SRI MANAKULA VINAYAGAR ENGINEERING COLLEGE
(An Autonomous Institution)
Puducherry - 605 107

DEPARTMENT OF INFORMATION TECHNOLOGY

U20ITCM02 – MOBILE COMPUTING

YEAR: III SEMESTER : V

REGULATION:2020

VISION, MISSION AND PROGRAM EDUCATIONAL OBJECTIVES

VISION OF THE INSTITUTION

To be globally recognized for excellence in quality education, innovation and research for the transformation of lives to serve the society.

MISSION OF THE INSTITUTION

M1: Quality Education: To provide comprehensive academic system that amalgamates the cutting edge technologies with best practices.

M2: Research and Innovation: To foster value-based research and innovation in collaboration with industries and institutions globally for creating intellectuals with new avenues.

M3: Employability and Entrepreneurship: To inculcate the employability and entrepreneurial skills through value and skill based training.

M4: Ethical Values: To instil deep sense of human values by blending societal righteousness with academic professionalism for the growth of society.

VISION OF THE DEPARTMENT

To be a pioneer in the field of Information Technology by achieving academic excellence, involving in research & development and promoting technical & professional expertise.

MISSION OF THE DEPARTMENT

Expertise: To impart quality education and create excellent engineers with strong analytical, Programming and Problem solving skills to meet the ever changing demands of IT industry

Eminence: To kindle creative thinking, innovation and foster value-based research in the field of information technology

Complaisant: To enrich the employability skills, inculcate entrepreneurial ideology and promote professional expertise

Exemplar: To instil moral values, ethical responsibilities and empowering graduates to be socially responsible and technically competent

PROGRAM EDUCATIONAL OBJECTIVES

PEO1 Fortify: To prepare the students with fundamental knowledge in programming languages and in developing applications

PEO2 Equip: To develop skill in understanding the complexity in networking, security, data mining, web technology and mobile communication so as to develop innovative applications and projects in these areas for the betterment of society, as well as to enable them to pursue higher education

PEO3 Endow: To enable the students as full-fledged professionals by providing opportunities to enhance their analytical, communication skills and problem solving skills along with organizing abilities

PEO4 Conventional: To familiarize the students with the ethical issues in engineering profession, issues related to the worldwide economy, nurturing of current job related skills and emerging technologies

U20ITCM02	MOBILE COMPUTING (Common to IT and CSE)	L	T	P	C	Hrs
		3	0	0	3	45

Course Objectives

- To understand the basic concepts of mobile computing
- To be familiar with the network protocol stack
- To learn the basics of mobile telecommunication system
- To be exposed to Ad-Hoc networks
- To gain knowledge about different mobile platforms and application development

Course Outcomes

After completion of the course, the students will be able to

CO1 - Explain the basics of mobile telecommunication system **(K2)**
CO2 - Articulate the required functionality at each layer for given application **(K2)**
CO3 - Identify solution for all functionality at each layer. **(K1)**
CO4 - Use simulator tools and design Ad hoc networks **(K3)**
CO5 - Develop a mobile application **(K6)**

UNIT I INTRODUCTION **(9 Hrs)**

Mobile Computing - Mobile Computing Vs Wireless Networking - Mobile Computing Applications - Characteristics of Mobile computing - Structure of Mobile Computing Application. MAC Protocols - Wireless MAC Issues - Fixed Assignment Schemes - Random Assignment Schemes - Reservation Based Schemes.

UNIT II MOBILE INTERNET PROTOCOL AND TRANSPORT LAYER **(9 Hrs)**

Overview of Mobile IP - Features of Mobile IP - Key Mechanism in Mobile IP - route Optimization. Mobile TCP- WAP - Architecture - WDP - WTLS - WTP -WSP - WAE - WTA Architecture - WML

UNIT III MOBILE TELECOMMUNICATION SYSTEM **(9 Hrs)**

Global System for Mobile Communication (GSM) - Services & Architecture- Protocol-Connection Establishment - General Packet Radio Service (GPRS) - Universal Mobile Telecommunication System (UMTS) - Handover - Security.

UNIT IV MOBILE AD-HOC NETWORKS **(9 Hrs)**

Ad-Hoc Basic Concepts - Characteristics - Applications - Design Issues - Routing Popular Routing Protocols - Vehicular Ad Hoc networks (VANET) - MANET Vs VANET - Security.

UNIT V MOBILE PLATFORMS AND APPLICATIONS **(9 Hrs)**

Mobile Device Operating Systems - Special Constrains & Requirements - Commercial Mobile Operating Systems - Software Development Kit: iOS, Android, BlackBerry, Windows Phone - M- Commerce - Structure - Pros & Cons - Mobile Payment System - Security Issues.

Text Books

1. Prasant Kumar Pattnaik, Rajib Mall, “Fundamentals of Mobile Computing”, PHI Learning Pvt. Ltd, New Delhi - 2012.
2. Jochen H. Schller, “Mobile Communications”, Second Edition, Pearson Education, New Delhi, 2007
3. C.K.Toh, “AdHoc Mobile Wireless Networks”, First Edition, Pearson Education, 2002.

Reference Books

1. Dharma Prakash Agarval, Qing and An Zeng, “Introduction to Wireless and Mobile systems”, Thomson Asia Pvt Ltd, 2005.
2. William.C.Y.Lee,“Mobile Cellular Telecommunications-Analog and Digital Systems”, Second Edition,TataMcGraw Hill Edition ,2006.
3. UweHansmann, LotharMerk, Martin S. Nicklons and Thomas Stober, “Principles of Mobile Computing”, Springer, 2003.

Web References

1. Developers : http://developer.android.com/index.html
2. Apple Developer : https://developer.apple.com/
3. Windows Phone DevCenter: http://developer.windowsphone.com 9. BlackBerry Developer : http://developer.blackberry.com/

COs/POs/PSOs Mapping

COs	Program Outcomes (POs)												Program Specific Outcomes (PSOs)		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
1	2	1	-	-	2	2	3	2	2	2	2	2	2	3	2
2	2	1	-	-	2	2	3	2	2	2	2	2	2	3	2
3	2	1	-	-	2	2	3	2	2	2	2	2	2	3	2
4	3	2	1	1	3	3	3	3	3	3	3	3	3	3	3
5	3	2	1	1	3	3	3	3	3	3	3	3	3	3	3

Correlation Level: 1-Low, 2-Medium, 3- High

Unit I

Introduction

Syllabus

Mobile Computing - Mobile Computing Vs wireless Networking - Mobile Computing Applications - Characteristics of Mobile computing - Structure of Mobile Computing Application. MAC Protocols - Wireless MAC Issues - Fixed Assignment Schemes - Random Assignment Schemes - Reservation Based Schemes.

Contents

1.1 Mobile Computing

AU : June-16, Dec.-17

It is the computation made over physical mobility. Mobile computing system permits the user to perform a task from a distant place from the device. The mobile computing is also known by different names according to its role in that context few examples are listed below.

1) **Virtual home environment**

   It is denoted as " VHE". It is possible under VHE to operate a device like heater in a person's home though he is away from his place. He has a virtually available feeling at his home.

2) **Nomadic computing**

   The entire mobile computing environment is nomadic in nature and it moves with the roaming user. It is possible for both remote and local services.

3) **Wearable computer**

   The wearable computers are used like wearable accessories like shoes, clothes etc. by human beings. A person can wear it provided these computers have extra attributes than conventional mobile computers. Actually the wearable computers are those which can be adorned by a person like an accessory hat, shoe etc.

1.2 Evolution of Mobile Communication

AU : Dec.-16

The wireless communication has developed worldwide from the year 1897 by means of radio and the development of the technology is due to revolution in the fields like

i) RF circuit fabrication

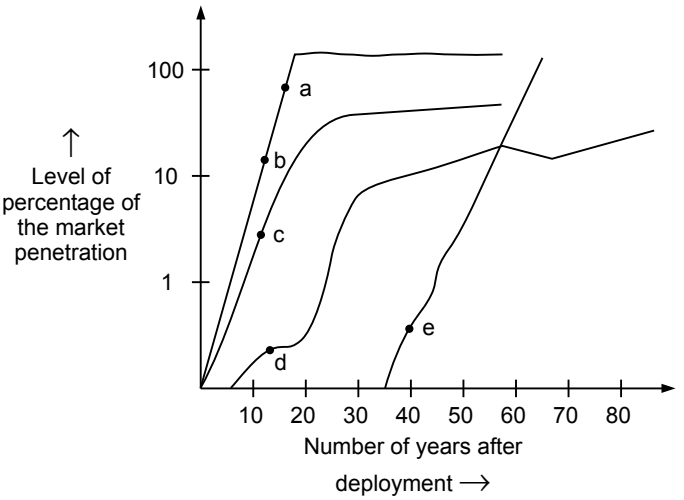
ii) Large scale circuit integration

iii) Digital circuit design

iv) Miniaturization technologies.

The impact of development of mobile communication is personal communication services. The cellular concepts emerged appreciably and slowly developed by Bell Laboratories in the period between 1960 and 1970. An exponential growth of wireless communication was observed. While comparing wireless technologies with other communications the penetration of wireless application is more in our day-to-day life. The cellular as well as personal communication services have revolutionized the communication field.

The drastic growth of mobile communication is compared here with other technologies in a graph.



a - Video cassette recorder - 1979 Year of introduction
b - Television - 1946
c - Automobile - 1900
d - Telephone - 1877
e - Mobile telephones - 1946

Fig. 1.2.1

The cellular mobile communication technology emerged slowly and developed worldwide. At the same time it has penetrated into the market for long time with high demand than other technologies. It has an appreciable growth rate as seen in the graph.

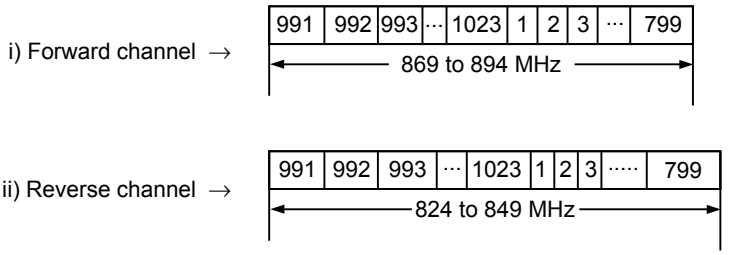
In the year 1934 the police radio systems used the Amplitude Modulation (AM) systems for transmission purposes. In early cellular the major problem faced was vehicular ignition noise. It is also interesting that in 1960's the majority of mobile users were not linked through PSTN and they were not capable to dial the telephone numbers directly. In the year 1995 the number of mobile users in US was 37 % of the total population. The growth of cellular mobile users was approximately from 25000 to 25 million and this took roughly one decade. (From 1984 to 1993).

The number of consumers in wireless communications increases every year worldwide.

In early days the FM push-to-talk telephone systems were popular. In the period of 1940 this system used frequency of 120 kHz, such that only one person can talk at a time. It was known as half duplex mode. But the FCC increased the number of channels in each market and at the same time it does not need an extra spectrum allocation. It was possible with new technologies enabling reducation in bandwidth from 120 kHz to 60 kHz. Later automatic channel trunking was also possible and it was named as Improved Mobile Telephone Service (IMTS). With this IMTS full duplex mode was brought in. In the year 1968 AT and T Bell Laboratories recommended the concepts of the cellular mobile communication to the respective FCC and in the year 1983 FCC

assigned 666 duplex channels for the US mobile systems named as Advanced Mobile Phone System (AMPS). It is also worth noting that FCC insisted to have 'duopoly' in each city. That is in each city/market only two service providers were allowed to have a healthy competition in the market. An additional 166 channels of 10 MHz frequency were permitted in US cellular system to meet the demand scenario.

US cellular radio service :



Some of the main problems the cellular mobile system faced are

i) Interference

ii) Less encryption techniques

iii) Spectrum inefficiency.

In the year 1991 the US Digital Cellular (USDC) system was implemented and this USDC Standard or Electronic Industry Association Interim Standard IS-54 enabled the main advantage of replacing few single user analog channels with that of the digital channels.

Comparing AMPS with USDC system the digital USDC provided more capacity to the cellular mobile world. It was due to the reasons, the USDC applied the techniques mentioned below.

i) $\frac{\pi}{4}$ differential quadrature phase shift keying.

ii) Speech coding.

iii) Time division multiple access.

Later a better cellular mobile system using Code Division Multiple Access (CDMA) was developed by the Qualcomm, Inc which was then standardized by the respective Telecommunications Industry Association (TIA) and the system was named as Interim Standard (IS-95).

The IS-95 allowed many number of mobile users by Direct Sequence Spread Spectrum (DSSS) technique. The CDMA cellular phone systems were independent of interference problems and provided better call quality than the first generation (1G) AMPS cellular system.

Some of the mobile standards of North America, Japan and Europe are listed below.

	Mobile standard	Year of introduction	Multiple access / Modulation	Bandwidth of channel
1) North America	a) AMPS (Cellular)	1983	FDMA / FM	30 kHz
	b) USDC (Cellular)	1991	TDMA / $\frac{\pi}{4}$ DQPSK	30 kHz
	c) CDPD (Cellular)	1993	(FH/Packet) / GMSK	30 kHz
	d) IS-95 (Cellular/PCS)	1993	CDMA (QPSK/BPSK)	1.25 MHz
2) Japan	a) JTACS (Cellular)	1988	FDMA / FM	25 kHz
	b) PDC (Cellular)	1993	TDMA / $\frac{\pi}{4}$ – DQPSK	25 kHz
	c) NTT (Cellular)	1979	FDMA/FM	25 kHz
	d) PHS (Cordless)	1993	TDMA / $\frac{\pi}{4}$ – DQPSK	300 kHz
3) Europe	a) ETACS (Cellular)	1985	FDMA / FM	25 kHz
	b) GSM (Celluar/PCS)	1990	TDMA / GMSK	200 kHz
	c) CT2 (Cordless)	1989	FDMA / GFSK	100 kHz
	d) DECT (Cordless)	1993	TDMA / GFSK	1.728 MHz

AMPS - Analog Mobile Phone System.

USDC - US Digital Cellular.

CDPD - Cellular Digital Packet Data.

IS-95 - Interim Standard-95.

JTACS - Japanese Total Access Cellular Systems.

PDC - Pacific Digital Cellular.

NTT - Nippon Telephone and Telegraph Company.

PHS - Personal Handy Phone System.

ETACS - European Total Access Cellular System.

GSM - Global System for Mobile.

CT2 - Cordless Telephone. (CT2)

DECT - Digital European Cordless Telephone.

In the examples of cellular, cordless and PCS systems each one of them has unique advantages and facilities with respect to mobile comunication technology. Thus the transition from analog mobile phones to digital mobile phones was made along a number of years and today digital cellular telephony is very popular worldwide due to its several technical advantages, including cellular coverage capability.

1.2.1 Examples of the Cellular Radio Communication

1. Cellular telephone system.
2. Cordless Telephone (CT) system.
3. Paging system.

These examples are given below.

Example 1 : Cellular telephone system

The cellular telephone system mainly helps to connect a Public Switched Telephone Network (PSTN) and any distant/near user provided the user is available within the corresponding radio range. (A basic cellular system is given below.) The mobile switching center or Mobile Telephone Switching Office (MTSO) connects the mobile units (called parties) to the PSTN. Every cell of the particular geographical area has its own base station with a transceiver, an antena, and also a control circuitry.

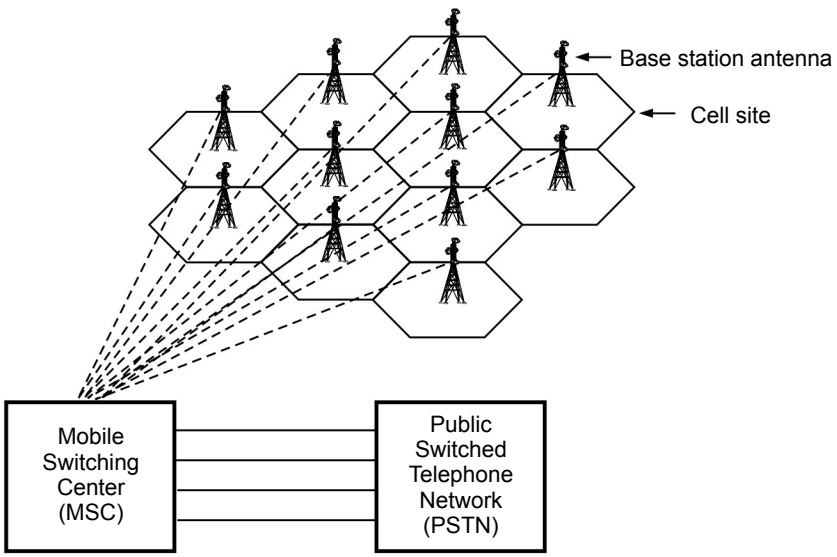


Fig. 1.2.2 Cellular system

The base stations are capable of handling many full duplex cellular communications. The mobile switching center can handle atleast 5000 telephonic conversation at a time and 1,00,000 cellular users/subscribers in a network. The cellular communication is made possible between mobile units and the base stations with the help of Common Air Interface (CAI) which specifies four channels.

They are :

1. Forward Control Channels (FCC)
2. Reverse Control Channels (RCC)
3. Forward Voice Channels (FVC) and
4. Reverse Voice Channels (RVC).

The control channels mentioned here are also termed as setup channels. They will have calls that are in progress but they usually send and receive data messages carrying call initiation and requests for services.

The Forward Control Channels (FCC) are also termed as "BEACONS" since they continuously broadcast the traffic requests for the mobile units within the cellular system. As soon as the cell phone is switched on it scans the control channels searching for the strongest signal of a base station. When the call progresses the mobile switching center adjusts the power transmitted (P_T) of the mobile unit and alters the channel of the mobile unit and also the base station so as to maintain the call quality eventhough the mobile unit is non-stationary.

The call in progress continues irrespective of the frequency changes from one base to another base station. Such a call continued process without termination is called as 'Hand off' technique. As the mobile moves and the signal strength reduces when it is away from its base station of cell, the next base station of the neighbouring cell where the mobile enters in will take charge of the call. A relay like process thus takes place within several base stations of the entire cellular system simply to sustain the call developed between two subscribers.

Whenever a mobile originates a call, a request signal will be sent through reverse control channel. By seeing this request the mobile unit will transmit its Mobile Identification Number (MIN), telephone number of its called subscriber, and the Electronic Serial Number (ESN). Then the MSC will check the proper validity of the signals sent by the mobile and responds to its request by connecting the called subscriber through PSTN.

The mobile communication establishes call, maintains it, and terminates as the call is over. It enables communication eventhough the distance between subscriber is large.

Example 2 : Cordless Telephone (CT) system

The cordless telephone systems are full duplex systems and it is intended to link a portable handset to the dedicated base station which in turn is connected to a particular dedicated telephone line. For this specific telephone number on Public Switched Telephone Network (PSTN) is used.

The first generation (1G) cordless telephone systems came into existance in 1980's. But the distance the system covered was only few meters.

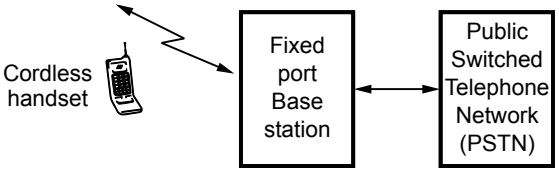


Fig. 1.2.3 Cordless Telephone (CT) system

Later the second generation (2G) cordless systems the distance was not a problem and the subscribers used cordless systems in mobile environment also. The system was good only if the subscriber availability was within the coverage of base station.

The cordless system also work together with paging system such that the roaming subscriber can first be paged and he or she can respond to it with the help of cordless telephone. In the simple cordless system shown above it illustrates that the cordless handset is linked to PSTN through the base station (fixed port). The cordless handset has a wireless link with its dedicated base station. The cordless systems are divided into two namely Analog CT and Digital CT.

In the early days these cordless systems were analog (Analog CT). They provided analog voice transmissions and enabled mobility within a limited distances. But they had many demerits such as

i) Poor call qualities

ii) Interference

These problems urged the need for digital cordless (Digital CT) systems. They provided better voice quality similar to wired telephone system.

Example for digital cordless system is

CT2 / Common Air Interface (CAI)

Some of the main criteria of CT2 system are

i) Voice signal is digitized through 32 kb/sec Adaptive Differential Pulse Code Modulation (ADPCM) technique.

ii) Bit stream compression facility.

iii) Final bit stream transmission at a rate of 72 kb/sec through Gaussian Frequency Shift Keying (GFSK).

iv) Immune to errors.

v) Supports data transmissions effectively upto 32 kb/sec.

vi) Traffic can be separated with the Time Division Duplex (TDD) access technique.

Note This CT2 standard does not provide for the mobility status and the later version CT2 + standard was used for this purpose.

Example 3 : Paging Systems

The paging systems are communication systems and they can transmit brief messages to subscribers. The message sent may be an alphanumeric message, numeric message or even a voice data. Paging systems also include news headlines, faxes and stock quotations. It may be sent to a particular paging subscriber through the paging system access number with a modem or a telephone keypad. Such a message is called as page.

In a technique called 'simulcasting' the wide paging systems sends a page from each base station simultaneously.

The important performance metrics used in decision-making process under hand off situations (mobility management) are listed below.

1. Probability of call blocking
2. Probability of call dropping.
3. Probability of call completion.
4. Handoff delay.
5. Rate of handoff.
6. Probability of an incomplete handoff.
7. Probability of handoff blocking.
8. Interruption time duration.
9. Handoff probability.

Strategies used to calculate the instant of handoff are :

1. Relative signal strength method.
2. Relative signal strength with hysteris method.
3. Relative signal strength with threshold method.
4. Prediction techniques.

In a wide area paging system a paging control center is available that connects the PSTN to different paging terminals.

Thus paging systems enable communication with subscribers irrespective of their roaming state. But the system requires large transmitter powers in the order of kilowatts and uses only low data rates for providing proper coverage.

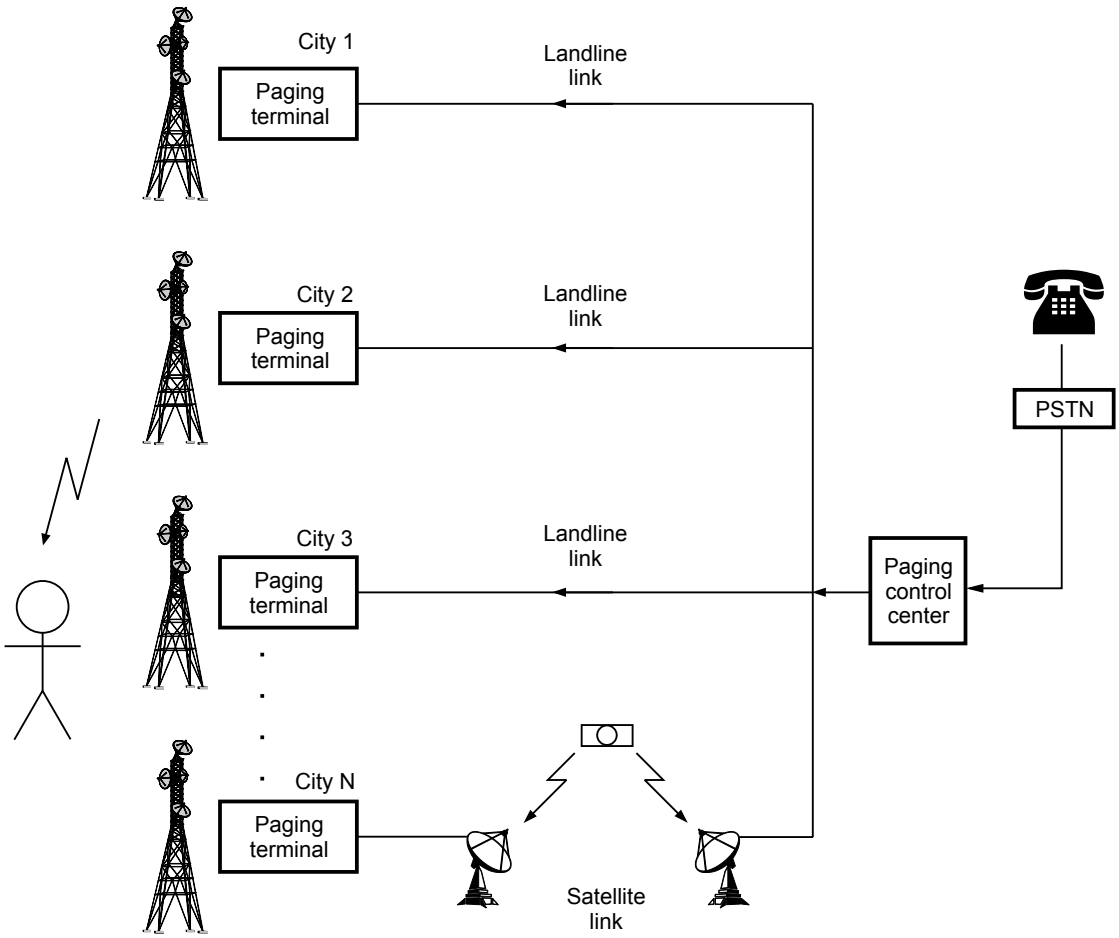


Fig. 1.2.4 Wide area paging system

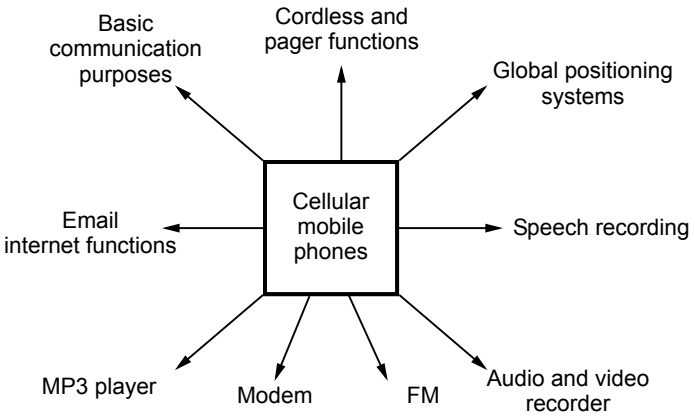


Fig. 1.2.5

There are several functionalities possible with cellular mobile phones as shown above which includes the pager functions too. It is helpful in sending short messages which are highly used by subscribers. The short message or page is sent to a subscriber wherever he is, and it is the main advantage of these system in spite of low data rates and large transmitter power requirements.

1.2.2 Cellular Mobile Communication

Important terminologies

1. **Cell :** It is smallest geographical area considered for cellular mobile communication.
2. **Base station (BS) :** Base station provides functionalities between mobile unit and Mobile Switching Center (MSC). The base station is located in each cell and it links the subscriber mobile unit with the MSC.
3. **Cell splitting :** In high cellular traffic regions, a larger cell is divided into smaller cells to have complete radio coverage.
4. **Handoff :** When mobile unit moves from one cell to another cell the call in progress will be handed over form one base transceiver to the base transceiver of the new cell where the mobile unit enters so that the call in progress is not disturbed and such a process is called as "Handoff".
5. **Cell sectoring :** A cell can be divided into many sectors. For example, from 3 sectors to 6 sectors in a hexagonal cell. The directional antenna should focus on each sector.
6. **Umbrella cell pattern :** A single large cell (Macro cell) consists of many small cells (Micro cells) and there will be interaction between the micro and macro cells.
7. **Control channel :** They are used for necessary exchange of information related to setting up and establishing cell base stations and the mobile units.
8. **Traffic channels :** They are used for carrying data or voice connections between different users.
9. **Frequency reuse :** It is a concept followed in cellular communication for efficient spectrum utilization. The same carrier frequency is reused by many cells in a cellular cluster and it is known as 'frequency reuse' scheme.
10. **Fading :** Fading is an effect in mobile radio propogation. It is common in multipath mobile signalling environment.
11. **Mobile Telecommunication Switching Office/Mobile Switching Center (MTSO/MSC) :** It is the main unit that connects the base transceiver station and the Public Switched Telephone Network (PSTN) in mobile communication.

11. Parameters for micro cells

Cell radius	$\rightarrow$ 0.1 - 1 km.
Delay spread (average value)	$\rightarrow$ 10 - 100 nsec.
Max bit rate	$\rightarrow$ 1 Mb/sec.
Transmission power (P_T)	$\rightarrow$ 0.1 - 1 watt.

12. Parameters for macro cells

Cell radius	$\rightarrow$ 1 - 20 km.
Delay spread (average value)	$\rightarrow$ 0.1 - 10 μsec.
Max bit rate	$\rightarrow$ 0.3 Mb/sec.
Transmission power (P_T)	$\rightarrow$ 1 - 10 watt.

13. Page

It is a brief message that is broadcast over an entire service area, generally in a simulcast type by many base stations at a time.

14. Forward channel

It is a radio channel used for transmission of information from base station to the mobile unit.

15. Reverse channel

It is a radio channel used for transmission of information from mobile unit to the base station.

16. Simplex systems

These are the communication systems that provide only one way communication.

17. Subscriber

A mobile phone user who pays subscription charges for using a cellular mobile communication system.

18. Mobile station

Mobile station is mainly intended for use while in movement at any location. It can be hand-held personal units that is portable or installed in moving vehicles.

19. Full duplex systems

The transmission and reception is typically on two different channels (FDD) even though new cordless systems are using TDD scheme. It is a communication system that allows two way communication simultaneously.

20. Half duplex systems

The communication systems that allow two way communication by using same radio channel for both transmission and reception. The user can transmit or receive at any time.

21. Transceiver

It is a device used for both transmitting and receiving radio signals.

22. Roamer

It is a mobile station that operates in a service area other that the subscribed service area.

23. PSTN

It is the public switched telephone network to which the Mobile Telephone Switching Center (MTSO) is connected.

1.2.3 Trends in Cellular Radio and Personal Communications

With the help of digital signal processing, RF technology, network intelligence the personal wireless systems have developed worldwide and provide many number of services to subscribers in their unique way. The Personal Communication Services (PCS) initiated in the United Kingdom and the frequency spectrum allotted was in the range 1800 MHz. It focussed on developing Personal Communication Networking (PCN).

The advantage of PCN is that the subscriber can receive or make a call irrespective of the roaming status. The Personal Communication Systems (PCS) includes several network features and provides more personalization, than the available cellular systems.

Then the indoor wireless networking got all the importance due to the better network connectivity within the building premises. One such standard is HIPERLAN compatible with indoor wireless standard and it was developed by European Telecommunications Standard Institute (ETSI).

An important worldwide standard known as Future Public Land Mobile Telephone System (FPLMTS) or International Mobile Telecommunication 2000 (IMT-2000) emerged in the year 1995 and it was developed by International Telecommunications Union (ITU). This IMT-2000 is a third generation (3G) standard and some of its advantages are

i) Global compatibility.

ii) Integrate paging, cordless and the cellular mobile system and LEO satellites as a single mobile system.

iii) Supports multi-function.

It is an excellent digital mobile radio system accepted worldwide. The satellite mobile systems incorporates good paging systems, data collection, global roaming and emergency communications. One such example is network of LEO satellites.

The fundamental technological developments has thus helped the wireless personal communication systems to grow rapidly and the demand it has is also high. The wireless networking will surely improve further to meet more requirements and additional features in wireless personal communication field.

Mobile Computing :

It is a real computation over physical mobility. It allows the user to execute a task/job even from a distant place. This mobile computing environment is also known by several names like,

- Virtual home environment.
- Nomadic computing etc.

1.3 Mobile Computing-Structural View

AU : June-16, Dec.-16,17, May-18

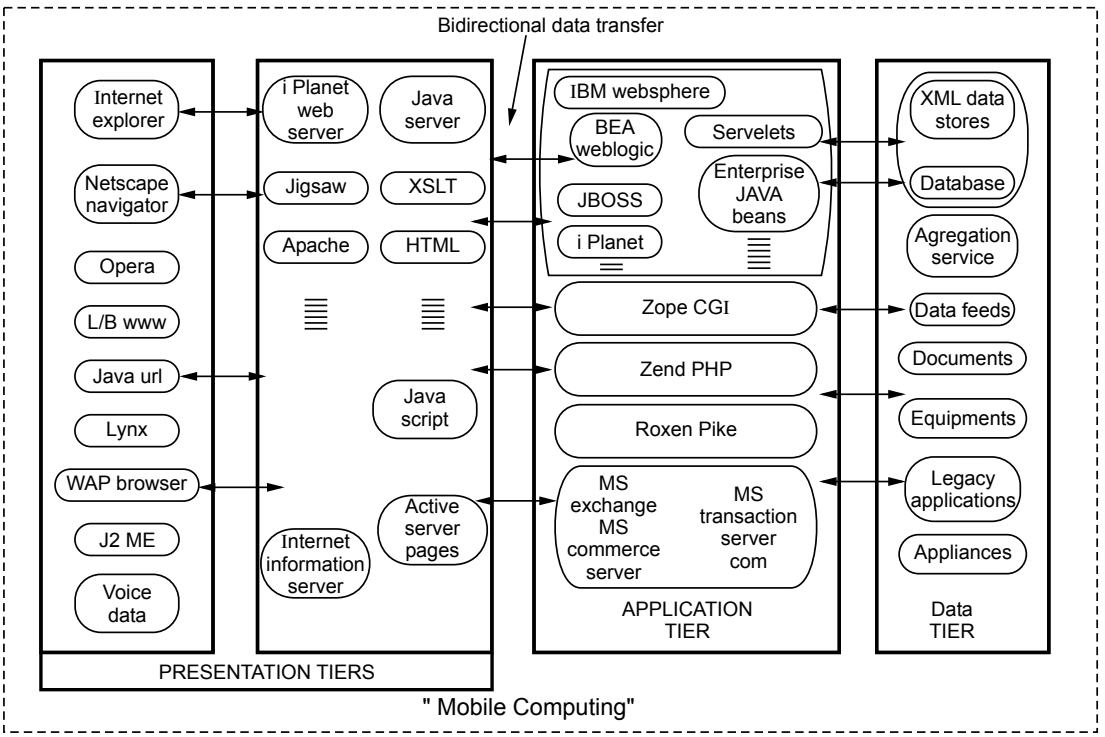
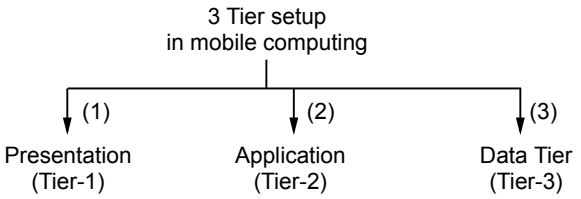


Fig. 1.3.1 Architecture of mobile computing

The three tier structure depicted is used mainly for mobile environment. They are presentation tier, data tier and application tier.



The presentation layer is concerned about user interaction. Its applications run on the client devices. This layer also includes web browsers, and the customized client programs.

The application tier is also known as middle tier which is like an "engine" to the automobile. It plays a vital role in wireless LAN applications. It performs the processing of user input, obtaining information and then making decisions. This layer includes technology like Java, "NET" services, cold fusion web logic, iplanet, 'Z end' etc. It is database independent.

The middleware also covers a wide range of software systems, mobile application support etc. The two independent open objects can be connected through this middleware as a software gateway.

There are many classifications available under middleware.

1.3.1 Architecture of Mobile Computing

The mobile computing architecture is given in figure shown above. They are simple and efficient. One example of this network is three-tier architecture as in the diagram. It mainly consists of user interface (tier-1), access network, middle tier (tier-2) are data tier (tier-3). (See Fig. 1.3.2 on next page).

1.3.2 The Detailed study of the Architectural Modules

The first layer is the user interface or a presentation tier.

a. Message-oriented middleware are (MOM).

b. Transaction processing middleware (TP).

c. Communication middleware (CM).

d. Database middleware (DM).

e. Distributed object and components (DOC).

f. Transcoding middleware (TM).

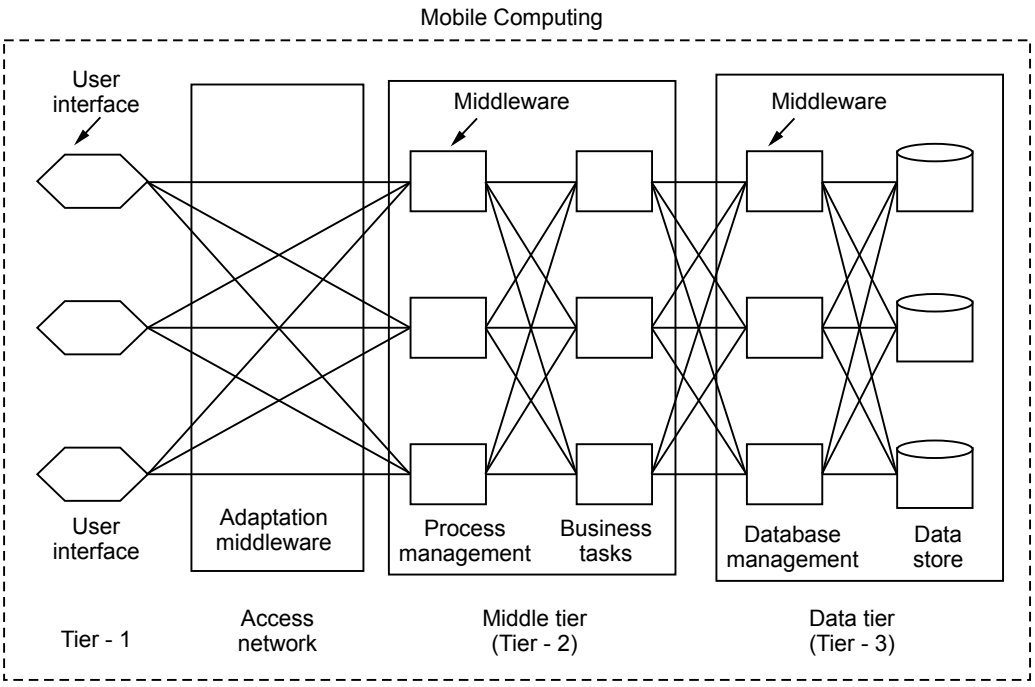


Fig. 1.3.2 An example for mobile computing - "Three tier architecture"

1.3.2.1 Message-Oriented Middleware (MOM)

The message oriented middleware is generally asynchronous, peer to peer which works in a subscribe method. One or many objects may subscribe to a particular event. When an event occurs it will be subscribed or published by asynchronous loosely coupled object. The MOM monitors the occurrence of events. The Request/Response scheme is more flexible with MOM method. Hence the message oriented middle is more appropriate for event driven applications. An example for MOM under Java is known as Java Message Service (JMS).

1.3.2.2 Transaction Processing Middleware (TP)

It is suited for developing transaction based distributed applications.

The number of client requests are properly mapped to different application tasks through application service routines. (See Fig. 1.3.3 on next page).

In an ideal TP system, the device for input and output can be different. The transaction processing is independent of database architecture. The TP middleware helps to reduce the resources by multiplexing technique, which in turn may reduce the response time.

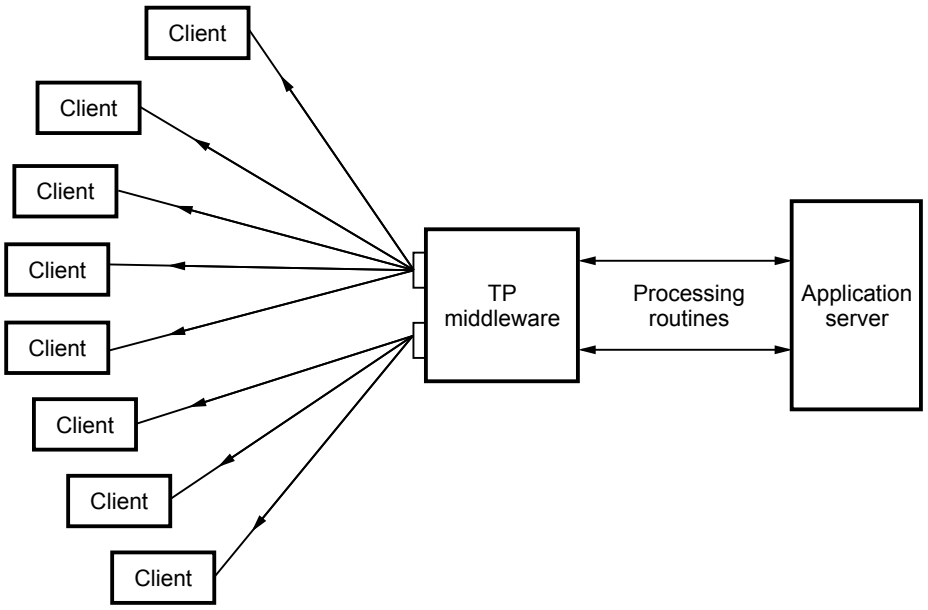


Fig. 1.3.3 Transaction processing (TP) middleware

1.3.2.3 Database Middleware (DM)

The database middleware is responsible for maintaining the entire data involved in communication. In data tier their are database management and data store facilities. User interface can interact with data tier through access network and middle tier.

1.3.2.4 Communication Middleware (CM)

It is used to connect one application to another application through communication middleware. In telecommunication field there are numerous elements in the core and the user interface is via the telnet. The communication between nodes are finally established.

1.3.2.5 Distributed Object and Components (DOC)

The Common Object Request Broker Architecture termed as CORBA is on of the best example for distributed objects and components. Many network programming tasks like framing, error handling etc. are simplified using CORBA. Many number of clients can be handled with high reliability and hit rates.

1.3.2.6 Transcoding Middleware (TM)

To attend the request or need of the user/client, the transcoding middleware is used to transform one format of data to another format. Actually content adaptation is done by transcoding to meet the requirement of each device.

The application tier or the so called middleware has to play role in mobile computing architecture. The reliability of the entire system is enhanced by the performance of middleware.

1.4 Functions of Mobile Computing

AU : June-16, Dec.-16

A computing environment is said to be mobile if it supports few of the characteristics mentioned below.

1. **User mobility :**

   Though the user roams from one place to another he should be able to use the same service. This service may be a remote network or home network.

2. **Bearer mobility :**

   In this case the user may move from one bearer to another bearer but use the same service.

3. **Host mobility :**

   In host mobility the user device can be either a server or a client. If it is a host mobility the mobility of that IP should be given more care. But if it is server or host mobility, some complexities will change.

4. **Service mobility :**

   Though the user changes from one service to another service it should remain enabled and if a user is sending a mail and he refers some information in his PC stored file for adding in his mail he should be allowed to do so.

1.5 Mobile Computing Vs Wireless Networking

AU : May-17,18, Dec.-16,17

- Mobile computing denotes collecting information and computational services in its mobile environment.
- But the wireless networking provides fundamental communication infrastructure.
- The mobile computing is based on the wireless networking environment and enables accessing data in mobile status.
- Wireless networking needs low investments and low setup time for setting up a network.
- Wireless local area network, Personal area network, Ad-hoc networks are some of the types of wireless networks.
- The wireless networks are of two types namely,

  i) Extension of the wired networks and ii) Ad-hoc networks.
- An Ad-hoc networks needs no infrastructure.
- It is based on the multi-hop wireless communications.
- On the other hand an example of wireless network is Wireless LAN (WLAN).

1.6 Characteristics of Mobile Computing

AU : June-16, Dec.-16, May-18

Adaptation :

In mobile computing environment adaptation refers to bandwidth management. It has to adjust with bandwidth fluctuations if any without the knowledge of the subscriber. There are several factors like handoff, noise etc. that influences the adaptation of computing environment.

Personalization :

In mobile computing scenerio the services can be personalized using the subscriber's profile. Hence they can avail their information with their handheld devices.

Ubiquity :

The word ubiquity in mobile computing is the ability of subscriber to compute informations from anywhere at anytime.

For example a sales representative can do his transactions from anywhere.

Location Awareness :

In mobile computing a handheld device equiped with Global Positioning System (GPS) can track the position of subscriber and inform it to the tracking station.

There are several applications that provide value added services by informing position-based services.

Some of the important applications are traffic control, emergency services where the computing environment dynamically monitor and the location informations to reduce congestion.

Broadcast :

In mobile computing environment data is efficiently transmitted to several subscribers simultaneously. For example a common advertising information is being sent to many users at a time.

1.7 Motivation for a Specialized MAC

AU : June-16, May-17, 18, Dec.-17

For the wireless domain their are many medium access control (MAC) algorithms are used. The MAC comprises mechanisms that can regulate user access to required medium using a multiple access scheme either TDM, FDM, CDM or SDM. The MAC resembles traffic regulations in the highway/multiplexing. MAC belongs to the layer 2, (OSI) the data link control layer (DLC). This layer 2 is subdivided into logical link control (LLC), and MAC.

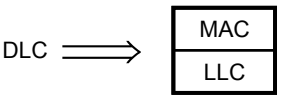


Fig. 1.7.1

MAC with CDM assign specific codes to allow the separation of various users in a code space. The MAC schemes can be elaborated from wired networks say, for example, the carrier sense multiple access with collision detection (CSMA/CD).

A sender can sense the medium wheather it is free or not. The sender will wait if the medium is busy. In case sender detects a collision signal in its sending process then it will send a jamming signal. In case of wireless network the strength of signal will get reduced in proportion to the square of the distance. In wireless environment there is a chance of several obstacles.

1.7.1 Hidden and Exposed Terminal

Consider a sender 1 use a carrier sense and detects an idle medium. As the sending procedure starts assume there occurs collision, due to sender 2. Such a situation dealt in hidden and exposed terminal.

In the example shown below the terminal A starts to send towards B. The terminal C wants to send information to B and it senses the medium. If the medium appears to be free (carrier sense fails), C starts sending and it leads to collision at junction of B.

The terminal A cannot realize this collision taken place and it continues with its own transmission.

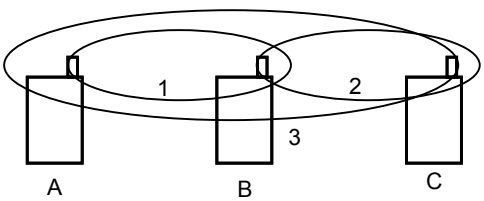


Fig. 1.7.2 Hidden and exposed terminals

The terminal A is hidden for C and C is hidden for A. In other case consider B sends to A and C wants to send data to other mobile that is not in interference ranges of A and C. Now the C senses carrier and finds that the carrier is busy. The terminal C postpones the transmission until it detects the medium as idle. If there is a collision at B it does not affect A since it is very weak and it propagates to A.

In this case the terminal C is exposed to terminal B.

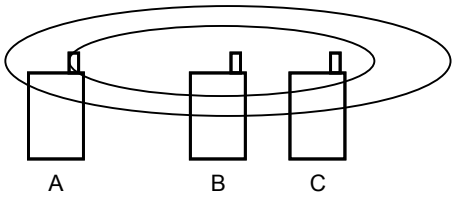


Fig. 1.7.3 Near and far terminals

In near and far terminal case, assume the terminals A and B are sending with same amount of transmission power. The signal strength reduces in proportion to square of the distance involved. For example, B's signal would drown out A's signal and hence terminal C cannot receive the A's signal. If C acts as bare station and coordinating medium accessing job. Then terminal B would drown out terminal A on the physical layer.

The wireless network using CDM has the problem of near/far effect. The signals arrives at the receiver with approximately uniform strength.

On the other hand if a person is closer to one but talks to a third person standing away from him will speak loudly to the third person to overcome the speech of the person close to him. The method of using codes (CDM) helps in reducing interference in wireless environment.

Also an accurate power control is required to receive all the senders with same strength at the receiver end.

1.7.2 Multiple Access Techniques

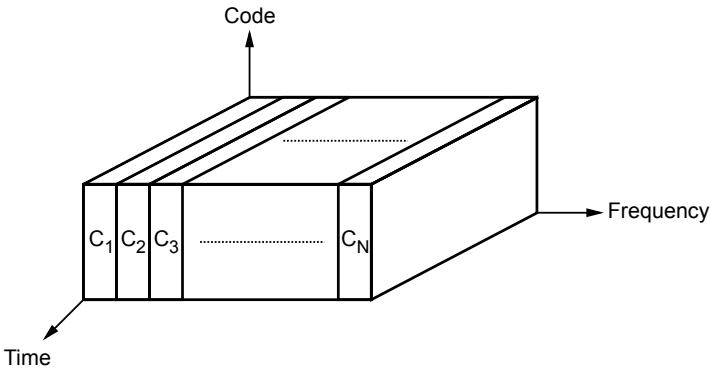
For wireless environment there are several multiple access techniques available. They are listed below.

1. Frequency division multiple access (FDMA)
2. Time division multiple access (TDMA)
3. Code division multiple access (CDMA)
4. Space division multiple access (SDMA).

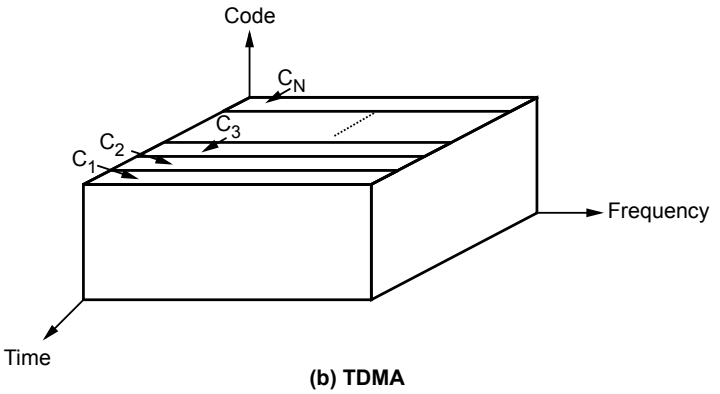
Each one of the multiple access technique are discussed and at the end their features are tabulated and compared.

1.8 Multiple Access Schemes-FDMA, TDMA, CDMA and SDMA

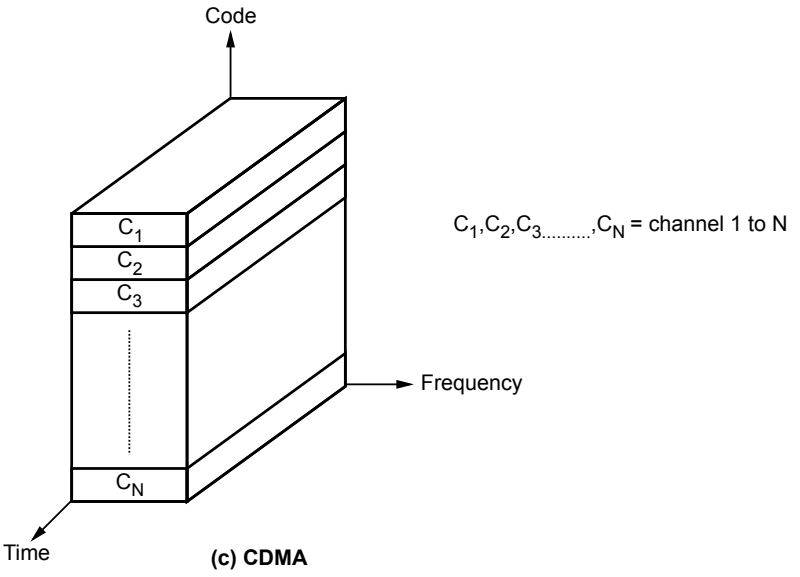
AU : Dec.16,17



(a) FDMA



(b) TDMA



(c) CDMA

Fig. 1.8.1 Multiple access schemes

i) Frequency division multiple access (FDMA) :

In FDMA individual channels $(c_1, c_2, \ldots c_N)$ are assigned to individual subscriber/user as in Fig. 1.8.1 (a) above. A unique frequency band or a channel is allocated to each subscriber, and assignment of channels is done on demand basis. If there is a request for service a channel will be assigned to that user.

ii) Time division multiple access (TDMA) :

In TDMA systems the entire radio spectrum is split into time slots (slices) and each slot is allocated to individual user. The method used by TDMA system is also known as "buffer-and-burst" method. With TDMA only digital message/data and its modulation are used where as FDMA engages analog FM systems. The transmission of signals from several users is interlaced together into a frame structure which is then repeated continuously. A frame basically consists of the following.

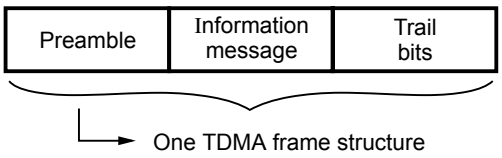


Fig. 1.8.2

i) Information message ii) Trail bits and iii) Preamble

In the TDMA/TDD technique, in a frame information half of the time slots are used only for forward link where as other half of time slots are used for reverse link channels. TDMA is popular because a single carrier frequency is divided as many time slices and they are used by a large number of subscribers by providing one time slice to one user.

One of the main advantages of TDMA scheme is simpler hand off schemes.

iii) Code division multiple access (CDMA) :

In CDMA the narrow band message signal is multiplied with a larger bandwidth signal which is called as spreading signal. This spreading signal is a pseudonoise code sequence with chip rate greater than the message data rate. A pseudorandom code word of each user is orthogonal to the code words of other users.

As in Fig. 1.8.1 (c) there are 'N' no. of channels available and these channels are allotted codes which are unique. Each channel has its own unique code word so that in CDMA interference problem is minimized.

In CDMA the stronger received mobile signal produces noise at the BS demodulators for weaker signals so that the weaker signal may not be received properly. It is called as

near far problem and by using proper power control methods it can be suppressed. In spite of this near far effect, CDMA posses the advantage of using same frequency by many users.

iv) Space division multiple access (SDMA) :

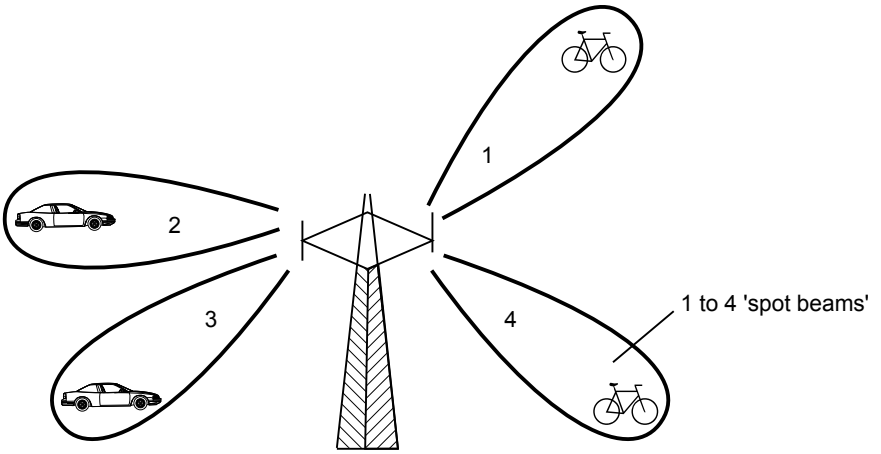


Fig. 1.8.3 SDMA spatially filtered antenna at base station serves multiple subscribers

In space division multiple access (SDMA) spot beam antennas are used to serve multiple users.

The covered regions (with many users) will be served by a single frequency like TDMA/CDMA or various frequencies like FDMA. Sectorized antennas and adaptive antennas can be used for SDMA technique. Using the same channel, all the users in the systems can establish communication. The base station antenna should be capable of spatially filter each user accurately so that less power is enough for entire functionality and the reverse link for every user will be greatly improved.

All the access schemes can also be grouped as narrow band technique and wideband technique according to the method of bandwidth allocation.

1.8.1 Wide Band System - Advantages

The transmission bandwidth of a single channel is larger than coherence bandwidth of the channel with wideband systems. Multipath fading does not affect wideband systems. The CDMA and TDMA system uses either time division duplexing TDD or frequency division duplexing FDD techniques.

1.8.2 Features of Three Multiple Access (FDMA, TDMA and CDMA) Techniques

1. FDMA :

- The FDMA scheme can carry only one telephone circuit at same time.
- If a FDMA channels is not used at particular time, then it will be idle and any other user cannot use it.
- The base station and the mobile station transmit at a time without any break after the assignment of voice channel.
- The FDMA channel bandwidths are narrow.
- The FDMA cell site system cost are higher when compared to that of the TDMA system.
- This technique needs proper RF (radio frequency) filtering to reduce adjacent channel interference (ACI).
- The FDMA systems are less complex than TDMA schemes.
- Duplexers are used by FDMA mobile schemes.
- Synchronization and framing bits are required for FDMA systems since continuous transmission is taking place.

Note In FDMA system use, same antenna at base station is shared by all channels and the power amplifiers are basically nonlinear. These affect the signal and "signal spreading" takes place in frequency domain which in turn generates intermodulation (IM) frequency. It is very important to reduce IM while dealing with FDMA schemes.

2. TDMA :

It divides the radio spectrum into time slots. Each user is alloted one slot and only he can use it. There can be 'n' number of time slots according to the bandwidth. A delay can be used between forward and reverse channels.

- TDMA actually shares single carrier with many number of users.
- The data transmission is not continuous for TDMA users.
- TDMA uses different time slots for the transmission and reception.
- The transmission rates are very high in TDMA schemes and hence adaptive techniques are used.
- High synchronization is required in TDMA systems due to their burst transmission.
- Preamble is important in TDMA which bears synchronization and address information.
- The bandwidth is allotted to different users on demand basis.

3. CDMA :

- The code division multiple access schemes provide individual code for each users.
- Multipath fading is reduced in CDMA.
- CDMA has to meet self-jamming problem.
- Near-far effect is a disadvantage in CDMA technique.
- Since each user is provided with a separate code, CDMA assures interference free communication.
- It uses Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS) methods for spread spectrum mechanisms.
- CDMA guarantees high degree of security than other schemes.
- The channel datarates are very high.

1.8.3 Comparison of SDMA, TDMA, FDMA and CDMA Techniques

Sr. No.	Approach	TDMA	FDMA	CDMA	SDMA
1	Principle	Message sending time into disjoint time-slots, fixed pattern/demand driven.	Message is in different segments of frequency as disjoint subbands.	Spreads the spectrum using orthogonal codes.	Segment space into sectors/cells.
2	Terminals	All the terminals are active for short time periods on same frequency.	Every terminal has its own frequency, which is uninterrupted.	All the terminals are active at same moment which is uninterrupted.	Only one terminal is active in one sector/one cell.
3	Signal Separation	Synchronization is done in time domain.	Filtering in frequency domain is done.	Code plus special receivers arrangement.	Directed antennas/cell structure.
4	Advantage	– Full digital in nature. – Flexible – Easy to establish.	– Robust – Easy establishment – Simple	– Flexible. – Soft handover – Less planning is enough.	– Simple. – Increases the capacity.
5	Disadvantages	– Requires a guard space – Synchronization is difficult	– Not flexible – Resources are limited.	– Receivers are complex in nature. – Needs more complicated power control for senders.	

6	Application	Used in mobile networks.	Combined with TDMA/SDMA for hopping and reuse mechanisms.	– Integrated with TDMA/FDMA for application. – This is a complex scheme.	It is used only in combination with TDMA, FDMA (or) CDMA scheme for applications.
7	Scheme	Time slices are used	Frequency slices are used.	Individual codes for each user.	Segments the space in each sector.

1.9 Random Assignment Schemes

AU : Dec.-16, May-17,18

There are several random assignment schemes and used for the MAC protocols. They include,

- ALOHA
- Slotted ALOHA
- CSMA
- CSMA/CD and CSMA/CA

i) ALOHA schemes :

ALOHA in communication is a random assignment scheme. The basic ALOHA also known as pure ALOHA protocol is used for it.

Consider that a communication node need to send data simply start to transmit. The pure ALOHA scheme does not check wheather the channel is busy. Once if a frame of data is received at the destination end then next frame will be sent or otherwise if the frame is not received then the same frame will be sent again.

If there is no congestion then pure ALOHA is quite enough. But if there are several senders need to transmit then collisions world occur.

For this situation slotted ALOHA random access scheme holds good. In slotted ALOHA entire time is divided into slots where all the slots are of equal size. The packet size is kept with a restriction. Consider a node wants to transmit it can do its job only at beginning of the time slot. Beacon signals are made use of for marking the slots beginning.

Note If there are many stations want to send data the slotted ALOHA is not a much suitable scheme.

ii) CSMA schemes :

A Carrier Sense Multiple Access (CSMA) is a random assignment scheme. In this technique a node first senses wheather the medium is free and then it starts to transmit.

There are two methods of CSMA namely,

- CSMA/Collision Detection (CD)
- CSMA/Collision Avoidance (CA)

In CSMA/CD random access technique, if the sender wants to transmit data it first senses the channel and finds whether it is free. Though the transmitting channel is sending data collision may occur in the channel. A destination node only can find any corrupted frame. Hence a retransmission may be required and channel is not utilized properly.

But a collision avoidance random access scheme is a much better technique than CSMA/CD scheme in avoiding collisions, in the channel, when there is a chance of collision occurance.

In CSMA/CA a node waits till the channel becomes free and then starts to transmit. If the medium is sensed to be busy a node will again wait for a particular time till the channel becomes free. Here any two nodes would not send data simultaneously.

1.10 Reservation-Based Schemes

AU : Dec.-17

A simple reservation-based scheme is Ready To Send (RTS)/Clear-To-Send (CTS). When a node need to transmit data it sends an RTS packet to receiver side before transmission getting started. At the destination the receiver transmits a CTS packet only then data transfer starts. If some other node wants to transmit packets it has to first sense a CTS packet. It makes sure that transmitting node has completed its transmission.

In the case of contension-based MAC protocol when a node need to transfer data it sends message for reserving the medium by just using a control message.

Some of the example schemes of RTS/CTS based medium access control (MAC) protocols includes,

- MACA
- MACAW
- S-MAC protocols.

1.10.1 MACA Scheme

The MACA protocol is nothing but multiple/access collision avoidance protocol. The hidden or exposed problem in MAC is avoided using MACA. It can also regulate transmitter's power. If a node makes use of MACA scheme it sends a request signal to the RTS to the destination (receiver).

All other sender's get this information and hence they will get out of their transmissions. If the receiver is free it will now responding with that of a CTS.

Eventhough MACA is a collision avoidance protocol there may be a collision occurance during the transmission of an RTS packet.

Hidden and exposed terminal problems can be avoided with the MACA protocols.

1.11 Applications of Mobile Computing

AU : Dec.-16

Mobile computing provides several aplications and they are user friendly. Some of the applications include;

i) Vehicular mobile computing :

Vehicles will include weather forecasting, road conditions, along with news, music etc. Mobile computing enables many user friendly facilities. For personal system communications GSM phones might be available offering the voice and data connectivity with 384 kbits per second.

Mobile computing will be useful in emergency situations in wirelessly contacting the nearest hospitals and help in patient assistance etc.

ii) Business environments :

Mobile computing is useful where a simple device is represented by sensors transmitting state information. Also pagers, mobile, phones with full colour graphic delay will be useful in business applications. The PDA's, Palmtop/pocket computer etc are user friendly as it simplifies several calculations.

Thus mobile computing is useful in different fields and many applications are made possible.

Review Questions

Part A

1. *Define mobile computing.*
2. *Write a short note on mobile networking.*
3. *List any two mobile computing application.*
4. *Give two characteristics of mobile computing.*
5. *Comment on MAC protocol.*
6. *Write a short note on fixed assignment schemes.*
7. *What is virtual home environment ?*
8. *What are the three tier setup in mobile computing ?*
9. *Mention three applications of mobile computing.*
10. *List the advantages of mobile computing.* **(Refer section 1.1)** **AU : June-16, Marks 2**

11. *Explain hidden and exposed terminal problems in infrastructure - less network.* **(Refer section 1.7.1)** **AU : June-16, Marks 2**

12. *What are the different random assignment scheme in MAC ?* **(Refer section 1.9)** **AU : Dec.-16, Marks 2**

13. *Differentiate mobile computing and wireless networking.* **(Refer section 1.5)** **AU : May-17, Marks 2**

14. *List some random assignment scheme.* **(Refer section 1.9)** **AU : May-17, Marks 2**

15. *List out the differences between mobile computing and wireless networking.* **(Refer section 1.5)** **AU : Dec.-17, Marks 2**

16. *"MAC protool designed for infrastructure based wireless network may not work satisfactory in infrastructure-less environment." - Justify.* **(Refer sections 1.7 and 1.7.1)** **AU : Dec.-17, Marks 2**

17. *Distinguish between mobile computing and wireless networking.* **(Refer section 1.5)** **AU : May-18, Marks 2**

18. *List the issues of wireless MAC.* **(Refer section 1.7)** **AU : May-18, Marks 2**

Part B

1. *Explain the structure of mobile computing.*
2. *Explain the MAC protocols in detail.*
3. *Define mobile computing. Explain its characteristics and applications.*
4. *Explain the fixed assignment schemes and random assignment schemes.*
5. *Write short notes on,*
   i) Mobile computing environment and ii) MAC protocols.
6. *Explain the characteristics of Mobile computing.* **(Refer sections 1.4, 1.6)** **AU : June-16, Marks 8**
7. *Explain the structure of Mobile Computing Application.* **(Refer sections 1.3, 1.3.1)** **AU : June-16, Marks 8**
8. *Explain the various taxonomy of MAC protocols in detail.* **(Refer sections 1.7, 1.7.1)** **AU : June-16, Marks 16**
9. *Differentiate between FDMA, TDMA and CDMA.* **(Refer section 1.8.3)** **AU : Dec.-16, Marks 16**
10. *Explain the distinguishing features of various generations of wireless networks.* **(Refer section 1.2.2 to 1.6)** **AU : Dec.-16, Marks 8**

11. *Describe the applications of mobile computing.* **(Refer section 1.11)**
AU : Dec.-16, Marks 8

12. *Explain the wireless MAC issues in detail.* **(Refer sections 1.7 and 1.7.1)**
AU : May-17, Marks 8

13. *Explain fixed assignment scheme with a neat diagram.* **(Refer section 1.7)**
AU : May -17, Marks 8

14. *Explain hidden and exposed terminal problem in infrastructure-less network.*
(Refer section 1.7.1) **AU : Dec.-17, Marks 8**

15. *Describe architecture of mobile computing.* **(Refer section 1.3.1)** **AU : Dec.-17, Marks 8**

16. *What are the fixed assignment schemes of MAC protocol ? Explain their mehanism in detail. Compare and contrast them.*
(Refer sections 1.7.2, 1.8.3 and 1.10) **AU : Dec.-17, Marks 16**

17. *Discuss in detail the structure of a mobile computing application.*
(Refer section 1.3) **AU : May-18, Marks 6**

18. *List the characteristics of mobile systems.* **(Refer section 1.6)** **AU : May-18, Marks 6**

19. *What is CSMA ? What are the categories of CSMA ? Explain their working with advantages and disadvantages.* **(Refer section 1.9)** **AU : May-18, Marks 7**

❑❑❑

Notes

Unit II

Mobile Internet Protocol and Transport Layer

Syllabus

Overview of Mobile IP - Features of Mobile IP - Key Mechanism in Mobile IP - route Optimization. Overview of TCP/IP - Architecture of TCP/IP- Adaptation of TCP Window - Improvement in TCP Performance.

Contents

2.1 Overview of Mobile IP

AU : May-18

Whenever the user is connected to an application(s) across the Internet it is said to be in mobile status. The routers actually uses the IP address in IP datagram to do the routing function. The network portion of an IP address helps routers to send datagram from source computer to network where the target computer is attached (connected) with. Mobile IP can also deal with dynamic IP addresses.

Terminologies related to mobile IP :

- Home address : The IP address on the network is known as home address.
- Home network : A mobile node is designated to a network which is called as home network.
- Foreign agent : The router on the foreign network is called as foreign agent.
- Foreign network : Whenever the mobile node moves the attachment point to another network then it is called as foreign network.

Home agent : The mobile node that communicates with the router of its home network is called as a "home agent".

Care of address : It is the address that is used to identify the location of foreign agent.

The mobile IP is explained with an example in next chapter.

2.1.1 Mobile IP

The mobile internet protocol is denoted as mobile IP.

The 'MOBILE IP' is similar to the handoff or roaming situation in cellular mobile network. The handoff technique helps the user to continue conversation inspite of his mobility.

Likewise the user who is connected through Internet and his point of attachment changes dynamically. But all the connections established are maintained without any disturbances though his underlying network properties change. Basically the IP address changes from one network to another network. It holds good if the user is static in his particular network. The 'MOBILE IP' enhances the efficiency of network and friendly with the users.

Inspite of mobility the user finds the connections are still available by this technique.

2.1.1.1 Goals and Requirements of Mobile IP

In wireless and wired networks as soon as a person leaves his home network packet data reception is immediately stopped. Because of routing mechanisms packet reception

in mobile status is not possible. On the otherhand addresses of all the computers in internet has to be kept stored but it is not practically implementable.

Only if the receiver is available within the physical subnet it will continue to get data packet. For this the correct topological address is a must. Also higher layer protocols like TCP always relays on the IP addresses. Hence any change of IP address may break the TCP connection. A TCP connection can be identified with informations like

- Source IP address
- Source port
- Destinations IP address
- Destination port.

A charge of IP address will affect TCP connection that has been established. Change of IP address may be a quick solution but it does not work practically.

Hence apart from this some of the requirements as an alternate to this quick solutions are

- Compatibility with other computers
- Transparency of mobility status
- Scalability
- Efficiency
- Security.

2.2 Basic Capabilities and Features of Mobile IP AU : Dec.-16, 17, May-18

Node : Node is a router or a host.

Mobile node : It is not a must that a mobile node should change its location with changing of its IP address. A host may change its attachment point from one network to another.

- **Home agent**

It (router on home network on mobile node) tunnels datagrams to mobile node whenever mobile node is away from its home network. Home agent also maintains the location data (information) for mobile node.

- **Home address**

It is an IP address assigned for a period to a mobile node. Wherever the home agent is connected to network this address remains unchanged.

- **Correspondent node**

The mobile node communicates with a peer and called as correspondent node. It can be stationary or mobile.

- **Link**

  It is a medium used for communication of nodes at link layer.

- **Tunnel**

  It is the path that is followed by datagram when encapsulated. At destination side the delivered datagram is decapsulated.

- **Foreign network**

  Except mobile nodes's home network all other network can be treated as foreign network.

- **Care-of-address**

  Whenever mobile node is away from its home network the care-of-address is the termination point of a tunnel (path) towards the mobile node.

- **Home network**

  Mobile node which is assigned to network is called as home network.

- **Foreign agent**

  A router available on a foreign network is known as foreign agent.

Three basic capabilities of mobile IP to support and enhance its operations :

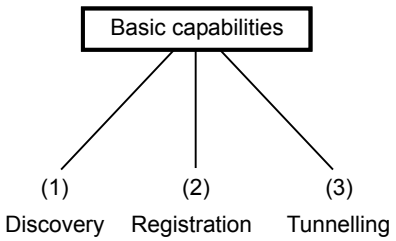


Fig. 2.2.1

1) Discovery

Mobile node makes use of discovery procedure for identifying the home agents and also the foreign agents.

2) Registration

Mobile node makes use of registration (authenticated) procedure to intimate the care-of-address to a home agents.

3) Tunnelling

It is used for forwarding the IP datagram from home address to a care-of-address.

(See Fig. on next page)

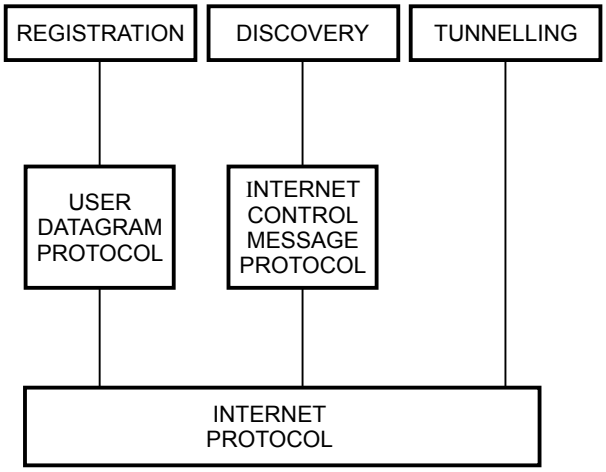


Fig. 2.2.2 Mobile IP - Protocol support concept

2.3 Mobile IP-Mechanism

AU : June-16, Dec.-16, 17, May-17, 18

Mobile IP

Mobile Internet Protocol is denoted as mobile IP. A schematic diagram of it is shown below. The connectivity in the network is represented as links.

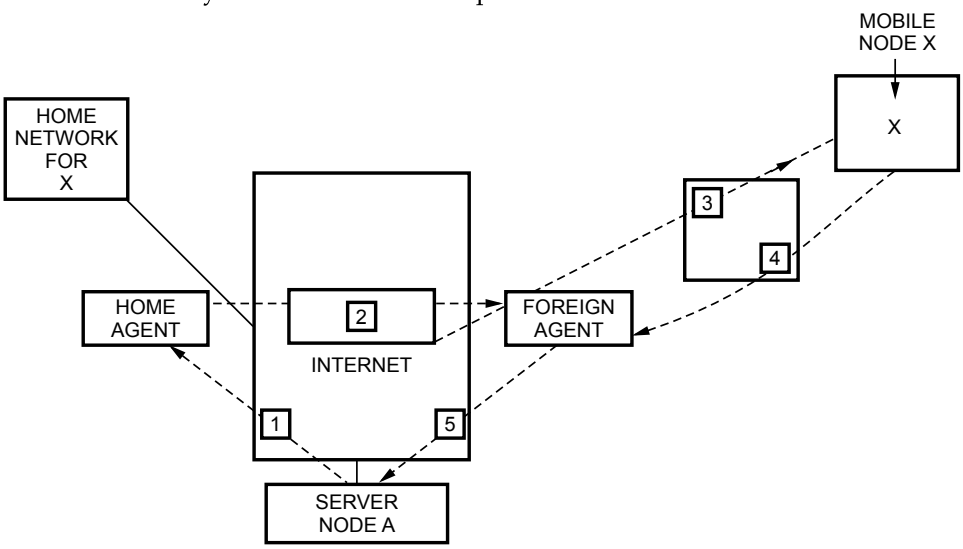


Fig. 2.3.1 Mobile IP schematic diagram architecture

Case study

The server 'A' (say) wants to send an IP datagram to a node X. The home address of X is known to A. The server A does not know whether X is in its home network or not. A sends packet to X with home address of X as its destination Internet protocol address in the IP header. The IP datagram then routed to X's home network area.

At the X's home location network the IP datagram is intercepted by the available home agent. The home agent also discovers that 'X' is a foreign network. Then the home agent encapsulates the full datagram inside a new IP datagram.

At the distant network the IP datagram which is incoming is intercepted by the foreign agent. The foreign agent acts as a counter part of this home agent in the foreign network.

X intends to respond to the message and it sends traffic to 'A'. In this example A is not mobile. Hence A has a fixed Internet Protocol (IP) address. For routing X's IP datagram to A, each datagram is sent to a router in a foreign network, and this router is a foreign agent.

The IP datagram from X to A then travels across the network using A's address (IP) as its destination address.

It is important that a mobile IP should have three basic capabilities.

i) Discovery

ii) Registration

iii) Tunneling.

Each of the above are discussed in detail below.

i) Discovery

Each mobile node uses a particular discovery procedure to identify the respective home and foreign agents. This mobile IP discovery procedure is built on the top of an existing router discovery. The router can detect the entry of any new mobile node. The router will periodically issue a router advertisement message. The mobile node by noticing this advertisement message will compare the network portion of the router IP address with network portion of its IP address allocated by the home network.

ii) Registration

If a mobile node obtains an address (care-of-address) from the distant network (foreign) then it should be registered with the home agent. The mobile node sends a request for registration to its home agent along with care-of-address information. Whenever the home agent receives the registration request information the routing table is updated and it sends back the registration reply to the mobile node. Registration thus is done to inform the home agent about its address.

Authentication

It is a part of registration phase. The mobile host has to be authenticated. A digital signature is generated using the MD5 hashing algorithm and 128 bit secret key. The mobile node and the home agent will share a common key for security purpose and this key is not known by any third party or intruders. A triplet (home address, registration

life time and care-of-address) is maintained at the home agent at the end of registration. This is known as binding the mobile node.

The registration process has four important steps.

1. The mobile node sends a registration request to foreign agent for forwarding its service from the foreign agent.
2. This request from mobile node is relayed to home agent of mobile node by the foreign node.
3. The home agent rejects or accepts it and reply is sent.
4. Finally the foreign agent relays the reply message to the corresponding mobile node which actually requested it.

iii) Tunnelling

Introduction

A tunnel basically establishes a pipe (virtual pipe) for their data packets to travel from tunnel entry and tunnel end point.

But tunnelling a packet does not affect the data. Tunnelling is done using encapsulation.

The encapsulation is a mechanism of picking a data packet containing a packet header and data and then fitting it together into the data packet of next new packet. An opposite procedure of the same is called as decapsulation.

2.3.1 IP-in-IP Encapsulation

For performing encapsulation their are different ways available. In case of Mobile IP it is conventional method to use IP-in-IP encapsulation.

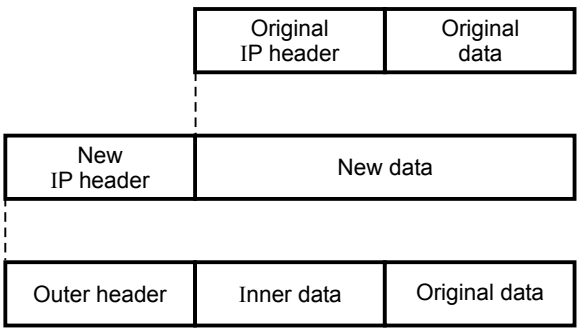


Fig. 2.3.2 IP encapsulation

In IP-in-IP encapsulation the version is 4 for IP version 4 as mentioned. The Internet Header Length (IHL) denotes the length of outer header with 32-bit words. TTL must

be high such that it helps packets to reach the end point of tunnel. Other fields are also shown in IP encapsulation in mobile IP Fig. 2.3.3.

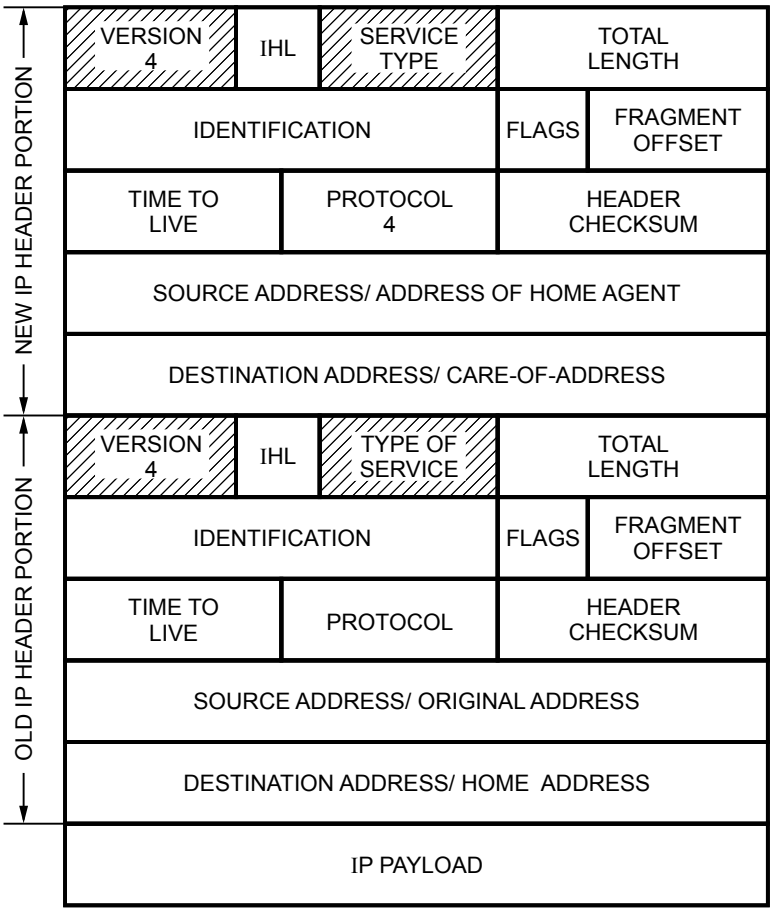


Fig. 2.3.3 IP encapsulation in mobile IP

2.3.2 Minimal Encapsulation

In the IP-in-IP encapsulation method many fields are just redundant. Hence it is better to use minimal encapsulation as an optimal method of encapsulation. The tunnel entry and end point are defined. Here the field for header consists of value 55. The type of protocol and the address of mobile nodes are required. For fragmentation offset no field is specified in minimal encapsulation.

The 'S' is set bit. IP cheksum TTL, flags, IP identification are available as shown in Fig. 2.3.4. The minimal encapsulation will not entertain/work with previously fragmented data packets.

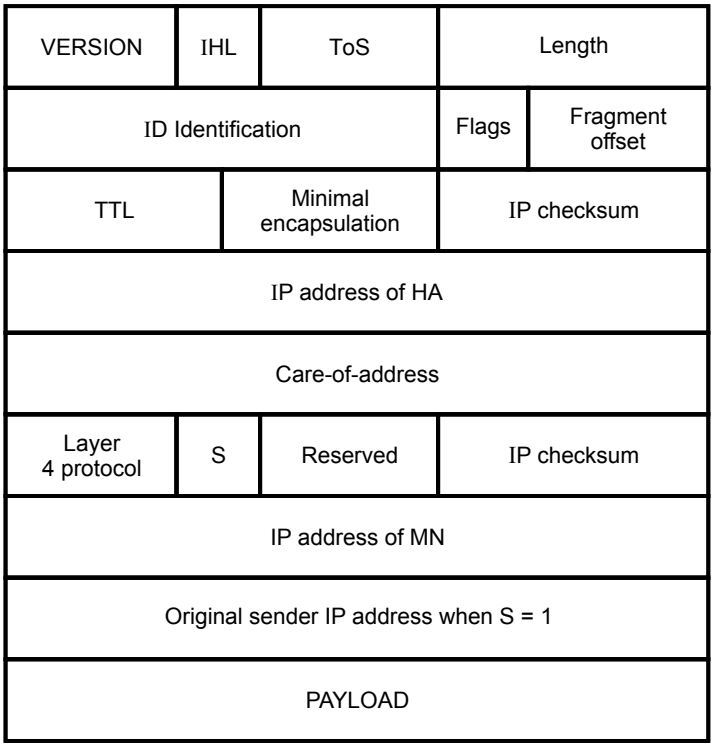


Fig. 2.3.4 Minimal encapsulation

In the tunnelling operation of mobile-IP, IP-within-IP encapsulation (embedding) mechanism is applied. For this a new IP header called as tunnel header is added by home agent. Therefore the home agents address is the tunnel source IP address itself.

IP packet delivery

For the delivery of data packets to and from the mobile node the needed entities are

- Home network
- Router (Home Agent) - (HA)
- Router (Foreign Agent) - (FA)
- Internet
- Mobile Node (MN)
- Correspondent Node (CN)

If CN want to transmit a packet to MN the mobile IP should be capable to support the hiding of mobility of MN, because the CN need not be informed about the status of MN.

Once if a packet is being sent to MN from CN, the Internet that does not have the location of MN currently will route the packet to the HA to which MN belongs to.

This HA will know the present location of MN. The data packet is not simply forwarded to the subnet but prior to that it is encapsulated and then tunnelled to Care-of-Address(CoA). A new header is also added.

Then the Foreign Agent (FA) will decapsulate it and eliminate this header added additionally forward it to the destination node.

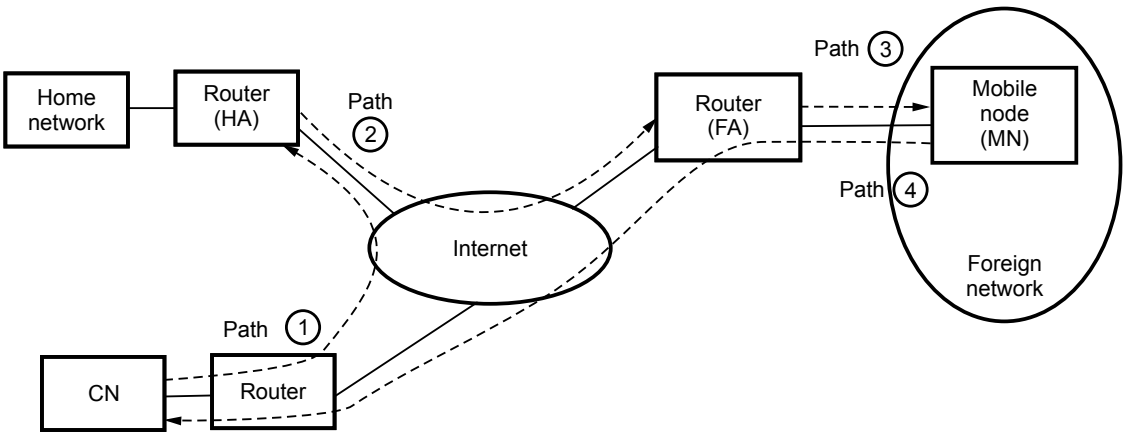


Fig. 2.3.5 Packet delivery procedure

Thus the packet delivery procedure through Internet takes place with the help of routers and agents as discussed above.

Note Shaded fields in the IP encapsulation represents the fields that are carried directly from inner IP header to that of the outer IP header portion.

2.4 Routing

AU : May-17

The importance of routing is essentially the distributing ability with the shortest path that is possible. Each node in the network prefers a shortest neighbour to it. The process of forwarding continues till the packet reaches the destination. The objective of routing concept is to reach the destination with an optimal path. The routing should also satisfy the needs of an ad hoc network. The router should be capable of performing few important functions.

1. Router should provide a link between the networks.
2. It should provide routing and delivery of data between processes on the end systems attached to various networks.

3. Routing should be such that it is able to do all functions without modification of architecture of networks and subnetworks.

Router should also be able to make differences among networks like addressing schemes, interfacing methods and maximum possible packet sizes.

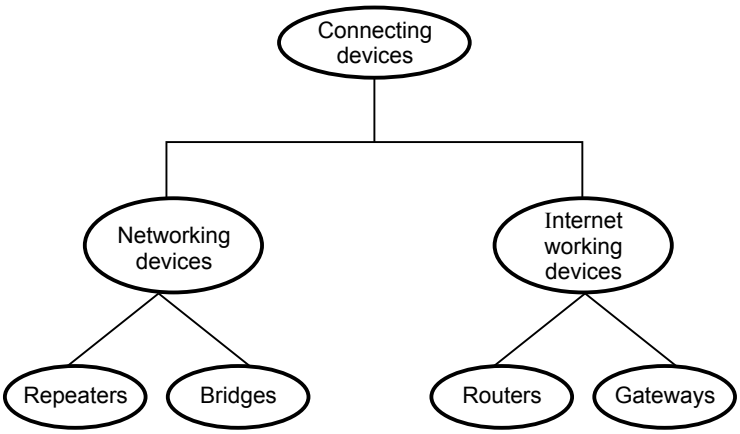


Fig. 2.4.1 Connecting devices in a network

When two or more devices are connected for sharing the data/resources it forms a network. The network so formed can be a Local Area Network (LAN). Depending upon the coverage distance the network is also classified as local area network (LAN), Metropolitan Area Network (MAN) and wide area networks (WAN). When entirely separate networks change information (data) between them it is known as internetwork or simply Internet. Now it is important to connect or link many Local Area Networks (LAN's) into an Internet requires more (additional) internetworking devices called as routers and gateways. Hence the Internet is nothing but interconnection of networks.

The important devices associated with Internet are,

1. Repeaters
2. Bridges
3. Routers
4. Gateways.

The repeaters mentioned here acts on the physical layer. The bridges make use of addressing protocols and influences flow control of a LAN setup, and are active in Data Link Layer (DLL). The routers provides between two similar (but separate) Local Aarea Networks (LAN's). Router is highly active in network layer of OSI model.

The last one called as gateways facilitates translation services between the incompatible LAN's and active in all the layers. The bridge device in a network has many types.

1. Simple bridge 2. Multiport bridge 3. Transparent bridge.

Whenever the bridges used to connect different LAN's many aspects are given consideration. Some of them are listed below;

a. Frame format

b. Data rate

c. Payload size

d. Address bit order.

The bridges and repeaters in a network are mainly hardware devices that are capable of doing special tasks.

But the devices called routers are different from these types. They consists of software that makes them to find which of the available paths is appropriate for a particular type of transmission at that time. They can function at three main layers. They are,

1. Physical layer

2. Datalink layer

3. Network layer of OSI standard model.

Router can relay the packets among different networks (i.e. interconnected networks). Routers acts like stations on a network. Router switches the packet from a network to other network which wants to receive it. Routers thus directs the packets to the router of destination side in the proper path. It has addresses, and links to which it continues the job and two or more networks at a particular instant of time period. (Refer Fig. 2.4.2 on next page.)

There are four networks connected through routers denoted as 'R' here. These routers are responsible to direct the packets of data in right direction towards destination. If the received packet's address of node to which it has to be sent is foreigner to that particular router then router is capable of determining the correct relay point in the network to which this received packet should be actually sent such that it reaches its destination in that network successfully. The concepts considered in routing are,

1. Least cost routing

2. Adaptive routing

3. Non adaptive routing.

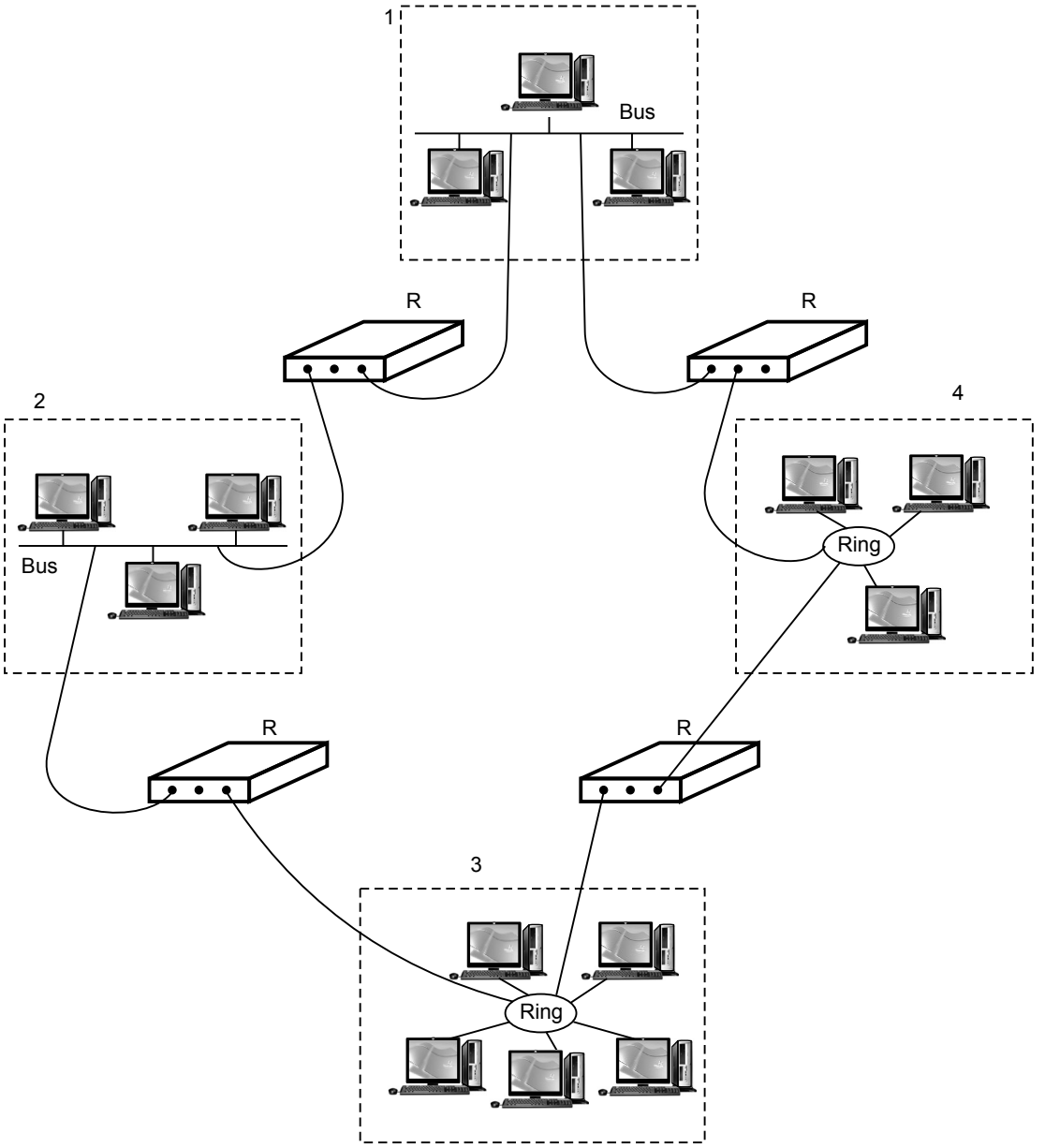


Fig. 2.4.2 Routers (R) in an Internet with four networks (1, 2, 3, 4)

2.4.1 Routing Types

1) Least Cost Routing

This routing is based on efficiency of the system. The shortest path also denotes the cheapest path possible. The number of hops required for the packets to reach the destination also counts. The less number of hops is economical and expresses an efficient routing.

If the pathway requires least number of relays it is termed as hop-count routing. In this scheme every link is treated to be equal length. The decision of best short route is made by finding the summation of all lengths of all the links used by the path.

2) Adaptive routing

In this routing method depending upon the changes in topology and nature of the given network every router will select a new route (way) for every packet.

If a router decides a pathway, it passes the packet (data) to next router on the same path and then does not worry about it. The new router may follow the same path for transmission or selects a different path also.

The life time determination of the packet is also an important factor. The hand off mechanism from one router to another router enables lesser logic and control factors which must be present in the frame. The acceleration of the packet is also enhanced. Each packet added with a packet field called "packet life time" or "time to live" (TTL) which is considered before a packet is lost or destroyed.

3) Non adaptive routing

In this scheme the routing decisions are made according to changes of network topologies. Thus routing method may be adopted according to expected efficiency.

2.4.2 Destination Sequenced Distance Vector Routing (DSDV)

The Destination Sequenced Distance Vector Routing (DSDV) is a table driven algorithm based on Bellman Ford routing mechanism. It is highly useful for mobile networks. There are two types of mobile networks namely,

1. Infrastructured network
2. Ad hoc network.

In the first type it has the fixed and wired gateways and in the second type it consists of infrastructureless mobile network. It has no fixed routers. All the nodes are flexible with dynamic connections in the network in a arbitrary manner. The applications of ad hoc network are meetings where quick information sharing is a must and emergency search and rescue operation cases etc. The ad hoc network of early days had few drawbacks like the following.

1. High power consumption
2. Low bandwidth.
3. High error rates

The routing information must be properly advertised by broadcasting or multicasting the packets that are transmitted periodically.

Decision has to be made based on the data and delaying of advertising the routes are allowed. The idea of delaying is to avoid many number of rebroadcasts in the network due to instability.

The two types of protocols are table driven routing protocol and source initiated (demand-driven type) routing protocol.

The table driven routing protocol tries to maintain consistent and up-to-date routing related information from each node to every other node in the network.

The DSDV protocol under this category requires every mobile station to advertise to every current neighbour. The entries of the list may dynamically change and it makes way for requirement of frequent advertisements to take place. Hence every node can have knowledge about every other mobile computer.

The DSDV protocol enables shortest number of hops for a route to a destination. The mobile computers frequently link with base stations that allows them to exchange information with other computers connected in the wired networks.

In an ad hoc network movement of host (mobile host) is supported by this protocol. For example the mobile host (MH_1, MH_2, MH_3 ....) can move in an ad hoc network.

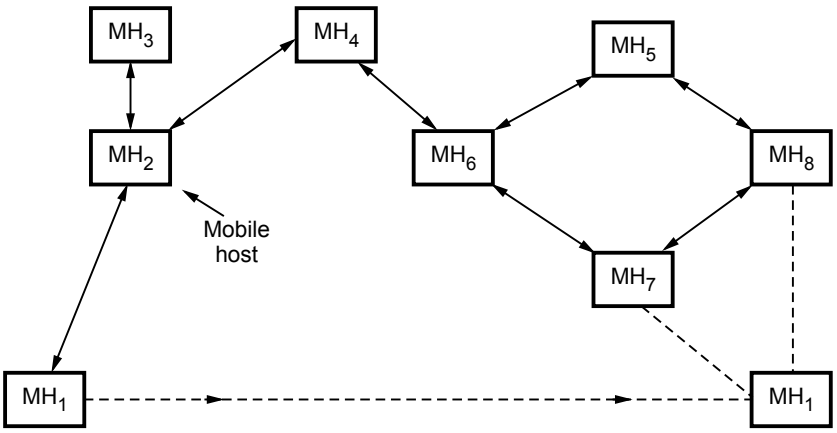


Fig. 2.4.3 Movement enabled in an ad hoc network

The movement of each mobile host (MH_i) is possible and each one has its sequence number. A table is maintained and updated as the hopping takes place. Advertisements of routing information in the network is made whenever required. The DSDV routing protocol well suits the movement of mobile hosts.

The fluctuations of routing has to be avoided. The updation of routes are done as per few important criteria.

1. Routes are preferred if sequence numbers are same and still the metric is lower.

2. Routes are preferred (most of the time) if the sequence numbers are newer.

To avoid damping fluctuations setting time has to be properly used. The setting has three fields keyed with first field.

1. Destination address field
2. Last settling time field
3. Average settling time field.

Advantages of DSDV protocol

1) The Dynamic Sequenced Distance Vector (DSDV) routing protocol guarantees loop free paths to every destination.
2) Effective protocol under table driven category for movement of mobile hosts.
3) It maintains stability.
4) Compatible with Ad hoc networks.
5) It is good for the system in steady state condition.
6) DSDV protocol models mobile computers as routers that co-operates to forward packets according to the needs of the network.
7) It can be utilized at either network layer (layer 3) or below the network layer (above the MAC layer), with few additional information along with the routing informations.
8) DSDV uses settling time and sequence number and hence enables the routing table free from damped fluctuations.

2.4.3 Dynamic Source Routing (DSR)

The Dynamic Source Routing (DSR) protocol is an on-demand protocol which is designed for multihopping wireless ad hoc networks. It provides two functions.

1) Route discovery
2) Route maintenance.

Route discovery : It is performed whenever a node wants to send a packet of data to a particular destination for which it does not have a route.

Route maintenance : It identifies a link failure on an active route or path. Once route failure is found then it is informed in such a way that it is maintained. Both the route discovery and route maintenance are available on an on-demand situation. Information cannot be exchanged in a periodical way.

A main difficulty in operation with Dynamic Source Routing (DSR) is handling congestion. While dealing with DSR protocol it is important to consider mobile status of devices. The impact they have created is high. Since ad hoc devices consists of mobile

MOBILE TCP

Introduction

The standard TCP used with fixed hosts and wired networks pose serious drop in throughput if used without modification in wireless environment. The reason is that standard TCP understands only congestion as the reason of packet loss and triggers congestion control mechanism whereas in wireless networks there can be many other reasons of packet loss like high bit error rate, frequency disconnection, improper handovers. In such a situation, applying congestion control mechanism would lead to serious drop in the throughput. Therefore there is need optimized algorithms for TCP in wireless environment. But fixed networks are already based on standard TCP and it is not possible to entirely change the entire TCP. Therefore the algorithms proposed should have the following goals.

1. It should not aim to modify the entire TCP because it is the based on which the whole of internet rely
2. The protocol should not trigger congestion control mechanism when it is not required
3. The network related problems on wireless link should be isolated from the fixed hosts

The TCP variants devised for wireless environment should adhere to these goals. In the previous module we discussed two protocols I-TCP and snooping TCP. Both are split connection protocols and divide the end-to-end TCP connection into two parts via an intermediate host. The connection between fixed host and intermediate host has standard TCP whereas optimized TCP resides on link between intermediately host and mobile host. In I-TCP the intermediately hosts act as proxy which takes packets from fixed host, gives acknowledgement and then forwards the packet to mobile host and same thing is repeated on other side. This completely loses end-to-end semantics of TCP because the packets are acknowledged even before they are delivered. The situation is worst when the mobile moves to new network. All the packets buffered for the mobile device needs to be forwarded moreover whole scheme fails when the intermediator crashes. As a revision to this scheme, snooping TCP was proposed in which the intermediator just caches the packets from fixed host towards the mobile host at the same time it snoops the flow of acknowledgements and packets header. In case of missing acknowledgements it forwards the cached packet to the mobile host. The scheme retains end- end semantics. Both I-TCP and Snooping TCP handles packet losses due to bit error rate and do not work well when packets are lost due to frequent disconnections.

In 1997, M-TCP was proposed by Brown & Singh. The protocol deals with the problem of periodic disconnection as compared to existing solutions of that time which deals with problem of high bit error rate. The proposed solution is to send the sender into persist mode when the mobile device goes into disconnection state. This is done by shrinking the window of the sender. In this module we will discuss the M-TCP protocol in detail and how it performs in the situation of frequent disconnections.

M-TCP

Let us see what are the reasons of frequent disconnections in mobile environment and what are the problems associated with it

Reasons of frequent disconnections

- Brief blackout period (or disconnection) during handovers
- Disconnections may also be caused by physical obstacles in the environment that block radio signals, such as buildings.
- Due to load on cells, the mobile device may not receive any bandwidth for large time **periods (call blocking)**

Problems with existing solutions during disconnections

- If the mobile is disconnected for a long period of time, the sender will invoke congestion control.
- For Snooping TCP, in the case of handoff's the new snoop will start with empty cache and till the cache is built ,there would be no retransmission or filtering and there would be decrease in throughput. The problem of degradation would be more serious when cell sizes are small (pico or micro cell) environment
- Serial Timeout: A serial time out is a condition wherein multiple consecutive retransmissions of same segment are transmitted to mobile while it is disconnected and these retransmissions are also loss. The retransmission timer also gets doubled with every retransmission(Fig 1).

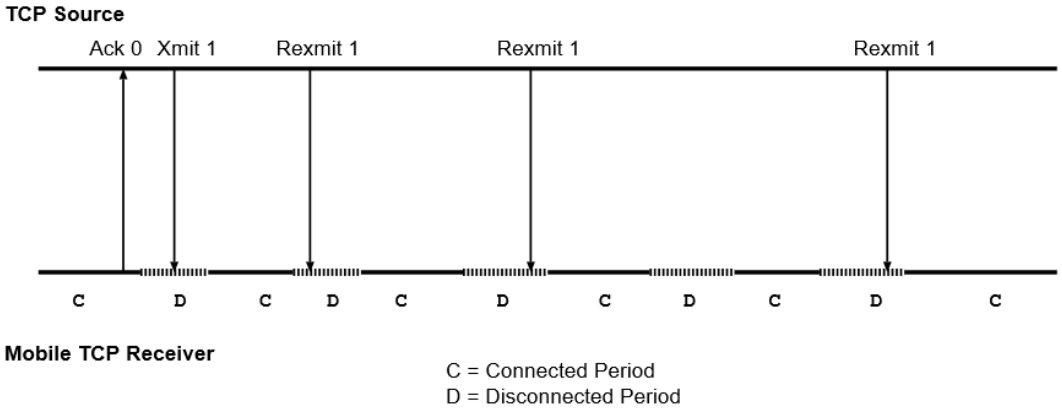


Figure 1: Serial Timeouts

In Fig. 1 , C & D indications connection & disconnection states It can be seen that retransmission are taking place in disconnection states which again triggers doubling of timer. Hence there is no activity till 64 sec even if the device regains connection. The split connection approached using TCP on both sides of connection respond poorly to lengthy disconnections

M-TCP is aims to solve the problem of frequent disconnection, preserving end-end semantics and throughput

M-TCP Architecture

- The authors of M-TCP proposed it as three-layer architecture (Fig. 2)
- Lowest level- Mobile host
- Next level- MSS (Mobile support station) is a node which controls mobile host
- Highest level- SH or a supervisory host controlling many MSS

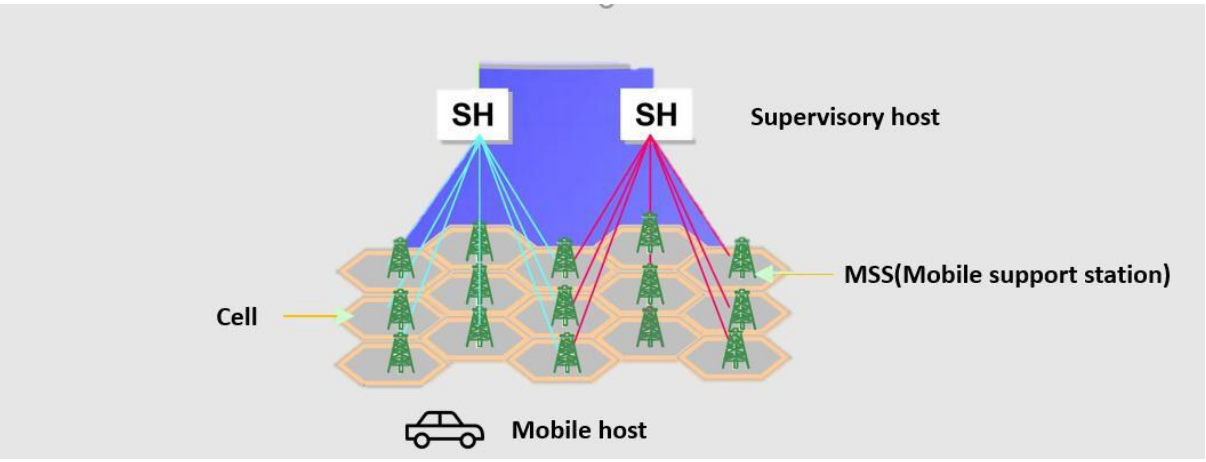


Figure 2: Layered M-TCP architecture

Advantage of having MSS

1. MSS are cheaper devices as they serve as only connection points whereas in I-TCP & snoop protocols, sophisticated MSS are used. Hence cost of infrastructure is increases particularly in case of picocelluar networks
2. No need to transfer the states when MH roams from one cell into another controlled by same MH

M-TCP: Transport layer Design

The proposed protocol divides the connection into two parts at SH supervisory host (Fig. 3).

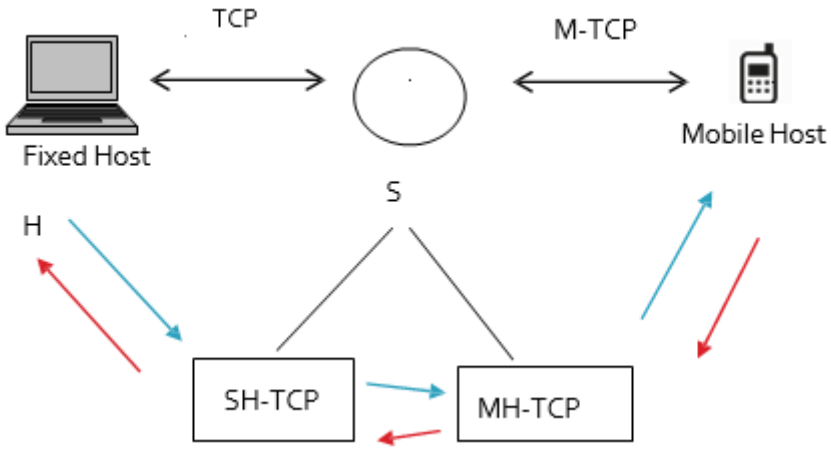


Figure 3: Layered M-TCP architecture

- The TCP sender on fixed network uses unmodified TCP to send data to the SH while SH uses modified TCP to send data to the MH.
- The TCP client at SH receiving data from fixed host is called SH-TCP
- TCP client at SH towards MH is called M-TCP .It receives packets from SH-TCP and passes to mobile host.
- The acknowledgements are received by M-TCP from mobile host and forwarded to SH- TCP which delivers it to the fixed host

SH-TCP client

- SH-TCP receives a packet from fixed host
- It passes it to M-TCP client.
- It does not acknowledge maintaining end-end semantics.
- M-TCP at SH passes the packet to MH
- It receives ACK's from Mobile host via M-TCP
- Sends the ACK's to Fixed Host

In a situation when disconnection is there, the approach is to choke the TCP sender when mobile device is disconnected & allow the sender to transmit at full speed when the connection is regained. The mode with choked window is called persist mode. According to RFC 1112, TCP clients go to persistent mode when window size is shrunk to zero. For this purpose, a new Ack is required. SH-TCP follows a strategy to send the sender into persistent mode. It keeps one Ack from mobile host unacknowledged. The strategy is as follows:

- Suppose the window size is 100.
- 70 bytes are sent to mobile host.
- Mobile host Acks all 70 bytes
- The SH-TCP sends Ack for only 69 bytes to the sender
- When the MH goes into disconnection state after acknowledging 70 bytes, it stops sending Acks.
- When M-TCP does not receive Ack's it assumes the mobile to be disconnected and informs SH TCP
- It uses the last Ack for 70th byte.
- Sends it to TCP sender along with window size update
- When TCP sender receives window size update message, it goes into persistent mode
- As long as the sender is in the persistent mode, no time out occur, no exponential back off of retransmission timers occur and neither it goes into slow start When connection is regained,
- When the MH regains the connection, it sends a greeting packet to SH.
- M-TCP receives it, passes it to SH-TCP.
- SH-TCP sends Ack to the sender and reopens it's receive window.
- The sender leaves persist mode and begin sending data again at full speed from bytes number w+1 where w is the last acknowledged byte.

The only issue with this strategy is when there only w' bytes to be sent to MH. According to protocol, SH-TCP would send Ack's for only W'-1. This will cause timeout at sender & trigger retransmission and after 12 retrains sender will quit. The solution to this is that when SH-TCP understands that there are no more Acks from the MH it should not allow the sender to go in persist mode. It should send the Ack for last byte.

Design of M-TCP:

The goal of M-TCP is to avoid serial timeouts & recover from losses due to disconnection. The modification made in this protocol is notification of wireless connectivity.

- M-TCP observes flow of Acks from MH
- If it does not receive Ack for some time, it understands mobile host is disconnected.
- M-TCP freezes all its timers. This is done to avoid congestion control mechanism at M- TCP
- It informs to SH-TCP about disconnection
- When the mobile host regains the connection, it sends a last Ack to mark the reconnection.
- M-TCP informs this to SH-TCP who opens senders transmit window
- When connection is gained, M-TCP at MH sends a specially marked Ack to M-TCP at SH, which contains Seq. no of highest byte received so far
- M-TCP unfreezes timers to resume operation

Advantage

- End-End semantics is maintained because the SH does not Ack message it just forwards Ack from MH
- No buffering of packets at SH as in I-TCP so it is not necessary to forward buffers to SH
- The efficiency of the TCP connection is not degraded due to disconnections since the sender is prevented from going into exponential backoff and slow-start
- If the MH moves from the domain of one SH into the domain of another SH, the old SH does not need to forward the socket buffers (as in I-TCP).

Limitations

- Errors on wireless link are also propagated to the fixed sender
- It assumes bit error rate to be very low which is not a valid assumption

Wireless Application Protocol

The Wireless Application Protocol (WAP) is a set of communication protocols and an application programming model based on the World Wide Web (WWW). Its hierarchical structure is quite similar to the TCP/IP protocol stack design.

What is Wireless Application Protocol (WAP)?

WAP stands for Wireless Application Protocol. It is a protocol designed for micro-browsers and it enables access to the internet in mobile devices. It uses the markup language WML (Wireless Markup Language and not HTML), WML is defined as an XML 1.0 application. It enables the creation of web applications for mobile devices. In 1998,

WAP Forum was founded by Ericson, Motorola, Nokia and Unwired Planet whose aim was to standardize the various wireless technologies via protocols. WAP protocol resulted from the joint efforts of the various members of WAP Forum. In 2002, WAP forum was merged with various other forums in the industry resulting in the formation of

Open Mobile Alliance (OMA)

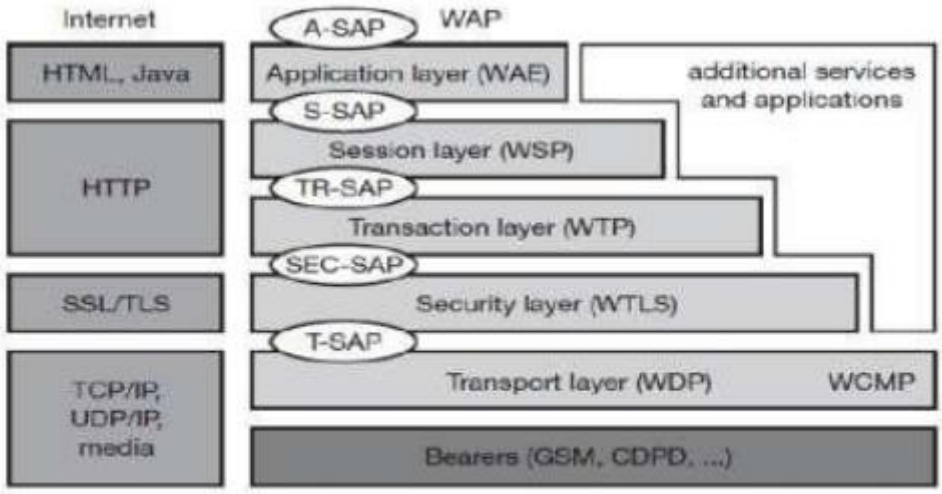


Fig 4.1 Components and Interface of WAP Architecture

WAP Model

The user opens the mini-browser in a mobile device. He selects a website that he wants to view. The mobile device sends the URL encoded request via network to a WAP gateway using WAP protocol.

The WAP gateway translates this WAP request into a conventional HTTP URL request and sends it over the internet. The request reaches to a specified web server and it processes the request just as it would have processed any other request and sends the response back to the mobile device through WAP gateway in WML file which can be seen in the micro-browser.

WAP Protocol stack

1. **Application Layer:** This layer contains the Wireless Application Environment (WAE). It contains mobile device specifications and content development programming languages like WML.
2. **Session Layer:** This layer contains Wireless Session Protocol (WSP). It provides fast connection suspension and reconnection.
3. **Transaction Layer:** This layer contains Wireless Transaction Protocol (WTP). It runs on top of UDP (User Datagram Protocol) and is a part of TCP/IP and offers transaction support.
4. **Security Layer:** This layer contains Wireless Transport Layer Security (WTLS). It offers data integrity, privacy and authentication.
5. **Transport Layer:** This layer contains Wireless Datagram Protocol. It presents consistent data format to higher layers of WAP protocol stack.

Why Use WAP?

The following advantages for wireless network operators, content producers, and end users were put out by WAP when it was first introduced in 1999:

Operators of wireless networks and mobile phones: WAP was created with the intention of enhancing already-existing wireless data services, such as voicemail, and facilitating the creation of new mobile applications. Without making any further infrastructure adjustments or phone modifications, these applications might be created.

Content Provider: For third-party application developers, WAP opened up a market for extra applications and mobile phone features. It was suggested that developers use the WML programming language to write applications for mobile devices.

End users: Access to online services like banking, entertainment, messaging, and other information on mobile devices should be simple and safe for users of mobile phones. WAP could also permit access.

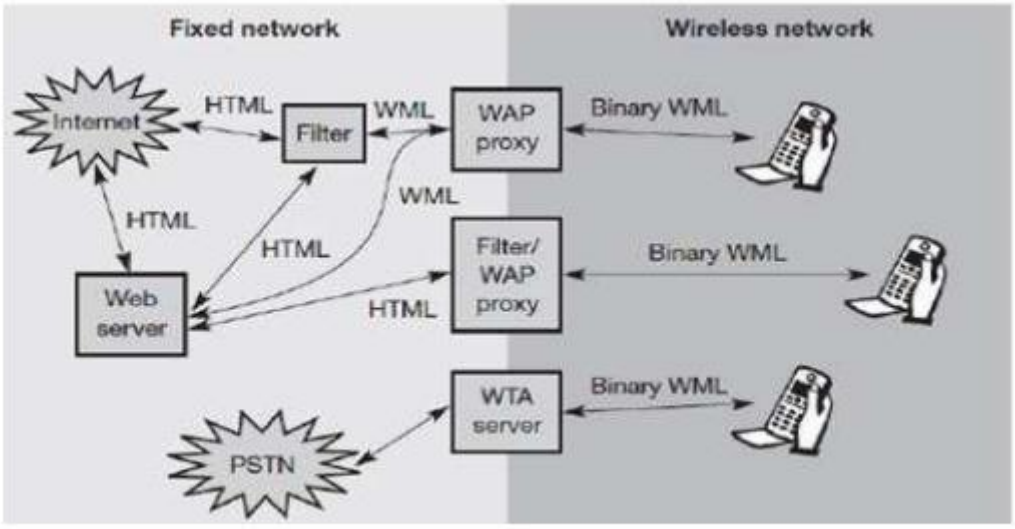


Fig 4.2 Examples of Integration of WAP Components

Advantages of Wireless Application Protocol

The benefits of Wireless Application Protocol, or WAP, are listed below:

- WAP is a rapidly evolving technology.
- Wireless Application Protocol is an open source that is totally free of cost.
- WAP can be used over multiple platforms.
- Neither it nor network standards are affected.
- Higher controlling possibilities are offered.
- It follows a model that is similar to the Internet.
- You can send and receive real-time data with WAP.
- WAP is supported by the majority of current mobile phones and devices.

Disadvantages of Wireless Application Protocol

The following is a list of various Wireless Application Protocol, or WAP, drawbacks:

- WAP connection speed is slow and number of connections are less.
- At some places it is very difficult to access the Internet, and also at some places it is totally impossible.
- Less secure.
- WAP provides a small User interface (UI)

Wireless Datagram Protocol (WDP)

The Wireless Datagram Protocol (WDP) operates on top of many different bearer services capable of carrying data. At the T-SAP WDP offers a consistent datagram transport service independent of the underlying bearer. To offer this consistent service, the adaptation needed in the transport layer can differ depending on the services of the bearer. The closer the bearer service is to IP, the smaller the adaptation can be. If the bearer already offers IP services, UDP is used as WDP. WDP offers more or less the same services as UDP.WDP offers source and destination port numbers used for multiplexing and demultiplexing of data respectively. The service primitive to send a datagram is TDUnitdata.req with the destination address (DA), destination port (DP), Source address (SA), source port (SP), and user data (UD) as mandatory parameters (see Figure 10.11). Destination and source address are unique addresses for the receiver and sender of the user data. These could be MSISDNs (i.e., a telephone number), IP addresses, or any other unique identifiers. The T-DUnitdata.ind service primitive indicates the reception of data. Here destination address and port are only optional parameters.

If a higher layer requests a service the WDP cannot fulfill, this error is indicated with the T-DError.ind service primitive as shown in Figure 10.11. An error code (EC) is returned indicating the reason for the error to the higher layer. WDP is not allowed to use this primitive to indicate problems with the bearer service. It is only allowed to use the primitive to indicate local problems, such as a user data size that is too large. If any errors happen when WDP datagram‘s are sent from one WDP entity to another (e.g. the destination is unreachable, no application is listening to the specified destination port etc.), the wireless control message protocol (WCMP) provides error handling mechanisms for WDP and should therefore be implemented. WCMP contains control messages that resemble the internet control message protocol messages and can also be used for diagnostic and informational purposes.

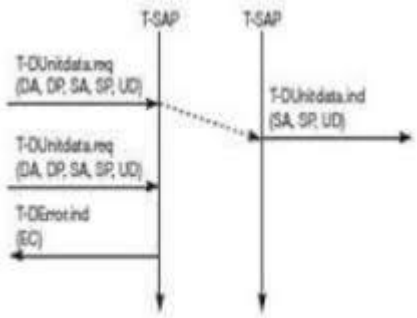


Fig 4.3 WAP Service Primitives

WCMP can be used by WDP nodes and gateways to report errors. However, WCMP error messages must not be sent as response to other WCMP error messages. In IP-based networks, ICMP will be used as WCMP (e.g., CDPD, GPRS). Typical WCMP messages are destination unreachable (route, port, address unreachable), parameter problem (errors in the packet header), message too big, reassembly failure, or echo request/reply. An additional

WDP management entity supports WDP and provides information about changes in the environment, which may influence the correct operation of WDP. Important information is the current configuration of the device, currently available bearer services, processing and memory resources etc. Design and implementation of this management component is considered vendor-specific and is outside the scope of WAP.

If the bearer already offers IP transmission, WDP (i.e., UDP in this case) relies on the segmentation (called fragmentation in the IP context) and reassembly capabilities of the IP layer as specified in (Postal, 1981a). Otherwise, WDP has to include these capabilities, which is, e.g., necessary for the GSM SMS. The WAP specification provides many more adaptations to almost all bearer services currently available or planned for the future (WAP Forum, 2000q), (WAP Forum, 2000b)

Wireless Transport Layer Security (WTLS)

If requested by an application, a security service, the wireless transport layer security (WTLS), can be integrated into the WAP architecture on top of WDP as specified in (WAP Forum, 2000c). WTLS can provide different levels of security (for privacy, data integrity, and authentication) and has been optimized for low bandwidth, high-delay bearer networks. WTLS takes into account the low processing power and very limited memory capacity of the mobile devices for cryptographic algorithms. WTLS supports datagram and

connection-oriented transport layer protocols. New compared to, e.g. GSM, is the security relation between two peers and not only between the mobile device and the base station . WTLS took over many features and mechanisms from TLS (formerly SSL, secure sockets layer, but it has an optimized handshaking between the peers.

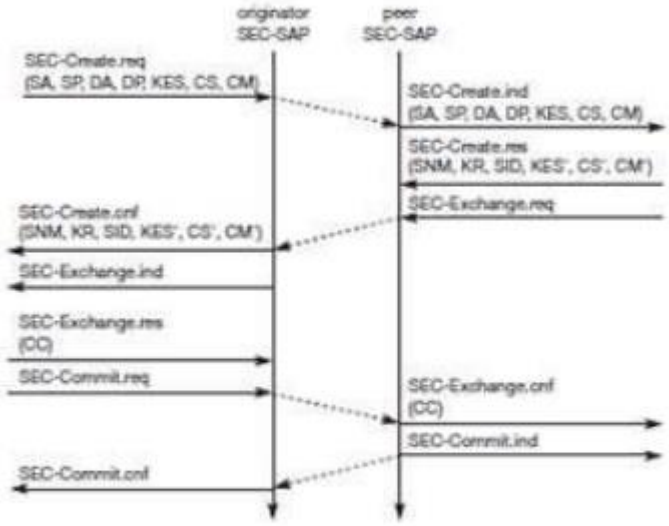


Fig 4.4 WTLS establishing a Secure Session

Before data can be exchanged via WTLS, a secure session has to be established. This session establishment consists of several steps: Figure illustrates the sequence of service primitives needed for a so-called ‗full handshake' (several optimizations are possible).

The originator and the peer of the secure session can both interrupt session establishment any time, e.g., if the parameters proposed are not acceptable.

The first step is to initiate the session with the SEC-Create primitive. Parameters are source address (SA), source port (SP) of the originator, destination address (DA), destination port (DP) of the peer. The originator proposes a key exchange suite (KES) (e.g., RSA, DH, ECC, a cipher suite (CS) (e.g., DES, IDEA, and a compression method (CM) (currently not further specified). The peer answers with parameters for the sequence number mode (SNM), the key refresh cycle (KR) (i.e., how often keys are refreshed within this secure session), the session identifier (SID) (which is unique with each peer), and the selected key exchange suite (KES'), cipher suite (CS'), compression method (CM'). The peer also issues a SEC-Exchange primitive. This indicates that the peer wishes to perform public-key authentication with the client, i.e., the peer requests a client certificate (CC) from the originator.

The first step of the secure session creation, the negotiation of the security parameters and suites, is indicated on the originator's side, followed by the request for a certificate. The originator answers with its certificate and issues a SEC-Commit.req primitive.

This primitive indicates that the handshake is completed for the originator‘s side and that the originator now wants to switch into the newly negotiated connection state. The certificate is delivered to the peer side and the SEC-Commit is indicated. The WTLS layer of the peer sends back a confirmation to the originator. This concludes the full handshake for secure session setup.

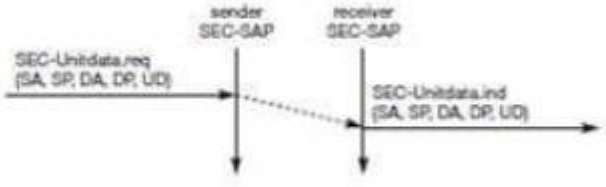


Fig 4.5 WTLS Datagram Transfer

After setting up a secure connection between two peers, user data can be exchanged. This is done using the simple SEC-Unit data primitive as shown in Figure 10.13. SEC-Unit data has exactly the same function as T-D Unit data on the WDP layer, namely it transfers a datagram between a sender and a receiver. This data transfer is still unreliable, but is now secure. This shows that WTLS can be easily plugged into the protocol stack on top of WDP. The higher layers simply use SEC-Unit data instead of T-D Unit data. The parameters are the same here: source address (SA), source port (SP), destination address (DA), destination port (DP), and user data (UD).

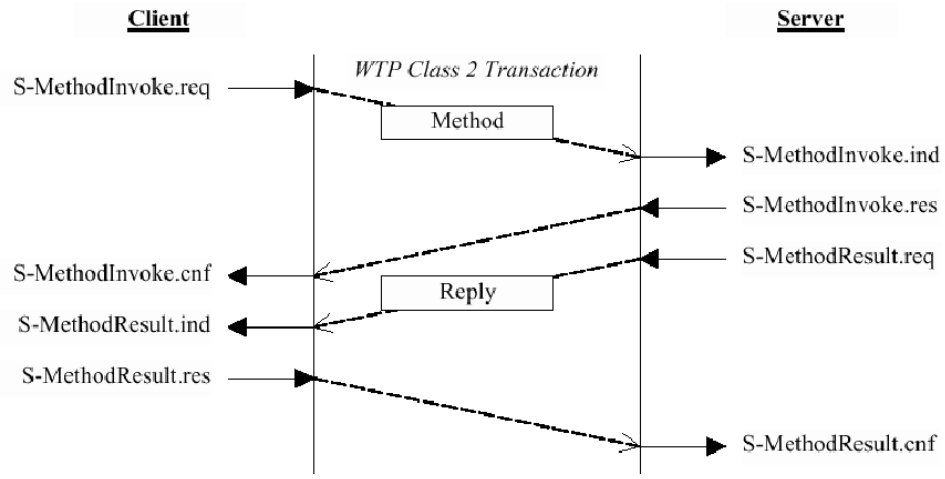
This section will not discuss the security-related features of WTLS or the pros and cons of different encryption algorithms. The reader is referred to the specification and excellent cryptography literature. Although WTLS allows for different encryption mechanisms with different key lengths, it is quite clear that due to computing power on the handheld devices the encryption provided cannot be very strong. If applications require stronger security, it is up to an application or a user to apply stronger encryption on top of the whole protocol stack and use WTLS as a basic security level only. Many programs are available for this purpose. It is important to note that the security association in WTLS exists between the mobile WAP-enabled devices and a WAP server or WAP gateway only. If an application accesses another server via the gateway, additional mechanisms are needed for end-to-end security. If for example a user accesses his or her bank account using WAP, the WTLS security association typically ends at the

WAP gateway inside the network operator‘s domain. The bank and user will want to apply additional security mechanisms in this scenario.

Future work in the WTLS layer comprises consistent support for application level security (e.g. digital signatures) and different implementation classes with different capabilities to select from.

Wireless session protocol (WSP)

The wireless session protocol (WSP) has been designed to operate on top of the datagram service WDP or the transaction service WTP (WAP Forum, 2000e). For both types, security can be inserted using the WTLS security layer if required. WSP provides a shared state between a client and a server to optimize content transfer. HTTP, a protocol WSP tries to replace within the wireless domain, is stateless, which already causes many problems in fixed networks. Many web content providers therefore use cookies to store some state on a client machine, which is not an elegant solution. State is needed in web browsing, for example, to resume browsing in exactly the same context in which browsing has been suspended. This is an important feature for clients and servers. Client users can continue to work where they left the browser or when the network was interrupted, or users can get their customized environment every time they start the browser. Content providers can customize their pages to clients‘ needs and do not have to retransmit the same pages over and over again. WSP offers the following general features needed for content exchange between cooperating clients and servers:



● **Session management:** WSP introduces sessions that can be established from a client to a server and may be long lived. Sessions can also be released in an orderly manner. The capabilities of suspending and resuming a session are important to mobile applications. Assume a mobile device is being switched off – it would be useful for a user to be able to continue operation at exactly the point where the device was switched off. Session lifetime is independent of transport connection lifetime or continuous operation of a bearer network.

B) Capability negotiation: Clients and servers can agree upon a common level of protocol functionality during session establishment. Example parameters to negotiate are maximum client SDU size, maximum outstanding requests, protocol options, and server SDU size.

c) Content encoding: WSP also defines the efficient binary encoding for the content it transfers. WSP offers content typing and composite objects, as explained for web browsing. While WSP is a general-purpose session protocol, WAP has specified the wireless session protocol/browsing (WSP/B) which comprises protocols and services most suited for browsing-type applications. In addition to the general features of WSP, WSP/B offers the following features adapted to web browsing:

d) HTTP/1.1 functionality: WSP/B supports the functions HTTP/1.1 offers, such as extensible request/reply methods, composite objects, and content type negotiation. WSP/B is a binary form of HTTP/1.1. HTTP/1.1 content headers are used to define content type, character set encoding, languages etc., but binary encodings are defined for well-known headers to reduce protocol overheads.

e) Exchange of session headers: Client and server can exchange request/reply headers that remain constant over the lifetime of the session. These headers may include content types, character sets, languages, device capabilities, and other static parameters. WSP/B will not interpret header information but passes all headers directly to service users.

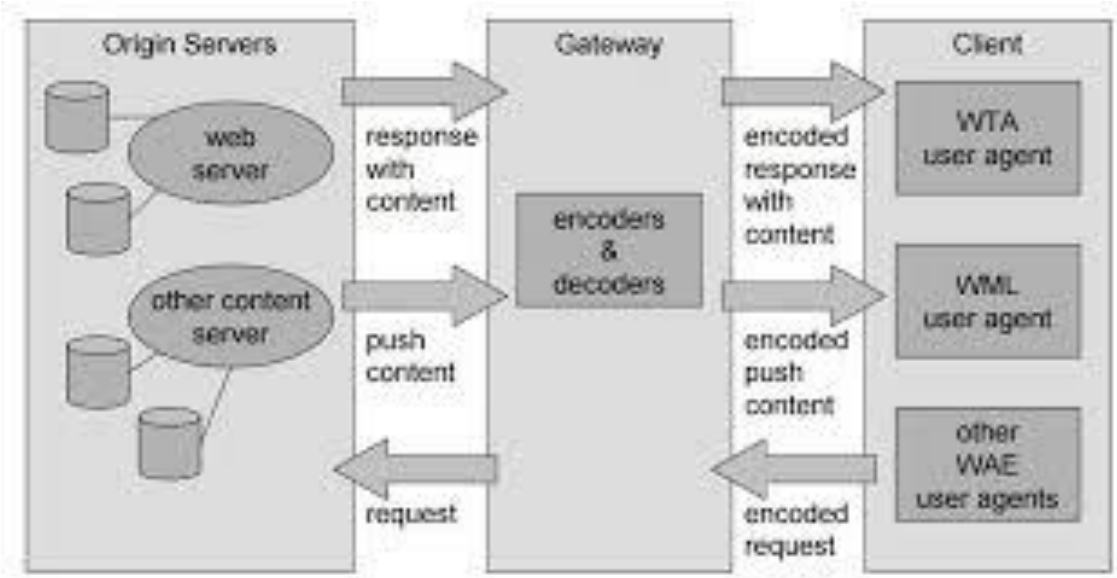
f) Push and pull data transfer: Pulling data from a server is the traditional mechanism of the web. This is also supported by WSP/B using the request/response mechanism from HTTP/1.1. Additionally, WSP/B supports three push mechanisms for data transfer: a confirmed data push within an existing session context, a non-confirmed data push within an existing session context, and a non-confirmed data push without an existing session context.

g) Asynchronous requests: Optionally, WSP/B supports a client that can send multiple requests to a server simultaneously. This improves efficiency for the requests and replies can now be coalesced into fewer messages. Latency is also improved, as each result can be sent to the client as soon as it is available.

As already mentioned, WSP/B can run over the transaction service WTP or the datagram service WDP. The following shows several protocol sequences typical for session management, method invocation, and push services.

WAE(Wireless Application Environment)

The main idea behind the wireless application environment (WAE) is to create a general-purpose application environment based mainly on existing technologies and philosophies of the world wide web. This environment should allow service providers, software manufacturers, or hardware vendors to integrate their applications so they can reach a wide variety of different wireless platforms in an efficient way. However, WAE does not dictate or assume any specific man-machine-interface model, but allows for a variety of devices, each with its own capabilities and probably vendor-specific extras (i.e., each vendor can have its own look and feel). WAE has already integrated the following technologies and adapted them for use in a wireless environment with low power handheld devices.



HTML, JavaScript, and the handheld device markup language HDML form the basis of the wireless markup language (WML) and the scripting language WML script. The exchange formats for business cards and phone books vCard and for calendars vCalendar have been included. URLs from the web can be used. A wide range of mobile telecommunication technologies have been adopted and integrated into the wireless telephony application (WTA).

Besides relying on mature and established technology, WAE focuses on devices with very limited capabilities, narrow-band environments, and special security and access control features. The first phase of the WAE specification developed a whole application suite, especially for wireless clients as presented in the following sections. Future developments for the WAE will include extensions for more content formats, integration of

further existing or emerging technologies, more server-side aspects, and the integration of intelligent telephone networks.

One global goal of the WAE is to minimize over-the-air traffic and resource consumption on the handheld device. This goal is also reflected in the logical model underlying WAE (Figure 10.29) showing some more detail than the general overview in Figure 10.10. WAE adopts a model that closely follows the www model, but assumes additional gateways that can enhance transmission efficiency.

A client issues an encoded request for an operation on a remote server. Encoding is necessary to minimize data sent over the air and to save resources on the handheld device as explained together with the languages WML and WMLscript. Decoders in a gateway now translate this encoded request into a standard request as understood by the origin servers. This could be a request to get a web page to set up a call. The gateway transfers this request to the appropriate origin server as if it came from a standard client. Origin servers could be standard web servers running HTTP and generating content using scripts, providing pages using a database, or applying any other (proprietary) technology. WAE does not specify any standard content generator or server, but assumes that the majority will follow the standard technology used in today‘s www.

The origin servers will respond to the request. The gateway now encodes the response and its content (if there is any) and transfers the encoded response with the content to the client. The WAE logical model not only includes this standard request/response scheme, but it also includes push services. Then an origin server pushes content to the gateway. The gateway encodes the pushed content and transmits the encoded push content to the client.

Several user agents can reside within a client. User agents include such items as: browsers, phonebooks, message editors etc. WAE does not specify the number of user agents or their functionality, but assumes a basic WML user agent that supports WML, WML script, or both (i.e., a _WML browser‘). Further domain specific user agents with varying architectures can be implemented. Again, this is left to vendors. However, one more user agent has been specified with its fundamental services, the WTA user agent. This user agent handles access to, and interaction with, mobile telephone features (such as call control). As over time many vendor dependent user agents may develop, the standard defines a user agent profile (UAProf), which describes the capabilities of a user agent. Capabilities may be related to hardware or software.

Examples are: display size, operating system, browser version, processor, memory size, audio/video codec, or supported network types. The basic languages WML and WML Script , and the WTA will be described in the following three sections.

WTA Architecture

Browsing the web using the WML browser is only one application for a handheld device user. Say a user still wants to make phone calls and access all the features of the mobile phone network as with a traditional mobile phone. This is where the wireless telephony application (WTA), the WTA user agent (as shown in Figure), and the wireless telephony application interface WTAI come in. WTA is a collection of telephony specific extensions for call and feature control mechanisms, merging data networks and voice networks.

The WTA framework integrates advanced telephony services using a consistent user interface (e.g., the WML browser) and allows network operators to increase accessibility for various special services in their network. A network operator can reach more end-devices using WTA because this is integrated in the wireless application environment (WAE) which handles device-specific characteristics and environments. WTA should enable third-party developers as well as network operators to create network-independent content that accesses the basic features of the bearer network. However, most of the WTA functionality is reserved for the network operators for security and stability reasons.

WTA extends the basic WAE application model in several ways:

● **Content push**: A WTA origin server can push content, i.e., WML decks or WMLScript, to the client. A push can take place without prior client request. The content can enable, e.g., the client to handle new network events that were unknown before.

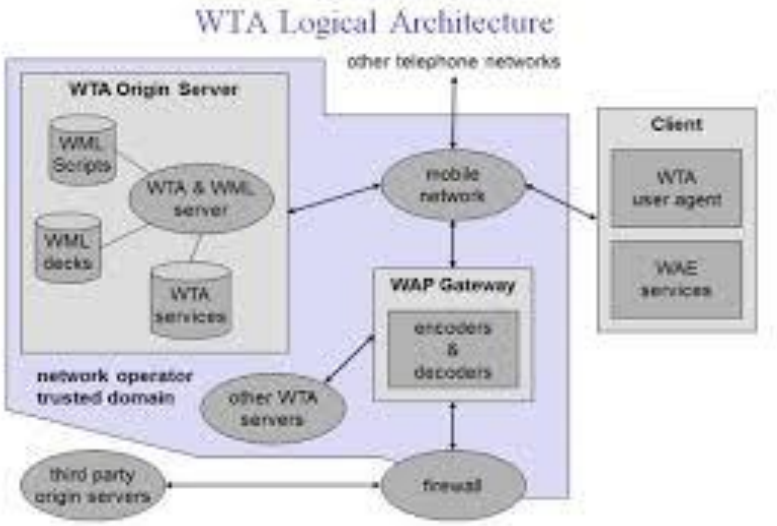
● **Access to telephony functions:** The wireless telephony application interface (WTAI, WAP Forum, 2000m) provides many functions to handle telephony events (call accept, call setup, change of phone book entries etc.).

● **Repository for event handlers:** The repository represents a persistent storage on the client for content required to offer WTA services. Content are either channels or resources. Examples for resources are WML decks, WMLScript objects, or WBMP pictures. Resources are loaded using WSP or are pre-installed. A channel comprises references to resources and is associated with a lifetime. Within this lifetime, it is guaranteed that all resources the

channel points to are locally available in the repository. The motivation behind the repository is the necessity to react very quickly for time-critical events (e.g., call accept). It would take too long to load content from a server for this purpose.

● **Security model:** Mandatory for WTA is a security model as many frauds happen with wrong phone numbers or faked services. WTA allows the client to only connect to trustworthy gateways, which then have to check if the servers providing content are authorized to send this content to the client. Obviously, it is not easy to define trustworthy in this context. In the beginning, the network operator‟s gateway may be the only trusted gateway and the network operator may decide which servers are allowed to provide content. Figure 10.30 gives an overview of the WTA logical architecture.

The components shown are not all mandatory in this architecture; however, firewalls or other origin servers may be useful. A minimal configuration could be a single server from the network operator serving all clients. The client is connected via a mobile network with a WTA server, other telephone networks (e.g., fixed PSTN), and a WAP gateway. A WML user agent running on the client or on other user agents is not shown here.



The client may have voice and data connections over the mobile network. Other origin servers within the trusted domain may be connected via the WAP gateway. A firewall is useful to connect third-party origin servers outside the trusted domain. One difference between WTA servers and other servers besides security is the tighter control of QoS. A network operator knows (more or less precisely) the latency, reliability, and capacity of its mobile network and can have more control over the behavior of the services. Other servers, probably located in the internet, may not be able to give as good QoS guarantees as the network operator.

Similarly, the WTA user agent has a very rigid and real-time context management for browsing the web compared to the standard WML user agent. Figure shows an exemplary interaction between a WTA client, a WTA gateway, a WTA server, the mobile network (with probably many more servers) and a voice box server. Someone might leave a message on a voice box server as indicated. Without WAP, the network operator then typically generates an SMS indicating the new message on the voice box via a little symbol on the mobile phone. However, it is typically not indicated who left a message, what messages are stored etc. Users have to call the voice box to check and cannot choose a particular message. In a WAP scenario, the voice box can induce the WTA server to generate new content for pushing to the client. An example could be a WML deck containing a list of callers plus length and priority of the calls. The server does not push this deck immediately to the client, but sends a push message containing a single

URL to the client. A short note, e.g., —5 new calls are stored", could accompany the push message. The WTA gateway translates the push URL into a service indication and codes it into a more compact binary format. The WTA user agent then indicates that new messages are stored. If the user wants to listen to the stored messages, he or she can request a list of the messages.

This is done with the help of the URL. A WSP get requests the content the URL points to. The gateway translates this WSP get into an HTTP get and the server responds with the prepared list of callers.

After displaying the content, the user can select a voice message from the list. Each voice message in this example has an associated URL, which can request a certain WML card from the server. The purpose of this card is to prepare the client for an incoming call. As soon as the client receives the card, it waits for the incoming call. The call is then automatically accepted. The WTA server also signals the voice box system to set up a (traditional) voice connection to play the selected voice message. Setting up the call and accepting the call is shown using dashed lines, as these are standard interactions from the mobile phone network, which are not controlled by WAP.

WML(Wireless Markup Language)

WML stands for Wireless Markup Language (WML) which is based on HTML and HDML. It is specified as an XML document type. It is a markup language used to develop websites for mobile phones. While designing with WML, constraints of wireless devices such as small display screens, limited memory, low bandwidth of transmission and small resources have to be considered. WAP (Wireless Application Protocol) sites are different from normal HTML sites in the fact that they are monochromatic (only black and white), concise and has very small screen space, due to which content in the WAP sites will be only

the significant matter, much like how telegraph used to work in the olden days. The concept WML follows is that of a deck and card metaphor. A WML document is thought of as made up of many cards. Just like how cards can be grouped to form a deck, a WAP site has many cards. One card will be displayed at a time on the screen, just like how one page is displayed at a time in an HTML website. Many cards can be inserted into a WML document, and the WML deck is identified by a URL. To access the deck, the user can navigate using the WML browser, which fetches the deck as required.

Features of WML:

- **Text and Images:** WML gives a clue about how the text and images can be presented to the user. The final presentation depends upon the user. Pictures need to be in WBMP format and will be monochrome.
- **User Interaction:** WML supports different elements for input like password entry, option selector and text entry control. The user is free to choose inputs such as keys or voice.
- **Navigation:** WML offers hyperlink navigation and browsing history.
- **Context Management:** The state can be shared across different decks and can also be saved between different decks.

Problems Faced by a Web Application When Used With a Mobile and Wireless Environment:

1. HTTP:

- **Bandwidth and delay:** HTTP is not made for low bandwidth and high delay connections in mind. HTTP protocol headers are large and redundant as HTTP is uncompressed and stateless.
- **Caching:** Caching is disabled by content providers as client companies cannot get feedback if a cache is placed between a server and a client. Users suffer from downloading the same content repeatedly from the server as HTTP is stateless.
- **Posting:** Sending some content from a client to a server will create additional problems if the said client is disconnected at that moment.

2. HTML: HTML was designed for use in creating content for webpages of the World Wide Web (www). It was meant only for desktop initially. Thus, when used in hand-held devices, some problems arise:

- Small display and low-resolution.
- Limited User Interfaces.
- Low-Performance CPU.

Enhancements needed for use of HTML in wireless environments:

- Image scaling

- Content Transformation: Documents in PDF or PPS should be transformed into the plain text as PDF occupies more memory.
- Content Extraction: To avoid longer duration waits, some content like headlines can be extracted from the document and presented to the user. This lets the user decide which information alone needs to be downloaded.

Enhancements needed for use of HTTP in wireless environments:

- **Connection Re-use:** Client and server can be used the same TCP (Transmission Control Protocol) connection for several requests and responses. Pipelining can be used to improve performance.
- **Caching Enhancements:** A cache could store cacheable response to reduce response time and bandwidth for further responses. Caching can be done in the mobile client's web browser itself by using a client proxy. A network proxy can also be used on the network side.
- **Bandwidth Optimization:** HTTP supports compression and also negotiates the compression parameters and compression styles. This will allow partial transmissions.

WMLScript:

WMLScript is the client-side scripting language of WML in Wireless Application Protocol(WAP) and whose content is static. It is similar to JavaScript. It is optimized for low power devices and is a compiled language. Some of the standard libraries of WMLScript are Lang, Float, String, URL, WML Browser, Dialog, and WMLScript Crypto Library.

Declaring A WML Document and Cards: To create a WML document, type it in notepad, just like for HTML. The first line should be something like this:

```
<?xml version="1.0"?>
   <!DOCTYPE wml PUBLIC
"-//WAPFORUM//DTD WML 1.1//EN" "http://www.wapforum.org/DTD/wml_1.1.xml">
   <wml>
      <card id="index"
           title="My WAP Site Using WML"
           newcontext="true">
      </card>
   </wml>
```

Which tells the phone that it is going to interpret a WML document and the WML standards. A card with the ID contents (used for linking) will be generated and the output at the top of the screen will be. It is extremely important to close all WML tags, unlike HTML tags. If you

do not close a WML tag, a card will not open at all. You have to close both the **<card>** and **<wml>** tags.

Example: The code below shows a sample WML coding for a small WAP site with two cards and a link to an external website.

```
<?xml version="1.0"?>
   <!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.2//EN"
"-//WAPFORUM//DTD WML 1.1//EN" "http://www.wapforum.org/DTD/wml_1.1.xml">

   <wml>

      <!-- This is first card-->
      <card id="one" title="First Card">
         <h1> Geeksforgeeks </h1>
         <p>
            A Computer Science Portal for Geeks
         </p>
      </card>

      <!-- This is second card-->
      <card id="two" title="Second Card">
         <p>
            This is created by WML
         </p>
      </card>

   </wml>
```

Output:

Comparison of WML with HTML:

- WML is used only for WAP sites on mobile phones and can be hosted only be WAP hosts that support WML. HTML can be hosted by any web server.

- WML sites are monochrome, unlike HTML sites.
- Coding is similar in many aspects but a badly coded WAP site will definitely not run as compared to a badly coded HTML site.
- It is must to close all WML tags as compared to the more lenient HTML coding.
- There are no alignment tags like the ** tag** in WML, as in HTML. Instead, **<p align=”center”>** has to be used for aligning text in WML.
- There are problems when using old HTML tags like **
** which have no closing tag. To get around this in WML, some tags have a “/” put on the end like **
**.
- Only WBMP format monochrome images are supported in WML whereas there is no such restriction in HTML.

) layer.

Unit III

Mobile Telecommunication System

Syllabus

Global System for Mobile Communication (GSM) - General Packet Radio Service (GPRS) - Universal Mobile Telecommunication System (UMTS).

Contents

3.1 Global System for Mobile (GSM)

AU : June-16,17, Dec.-16,17,May-18

3.1.1 GSM Architecture

The group of special mobile is sometimes known as global system for mobile and it is a second generation cellular mobile standard. Actually in 1980's many mobile systems with closer carrier frequencies under analog mobile phone systems faced many interferences and other problems, in European counters. A better approach which is a second generation digital system is the global system for mobile with acronym 'GSM'. In the age before GSM European countries used various cellular mobile standards which were not much efficient. GSM was initially functioning in 900 MHz band of frequency. The group of special mobile committee was a functioning group of CEPT. In the year of 1992 GSM modified its name to "Global system for mobile communications". The standards setting for GSM was under European Technical Standards Institute (ETSI).

In European countries GSM was first marketed in the year 1991. After two years other countries also evinced interest in this digital standard used for cellular communications technology.

The main aim of GSM was to provide 'roaming facility' for subscribers and to follow ISDN guidelines. It provides voice services that are compatible with ISDN standards.

GSM lies under second generation systems, that replaced first generation analog systems. Considering satellite uplink and downlinks, GSM was deployed using 890-915 MHz for uplinks and 935 to 960 MHz for downlink transmissions. GSM system used in United States in the band of 1900 MHz was called as Personal Communications Services (PCS). There are many GSM solutions known as GSM 900, GSM 1800 etc.

3.1.1.1 GSM Phone - Functional Block Diagram

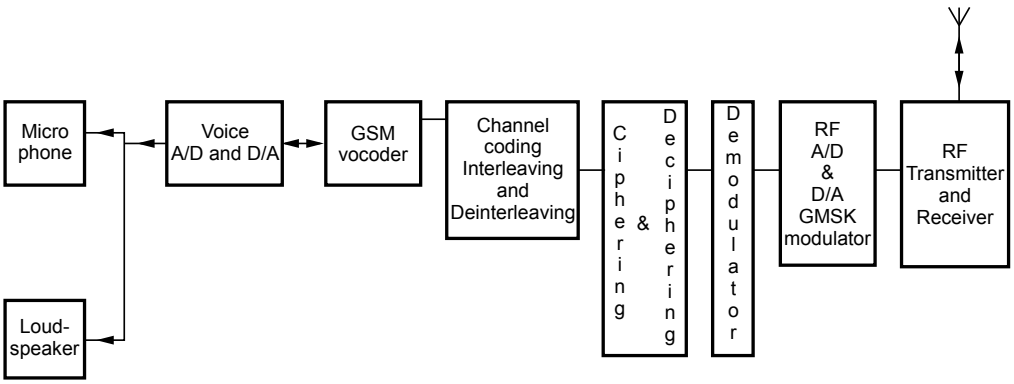


Fig. 3.1.1 GSM phone - functional block diagram

The global system for mobile (Group of Special Mobile) GSM phone functional block diagram is shown above. The transceiver antenna system receives or transmits RF signal. The analog to digital conversion and digital to analog conversions are done in opposite

directions depending upon transmission or reception. Microphone and loudspeakers are used in similar two directional ends.

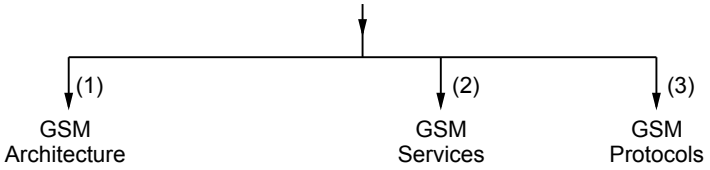
The channel coding is done with interleaving technique. Modulation and demodulation for transmission and reception. Equalization technique is also applied. Modulation scheme adopted is gaussian minimum shift keying digital modulation. The antenna is of MIMO (Multiple Input and Multiple Output) nature. User authentication is possible with GSM phones.

Depending upon the services provided by this standard there are six important category/examples.

1) Transactional service - Shopping - Booking	2) Travelling related services - Roaming - Weather	3) Personal service - Health monitoring - Budgeting
4) Mobile office - E-mail - Modem - Fax	5) Fun - Gambling - Online games	6) Security services - Emergency calls - Alarm provisions

There are three subtopics which are important under GSM.

In GSM architecture, the subsystems are



i) Network and Switching Subsystem (NSS)

ii) Radio Subsystem (RSS)

iii) Operation Support Subsystem (OSS)

3.1.1.2 Network and Switching Subsystem

The Network and Switching Subsystem (NSS) manages the connectivity between wireless networks and public networks. NSS contains

i) Mobile Services Switching Centre (MSC)

ii) Home Location Register (HLR)

iii) Visitor Location Register (VLR)

i) Mobile Services Switching Centre (MSC) :

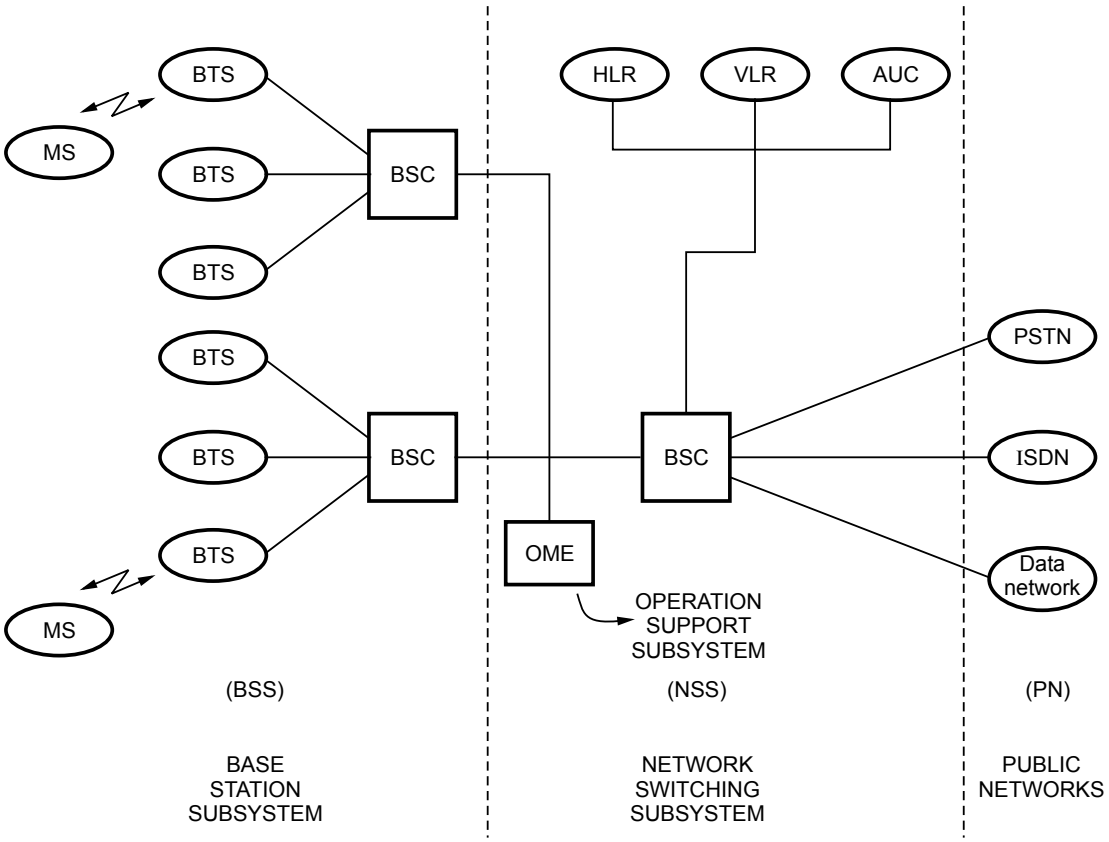


Fig. 3.1.2 GSM system architecture

The mobile switching centres acts as highly reliable ISDN switches. It establishes connections between BSC's and all other MSC's. A single MSC can manage many BSC's of a particular region. A typical gateway MSC is termed as GMSC and it has additional fixed networks like PSTN and ISDN.

ii) Home Location Register (HLR) :

The home location register is very important database used in GSM standard in the sense it consists of all user related information.

It consists of mobile subscriber ISDN number, the related services and authentication key facilities. The information regarding users (subscribers) are linked to it. HLR also involves itself with charging and accounting details of subscribers.

iii) Visitor Location Register (VLR) :

VLR is responsible for any visitors or new users entering the network. Whenever a new Mobile Subscriber (MS) enters the Local Area (LA) then visitor location register VLR has to take immediate action so that it copies all related information about that new user.

3.1.1.3 Radio Subsystem (RSS)

In GSM architecture the radio subsystem 'RSS' consists of two main parts.

i) Mobile stations ii) Base station subsystem

In a GSM network, it has many Base Station Subsystems (BSS's) where each one is controlled by a base station controller called 'BSC'. It is equipped to perform all functions which are important to maintain an individual mobile station. The BSS unit also consists of many base transceiver stations BTS's.

The base station controller can manage many BTS's. It can reserve many radio frequencies, handing over functions from one base transceiver station to another base transceiver station. It can also perform paging operation of MS. The multiplexing of many radio channels onto a fixed network is possible.

The subscriber identity module termed as 'SIM' with all user related information are available with Mobile Station (MS). The International Mobile Equipment Identity (IMEI) is used for identifying a mobile station in the network.

All authentication functions and specific user functions (e.g. charging) are possible only with SIM card.

Few important things contained in a SIM card are

1. Identifiers
2. Card type
3. Serial number
4. List of subscribed services
5. Personal Identity Number (PIN)
6. Authentication Key (K)
7. PIN Unblocking Key (PUK)
8. International Mobile Subscriber Identity (IMSI)
9. Compatible with locking of SIM in case of wrong PIN (for a three time trial).

3.1.1.4 Operation Subsystem (OSS)

All functions related to networking operations and maintenance are done by operation subsystem. Using the SS7 signalling the OSS can access other entities also.

It consists of

i) Operation and maintenance centre

ii) Authentication Centre (AuC)

iii) Equipment Identity Register (EIR)

i) Operation and Maintenance Centre (OMC)

The functions managed by the operation and maintenance systems are

1) Traffic monitoring

2) Subscriber and security management including billing

3) Status of network entities in a report form.

OMC is subjected to the concept of TMN Telecommunication Management Network, which is standardized by ITU-T. OMC monitors and maintains each MS, BSC, BS and MSC within entire GSM system.

It is also responsible for integrity and performance of each subscriber equipment within the system.

ii) Authentication Centre (AuC)

The user identification, protection of all user information are taken care of by authentication centre. It can also be kept safe as a part of Home Location Register (HLR).

iii) Equipment Identity Register (EIR)

EIR is responsible for all devices identification used in a network. It also maintains a list of stolen devices and malfunctioning devices.

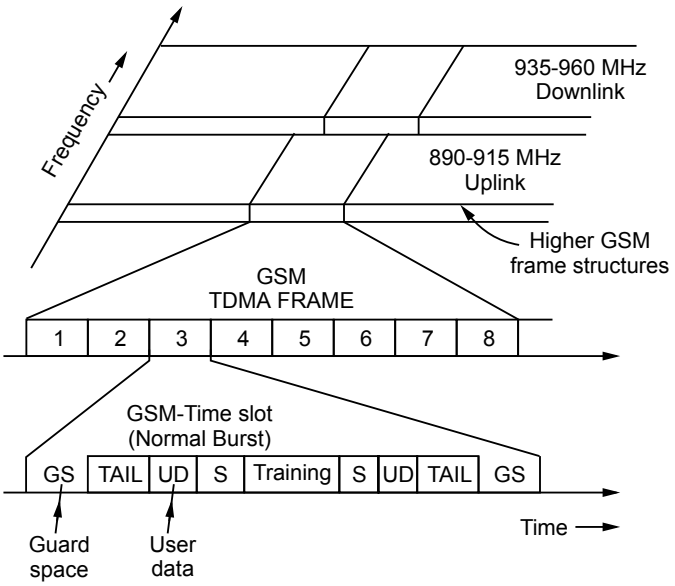


Fig. 3.1.3 GSM i) TDMA frame ii) Slots iii) Bursts

Significance of Radio Subsystem :

The frequency band used for uplink or (forward link) was 890-915 MHz and for downlink (Reverse link) was 935-960 MHz. The original frequency band for GSM was 25 MHz. The forward and reverse frequency bands are generally split into channels each with 200 kHz wide and they are known as Absolute Radio Frequency Channel Numbers (ARFCN's). It denotes forward and reverse channel pair and it is separated in the frequency of 45 MHz. TDMA concept can be used for time sharing to cover all subscribers.

Data can be transmitted as portions known as burst. It (time slot) will contain user and signalling information. The middle of the time slot of the GSM frame has the Training Sequence (TS) which is used to adapt the needed parameters of the receiver, and to select the strongest signal in multipath propagation environment.

3.1.1.5 Handover Procedure in GSM

When the mobile station moves out of the coverage range of Base Transceiver Station (BTS) handover is a must or when traffic is very high in a cell the handover is very important.

1) In Intracell handover the base station may decide to change carrier frequency while narrow band interference is high which disturbs transmission.
2) In the second case though the mobile station enters another cell it is still in the proper control of BSC of cell. In this case the BSC will change handover at the new carrier frequency of that new cell.
3) In case 3, GSM has to provide some handover functions between the cells those are controlled by different BSC's. This is because the BSC's can control only limited number of cells in a network. Then the handovers has to be controlled overall by the MSC.
4) In fourth case in Inter MSC handover, the handovers may be required between different MSC's.

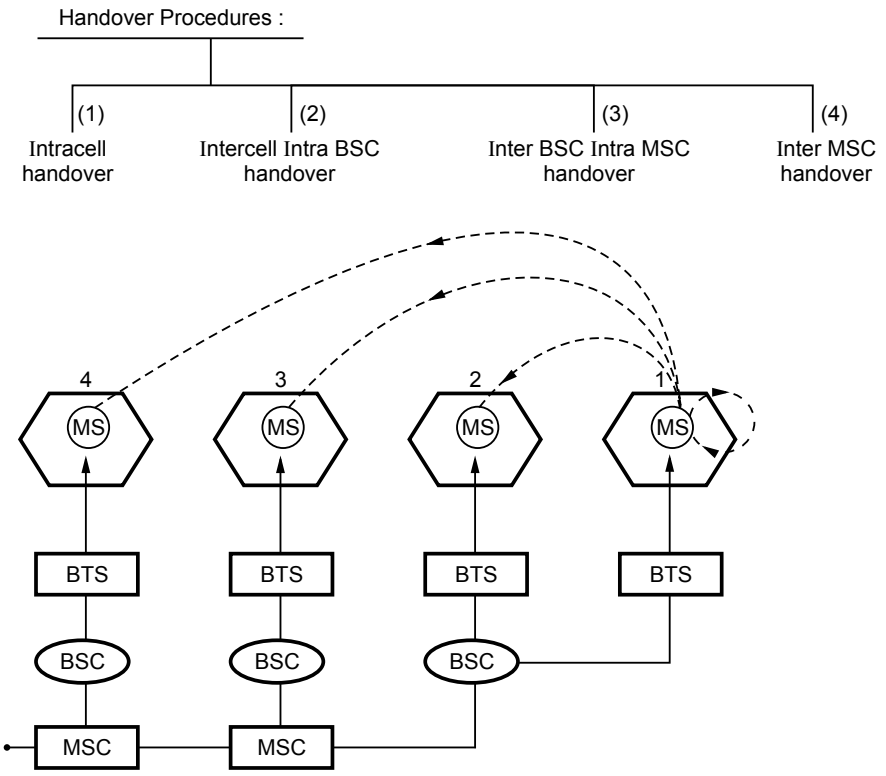
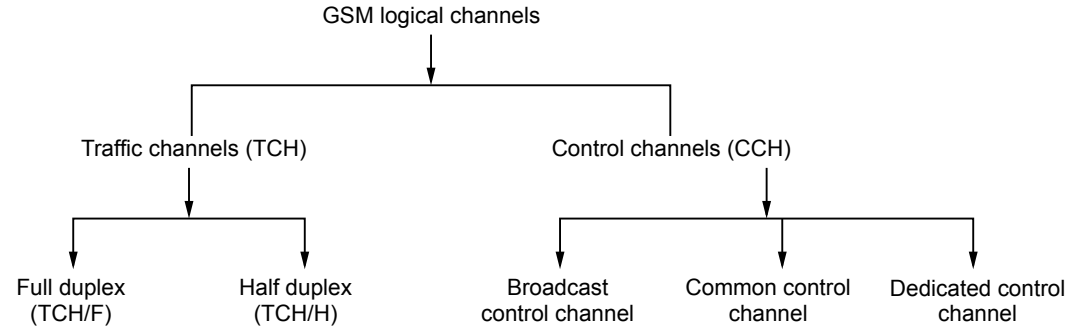


Fig. 3.1.4 Handover procedures

3.1.2 Channels

GSM has different types of logical channels and they are separated as traffic channels and control channels.



GSM uses traffic channels to transmit user data which can be voice, fax etc. This traffic channel may be full duplex or half duplex. For full duplex the data rate is 22.8 kb/sec and it is only 11.4 kb/sec in case of half duplex channels. For GSM standard a data rate of 13 kb/sec is good. If full duplex channel scheme is used 13 kb/sec is used for actual data transmission rate while the remaining is used for error correction purposes.

The control channels in GSM are responsible for mobility management.

3.1.2.1 Broadcast Control Channel

It is denoted as BCCH. It is used for signal information by Base Transceiver Station (BTS) to all MS, in a cell. There are few important channels known as Frequency Correction Channel (FCCH), Synchronization Channel (SCH). The FCCH is used for frequency correction information by BTS. SCH is helpful to transmit information about time synchronization. Basically FCCH and SCH are subchannels of BCCH.

The Common Control Channel (CCCH) is related to information transferring with respect to connection setup between BS and MS, (exchanged whenever required). Whenever a call has to be setup the MS seeks help of Random Access Channel (RACH) for sending data to base transceiver station. All channels described so far are unidirectional. The dedicated control channels are bidirectional.

The Dedicated Control Channels (DCCH) maintain a low data rate using Stand Alone Dedicated Control Channel (SDCCH) till the MS establishes TCH with the BTS. Signalling to MS regarding usage of TCH or SDCCH for connection setups BTS makes use of Access Grant Channel (AGCH), under common control channels. In DCCH there are SACCH and FACCH. The TCH and SDCCH has Slow Associated dedicated Control Channel (SACCH) and this channel is used for exchanging system information like signal power level and channel quality.

The channels (FACCH) are used for exchanging large amount of data in less period of time. Out of the three layers in GSM architecture the network layer plays a vital role in the sense it contains Radio Resource management (RR), Mobility Management (MM) and Call Management (CM).

The functions like call set, call maintenance and releasing radio channels are taken care by RR. Then registration, identification, authentication updating location, providing Temporary Mobile Subscriber Identity (TMSI replaces IMSI) are done by Mobility Management (MM). Finally the Call Management (CM) consists of three entities known as

a) Call Control (CC) b) Short Message Services (SMS)

c) Supplementary Services (SS)

Point to point connection establishment is possible in CM. It also provides functions to send in band tones known as Dual Tone Multiple Frequency (DTMF) over the entire GSM network. GSM is compatible with four 16 kbit/sec channels into a single channel of 64 kbit/sec and hence Pulse Code Modulation (PCM) can be applied for GSM. For signalling operations between BSC and MSC signalling system No. 7 (SS7) is used.

The advantage of using this GSM standard is its world wide localization of users facility. The particular phone number alloted is same and unique world wide and is quite a complex free design Roaming of subscribers between two providers in one country or in different countries is possible even with different providers.

To find or locate a MS the main features required are listed below :

i) International Mobile Subscriber Identity (IMSI)

ii) Mobile Station International ISDN Number (MSISDN)

iii) Temporary Mobile Subscriber Identity (TMSI)

iv) Mobile Station Roaming Number (MSRN)

Two opposite terms Mobile Terminated Call (MTC) and Mobile Originated Call (MOC) work very accurately in this network. MTC works in a situation where the calling station is outside the GSM network. MOC suits it to an environment when a call is purely initiated i.e. when MS transmits a request signal for a new connection in the GSM network.

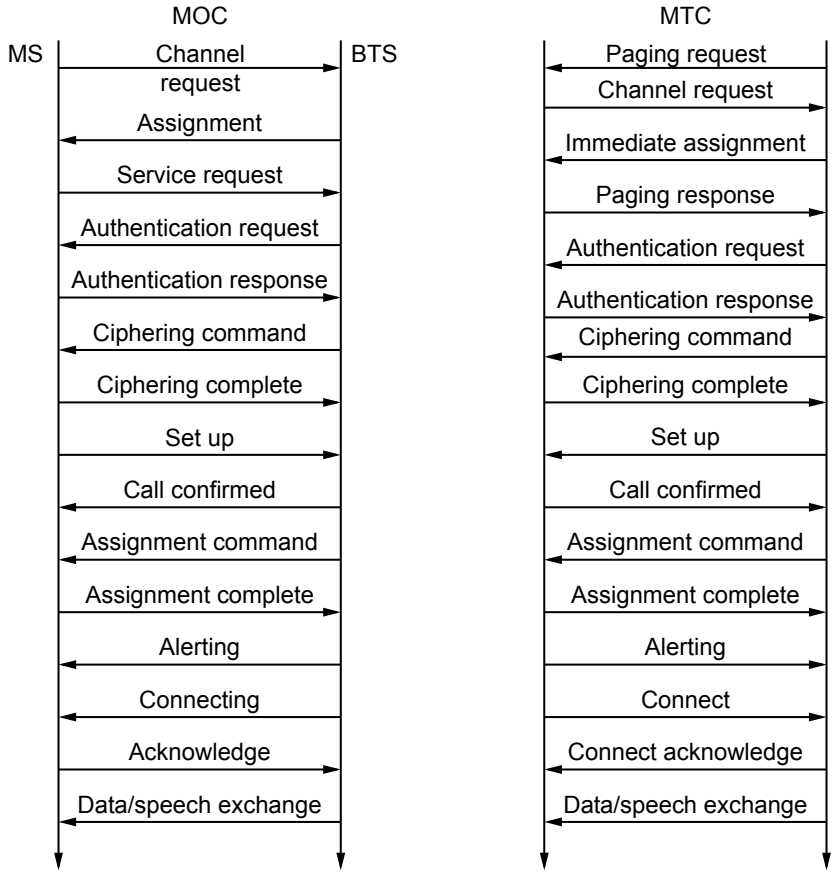


Fig. 3.1.5 Flow of message in MOC and MTC

The flow of messages for MTC and MOC under GSM are unique in nature.

In GSM network the movement of mobile station is around 250 km/hr. As the cell size is small (few kms) the faster will be the coverage done by MS.

3.1.3 Mobility Management

In mobile communication the mobile node changes its own physical location (i.e. address) in very less time. The mobility of user has to be strictly supervised so that it is easier to continue call communication smoothly. The methods of managing the mobility is hence very iportant. In such a procedure of mobility management there are two important types known as,

i) Location management. ii) Hand off management.

The location management procedure has two operations i.e. search and update.

Search operation : It is invoked by a node which needs connection establishment with that of a mobile node.

Update operation : It is also called as registration operation that is it gives information about the node's current location. The search operation is supported by the update operation. The search overhead (Cost) mainly depends on granularity and currency of the location information. Also organization of the location databases, location registrars is important because it stores the location related informations of the nodes.

Handoff management is the second task after performing location management. The aim of the technique is to ensure the connectivity of the network with the mobile node. The handoff procedure involves many subtasks. Like,

i) Deciding the time of handoff to access point.

ii) Choosing new access point from many access points in mobile node's vicinity.

iii) Getting resources (channels)

iv) Sending information to old access point so that it can reroute the packets.

The decision to make handoff initiated by two methods,

i) Either by the mobile node [Mobile Controlled Handoff (MCHO)].

ii) By the Access Point (AP) [Network Controlled Handoff (NCHO)]

It depends on many factors such as,

a) Quality of mobile communication between AP and mobile node.

b) Load on current AP that is running out of the communication channels.

The CDMA based technology assumes accurate and smooth handoffs.

Selecting a base station to which the handoff has to be made depends on few factors like,

i) SNR of beacon signals from access points.

ii) Mobile node's region may move in very short time intervals.

iii) Availability of the resources at the access point.

The main resources that has to be acquired in new cell are uplink and downlink channels.

Location management	- It assists in establishing new connections.
Handoff management.	- It ensures the connectivity of the mobile node with the network.

Both the operations completes mobility management.

Location management principles : The location management schemes uses many databases known as location registrars for maintaining the locations and other related information like service profile and preferences. One of the simple location management

scheme which uses single location registrar is known as Home Location Registrar (HLR). It maintains location information of all mobile nodes in the network.

As a whole simple location management scheme performs both search and update functions.

Design issues : To perform better location management an average time for which mobile node stays within a cell is known as cell residency time. It has be calculated accurately. The periodic time-based updates (dynamic updates) has to be monitored.

- As a mobile node is switched on then its HLR has to notified to ensure the current position of the node.
- To find the current location of mobile node first its HLR is notified and then the HLR contacts the current base station of cell where the node is available.

Dynamic update schemes :

The Registration Areas (RA) based location updates is a static update scheme. It does not include measurements of dynamic mobilities of the mobile node. Boundaries of RAs found with the aggregate mobility information patterns of mobile nodes.

The static boundaries leads to many location updates of mobile nodes two adjacent RAs. These type of ping-pong effects are avoided in dynamic update procedures.

The periodic updates are dynamic updates. They are example of dynamic update scheme. Apart from this there are some more dynamic update schemes. They are ;

i) Movement-based updates.

ii) Distance-based updates.

Both the methods are dynamic location update schemes.

Note To avoid roaming mobile node's location very often the technique known as per-user location caching can be used. For efficient implementation of the caching scheme the two parameters to consider are,

i) Location at which registrars has to be informed for caching.

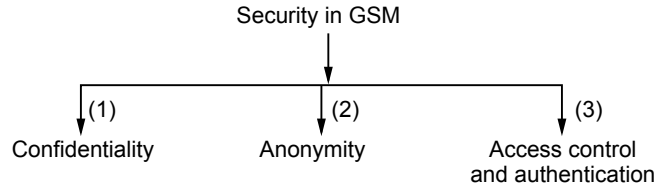
ii) At what time the location information has to be cached ?

The location information can be replicated. Partial replication is done under two organizations of location registrars. They are hierarchical and flat organization.

These location management procedures ensures the current location of the node. It is followed by the second task handoff procedure. Hence in mobility management both location and handoff management are done.

3.1.4 Security in GSM

The degree of security in GSM is higher with respect confidentiality information in Subscriber Identity Module (SIM) and Authentication Centre (AuC). Any unauthorised trial will be disabled and a PIN is maintained in this aspect.



1) Confidentiality :

To maintain confidentiality encryption and decryption techniques are used. The information about user (subscriber) is encrypted. Only an authorized person can decrypt it.

2) Encryption :

All information that are user related are encrypted. This ensures more privacy from the point of subscribers. If authentication process is over the base transceiver station and mobile station can work with proper encryption by using cipher key say 'K_c'. The Subscriber Identity Module (SIM), MS and the network calculate the same key 'K_c' which is based on a particular random value and the key itself is not transmitted. The cipher key 'K_c' is not generated using an individual key 'K_i', but generated using some random value with a particular algorithm intended for this purpose. The Base Transceiver Station (BTS) and the Mobile Station (MS) can encrypt at one end and decrypt at the other end. For example cipher key of 64 bits, is used.

3) Authentication :

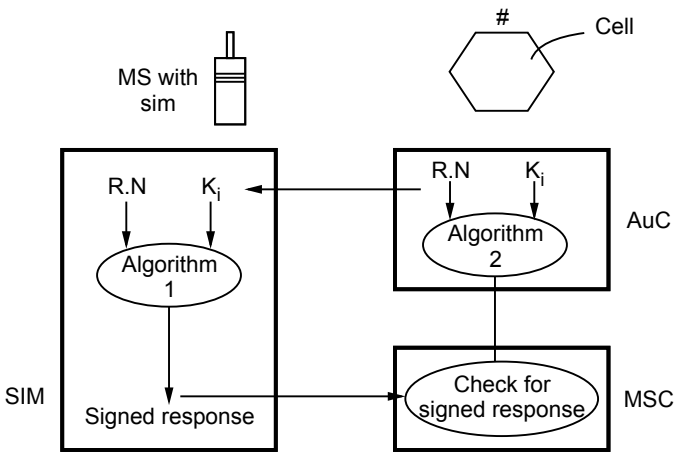


Fig. 3.1.6 Subscriber (user) authentication

Users can opt for any type of service that a GSM network can offer. The authentication is based on the SIM card that stores user related information. A Random Number (R.N) and Authentication Key (K_i) along with the specific algorithm is used for developing user authentication.

The access control generates a Random Number (R.N) and the SIM provides a signed response where Authentication Centre (AuC) does the basic generation of random values Random Number (R.N), signed response and secret key 'K_c'. Ultimately this is sent to Home Location Register (HLR). The visitor location register VLR sends random number R.N to the SIM where the subscriber and network does the same type of functions. When both match, the VLR will accept the subscriber (new) or simply it will reject it and hence higher user authentication is made possible in GSM networks.

Comparison of IS136, IS95 and GSM standards [2G standards].

Parameter	IS136	IS95	GSM
Year	1991	1993	1990
Type of access	TDMA	CDMA	TDMA
Spacing between forward and reverse channels	45 MHz	45 MHz	45 MHz
Bandwidth of channel	30 kHz	1250 kHz	200 kHz
Maximum power of mobile unit	3 W	0.2 W	20 W
Number of users per channels	3	35	8
Base station transmission band	869 MHz to 894 MHz	869 MHz to 894 MHz	935 to 960 MHz
Carrier signal bit rate	48.9 kbps	9.6 kbps	270.8 kbps
Bit rate of speech code	8 kbps	8/4/2/1 kbps	13 kbps
Frame size	40 msec	20 msec	4.6 msec

Table 3.1.1 Comparison of second generation mobile telephone systems

3.1.5 Mobile Number Portability (MNP)

The mobile number portability is related to routing of the mobile calls or sending messages (MMS or SMS) to a mobile number as it is ported. A central database (CDB) of the ported numbers is available. The network operator should copy the CDB status and has to decide which network should send a call to. This procedure is termed as All Call Query (ACQ) which is an efficient method with better scalability. The MNP systems follows the ACQ/CDB method for making call routing.

In case of decentralised model of the MNP a Flexible Number Register (FNR) can be used for managing database of ported in or ported out numbers for call routing procedures. Service providers uses HLR query services to findout the correct network of the cellular number whenever it routes messages and also voice calls to MNP enabled region.

The MNP provides more flexibility to the mobile users to change their service providers when required without changing their mobile number. The mobile gets attached to new service provider and the same number is used when the user is in roaming status.

The user can stay with his/her same cellular technology (GSM or CDMA). The MNP facility is allowed for both prepaid and postpaid users.

To port a number it would take sever working days (approx). The cost involved will be collected by the new service provider from the mobile user. One the service provider is changed it is expected to retain with this new provider atleast for three months period.

3.1.6 Tele-services in GSM

GSM provides voice-oriented tele-services. It comprises of encrypted voice transmission, data communication as PSTN, message services. The main goal of GSM is to provide high quality digital voice transmission. In GSM it offers emergency numbers. For an user the same number can be given and it can be used in entire Europe.

GSM provides simple short messaging services known as SMS where upto 160 characters transmission of message is possible. An extension of SMS, Enhanced Message Service (EMS) is allowed in which larger Message transmission upto 760 characters is permitted. Also next to EMS there is Multimedia Message Service (MMS) is provided by GSM. Here it offers larger picture transmission (GIF, JPG etc). Short video clippings can be sent.

A non-voice teleservice of GSM is group 3 fax service. In this fax data is sent as digital data. Using a transparent bearer service, fax data and fax signalling is done.

GSM hence provides many teleservices in the wireless network.

Note To increase the market value the MNP technique helps more by providing flexibility to mobile users.

3.2 General Packet Radio Service (GPRS) AU : June-16,17, Dec.-16

The General Packet Radio Service (GPRS) provides efficient packet mode of data transfer. GPRS is popular because it provides a cost effective packet services supporting internet applications.

GPRS allows other services like,

- Unicast
- Multicast and
- Broadcast

The important concepts of GPRS are :

i) The GSM system is capable of allocation time slots [from one to eight] in a time division multiplexing access frame for the GPRS radio channels.

ii) Demand based time slot allocation.

iii) Depending on a coding technique it is possible to have data rate up to 150 kbps with GPRS.

iv) The maximum data rate is not limited by GPRS.

v) GPRS is independent of the characteristics of radio channel.

vi) GPRS is dependent on type of the radio channel.

vii) GPRS supports point-to-point packet transfer service.

viii) With GPRS it is possible to maintain a virtual circuit within GSM network in case of change of the cells.

Security services provided by GPRS :

1. Access control
2. Authentication
3. User information confidentiality
4. User identity security

Reliability classes possible in GPRS (as per ETSI) :

Reliability Class	Service Data Unit (SDU)	SDU Probability	Duplicate SDU Probability
1	10^{-2}	10^{-2}	10^{-5}
2	10^{-4}	10^{-6}	10^{-5}
3	10^{-9}	10^{-9}	10^{-9}

GPRS provides many services without restricting data rates of transmission. The service precedence namely high, low, normal, reliability class, throughput and delay are determined by QoS profile. The delay in GPRS is mainly due to transmission delay and channel access delay in the network and GPRS does not append additional delay. Many security services like user authentication, access control, user information confidentiality,

user identity confidentiality are enabled with GPRS. There are also two important network elements available that plays a vital role in performance of GPRS.

They are GPRS support nodes called as GSN. There are many interfaces available for flexibility and system efficiency. The gateway GPRS support node acts between GPRS network and external Packet Data Networks (PDN). The CGSN is connected to other external networks like X.25 standard.

The General Packet Radio Service (GPRS) facilitates packet mode transfer for specific applications. This scheme involves a fully packet oriented data transmission.

For GPRS the GSM scheme allots between one and eight time slots within a TDMA frame structure. Demand assignment of time slots is possible and hence flexibility is high with GPRS. Fixed and preassigning of TDMA time slots is not a must. Point to point packet transfer service is allowed in GPRS which enables maintaining circuits in GSM network. A data rate of 150 kb/sec is generally met. The GPRS concept is not dependent on channel characteristics.

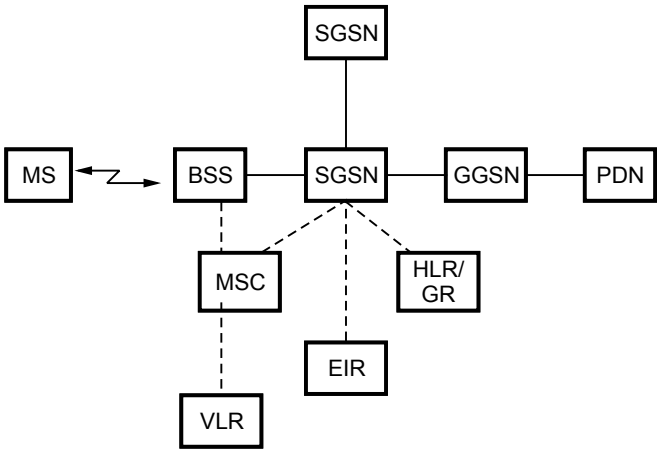


Fig. 3.2.1 'GPRS'-General packet radio service architecture

The data packets are transmitted from the PDN through the SGSN and GGSN which is directed to MS finally via BSS. The proper procedures of mobility management are also met. For data encryption purpose, a temporal identifier Temporal Logical Link Identity (TLLI) and a Ciphering Key Sequence Number (CKSN) are used. In GPRS transmission plane protocol structure, using the GPRS Tunnelling Protocol (GTP) all data transfer are done within GPRS (between GSN's). The reliable protocol TCP or

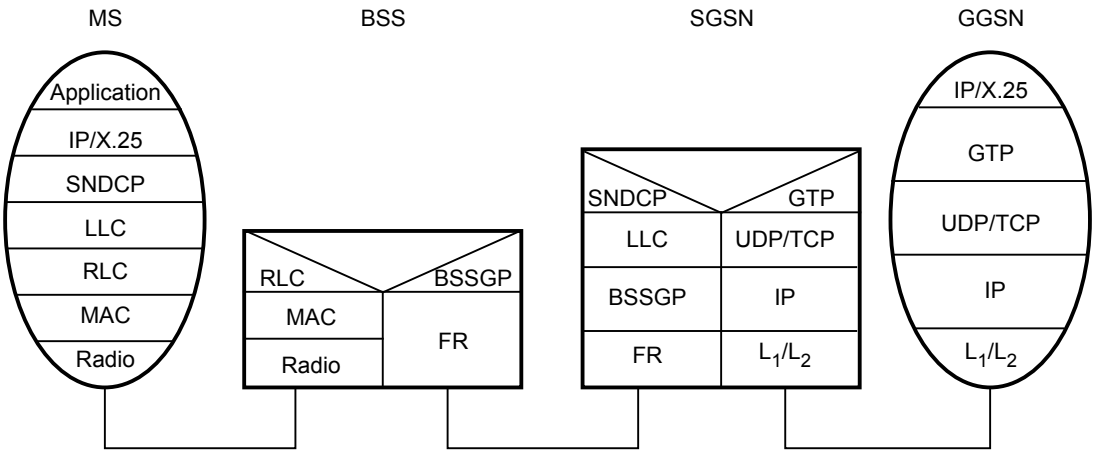


Fig. 3.2.2 GPRS - Transmission plane protocol-reference

non-reliable protocol namely UDP are two different protocols where any one of them can be used GTP. To adopt different characteristics of underlying networks in the system. Subnetwork Dependent Convergence Protocol (SNDCP) utilized between MS and SGSN.

Mainly the routing and QoS informations are sent with the help of Base Station Subsystem GPRS Protocol (BSSGP). Medium Access Control (MAC) with proper signalling procedures for radio channels and mapping the LLC frames with that of GSM channels and radio link protocol namely RLC facilitates reliable link.

The GPRS is an optimum and better system for transmission of packet-oriented data transmission.

3.2.1 PDP Context Procedure

The Packet Data Protocol (PDP) context provides a packet data connection with which Utran Equipment (UE) and the wireless network can exchange their IP packets. The usage of the packets data connections are restricted to particular services. They are accessed through access points. The PDP context is very important for UMTS packet data architecture.

To establish an end to end connection the PDP context has a record of the parameters that consists of required information.

Some of them are ;

i) PDP type.

ii) Address type of PDP.

iii) Quality of service (QoS) profile request.

iv) QoS parameters negotiable with network.

v) Type of authentication.

vi) Dynamic or static DNS (has to be selected)

The two main purposes for which PDP is designed for are listed below.

i) To allocate a PDP address, either a IPV4 or IPV6 (V-Versions) to the mobile terminal.

ii) To make a logical connection with that of the QoS profiles a group of QoS attributes which are negotiated and used by a PDP context via the UMTS wireless network.

Multiple PDP Context

It means a single mobile terminal can have several PDP context. Each multiple PDP contexts can have different QoS profiles at same time. The primary PDP context will be activated first. In case of multiple PDP context each context has many PDP address and different APN.

The multiple PDP contexts has two sub classifications like ;

(i) Multiple primary PDP contexts which can provide connectoins to the different PDN's.

(ii) Secondary PDP contexts to offer connections to same PDN with varius QoS.

Through many PDP's are available in multiple PDP context each one of them has unique PDP address. They allow simultaneous connections to many PDN's like internet for a single application. Each PDP context has its own QoS progile RAB (Radio Access Bearer), GTP tunnel, and NSAPI (Network Layer Service Access Point Identifier.) Each PDC in multiple PDP are independent of each other.

Note A secondary PDP context is associated with primary PDP context. The PDP address (i.e. IP addr) and its Access Point (AP) can be reused from the primary context. Both the primary and secondary PDP context can offer connection to same PDN with their own QoS.

3.2.2 Combined RA / LA Update Procedures

In General Packet Radio Service (GPRS) network the combined Routing Area/Location Area (RA/LA) update procedure is been used. The Mobile Station (MS) sends the routing area update request message to new SGSN.

For both the UMTS and GPRS systems the update types are namely,

(i) RA update. (ii) Periodic RA update.

(iii) Combined RA/LA update.

(iv) Combined RA/LA update with IMSI attachment.

In UMTS the 'follow on request' parameter is been used for indicating if the connection should be retained for any pending uplink traffic. This is not available in GPRS.

In case of GPRS it adds cell global identity information (RA, LA etc.) before the base station subsystem pass the messages to the SGSN. In GPRS the timer mechanisms ensures wheather Mobile Station (MS) initiates inter SGSN routing area update just before current updating procedures.

The old SGSN will forward buffered packet data to new SGSN. If the SGSN context request message is not received then the old SGSN continues its procedure. (In case of security fail). But the next step will be followed (In case of security success).

In RA/LA updates the new SGSN sends SGSN context acknowledge. Message to old SGSN that invalids SGSN-VLR (Visitor Location Register) association in the old mobility management context.

Then the new SGSN sends the update PDP context request message to GGSNs. As the message is received the GGSN PDP contexts are then modified.

Now the SGSN issues the update location information to inform HLR (Home Location Register) about the change of MS.

The old SGSN and HLR will exchange their cancel location message pair.

Then the HLR will insert the subscriber data to new SGSN.

For every PDP context that is active, extra tasks are been performed by SGSN.

Then location update (LA) will follow. A lookup table is maintained. Referring it the SGSN translates RA identity into VLR number and then sends the location update request message to VLR. It updates or creates the SGSN-VLR association.

Now the systematic GSM location update procedure is followed.

The new SGSN transmits routing area update accepting message to mobile station.

Then routing area complete message is sent by MS to new SGSN. If required reallocation complete message will follow it.

Note In GPRS during RA update packet forwarding is done between new and older SGSN.

3.3 Universal Mobile Telecommunication System (UMTS)

AU : June-16, Dec.-16,17, May-18

3.3.1 W-CDMA (UMTS) – Third Generation Cellular System

The third generation cellular system, Universal Mobile Telecommunications System (UMTS) is an air interface and it was evolved in the year 1996, under European Telecommunications Standards Institute (ETSI). In third generation wireless telecommunications standards, UMTS is very popular due to its services and applications. The UMTS was submitted to International telecommunication union's IMT-2000 body by ETSI in the year 1998. The UMTS is also known as UMTS Terrestrial Radio Access (UTRA). The goal of UMTS was to provide high capacity cellular system. This UMTS (W-CDMA) technology has a smooth transition from 2G system so that it has a better backward compatability.

This 3G UMTS has the speciality such that any entertainment device, computers and telephone etc can access this wireless air interface network and can be connected to internet from anywhere and at any time. The packet data rate supported by UMTS is upto 2.048 Mb/sec for single user. There are many other features for W-CDM such as,

i) It provides private and public network features.

ii) The W-CDMA needs allocation of 5 MHz frequency spectrum and it is a significant difference when compared to other standards.

iii) It has interoperability for all GSM, GPRS, IS-136 (PDC) and EDGE applications.

iv) It applies direct sequence spread spectrum chip rate more than 16 megachips/sec for single user.

v) This system provides atleast six times the spectrum efficiency than a GSM standard.

3.3.1.1 UMTS - An Overview

The European proposal for IMT-2000 is called as Universal Mobile Telecommunication System (UMTS). It made a big revolution in the third generation era. The group of special mobile (GSM) enhancement towards UMTS is often known as “EDGE” technology which stands for enhanced data rates are upto 384 kbits/sec using 200 kHz wide carrier with same frequencies as that of GSM. The basic structure of UMTS comprises of user equipment, radio network subsystem and core network. UMTS supports FDD and TDD modes. The FDD mode for UTRA uses the wideband CDMA (W-CDMA) with direct sequence spread spectrum (DSSS) scheme. Hence the up and downlinks under FDD uses different frequencies. The uplink carrier is around 1920 to 1980 MHz.

GSM also fits itself into ETSI and termed as global multimedia mobility (GMM). UMTS provides different services.

1. Real time services
2. Bearer services
3. Non real time services
4. Circuit and packet switched methods of transmissions.

3.3.1.2 UMTS - Architecture

UE - User Equipment
UTRAN - UTRA Network
CN - Core Network

Fig. 3.3.1 UMTS - architecture - Basic block diagram

The UTRA network called as 'UTRAN' enables cell level mobilities and it has many radio network subsystems (RNS). The main functions of RNS is listed below.

1. Call handover control
2. Channel ciphering and deciphering
3. Radio resource management

In the architecture of UMTS, the user equipment (UE) is connected to core network 'CN' via UTRAN block.

Functions like,

1. Gateways to other (external) networks
2. Inter system handover are handled by core network

There are two types of modes compatible with UTRA system.

a. UTRA FDD mode

b. UTRA TDD mode

The wideband CDMA namely W-CDMA is used for UTRA FDD and up and downlinks use separate frequencies. FDD mode can provide 250 channels (approx), for handling user traffic; (e.g. voice channel facility). Direct sequence spread spectrum (DS) coding is compatible and data rate of 2 Mbits/sec can be achieved here. Many logical and physical channels can be assigned. User data (from layer two and higher layer) is sent over uplink dedicated physical data channel (uplink DPDCH) and in UTRA, the FDD mode makes use of wideband CDMA (W-CDMA) along with Direct Sequence Spreading (DSS). The mobile uplink frequency range is from 1920 MHz to 1980 MHz and the downlink frequency used by base station is from 2110 MHz to 2170 MHz. It is

possible to accommodate 250 channels approximately with this specified frequency spectrum range. Like GSM, in UTRA technology there are logical and physical channels available for the users. In uplink the uplink dedicated physical data channel (uplink DPDCH) is used to transport user data/information. The uplink dedicated physical control channel (uplink DPCCH) is used in transport layer to control data (like data used for controlling power).

The control data from mobile station is carried by physical random access channel (PRACH) for random access purposes.

In downlink case the user data/information and control data from layer one are carried by downlink dedicated physical channel (DPCH downlink). The chip rate may be 4.096 Mchip/sec and it may be extended for different applications in future upto 16.384 Mchip/sec.

The modulation scheme used is QPSK. CDMA technique which is compatible with UTRA has many features like,

i) Localization of mobile stations.

ii) Soft handovers.

iii) High degree of accuracy.

CDMA scheme has a drawback of "complex power control" during a "call progress".

3.3.1.3 UTRA - TDD Mode

The time division duplexing mode of the UTRA technology makes use of wideband TDMA/CDMA for the medium access and the up/down links uses the same frequency. The data rate is 2 Mbit/sec for about 120 channels (approx) in case of the user traffic. The direct sequence (DSS) type of spreading code is applied and the modulation scheme used is QPSK. In TDD the power controlling can be slower than the FDD because the number of power controlling cycles in one second are less. It is worth noting that the frame structures of FDD and TDD are same and hence both the schemes can coexist in necessary conditions.

The W-CDMA-UMTS is also called as UTRA-FDD. The physical layer of this standard can be related to be radio interface when observing one particular link between base station and a terminal. The air interface protocol structure of WCDMA is shown below.

The physical layer provides transfer services information to the next layer using various types of channels. While considering channels there are three important types of channels which have to be considered. They are

i) Logical channels

ii) Transport channels

iii) Physical channels

3.3.2 Protocol Structure of W-CDMA (UMTS)

In the protocol structure block diagram all the three channels are shown. The **logical channels** are responsible for transfer of information between RLC and MAC layers. The physical channel clearly defines the required code and frequency ranges for both up and downlinks. The characteristics of the data/information is sent over the channel by transport channels. In the W-CDMA the physical layer provides services to the respective MAC layer through the transport channels.

i) Physical Channels in W-CDMA

In W-CDMA some of the physical channels carry information on the downlink channels as listed below.

- CPICH (Common Pilot Channel)
- SCH (Synchronization Channel)
- AICH (Acquisition Indication channel)
- PICH (Paging Indication Channel)
- CSICH (CPCH Status Indication Channel)
- CD/CA-ICH (Collision Detection/Channel)
- Assignment indication channel

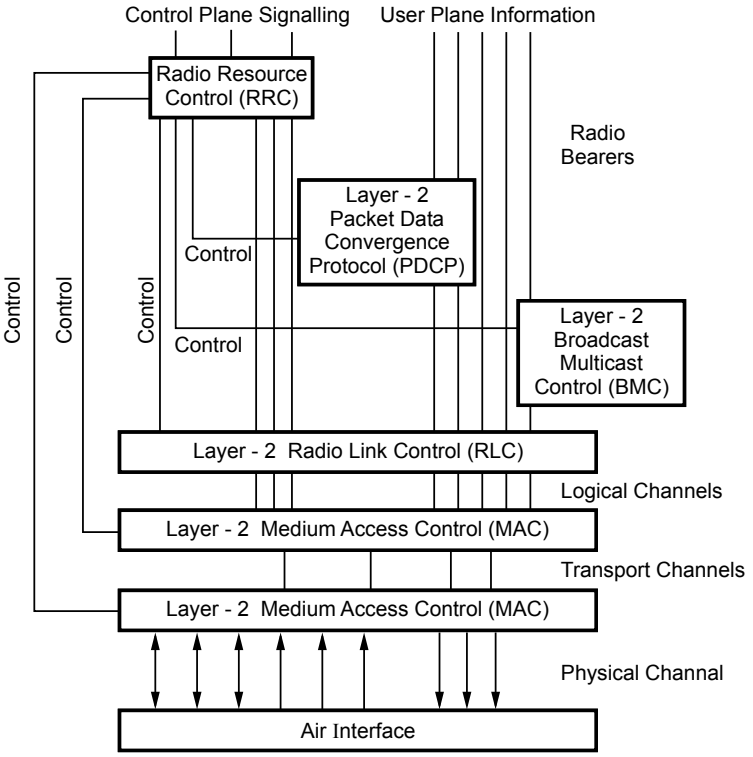


Fig. 3.3.2 Air interface protocol structure of W-CDMA (UMTS)

The first two channels CPICH and SCH have to be transmitted by every base station. The various transport channels are mapped on different physical channels. A few physical and transport channels are identical. Let this group be X.

On the other hand a few physical channels act as carriers for a portion of the transport channels. This group of channels let it be denoted as Y. A simple mapping of transport channels onto physical channels is shown below.

	Transport channel		Physical channels
Group X	RACH	→	PRACH (Physical Random Access Channel)
	BCH	→	PCCPCH (Primary Common Control Physical Channel
	DSCH	→	PDSCH (Physical Downlink Shared Channel)
	CPCH	→	PCPCH (Physical Common Packet Channel)
	PCH FACH	→	SCCPCH (Secondary Common Control Physical Channel)
Group Y	DCH	→	DPCCH (Dedicated Physical Control Channel)
		→	DPDCH (Dedicated Physical Data Channel)

Thus the transport channels are mapped onto the physical channels.

Then the important transmission characteristics of W-CDMA includes,

1) Identical characteristics of up and downlinks.

   i) Radio frame structure of 10 msec.

   ii) Spreading/channelization codes (OVSF codes)

   iii) System frame number (SFN) of 12 bits.

   iv) Chip rate of 3.84 Megachips/sec

   v) Channel spacing of 5 MHz.

   vi) Long code of 38400 chips.

2) Uplink channel characteristics.

   In W-CDMA the uplink channel characteristics the main operations are

   i) Spreading

   ii) Scrambling

   iii) Modulation

After spreading and scrambling it forms the CDMA signal. (See Fig. 3.3.3 on next page).

The Walsh codes are used in WCDMA. The spreading codes in WCDMA are known as orthogonal variable spreading factor (OVSF) codes. Then spreading factor can vary from 4 to 512. This standard uses 3.84 megachips/sec chip rate and maintained as

constant. By using shorter spreading codes higher data rates and by using longer spreading codes lower data rates are obtained. Thus by decreasing spreading factor the data rate can be increased. But it will also reduce the number of cellular users which can be supported. The reason is fewer codes are only available in case of shorter spreading factor.

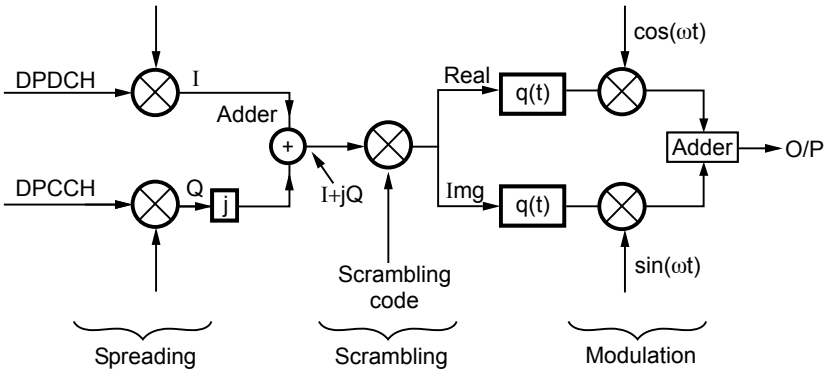
In case of demodulation pilot symbols are used. The channels DPCH, CCPCH and the PRACH carriers pilot symbols.

In spreading at the transmitter end, the channelization code is capable of identifying the physical data channels DPDCH and control channels (DPCCH) with the code length.

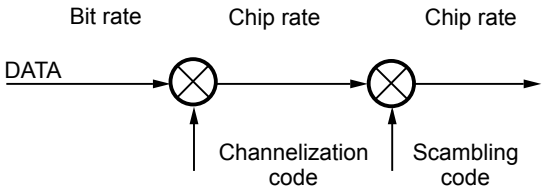
The process of scrambling follows the spreading. It uses gold code that has a pseudorandom characteristics. The long code has 10 msec frame and used at rake receiver in base station. The short code is used when the base station applies multiuser detection techniques.

In modulation combine Inphase-Quadrature, code multiplexing is used (i.e. dual channel QPSK scheme).

The transmission power can be reduced by having faster power control in the uplinks.



(a)

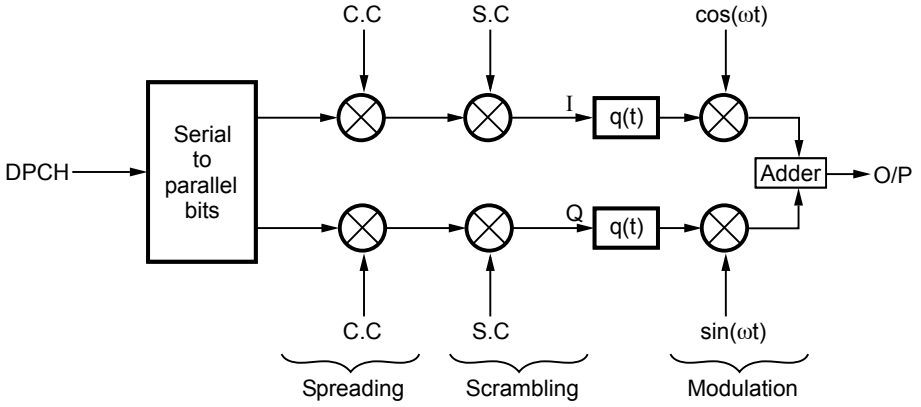


(b)

Fig. 3.3.3 Transmission characteristics

a) W-CDMA (UMTS) uplink spreading, scrambling and modulation operations
b) Spreading and scrambling

In downlink channel characteristics the same functions dealt under uplink are done and at first the DPCH serial bits are converted to parallel bits so as to have correct mapping in inphase and quadrature branches effectively.



S.C. - Scrambling code
C.C. - Channel code

Fig. 3.3.4 WCDMA (UMTS) Downlink operations, spreading, scrambling and modulation

In spreading that is based on OVSF codes operating limit is upto 512 chips. The scrambling uses gold codes for a time frame of 10 msec (i.e. 38400 chips). Under channels SCH, the primary and secondary SCH are used. The primary SCH consists of a code of 256 chips and in secondary SCH it can generate upto 64 various code words, for identifying common channels having continuous transmission. In modulation quadrature phase shift keying with relevant time-multiplexed data and control system are used.

Transport Channels

The main characteristics of information that the transport channels can provide is summarized below :

i) The shared information for up or downlink.
ii) The control information for up or downlink.
iii) Power control characteristics.
iv) Managing the collision risk.
v) Mobile station identification.
vi) Beam forming information.
vii) Data rate variation.
viii) Broadcast coverage area

- In entire cellular area or in a selected cell alone.

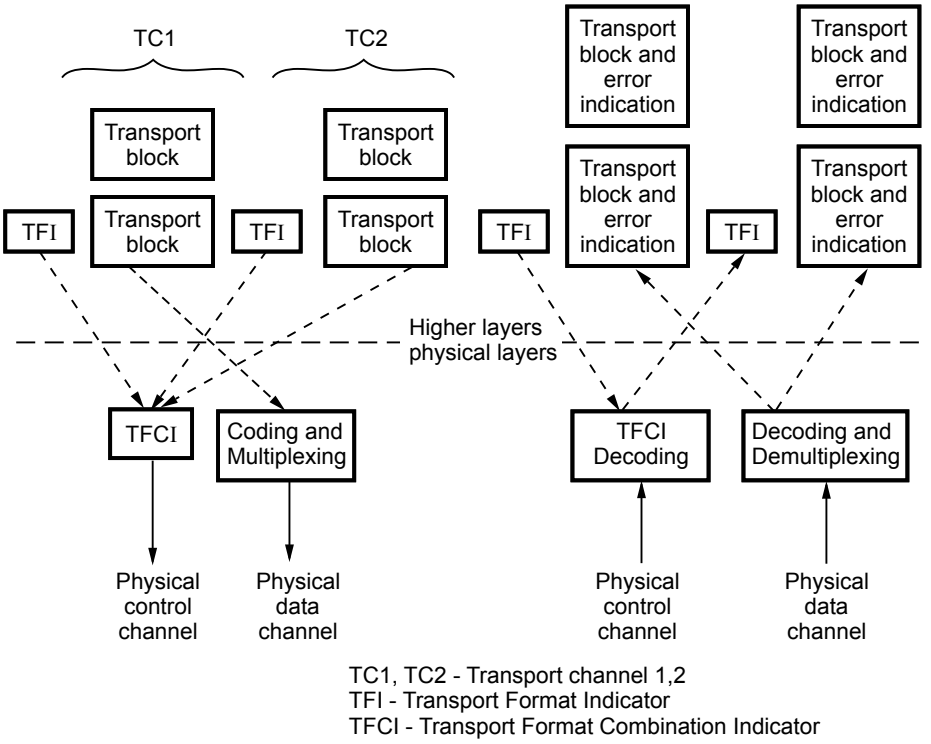


Fig. 3.3.5 Higher layers and physical layers (W-CDMA (UMTS))

The interaction between physical and higher layers are shown in the diagram. Every transport channel carries the transport format indicator (TFI). The physical layer does the function of combining all the TFI information from various transport channels to form the Transport Format Combination Indicator denoted as TFCI. This TFCI is useful as it informs the mobile equipment about availability of active transport channel, in the current frame.

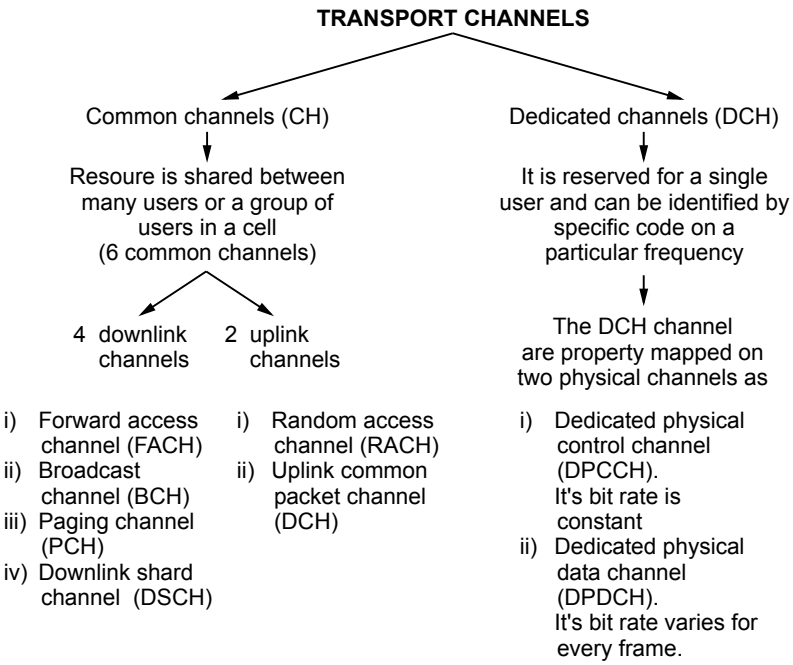
The TFI is added to each TC such that

{TFI + TC} is done where

{TC} → Coding and multiplexing in bank of transport channels.

and {TFI} → Physical control channel (PCEH)

It is possible to divide the transport channels into common channel and dedicated channel for a specific operation.



Hence the transport channel has common and dedicated channels and uses them according to the nature of the operational requirement, in transport channels of W-CDMA(UMTS).

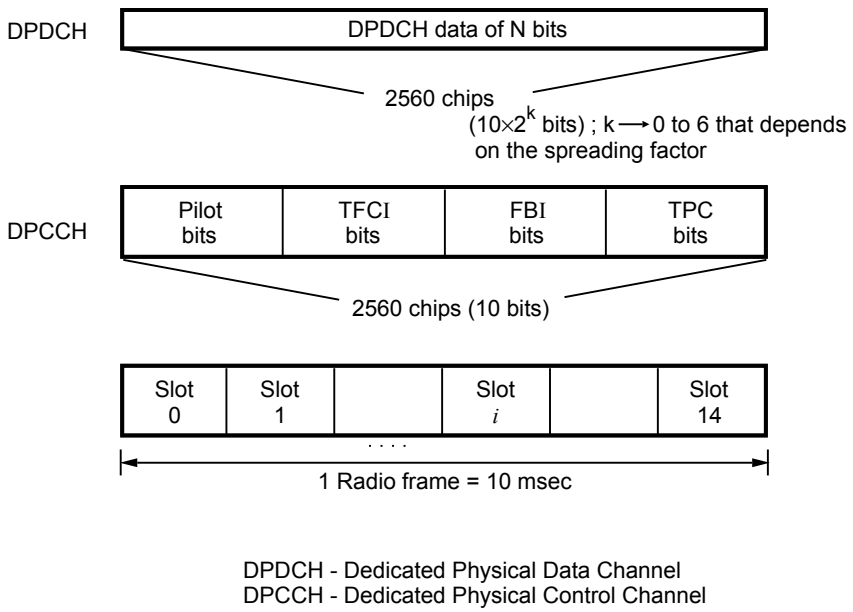


Fig. 3.3.6 The uplink DPDCH and DPCCH frame and slot structures

User Data Transmission

In the user data transmission it makes use of slot structure of radio frame with 15 slots in 10 msec time period. The duration of a slot is about 2560 chips. It has a chip rate of 3.84 megachips/sec. The parallel code channels are being used for handling higher data rates.

The user data transmission when combined with Random Access Channel (RACH) has a particular future preamble and it is sent before the data transmission. The uplink frame and slot structure is shown in the diagram above where one radio frame period is 10 msec. For fast power control the uplink common packet channel is used.

In case of downlink the bit rates and symbol rates are same as the uplink. The downlink channel is of dedicated physical channel (DPCH) and (DPDCH) type. The bit rate in DPDCH is not fixed and it varies. It also uses time multiplexing for physical control information and also the user data information respectively.

Also there are three classes of frames in RLP. They are

i) New data frame :

They are transmitted with lowest priority.

ii) Control frames :

They are used to carry control information and it is given top priority.

iii) Retransmitted data frame :

They are meant for retransmitting the old data frame according to instructions given.

3.3.3 Communication between Layers and Sublayer

Structures :

Establishing communication between the respective layers and sub layers is done using primitives. The MAC, LAC and layer 3 (upper layers) uses the primitives for passing the data and control information between intended layers. Also the actual data unit is considered as a parameter of the respective primitive.

Consider that a PDU has to be sent from LAC sublayer. Now the LAC sublayer will invoke the service data unit (SDU) primitive to request the service from the MAC layer. There are four different primitives which are effectively used for communication. It is shown in the diagrams below for both the transmit and receive side.

E.g. : Transmit side :

i) Consider layer 3 wants to send a PDU. It makes a request for service from the next LAC sublayer by using the L2-data primitive as shown.

ii) If the SAR or LAC sublayer need to transmit a PDU i.e. from layer 3 then the LAC sublayer will invoke the SDU ready primitive thus requesting a service from respective MAC layer.

iii) In case if enough space is available for bearing data transfer function over physical channels then the MAC layer transmits the "Availability-Primitive" to express the event occured, as an indication to the service requester.

iv) Once the 'Availability-Primitive' is received, the LAC sublayer transmits MAC-Data primitive to that of the MAC, for requesting data transport service effectively.

On the other hand there are two important primitives which are used at receive end.

Receive side :

i) The MAC layer makes use of the MAC-Data primitive to the LAC sublayer.

ii) Once the processing is over, then it is informed to layer 3 as follows. The LAC sublayer sends a PDU using 'L2-Data primitive' to the layer 3 to express the reception of signalling data.

Upper layer in the structure :

The operation of the entire IS-2000 system is controlled effectively by the signalling entity. There are four main states available, namely,

i) Mobile station initialization

ii) Mobile station idle

iii) System access

iv) Mobile station control on traffic channel

All these four states have similarity with the IS-95 standard as backward compatability.

Also the packet data transmission involved has three modes when the mobile is in traffic channel substate. The modes are

a. Active mode b. Control hold mode c. Dormant mode

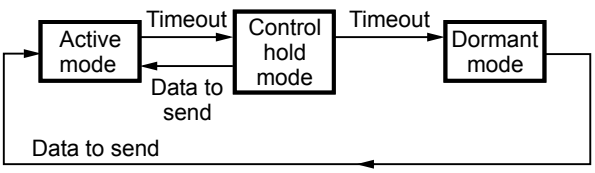


Fig. 3.3.7 Packet data transmission with three modes

In the active mode there is exchange of user packet data and the respective dedicated signalling data between base station (BTS) and the mobile station (MS). Then the control mode in packet data transmission helps to maintain the MAC control and the power control functions using dedicated control channel in the system.

Finally the dormant mode is mainly applied in 'mobile station idle state' to keep the information regarding user's packet data service registration (UPDR) and relevant connections. At any point a mobile is in any one of three modes or in a state of transition between these modes. In addition to this the signalling entity also keeps track of setup, maintenance etc. regarding a call. Thus the call processing functions are effectively handled by the signalling entity in the system.

Power Control

It is very important to have proper power control in forward and receive end under cdma 2000 standard to improve accuracy and speed and finally system capacity. At the receive end the power control is mainly to reduce the differences in the power levels of signal that is received from many transmitters from base station. On the other hand in forward end power control is to reduce the differences in power levels of received powers present in same band that allows many users to exist on the system.

The main types of power control used are

i) Power control in reverse link

This type mainly makes sure that all the received link signals are at same power level (nearly). Hence interference can be minimized among all the mobile signals, in reverse link. By using open loop and closed loop setups the power control is implemented.

ii) Closed loop power control in forward link

The closed loop power control is used in forward link and it is used to reduce the received power level from various transmitters at the mobile end. Then the EC/NO (Energy to noise) and the FER error rate of the signal received is measured by the mobile continuously with respect to the forward link.

The four entities of MAC layer Radio Link Protocol (RLP), Signalling Radio Burst Protocol (SRBP), dedicated channel multiplex sublayer and common channel multiplex sublayer is shown in the protocol architecture in IS-2000 (cdma 2000).

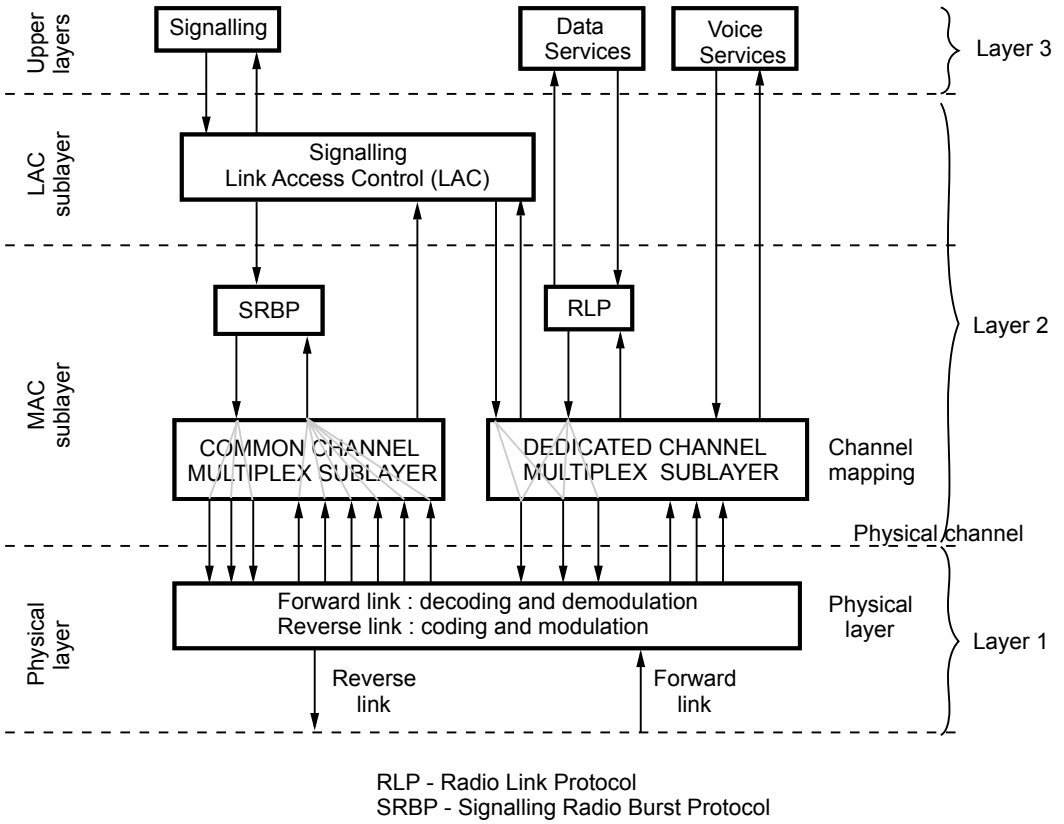


Fig. 3.3.8 Protocol architecture in IS-2000 (evolution of IS-95/cdma 2000) from the mobile perspective

3.4 Dynamic Host Configuration Protocol (DHCP) AU : June-16, Dec.-16

DHCP was developed from protocol called as Bootstrap protocol (BOOTP). This standard was released in 1985. It supports static information for clients that includes IP addresses. To manage dynamic configuration information and dynamic IP addresses IETF standardized an extension to 'BOOTP' known as dynamic host configuration protocol (DHCP).

3.4.1 Application of DHCP

1. DHCP helps to drag the management of IP addresses from distributed client servers to centrally managed servers.
2. In the sites with more TCP/IP clients, DHCP yields support to manage large number of clients effectively.

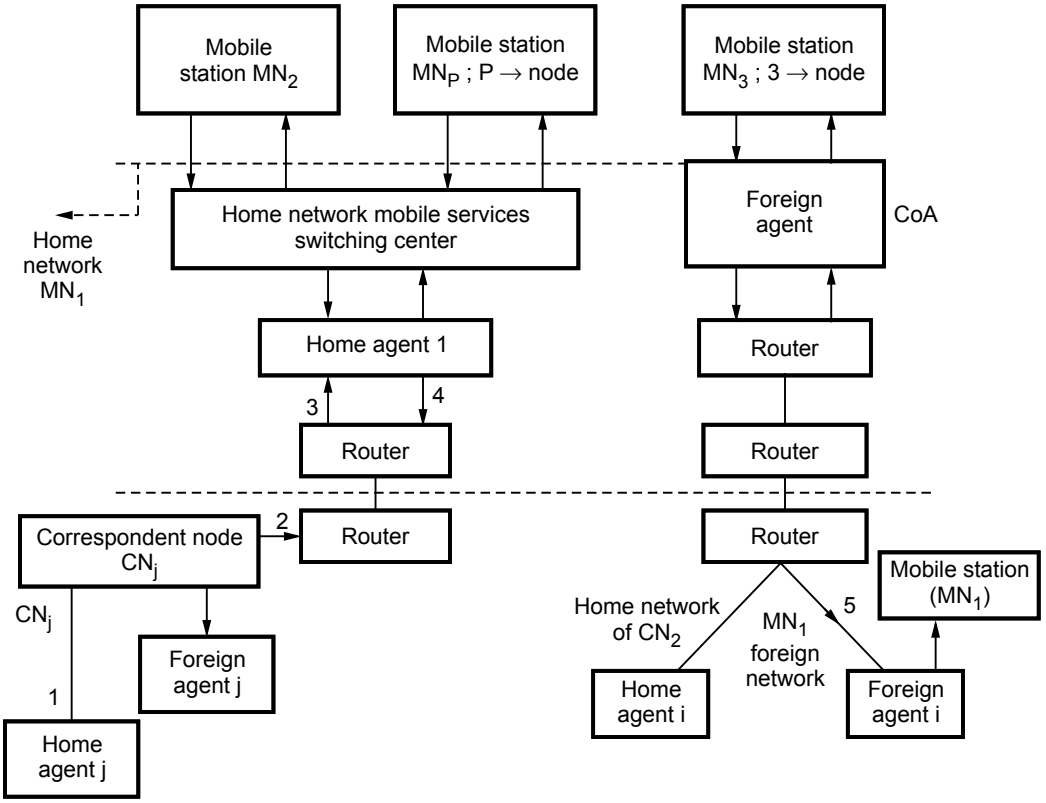


Fig. 3.4.1 Mobile IP network applying triangular routing [without mobility binding]

3. DHCP is useful in sites with fewer TCP/IP addresses than the number of clients.
4. In sites that needs frequent movement from host to host with different locations DHCP is used.
5. DHCP is used in sites where laptop computers have to move among different networks within a particular site.
6. It is used for diskless clients.

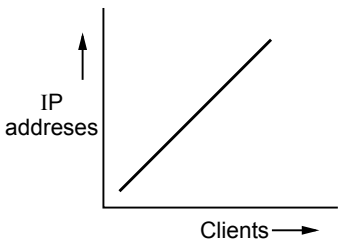


Fig. 3.4.2 Client Vs number of IP addresses

As the number of clients grows up the need for IP addresses is more. There is a chance of scarcity of IP addresses availability. This scarcity can be minimized with the help of DHCP. There are two ways possible.

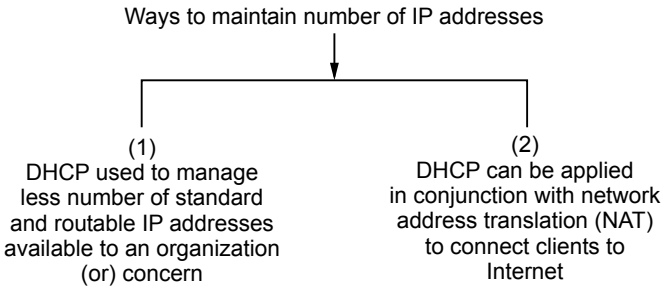


Fig. 3.4.3

By using these methods accessible IP addresses are made easy to some extent in networking.

3.4.1.1 BOOTP Protocol

The Bootstrap [BOOTP] protocol is used in application layer in TCP/IP protocol suite and it supports several mobile applications. The application layer enables communication between application processes on separte hosts environment.

The dynamic host configuration protocol was developed from Bootstrap Protocol (BOOTP). The BOOTP is client server protocol which was designed to furnish four information. The problems associated with BOOTP are given below.

Problems with BOOTP

When a node (computer) is attached to TCP/IP internet (connection established) should be aware of these above said four information.

1. Its subnet mask.
2. Internet protocol (IP) address.
3. Internet protocol (IP) address of a router.
4. Internet protocol (IP) address of a name server.

Actually this Bootstrap Protocol (BOOTP) is not a dynamic configuration protocol. Whenever a client requests IP address the server machine with BOOTP searches a table which matches physical address of client with Internet Protocol (IP) address. This link between client and IP address is predetermined.

BOOTP cannot address a few problems like

1. If a host moves from a physical network to another network.
2. If a host seeks a temporary Internet Protocol (IP) address.

There are critical situation where BOOTP cannot decide what to do next.

3.4.2 Significance of Dynamic Host Configuration Protocol

But Dynamic Host Configuration Protocol (DHCP) provides dynamic configuration. It is an extension to the BOOTP and compatible with it. If a host is running BOOTP client

it can also request a configuration (example : static configuration) from a DHCP server node. The advantages of DHCP are;

1) Whenever a host moves from one network to another network or to connect or disconnect with a network.
2) DHCP also provides temporary IP address for a particular predetermined time period.

3.4.3 Components of Dynamic Host Configuration Protocol

The Dynamic Host Configuration Protocol (DHCP) is built on a client-server model. It has designated server hosts allocating the network addresses and delivering configuration parameters to the dynamically configured hosts. The term 'client' refers to host that request initialization parameters and the term 'server' refers to a host that can provide initialization parameters through dynamic host configuration protocol. The DHCP mainly provides configuration parameters to the internet hosts. It consists of two components.

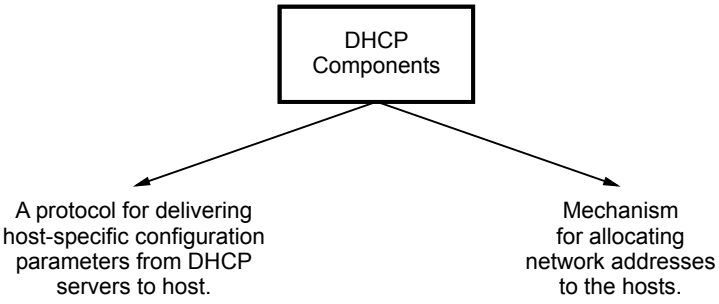


Fig. 3.4.4 DHCP components

The DHCP supports three important mechanisms for the IP address allocation.

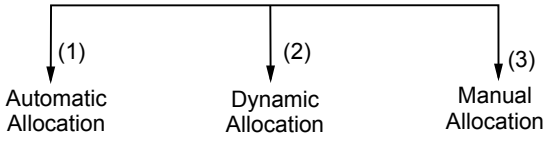


Fig. 3.4.5 Three mechanisms for IP address allocation

1) Automatic allocation is also possible. Wherein the DHCP assigns permanent IP address to a particular client.
2) With the dynamic allocation DHCP assigns IP address to a client for a particular period of time.

3) In the manual allocation a client's IP address is assigned by network administrator, where the DHCP is used to inform the address assigned to the client.

Note : Whenever permanent IP address pool is not required and if temporary IP addresses are enough for a set of clients in this case it is better to have dynamic allocation mechanism.

Only in dynamic allocation method automatic reuse of an address is done.

Importance of DHCP

DHCP is a widely used protocol for configuring hosts like PC's, printers and workstations. The DHCP servers allocates mainly IP addresses from a pool of IP addresses to a set of clients with the help of network administrator as discussed so far. Hence dynamic host configuration protocol which was created by Internet Engineering Task Force (IETF) streamlines the efficiency of the network connectivity that is used by mobile IP protocols.

The DHCP protocol is used by three different agents as we know server, client and relay agent. This DHCP server is actually a central server configured on a site's network that can provide DHCP services. The client (software program) interacts with DHCP server.

The client/server relationship is perfectly used by DHCP for allocating IP addresses and keeping track of their usage. Whenever a user boots a particular client system and that system broadcasts a request for DHCP server for issuing an IP address.

The DHCP can also pass additional information for a booting system.

Sequence :

1. Client issues request for booting.
2. Server receives the packet.
3. Compares it with database of possible parameters.

The IP address may be of static or dynamic type.

Static IP address : It is permanently assigned to the client.

Dynamic IP address : It is not assigned to the client till it gets booted and address given by the server.

Hence the dynamic host configuration (DHCP) protocol is considered as "a protocol of choice".

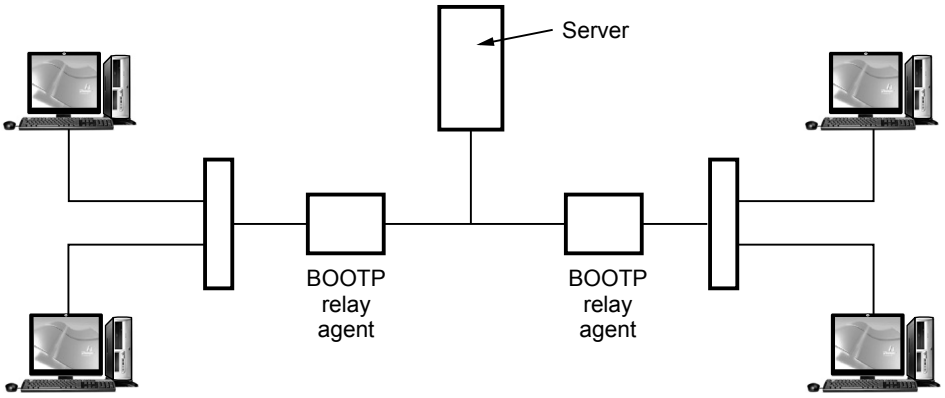


Fig. 3.4.6 DHCP - Clinet/server environment

Note : The DHCP responds to a particular period of time (server responds with IP address) which is also known as "lease" for which period the client makes use of the address assigned to it.

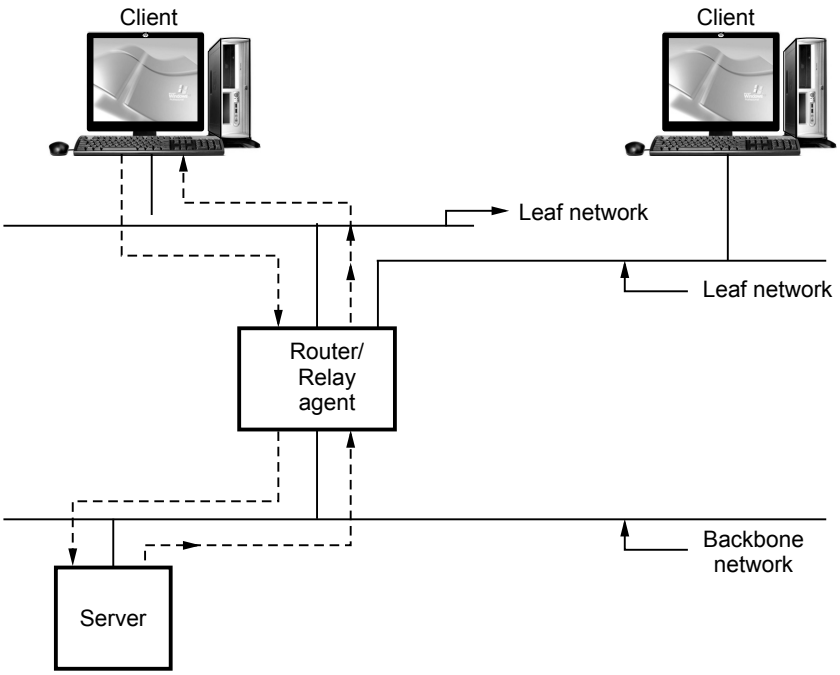


Fig. 3.4.7 DHCP - Client/server interaction sample

With this client/server interaction setup DHCP enables computers on a network to configure themselves.

DHCP makes it possible for users of wireless devices to move within an organization that is with various networks. (from home to work) for this the DHCP client and server work together to handle the roaming status and to assign IP address on new networks efficiently.

The wireless LAN should meet some basic requirements. It should have high capacity, full connectivity, to cover short distances etc.

Review Questions

PART A

1. *Define GSM.*
2. *Write a note on network and switching subsystem.*
3. *What are GSM channels ?*
4. *Write a note on handover procedure in GSM.*
5. *What is GPRS ?*
6. *Draw the GPRS architecture.*
7. *What are LLC, RLC, MAC in GPRS ?*
8. *Define UMTS.*
9. *List two advantages in third generation wireless networks.*
10. *What is PDP context procedure ?*
11. *List the 3 important features of GSM security.* **(Refer section 3.1.4)** **AU : June-16, Marks 2**
12. *What are the main elements of UMTS.* **(Refer section 3.3.1)** **AU : June-16, Marks 2**
13. *Name the Teleservices provided by GSM.* **(Refer section 3.1.6)** **AU : June-17, Marks 2**
14. *Illustrate the use of BOOTP protocol.* **(Refer section 3.4.1.1)** **AU : Dec.-16, Marks 2**
15. *Define Handoff. What are its types ?* **(Refer section 3.1.3)** **AU : Dec.-17, Marks 2**
16. *List the services of GPRS.* **(Refer section 3.2)** **AU : Dec.-17, Marks 2**
17. *What is frequency range of uplink and downlink in GSM network ?* **(Refer section 3.1)** **AU : May-18, Marks 2**

PART B

1. *Explain GSM services, security and handover procedures.*
2. *Explain the architecture of GSM.*
3. *What is GSM ? Explain its handover procedure and channels in detail.*
4. *Explain i) Mobile number portability and ii) Hardover procedures in GSM.*
5. *Explain GPRS in detail.*
6. *What is UMTS ? Explain UMTS in detail.*
7. *Explain the UMTS networks and list the advantages of third generation wireless standard.*
8. *Describe GSM architecture and its services in detail.* **(Refer section 3.1.1)** **AU : June-16, Marks 8**
9. *Explain GSM Authentication and Security.* **(Refer section 3.1.4)** **AU : June-16, Marks 8**
10. *Explain GPRS and its Protocol arechitecture.* **(Refer section 3.2)** **AU : June-16, Marks 8**
11. *Explain in detail about UMTS architecture architecture.* **(Refer sections 3.3.1.2, 3.3.1.3)** **AU : June-16, Marks 8**

12. *With a diagram explain DHCP and its protocol architecture.* **(Refer section 3.4)** **AU : June-16, Marks 8**
13. *What are the functions of authentication and encryption in GSM ? How is system security maintained.* **(Refer section 3.1.4)** **AU : Dec.-16, Marks 8**
14. *Explain in detail about the handovers of GSM.* **(Refer section 3.1.1.5)** **AU : Dec.-16, Marks 8**
15. *Explain the functions of GPRS protocol stack with a diagram.* **(Refer section 3.2)** **AU : Dec.-16, Marks 8**
16. *Explain in detail about UMTS architecture.* **(Refer sections 3.3.1.1 and 3.3.1.2)** **AU : Dec.-16, Marks 8**
17. *Explain the GSM architecture in detail.* **(Refer section 3.1.1)** **AU : June-17, Marks 16**
18. *Explain GPRS protocol architecture.* **(Refer section 3.2)** **AU : June-17, Marks 16**
19. *Explain GSM architecture and its services with neat diagram.* **(Refer section 3.1)** **AU : Dec.-17, Marks 16**
20. *Explain in detail about UMTS architecture and its services.* **(Refer section 3.3)** **AU : Dec.-17, Marks 16**
21. *Write in detail about the various types of handover in GSM. Also discuss the timeline diagram of the Intra MSC handover.* **(Refer section 3.1.1.5)** **AU : May-18, Marks 13**
22. *Explain in detail network architecture of UMTS with a neat diagram.* **(Refer section 3.3)** **AU : May-18, Marks 13**

❑❑❑

UMTS Handover

There are following categories of handover (also referred to as handoff):

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. In practice 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. Normally 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. In softer handover, 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.

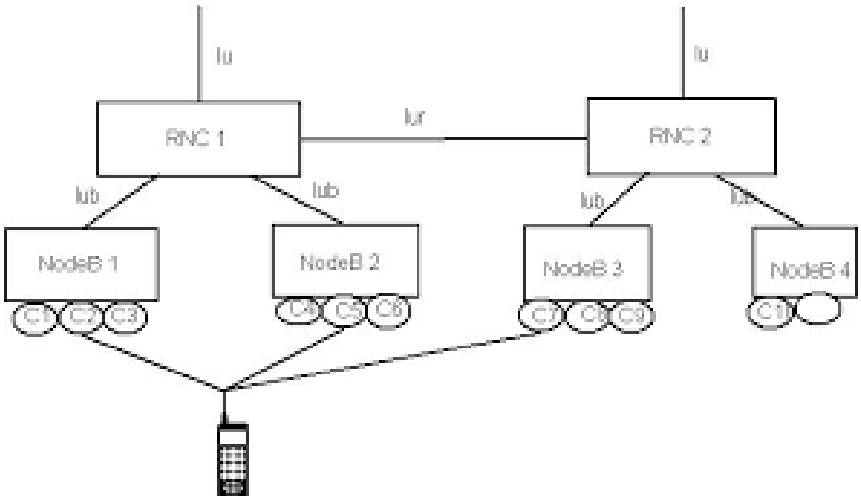
Generally we can distinguish between intra-cell handover and inter-cell handover. For UMTS the following types of handover are specified:

- Handover 3G -3G (i.e. between UMTS and other 3G systems)
- FDD soft/softer handover
- FDD inter-frequency hard handover
- FDD/TDD handover (change of cell)
- TDD/FDD handover (change of cell)
- TDD/TDD handover
- Handover 3G - 2G (e.g. handover to GSM)
- Handover 2G - 3G (e.g. handover from GSM)

The most obvious cause for performing a handover is that due to its movement a user can be served in another cell more efficiently (like less power emission, less interference). It may however also be performed for other reasons such as system load control.

Active Set is defined as the set of Node-Bs the UE is simultaneously connected to (i.e., the UTRA cells currently assigning a downlink DPCH to the UE constitute the active set). Cells, which are not included in the active set, but are included in the CELL_INFO_LIST belong to the Monitored Set.

Cells detected by the UE, which are neither in the CELL_INFO_LIST nor in the active set belong to the Detected Set. Reporting of measurements of the detected set is only applicable to intra-frequency measurements made by UEs in CELL_DCH state.



The different types of air interface measurements are:

Intra-frequency measurements: measurements on downlink physical channels at the same frequency as the active set. A measurement object corresponds to one cell.

Inter-frequency measurements: measurements on downlink physical channels at frequencies that differ from the frequency of the active set. A measurement object corresponds to one cell.

Inter-RAT measurements: measurements on downlink physical channels belonging to another radio access technology than UTRAN, e.g. GSM. A measurement object corresponds to one cell.

Traffic volume measurements: measurements on uplink traffic volume. A measurement object corresponds to one cell.

Quality measurements: Measurements of downlink quality parameters, e.g. downlink transport block error rate. A measurement object corresponds to one transport channel in case of BLER. A measurement object corresponds to one timeslot in case of SIR (TDD only).

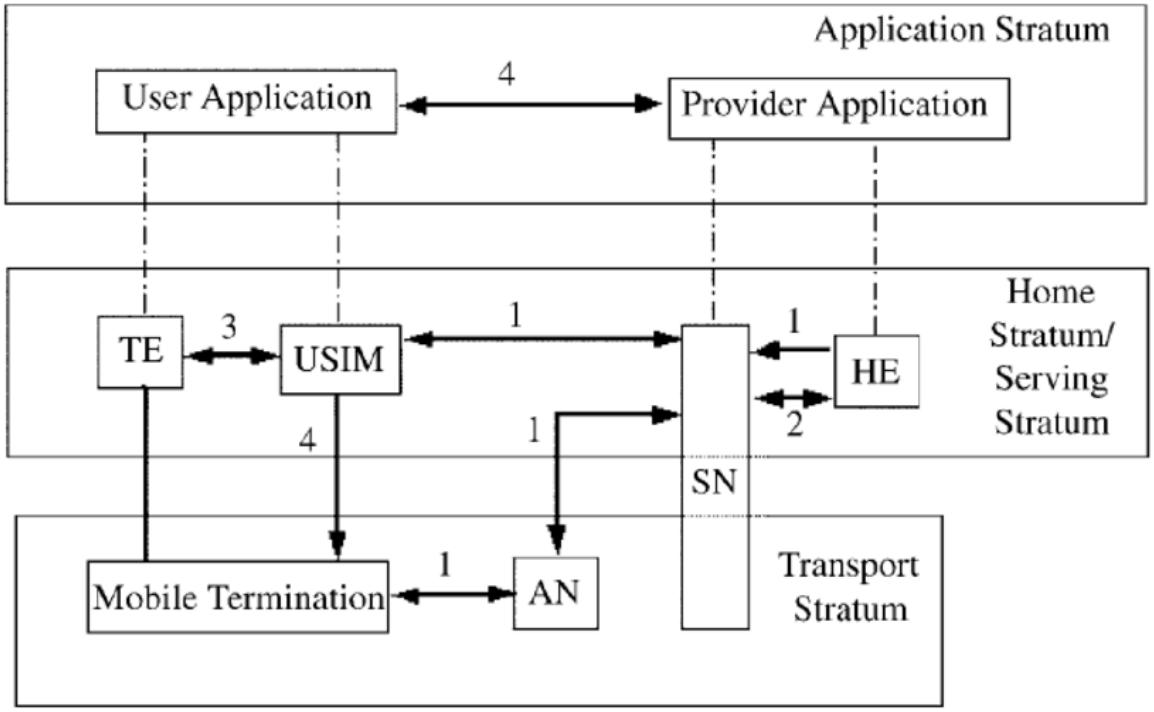
UE-internal measurements: Measurements of UE transmission power and UE received signal level.

UE positioning measurements: Measurements of UE position.

The UE supports a number of measurements running in parallel. The UE also supports that each measurement is controlled and reported independently of every other measurement.

UMTS Security

The security functions of UMTS are based on what was implemented in GSM. Some of the security functions have been added and some existing have been improved. Encryption algorithm is stronger and included in base station (NODE-B) to radio network controller (RNC) interface , the application of authentication algorithms is stricter and subscriber confidentially is tighter.



The main security elements that are from GSM:

- Authentication of subscribers
- Subscriber identity confidentially
- Subscriber Identity Module (SIM) to be removable from terminal hardware
- Radio interface encryption

Additional UMTS security features:

- Security against using false base stations with mutual authentication
- Encryption extended from air interface only to include Node-B to RNC connection
- Security data in the network will be protected in data storages and while transmitting ciphering keys and authentication data in the system.

- Mechanism for upgrading security features.

Core network traffic between RNCs, MSCs and other networks is not ciphered and operators can to implement protections for their core network transmission links, but that is unlike to happen. MSCs will have by design a lawful interception capabilities and access to Call Data Records (SDR), so all switches will have to have security measures against unlawful access.

UMTS specification has five security feature groups:

- **Network access security: the** set of security features that provide users with secure access to 3G services, and which in particular protect against attacks on the (radio) access link;
- **Network domain security:** the set of security features that enable nodes in the provider domain to securely exchange signalling data, and protect against attacks on the wireline network;
- **User domain security:** the set of security features that secure access to mobile stations
- **Application domain security:** the set of security features that enable applications in the user and in the provider domain to securely exchange messages.
- **Visibility and configurability of security:** the set of features that enables the user to inform himself whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.

UMTS specification has the following user identity confidentiality security features:

- **User identity confidentiality:** the property that the permanent user identity (IMSI) of a user to whom a services is delivered cannot be eavesdropped on the radio access link;
- **User location confidentiality**: the property that the presence or the arrival of a user in a certain area cannot be determined by eavesdropping on the radio access link;
- **User untraceability:** the property that an intruder cannot deduce whether different services are delivered to the same user by eavesdropping on the radio access link.

Air interface ciphering/deciphering in performed in RNC in the network side and in mobile terminals. Ciphering in function of air interface protocol Radio Link Control (RLC) layer or Medium Access control (MAC) layer.

Unit IV

Mobile Ad-hoc Networks

Syllabus

Ad-Hoc Basic Concepts - Characteristics - Applications - Design Issues - Routing - Essential of Traditional Routing Protocols -Popular Routing Protocols - Vehicular Ad-Hoc networks (VANET) - MANET Vs VANET - Security..

Contents

4.1 Mobile Ad-hoc Networks : Concept

AU : June-16, May-18

In recent years wireless network nodes became popular and as the applications using Internet is high. Sometimes an user may be interested in using a laptop computer without making routing functions via global Internet. For such cases Internet protocols will not be required. Thus the mobile computer users can be allowed to set up a short lived network with wireless communication devices, for a particular moment. This network is known as ad-hoc network. It is independent of infrastructure. Thus even when there is no infrastructure available an ad-hoc network can be formed.

The wireless computing devices are able to communicate with each other in ad-hoc networking, it is possible even there is no,

- Routers or
- Base stations or
- Internet service providers

The ad-hoc network and mobile ad-hoc network (MANET) are discussed in this chapter.

4.1.1 Characteristics of Ad-hoc Networks (MANET)

- The topology of ad-hoc networks is dynamic in nature and changes in their topology is possible. But to attain a reliable output quality frequent changes can be avoided.
- Due to wireless transmission their physical security is limited.
- The capacity of these network is lower when compared with wired networks.
- They experience higher loss rates, higher delays and also the jitter than the fixed type of networks.
- They use either exhaustible power supplies or batteries for getting energy. In network design it is very important to consider power saving.
- In a perfect 'ad-hoc network' it has all the seven layers from physical layer to application layer.
- In designing an ad-hoc network their exists high complexity with physical layer setups but in case of mobile networks it will be taken care by their base stations.
- The informations related to network destiny, link failures, nodes distributions has to be clearly defined for ad-hoc networks.
- To obtain a better network structure it is important that the MAC layer and network layer should collaborate with each other.
- The ad-hoc network is independent of any central control or infrastructure.

4.1.2 Advantages of Ad-hoc Networks

- Instant infrastructure in case of sudden meetings, unplanned interpersonal communications etc. Planned infrastructures are not required.
- Remote area networking : In paresely populated areas where infrastructure setup is difficult ad-hoc networks can be established.
- Effective system : The ad-hoc packet oriented network setup is less expensive and also effective. These ad-hoc networks provides a better solution for application specific cases.

A working group at IETF under ad-hoc networks focused on mobile ad-hoc networking termed as 'MANET' in the year of 2002.

A relation between MANET and mobile IP is shown in the Fig. 4.2.3.

4.2 Overview of MANET's and Design Issues

AU : May-17,18

The "mobile ad-hoc networks" MANETs have many advantages and one of the most important advantage is its "Infrastructure independent" nature. The ad-hoc networks does not need infrastructure's that is required for other wireless networks. The term infrastructure includes need of base stations, routers etc.

The ad-hoc networks are composed of the equal nodes that can communicate with each other through wireless links. Their is no central control for their work.

The important features of ad-hoc networks and MANET's are discussed in detail in this chapter.

The term MANET describes mobile, wireless, distributed multihop networks that could operate independent of infrastructure. A MANET network is composed of mobile, autonomous, wireless nodes that could be connected at network edges to that of the fixed wired Internet. Initially MANET is developed due to military requirements where infrastructure less, line of sight operations are required.

Salient features of MANET includes

1) Network size

It refers to the geographical coverage area that could be covered by the network. The number of nodes for a given geographical area represent network density.

2) Connectivity

It refers to many issues. One such is the number of neighbouring nodes that could link to them directly. This link may be bidirectional. Connectivity also refers to link capacity between any two nodes.

Unit IV

Mobile Ad-hoc Networks

Syllabus

Ad-Hoc Basic Concepts - Characteristics - Applications - Design Issues - Routing - Essential of Traditional Routing Protocols -Popular Routing Protocols - Vehicular Ad-Hoc networks (VANET) - MANET Vs VANET - Security..

Contents

4.1 Mobile Ad-hoc Networks : Concept

AU : June-16, May-18

In recent years wireless network nodes became popular and as the applications using Internet is high. Sometimes an user may be interested in using a laptop computer without making routing functions via global Internet. For such cases Internet protocols will not be required. Thus the mobile computer users can be allowed to set up a short lived network with wireless communication devices, for a particular moment. This network is known as ad-hoc network. It is independent of infrastructure. Thus even when there is no infrastructure available an ad-hoc network can be formed.

The wireless computing devices are able to communicate with each other in ad-hoc networking, it is possible even there is no,

- Routers or
- Base stations or
- Internet service providers

The ad-hoc network and mobile ad-hoc network (MANET) are discussed in this chapter.

4.1.1 Characteristics of Ad-hoc Networks (MANET)

- The topology of ad-hoc networks is dynamic in nature and changes in their topology is possible. But to attain a reliable output quality frequent changes can be avoided.
- Due to wireless transmission their physical security is limited.
- The capacity of these network is lower when compared with wired networks.
- They experience higher loss rates, higher delays and also the jitter than the fixed type of networks.
- They use either exhaustible power supplies or batteries for getting energy. In network design it is very important to consider power saving.
- In a perfect 'ad-hoc network' it has all the seven layers from physical layer to application layer.
- In designing an ad-hoc network their exists high complexity with physical layer setups but in case of mobile networks it will be taken care by their base stations.
- The informations related to network destiny, link failures, nodes distributions has to be clearly defined for ad-hoc networks.
- To obtain a better network structure it is important that the MAC layer and network layer should collaborate with each other.
- The ad-hoc network is independent of any central control or infrastructure.

4.1.2 Advantages of Ad-hoc Networks

- Instant infrastructure in case of sudden meetings, unplanned interpersonal communications etc. Planned infrastructures are not required.
- Remote area networking : In paresely populated areas where infrastructure setup is difficult ad-hoc networks can be established.
- Effective system : The ad-hoc packet oriented network setup is less expensive and also effective. These ad-hoc networks provides a better solution for application specific cases.

A working group at IETF under ad-hoc networks focused on mobile ad-hoc networking termed as 'MANET' in the year of 2002.

A relation between MANET and mobile IP is shown in the Fig. 4.2.3.

4.2 Overview of MANET's and Design Issues

AU : May-17,18

The "mobile ad-hoc networks" MANETs have many advantages and one of the most important advantage is its "Infrastructure independent" nature. The ad-hoc networks does not need infrastructure's that is required for other wireless networks. The term infrastructure includes need of base stations, routers etc.

The ad-hoc networks are composed of the equal nodes that can communicate with each other through wireless links. Their is no central control for their work.

The important features of ad-hoc networks and MANET's are discussed in detail in this chapter.

The term MANET describes mobile, wireless, distributed multihop networks that could operate independent of infrastructure. A MANET network is composed of mobile, autonomous, wireless nodes that could be connected at network edges to that of the fixed wired Internet. Initially MANET is developed due to military requirements where infrastructure less, line of sight operations are required.

Salient features of MANET includes

1) Network size

It refers to the geographical coverage area that could be covered by the network. The number of nodes for a given geographical area represent network density.

2) Connectivity

It refers to many issues. One such is the number of neighbouring nodes that could link to them directly. This link may be bidirectional. Connectivity also refers to link capacity between any two nodes.

3) Network topology

The user mobility can affect the network topology. Due to it the network protocols has to adapt to topology changes. Conversely when nodes are inoperative due to dead batteries their will be rapid changes in topology.

4) User traffic

The design of MANET is thick related with user traffic. It includes some conditions like,

- Does the user traffic consist of bursty, shorter packets without periodic delays ?
- Does it contain longer packets sent periodically with fixed time bounds ?
- Or is it a combination of these two suitations ?

5) Operational environment

It refers to terrain whether it is a urban, rural or maritime etc. Due to any one of this LOS may not exist.

6) Energy

In MANET there is no availability of fixed base stations. A low energy network approach is tried with battery operated store and forward nodes in the network.

If some nodes are not participating in network operations shutting them for some time can be done.

In addition to there issues cost involved in MANET designed is also high that has to be planned with a proper balance with network features.

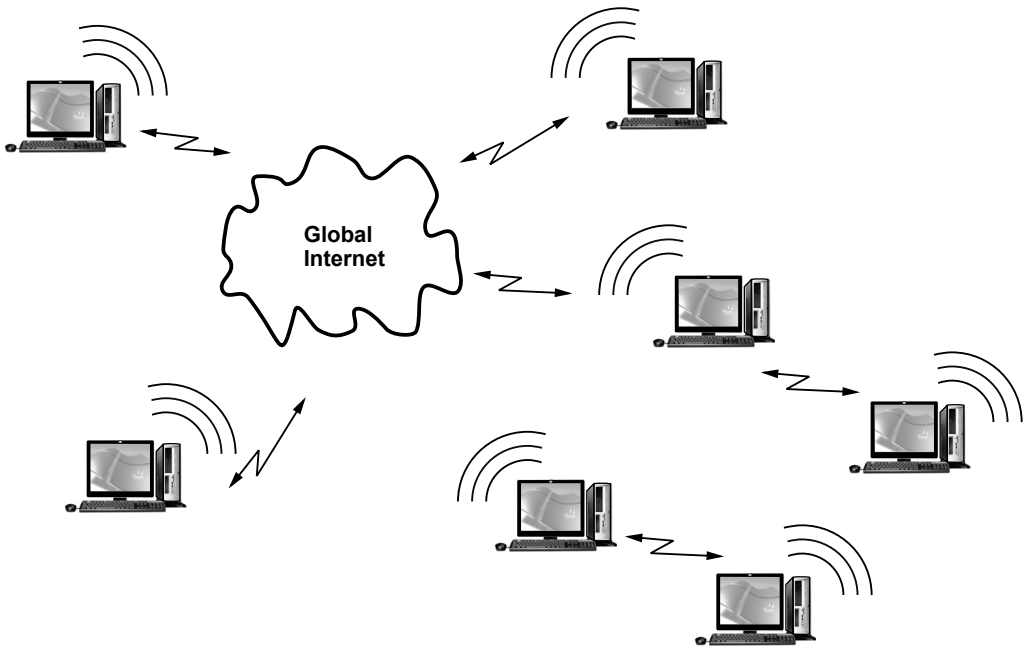


Fig. 4.2.1 MANET connected to Internet

Example for MANET

An example of MANET connected to Internet is shown above. Individual nodes transmits and receives data with globalized Internet arrangement.

A simple ad-hoc network composed of nodes and the complexity involved with network setup are shown in following diagrams.

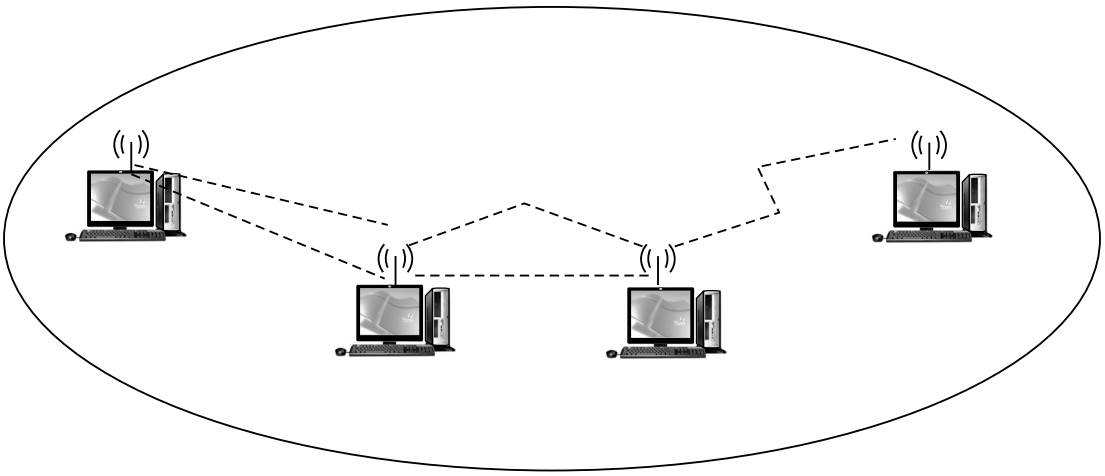


Fig. 4.2.2 Mobile ad-hoc network (MANET)

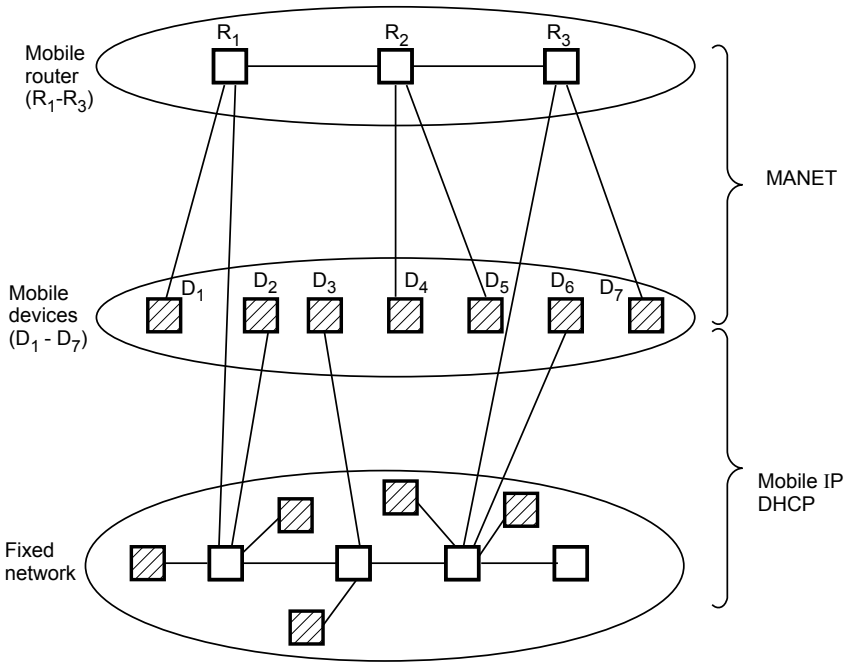


Fig. 4.2.3 MANET and mobile IP [→ Router ; → End system]

The mobile router (I) and mobile devices (II) forms MANET as shown here. It's relation with fixed network is established.

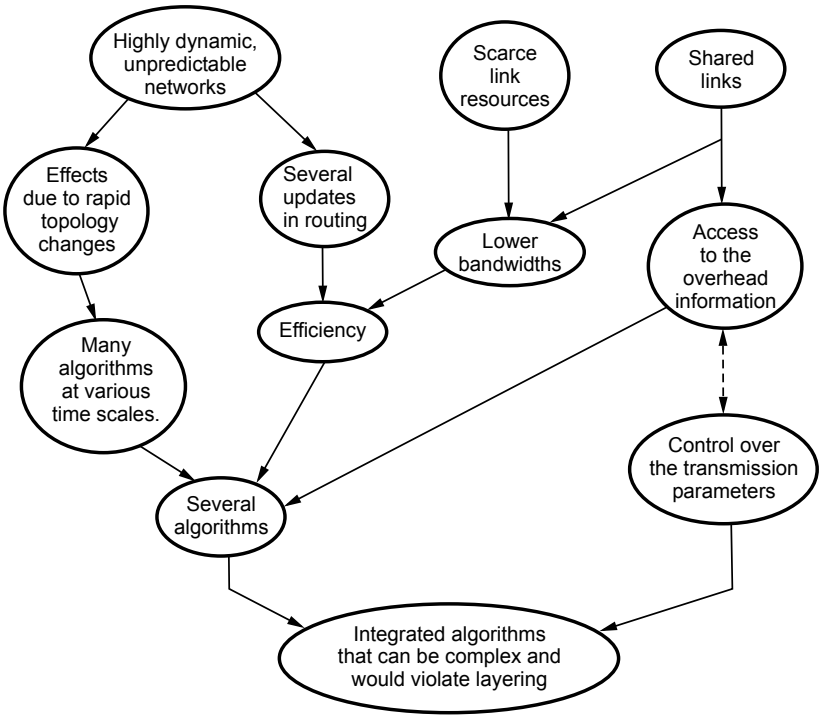


Fig. 4.2.4 Complexities in 'ad-hoc' network arrangement

4.3 Properties of Ad-hoc Networks

- The protocol design of ad-hoc networks are different from the fixed wired networks.
- In Mobile Ad-hoc Network (MANET) their is no dedicated network infrastructure devices available. The MANET is an architectureless wireless network. The radio propagation range of MANET is limited.
- Because of its range limitation, for covering a short distance it has to undergo many hops.
- In few specific scenarios for communication with other networks outside some of the devices have network connections with the outside base stations (BTS) and these devices acts as gateways for ad-hoc networks.
- The gateway devices are known as weakly connected ad-hoc networks.
- MANET's have two main features of wireless computing known as
  1) Weak connectivity and
  2) Resource constraints.
- MANET's have difficulties in managing bandwidth efficiency and data availability.

- Data management policies of architecture based wireless network cannot be applied directly to MANET's.
- The gateways of MANET's are not reliable as the base stations of other wireless networks.
- The gateways communications only with local hosts at low frequencies.
- MANET's are mainly peer-to-peer (P2P) networks.
- In MANET's there is no pre-existing infrastructures.
- These networks has limited accesses to a base station.
- They have power limitations.
- Their is no centralized controlling mechanisms.

4.4 Routing in MANET

AUI : Dec.-16, May-17,18

Routing is a complex task in ad-hoc networks. The destination node may be out of range with respect to source node which is transmitting data packets.

The purpose of routing is to find correct path between the source and destination for forwarding packets. If infrastructure is available in wireless networks routing will be an easier task because there the cells are defined.

But in ad-hoc network independent of infrastructure routine is tough task.

Thus in ad-hoc networks,

- The traditional routing algorithms will not be suitable.
- Centralized approaches will not be appropriate.
- Several nodes in network should have routing capability.
- They have no connection and ad-hoc network between nodes and they experience fast changing environment.
- If the load is less a method called as "flooding" can be applied in ad-hoc networking. But flooding is not an efficient method. To avoid looping as packets are forwarded, a hop counter should be used because the knowledge of maximum number of hops is very important. Still this flooding technique is not much used for packet forwarding.

4.4.1 Fundamental Steps in Routing

i) Forwarding the packets to next hop. That is from an input interface to an output interface in a traditional wired network.

ii) While forwarding packets sender much check for following parameters.

a) Packet reaching the destination.

b) Minimize the number of hops/path length.

c) Minimize the delay.

d) Minimize the packet loss.

e) Minimize cost involved.

4.4.2 MANET Vs Traditional Routing

- In MANET's each node is a potential router whereas most of the nodes in traditional wired networks do not route the packets.
- In MANET the nodes transmit and receive their own packets and they also forward packets to other nodes.
- In MANET the topology is dynamic because of the mobile nodes but relatively it is static in case of traditional routing methods.
- The routing in MANET must consider the layer 2 and layer 3 informations whereas in traditional routing protocols they rely on layer 3 information only.
- In MANET the link layer informations includes the data about connectivity and interferences.

  Main issues to be addressed by routing protocol in MANET are,

  1) Routing discovery

  2) Data forwarding

  3) Route maintenance.

4.5 Types of MANET Routing

AU : June-16, Dec.-16, 17, May-17,18

The MANET's routing protocols are classified as proactive (table-driven) and reactive (on-demand) types.

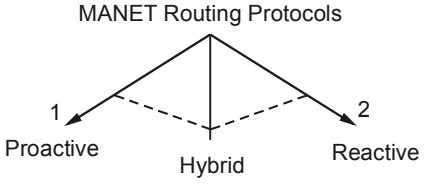


Fig. 4.5.1

These classification depends upon how they respond to any changes in network topology.

If a host is running a proactive protocol will react to topology change by propagating routing related informations to the neighbours. Such information transmission takes place whenever there is a change in link state is detected.

Two broader classification of routing protocols are unicast and multicast types.

1) Unicast routing protocols

a) Proactive protocols : Examples of the proactive (table-driven) protocols are

i) Destination sequenced Distance Vector (DSDV) protocol.

ii) Wireless Routing Protocol (WRP).

b) On-demand routing protocol : In this routing protocol routes are constructed according to the demand. It tries to find or maintain routes whenever necessary.

Examples of on-demand protocol are,

i) Dynamic Source Routing (DSR)

ii) Signal Stability based Adaptive Routing (SSA)

iii) Ad-hoc On-demand Distance vector Routing (AODV)

iv) Temporaly Ordered Routing Algorithm (TORA)

These protocols are reactive natured.

c) Hybrid routing protocol : A combination of reactive and proactive approach is also made. It is known as hybrid routing protocol.

Example of hybrid routing protocol proposal is Zone Routing Protocol (ZRP).

DSDV is like traditional distance vector routing technique. It is also called as "Bellman-Ford routing algorithm". The DSDV has few modified procedures to reduce routing loops.

Important operations of DSDV.

i) Each router in the network collects informations from all its neighbours.

ii) After gathering information node searches for a shortest path to route the packet.

iii) A new routing table is generated.

iv) Then the router will broadcast this table to its neighbours. Due to this function the other node (neighbours) are triggered to recompute their respective routing table.

v) This process continues till the routing information becomes stable.

4.5.1 Destination Sequence Distance Vector (DSDV)

Two important routing algorithms commonly used in MANET are,

a) Destination Sequence Distance Vector (DSDV)

b) Dynamic Source Routing (DSR)

In ad-hoc networks Destination distance vector (DVR) protocol was applied at first and then later the On-demand Distance Vector (AODV) protocol was used. The performance of DVR was not efficient, due to count-to-infinity problems. Because every

node exchanges with its neighbour table at regular periods. Changes that takes place at a node in network slowly propagates and thus it is not a better protocol to apply.

Some features added to DVR algorithm is known as Destination Sequence Distance Vector (DSDV) routing algorithm. Two features appended with DVR are namely,

i) Sequence numbers

ii) Damping.

i) Sequence numbers

Every routing advertisement should come with sequence number. These sequence numbers helps to apply the advertisements in a proper order. It helps to avoid looping.

ii) Damping

If the transcient changes in network topology prolongs for negligible time then it may not degrade the performance of routing mechanisms. A node waits if changes are unstable and this waiting time will depend on the time taken between first and the best advertisement of routing path to a definite destination node.

4.5.2 Dynamic Source Routing (DSR)

In this routing the routing task is divided into two different problems. It was analyzed in the period 1996 to 2002.

- Route discovery : It is nothing but the node searches for a correct destination for transmitting packet and currently their may be no correct route available.
- Route maintenance : If node has discovered a correct node it starts forwarding packets through it. But if the node transmits packets for a long time then in that case it has to make sure wheather the route is held upright. Thus route maintenance is essential for making sure of packet delivery to the intended node.

Like token rings in fixed type of networks also this DSR can be used. The periodic routing updates are not applied in this method.

Routing mechanism in DSR

Whenever a node discovers a route it will broadcast a route request with two parameters namely,

1) Identifier

2) Destination address.

If a node receives a route request it has to do the following things.

- If the node had received the request that is identified by unique identifier the node will drop its request packet.
- Once the node recognizes its destination node's address it shows that request has reached its target.

If it does not recognize the node will append its address to the list and then broadcast the new updated route request in the network.

4.5.3 Multicast Protocols for MANET's

In multicasting protocols the two classification are

i) Source-based protocol

ii) Core-based protocol.

These classification is based on how multicast tree constructions are made. The source-based protocol attempts to maintain a per source multicast tree from every source host to the members in the corresponding multicast group. Thus there will be many multicast trees in the network.

In core-based protocol there will be one multicast tree that is rooted at core host. There are several applications served by multicasting. One such is video conferencing.

In MANET due to its host mobility, broadcasting nature of wireless environment, interference, applying multicasting is difficult than in the case of other wireless and wired networks.

Under On-Demand Multicast Routing Protocol (ODMRP) the multicast tree is formed by periodical JOIN packets of host source.

Consider the source node 'S'. It will flood the JOIN_DATA packets to all other nodes in the network. When a host node receives first JOIN_DATA packet it will rebroadcast it to form a reverse path with the previous host. Each host in the network acts as multicast receiver. It receives JOIN_DATA packet and replies in turn with a JOIN_TABLE packet to the upstream to establish reverse paths.

The process repeats until source host 'S' is reached. The method of packet forwarding is for Fig. 4.5.2 (a) is shown in Fig. 4.5.2 (b). (See Fig. 4.5.2 on next page).

As the JOIN_TABLE is received a host has to build a multicast table so as to facilate future packet forwarding.

For example the host B receives the R_1's JOIN_TABLE as shown in Fig. 4.23.

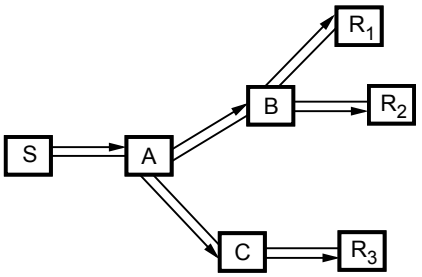
It will add R_1 as its next hop step. Assume B receives R_2's JOIN_TABLE. Now it will also add R_2 as its next hop step.

A simple final multicast table for each host is shown in Fig. 4.23 (c) in propagation of data packets.

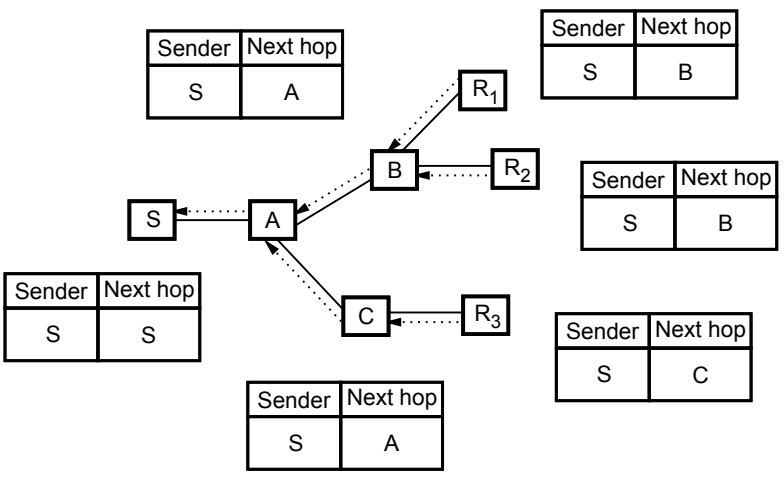
4.5.3.1 Multicast AODV Protocol

The on-demand distance vector routing protocol known as multicast AODV is an extension of unicast AODV protocol. Here the multicast tree is updated whenever a new host joins the multicast group. For making process of tree updation easier the route request packet (RREQ) is being broadcast.

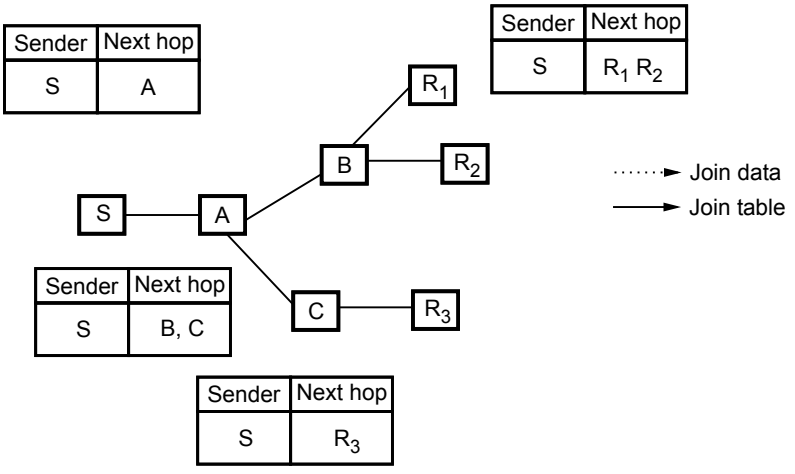
In case a host receives a RREQ and if the host is not a member of multicast group, then it will rebroadcast RREQ to the neighbouring members of the network.



(a) Load_data packets propagation



(b) Load_table packets propagation



(c) Last multicast table

Fig. 4.5.2 On-demand multicast routing protocol

But if the host is a member of multicast group and if this host receives a RREQ then it will give route reply (RREP) packet data to the sending host (S). Now the multicast table will be updated. By these processes forward path will be created.

If two RREQ's are received at a time then depending upon minimum number of hop count the one with minimum hop count will be selected.

MACT

It is multicast activation (MACT) packet. The source S will unicast a MACT packet to the next hop step. On receiving a MACT packet the next hop will enable for source host (route with minimum hop count) and it leads to multicast tree.

This procedure continues till a multicast member is reached successfully.

Distance vector algorithm design issues.

- The distance of each link in the network is a metric that has to be minimized.
  a) Distance of each link may have 'distance' 1 to reduce hop count.
  b) The algorithm attempts to reduce distance.
- The routing table at each node
  a) Specifies the next hop for each destination.
  b) Specifies the distance to the destination.
- Neighbours can also exchange routing table.
  Information for finding a route (or a better route) to reach the destination.

4.6 Vehicular Ad-hoc Networks (VANET) AU : June-16, Dec.-17, May-17,18

- VANET is a type of MANET with a few essential modifications.
- In order to regulate the traffic on the road and avoid accidents VANET is designed to provide real time information to the driver.
- With a range of about 300 m the vehicles which are embeded with sensors communicate with each other and other mobile facilitating devices.
- A VANET is a type of MANET where a group of moving vehicles forms a network.
- In larger networks multi-hop communication may result.
- If a vehicle goes out of the signal range it might be excluded from the network where it belongs to.
- In similar way a vehicle may enter into VANET's range and can join the network.
- Geographical information can be disseminated by VANET and can assist the driver in the moving vehicle.
- VANET helps the driver by giving warning information in advance in the form of messages.

Mobile computing

Mobile computing also refers to nomadic computing. It is capable of compute information remotely in mobile environment. Mobile computing comprises of two main concepts.

They are i) Mobility and ii) Computing

In computing, it carries out few processing steps related to services on a remote system.

Mobility denotes changing location while communication is on process.

4.7 MANET Vs VANET

AU : June-16, Dec.-16, 17, May-17, 18

MANET	VANET
It is mobile ad-hoc network.	It is vehicular ad-hoc network.
MANET has collection of mobile nodes.	VANET has collection of nodes where nodes refers to vehicles on roadside.
MANET is independent of infrastructure.	In VANET the vehicular nodes would communicate to network or nearest base station.
The nodes in MANET are random in nature.	Movement of nodes in VANET is restricted to road topology.
In MANET nodes may not experience random changes.	VANET experience random change in topology.

Security

Security is a critical issue as far as MANET is concerned. Preventing a deliberate attack on the network and blocking malicious content becomes all the more difficult nature of MANET. As the attack comes from within the network detection and prevention become cumbersome. Jamming the network and tying up the network with voluminous data overload could be easily done. Routing tables could be easily manipulated to convey misinformation so as to breach network security easily. Some of the major issues which cause serious security concern are discussed below :

Power supply : By spreading misinformation as mentioned above the network could be held up unnecessarily causing depletion in the battery backup.

Network boundary : The boundary cannot be demarcated as the mobile nodes take up the function of a router. Malicious content can be easily transmitted and using firewall becomes very difficult as it is impossible to judge the nature of the data flow.

Encryption : Encryption is rendered futile due to the limitations in computation. Without encryption the data remains exposed and vulnerable to attack.

Jamming : This could be easily done if a node is deliberately broadcasting misinformation and holding up data flow.

Security characteristics : The security characteristics of a network should ensure that it remains robust even in the eventuality of an attack.

Network sustainability : The flow of information should not be curtailed due to jamming.

Network authentication : Transmission must occur only between authenticated nodes and should be able to avoid decays.

Information security : Unauthorised access to the information must be strictly avoided.

Security issues are explained in the following chapter.

4.8 Security in MANET's

In recent years the mobile ad-hoc networks (MANET's) have attained tremendous attention due to its self configuration and self maintenance features. The aim of security solutions in MANETs is to provide security services like,

- Confidentiality
- Integrity
- Anonymity
- Availability to the mobile users.

Thus for security it is important to protect their protocol stack. The table shown below describe the security issues in each layer of protocol stack of MANET.

"In MANET the protection of the fundamental functionality to deliver data bits from one node to another node" is given top priority in providing security.

Sr. No.	Layer in protocol stack	Security issues in each layer
1.	Physical layer	Preventing the signal jamming deniel of service attacks.
2.	Data link layer	Protecting wireless MAC protocol and to provide link layer security support.
3.	Network layer	Protecting the ad-hoc routing and forwarding protocols.
4.	Transport layer	Securing and authenticating end-to-end communications through data encryption techniques.
5.	Application layer	Detection and prevention of viruses, worms, malicious codes etc.

Table 4.8.1 : Security issues in MANET

The multihop connectivity is provided in mobile ad-hoc networks in two different steps.

Step 1 : Ensuring single hop connectivity through the link layer protocols.

Example : Wireless Medium Access Control (MAC).

Step 2 : Extending connectivity to multiple hops through the network layer routing and data forwarding protocols.

Example : Ad-hoc routing.

There are two approaches for protecting MANET's namely proactive (prevents attacker in first place through cryptographic techniques) and reactive (detects security threats and react accordingly and it is posteriori natured) approaches.

The proactive approach is used for ensuring correctness of routing states whereas in the reactive approach is used for protect packet forwarding functions.

But as the number security features are increased there will be more computational complexity and it is also not economical.

4.8.1 Multifence Security Solution

In MANET multi-hop connectivity is provided through the distributed protocols in link and network layers. A better security approach is to have both proactive and reactive methods and all the three components should be encompased. The three components are

i) Prevention

ii) Detection

iii) Reaction.

The prevention component find the attacker by increasing the difficulty of entering the system. The detection and reaction components discovers only the occasional intrusions and take reactions so as to avoid pertaining adverse effects. The prevention component is achieved by secure ad-hoc routing protocols.

4.8.2 Network Layer Security

It is concerned with protecting network layer's functionalities for delivering packets through multihop ad-hoc forwarding method between mobile nodes. The proposals can be classified into two categories,

i) Secure ad-hoc routing protocols.

ii) Secure packet forwarding protocols.

4.8.3 Message Authentication Primitives

The messages are being transmitted between the nodes in the network. The content of these messages has to be authenticated and for security there are three cryptographic primitives are widely used. They are,

1) Message authentication codes

2) Digital signature

3) One-way HMAC key chain.

1) Message authentication codes

In this technique two node share a common secret symmetric key (k). They can generate and also check a message authenticator $h_k(\cdot)$ with help of a hash function 'h'.

A 'HMAC' could be verified by an intended receiver only ; the HMAC is a popular security primitive used for network layer.

2) Digital signature

It is based on asymmetric key cryptography. It includes signing or decrypting and the verifying or encrypting functions. It is not resilient against disk operating system attacks because an attacker may include false signatures and blocks verification process. If public key is known to all nodes then each node can verify digital signature such that digital signatures are more scalable to several receivers.

3) One-way HMAC key chain

There are many one-way cryptographic functions are available so that if output $\int (x)$ is given it not feasible to calculate input x value. Just by applying $\int (\cdot)$ in repeated manner on an initial input value then a chain of outputs can be found.

The computations incorporated in one-way key-chain-based authentication is less and an authenticator can verify larger number of receivers.

Notes

- Hash-chain based authentication need clock synchronization.
- Receivers should buffer a message for verifying when the key was revealed.
- A timer should be gauged carefully to monitor any second round of communication taking place due to key release.

Review Questions

Part A

1. *What is MANET?*
2. *What are the advantages of MANET?*
3. *List any three characteristics of ad-hoc networks ?*
4. *Mention any four advantages of MANET.*
5. *Write two properties of MANET.*
6. *What are the types of MANET routing protocols ?*
7. *What are the fundamental steps in routing ?*
8. *Write a note on VANET.*
9. *List any two security issues in MANET.*
10. *What is traditional routing ?*
11. *List the characterstics of MANETs.* **(Refer section 4.1.1)** **AU : June-16, Marks 2**
12. *Compare MANET Vs. VANET.* **(Refer section 4.7)** **AU : June-16, Marks 2**
13. *What is multicasting ?* **(Refer section 4.5)** **AU : Dec.-16, Marks 2**
14. *Compare and contrast MANET Vs VANET.* **(Refer section 4.7)** **AU : Dec.-16, Marks 2**
15. *List the applications of MANETs.* **(Refer section 4.2)** **AU : May-17, Marks 2**
16. *Distinguish proactive and reactive protocols.* **(Refer section 4.5)** **AU : May-17, Marks 2**
17. *What is the purpose of DHCP ?* **(Refer section 4.2)** **AU : May-18, Marks 2**
18. *Compare VANET with MANET.* **(Refer section 4.7)** **AU : May-18, Marks 2**
19. *Differentiate cellular with adhoc networks.* **(Refer sections 4.1 and 4.1.1)** **AU : May-18, Marks 2**

Part B

1. *What is MANET ? Explain the characteristics and applications of MANET.*
2. *Discuss the routing in MANET in detail.*
3. *Explain traditional Vs MANET routing protocol in detail.*
4. *Write short note on : i) MANET ii) VANET and iii) Traditional routing*
5. *Explain vehicular ad-hoc networks in detail.*
6. *What are the applications of MANET ? Explain any one type of routing.*
7. *Explain MANET Vs VANET in detail.*
8. *What are the popular routing protocols used in MANET ? Explain.*
9. *Explain the characteristics of MANET. Comment on traditional routing protocols.*
10. *Explain the security issues in MANET in detail.*
11. *Explain Characteristics, Applications of MANET.* **(Refer sections 4.1, 4.1.1 and 4.1.2)** **AU : June-16, Marks 8**

12. *Explain DSR routing protocols in detail.* **(Refer sections 4.5 and 4.5.2)** **AU : June-16, Marks 8**

13. *Draw and explain the architecture of VANET.* **(Refer section 4.6)** **AU : June-16, Marks 8**

14. *Explain the various Security and attacks on VANET.* **(Refer section 4.7)** **AU : June-16, Marks 8**

15. *Explain the traditional routing protocols.* **(Refer sections 4.4 and 4.4.2)** **AU : Dec.-16, Marks 16**

16. *What are multicast routing protocols ?* **(Refer section 4.5)** **AU : Dec.-16, Marks 8**

17. *What are reactive and proactive protocols ? Specify its advantages and disadvantages.* **(Refer section 4.5)** **AU : Dec.-16, Marks 8**

18. *Explain the design issues of MANET routing protocols in details.* **(Refer sections 4.4 and 4.5)** **AU : May-17, Marks 16**

19. *Explain any two VANET routing protocol with an example.* **(Refer sections 4.6 and 4.7)** **AU : May-17, Marks 16**

20. *Discuss route discovery and route maintenance mechanisms in DSR with illustrations. List its merits and demerits* **(Refer section 4.5.2)** **AU : Dec.-17, Marks 16**

21. *Describe the architecture of VANET with the functionality of the components. Compare VANET with MANET.* **(Refer sections 4.6 and 4.7)** **AU : Dec.-17, Marks 16**

22. *Describe the architecture of VANET with a neat diagram.* **(Refer section 4.6)** **AU : May-18, Marks 13**

23. *Explain the design issues in MANET and the applications of adhoc network..* **(Refer sections 4.2)** **AU : May-18, Marks 13**

24. *Consider the network given below. Here 'S' is source node and 'D' is target node. Illustrate the process of route discovery, route reply, data delivery and route caching using DSR. Explain the approach.* **(Refer sections 4.4.1, 4.5.2 and 4.5.3)** **AU : May-18, Marks 15**

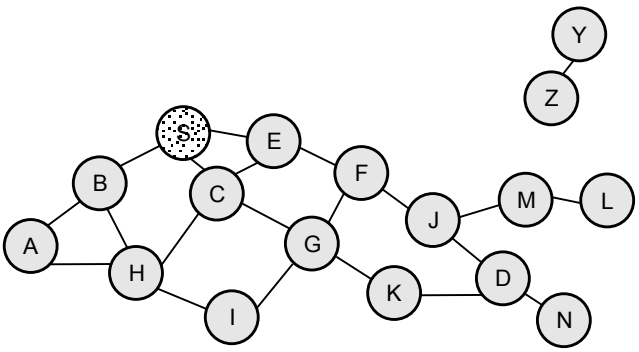


Fig. 4.1

25. *Enumerate the processes involved in data packet delivery using mobile IP in adhoc networks.* **(Refer sections 2.3, 2.3.2, 4.4 and 4.4.1)** **AU : May-18, Marks 15**

Notes

Unit V

Mobile Platforms and Applications

Syllabus

Mobile Device Operating Systems - Special Constrains & Requirements - Commercial Mobile Operating Systems - Software Development Kit: iOS, Android, BlackBerry, Windows Phone - M - Commerce - Structure - Pros & Cons - Mobile Payment System - Security Issues.

Contents

5.1 Mobile Device Operating Systems

The main responsibility of mobile devices is to monitor effective utilization of the resources by attending to several tasks. The resources may include, processor, files, memory and other devices, like speaker, keyboard, camera etc.

Basically mobile devices have to process many applications that may run several tasks. Each task in it may have many threads.

They might be voice communication, e-mail, text messaging, recording and so on. The operating system of the mobile device acts as an interface to the user of the mobile device and also interacts with other devices.

5.2 Special Constraints and Requirements of Mobile Operating System

AU : May-17,18, Dec.-16,17

A mobile device has several constraints. One of them is handling a limited energy in the battery. The complex tasks has to be completed fast and goes to sleep mode. But this is not the case with traditional computer. Hence the mobile device is turned on often, and a mobile operating system (OS) undergoes booting process many times.

In addition to this the size of Kernal is very small. In design of mobile device operating system meets many constraints to work efficiently.

The specific constraints of mobile OS are listed here.

Processing power

The mobile OS has limited processing power. Few processors are energy efficient, cost effective and also powerful. The chip size and off-chip memory size is limited.

Since the mobile OS has to overcome the problems like restricted power, storage etc. it can process only lesser number of functions.

Battery power

The mobile device has to be light weight to make ease of portability. Mobile device has smaller battery. The mobile OS is expected to consume only less power.

The processor and the display screen are often put to sleep mode for managing with little power.

Memory

A mobile device has lesser volatile and permanent storage. As the memory is less, the OS has to be smaller. But the OS should be capable of processing several tasks to serve the market demand. The Kernel size has to be planned carefully.

Limited screen size and keyboard

The screen size of mobile device should be small for better portability. This leads to limited size of displaying screen.

The mobile device can have a smaller size keypad or a display screen (acting as keypad) in touch screen mode with the help of stylus. But still comparing to desktop systems the documentation jobs including typing are difficult in the hand held mobile devices.

Bandwidth

The wireless medium is susceptable to noise, multipath fades and would result in higher Bit Error Rates (BER). In mobile environment the bandwidth also fluctuates which may cause noise in the device performance. This results in hand-offs in the communication. For uninterrupted communication factors like prefetching, data caching, and integration are useful.

5.3 Service Requirements

Particular communication protocol

A mobile device has to communicate with the nearest base station, peripheral devices and other devices. The communication protocols used are based on 1G and 2G technology. To communicate with other computers TCP / IP and WLAN protocols are also used.

Compliance with open standards

If open standards are accepted then it will facilitate more applications from user's end. The mobile OS has to consider smaller screen size, limited memory, limited battery power, less weight in its designing aspects.

Library support

The mobile OS should offer Library support for various applications in order to make it convenient for the developers. The basic library support includes facilitating e-mail, SMS, bluetooth, MMS and GSM / GPRS related functionalities. Thus the mobile OS needs the above service requirements.

An interface should consider access control data and also the voice communication with that of the base station making use of various protocols.

Also an operating system recognizes input information from the keyboard, analyze it and send the output information to the display.

It also interfaces with other devices like computer, printer etc. Some of the popular device operating systems include,

1. Symbian
2. Android
3. Windows mobile
4. Palm OS
5. Blackberry
6. iOS etc.

5.4 Device Management

The challenges included in device management is discussed below. The challenges involved in device management are ;

- Device location tracking.
- User-device relationship.
- Updating software of the existing devices.
- Installation of new software and adaptability.
- Providing secured access to the device information.
- Control of device versions and softwares.

Software distribution

It deals with problem of obtaining new software or updating existing software to the devices. A better device management system must consider following issues into consideration.

- Hardware version management.
- Hardware capabilities.
- Software version management.
- Device connectivity.
- Library Management.
- Insecured connections.
- Unstable connections.
- Updating operating system.

Approaches

For pervasive devices all the above solutions cannot be attended. To achieve device management the devices has to be separated from each other by using unique identifiers. There are few techniques available to counter software download problem. It includes ;

- Hardware capabilities.

- Library management.
- Hardware and software versions management.
- Insecured connections.
- Updation of operating systems.
- Devices connectivity

In system design of device management both the server side and pervasive computing devices has to be considered. The data management in server layer can be solved with IT or database management systems like Hewlett-Packard open view Tivoli (IBM) etc.

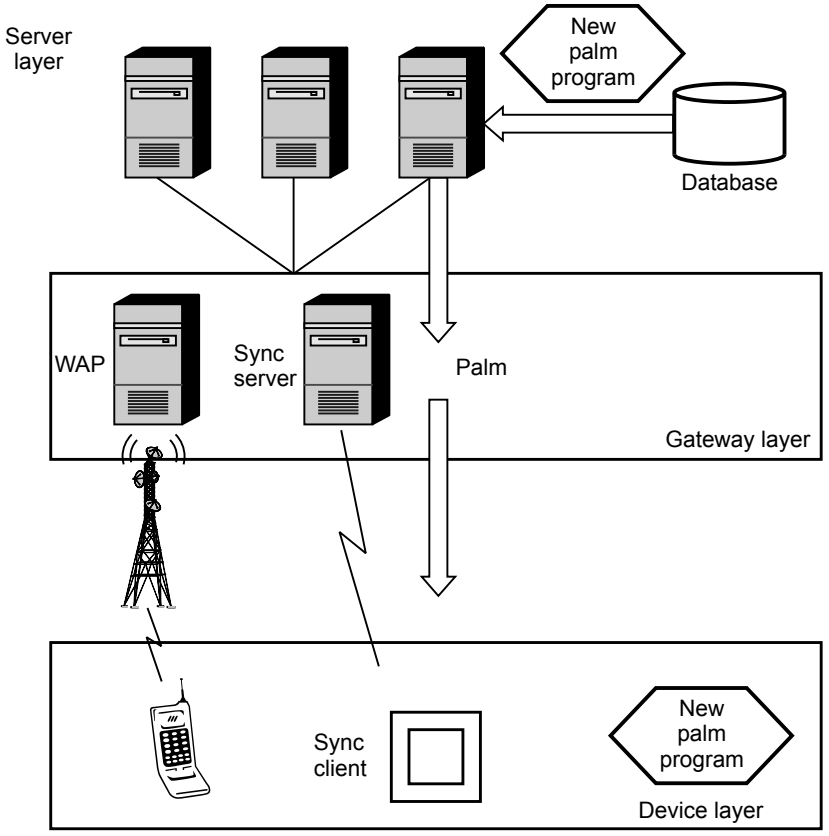


Fig. 5.4.1 Device-management System

In the above device management system the gateway layer consists of the device gateway for every single device with proper synchronization. The software updation problems can be solved with proper synchronization.

5.5 Commercial Mobile Operating Systems

AU : June-16, Dec.-16, May-17,18

Designing an operating system for mobile device is a difficult task. The mobile OS should have a set of expected core capabilities for supporting the mobile devices. The mobile OS also be capable to allow a vendor to develop an application software with the device.

Some of the mobile operating devices are given below.

5.5.1 Palm OS

The Palm OS is a successful operating system for the PDA'S. The Palm OS is intended for PDA'S. It comprises of limited numbers of features attractive like low memory and processor usage. Due to restricted memory usage longer battery life is guaranteed. The Palm OS was mainly designed for better use of touch-screen based user interfaces. Palm OS was developed by Palm computing for PDA's. It was improved with more facilities for several mobile devices, like smart phones.

The main features of Palm OS include :

- It has elementary memory management system.
- Palm provides Palm emulator.
- Handwriting recognization of input is possible with Palm OS.
- It also supports recording and playback in the system.
- Palm OS is a single-operating system.

The architecture of Palm OS consists of user interface, memory management, system management, and communication unit.

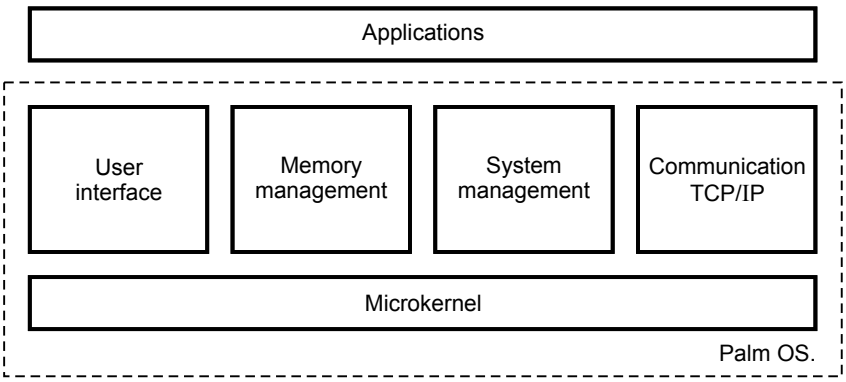
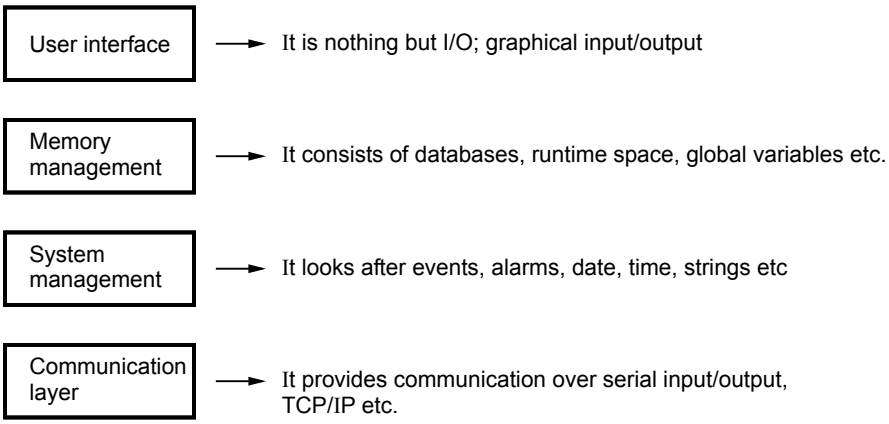


Fig. 5.5.1 Palm OS architecture



The main features of Palm OS are,

- User management
- Task management
- Power management
- User interface
- OS size
- Memory management.

The memory management is divided into available memory into, dynamic heap dynamically allocated memory and storage. The Palm OS supports C and C++ softwares. At the beginning stage C++ is useful and for extensive works C is used. The Palm development environment consists of Software Development Kit known as (SDK) which is based on GNU for windows etc.

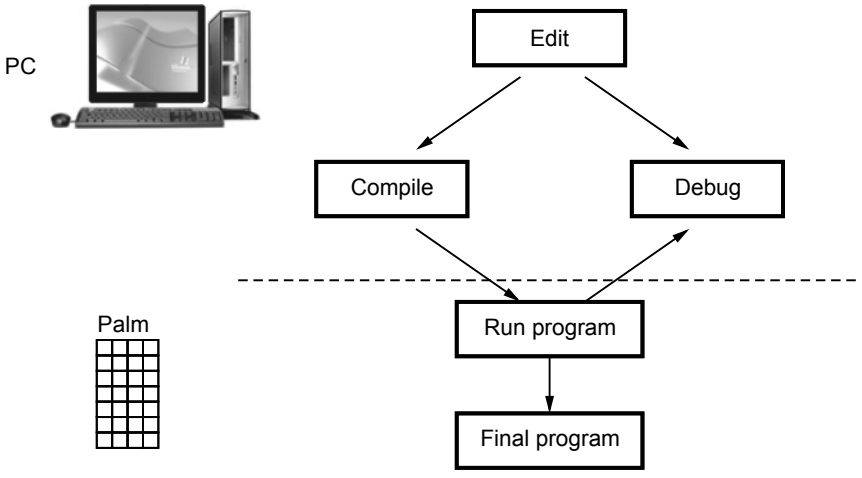


Fig. 5.5.2 Palm development cycle

The palm supplies a palm emulator that can emulate the palm hardware on the personal computer PC. This can be downloaded to real palm device. A simple palm development cycle is shown above. The program can be edited, compiled and allowed to run with palm platform. The palm applications are synchronous and event-driven. They consists of event handling and main event loop.

5.5.2 EPOC

The EPOC OS was created by the Psion and it is presently maintained by Offspring company called as 'Symbian'. It was founded by Psion, Motorola, Ericsson, Panasonic and Nokia in the year 1998. This OS was meant for phones.

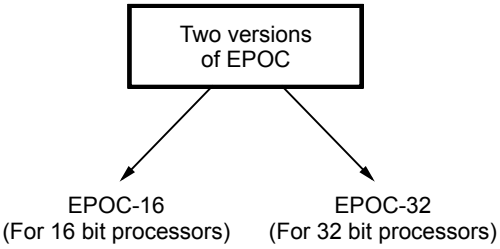


Fig. 5.5.3

The EPOC has captured Asian market. EPOC is capable of displaying 256 colors. In EPOC core operating system functionality multitasking is possible. When compared with Palm OS which can handle one task at a time. The EPOC OS can handle multiple tasks at same time.

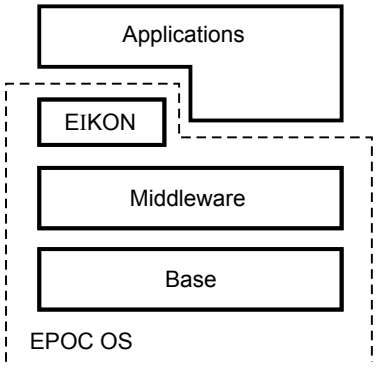


Fig. 5.5.4 EPOC operating system architecture

The EPOC operating system consists of

- User management
- Task management
- Memory management and
- User interface

The different programming languages that are supported by the EPOC OS are Java, C++, BASIC - like language etc. For system development the language choice is C++ .

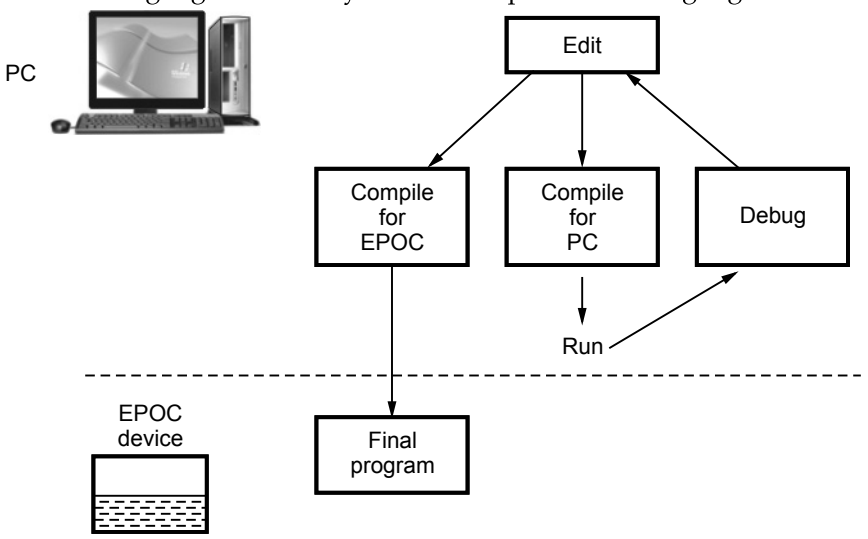


Fig. 5.5.5 EPOC development cycle

EPOC OS relies on multitasking. It supports both synchronous and asynchronous applications.

5.5.3 Windows OS

It is an embedded OS developed by Microsoft. The window CE is basically a modular OS and it is configured by device manufacturer. In its architecture the kernel provides necessary memory management, task scheduling and interrupt handling. The user interface functions of the graphical output and user input are integrated by the Graphics Windows and Event Manager (GWE). The possible communication interface are infrared communication through TCP/IP, IrDA and serial drivers etc.

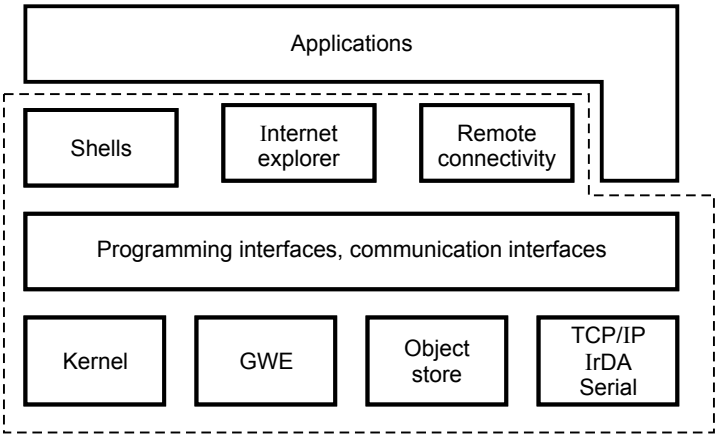


Fig. 5.5.6 Windows CE architecture

The main features offered by Windows CE are,

- User management
- Task management
- User interface
- Memory Management
- Operating system size etc.

The software development for Windows CE is mainly based on Win 32 API. It concentrates on application software development. The related professional development tools are Visual Basic, Visual C++ etc.

The Windows CE is popular due to its wider application support platform.

In the evolution of Windows mobile OS from the year 1996 to 2010, it is improved as Windows CE Versions 1.0, 2.0, Pocket PC, Windows mobile and then Windows phone 7.

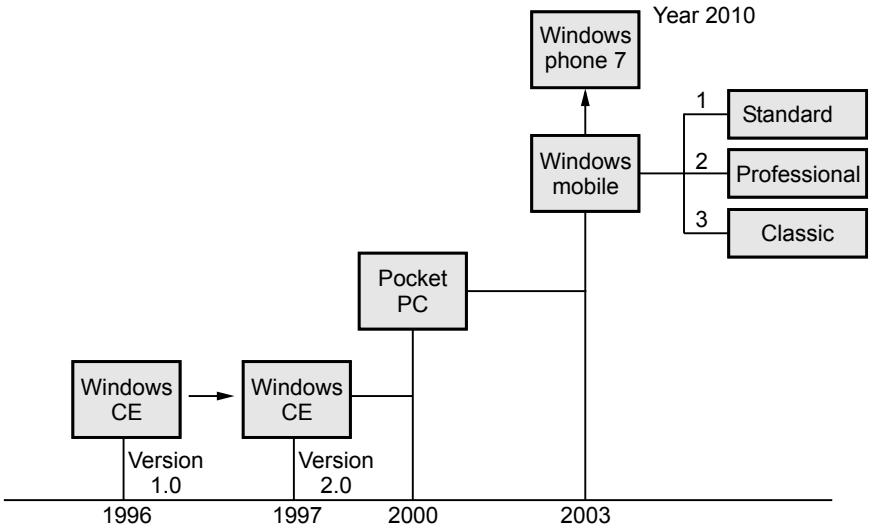


Fig. 5.5.7 Windows mobile OS

The Windows mobile OS is available from the Microsoft. This operating system supports the touch screen facility for the user. The family of Windows mobile OS has three types namely standard, professional and classic. The first two types are planned for smartphone design whereas the classic type OS is focussed for PDA's and not for the cell phone design.

Some Features of Windows Mobile OS :

- For security cryptographic library is available.
- Virtual memory management is provided.

- The GWE can handle input and output (GWE - Graphics/Window/Event Manager).
- An improved version of Windows mobile OS may also support multitasking tasks.

5.5.4 Symbian OS

The Symbian OS was the popular OS in smart phone operating system. It was the OS used in mobile handsets that was manufactured by Ericsson, Panasonic, Nokia and Samsung. Symbian OS was developed with some of the mobile device manufacturers as mentioned above. It was suitable for installing in smart phones.

The symbian OS is a multitasking real time, 32 bit OS and it runs on the ARM-based processors design. Also the design of Symbian OS is micro-Kernal based. The other features include;

- Whenever application is not responding to a particular event CPU is switched in low-power mode.
- It is designed for low memory and power requirements.
- It also supports pre-emptive multitasking tasks.
- Symbian OS supports many networking and communication protocols.

5.6 Software Development Kit

AU : June-16, Dec.-17, May-18

It includes operating systems such as

i) iOS

ii) Android Operating System

iii) Blackberry Operating System

5.6.1 iOS

The iOS was the sleek mobile device. The iPhone which made a revolution in the smart phone market. Also iPhone replaced the popular iPod. The iOS was developed in 2007 by Apple and iOS was suitable OS for iPhone. This iOS is a proprietary OS owned by Apple. It was not designed to be made use by other mobile phone vendors. iOS has features like;

- Better user interaction including swipe, tap etc.

5.6.2 Android

In the year 2005 Google made a small beginner company known as Android, that was developing an OS for mobile hand held devices which was based on Linux. An open handset alliance was set up by Google in the year 2007.

Android operating system is a open source software for mobile handheld devices that has been developed by around 82 companies with several technical collaboration. Android provided many user friendly features.

Android permits other application developers for coding with Java.

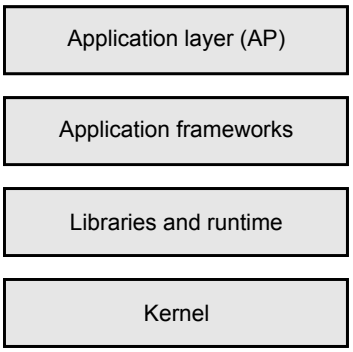


Fig. 5.6.1 : Android simple software stack

The simple Android code has four layers :

i) Application Layer (AP) :

The applications such as email, SMS, calender, web browser etc. are written using Java (J2ME). Android provides most of the basic applications.

ii) Application framework :

It is used for implementing a structure for variety of applications. This framework facilitates the user with services to develop applications.

The system manager includes content provider and manager.

iii) Library and runtime :

Android OS has libraries and runtime. Multiple languages such as C and C++ are used for its library. A Java interface is made use for calling a library function.

The runtime contains two main components. A group of libraries is used. The second runtime component is Dalvik virtual machine. A Java program is translated into machine code of device using Dalvik virtual machine.

This code is executed by the OS. It is then compiled to an ARM code, and also installed with help of Android Kit (SDK).

iv) Kernel :

The Kernel of Android OS is based on Linux Kernel. Android implements its mobile device drivers, process management, memory management and also networking functions based on Linux Kernel code.

- Android permits applications to run concurrently.
- Multitasking is possible with this OS.

Advantages of Android OS Include

i) It has open platform and suitable for many mobile phones.

ii) It needs lower footprint of 250 kB.

iii) It supports libraries and robust in nature.

iv) It has an integrated web browsing.

v) It uses Java as open programming language and it is user friendly.

5.6.3 Blackberry OS

The Blackberry OS is designed for the Blackberry smart phone systems which is produced by RIM (Research In Motion Limited). Blackberry OS is a proprietary operating system. It facilitates an excellent email system in the market.

- It provides high degree of security with good on-device message encryption.
- It allows instant mailing.

5.7 M-Commerce

AU : June-16, Dec.-16, May-17, 18

Mobile Commerce (M-Commerce) is an application of mobile computing. The activities linked to selling buying, or any service are included in M-Commerce in mobile devices. Buying and selling in M-Commerce is made and care has to be taken in making payment with security. The mobile payment is in e-payment mode.

There are several applications possible with this M-Commerce. Also the two categories of it are namely :

i) Business-to-Consumer (B2C) applications.

ii) Business-to-Business (B2B) applications.

i) B2C applications :

In this type a product/service can be sold by a business firm to a consumer.

B2C applications includes,

- Advertising
- Mobile ticketing task
- Product information
- Payment services
- Loyalty services
- Catalogue shopping etc.

ii) B2B applications :

It is a form of commerce where a product/service can be sold from company firm to the dealers, and not to the consumer directly.

Some of the B2B applications includes,

- Stock tracking and control tasks,
- Inventory management etc.

5.8 Structure of M-Commerce

AU : June-16, Dec.-16, May-17

A simple architecture of a mobile commerce (M-Commerce) is shown below. Each layer in it has its own functionality to perform in the framework.

The layers includes mobile device, client, application and host computer linked with Internet.

Some of the features required by the device for enabling M-Commerce are;

- Camera facility
- Internet
- RFID
- SMS and MMS
- Ability for scanning bar codes
- Efficient display system.

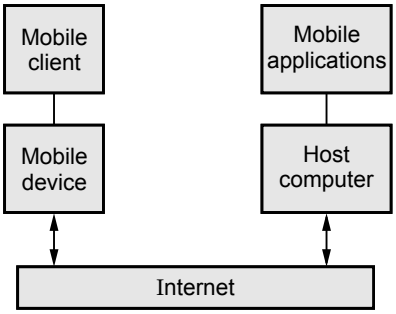


Fig. 5.8.1 A simple architecture of M-commerce framework

Network :

The user's requests are sent to the neighbouring wireless access point (WLAN) or to a Base Station (BS).

For M-Commerce wired networks are not essential. The server or a host computer are connected with Internet.

Mobile middleware :

The use of middleware is to map the Internet contents to mobile devices with transparency. Then it would support many operating systems and protocols. Middleware also provide secured communication with encryption and decryption techniques.

Host computers or servers :

It stores all informations required for M-commerce application. Most of the application programs consists of three main components namely;

Database servers : Used to store data.

Web servers : Help for interacting with mobile device

Support software : To implement the useful business logic of M-Commerce.

In M-Commerce all the four layers forms the structure or framework to handle several applications.

Pros and Cons :

The Mobile Commerce (M-Commerce) has several advantages and disadvantages.

i) Advantages :

- Mobile handheld devices can be personalized.

- The advantages of using M-Commerce in business organization includes, cost savings, business opportunities etc.
- M-Commerce is user friendly, providing light weight, flexibility etc.

ii) Disadvantages :

- The mobile devices has small screen which might limit user's menu choice, text typing capabilities.
- Mobile devices usually do not provide processing power or graphics of personal computers.
- Restricted bandwidth limits reach of M-Commerce everywhere in practical scenario.

5.9 Mobile Payment Systems

AU : June-16, Dec.-16,17, May-18

A number of mobile payment methods are in vogue viz

1) Micro payment

2) Credit card

3) Bank payment

Payment is usually made in by the service provider e.g. bank and the appropriate recovery made from the user.

1) Micro payment :

Payment made for purchase of Coca Cola by vending machines is a case in point. The service provider and phone company coordinate in managing the vending machine process. The mobile phone call made by the customer and the vending machine interact. This enables smaller purchases easier.

2) Credit card :

When the credit card and the mobile phone of the user are linked making an M-payment Via the Credit card to the vender is possible. Payment is easily made into the account of the seller.

3) Bank payment : Through Bank the payment can be done by linking, the bank account and mobile number. Payment on purchase is directly made into the account of the seller from the account of the buyer which are all linked by the mobile.

Security Aspects

This is a very tacklish issue which has a number of ramifications. Tracking the mobile device could itself be hectic The problems of misuse can be aggravated due to theft or loss. The identity of the user cannot be ascertained and dubious users can easily get away with fraud.

M payments are attractive, easy and customer friendly. However using the mobile to make payments is not without its risks. Simplification in the payment procedures does not automatically enable authenticated money transfers and online purchases.

5.10 Security

AU : June-16, Dec.-16

- Mobile commerce has better security and privacy.
- Subscribers of mobile devices would be difficult task for tracing due to roaming.
- Mobile devices also work in both on-line and off-line.
- But when a mobile device is lost it is a complex task to trace the device.
- Authentication mechanism still has to improve for M-Commerce devices.

Review Questions

Part A

1. *What is the significance of device OS ?*
2. *List two constraints of mobile device OS.*
3. *Mention any two mobile operating system.*
4. *Write a note on Palm OS.*
5. *What is the function of iOS ?*
6. *Write a note on Android.*
7. *List the four layers of structure of Android.*
8. *Write a note on Blackberry.*
9. *What is M-Commerce ? Give two advantages.*
10. *Write a short note on mobile payment system.*
11. *What is M- Commerce ?* **(Refer section 5.7)** **AU : June-16, Marks 2**
12. *Differentiate E-Commerce and M-Commerce.* **(Refer section 5.7)** **AU : Dec.-16, Marks 2**
13. *Explain the pros and cons of M-commerce* **(Refer section 5.8)** **AU : May-17, Marks 2**
14. *What are limitations of mobile computing ?* **(Refer section 5.2)** **AU : Dec.-16, Marks 2**
15. *What are the special constrains and requirements of mobile O/S* **(Refer section 5.2)** **AU : May-17**
16. *What are the constraints in mobile OS ?* **(Refer section 5.2)** **AU : Dec.-17**
17. *What are the advantages and disadvantages of BlackBerry OS ?* **(Refer section 5.6.3)** **AU : Dec.-17**
18. *What is M-Commerce ? List its disadvantages.* **(Refer section 5.7)** **AU : May-18**
19. *What are the constraints of mobile device OS ?* **(Refer section 5.2)** **AU : May-18**