_b , Chipping sequence consists of smaller pulses called chips with a duration t_c .

* If chipping sequence is generated properly it appears as random noise. This is sometimes called as pseudo-noise sequence

Spreading factor $S = \frac{t_b}{t_c}$ determine B.W of resulting signal

(If Original sig need B.W W ,
 Resulting sig need $S \cdot W$ after spreading)



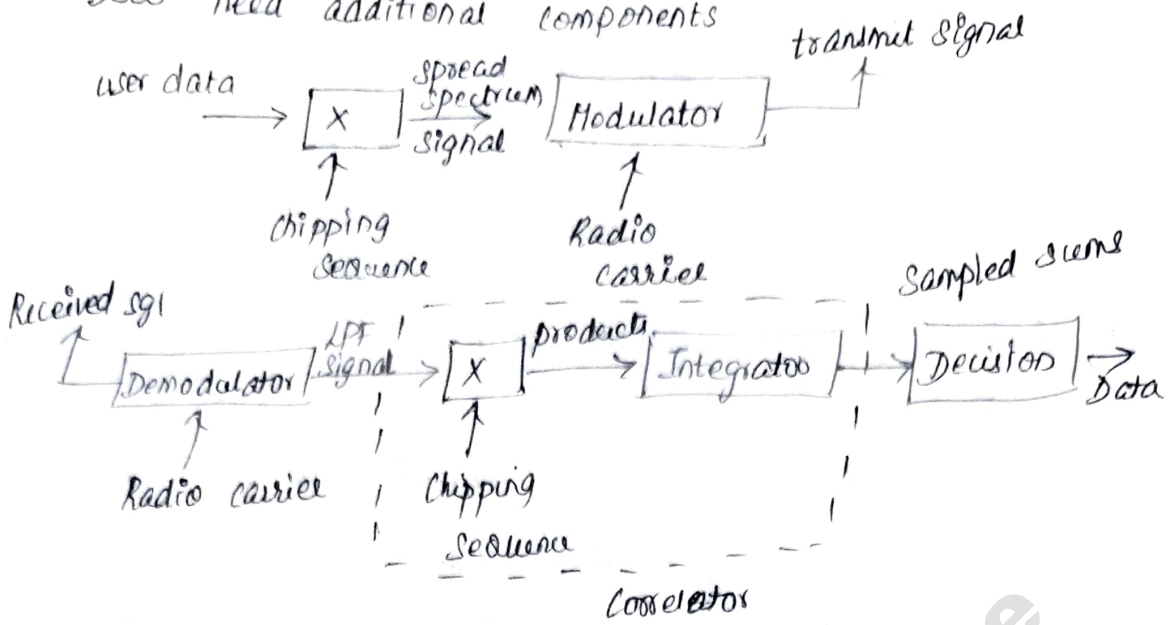
000
 011
 101
 110

chipping sequence

Resulting signal

Spreading user data with chipping seq called digital modulation

DSSS need additional components



1. Spreading user data with chipping sequence (digital Modulator)
 eg: Assuming U-D B.W 1MHz, spreading above 11-chip Barker code would result in signal with 11MHz B.W. The radio carrier then shifts signal to f_c . (eg 2.4 GHz in ISM band)

2. (DSSS receiver complex than tx) rx need to perform inverse functions of a transmitter modulation steps. (Noise & Multipath propagation require additional Mechanisms to reconstruct the original data.)

Steps in receiver

1. Demodulation of received signal. (achieved using same carrier as transmitter reversing the modulation & results in a signal with approx same B.W as original spread spectrum signal.)

2. Additional filter applied to generate the signal

If tx & rx synchronized properly & signal not too much distorted. DSSS works perfectly

eg sending user data 01

Applying 11 chip Barker Code

Results in 1011011100001001000111.

On receiver side, signal XORed bit wise after demodulation with same barker code as chipping seq

Results in sum of products equal to 0 for the first bit & to 11 for second bit

Decision unit now map first sum (= 0) to a binary 0,

Second sum (= 11) to binary 1 that constitutes original user data.

Dis - 7 sampling rates. More complex hardware

(ii) Frequency hopping spread spectrum (in order to avoid jammer, center freq of tx & rx shifts in freq coord)

eg: Radio station

* For FHSS, total available BW is split into many channels of smaller BW + guard band b/w channels. It called in pairs random channel

* Tx & Rx stay on ^{one of} these channels for certain time & then hop to another channel. This sys implements FDH/TDM.

* The pattern of channel usage called hopping sequence. The time spend on a channel with a certain frequency is called dwell time

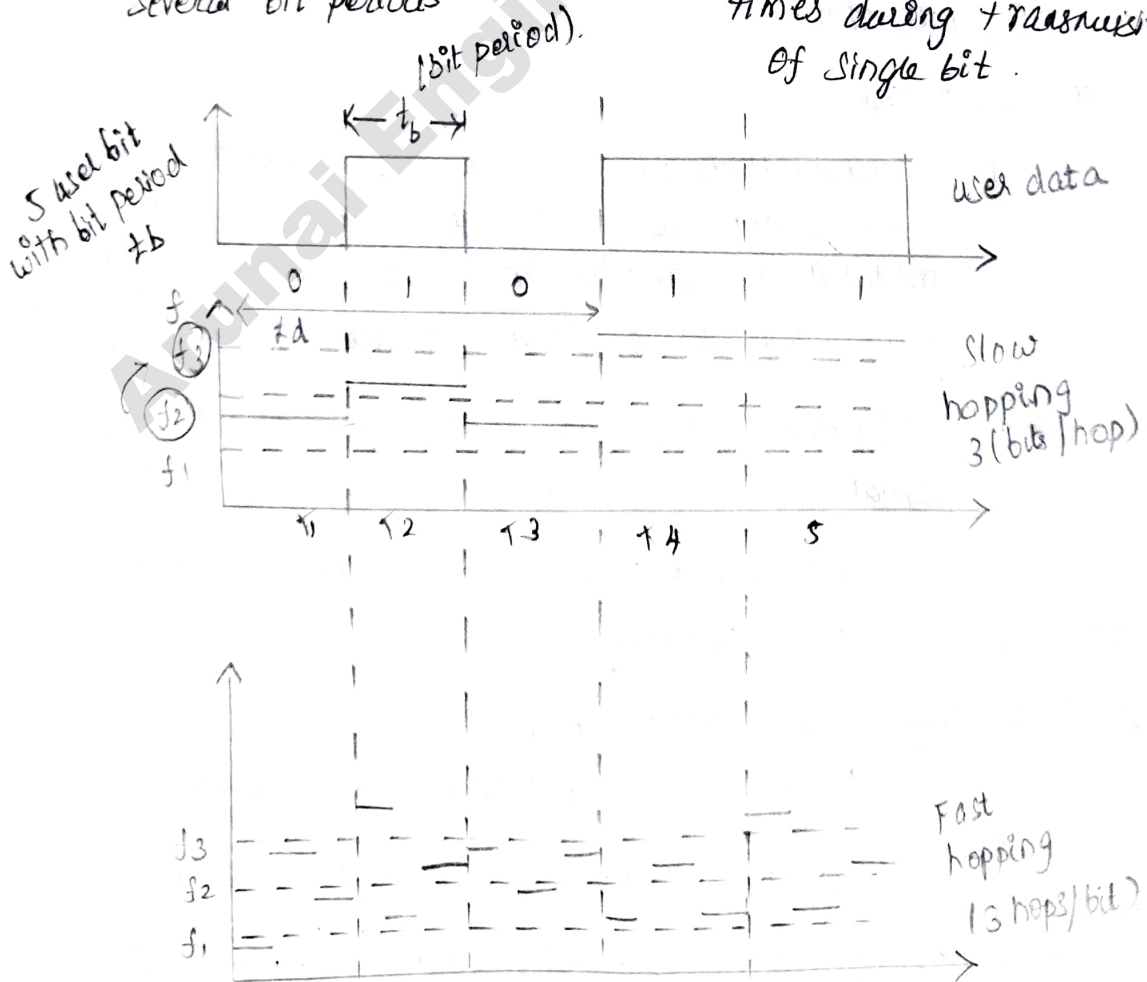
FHSS → two variants (slow & fast hopping).

Slow

Fast

1. tx uses 1 freq for several bit periods

tx changes freq several times during transmission of single bit.



In slow hopping,

⇒ Figure shows five user bits with a bit period T_b

⇒ Performing slow hopping, tx uses freq f_2

uses freq $f_2 \rightarrow tx$ 1st 3 bits during dwell time t_d .

Then, transmitter hops to next freq f_3 .

⇒ Cheaper & have relaxed tolerances, but they are not as immune to narrow band interference & as fast hopping systems.

In Fast hopping

* the transmitter hops three times during a bit period.

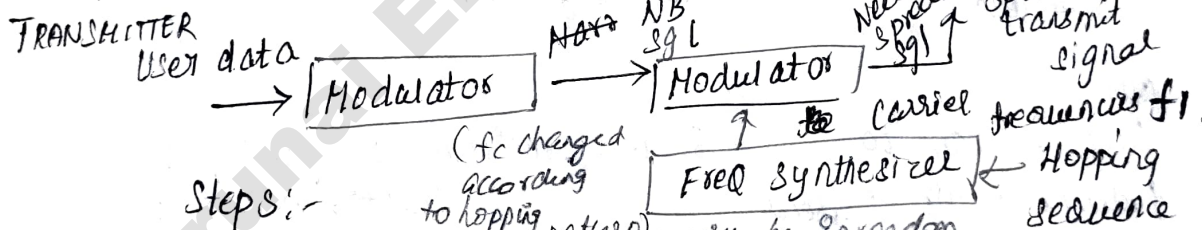
In Figure,

⇒ tx hops three times during a bit period.

* More complex to implement / tx & Rx have to stay synchronized with in smaller tolerances to perform hopping at more or less the same points in time).

* (This method is much better at overcoming the effects of narrowband interference & frequency selective fading as they only stick to one freq for a very short time)

Simplified FHSS tx & Rx



Steps:- 1. (Modulation) of user data according to of one D-A modulation schemes (eg FSK or BPSK) (Result in NB sgl)

If FSK used $\rightarrow f_0$ for binary 0
 f_1 for binary 1

2. (Frequency hopping) based on Hopping Sequence

Hopping seq fed in freq syn. generates carrier frequencies f_i

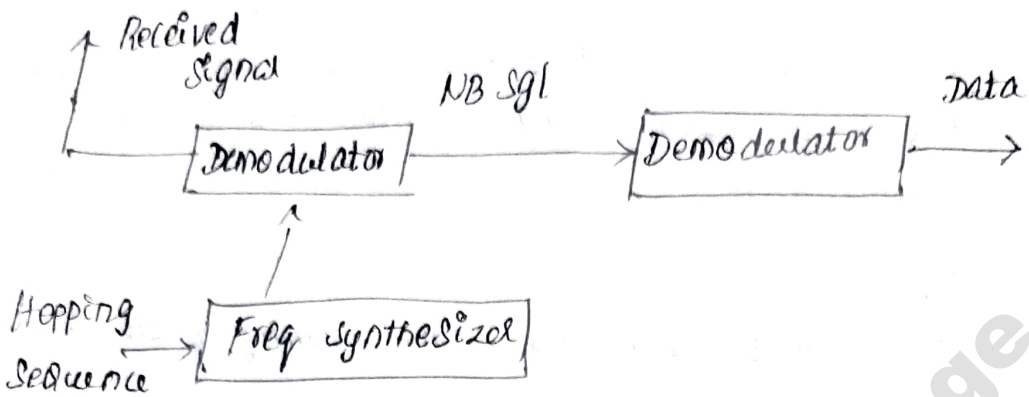
3. Modulation - uses modulated NB sgl & f_c to generate

New spread sgl with freq $f_i + f_0$ for 0

$f_i + f_1$ for a 1.

If different FHSS uses hopping sequences that never overlap (if 2 tx never use same freq. at same time, then these two don't interfere)

RECEIVER



receiver of FHSS s/m has to know the hopping sequence

& must stay synchronized.

* Demodulation

Comparison

DSSS

FHSS

- | | |
|---|--|
| 1. Spreading is simpler | 1. Spreading is complex. |
| 2. Sampling rates higher | |
| 3. More complex hardware implementation | 2. It only use a portion of total band at any time |
| 2. Always use total BW available. | |

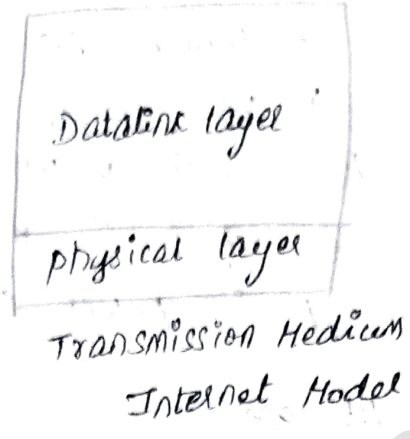
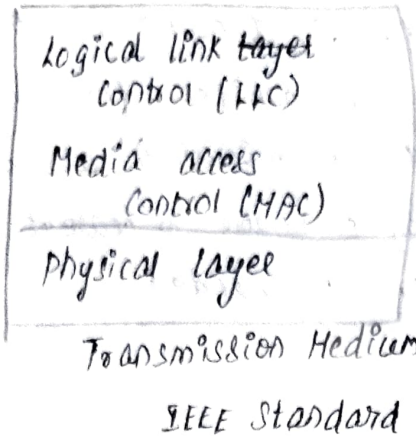
Adv

- | | |
|---|---|
| 3. More resistant to fading & multipath effects | 3. less resistant to fading & multipath effects |
| 4. DSSS signal are much harder to detect without knowing the spreading code. Detection is virtually impossible. | |

If each sender has its own pseudo-random number sequence for spreading the sgl (DSSS or FHSS) the system implements CSMA.

MAC (Medium access control)

The Medium access control data communication protocol sub-layer also known as Medium access control



CSMA/CD not suited for wireless networks

- * Signal strength decreases proportional to the square of the distance
- * the sender would apply CS & CD, but the collisions happen at the receiver, it might be the case, that a sender can't hear the collision. i.e. (CD doesn't work)

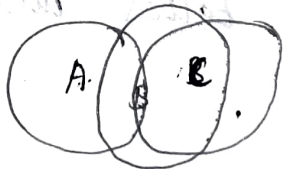
* CS might not work, if a terminal is 'hidden'

Hidden & Exposed terminals

Hidden terminal (Cause collision)

CS fails because hidden terminals

- * A sends to B, C cannot receive A
- * C wants to send to B, C senses a "free medium"
- * collision at B, A cannot receive the collision CD fails
- * A is hidden for C



Exposed terminal (unnecessary data)

- * B sends to A, C wants to send to another terminal (not A or B)
- * C has to wait, CS signals a medium in use, it
- * But A is outside the radio range of C, (therefore waiting is not necessary) ^{postponed transmission}
- * C is Exposed to B.

Near & far terminals

Terminal A & B send, C receives

* Signal strength decreases proportional to $\sqrt{\text{distance}}$

* terminal B's signal, \therefore drowns out A's sigl.

* If C for eg was an orbiter for sending signals

terminal B would drown out terminal A already on

the physical layer. (Making C unable to hear out A)

Problem:- precise power control is needed.

ACCESS METHODS:-

(i) SDMA

* used for allocating a separated space to users in

wireless N/w's.

* App:- assigning optimal Base Station to Mobile Phone user.

* HAC algorithm

Now decide which base station is best,

which frequencies (FDM), TDM, CDM are still available.

BASIS of SDMA algorithm:-

* Formed by cells & Sectorized antennas which

constitute the infrastructure implementing SDMA.

* Adv:- not requiring any Mux element

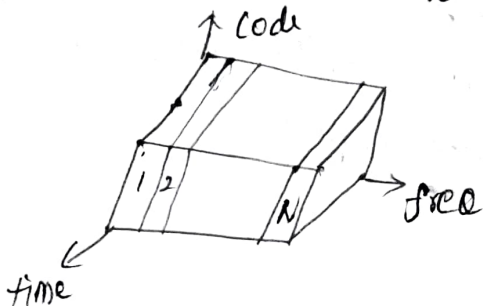
* It's usually combined with other multiplexing techniques to better utilize the individual physical

channels

(ii) FDMA

FDM describes schemes to subdivide the frequency

dimension into several non-overlapping freq bands.



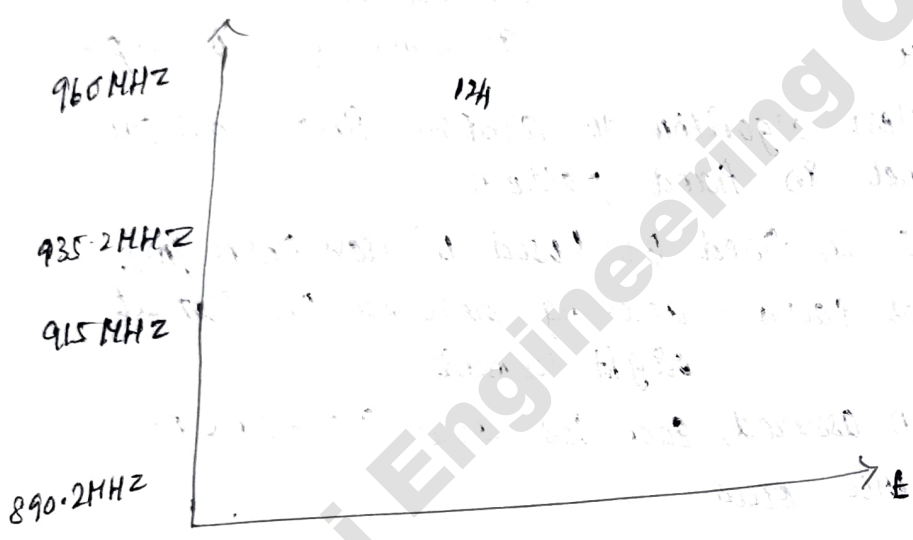
* FDMA Employed to allow several user to transmit simultaneously on one satellite transponder by assigning a specific frequency within the channel to each other

* Each conversation gets its own, unique, radio channel. channels \rightarrow narrow (usually 30 kHz or less) are defined either transmit or receive.

* FDM is often used for simultaneous access to the medium by MS & BS in cellular N/W's establishing a duplex channel.

* This is also called as FDD. freq division duplexing.

FDM for multiple access & duplex



uplink \rightarrow The two frequencies from mobile to base station

downlink \rightarrow from base to mobile station.

The basic freq allocation for GSM is fixed & regulated by national authorities.

- uplinks \rightarrow use band b/w 890.2 & 915 MHz
- downlink \rightarrow use 935.2 to 960 MHz

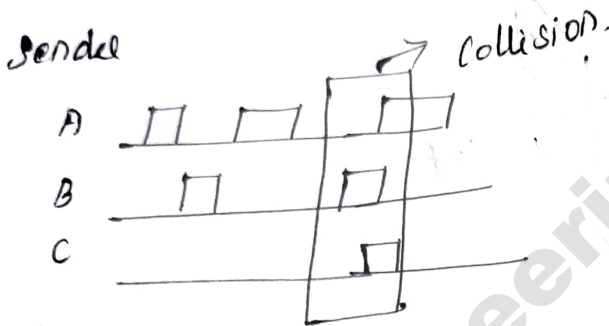
Assigning diff slots for uplink & downlink using same freq called TDD (Time division duplex)

Dis:-

- wastes lots of B/W
- too static,
- too inflexible for data communication

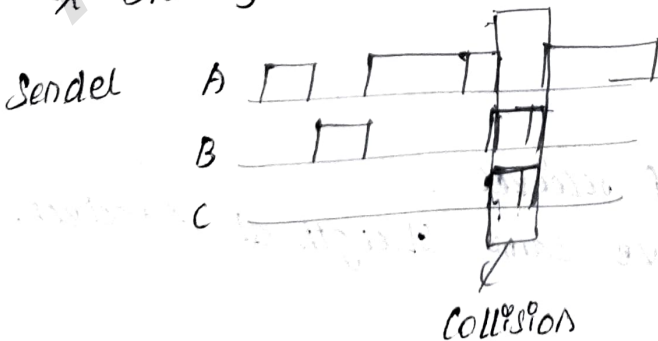
(ii) classical Aloha

- * TDM is applied without controlling Medium access
- Each station access the Medium at any time
- * Random access scheme, [If 2 station access same medium collision occur.
- * Retransmission of data req.



(iii) Slotted Aloha

- * Introduction of time slots.
- * all senders have to be synchronized, & start only at beginning of time slot
- * If station missed the time slot, station must wait beginning of next time slot
- * slotting doubles the throughput

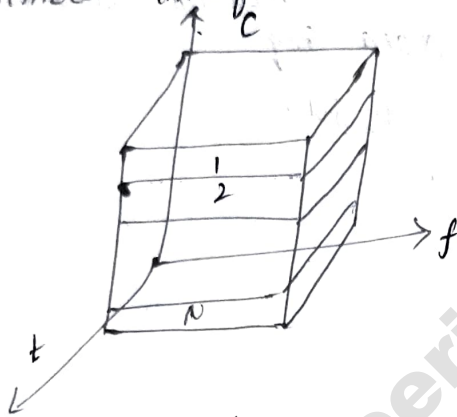


(iii) CSMA

- * To minimize chance of collision, \therefore \uparrow performance.
- * It is based on principle
 - * Sense before transmit
 - * Listen before talk.

(iv) CDMA

It applies codes with certain frequencies characteristics to the transmission to separate different users in code space & to enable access to a shared medium without interference.



All terminals send on same freq, probably at same time & can use the whole B.W. of the transmission channel.

Each sender \rightarrow unique random no, Sender XOR with random no.

The receiver can tune in to signal, if it knows pseudo random no; tuning is done via correlation function.

Dis :-

- * Higher complexity of receiver
- * All sigs would have same strength at receiver.

Adv:-

- * All terminals can use the same freq, no planning needed.
- * Huge code space (eg 232) compared to frequency space.
- * Soft hand over

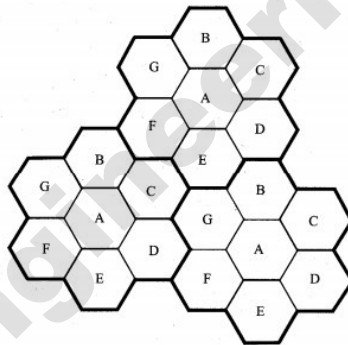
UNIT-2

MOBILE TELECOMMUNICATION

SYSTEM

INTRODUCTION TO CELLULAR SYSTEM

- Wireless communication technology in which several small exchanges (called cells) equipped with low-power radio are interconnected through a central exchange
- As a receiver (cell phone) moves from one place to the next,
 - Its identity, location, and radio frequency is handed-over by one cell to another without interrupting a call



Features

- Higher capacity, higher number of the users
 - Cellular systems can reuse spectrum according to certain patterns
 - Each cell can support a maximum number of users

-
- Mobile devices use less power than with a single transmitter or satellite since the cell towers are closer
 - Larger coverage area than a single terrestrial transmitter
 - Additional cell towers can be added indefinitely and are not limited by the horizon
 - Support user localisation and location based services
 - Less transmission power needed
 - Smaller cells also allow for less transmission power

BASIC CELLULAR SYSTEMS

The two basic cellular systems are

- Circuit-switched system
- Packet-switched system

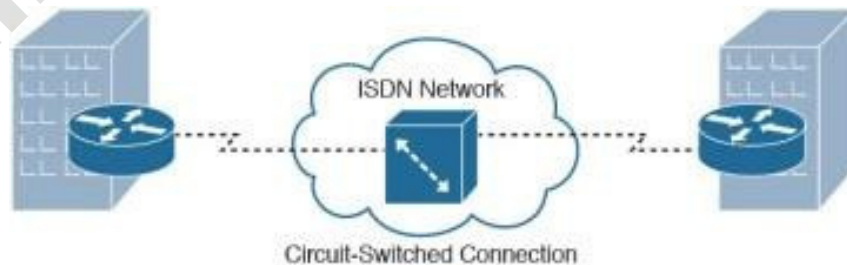
CIRCUIT-SWITCHED SYSTEM

Circuit switching requires a dedicated physical connection between the sending and receiving devices.

Example

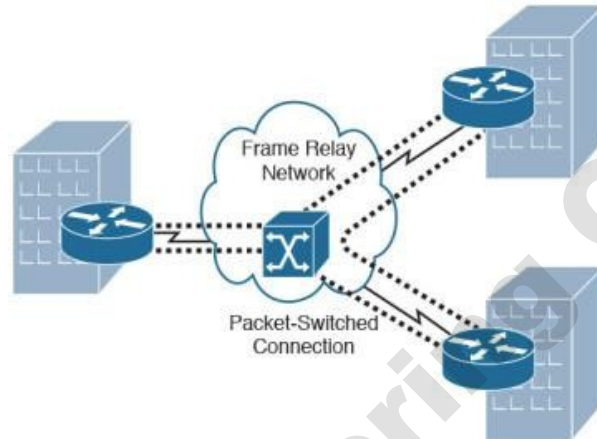
Parties involved in a phone call have a dedicated link between them for the duration of the conversation. When either party disconnects, the circuit is broken, and the data path is lost. This is an accurate representation of how circuit switching works with network and data transmissions.

The sending system establishes a physical connection, and the data is transmitted between the two. When the transmission is complete, the channel is closed.



PACKET-SWITCHED SYSTEM

Each packet is assigned source and destination addresses. Packets are required to have this information because they do not always use the same path or route to get to their intended destination. Packets can take an alternative route if a particular route is unavailable for some reason.



COMPARISON BETWEEN CIRCUIT-SWITCHED SYSTEM AND PACKET-SWITCHED SYSTEM

FEATURES	CIRCUIT SWITCHING	PACKET SWITCHING
Orientation	Connection oriented	Connectionless
Purpose	Initially designed for Voice communication	Initially designed for Data Transmission
Flexibility	Inflexible, because once a path is set all parts of a transmission follows the same path	Flexible, because a route is created for each packet to travel to the destination
Order	Message is received in the order, sent from the source	Packets of a message are received out of order and assembled at the destination

Technology/ Approach	Circuit switching can be achieved using two technologies, either Space Division Switching or Time-Division Switching	Packet Switching has two approaches Datagram Approach and Virtual Circuit Approach
Layers	Circuit Switching is implemented at Physical Layer	Packet Switching is implemented at Network Layer
Resource	Resource reservation is the feature of circuit switching because path is fixed for data transmission.	There is no resource reservation because bandwidth is shared among users.
Wastage	Wastage of resources are more in Circuit Switching	Less wastage of resources as compared to Circuit Switching
Reliability	More reliable	Less reliable

GENERATIONS OF TELECOMMUNICATION SYSTEMS

- 1G (first generation)
 - Voice-oriented systems based on analog technology
 - Example
 - Advanced Mobile Phone Systems (AMPS)
 - Cordless systems
- 2G (second generation)
 - Voice-oriented systems based on digital technology
 - More efficient and used less spectrum than 1G
 - Example
 - Global System for Mobile (GSM)
 - US Time Division Multiple Access (US-TDMA)

-
- 3G (third generation)
 - High-speed voice-oriented systems integrated with data services
 - Example
 - General Packet Radio Service (GPRS)
 - Code Division Multiple Access (CDMA)
 - 4G (fourth generation)
 - Still experimental, not deployed yet;
 - Based on Internet protocol networks and will provide voice, data and multimedia service to subscribers

GSM

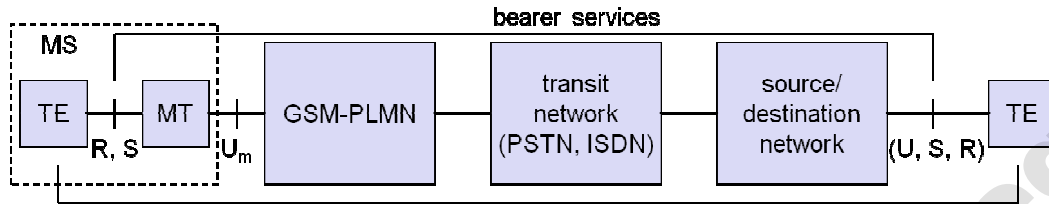
- Formerly: Groupe Spéciale Mobile
 - Founded in 1982
- Now: Global System for Mobile Communication
 - With the specification of Pan-European standard (ETSI, European Telecommunications Standardisation Institute)
 - Most successful digital mobile telecommunication system
 - Second generation cellular system
- Primary goal
 - Provide a mobile phone system that allows users to roam throughout Europe and provides voice services compatible to ISDN and other PSTN systems
- Characteristics
 - Provide voice services and data delivery using digital modulation

GSM SERVICES

GSM has defined the following three different categories of services

- Tele-services
- Bearer Services
- Supplementary services

Reference model



MS-Mobile Station	TE – Terminal	MT – Mobile Termination
PLMN – Public Land Mobile Network	PSTN – Public Switched Telephone Network	ISDN – Integrated Services digital Network

- MS connected to GSM-PLMN via U_m interface
- GSM-PLMN is connected to transit network (PSTN or ISDN)
- The transit network is connected to source/destination network

TELE SERVICES

- Focus on high quality voice-oriented tele services via mobile phones
- Comprises
 - Encrypted voice transmission
 - Message services
 - Basic data communication
- Voice related services offered by GSM
 - Mobile telephony
 - Offers the traditional bandwidth of 3.1 kHz
 - Goal of GSM
 - Provide high-quality digital voice transmission with the typical bandwidth of 3.1 kHz of analog phone systems
 - Emergency number
 - Common number used by all

-
- Mandatory for all providers with free of charge
 - Has highest priority - preempts other connections
 - Automatically setup with closest emergency center
 - Multi Numbering
 - Several ISDN phone numbers per user possible
 - Additional services (Non-Voice Teleservices)
 - Short Message Service (SMS)
 - Offers transmission of messages of up to 160 characters
 - Also transfers logos, ring tones, horoscopes and love letters
 - Do not use the standard data channels of GSM
 - Used for the following applications
 - Displaying road conditions
 - E-mail Headers
 - Stock quotes
 - Used to reach a mobile phone from within the network
 - Used for updating mobile phone software or for implementing so-called push services
 - Enhanced Message Service (EMS)
 - Successor of SMS
 - Offers transmission of
 - Messages up to 760 characters
 - Formatted text,
 - Animated pictures
 - Small images
 - Ring tones

-
- Multimedia Message Service (MMS)
 - Offers the transmission of
 - Larger pictures (GIF, JPG, WBMP)
 - Short video clips
 - group 3 fax
 - Fax data is transmitted as digital data over the analog telephone network according to the ITU-T standards T.4 and T.30 using modems

BEARER SERVICES

- Telecommunication services to transfer data between access points
 - R and S interfaces
 - Provide network independent data transmission from end device to mobile termination point.
 - U interface
 - Provides the interface to the network (TDMS, FDMA, etc.)
- Types
 - Transparent bearer services
 - Use the functions of the physical layer to transmit data
 - Has a constant delay and throughput if no transmission errors occur
 - To increase transmission quality using Forward Error Correction (FEC)
 - Do not try to recover lost data
 - No error control of flow control, only FEC
 - Non-transparent bearer services
 - Use protocols of layers two and three to implement error correction and flow control
 - Use the transparent bearer services in addition to radio link protocol (RLP)

-
- Protocol comprises
 - Mechanisms of High-Level Data Link Control (HDLC)
 - Selective-reject mechanisms to trigger retransmission of erroneous data
 - Error control, flow control
 - Different data rates for voice and data (original standard)
 - Voice service (circuit switched)
 - Synchronous: 2.4, 4.8 or 9.6 Kbps.
 - data service (circuit switched)
 - Synchronous: 2.4, 4.8 or 9.6 kbit/s
 - Asynchronous: 300 - 1200 bit/s
 - data service (packet switched)
 - Synchronous: 2.4, 4.8 or 9.6 kbit/s
 - Asynchronous: 300 - 9600 bit/s

SUPPLEMENTARY SERVICES

- Provides services in addition to the basic services
- Important services
 - User identification
 - Call forwarding(or Redirection)
 - Automatic call-back
 - Conferencing with up to 7 participants
- ISDN features
 - Closed user group
 - Multiparty communication

GSM SYSTEM ARCHITECTURE

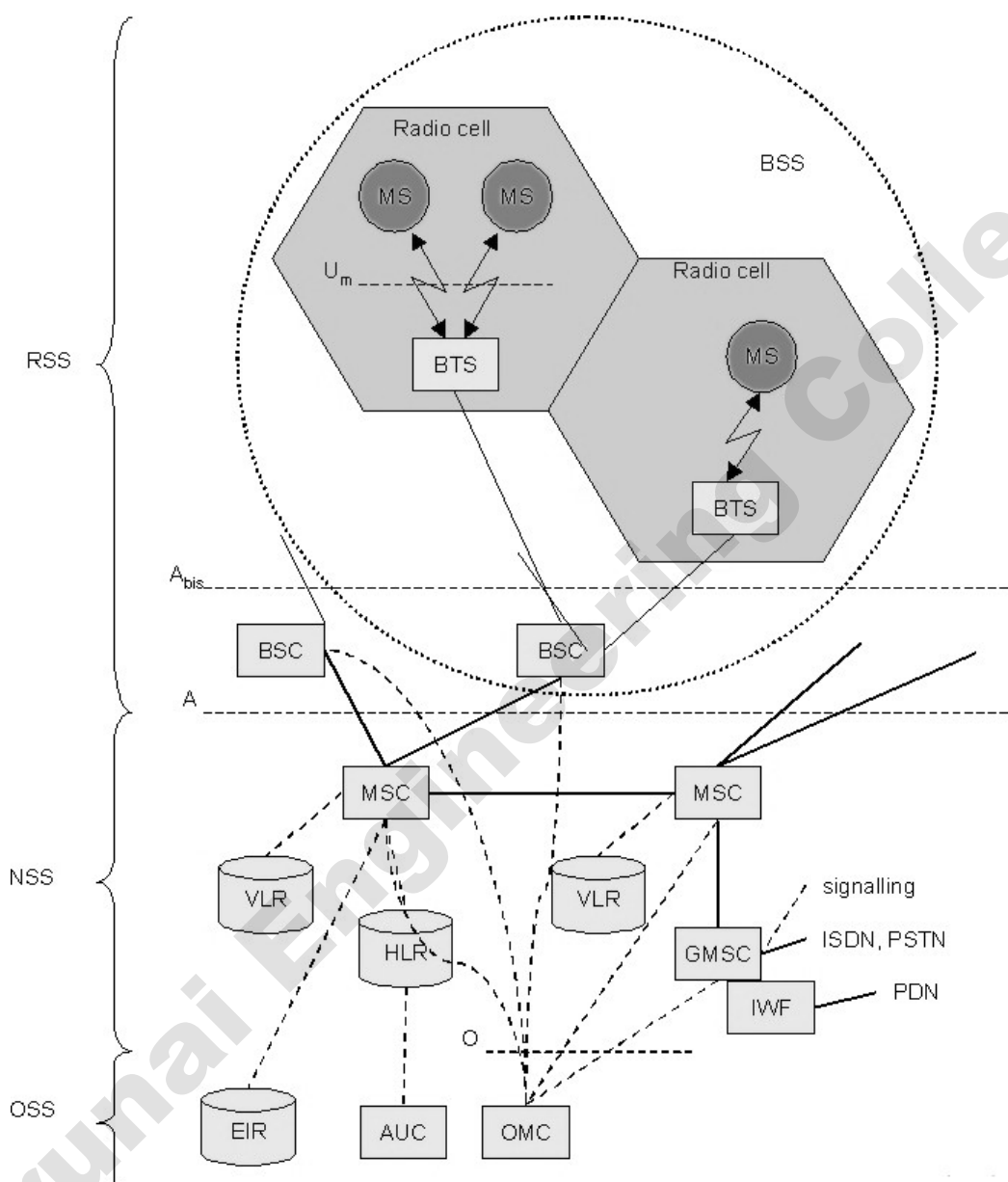
- GSM is a Public Land Mobile Network (PLMN)

Subsystems of GSM Architecture

- Radio SubSystem (RSS)
- Network and Switching Subsystem (NSS)
- Operation SubSystem (OSS)

Types of Interface

- **A interface**
 - Makes the connection between the RSS and the NSS
 - Based on circuit-switched PCM-30 systems (2.048 Mbit/s), carrying up to 30 64 kbit/s connections
- **O interface**
 - Makes the connection between the RSS and the OSS
 - Uses the Signalling System No. 7 (SS7) based on X.25 carrying management data to/from the RSS
- **U_m interface**
 - Makes the connection between the BTS and MS
 - Contains all the mechanisms necessary for wireless transmission
- **A_{bis} interface**
 - Makes the connection between the BTS and BSC
 - Consists of 16 or 64 kbit/s connections



Functional architecture of a GSM system

RADIO SUBSYSTEM (RSS)

- RSS comprises all radio specific entities
 - Base Station Subsystem (BSS)
 - Contains many
- BSSs which are controlled by a BSC
- BTSs
 - Performs all functions necessary to
- Maintain radio connections to an MS
- Coding/decoding of voice
- Rate adaptation to/from the wireless network part
 - Base Transceiver Station (BTS)
 - Comprises all radio equipment necessary for radio transmission
- Radio Equipments
 - Antennas
 - Signal processing
 - Amplifiers
- Form a radio cell or several cells using sectorized antennas
 - Cell can measure between some 100 m and 35 km depending on the environment
 - Buildings
 - Open space
 - Mountains etc.
 - Base Station Controller (BSC)
 - Manages the BTSs
 - Reserves radio frequencies

-
- Handles the handover from one BTS to another within the BSS
 - Performs paging of the MS
 - Multiplexes the radio channels onto the fixed network connections at the A interface
 - Mobile Station (MS)
 - Comprises all user equipment and software needed for communication with a GSM network
 - MS consists of user independent
 - Hardware
 - Software
 - Subscriber Identity Module (SIM)
 - Stores all user-specific data that is relevant to GSM
 - Only emergency calls are possible without SIM
 - International Mobile Equipment Identity (IMEI)
 - Used to identify the MS
 - Used to personalize any MS using the SIM
 - User-specific mechanisms like charging and authentication are based on the SIM
 - Device-specific mechanisms like theft protection are based on IMEI
 - SIM card contains
 - a personal identity number (PIN)
 - Used to unlock the MS
 - Using the wrong PIN three times will lock the SIM
 - a PIN unblocking key (PUK)
 - Needed to unlock the SIM

-
- an authentication key K_i
 - the international mobile subscriber identity (IMSI)
 - Card-type
 - Serial number
 - A list of subscribed services
 - MS stores dynamic information while logged onto the GSM system
 - cipher key K_c
 - Location information
 - Temporary Mobile Subscriber Identity (TMSI)
 - Location Area Identification (LAI)

NETWORK AND SWITCHING SUBSYSTEM (NSS)

- The “heart” of the GSM system
- Connects the wireless network with standard public networks
- Performs handovers between different BSS
- Supports
 - Charging
 - Accounting
 - Roaming of users between different providers

Switches and databases of NSS

- **Mobile services switching center (MSC)**
 - High-performance digital ISDN switches
 - Used to set up connections to other MSCs and to the BSCs through A interface
 - Form the fixed backbone network of a GSM system
 - Connect to

-
- Fixed networks, such as PSTN and ISDN, using Gateway MSC (GMSC)
 - Public Data Networks (PDN), such as X.25, using Interworking Functions (IWF)
 - Standard Signaling System No. 7 (SS7)
 - Used for handling all signaling needed for
 - connection setup,
 - connection release and
 - handover of connections to other MSCs
 - Features
 - Number portability
 - Free phone/toll/collect/credit call
 - Call forwarding
 - Three-way calling etc
 - Performs all functions needed for supplementary services
 - Call forwarding
 - Multi-party calls
 - Reverse charging etc.,
 - **Home Location Register (HLR)**
 - Database that stores all user-relevant information
 - Static information
 - Mobile subscriber ISDN number (MSISDN)
 - Subscribed services
 - Example
 - Call forwarding

-
- Roaming restrictions
 - GPRS
 - International mobile subscriber identity (IMSI)
 - Dynamic information
 - Current location area (LA) of the MS
 - Mobile subscriber roaming number (MSRN)
 - Current VLR and MSC
 - **Visitor Location Register (VLR)**
 - Dynamic database that stores all important information needed for the MS users currently in the location area (LA)
 - If a new MS comes into an LA,
 - VLR is responsible to copy all that user's relevant information from the HLR
 - Purpose
 - Avoids frequent HLR updates
 - Long-distance signaling of user information

OPERATION SUBSYSTEM (OSS)

- Contains the necessary functions for
 - Network operation and
 - Maintenance

Entities

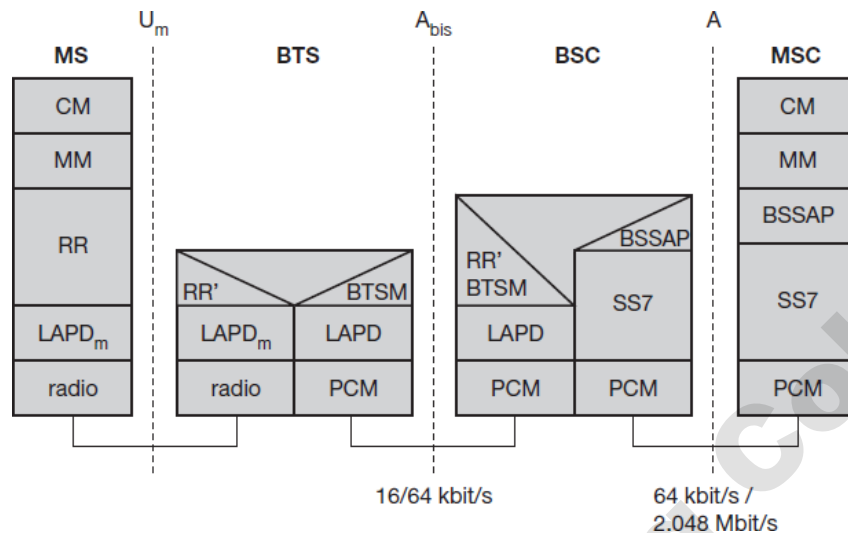
- **Operation and Maintenance Center (OMC)**
 - Monitors and controls all other network entities via the O interface
 - Management functions
 - Traffic monitoring

-
- Status reports of network entities
 - Subscriber and security management
 - Accounting and billing
 - Use the concept of telecommunication management network (TMN)
 - **Authentication Centre (AuC)**
 - Used to protect user identity and data transmission
 - Generates the values needed for user authentication in the HLR using
 - Authentication algorithms
 - Encryption keys
 - **Equipment Identity Register (EIR)**
 - Database for all IMEIs
 - Stores all device identifications registered for the network
 - Contains
 - List of stolen (or locked) devices (black list)
 - List of valid IMEIs (white list)
 - List of malfunctioning devices (gray list)
 - Used to
 - track handsets using IMEI
 - Block calls from stolen, unauthorized or defective mobiles

GSM PROTOCOL LAYERS FOR SIGNALING

The figure shows the signaling protocols between

- MS and BTS between U_m interface
- BTS and BSC between A_{bis} interface
- BSC and MSC between A interface



Protocol architecture for signaling

MS and BTS between U_m interface

- The air interface is used for exchanges between MS and BTS
- It is used for transmitting signals further

BTS and BSC between A_{bis} interface

- This is a BSS internal interface linking the BSC and BTS and it has not been standardized
- The A_{bis} interface allows control of the radio equipment and radio frequency allocation in the BTS

BSC and MSC between A interface

- The A interface linking the BSC and MSC
- The A interface manages the allocation of suitable radio resources to the MSs and mobile management

GSM protocol layers

- **Mobility management (MM)**

- The MM layer is in-charge of maintain the location data, in addition to the authentication and ciphering procedures

-
- **Communication Management (CM)**
 - The CM layer consists of setting up call at the user request
 - Its functions are call control, which manages the supplementary services configuration, short message services which provides point-to-point short message services
 - **Radio Resource (RR)**
 - The RR management layer is in-charge of establishing and maintaining a stable uninterrupted communication path between the MSC and MS over which signaling and user data can be covered
 - Handovers are part of the RR layer responsibility
 - Most of the functions are controlled by the BSC, BTS and MS though some are performed by the MSC
 - The RR layer is the part of the RR functionality which is managed by the BTS
 - **Base Transceiver Station Management (BTSM)**
 - The BTSM is responsible for transferring the RR information to the BSC

Link Access Protocol for the ISDN D-Channel (LAPD):

- Provides error free transmission between the BSC and MSC

LAPDm:

- It is a modified version of the LADP protocol
- The layer two protocols are provided for by LAPDm over the air-interface
- The main modification are due to the tight synchronization required in TDMA and its error protection mechanism required over the air-interface

Base Station System Application Part (BSSAP):

- The BSSAP is split into two parts the Base station system management application part(BSSMAP) and the direct transfer application part (DTAP)
- The message exchanges are handled by SS7

-
- Messages which are not transparent to the BSC are carried by the BSSMAP which supports all of the procedures between the MSC and the BSS that require interpretation and processing of information related to single calls and resource management

SS7

- Signaling system no.7 is used for signaling between MSC and BSC
- This protocol also transfer information between MSCs, HLR, VLR, Auc, EIR and MOC

GSM CONNECTION ESTABLISHMENT

LOCALIZATION

The localization is a process by which a mobile station is identified, authenticated and provided service by a mobile switching center through the base station controller and base Tran receiver either at the home location of the MS or at a visiting location. Mobile service providers, on the other hand will provide services to the user only after identifying the mobile station (MS) of the user and verifying the services subscribed to by the user or the services presently allowed to that MS. Localization mechanism of the GSM system fulfils both the requirement. GSM distinguishes explicitly between the user and the equipment. It also distinguishes between the subscriber identity and the telephone number.

GSM deals with many addresses and identifiers.

- **Mobile Subscriber ISDN Number (MSISDN)**
 - The MSISDN number is the real telephone number as is known to the external world.
 - MSISDN number is public information.
 - This is a number published and known to everybody.
 - In GSM a mobile station can have multiple MSISDN number
- **International Mobile Subscriber Identity (IMSI)**
 - When registered with a GSM operator each subscriber is assigned a unique identifier.
 - The IMSIO is stored in the SIM card and secured by the operator.

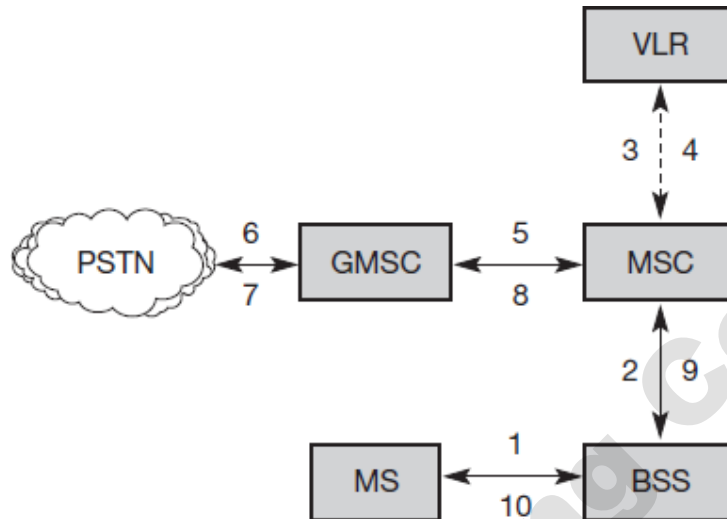
-
- A mobile station can only be operated when it has a valid IMSI
 - The IMSI consists of several parts
 - 3 decimal digits of mobile country code (MCC)
 - 2 decimal digit of mobile network code (MNC)
 - Maximum 10 decimal digits of mobile subscriber identification number (MSIN)
 - **Temporary Mobile Subscriber Identity (TMSI)**
 - Temporary identifier assigned by a serving VLR
 - It is used in place of the IMSI for identification and addressing of the mobile station
 - TMSI is assigned during the presence of the mobile station in a VLR.
 - Thus, it is difficult to determine the identity of the subscriber by listening to the radio channel.
 - The TMSI is never stored in the HLR.
 - However, it is stored in the SIM card. Together with the current location are, a TMSI allows a subscriber to be identify uniquely
 - **Mobile Station Roaming Number (MSRN)**
 - When a subscriber is roaming in another network a temporary ISDN number is assigned to the subscriber
 - This ISDN number is assigned by the local VLR in charge of the mobile station
 - The MSRN has the same structure as the MSISDN

Calling

There are different methods and protocols are used for establishing connection and maintaining communication in calling to and from mobile devices in a GSM network. The various types of calls handled by a GSM network are:

- Mobile originated call (MOC)
- Mobile Terminated call (MTC)

Mobile originated call (MOC)



1,2: Connection request

3,4: Security check

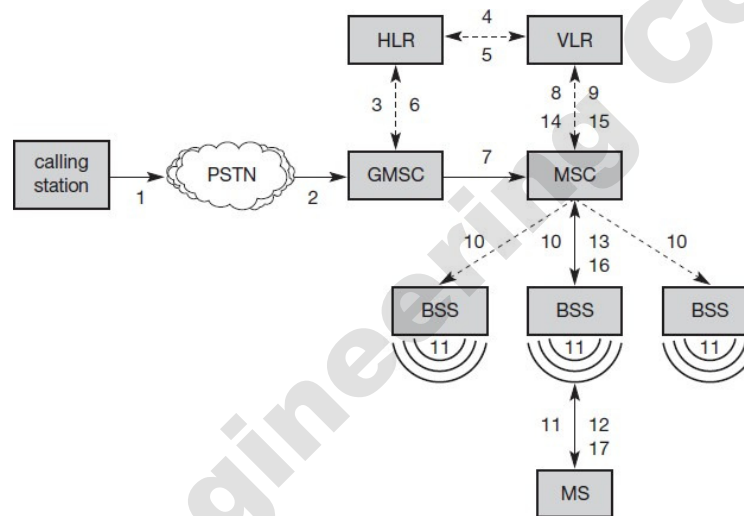
5-8: check resources (free circuit)

9-10: set up call

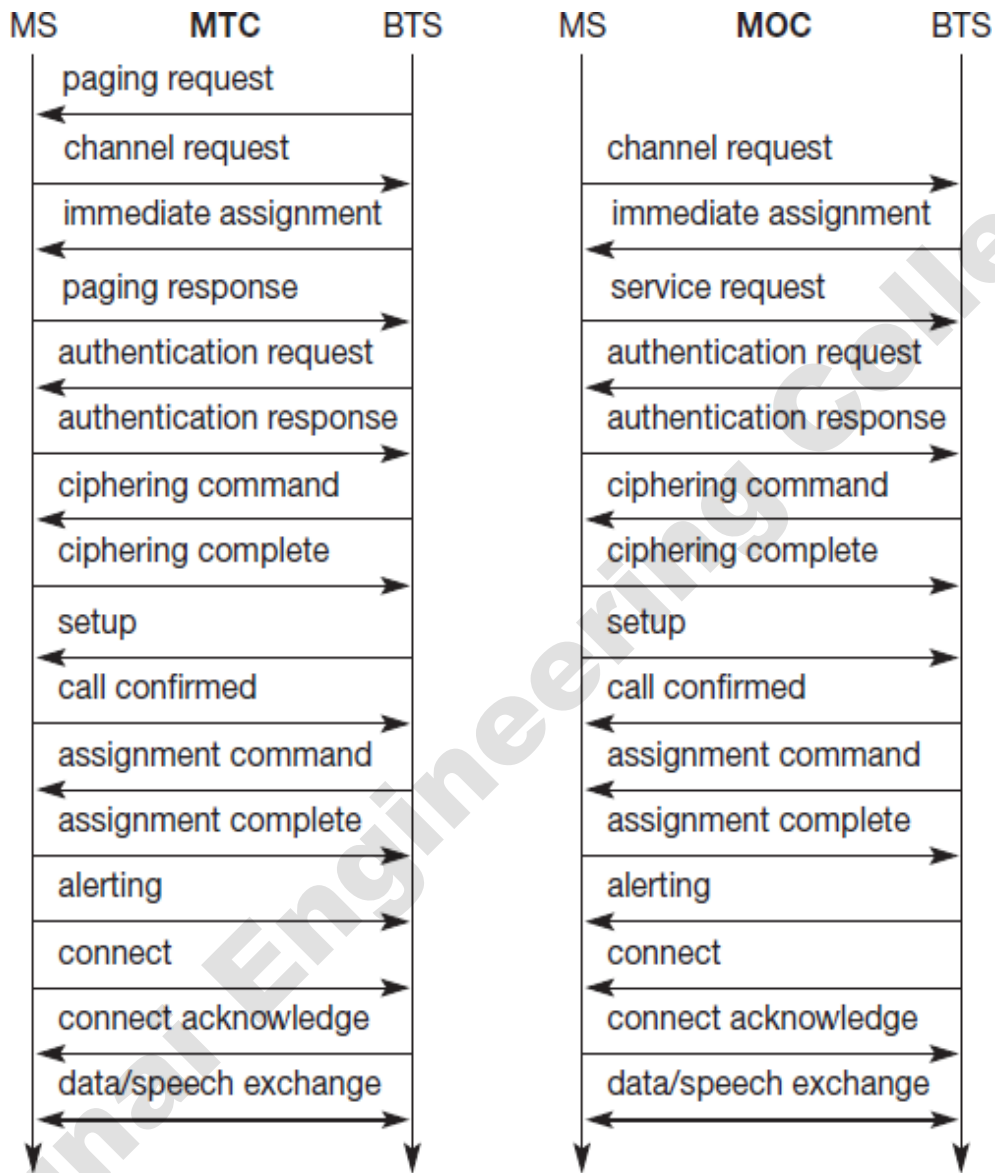
- Channel Request
 - MS requests for the allocation of a dedicated signaling channel to perform the call setup
- After allocation of a signaling channel the request for MOC call setup, including the TMSI (IMSI) and the last LAI, is forwarded to the VLR
- VLR requests the AC via HLR for Triples (if necessary).
- VLR initiates Authentication, Cipher start, IMEI check (optional) and TMSI Re-allocation (optional).
- If all these procedures have been successful, MS sends the Setup information (number of requested subscriber and detailed service description) to the MSC.

- The MSC requests the VLR to check from the subscriber data whether the requested service an number can be handled (or if there are restrictions which do not allow further proceeding of the call setup)
- If the VLR indicates that the call should be proceeded, the MSC commands the BSC to assign a Traffic Channel (i.e. resources for speech data transmission) to the MS
- The BSC assigns a Traffic Channel TCH to the MS
- The MSC sets up the connection to requested number (called party).

Mobile Terminated call (MTC)



- 1: Calling a GSM subscriber
- 2: Forwarding call to GMSC
- 3: Signal call setup to HLR
- 4, 5: Request MSRN from VLR
- 6: Forward responsible MSC to GMSC
- 7: Forward call to current MSC
- 8, 9: Get current status of MS
- 10, 11: Paging of MS
- 12, 13: MS answer
- 14, 15: Security checks
- 16, 17: Setup connection



Message flow for MTC and MOC

GSM Security

The SIM stores personal, secret data and is protected with a PIN against unauthorized use.

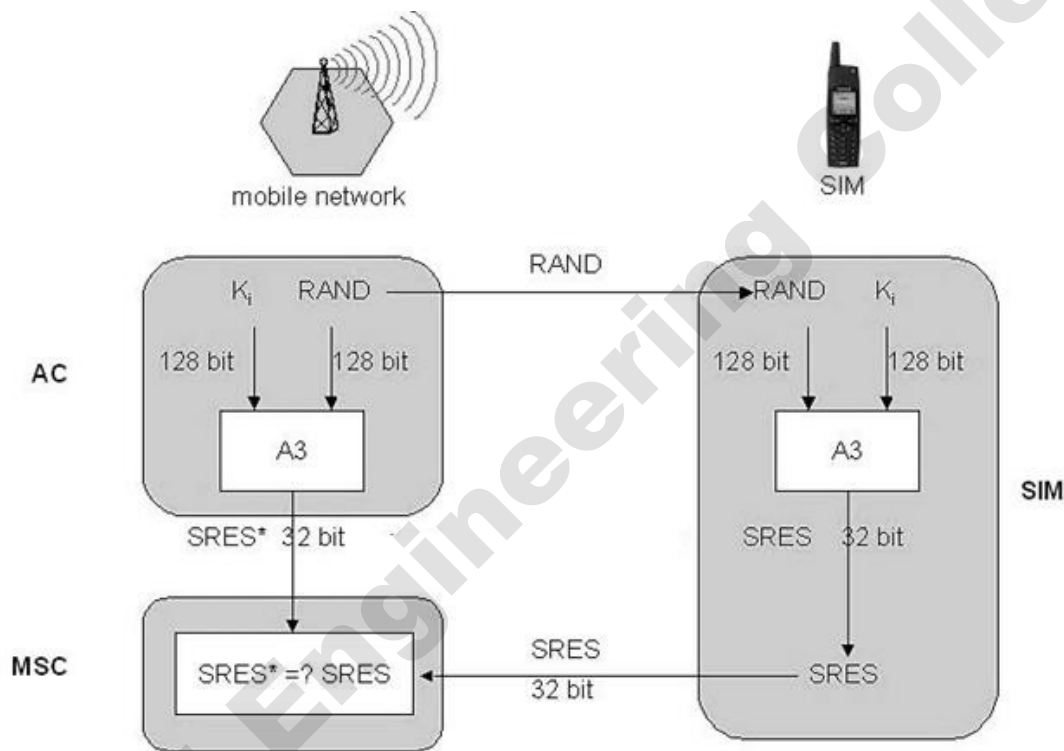
Security Services

- Access control and authentication
 - Authenticates the valid user for the SIM
 - User needs a secret PIN to access the SIM
 - Authenticates the subscriber
 - Based on a challenge-response scheme
- Confidentiality
 - Encrypt all user related data
 - BTS and MS apply encryption to
- Voice
- Data
- Signaling
 - Exists only between MS and BT
- Anonymity
 - To provide user anonymity
 - Encrypt all data before transmission
 - User identifiers are not used in transmission
 - GSM transmits a temporary identifier (TMSI),
- TMSI - newly assigned by the VLR after each location update
- VLR can change the TMSI at any time

Algorithms specified in GSM

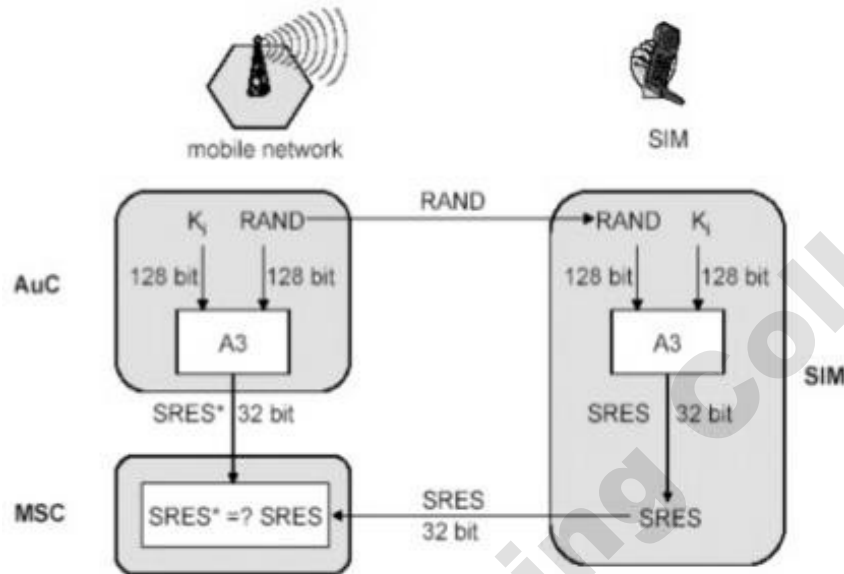
1. A3 for authentication
2. A5 for encryption
3. A8 for key generation

AUTHENTICATION



- Authentication is based on the SIM, which stores the user identification IMSI and the algorithm used for authentication A3
- Authentication uses a challenge-response method
- For authentication, the VLR sends the random value $RAND$ to the SIM.
- Both sides, network and subscriber module, perform the same operation with $RAND$ and the key K_c

ENCRYPTION



- To ensure privacy, all messages containing user-related information are encrypted in GSM over the air interface.
- After authentication, MS and BSS can start using encryption by applying the cipher key K_c
- MS and BTS can now encrypt and decrypt data using the algorithm A5 and the cipher key K_c

Advantages of GSM

- Communication
 - Mobile, wireless communication
 - Support for voice and data services
- Total mobility
 - International access, chip-card enables use of access points of different providers
- Worldwide connectivity
 - One number, the network handles every location.

-
- High capacity
 - Better frequency efficiency, smaller cells, more customers per cell.
 - High transmission quality
 - High audio quality and reliability for wireless, uninterrupted phone calls at higher speeds (e.g., from cars, trains).
 - Security functions
 - Access control, authentication via chip-card and PIN

Disadvantages of GSM

- No end-to-end encryption of user data
- Reduced concentration while moving
- Electromagnetic radiation
- High complexity of system
- Several incompatibilities within the GSM standards

GENERAL PACKET RADIO SERVICE (GPRS)

- Integrated with GSM
- Improves and simplifies internet access
- Transfers data packets from GSM mobile stations to external packet data networks
- GSM vs GPRS
 - GSM – Uses a billing system based on the time of connection
 - GPRS – Uses a billing system based on the amount of transmitted data
 - Connection set up times are reduced
 - Get charged only for the amount of transmitted data
- Enables new service opportunities

GPRS Services

- Point-to-point (PTP) service
 - Packet Transfer service between two users
 - Versions
 - PTP Connection Oriented Network Service (PTP-CONS)
- Maintains the virtual circuit upon change of the cell within the GSM network
 - PTP Connectionless Network Service (PTP-CLNS)
- Supports application based on the Internet Protocol (IP)
- Point-to-multipoint (PTM) service
 - Called as multicasting
 - Data transfer service from one user to multiple users
 - Types
 - Multicast PTM
 - Group call PTM
- QoS profile
 - Determines
 - service precedence (high, normal, low)
 - reliability class
 - delay class
 - user data throughput
- Delay
 - Introduced by external fixed network
 - Incurred by
 - channel access delay

-
- coding for error correction
 - transfer delays
 - Tries to forward packet as fast as possible
 - Security services
 - Authentication
 - Access control
 - User identity confidentiality
 - User information confidentiality

GPRS ARCHITECTURE

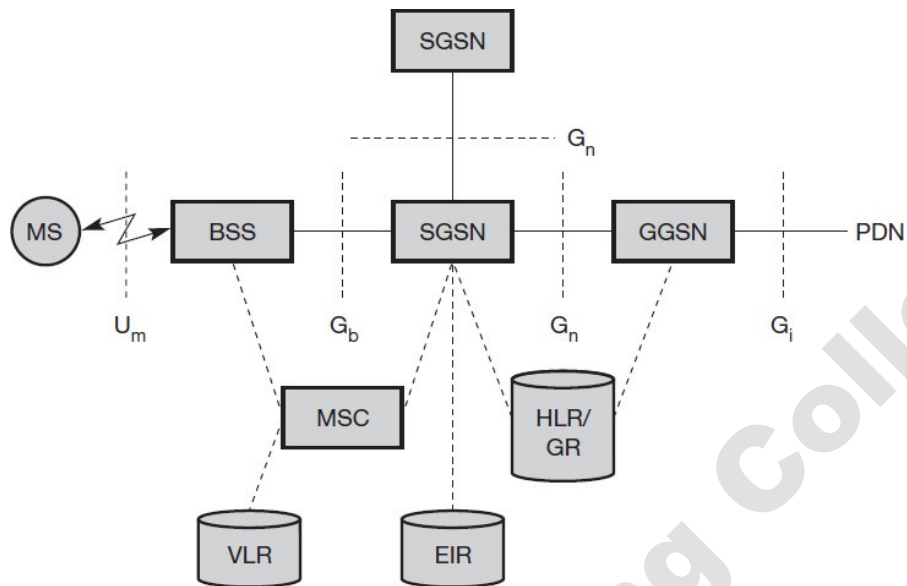
- GPRS have 2 network elements called as GPRS Support Nodes(GSN)
 - gateway GPRS support node (GGSN)
 - serving GPRS support node (SGSN)

Gateway GPRS Support Node (GGSN)

- Interworking unit between GPRS network and external packet data networks (PDN)
- Contains routing information for GPRS users
- Performs address conversion
- Tunnels data to a user
- Connected to external networks via the G_i interface
- Transfers packets to the SGSN via G_n interface

Serving GPRS Support Node (SGSN)

- Supports the MS via the G_b interface
- Requests user addresses from the GPRS register (GR)
 - Keeps track of the individual MSs' location
 - Stores all GPRS-relevant data
- Responsible for collecting billing information
- Performs access control



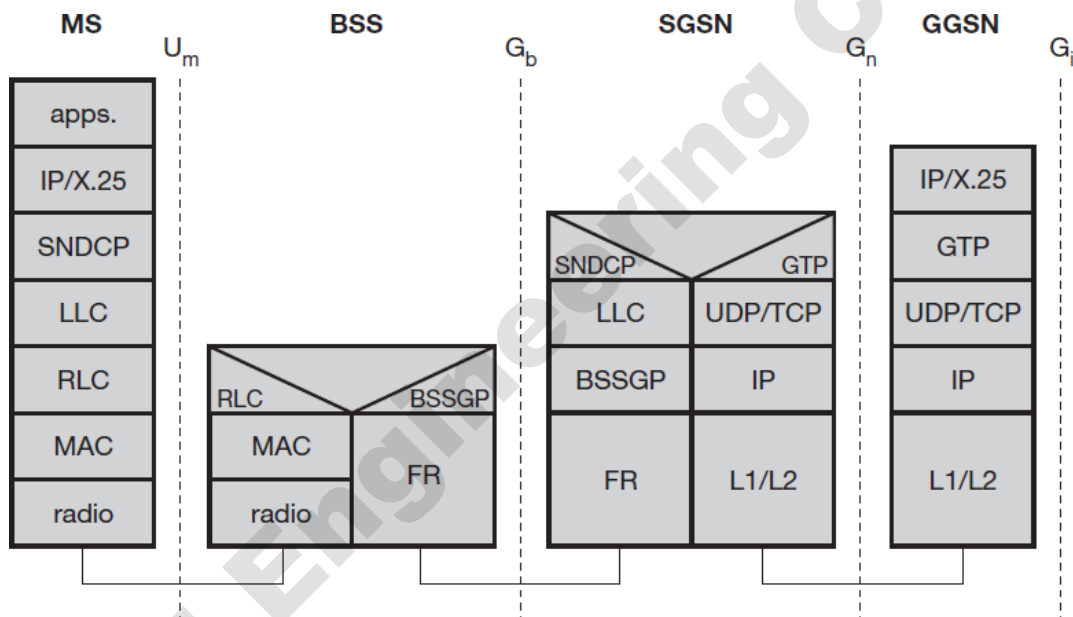
- In above figure packet data is transmitted from a PDN, via the GGSN and SGSN directly to the BSS and finally to the MS.

Mobility management

- Before sending any data over the GPRS network, an MS must attach to it
- Attachment Procedures
 1. Assigns a temporal identifier, called a temporary logical link identity (TLLI)
 2. Assigns a ciphering key sequence number (CKSN) for data encryption.
 3. For each MS, GPRS context
- Set up and stored in the MS and in SGSN
- Comprises
 - MS status
 - Ready
- Every movement of the MS is indicated to the SGSN
 - idle

- all context is deleted
 - standby
- only movement across routing areas is updated
 - CKSN
 - Flag indicating if compression is used
 - Routing data

PROTOCOL ARCHITECTURE



- All data is transferred using the GPRS tunneling protocol (GTP)
- GTP can use two different transport protocols
 - Reliable TCP
 - Non-reliable UDP
- Sub-network dependent convergence protocol (SNDCP)
 - Used between an SGSN and the MS
 - Adapt to the different characteristics of the underlying networks

-
- On top of SNDCP and GTP,
 - User packet data is tunneled from the MS to the GGSN and vice versa.
 - LLC is used for high reliability of packet transfer between SGSN and MS
 - Base station subsystem GPRS protocol (BSSGP)
 - Used to convey routing and QoS-related information between the BSS and SGSN
 - Radio Link Protocol (RLC)
 - Provides a reliable link
 - Used to transfer data over the U_m interface

End –to –End data transfer

Steps:

- TCP on top of IP tunnels the IP packets to the GGSN
- GGSN forwards them into the PDN
- PDNs forward their packets for a GPRS user to the GGSN
- GGSN asks the current SGSN for tunnel parameters, and forwards the packets via SGSN to the MS
- MSs are assigned private IP addresses which are then translated into global addresses at the GGSN

Advantage:

- Protects MSs from attacks

Disadvantage:

- Private addresses are not routed

GPRS APPLICATION

- Communications
 - E-mail
 - Fax
 - Unified messaging and intranet/internet access, etc.
- Value-added services
 - Information services and games, etc.
- E-commerce
 - Retail
 - Ticket purchasing
 - Banking and financial trading, etc.
- Location-based applications
 - Navigation
 - Traffic conditions
 - Airline/rail schedules and location finder, etc.
- Vertical applications
 - Freight delivery
 - Fleet management
 - Sales-force automation.
- Advertising
 - Advertising may be location sensitive
 - Example
 - A user entering a mall can receive advertisements specific to the stores in that mall.

GPRS ADVANTAGES

- Allow broadcast, multicast and unicast services
- Cheaper packet transfer for internet applications
- Needs no connection setup prior to data transfer

GPRS Disadvantages

- Needs additional hardware and software

Universal Mobile Telecommunication System (UMTS)

- European proposal for IMT-2000 prepared by ETSI
- Third generation cellular system
- EDGE
 - EDGE - Enhanced data rates for global (or: GSM) evolution
 - Initial enhancement of GSM toward UMTS
 - Uses enhanced modulation schemes
 - Introduced incrementally offering some channels with EDGE enhancement that can switch between EDGE and GSM/GPRS
- CAMEL
 - CAMEL stands for Customized Application for Mobile Enhanced Logic
 - New additions to GSM Besides enhancing data rates
 - Introduce intelligent network support
 - System supports for the creation of a **virtual home environment (VHE)** for visiting subscribers
 - GSMoU (1998) provides many proposals covering
 - QoS aspects
 - Roaming
 - Services

-
- Billing
 - Accounting
 - Radio aspects
 - Core networks
 - Access networks
 - Terminal requirements
 - Security
 - Application domains
 - Operation and maintenance
 - Migration aspects
 - GMM
 - UMTS fits into a bigger framework developed in the mid-nineties by ETSI, called global multimedia mobility (GMM)
 - ETSI developed basic requirements for UMTS and for UTRA, the radio interface
 - GMM provides an architecture to integrate
 - Mobile and fixed terminals
 - Different access networks
 - GSM BSS
 - DECT
 - ISDN
 - UMTS
 - LAN
 - WAN
 - CATV

-
- MBS
 - Core transport networks
 - GSM NSS+IN
 - ISDN+IN
 - B-ISDN+TINA
 - TCP/IP
 - ETSI selected two for UMTS
 - For the paired band (using FDD as a duplex mechanism)
 - ETSI adopted the W-CDMA (Wideband CDMA) proposal
 - Used for public mobile network providers
 - For the unpaired band (using TDD as duplex mechanism)
 - TD-CDMA (Time Division CDMA) proposal is used
 - Used for local and indoor communication

Features

- High quality speech
- High speed packet access
- Hand over to GSM/GPRS
- Multimedia messaging service
- Multimedia telephony for IMS
- IP-based multimedia core network subsystem
- Operation in other frequency bands
- Multimedia broadcast multicast service
- Wireless LAN inter-working
- Network selection

Functionalities

- Transfer of user data
- Radio channel ciphering and deciphering
- Services related to broadcast and multicast services
- CBS status reporting
- Data volume reporting
- Admission control
- Congestion control
- System information broadcasting
- Paging support
- Positioning

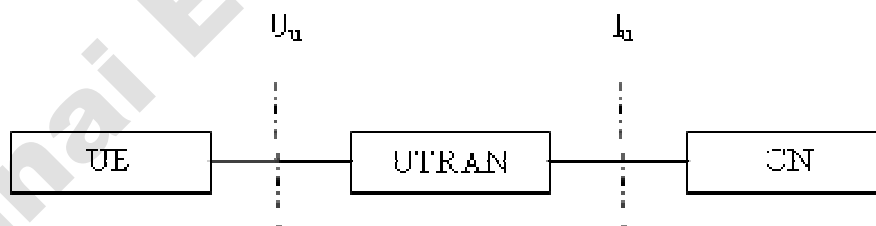
Advantages

- Gives significantly enhanced capacities to operators

Dissimilarities from 2G mobile system

- Higher speech quality
- Higher data rates
- Virtual home environments

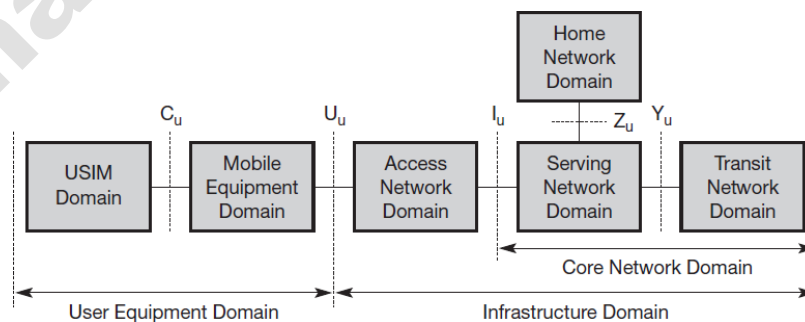
UMTS System Architecture



Components

- User Equipment (UE)
 - Terminal device used by the end users (cell phone).
- UTRA network (UTRAN)
 - Handles cell level mobility
 - Comprises several radio network subsystems (RNS)
 - RNS functions
 - Radio channel ciphering
 - Deciphering
 - Handover control
 - Radio resource management
 - Connected to UE through U_u interface
 - Equivalent to BSS in GSM
- Core Network(CN)
 - Connected to UTRAN through I_u interface
 - Equivalent to NSS in GSM
 - CN functions
 - Inter-system handover
 - Gateways to other networks
 - Performs location management

Domains and Interfaces



-
- User equipment domain
 - USIM Domain
 - Contains the SIM for UMTS
 - Contains a microprocessor for enhanced program execution
 - Performs functions for
 - encryption
 - authentication of users
 - stores all the user-related data
 - Mobile Equipment Domain
 - End device
 - Contains functions for
 - Radio transmission
 - User interfaces
 - Infrastructure domain
 - Access Network Domain
 - Contains the radio access networks (RAN)
 - Core Network Domain
 - Serving Network Domain
 - Comprises all functions currently used by a user for accessing UMTS services
 - Home Network Domain
 - Functions related to the home network of a user
 - Transit Network Domain
 - May be necessary if the serving network cannot directly contact the home network

UMTS HANDOVER

Handover means transfer of user connection from one radio channel to other.

Types of handover

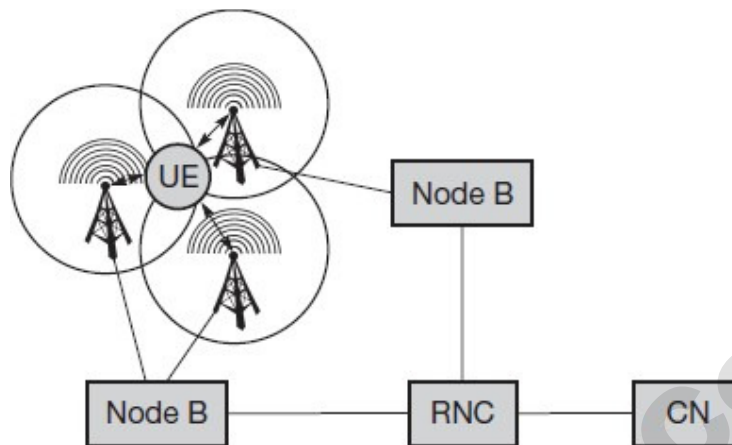
- **Hard Handover**
 - Hard handover means that all the old radio links in the UE are removed before the new radio links are established.
 - Hard handover can be seamless or non-seamless.
 - Seamless hard handover means that the handover is not perceptible to the user.
 - A handover that requires a change of the carrier frequency (inter-frequency handover) is always performed as hard handover.

Soft Handover

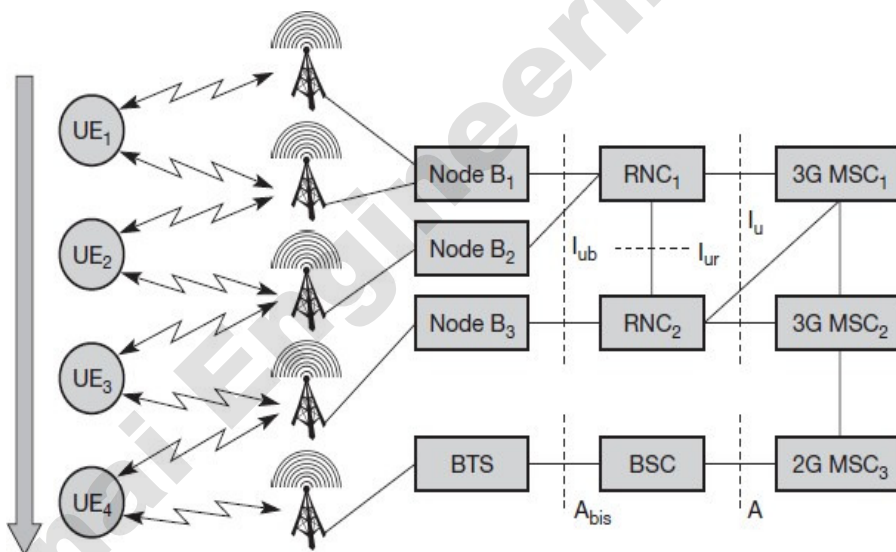
- Soft handover means that the radio links are added and removed in a way that the UE always keeps at least one radio link to the UTRAN.
- Soft handover is performed by means of macro diversity, which refers to the condition that several radio links are active at the same time.
- Soft handover can be used when cells operated on the same frequency are changed.

Softer handover

- Softer handover is a special case of soft handover where the radio links that are added and removed belong to the same Node B (i.e. the site of co-located base stations from which several sector-cells are served).
- Macro diversity with maximum ratio combining can be performed in the Node B, whereas generally in soft handover on the downlink, macro diversity with selection combining is applied.



Macro- diversity supporting soft handovers



Common types of handovers

- **Intra-node B, intra-RNC**
 - UE1 moves from one antenna of node B1 to another antenna
 - Type of handover is called **softer handover**
 - In this case node B1 performs combining and splitting of the data streams

-
- **Inter-node B, intra-RNC**
 - UE2 moves from node B1 to node B2
 - In this case RNC1 supports the soft handover by combining and splitting data
 - **Inter-RNC**
 - When UE3 moves from node B2 to node B3 two different types of handover can take place
 - The **internal inter-RNC** handover is not visible for the CN
 - RNC1 can act as SRNC, RNC2 will be the DRNC
 - CN will communicate via the same interface IU all the time
 - As soon as a relocation of the interface IU takes place (relocation of the controlling RNC), the handover is called an **external inter-RNC** handover.
 - Communication is still handled by the same MSC1, but the external handover is now a hard handover
 - **Inter-MS**
 - It could be also the case that MSC2 takes over and performs a hard handover of the connection.
 - **Inter-system**
 - UE4 moves from a 3G UMTS network into a 2G GSM network.

This hard handover is important for real life usability of the system due to the limited 3G coverage in the beginning.

UMTS SECURITY The

UMTS Standard

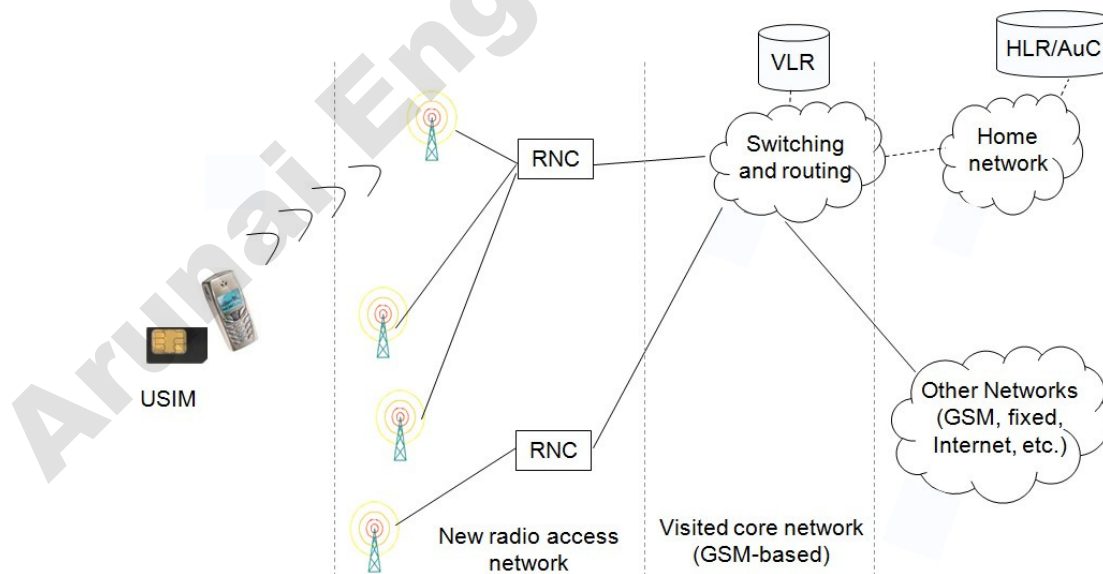
- Third generation (3G) mobile phones are characterised by higher rates of data transmission and a richer range of services
- Universal Mobile Telecommunications System (UMTS) is one of the new 3G systems
- The UMTS standards work started in ETSI but was transferred to a partnership of regional standards bodies known as 3GPP in 1998

- the GSM standards were also moved to 3GPP at a later date
- UMTS introduces a new radio technology into the access network
 - Wideband Code Division Multiple Access (W-CDMA)
- An important characteristic of UMTS is that the new radio access network is connected to an evolution of the GSM core network

Principles of UMTS Security

- Build on the security of GSM
 - adopt the security features from GSM that have proved to be needed and that are robust
 - try to ensure compatibility with GSM to ease inter-working and handover
- Correct the problems with GSM by addressing security weaknesses
- Add new security features
 - to secure new services offered by UMTS
 - to address changes in network architecture

UMTS Network Architecture



GSM Security Features to Retain and Enhance in UMTS

- Authentication of the user to the network
- Encryption of user traffic and signalling data over the radio link
 - new algorithm – open design and publication
 - encryption terminates at the radio network controller (RNC)
 - further back in network compared with GSM
 - longer key length (128-bit)
- User identity confidentiality over the radio access link
 - same mechanism as GSM

New Security Features for UMTS

- Mutual authentication and key agreement
 - extension of user authentication mechanism
 - provides enhanced protection against false base station attacks by allowing the mobile to authenticate the network
- Integrity protection of critical signalling between mobile and radio network controller
 - provides enhanced protection against false base station attacks by allowing the mobile to check the authenticity of certain signalling messages
 - extends the influence of user authentication when encryption is not applied by allowing the network to check the authenticity of certain signalling messages.

UMTS Authentication: Protocol Objectives

- Provides authentication of user (USIM) to network and network to user
- Establishes a cipher key and integrity key
- Assures user that cipher/integrity keys were not used before
- Inter-system roaming and handover
 - compatible with GSM: similar protocol

- compatible with other 3G systems due to the fact that the other main 3G standards body (3GPP2) has adopted the same authentication protocol

UMTS Mutual Authentication Algorithm

- Located in the customer's USIM and in the home network's AuC
- Standardisation not required and each operator can choose their own
- An example algorithm, called MILENAGE, has been made available
 - open design and evaluation by ETSI's algorithm design group, SAGE
 - open publication of specifications and evaluation reports
 - based on Rijndael which was later selected as the AES

UMTS Encryption Principles

- Data on the radio path is encrypted between the Mobile Equipment (ME) and the Radio Network Controller (RNC)
 - protects user traffic and sensitive signalling data against eavesdropping
 - extends the influence of authentication to the entire duration of the call
- Uses the 128-bit encryption key (CK) derived during authentication

UMTS Encryption Mechanism

- Encryption applied at MAC or RLC layer of the UMTS radio protocol stack depending on the transmission mode
 - MAC = Medium Access Control
 - RLC = Radio Link Control
- Stream cipher used, UMTS Encryption Algorithm (UEA)
- UEA generates the keystream as a function of the cipher key, the bearer identity, the direction of the transmission and the 'frame number' - so the cipher is re-synchronised to every MAC/RLC frame
- The frame number is very large so keystream repeat is not an issue

UMTS Encryption Algorithm

- One standardised algorithm: UEA1
 - located in the customer's phone (not the USIM) and in every radio network controller
 - standardised so that mobiles and radio network controllers can interoperate globally
 - based on a mode of operation of a block cipher called KASUMI

UMTS Integrity Protection Principles

- Protection of some radio interface signalling
- protects against unauthorised modification, insertion and replay of messages
- applies to security mode establishment and other critical signalling procedures
- Helps extend the influence of authentication when encryption is not applied
- Uses the 128-bit integrity key (IK) derived during authentication
- Integrity applied at the Radio Resource Control (RRC) layer of the UMTS radio protocol stack
- signalling traffic only

UMTS Integrity Protection Algorithm

- One standardised algorithm: UIA1
 - located in the customer's phone (not the USIM) and in every radio network controller
 - standardised so that mobiles and radio network controllers can interoperate globally
 - based on a mode of operation of a block cipher called KASUMI

UMTS Encryption and Integrity Algorithms

- Two modes of operation of KASUMI
 - stream cipher for encryption
 - Message Authentication Code (MAC) algorithm for integrity protection
- Open design and evaluation by ETSI SAGE

Arunai Engineering College