UNIT V

MOBILE PLATFORMS AND APPLICATIONS

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

1) What is Android and its advantages?

It is an open-sourced operating system that is used primarily on mobile devices, such as cell phones and tablets. It is a Linux kernel-**based system that's been equipped with rich components that allows** developers to create and run apps that can perform both basic and advanced functions.
Advantages

- Open-source
- Platform-independent
- supports various technologies (camera, Bluetooth, wifi, speech, EDGE)

2) What Is the Google Android SDK?

The Google Android SDK is a toolset that developers need in order to write apps on Android enabled devices. It contains a graphical interface that emulates an Android driven handheld environment, allowing them to test and debug their codes.

3) What is the Android Architecture?

Android Architecture is made up of 4 key components:
– Linux Kernel
– Libraries
– Android Framework
– Android Applications

4) Describe the Android Framework.

The Android Framework is an important aspect of the Android Architecture. Here you can find all the classes and methods that developers would need in order to write applications on the Android environment.

5) What is the use of an activityCreator?

An activityCreator is the first step towards the creation of a new Android project. It is made up of a shell script that will be used to create new file system structure necessary for writing codes within the Android IDE.

6) Describe Activities.

Activity: Each activity presents a GUI screen of an application. An activity is a single, focused thing that the user can do. Whenever user click on GUI the next Activity will be start and new GUI set base on coding.

For example, a chat application might have one activity that allows to create a chat, another to view the previous chat sessions, etc

7) What are Intents?

Intent is exactly what it describes. It's an "intention" to do an action. Intents displays notification messages to the user from within the Android enabled device. It can be used to alert the user of a particular state that curred. Users can be made to respond to intents.

8) Differentiate Activities from Services.

Activities can be closed, or terminated anytime the user wishes. On the other hand, services are designed to run behind the scenes, and can act independently. Most services run continuously, regardless of whether there are certain or no activities being executed.

9) Define POS. (Nov/Dec 2016)

Point-of-Sale (PoS) usually means a checkout counter in a shop or supermarket. More specifically, the point-of-sale often refers to the hardware and software used for handling customer purchases at the checkout desks. An example of a PoS terminal is an electronic cash register. Nowadays, the point-of-sale systems are used in almost every supermarket and are used in many retail stores too.

10) What is the importance of Android in the mobile market?

Developers can write and register apps that will specifically run under the Android environment. This means that every mobile device that is Android enabled will be able to support and run these apps. With the growing popularity of Android mobile devices, developers can take advantage of this trend by creating and uploading their apps on the Android Market for distribution to anyone who wants to download it.

11) What do you think are some disadvantages of Android?

Android is an open-source platform, and the fact that different Android operating systems have been released on different mobile devices, there’s no clear cut policy to how applications can adapt with various OS versions and upgrades. One app that runs on this particular version of Android OS may or may not run on another version.

The mobile devices such as phones and tabs come in different sizes and forms, it poses a challenge for developers to create apps that can adjust correctly to the right screen size and other varying features and specs.

12) What is ADB?

Adb is short for Android Debug Bridge. It allows developers the power to execute remote shell commands. Its basic function is to allow and control communication towards and from the emulator port.

13) What are the four essential states of an activity?

Active – if the activity is at the foreground
Paused – if the activity is at the background and still visible
Stopped – if the activity is not visible and therefore is hidden or obscured by another activity
Destroyed – when the activity process is killed or completed terminated

14) Differentiate E-Commerce and M-Commerce.(Nov/Dec 2016)

E-commerce or electronic **commerce**, is the process of buying and selling goods, products and services over electronic systems such as internet, telephone and **e**-mail.

M-Commerce or **mobile commerce** is process of buying and selling products and services through wireless handheld devices such as cell phones or PDAs

15) What role does Dalvik play in Android development?

Dalvik serves as a virtual machine, and it is where every Android application runs. Through Dalvik, a device is able to execute multiple virtual machines efficiently through better memory management.

16) What is Radio Frequency Identification?

A Radio Frequency Identification (RFID) tag attached to a product, animal, or person for the purpose of identification and tracking, makes use of radio waves. Some tags can be read from several metres away and beyond the line of sight of the reader.

17) Do all mobile phones support the latest Android operating system?
Some Android-powered phone allows you to upgrade to the higher Android operating system version. However, not all upgrades would allow you to get the latest version. It depends largely on the capability and specs of the phone, whether it can support the newer features available under the latest Android version.

18) What is portable wifi hotspot?

Portable Wi-Fi Hotspot allows you to share your mobile internet connection to other wireless device. For example, using your Android-powered phone as a Wi-Fi Hotspot, you can use your laptop to connect to the Internet using that access point.

19) What is an action?

In Android development, an action is what the intent sender wants to do or expected to get as a response. Most application functionality is based on the intended action.

20) What is the difference between a regular bitmap and a nine-patch image?

In general, a Nine-patch image allows resizing that can be used as background or other image size requirements for the target device. The Nine-patch refers to the way you can resize the image: 4 corners that are unscaled, 4 edges that are scaled in 1 axis, and the middle one that can be scaled into both axes.

21) What language is supported by Android for application development?

The main language supported is Java programming language. Java is the most popular language for app development, which makes it ideal even for new Android developers to quickly learn to create and deploy applications in the Android environment.

Inventors of android: Andy Rubin, Rich Miner, Nick Sears

22) Features of Android OS?

Live wallpaper , Camera , Messaging, Bluetooth, WIFI, Web Browsing, Music, **Alarm etc.**

- Google now (voice assistant)
- NFC (Near Field Communication)
- Unlock your phone by your face
- Use your phone with joystick to enjoy gaming experience
- Connect your phone with LED TV via MHL or micro HDMI cable
- Screen Capture
- Multitasking Future (Task Switcher)
- Data Usages (Check and also set limit from device)

23) Tools Required for Developing Android Apps?

Tools:

- Java Development Kit (**JDK**)
- Android Development Tools (**ADT**) - Android Studio by Google
- Software Development Kit (**SDK**)

Languages:

- Java
- XML

24) Android application main components are?

Components	Description
Activities	They dictate the UI and handle the user interaction to the smartphone screen
Services	They handle background processing associated with an application.
Broadcast Receivers	They handle communication between Android OS and applications.
Content Providers	They handle data and database management issues.

25) What is AVD?

AVD Stand for Android Virtual Device (emulator), The Android SDK includes a mobile device emulator - a virtual mobile device that runs on your computer.

26) Give four examples of Mobile OS? (May/June 2015)

The mobile OS has to also facilitate third party development of application software and yet allow manufacturers of different brands of mobile devices to build their choice set of functionalities for the users.

Types of Mobile Operating System:

- Windows Mobile
- Palm OS
- Blackberry OS
- Symbian OS
- iPhone OS (iOS)
- Android OS

27) What is M-Commerce? (May/June 2015)

Mobile commerce, involves carrying out any activity related to buying and selling of commodities, services, or information using the mobile hand-held devices.

The popularity of m-commerce can be traced to the convenience it offers both to the buyers and sellers.

An important issue in M-commerce is how payments can be made securely and rapidly as soon as a buyer decides to make a purchase.

The use of computers and networking in trade related transactions has been limited to automatic teller machines (ATMs), banking networks, debit and credit card systems, electronic money and electronic bill payment systems (E-payment).

PART – B

1. Explain Operating System Responsibilities in Mobile Devices? And explain how the resources managed by the OS.

Managing Resources

The operating system of a mobile device is to facilitate ***efficient utilization of the resources*** of the device by performing multiple tasks. The resources that are managed by the operating system include processor, memory, files, and various types of attached devices such as camera, speaker, keyboard, and screen.

Typically, a mobile device is expected to run multiple applications at the same time and each application may in turn require running multiple tasks.

A task can have multiple threads. A few examples of such applications include voice communication, text messaging, e-mail, video play, music play, recording, web browsing, running remote applications, etc.

As an example ***scenario of usage of a smartphone,*** consider the following: a person might be listening to music, at the same time he might answer an incoming call, and an SMS might arrive at the same time which he might like to look-up while the call is still on.

Such a scenario requires ***concurrent execution of multiple tasks***. When multiple tasks contend to use the same set of resources, the OS acts like a traffic cop—ensuring that different tasks do not interfere with each other.

Providing Different Interfaces

The operating system of a mobile device on the one hand provides a highly interactive interface to the user of the device and on the other interfaces with other devices and networks.

An important interface concerns control, data, and voice communications with the base station using different types of protocols.

An OS takes care of recognizing inputs from the keyboard, sending outputs to the display screen, and interfacing with peripheral devices such as other mobile devices, computers, printers, etc.

For the sake of brevity, we shall refer to the operating system used in a mobile hand-held device as a mobile OS.

The mobile OS marketplace is dominated by Symbian, Android, Windows mobile, Palm OS, iOS, and Blackberry OS.

2. Explain the components of Mobile Operating System? (May/June 2016)

Mobile O/S—A Few Basic Concepts

The operating system providing a set of services to the application programs. The operating system is usually structured into a kernel layer and a shell layer.

The shell essentially provides facilities for user interaction with the kernel. The kernel executes in the supervisor mode and can run privileged instructions that could not be run in the user mode.

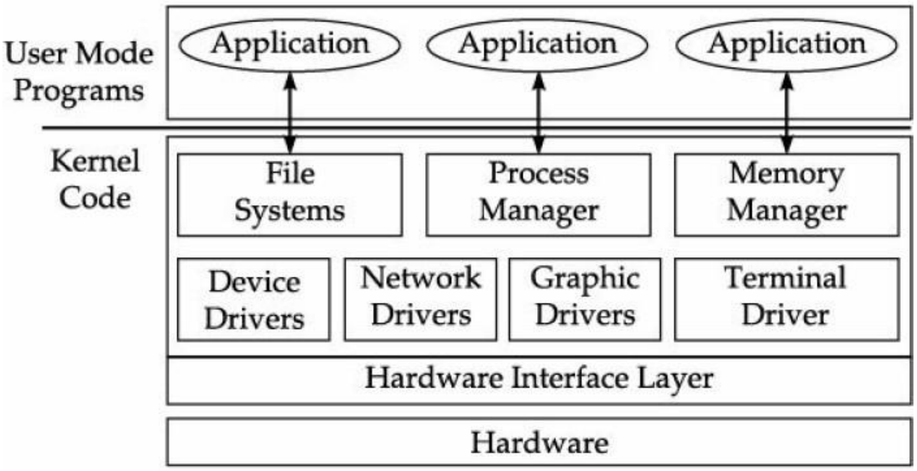
During booting, the kernel gets loaded first and continues to remain in the main memory of the device. This implies that in a virtual memory system, paging does not apply to the kernel code and kernel data. Therefore the kernel is called the ***memory resident*** part of an operating system.

The shell programs are usually not memory resident. The kernel of the operating system is responsible for interrupt servicing and management of processes, memory, and files.

The traditional operating systems such as Unix and Windows are known to have a monolithic kernel design.

In a monolithic kernel OS design, the kernel essentially constitutes the entire operating system code, except for the code for the shell.

The principal motivation behind this monolithic design was the belief that in the supervisor mode, the operating system services can run more securely and efficiently.



(a) Monolithic kernel

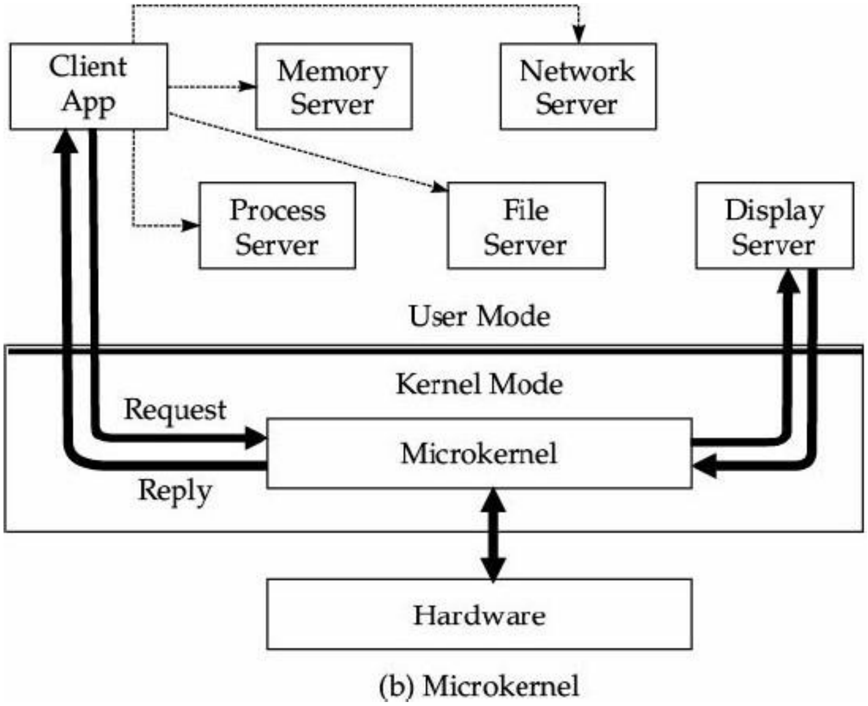


Figure 9.1 ***Monolithic design versus microkernel design of an operating system.***

The main problem with the monolithic kernel design is that it makes the kernel massive, non-modular, hard to tailor, maintain, extend, and configure.

The microkernel design approach tries to minimize the size of the kernel code. Only the basic hardware-dependent functionalities and a few critical functionalities are implemented in the kernel mode and all other functionalities are implemented in the user mode.

Most of the operating system services run as user level processes. The main advantage of this approach is that it becomes easier to port, extend, and maintain the operating system code.

The kernel code is very difficult to debug compared to application programs. The reason for this is that a bug in a kernel code can crash the system, thus crashing the debugger too.

Further, even when some operating system service crashes while being used by a user, it does not bring down the entire system. This is one reason as to why a microkernel operating system could be expected to be more reliable than an equivalent monolithic kernel operating system.

The overall architectural difference between a monolithic kernel and a microkernel architecture is: To restrict the size of the kernel of a mobile OS to the minimum, most mobile OS are, to different extents, based on the microkernel design.

3. Explain the special features that an operating system for a mobile device needs to support compared to the features provided by a traditional operating system.

Special Constraints and Requirements of Mobile O/S

A few special features that are required to be supported by a mobile OS, but are not present in traditional operating systems. A mobile device is powered by severely limited energy stored in a tiny battery.

Limited memory

A mobile device usually has much less permanent and volatile storage compared to that of a contemporary desktop or laptop. To cope with the limited memory of a mobile device, the OS must be as small as possible and yet provide a rich set of functionalities to meet user demands.

Limited screen size

The size of a mobile handset needs to be small to make it portable. This limits the ***size of the display screen***. Consequently, new innovative user interfaces need to be supported by the mobile OS to overcome this constraint and minimize user inconveniences.

For example, many handsets provide easy configurability of the interface to suit individual preferences, switching between menu and iconic interfaces, etc.

Miniature keyboard

Mobile handsets are either provided with a small keypad or the small-sized display screen is designed to be used as a keyboard in a touch screen mode using a stylus. In both these arrangements, typing in the documents and entering the string commands is difficult. This mandates the provision of some facility for word completion prompts and availability of capabilities for free form handwriting recognition.

Limited processing power

A vast majority of modern mobile devices incorporate ARM-based processors. These processors are certainly energy efficient, powerful, and cheaper compared to the desktop or laptop processors, yet these are significantly slower. The sizes of the on-chip and off-chip memory are also restricted.

The cope with the restricted processing power, storage, and battery power, usually the operating system is made to provide only a limited number of functionalities that are useful in the actual operation of the mobile.

Activities such as mobile application development that require use of memory-intensive utility programs, such as editors and compilers, are carried out on a desktop or laptop, and only after the application is completely simulated and tested, it is cross-compiled and downloaded onto the mobile device.

Limited battery power

Mobile devices need to be as lightweight as possible to increase their portability. Due to the severe restrictions that are placed on their size and weight, a mobile device usually has a small battery and often recharging cannot be done as and when required.

In spite of the small battery, a mobile phone is expected to support long talk time without the need to recharge frequently.

Consequently, the operating system for a mobile device needs to be not only computationally efficient, but also at the same time expected to minimize power consumption.

The techniques used by an OS to ***reduce power consumption*** include putting the processor and display screen into sleep mode within a few seconds of inactivity, and varying the intensity of transmitted antennae power as per requirement, etc.

Limited and fluctuating bandwidth of the wireless medium

The operating system of a mobile handset needs to run complex protocols due to the inherent problems caused by mobility and the wireless medium.

A wireless medium is directly susceptible to atmospheric noise, and thereby causes high bit error rates.

The bandwidth of a wireless channel may fluctuate randomly due to atmospheric noise, movement of some objects, or the movements of the mobile handset itself. This can show up as short-term fades.

There can be relatively longer-term disconnections due to handoffs. In this context, uninterrupted communication requires a special support for data caching, pre-fetching, and integration.

4. Explain the facilities that are not supported by a traditional operating system and are mandated to be supported by a mobile device and the specific operating system service reguirements that it makes use of.

Special Service Requirements

Several facilities and services that are normally not expected to be supported by a traditional operating system are mandated to be supported by a mobile OS. We identify a few important ones in the following.

Support for specific communication protocols

Mobile devices are often required to be connected to the base station and various types of peripheral devices, computers and other mobile devices. This requires enhanced communication support.

The types of communication protocols used for communication with the base station depend on the generation of the communication technology (1G, 2G, etc.) in which the mobile device is deployed. For communication with other devices and with computers, TCP/IP and wireless LAN protocols also need to be supported.

For web browsing as well as communication with other personal devices such as pen drive and headphones, though mobile devices are equipped with USB and other types of ports, mobility constraints often make infrared or Bluetooth connections preferable. This mandates the operating system to support multiple interfacing protocols and hardware interfaces.

Support for a variety of input mechanisms

A miniature keyboard forms the main user input mechanism for an inexpensive mobile device. Sophisticated mobile devices (smartphones) usually support the QUERTY keyboard. Many recent mobile devices also support touchscreen or even stylus-based input mechanisms along with the handwriting recognition capability.

A mobile OS needs to support a variety of input mechanisms to make it generic and usable by different manufacturers of mobile devices.

Compliance with open standards

Adhering to an open standard facilitates the development of innovative applications by third-party developers. To facilitate the third party software development as well as to reduce the cost of development and time-to-market by the mobile handset manufacturers, the OS should adhere to open standards.

Smart phones come in many different shapes and sizes and have varying screen sizes and user input capabilities. Therefore, the user interface and networking capabilities of a mobile OS need to be designed keeping these diversities in view.

Extensive library support

The cost-effective development of third party applications requires extensive library support by the OS. Library support includes the availability of programmer callable primitives for email, SMS, MMS, Bluetooth, multimedia, user interface primitives, and GSM/GPRS functionalities.

5. Explain the commercial operating systems for mobile phones and mention the important characteristics of each one.

A Survey of Commercial Mobile Operating Systems

It is a challenging task to design a mobile OS with a set of core capabilities that are expected to be supported by mobile devices and with a consistent programming environment across all smart phones that install the OS.

The mobile OS has to also facilitate third party development of application software and yet allow manufacturers of different brands of mobile devices to build their choice set of functionalities for the users.

Types of Mobile Operating System:

- Windows Mobile
- Palm OS
- Blackberry OS
- Symbian OS
- iPhone OS (iOS)
- Android OS

Windows Mobile

- Windows CE (Compact Edtion) - designed specifically for handheld devices, based on Win32 API. It is run on Pocket PCs, Smartphones and Portable media centers.
- PDA (Personal Digital Assistant), palmtop computer, PocketPC were original intended platform for the Windows Mobile OS
- It provides ultimate interoperability.
- Users with various requirements are able to manipulate their data.
- It provides for ***deterministic scheduling of time-constrained tasks.***
- Windows mobile operating system to be used across a wide cross section of mobile phone manufacturers.
- Microsoft defined a hardware specification for hand-held computers that can run its *Windows Mobile* operating system in order to simplify the design of the operating system and to reduce the number of versions of the operating system. It was also intended to make the cell phones manufactured by different vendors appear uniform.
- Microsoft later renamed its Pocket PC operating system to *Windows Mobile Classic*. Windows mobile classic operating systems support ***touch screen-based user interface***.

A family of Windows Mobile support three operating systems:

Windows Mobile Standard and Windows Mobile Professional are targeted for use in smartphones, and *Windows Mobile Classic* is not targeted for cell phones, but for PDAs.

Many ***third-party software applications*** are available for Windows mobile. These software applications can be purchased via the ***Windows Marketplace for mobiles***.

The marketplace is a website maintained by Microsoft, where different application developers can submit their applications for download by the subscribers.

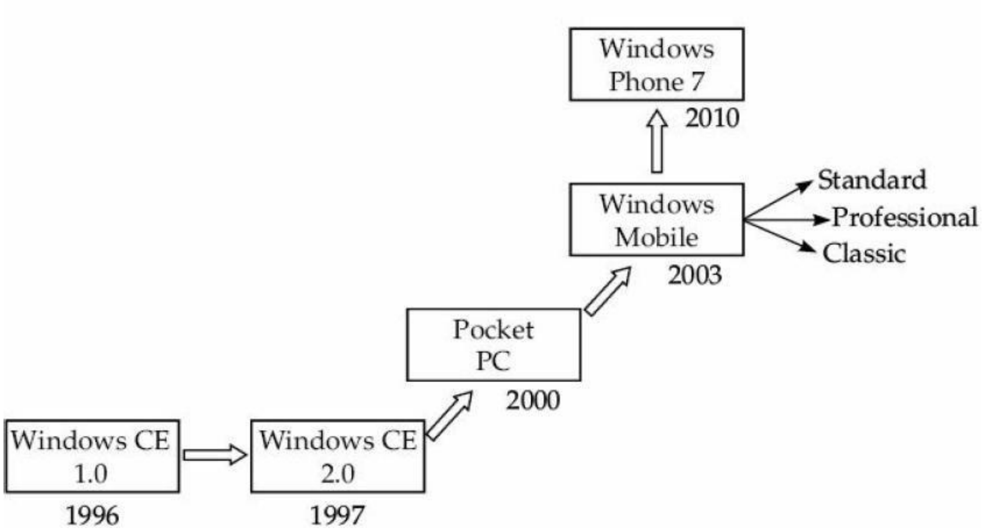


Figure 9.2 ***Evolution of Microsoft's mobile OS.***

Microsoft passes on 70% of the fee received to the developers hosting their applications. Windows mobile has recently been superseded by Windows Phone7.

The Windows mobile was the joint announcement in 2011 by Microsoft and Nokia of a partnership between their companies. They announced that Windows Phone 7 operating system would be used as the operating system for Nokia smartphones.

The mobile OS marketplace would henceforth see a three horse race and named Android and iOS, the main competitors of Windows Phone 7.

Windows Phone 7 is a significant improvement over the Windows mobile operating system.

Microsoft has not maintained backward compatibility with the Windows mobile operating system, meaning that a mobile application that runs on the Windows mobile may not run on the Windows phone OS.

Microsoft has defined the hardware specifications that a Windows Phone 7 device must meet. For example, it should support a screen resolution of 800 X 480 pixels. Windows Phone 7 devices need to have an accelerometer and a compass.

Windows phone operating system provides a ***touchscreen interface*** with facilities for both command and text input. The operating system detects when a device has been rotated from portrait to landscape orientation.

<u>A few important features of the Windows mobile OS are the following:</u>

- The Graphics/Window/Event manager (GWE) component handles all input and output.
- Provides a virtual memory management.
- Supports security through the provision of a cryptographic library.
- Application development is similar to that in the Win32 environment.
- Many programmers have knowledge of Win 32-based application development.

- At present, it does not provide true multitasking. An application in the background goes into hibernation and gets active only when it comes to foreground.
- Microsoft may support true multitasking in the future versions of the Windows Phone operating system.

Palm OS

Palm OS (also known as Garnet OS) is a proprietary operating system that was developed by Palm Computing in 1998 for its highly successful PDA called Palm Pilot. Palm OS was designed for ease of use with the provision of a touchscreen-based graphical user interface.

Palm OS was upgraded to facilitate installation in several different mobile devices, such as smartphones of different makes, wrist watches, hand-held gaming consoles, bar code readers and GPS devices.

The key features of the current Palm OS (named Garnet) are the following:

- It is essentially a simple single-tasking operating system. As a result, only one application can run at a time. For example, if you are on voice communication, you cannot use the calculator, or read an SMS.
- It has an elementary memory management system. To keep the operating system small and fast, Palm OS does not isolate the memory areas of applications from each other. Consequently, any misbehaving application can crash the system.
- Palm supplies Palm emulator, which emulates the Palm hardware on a PC. This allows Palm programs to be developed and debugged on a PC before being run on the Palm hardware.
- It supports a handwriting recognition-based system for user input.
- It supports a facility called HotSync technology for data synchronization with desktop computers.
- It supports sound playback and recording capabilities.
- It incorporates a very simple and rudimentary security model in which a device can be locked by password.
- The different interfaces supported include Serial port/USB, infrared, Bluetooth and Wi-Fi connections.
- It uses a proprietary format to store calendar, address, task and note entries and yet are accessible by third-party applications.

Blackberry Operating System

Blackberry operating system is a proprietary operating system designed for BlackBerry smartphones produced by Research In Motion Limited (RIM).

Being a proprietary operating system, details of its architecture have not been published. But, at the user level, the very good email system that it deploys is easily noticed.

It supports instant mailing while maintaining a high level of security through ondevice hardware-based message encryption

Symbian OS

Symbian operating system was developed through a ***collaboration among a few prominent mobile device manufacturers*** including Nokia, Ericsson, Panasonic, and Samsung.

Its objective was to develop a single industry standard operating system.

In 2008, Ericsson, Sony, Panasonic, and Samsung pulled out of the collaboration, selling their stake to Nokia. Around the same time, Google announced Android as an open operating system.

The Symbian source code was published under **Eclipse Public License (EPL) in February 2010**. This event was reported to be the largest codebase transition from proprietary to **Open Source in the entire history.**

Symbian OS is a real time, multitasking, pre-emptive, 32-bit operating system that runs on ARMbased processor designs.

<u>Symbian comes in two major flavours.</u>

(a) **Series 60:** It support large sized colour screen, easy-to-use interface and an extensive suite of applications make it well-suited to support advanced features such as rich content downloading and MMS (Multimedia Messaging Service). Series 60 was mainly being used on Nokia’s smartphones and Samsung handsets.

(b) **UIQ interface:** UIQ (earlier known as User Interface Quartz) is a software package developed by UIQ Technology for Symbian OS. Essentially, this is a graphical user interface layer that provides capabilities for third-party application developers to develop applications and effortlessly create user interfaces.

<u>A few other important features supported by the Symbian operating system are given below:</u>

- It supports a number of communication and networking protocols including TCP, UDP, PPP, DNS, FTP, WAP, etc. For personal area networking, it supports Bluetooth, InfraRed and USB connectivity.
- Open standards and ***interoperability.***
- Open application environment.
- Flexible User Interfact Design
- It supports ***pre-emptive multitasking scheduling and memory protection***.
- Symbian is a ***microkernel-based operating system.*** It is optimized for low-power and memory requirements.
- Fully object-oriented design paradigm and component based.

- All Symbian programming ***is event-based***, and the CPU is switched into a low-power mode when the applications are not directly dealing with an event. This is achieved through a programming idiom called ***active objects.***
- Carbide is an Integrated Development Environment (IDE) toolkit that is available for C++ application development on Symbian OS.
- Symbian works as an ***Eclipse plug-in.*** Development kits are available at Nokia and the Symbian Foundation websites.

iOS

- iOS Founder were Steve Wozniak and Steve Jobs.
- Developed and distributed by Apple. Inc.,
- Apples mobile operating system considered the foundation of the iPhone
- iPhone OS was first unveiled in Jan 2007 at the Macworld Conference and Expo
- Released June 2007
- Originally designed for the iPhone but now supports iPod touch, iPad, and Apple TV
- iOS is derived from Mac OS.
- Apple ***does not license iOS for installation on third-party hardware.***
- The user interactions with OS include gestures such as *swipe*, *tap*, *pinch*, and *reverse pinch*, all of which have specific definitions within the context of the iOS operating system.
- The other innovative user interactions are internal accelerometers used by some applications for shaking the device as the undo command, rotating the device in three dimensions to switch the display mode from portrait to landscape, etc.

Android OS:

- Android is a Linux-based operating system for mobile devices such as smartphones and tablet computers. There are more than 4,00,000 apps in Android Markets
- Android specially developed for applications. Android has a better app market.
- The Android is an open source
- Android, Inc. found in Palo alto in California united states by Andy Rubin. - October 2003
- In 2005, Google acquired a small startup company called Android, which was developing an operating system for mobile devices based on Linux.
- The Open Handset Alliance, a group of serveral companies was formed – 5 Nov 2007. To develop the Android operating system as an open source software for mobile devices.
- Android Beta SDK Released – 12 Nov 2007.

- Android can run multiple apps at the Same Time.Also support optimized graphics VGA, 2D graphics and 3D graphics
- Google could embed its search engine into Android, the way Internet Explorer is ***embedded into Windows.***
- Android provided the ability to seamlessly use either a phone-based keyboard or a touchscreen.
- Mobile users expect to browse real web pages, and not the simplified mobile versions of those pages.
- Many mobile handsets support browsing alternative sites provided by many website operators for mobile handsets with small screens and limited interfacing capabilities.
- Android operating systems by providing a built-in full web browser capable of rendering full web pages and not just small mobile versions.
- An important handicap of the competing operating systems is ***the difficulty of development of third-party applications***.
- Apple does not facilitate ***third party application development*** and is implicitly promoting a ***closed proprietary environment,*** where the internal working of the operating system is not exposed to the developers.
- A prominent advantage that Android holds out is that Android SDK works in Eclipse environment. Since many developers are already exposed to these standard technologies, there is a **large pool of developers available** for working on projects on the **Android platform**.
- It provides an RDBMS SQLite for data storage and data sharing across various applications.
- It has several innovative pre-installed applications such as Gmail, Maps, voice search, etc.
- Android allows application developers to write code in the Java language. It facilitates the development of applications with the help of a set of core Java libraries developed by Google.

The Android code is structured into four different layers as shown in Fig. 9.3.

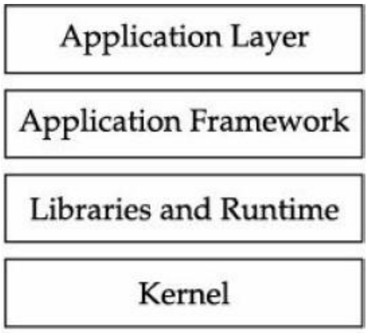


Figure 9.3 *Android software stack.*

Application layer

The Android operating system comes with a set of basic applications such as web browser, email client, SMS program, maps, calendar, and contacts repository management programs. All these applications are written using the ***Java programming language J2ME.***

Application framework

An application framework is used to implement a standard structure for different applications. The application framework essentially provides a set of services that an application programmer can make use of. The services include managers and content providers.

Content providers enable applications to access data from other applications. A notification manager allows an application to display custom alerts on the status bar.

Libraries and runtime

The available libraries are written using multiple languages such as C and C++. These are called through a Java interface. These include a Surface Manager, 2D and 3D graphics, Media Codecs like MPEG-4 and MP3, an SQL database SQLite and the web browser engine called WebKit.

The Android runtime consists of two components.

1. The core libraries of the Java language.
2. Dalvik virtual machine.

- Most applications that run on Android are written in Java.
- Dalvik translates a Java application program into machine code of the mobile device and executes it by invoking the operating system.
- These can be compiled to ARM native code and installed using the Android native development kit (SDK).

  Every Android application runs its own process with its own instance of the Dalvik virtual machine.

Kernel

Android kernel has been developed based on a version of Linux kernel. However, it has excluded the Native X Window System and does not support the full set of standard GNU libraries.

Based on the Linux kernel code, Android implements its own device drivers, memory management, and process management and networking functionalities. Android is ***multitasking*** and allows applications to run concurrently.

For example, it is possible to hear music and read or write an email at the same time. Google initially maintained the kernel code they contributed to in the ***Linux public distribution***. Google maintains its own code tree. This has marked the branching of Android from Linux code in the public distribution.

6. Compare and contrast the various Mobile OS?(Nov/Dec 2016)

Types of Mobile Operating System:

- Windows Mobile
- Palm OS
- Blackberry OS
- Symbian OS
- iPhone OS (iOS)
- Android OS

(Write the short notes on above OS – Refer Q.No : 5)

Android provides a flexible UI and is rich in features, being based on the open source Linux. Windows Phone lacks many features provided by Android, and iOS.

A major reason behind Android's success is that it facilitated competitiveness of hardware makers without good software capabilities. The royalty-free Linux-based Android has been adopted by all the major Asian handset makers such as Samsung, HTC, LG, etc. as well as Motorola and Sony Ericsson.

All these operating systems have very small footprint, run on ARM-based processors, and support demand paging.

Feature	Android	Symbian OS	Windows Phone 7
Feature License	Public, Free, and Open Source	Initially was private, later became public	Proprietary
Footprint	250 KB	200 KB	300 KB
Change of UI	Possible	No	No
Power management	Yes	Yes	Yes
Kernel	Linux with minor changes	Proprietary	Win CE
True multitasking	Yes	Yes	No
Premeptive scheduling	Yes	Yes	Yes
Demand paging	Yes	Yes	Yes
. CPU architecture supported	ARM, MIPS, X86	ARM	ARM

7. Briefly explain how an operating system for a sensor network is different from a traditional operating system.

Operating Systems for Sensor Networks

A sensor node is tiny and needs to operate in an extremely power-constrained environment. Consequently, it deploys a rudimentary operating system and does not have a kernel mode of operation. It does not support dynamic memory allocation nor does it support virtual memory. It also does not use tasks, signals, and exceptions, but uses functional call in its place.

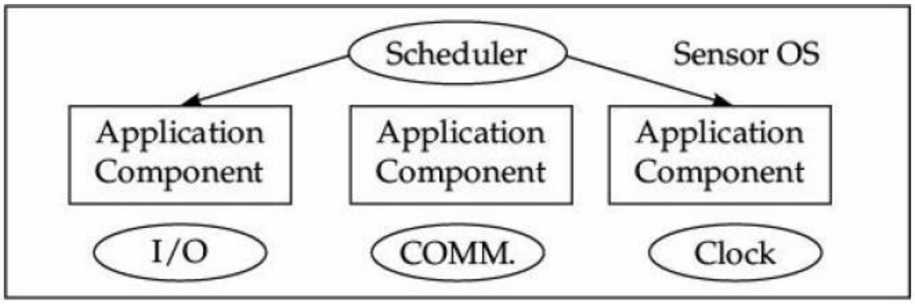


Figure 9.4 *Schematic model of the structure of a sensor operating system.*

Observe that the cheduler invokes the different application components in response to a specific event.The important operating systems that are available for sensor nodes include TinyOS, Contiki OS, Lite oS, and MANTIS.

8. Write short notes on Android SDK (May/June 2016)

SDK Android Software Development Kit (SDK)

Cell phones are small in size and therefore can easily be carried everywhere like a wallet. Considering their portability and the powerful feature sets that they provide, they have now come to play an important **part in today’s society.**

The mobile phones implement new and innovative functionalities. For example, many handsets provide facilities for radio and television reception, timer and clock, Internet access, camera, and calculator,etc.

A successful mobile operating system needs to facilitate the development of ***third-party applications.*** The open operating systems stand out in facilitating the development of third-party applications and Android application development tools have now been well received.

Android SDK Environment

The Android SDK (Software Development Kit) is a ***mobile application development frame work*** using which developers can create applications for the Android platform. The Android SDK provides the ***tools and libraries necessary to develop applications*** that can run on Android-based devices.

Advantages:

- Android SDK is the low processor of RAM requirements.
- Android SDK can be installed on almost all common operating systems such as Windows, Mac OS, and Linux.

The SDK comes with an Integrated Development Environment (IDE) and other tools which are required to develop applications. Android SDK converts Java byte **code to Android's Dalvik VM byte code.** The android-based applications, the developer codes the applications using Java.

The environment to develop applications for Android consists of the Android SDK, the IDE Eclipse and the Java Development Kit (JDK). After installing the SDK, which is done by simply extracting the downloaded ZIP file in a folder, the path to the SDK has to be set in the path environment variable. Eclipse can be used as the IDE, which also automatically installs the Android SDK as a plug-in.

Features of SDK

Using the SDK, one can either run the application on the actual Android device or a software emulator on the host machine. This is achieved by using the Android Debug Bridge (ADB) available with the SDK.

ADB is a client-server program and includes three main components:

- A client program which runs on the developer's (called host) machine. One can invoke aclient from a shell by issuing an adb command.
- A daemon program which runs as a background process on each emulator or device instance.
- It is the part that actually manages the communication with the handset or the emulator and helps in executing the application.
- A server program which runs as a background process on the host machine. The server manages communication between the client and an adb daemon that runs on the emulator or the Android handset.

Android Application Components - Application components are the ***essential building blocks*** of an Android application.

The following are the ***four components of an Android application.***

Activity: Each activity presents a GUI screen of an application. For example, a chat application might have one activity that allows to create a chat, another to view the previous chat sessions, etc. Different activities form a cohesive chat application.

Content providers: Content providers are used for reading and writing data that are either private to an application or shared across applications. By using the content provider, an application can query or modify the stored data.

***Service**:* A service denotes a background task and not for interacting through a user interface. For example, a service might play music in the background while the user is interacting with a different application.

Broadcast receivers: The broadcast receiver responds to broadcast announcements by an application. For **example,** a battery monitoring application might broadcast that the ***battery is low***. Based on this, the music player might reduce the volume or the screen display may be dimmed.

Android Software Stack Structure

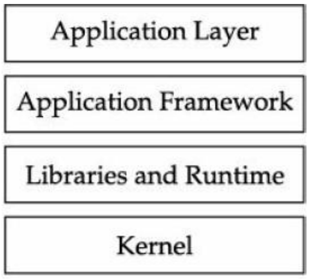


Figure – Android Stack Structure

To a user of a mobile handset, various functionalities are provided by a cooperative working of a number of application programs and system programs. These collections of programs can be decomposed into a hierarchy of four layers.

(Write short notes on each layer in the above diagram – Refer Q.No:5 Android OS)

Advantages of Android

- The mobile platform Android is an open platform and can be ported on almost every type of cell phone.
- The Android SDK to develop applications is possible on every operating system.
- Android requires a low footprint of 250 KB.
- The emulator of the Android platform has a modern design and is easy to use.
- Application installation on the emulator/device is possible via Android Debug Bridge (ADB) or via Eclipse
- Google offers a very good documentation as well as many examples which cover the most basic and important techniques used to get in touch with Android and the application development on it.
- Android supports robust libraries for media access, communication and data transfer Android offers a real database SQLite using which meaningful data manipulation and data Sharing across applications is possible.
- Android has an integrated web browser which gives an experience similar to web browsing using a desktop PC.
- Android uses the standardized and open programming language Java.

9. What do you understand by M-commerce? What are the advantages and disadvantages of M-Commerce.

Mobile Commerce

Mobile commerce, involves carrying out any activity related to buying and selling of commodities, services, or information using the mobile hand-held devices.

The popularity of m-commerce can be traced to the convenience it offers both to the buyers and sellers.

An important issue in M-commerce is how payments can be made securely and rapidly as soon as a buyer decides to make a purchase.

The use of computers and networking in trade related transactions has been limited to automatic teller machines (ATMs), banking networks, debit and credit card systems, electronic money and electronic bill payment systems (E-payment).

Pros and Cons of M-Commerce

Advantages

1. For the business organization, the benefits of using M-commerce include customer convenience, cost savings, and new business opportunities.

2. From the customer's perspective, M-commerce provides the flexibility of ***anytime, anywhere*** shopping using just a lightweight device. The customer can save substantial time compared to visiting several stores for identifying the right product at the lowest price.

3. Mobile devices can be highly personalized, thereby providing an additional level of convenience to the customers. For example, a repeat order for some items can be placed at the touch of a button.

Disadvantages

1. Mobile devices do not generally offer graphics or processing power of a PC. The users are therefore constrained to use small screen and keyboard and low resolution pictures and videos.

2. The small screens of mobile devices limit the complexity of applications. For example, the menu choice, and text typing capability are severely constrained

3. The underlying network imposes several types of restrictions. For example, the available bandwidth is severely restricted, and international reach is prohibitively expensive.

10. What do you mean by the 4 Ps of commerce? Explain the different forms of commerce that are obtained by varying the interpretation of the Ps.

Money is now an important element of all business and trade. In older times, money did not exist. What existed was a simple “barter system” where things could be exchanged, say, fish for grains, The evolution of currency (money) gave birth to the concept of a “marketplace”.

In a marketplace, commerce is a function of ***4 Ps—Product, Price, Place and Promotions***. Once the marketplace came into existence, a few pioneers realized that people would be ready to pay extra if products could be delivered at the customer’s doorsteps. A small change to two of the Ps, Price and Place, led to the convenience of getting products at customers’ homes.

The concept of “Street Vendors” was born. When the postal system came into being, sellers found a new avenue and started using mails to describe their products. It ultimately led to the concept of ***“Mail Order Cataloguing”.***

A mail order catalogues buys goods and then sells those goods to the prospective customers. A mail order catalogue is a list of the goods that the cataloguer deals with. The evolution of the **―Teleshopping‖** networks was inevitable with the development of the Internet.

The Internet has already reached the home of most customers. In this context, the distribution channel has started to assume a new meaning to thee-marketer. With options of ***paying online*** through debit and credit cards, on-line transactions have become purely electronic. The M-commerce has been adopted by the mobile phone users.

11. Explain the various applications of M-commerce? (May/June 2016) (Nov/Dec 2016)

Business-to-Consumer (B2C) Applications

Business-to-consumer (B2C) is a form of commerce in which products or services are sold by a business firm to a consumer. B2C is an important category of mobile commerce applications and is reported to be nearly half of the total M-commerce market (Varshney et al., 2000). A few examples ofB2C applications are given below:

Advertising

Using the demographic information collected by the wireless service providers and based on the current location of a user, a good targeted advertising can be done. The wireless service provider may also keep track of the history of the purchases made by customers by directing advertisements to mobile phones. Customers may also solicit specific advertisements.

For example, suppose a consumer in a shop is fascinated by a new electronic product and wishes to buy it but only after getting more details about it. For this purpose, he can view all the relevant advertisements for the product by taking the picture of the bar code using his mobile device.

Comparison shopping

Consumers can use their mobile phones to get a comparative pricing analysis of a product at different stores and also the prices of the related products.

For example, suppose consumers visiting a shop can use their mobile phones to access a web-based comparison shopping application. By scanning the bar code on a product, the consumer can see the price of this product at different shops in the adjacent area.

Information about a product

Consumers can access additional information about products through their mobile phones.

Assume that a consumer buys some medicine in a pharmacy shop, but cannot read the dosage instructions on the carton given in German and Spanish languages only. The consumer can, however, scan the barcode on the pack using the mobile device to read the dosage instructions in the English language, which he knows.

Mobile ticketing

Mobile phones can be used to purchase movie tickets (called m-tickets) using credit cards. After the payment is received, a unique bar code is sent to the purchaser’s mobile phone by an SMS. The purchase can gain entry to the movie hall by showing the bar code downloaded into the mobile device to a bar code reader at the entrance.

Loyalty and payment services

In this application, mobile phones can replace the physical loyalty cards. Having signed up for a supermarket loyalty scheme, a unique bar code is sent to a consumer’s mobile phone. After shopping at the same supermarket, the consumer shows the bar code at the cash counter and accumulates points based on the total amount spent.

Mobile phones can be used to make payments. For example, consumers can buy canned drinks from a vending machine by moving their phones close to an RFID enabled phone reader. Payment is made **through the person’s mobile phone bill. Consumers pay their bills by simply scanning the bar code on the** bill and using their mobile phones to process payment.

Interactive advertisements

In an interactive advertisement, customers can scan a bar code in an advertisement for a product appearing on a TV screen using their mobile phones. By scanning the bar code, the consumer can order the product by invoking an internet application.

Catalogue shopping

Mobile phones can be used to place orders for products listed in a catalogue. For example, a consumer might receive a catalogue by SMS from a catalogue shopping company. Each product on sale is accompanied by a unique bar code. By scanning the bar codes, the consumer can buy products directly from the catalogue shopping company.

Business-to-Business (B2B) Applications

Business-to-business (B2B) is a form of commerce in which products or services are sold from a company to its dealers.

For example, a company that manufactures TV sets would normally sell it through a dealer network rather than selling the product directly to the consumers. Here, the manufacturer and the dealers are said to be the B2B partners. A few examples of B2B applications of M-commerce are given below.

Ordering and delivery confirmation

The Mobile phones can be used by dealers to order products. The orders can be sent to the supplier in a standard format. By scanning the bar code on a product by using the camera of a mobile phone and specifying the quantity required through a simple application, a dealer can automatically re-order goods.

Mobile phones can be used to gather information about the status of consignments during the transport and delivery process. By reading the bar code on a packet using a mobile device, a truck driver can confirm in real-time that a consignment has been delivered.

Stock tracking and control

Mobile phones can be used to keep track of the stock in a distributed inventory system and send updates to a central database. By using a mobile phone to scan bar codes or RFID tags on products, employees can update the stock in real time.

Mobile phones are the particularly attractive tools where the stock is stored in many locations.

For example, stock control of apparel items warehouse din the various department stores.

Supply Chain Management (SCM)

Information about the supply chain processes can be made available via mobile devices. By scanning an RFID tag using a mobile phone; it is possible for a manager or anyone in the supply chain to check information about a product's state in the supply chain. This kind of accurate information can help manage the business efficiently.

Mobile inventory management

An interesting new B2B application reported a **―rolling inventory‖** consisting of multiple trucks carrying large amounts of goods. Whenever a store needs certain goods, it locates the nearest truck to take delivery of the required goods. This reduces the amount of inventory and cost for both the producers and the retailers. It also has the potential to drastically reduce the delivery times and help in just-in-time delivery of goods.

12. Explain the functionalities of the various layers of the architecture of a mobile commerce framework.

Structure of Mobile Commerce

- In mobile commerce, a content provider implements an application by providing two sets of programs:

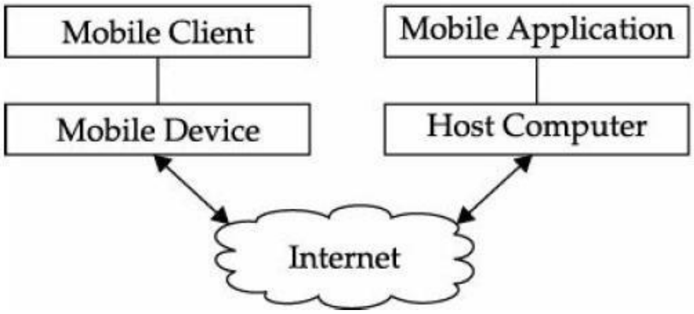


Figure 11.1 *Architecture of a mobile commerce framework.*

- **The client-side Programs**
  - The client-side programs run on the micro browsers installed on the users' mobile devices.
- **The server-side Programs**
  - To perform a database access and computations, reside on the host computer (servers).

Mobile devices

Hand-held devices essentially present user interfaces to the mobile users. The users specify their requests using the appropriate interface programs, which are then transmitted to the mobile commerce application on the Internet. The results obtained from the mobile commerce application are displayed in suitable formats.

Mobile middleware

The main purpose of mobile middleware is to seamlessly and transparently map the Internet content to mobile phones that may sport a wide variety of operating systems, markup languages, micro browsers, and protocols. Most mobile middleware also handle encrypting and decrypting communication in order to provide secure transactions.

Network

Mobile commerce has become possible mainly because of the availability of wireless networks. User requests are delivered either to the closest wireless access point (in a wireless local area network environment) or to a base station (in a cellular network environment).

Wired networks are optional for a mobile commerce system. However, host computers (servers) are generally connected to wired networks such as the Internet. So user requests are routed to these servers using transport and/or security mechanisms provided by wired networks.

Host computers

Host computers are essentially servers that process and store all the information needed for mobile commerce applications. Most application programs used in the mobile commerce are hosted on these. These applications usually consist of three major components: web servers, database servers, and application programs and support software.

The web servers help interact with the mobile client. The database servers store data. The application program is the middleware that implements the business logic of the mobile commerce application.

13. Explain the Mobile Payment Schemes and Security Issues? (May/June 2016) (Nov/Dec 2016)

Mobile Payment Systems

Mobile payments are a natural evolution of E-payment schemes. A mobile payment (or M-payment) may be defined as any payment instrument where a mobile device is used to initiate, authorize and confirm an exchange of financial value in return for goods and services.

Mobile devices include mobile phones, PDAs, and any other device that connects to a mobile network for making payments.

A mobile device can also be used for payment of bills (especially utilities and insurance premiums) with access to account-based payment instruments such as electronic funds transfer, Internet banking payments, direct debit and electronic bill presentment.

The simple message exchange via short messaging services (SMS) may prove more successful. The important payment solutions will be SMS-based, which can easily be charged to the mobile phone bill of customers.

The problems of M-payment schemes are those of security, privacy, and guarding against frauds. The challenges for providing secure transactions are many and range from physical theft of a mobile device which can be subsequently used for fraudulent payments.

Mobile Payment Schemes

Three popular types of M-payment schemes are currently being used:

(a) Bank account based
(b) Credit card based
(c) Micropayment

In each of these approaches, a third party service provider (bank, Credit Card Company, or telecom **company)** makes a payment on the customer’s behalf. An important question that needs to be answered is since the third party incurs an overhead in making the payment, how would it recover the cost.

First, the service provider may require pre-payment from users, leading to some financial gain through investment of this fund. A service provider may charge a small amount as service charge, which can decrease with increasing customer base.

Bank account based M-payment

The bank account of the customer is linked to his mobile phone number. When the customer makes an M-payment transaction with a vendor or in a shopping complex, based on a Bluetooth or wireless LAN connectivity with the vendor, the bank account of the customer is debited and the alue is credited to the vendor's account.

Credit card based M-payment

In the credit card based M-payment, the credit card number is linked to the mobile phone number ofthe customer. When the customer makes an M-payment transaction with a merchant, the credit card is charged and the value is credited to the merchant's account.

Micropayment

Micropayment is intended for payment for small purchases such as from vending machines. The mobile device can communicate with the vending machine directly using a Bluetooth or wireless LAN connection to negotiate the payment and then the micropayment is carried out.

A customer makes a call to the number of a service provider where the per call charge is equal to the cost of the vending item. Thus, the micropayment scheme is implemented through the cooperation of the mobile phone operator and a third party service provider. This approach has been used for vending from Coca-Cola machines.

Security Issues

Trace: Users of mobile devices can be difficult to trace because of roaming of the users. Also, the mobile devices go on-line and off-line frequently. Thus, attacks would be very difficult to trace.

Loss or Theft: A mobile device that is stolen or has fallen into wrong hands can cause frauds that are difficult to track and prevent. A major problem in this regard is the lack of any satisfactory mechanism to authenticate a particular user.

14. What is RFID? Explain few application in which RFID is useful.(6) (Nov/Dec 2016)

Radio Frequency Identification (RFID)

A Radio Frequency Identification (RFID) tag attached to a product, animal, or person for the purpose of identification and tracking, makes use of radio waves. Some tags can be read from several metres away and beyond the line of sight of the reader.

Loyalty and payment services

The mobile phones can replace the physical loyalty cards. Having signed up for a supermarket loyalty scheme, a unique bar code is sent to a consumer's mobile phone. After shopping at the same supermarket, the consumer shows the bar code at the cash counter and accumulates points based on the total amount spent.

Mobile phones can be used to make payments. For example, consumers can buy canned drinks from a vending machine by moving their phones close to an RFID enabled phone reader. Payment is made through the person's mobile phone bill. Consumers pay their bills by simply scanning the bar code on the bill and using their mobile phones to process payment.

Stock tracking and control

Mobile phones can be used to keep track of the stock in a distributed inventory system and send updates to a central database. By using a mobile phone to scan bar codes or RFID tags on products, employees can update the stock in real time.

Mobile phones are the particularly attractive tools where the stock is stored in many locations.
For example, stock control of apparel items warehouse din the various department stores.

Supply Chain Management (SCM)

Information about the supply chain processes can be made available via mobile devices. By scanning an RFID tag using a mobile phone; it is possible for a manager or anyone in the supply chain to check information about a product's state in the supply chain. This kind of accurate information can help manage the business efficiently.

<u>University Questions</u>
<u>May/June 2015</u>

<u>Part A</u>

1. Give four examples of Mobile OS? (Q.No:26)
2. What is M-Commerce? (Q.No:27)

<u>Part B</u>

(a) (i) Explain the components of Mobile Operating System? (8) (Q.No:2)
(ii) Write short notes on Android SDK? (8) (Q.No:8)
(Or)
(b) (i) Explain the various applications of M-Commerce? (8) (Q.No:11)
(ii) Explain the Mobile Payment Schemes and Security Issues? (4+4) (Q.No:13)

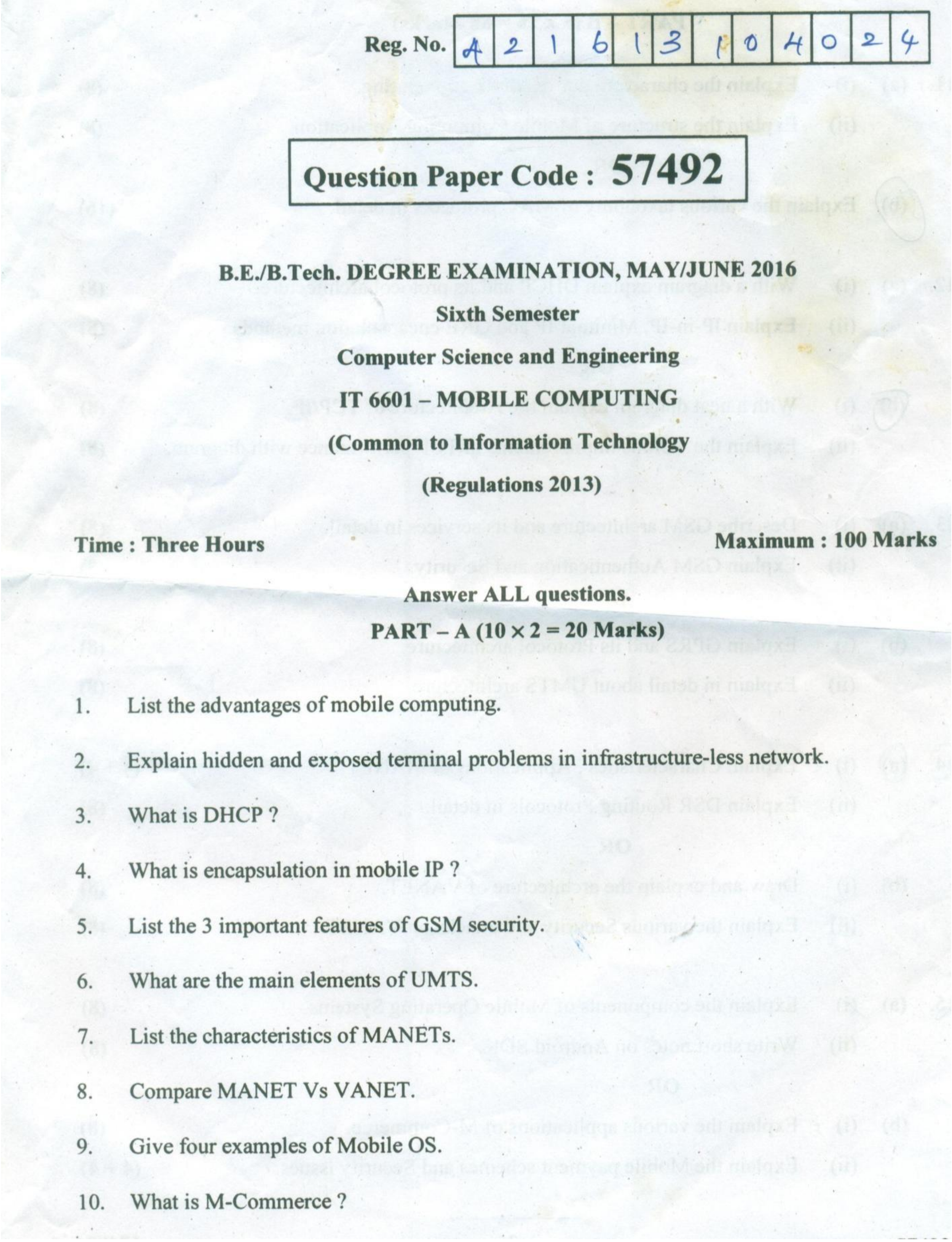
<u>Nov/Dec 2016</u>

<u>Part A</u>

1. Define POS? (Q.No:9)
2. Differentiate E-Commerce and M-Commerce.(Q.No:14)

<u>Part B</u>

(a) (i) Compare and contrast the various Mobile OS.(10)
(ii) Discuss the applications of M-Commerce.(6) (Q.No:11)
(Or)
(b) (i) Explain Mobile Payment Models and security issues.(10) (Q.No:13)
(ii) What is RFID? Explain few applications in which RFID is useful. (6) (Q.No:14)



Reg. No. A 2 1 6 1 3 1 0 4 0 2 4

Question Paper Code : 57492

B.E./B.Tech. DEGREE EXAMINATION, MAY/JUNE 2016

Sixth Semester

Computer Science and Engineering

IT 6601 – MOBILE COMPUTING

(Common to Information Technology)

(Regulations 2013)

Time : Three Hours **Maximum : 100 Marks**

Answer ALL questions.

PART – A (10 × 2 = 20 Marks)

1. List the advantages of mobile computing.

2. Explain hidden and exposed terminal problems in infrastructure-less network.

3. What is DHCP ?

4. What is encapsulation in mobile IP ?

5. List the 3 important features of GSM security.

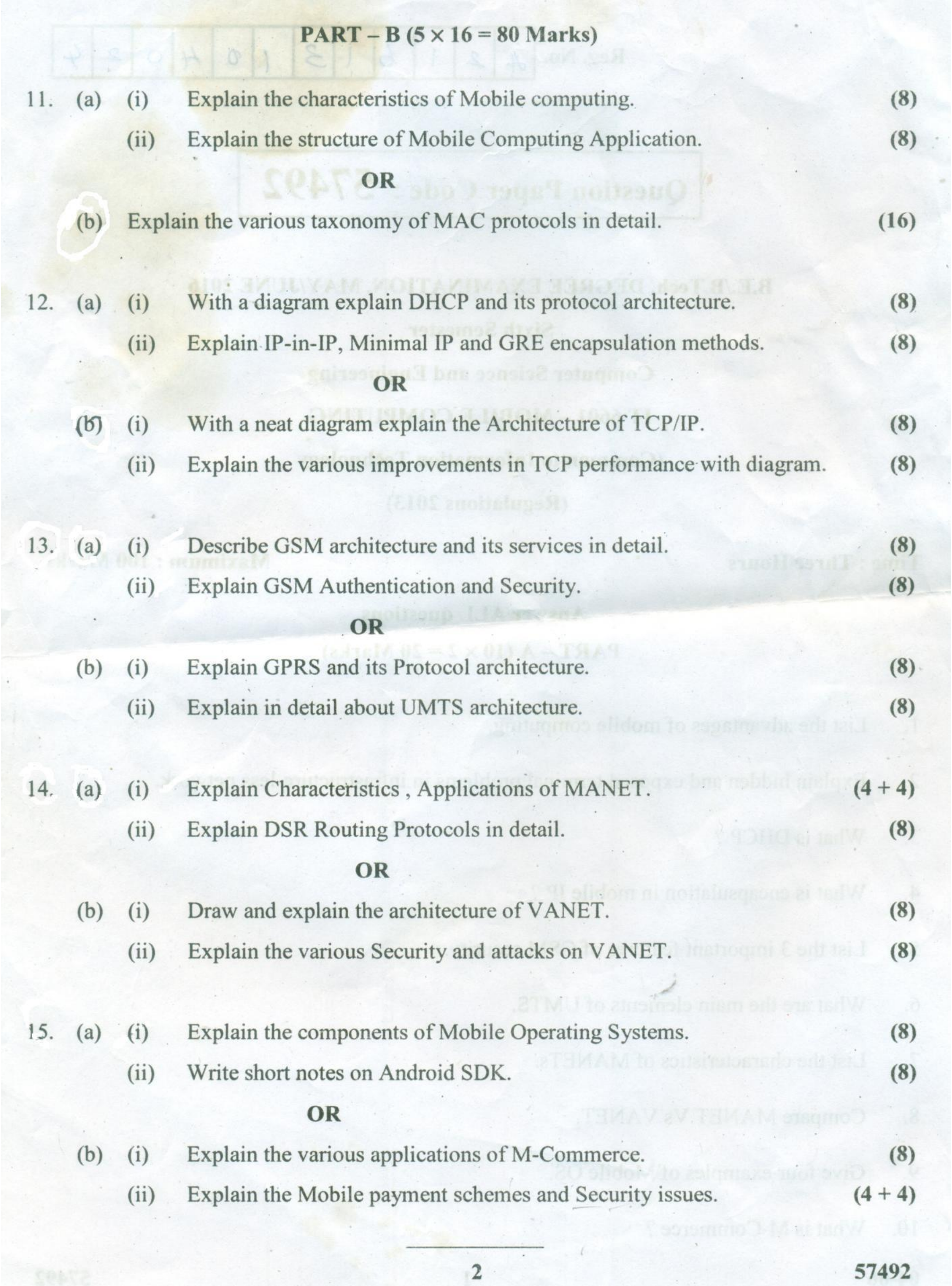
6. What are the main elements of UMTS.

7. List the characteristics of MANETs.

8. Compare MANET Vs VANET.

9. Give four examples of Mobile OS.

10. What is M-Commerce ?



PART – B (5 × 16 = 80 Marks)

11. (a) (i) Explain the characteristics of Mobile computing. **(8)**

(ii) Explain the structure of Mobile Computing Application. **(8)**

OR

(b) Explain the various taxonomy of MAC protocols in detail. **(16)**

12. (a) (i) With a diagram explain DHCP and its protocol architecture. **(8)**

(ii) Explain IP-in-IP, Minimal IP and GRE encapsulation methods. **(8)**

OR

(b) (i) With a neat diagram explain the Architecture of TCP/IP. **(8)**

(ii) Explain the various improvements in TCP performance with diagram. **(8)**

13. (a) (i) Describe GSM architecture and its services in detail. **(8)**

(ii) Explain GSM Authentication and Security. **(8)**

OR

(b) (i) Explain GPRS and its Protocol architecture. **(8)**

(ii) Explain in detail about UMTS architecture. **(8)**

14. (a) (i) Explain Characteristics , Applications of MANET. **(4 + 4)**

(ii) Explain DSR Routing Protocols in detail. **(8)**

OR

(b) (i) Draw and explain the architecture of VANET. **(8)**

(ii) Explain the various Security and attacks on VANET. **(8)**

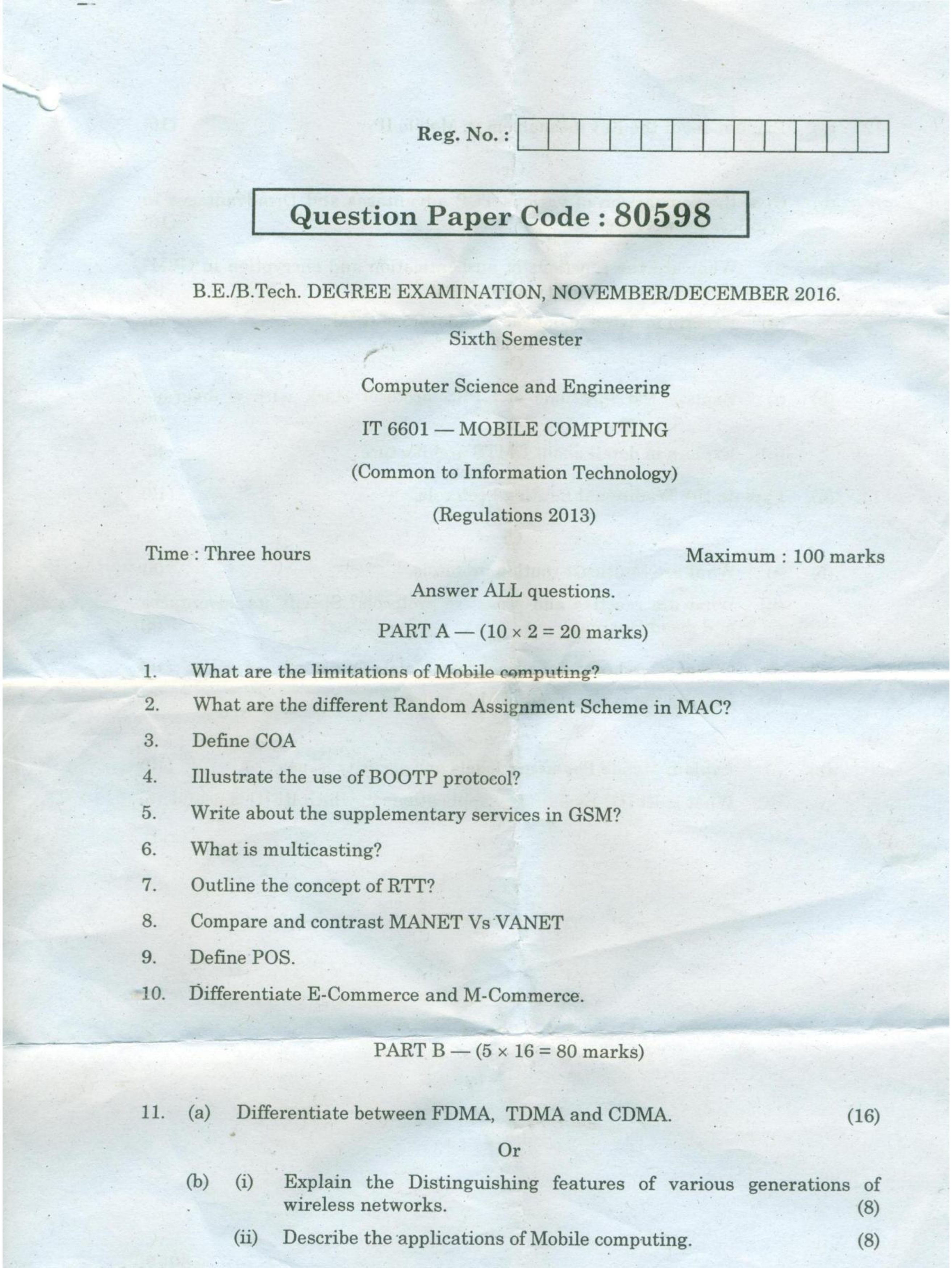
15. (a) (i) Explain the components of Mobile Operating Systems. **(8)**

(ii) Write short notes on Android SDK. **(8)**

OR

(b) (i) Explain the various applications of M-Commerce. **(8)**

(ii) Explain the Mobile payment schemes and Security issues. **(4 + 4)**



Reg. No. : □□□□□□□□□□□□

Question Paper Code : 80598

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2016.

Sixth Semester

Computer Science and Engineering

IT 6601 — MOBILE COMPUTING

(Common to Information Technology)

(Regulations 2013)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. What are the limitations of Mobile computing?
2. What are the different Random Assignment Scheme in MAC?
3. Define COA
4. Illustrate the use of BOOTP protocol?
5. Write about the supplementary services in GSM?
6. What is multicasting?
7. Outline the concept of RTT?
8. Compare and contrast MANET Vs VANET
9. Define POS.
10. Differentiate E-Commerce and M-Commerce.

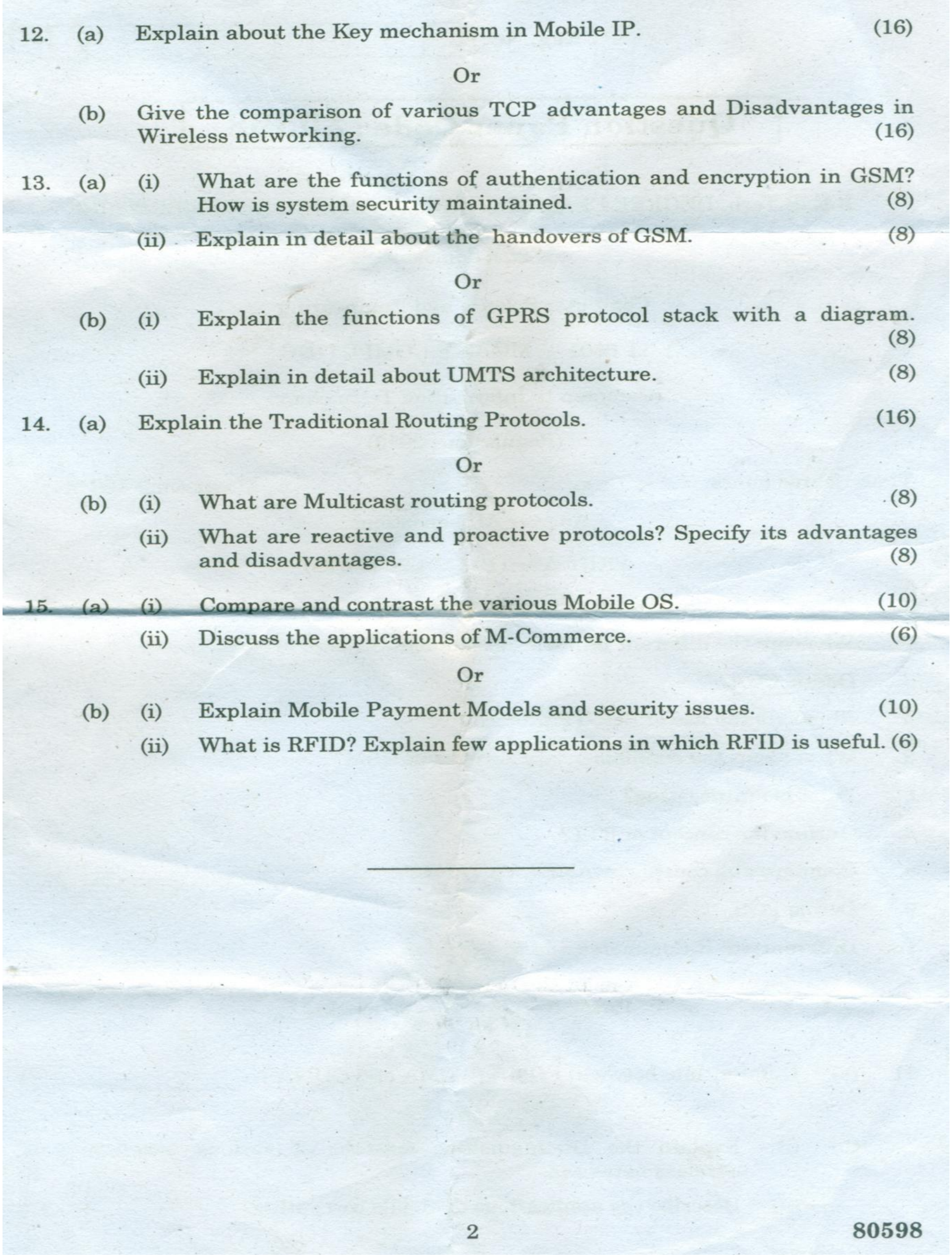
PART B — (5 × 16 = 80 marks)

11. (a) Differentiate between FDMA, TDMA and CDMA. (16)

Or

(b) (i) Explain the Distinguishing features of various generations of wireless networks. (8)

(ii) Describe the applications of Mobile computing. (8)



12. (a) Explain about the Key mechanism in Mobile IP. (16)

Or

(b) Give the comparison of various TCP advantages and Disadvantages in Wireless networking. (16)

13. (a) (i) What are the functions of authentication and encryption in GSM? How is system security maintained. (8)

(ii) Explain in detail about the handovers of GSM. (8)

Or

(b) (i) Explain the functions of GPRS protocol stack with a diagram. (8)

(ii) Explain in detail about UMTS architecture. (8)

14. (a) Explain the Traditional Routing Protocols. (16)

Or

(b) (i) What are Multicast routing protocols. (8)

(ii) What are reactive and proactive protocols? Specify its advantages and disadvantages. (8)

15. (a) (i) Compare and contrast the various Mobile OS. (10)

(ii) Discuss the applications of M-Commerce. (6)

Or

(b) (i) Explain Mobile Payment Models and security issues. (10)

(ii) What is RFID? Explain few applications in which RFID is useful. (6)

UNIT IV MOBILE AD-HOC NETWORKS

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.

PART A

1. **What is Adhoc Network?**

   Adhoc network is defined as a set of mobile devices can communicate with each other in the **absence of** any form of fixed networking infrastructures such as **hubs, routers, base stations**, etc.

2. **What is Mobile Adhoc Network?**

   A MANET is a collection of mobile nodes that communicate with each other over bandwidth constrained wireless links without any infrastructure support.

3. **List the characteristics of MANETs?(May/June 2016)**

   - Lack of fixed infrastructure:
   - Dynamic topologies:
   - Bandwidth constrained, variable capacity links:
   - Energy constrained operation:
   - Increased vulnerability:

4. **What are the applications of MANET?**

   1. Communication among portable computers
   2. Environmental monitoring
   3. Military
   4. Emergency applications

5. **What are the types of traffic?**

   The common traffic types are the following:

   - Bursty traffic
   - Large packets sent periodically
   - Combination of the above two types of traffic

6. **What are the three important ways in which a MANET routing protocol differs from routing of packets in a traditional network?**

   1. In a MANET, each node acts as a router, whereas ordinary nodes in a traditional wired network do not participate in routing the packets.

2. In a MANET, the topology is dynamic because of the mobility of the nodes, but it is static in the case of traditional networks. Thus, the routing tables in a MANET quickly become obsolete, making the routing process complicated.
3. In the simple IP-based addressing scheme deployed in wired networks, the IP address encapsulated in the subnet structure does not work because of node mobility.

7. What are the types of communications?

- *Unicast:* A message is sent to a single destination node.
- *Multicast:* A message is sent to a selected subset of the network nodes.
- *Broadcast:* A message is sent to all the nodes in the network.

8. What are the types of popular MANET routing protocols?

1. Destination-Sequenced Distance-Vector Routing Protocol
2. Dynamic Source Routing (DSR) Protocol
3. Ad Hoc On-demand Distance Vector (AODV)
4. Zone Routing Protocol(ZRP)
5. Multicast Routing Protocols for MANET

9. What is tree based protocol?

Tree-based schemes establish a single path between any two nodes in the multicast group. These schemes require minimum number of copies per packet to be sent along the branches of the tree. Hence, they are bandwidth efficient.

10. What is mesh based protocol?

Mesh-based schemes establish a mesh of paths that connect the sources and destinations. They are more resilient to link failures as well as to mobility.

The major disadvantage of this scheme is that multiple copies of the same packet are disseminated through the mesh, resulting in reduced packet delivery and increased control overhead under highly mobile conditions.

11. Define VANET.

- Vehicular Adhoc Network.
- A Vehicular AdHoc Network (VANET) is a special type of MANET in which moving automobiles form the nodes of the network.
- A vehicle communicates with other vehicles that are within a range of about 100 to 300 metres. Multi-hop communication often results in rather large networks.
- In a city or a busy highway, the diameter of the network can be several tens of kilometres.
- Any vehicle that goes out of the signal range of all other vehicles in the network is excluded from the network.

- A vehicle that was outside the communication range of all other vehicles of a VANET can come in the range of a vehicle that is already in the network and as a result can join the network.

12. What are the design issues in MANET?

- Network size and node density
- Connectivity
- Network topology
- User traffic
- Operational environment
- Energy constraint

13. What are the characteristics of secure Adhoc Network?

Availability: It should be able to survive denial-of-service (DoS) attacks.

Confidentiality: It should protect confidentiality of information by preventing its access by unauthorized users.

Integrity: It should guarantee that no transferred message has been tampered with.

Authentication: It should help a node to obtain guarantee about the true identity of a peer node.

Non-repudiation: It should ensure that a node having sent a message, cannot deny it.

14. What are the two phases of DSR?

Route discovery

- Route discovery allows any host to dynamically discover the route to any destination in the ad hoc network.
- When a node has a data packet to send, it first checks its own routing cache.
- If it finds a valid route in its own routing cache, it sends out the packet using this route.
- Otherwise, it initiates a route discovery process by broadcasting a route request packet to all its neighbours.

Route maintenance

- Route maintenance is the process of monitoring the correct operation of a route in use and taking any corrective action when needed.
- When a host (source) while using a route, finds that it is inoperative, it carries out route maintenance.
- Whenever a node wanting to send a message finds that the route is broken, it would help if it already knows of some alternative routes.

15. What is the use of VANET?

A VANET can help drivers to get advance information and warnings from a nearby environment via message exchanges.

16. What is network topology?

The topology of a network denotes the connectivity among the various nodes of the network.

17. What are the classification of Unicast MANET Routing Protocols?

- Unicast routing protocols in MANETs are classified into **proactive** (table-driven), **reactive** (ondemand) and **hybrid protocols**.
- This classification is based on how a protocol manages to determine the route correctly in the presence of topology changes.

18. What is proactive protocol?

- A proactive routing protocol is also known as a *table-driven* routing protocol.
- In this protocol, each node in a routing table maintains information about routes to every other node in the network.
- These tables are periodically updated in the face of random network topology changes.
- Example Protocol: Destination Sequenced Distance Vector (DSDV) protocol.

19. What is reactive protocol?

- A reactive routing protocol is also known as an on-demand routing protocol, since in this protocol nodes do not maintain up-to-date routes to different destinations, and new routes are discovered only when required.
- When a node does not have knowledge about any route to a specific destination, it uses a flooding technique to determine the route.

Two examples of on-demand routing protocols are:

(i) Dynamic source routing (DSR)

(ii) Ad hoc on-demand distance vector routing (AODV)

20. What is a hybrid protocol?

- Hybrid routing protocols have the characteristics of both proactive and reactive protocols. These protocols combine the good features of both the protocols.
- The hybrid routing protocols are designed to achieve increased scalability by allowing nodes with close proximity to work together to form some sort of a backbone to reduce the route discovery overheads.
- Most hybrid protocols proposed to date are zone-based, which means that the network is partitioned or seen as a number of routing zones by each node.
- An example of a hybrid routing protocol is the Zone Routing Protocol (ZRP).

21. Compare and contrast MANET Vs VANET. (May/June 2015) (Nov/Dec 2016)

- A MANET is a collection of mobile nodes that communicate with each other over bandwidth constrained wireless links without any infrastructure support.
- The nodes are mobile in VANETs as well as in MANETs. However, the VANET nodes (vehicles) can communicate with certain roadside infrastructures or base stations.
- The node mobility in a VANET is constrained to the road topologies, whereas the movement of nodes in a MANET is more random in nature.
- Considering that vehicles move over large distances at relatively high speeds, a VANET undergoes fast topological changes.
- A MANET, power is a major constraint but in VANET the battery power available in a vehicle is quite adequate.
- The issues such as the relatively larger size of VANETs compared to MANETs and the relatively high speed with which vehicles move, need to be appropriately considered for the design of an effective VANET.

22. Define Routing in MANET's and its purposes.

- Packet routing is usually a much more complex task in an ad hoc network compared to that of an infrastructure-based network. The main complications arise on account of continual topology changes and limited battery power of the nodes.
- When the destination node is not in the transmission range of the source node, the route has to be formed with the help of the intervening nodes in the network.
- The purpose of routing is to find the best path between the source and the destination for forwarding packets in any store-and-forward network.

23. What is multicasting? (Nov/Dec 2016)

Multicast is group communication where information is addressed to a group of destination computers simultaneously.*Otherwise a* message is sent to a selected subset of the network nodes.

PART B

1. Explain in detail the basic concepts of Adhoc network.

Adhoc Basics Concepts

How Is an Ad Hoc Network Set Up without the Infrastructure Support?

Adhoc network is defined as a set of mobile devices can communicate with each other in the **absence of** any form of fixed networking infrastructures such as **hubs, routers, base stations**, etc.

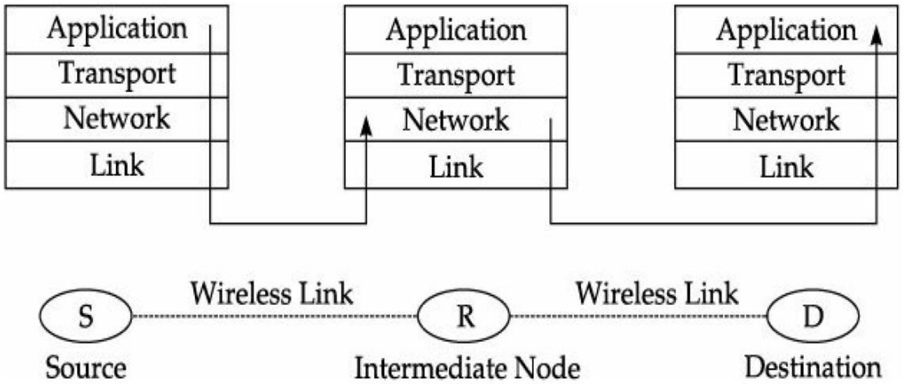


Figure 7.1 *A schematic model of a mobile ad hoc network.*

The mobile device S wants to communicate with the device D. Assume that S and D are not within the transmission range of each other and cannot directly communicate with each other.

They can take the help of node R to relay packets from each other. R is primarily an independent device and not a networking infrastructure, yet R is acting as some sort of a router operating at the network (or Internet) layer to facilitate communication.

Routing in a MANET

- In a wired network, a router determines the path that needs to be followed by a packet based on the information contained within the IP address of the destination, and uses this information to forward a packet towards its destination.

- In a MANET (Mobile Adhoc Network) the topology of the network and consequently the routes between different devices change dynamically as nodes move away or fail. Packet routing is a critical and complex issue in MANETs.

2. Explain Characteristics, Applications of MANET?(May/June 2016)

Characteristics

1. Lack of fixed infrastructure:

In the absence of any fixed networking infrastructure, a pair of nodes can either communicate directly when they are in the transmission range of each other, or they can communicate using a multi-hop communication that gets set up through several devices located between them.

2. Dynamic topologies:

Since the devices in a MANET are allowed to move arbitrarily, the network topology can change unpredictably. The rate of topology change depends on the speed of movement of the mobile devices. The speed of movement of a mobile device can vary greatly with the time of the day and the specific MANET application being considered.

3. Bandwidth constrained, variable capacity links:

Wireless links have significantly lower capacity than their wired counterparts. Further, factors such as fading, noise, and interference can change the available bandwidth of a wireless link arbitrarily with time. Consequently, the bandwidth of a link can change arbitrarily with time.

4. Energy constrained operation:

The nodes in a MANET rely on battery power. These batteries are small and can store very limited amounts of energy. On the other hand, transmissions and processing required during routing involve expenditure of substantial amount of energy causing the batteries to get rapidly drained out, unless the routing protocol is carefully designed. Therefore, energy conservation is usually considered to be an important objective of MANET routing protocols.

5. Increased vulnerability:

MANETs are prone to many new types of security threats that do not exist in the case of their wired counterparts. Many of these threats arise due to the underlying wireless transmissions and the deployment of collaborative routing techniques.

There are increased possibilities of eavesdropping, spoofing, denial-of-service attacks in these networks. It is very difficult to identify the attacker since the devices keep moving and do not have a global identifier.

Other characteristics:

A distributed peer-to-peer mode of operation, multi-hop routing, and relatively frequent changes to the concentration of nodes over any specific area.

MANET Operational Constraints

The nodes in a MANET have low processing capabilities and these are connected by low bandwidth wireless links. An appropriate routing protocol for a MANET should keep the computational and communicational overheads low, since the nodes in a MANET have low computational capability, storage capacity and battery power.

Applications

1. Communication among portable computers

- Miniaturization has allowed the development of many types of portables and computerized equipment, which have become very popular.
- Many of these portables work meaningfully when connected to some network, possibly a LAN or the Internet. For this, the portables are typically required to be within the range of some wireless hub.
- Satisfaction of this requirement would, however, drastically reduce the flexibility and the mobility of the devices.
- In this case, using MANET the audience can exchange notes, and also can surf the Web if at least one of the hand-held devices has access to Internet, for example, through a data card.
- If the mobile devices are present in sufficient density, network connections among them can be established seamlessly to form a MANET over which the nodes can communicate and carry out the network operations.

2. Environmental monitoring

- Continuous data collection from remote locations is considered important for several applications such as environmental management, security monitoring, road traffic monitoring and management, etc.
- Miniaturized sensors have proved to be an effective means of gathering environmental information such as rainfall, humidity, presence of certain animals, etc.
- A large number of sensors nodes are deployed in the environment. Such ad hoc sensor networks can be deployed to collect data from remote locations and the sensor nodes can even respond to some commands issued by the data collection centre.
- MANETs efficiently handle the introduction of new sensors into an already operational sensor network as well as can handle dynamic disconnections of nodes.
- Since each sensor acts as a hub, the range over which the sensors can be spread is tremendously increased.

3. Military

- Ad hoc networking of this equipment can allow a military setup to take advantage of an information network among the soldiers, vehicles, and military information headquarters.
- For example, an ad hoc network can be automatically set up at a battlefront among the equipment, and the hand-held devices can collect information from and disseminate command to the frontline personnel.

4. Emergency applications

- Ad hoc networks do not require any pre-existing infrastructure.These networks, therefore, can be deployed easily and rapidly in emergency situations such as a search and rescue operation after a natural disaster, and for applications such as policing and fire fighting.

3. Explain in detail about MANET Design Issues.

Network size and node density

- Network size and node density are the two important parameters of a MANET that need to be considered while designing an appropriate routing protocol for a network.
- Network size refers to the geographical coverage area of the network and network density refers to the number of nodes present per unit geographical area.
- For larger networks, clustering is essential to keep the communication overheads low.
- The cluster size as well as a specific clustering solution for a network would, to a large extent, depend on node density.

Connectivity

- The term connectivity of a node usually refers to the number of neighbours it has.
- Here a neighbor of a node is one that is in its transmission range.
- The term connectivity refer to ***a link between the two nodes.***
- The term link capacity denotes the bandwidth of the link. In a MANET, both the number of neighbouring nodes and the capacities of the links to different neighbours may vary significantly.

Network topology

- The topology of a network denotes the connectivity among the various nodes of the network. Mobility of the nodes affects the network topology.
- Due to node mobility, new links can form and some links may get dissolved. Other than mobility, nodes can become inoperative due to discharged batteries or hardware failures, and thereby cause changes to the topology.

- The rate at which the topology changes needs to be appropriately considered in the design of an effective network.

User traffic

- The design of a MANET is carried out primarily based on the anticipated node density, average rate of node movements, and the expected traffic.
- The traffic in a network can be of various types.
- A network protocol should leverage the characteristics of specific traffic types that are expected to improve its performance.

The common traffic types are the following:

- Bursty traffic
- Large packets sent periodically
- Combination of the above two types of traffic

Operational environment

- The operational environment of a mobile network is usually either urban, rural and maritime. These operational environments support the Line of Sight (LOS) communication.
- But, there can be a significant difference in the node density and mobility values in different operational environments, requiring different designs of mobile networks to suit an operational environment.

Energy constraint

- No fixed infrastructure exists in a MANET; the mobile nodes themselves store and forward packets. This additional role of mobile nodes as routers leads to nodes incurring perennial routing-related workload and this consequently results in continual battery drainage.
- Though this overhead is indispensable if the network is to be kept operational, the energy spent can be substantially reduced by allowing the nodes to go into a sleep mode whenever possible.

4. **Explain the Traditional Routing protocol. (Nov/Dec 2016)**

Essentials of Traditional Routing Protocol

- The purpose of routing is to find the best path between the source and the destination for forwarding packets in any store-and-forward network.
- Distance vector - router knows cost to each destination
- Link state - router knows entire network topology and computes shortest path

Link State Protocol (LSP)

- The term link state denotes the state of a connection of one router with one of its neighbours.
- Each router determines its local connectivity information, and floods the network with this information with a Link State Advertisement(LSA). As a router in the network receives this link state advertisement, it stores this packet in a link state packet database (LSPDB).
- This storage of link state advertisements in an LSPDB is in addition to the routing table that each router maintains. All routers in the network will have identical LSPBDs.
- Based on the bits and pieces of information stored in its LSPDB, each router constructs the connectivity information for the entire network as a graph using the Dijkstra's shortest path algorithm.
- Once a router constructs this graph, it computes the routing table from this and uses it in all its routing decisions.
- A router in the link state protocol bases its routing decisions on messages (link state advertisements) received from other routers in the network regarding their state of its connectivity with other routers.
- Every router constructs a graph representing the connectivity between the various nodes in the network based on the information received from other routers.
- The construction of the topology map of the entire network from bits and pieces of information received from other routers as similar to the solution of a zig-saw puzzle by putting together the different pieces of the puzzle.
- This graph representing the network is usually constructed in the form of a tree with the local router forming the root of the tree. The graph captures the shortest path route from the root to any other router.
- Once a node constructs this tree, it computes the best path from itself to every other node in the network and stores this information in the form of a routing table. This contrasts with the distance-vector routing protocols, in which each router shares its routing table with its neighbours. But in a link state protocol, only the connectivity related information is exchanged between routers, and no complete routes are exchanged.
- In a link state protocol, each router periodically determines the state of its links to its neighbours by exchanging hello packets with them across all its network interfaces.
- Based on the reply received from its neighbours, the router determines the state of the link in terms of the delay. Subsequently, the router forms a short message called the link state advertisement and sends it to its neighbours. A link state advertisement is also sent whenever a router experiences a connectivity change.
- A link state advertisement message contains:
    - The identity of the router originating the message.

- The identities of all its neighbours.
- The delays along various links to its neighbours.

A unique sequence number, which is formed by increasing the count every time the router forms a new link state advertisement.

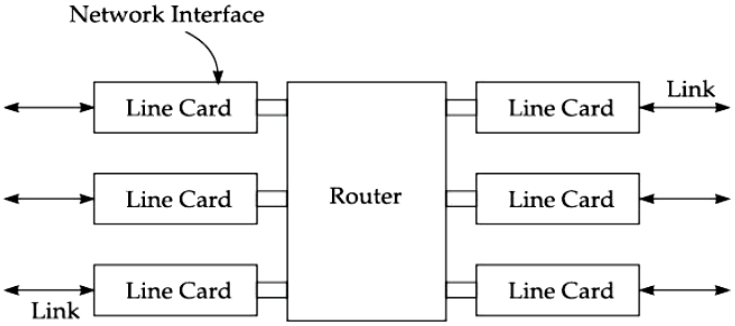


Figure 7.2 *Schematic diagram of a router.*

- The LSA is flooded throughout the network as follows:
- A router sends a copy of a link state advertisement to all of its neighbours.
- A router receiving this message examines the sequence number of the last link state advertisement from the originating router by consulting its LSPDB.
- If this received link state advertisement is more recent, it replaces the last message with the currently received message in its LSPDB, and also forwards a copy of this link state advertisement to each of its neighbours.
- Using the latest link state advertisements stored in its LSPDB, a router can easily reconstruct the network topology in the form of a tree by using the Dijkstra's iterative shortest path algorithm.
- This algorithm constructs the shortest path tree edge by edge, at each step adding one new edge, corresponding to the construction of the shortest path to a router.
- During the construction of the link state tree, if there are any inconsistencies among the reported link state advertisements from different routers, then the same have to be resolved.
- If one router reports that it is connected to another, but the other node does not report that it is connected to the first, then that link is not included on the tree.

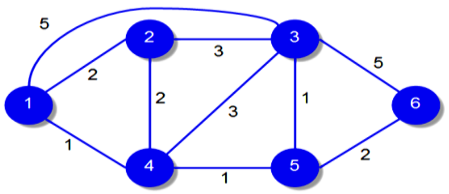
A router maintains two data structures: a tree containing nodes which are done, and a list of candidates.

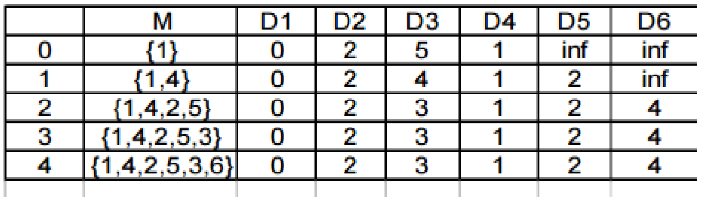
- The shortest path first (SPF) algorithm starts with both data structures empty.
    - All routers which are connected to the router just added to the tree, excepting any routers which are either already in the tree or in the candidate list, are added to the candidate list.
    - The delays from each router in the candidate list to every other router in the tree are compared. The candidate router having the shortest delay is moved into the tree and

attached to the appropriate neighbour router. Whenever a router is moved from the candidate list into the tree, it is removed from the candidate list.

- The above two steps are repeated till there are no more routers left in the candidate list. To form a routing loop, two neighbouring routers determine that the other is the best path to a given destination, and therefore packets traverse endlessly between them.
- Routing loops involving more than two nodes are also possible. Each node computes its shortest-path tree and its routing table without interacting in any way with any other node.
- Once the network topology has been determined in the form of a shortest path tree, a router forms its routing table and uses it to find the best route to any destination and can determine the optimal next hop for each destination in the network. Two Example of LSP: OSPF and IS-IS.

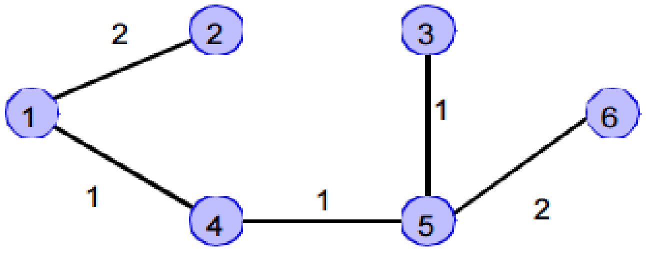
Example of LSP

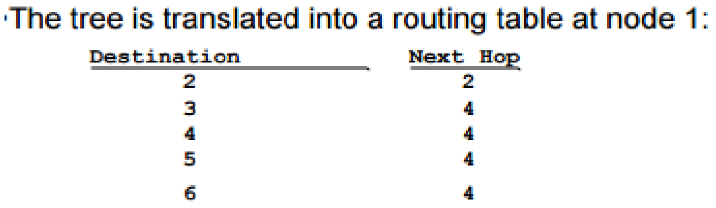




	M	D1	D2	D3	D4	D5	D6
0	{1}	0	2	5	1	inf	inf
1	{1,4}	0	2	4	1	2	inf
2	{1,4,2,5}	0	2	3	1	2	4
3	{1,4,2,5,3}	0	2	3	1	2	4
4	{1,4,2,5,3,6}	0	2	3	1	2	4

Routing Resulting Tree:





The tree is translated into a routing table at node 1:

Destination	Next Hop
2	2
3	4
4	4
5	4
6	4

Distance Vector (DV) Protocols(or) Bellman-Ford Algorithm

- The distance vector protocols get their name from the fact that they base their routing decisions on the
- distance to the destination in terms of the number of hops that a packet will have to traverse to reach its destination.
- The term vector here means that routes are advertised as a vector (distance, direction), where distance is the number of hops between the two nodes and direction is defined in terms of the next hop router to which the packets need to be forwarded.
- The distance vector routing protocols share everything they know about the various routes in the network with their neighbours by broadcasting their entire route table.
- Each node advertises its entire routing table to its immediate neighbours only.
- A router transmits its routing table that has been formed from its own perspective. That is, it represents the routes to various routers from itself.
- Each router learns routes from its neighbouring routers' perspectives, and based on this forms its own perspective of the routes and then advertises the routes from its own perspective.
- As a router receives the routing information of its neighbouring nodes, it updates its own routing table by examining the received information and in turn informs its own neighbours of the changes. This is also referred to as "routing by rumour" because routers are relying on the information they receive from other routers and have no way to determine if the information is actually valid.

Example Protocols:

- RIP (Routing Information Protocol)
- IGRP (Interior Gateway Routing Protocol).

The routers using the distance vector protocol have the following information:

- Direction in (or the specific network interface over) which a packet should be forwarded.
  Its own distance from the destination.
- The distance vector routing protocol requires each router to periodically send its entire route tables to all its neighbours.

5. What are reactive and proactive protocols? Specify its advantages and disadvantages.

(Nov/Dec 2016)

A Classification of Unicast MANET Routing Protocols

- Unicast routing protocols in MANETs are classified into proactive (table-driven), reactive (ondemand) and hybrid protocols.
- This classification is based on how a protocol manages to determine the route correctly in the presence of topology changes.

Proactive protocol:

- A proactive routing protocol is also known as a *table-driven* routing protocol.
- Each node in a ***routing table maintains information about routes*** to every other node in the network.
- These tables are ***periodically updated*** in the face of random network topology changes.
- Example protocol - Destination Sequenced Distance Vector (DSDV) protocol.

Reactive protocol:

- A reactive routing protocol is also known as an on-demand routing protocol, since in this protocol nodes do not ***maintain up-to-date routes*** to different destinations, and new routes are discovered only when required.
- When a node does not have knowledge about any route to a specific destination, it uses a flooding technique to determine the route.
- Two examples of on-demand routing protocols are:

  (i) Dynamic source routing (DSR)

  (ii) Ad hoc on-demand distance vector routing (AODV)

Hybrid routing protocols:

- Hybrid routing protocols have the characteristics of both proactive and reactive protocols. These protocols combine the good features of both the protocols.
- The hybrid routing protocols are designed to achieve increased scalability by allowing nodes with close proximity to work together to form some sort of a backbone to reduce the route discovery overheads.
- This is mostly achieved by proactively maintaining routes to nearby nodes and determining routes to far away nodes only when required using a route discovery strategy.
- Most hybrid protocols proposed to date are zone-based, which means that the network is partitioned or seen as a number of routing zones by each node.
- Example: Zone Routing Protocol (ZRP).

6. **Explain in detail about popular MANET routing protocols.**

Popular MANET Routing Protocols

1. Destination-Sequenced Distance-Vector Routing Protocol
2. Dynamic Source Routing (DSR) Protocol **(Refer Q.No:7)**
3. Ad Hoc On-demand Distance Vector (AODV)

4. Zone Routing Protocol
5. Multicast Routing Protocols for MANET **(Refer Q.No:8)**

1. Destination-Sequenced Distance-Vector Routing Protocol

- Destination-Sequenced Distance-Vector Routing (DSDV) is an important MANET routing protocol. It is based on the table-driven (proactive) approach to packet routing.
- In DSDV, each node in a MANET maintains a routing table in which all of the possible destinations and the number of hops to each destination are recorded.
- Each node maintains information regarding routes to all the known destinations. The routing information is updated periodically.
- Also, there is traffic overhead even if there is no change in network topology. Nodes maintain routes which they may never use.
- A sequenced numbering system is used to allow mobile nodes to distinguish stale routes from new ones. Updated routing tables are exchanged periodically among the nodes of the network to maintain table consistency.
- DSDV uses two types of route update packets. The first is known as *full dump*. This type of packet carries all the available routing information and can require multiple network protocol data units (NPDUs) to be transmitted.
- The mobile nodes maintain an additional table where they store the data received through the incremental routing information packets from various nodes.

Important steps in the operation of DSDV

1. Each router (node) in the network collects route information from all its neighbours.

2. After gathering information, the node determines the shortest path to the destination based on the gathered information.

3. Based on the gathered information, a new routing table is generated.

4. The router broadcasts this table to its neighbours. On receipt by neighbours, the neighbor nodes recompute their respective routing tables.

5. This process continues till the routing information becomes stable.

Table 7.1 is the routing table of the node N4 at the moment before the movement of nodes. The metric field in the routing table helps to determine the number of hops required for a packet to traverse to its destination.

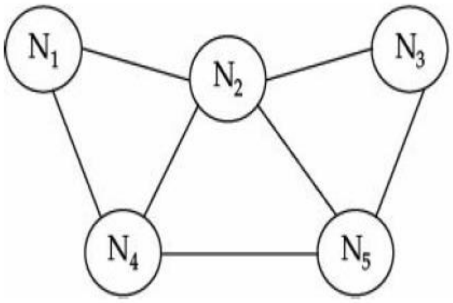
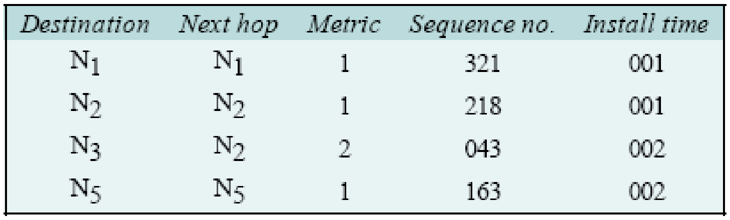


Figure 7.3 *An example of a MANET topology at a given instant of time.*



Destination	*Next hop*	*Metric*	*Sequence no.*	*Install time*
N_1	N_1	1	321	001
N_2	N_2	1	218	001
N_3	N_2	2	043	002
N_5	N_5	1	163	002

Figure- Routing Table

2. Ad Hoc On-demand Distance Vector (AODV)

- The route discovery and route maintenance activities in AODV are very similar to those for the DSR protocol.
- AODV does make use of hop-by-hop routing, sequence numbers and beacons.
- The node that needs a route to a specific destination generates a *route request*.
- The *route request* is forwarded by intermediate nodes which also learn a reverse route from the source to themselves.
- When the request reaches a node with route to destination, it generates a *route reply* containing the number of hops required to reach the destination.
- All nodes that participate in forwarding this reply to the source node create a forward route to destination.
- This route created from each node from source to destination is a hop-by-hop route.

Recollect that DSR includes the complete route in packet headers.

- The large headers can substantially degrade the performance, especially when the data content of packets is small.
- AODV attempts to improve upon DSR by maintaining routing tables at the nodes, so that the data packets do not have to contain the routes.
- AODV retains a positive feature of DSR, in that the routes are maintained only between those nodes that need to communicate.
- If a link break occurs while a route is being used to transmit a message, a route error message is sent to the source node by the node that observes that the next link in the route has failed.

3. Zone Routing Protocol

- The Zone Routing Protocol (ZRP) is a ***hybrid protocol***. It incorporates the merits of both on-demand and proactive routing protocols.
- A routing zone comprises a few MANET nodes within a ***few hops from the central zone***. Within a zone, a table-driven routing protocol is used.
- If a destination node happens to be outside the source's zone, ZRP employs an ***ondemand route discovery procedure*** which works as follows.
- The ***source node*** sends a route request to the ***border nodes*** of its zone, containing its own ***address, the destination address and a unique sequence number.***
- Border nodes are those nodes which are some ***predefined number of hops*** away from the source. Each border node checks its local zone for the destination.

7. Explain DSR Routing Protocols in detail?(May/June 2016)

- Dynamic Source Routing (DSR) protocol was developed to be suitable for use in a MANET having a reasonably small diameter of about 5 to 10 hops and when the nodes do not move very fast.
- DSR is a source initiated on-demand (or reactive) routing protocol for ad hoc networks.
- It uses source routing, a technique in which the sender of a packet determines the complete sequence of nodes through which a packet has to travel.
- The sender of the packet then explicitly records this list of all nodes in the packet's header. This makes it easy for each node in the path to identify the next node to which it should transmit the packet for routing the packet to its destination.
- In this protocol, the nodes do not need to exchange the routing table information periodically, which helps to reduce the bandwidth overhead associated with the protocol.
- Each mobile node participating in the protocol maintains a ***routing cache*** which contains the list of all routes that the node has *learnt*.
- Whenever a node finds a new route, it adds the new route to its *routing cache*. Each mobile node also maintains a sequence counter called ***request id*** to uniquely identify the last request it had generated.
- The pair < source address, request id > uniquely identifies any request in the ad hoc network.

DSR works in two phases:

(i) Route discovery and

(ii) Route maintenance.

Route discovery

- Route discovery allows any host to dynamically discover the route to any destination in the ad hoc network.
- When a node has a data packet to send, it first checks its own routing cache.
- If it finds a valid route in its own routing cache, it sends out the packet using this route.
- Otherwise, it initiates a route discovery process by broadcasting a route request packet to all its neighbours.
- The route request packet contains the source address, the request id and a route record in which the sequence of hops traversed by the request packet, before reaching the destination is recorded.

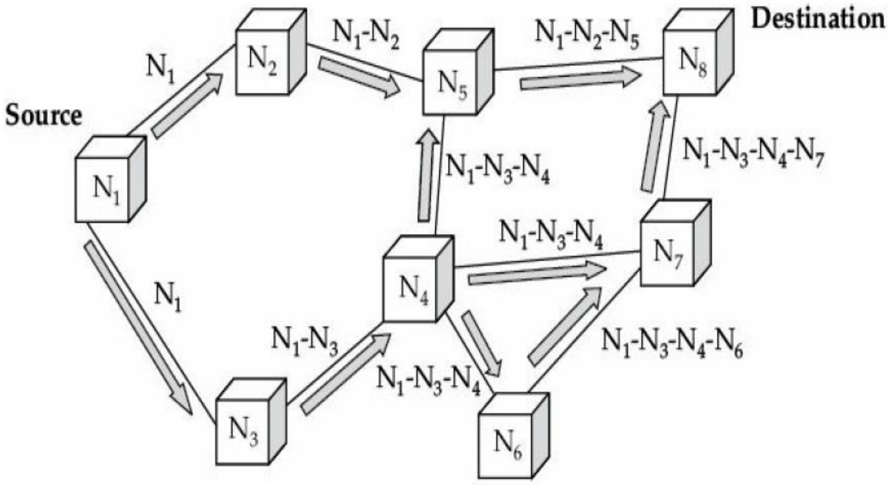


Figure 7.4 *An example of the route discovery process in DSR.*

- Suppose a node N1 wishes to send a message to the destination node N8. The intermediate nodes are N2, N3, N4, N5, N6, N7.
- The node N1 initiates the route discovery process by broadcasting a *route request* packet to its neighbours N2 and N3.
- Note that each node can have multiple copies of the route request packet arriving at it.
- The propagation of route reply is shown in Figure 7.5, and the acknowledgement messages from destination to source are indicated by thick arrows.

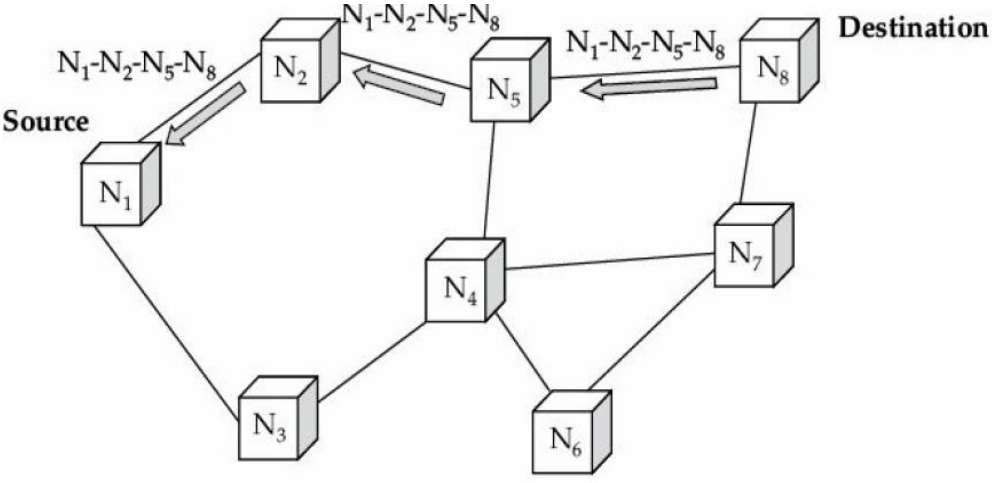


Figure 7.5 *An example of the propagation of route reply in DSR.*

Route maintenance

- Route maintenance is the process of monitoring the correct operation of a route in use and taking any corrective action when needed.
- When a host (source) while using a route, finds that it is inoperative, it carries out route maintenance.
- Whenever a node wanting to send a message finds that the route is broken, it would help if it already knows of some alternative routes.
- If it has another route to the destination, it starts to retransmit the packet using the alternative route. Otherwise, it initiates the route discovery process again.

8. What are Multicast Routing protocols. (Nov/Dec 2016)

Multicast is the delivery of a message to a group of destination nodes in a single transmission.

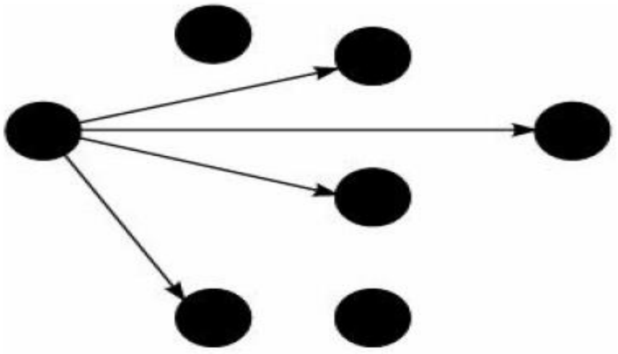


Figure 7.6 *Multicast transmission.*

For efficient operation of a multicast routing protocol, it is necessary to minimize the unnecessary packet transmissions as well as minimize the energy consumption. A multicast transmission should not be approximated by multiple unicast transmissions.

The popular MANET multicasting protocols are either tree-based or mesh-based:

Tree-based protocol

Tree-based schemes establish a single path between any two nodes in the multicast group. These schemes require minimum number of copies per packet to be sent along the branches of the tree. Hence, they are bandwidth efficient.

Mesh-based protocol

Mesh-based schemes establish a mesh of paths that connect the sources and destinations. They are more resilient to link failures as well as to mobility.

The major disadvantage of this scheme is that multiple copies of the same packet are disseminated through the mesh, resulting in reduced packet delivery and increased control overhead under highly mobile conditions.

9. Draw and Explain the architecture of VANET? (May/June 2016)

Vehicular Ad Hoc Networks (VANETs)

- A Vehicular Ad Hoc Network (VANET) is a special type of MANET in which moving automobiles form the nodes of the network.
- VANETs were initially introduced for vehicles of police, fire brigades, and ambulances for safe travelling on road.
- In this network, a vehicle communicates with other vehicles that are within a range of about 100 to 300 metres. Multi-hop communication often results in rather large networks.
- In a city or a busy highway, the diameter of the network can be several tens of kilometres.
- Any vehicle that goes out of the signal range of all other vehicles in the network is excluded from the network.
- A vehicle that was outside the communication range of all other vehicles of a VANET can come in the range of a vehicle that is already in the network and as a result can join the network.
- A VANET can offer a significant utility value to a motorist.

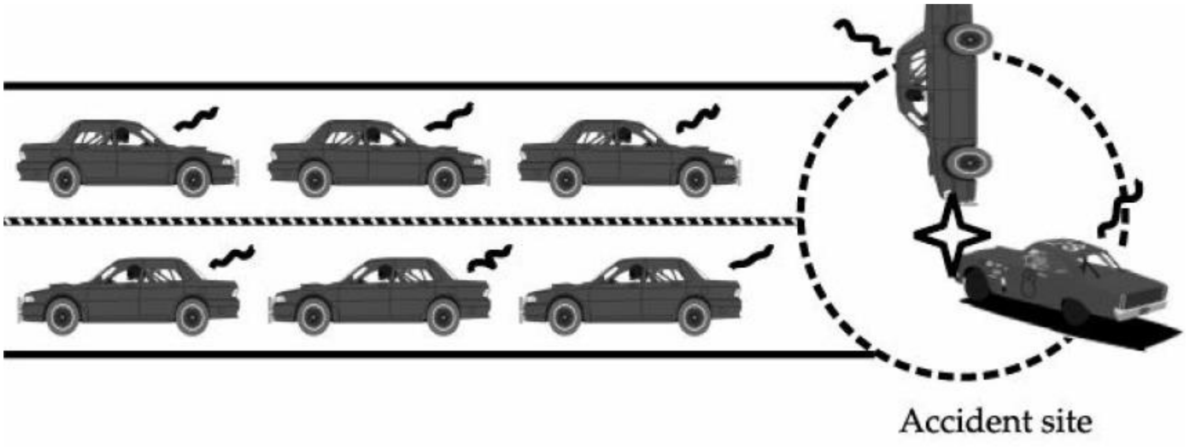


Figure 7.7 *A VANET use scenario.*

A few important uses of a VANET:

A VANET can help drivers to get advance information and warnings from a nearby environment via message exchanges.

For example two vehicles are involved in a collision in the fig.

- The trailing vehicles get advance notification of the collision ahead on the road.
- The driver can also get advance information on the road condition ahead, or a warning about the application of emergency electronic brake by a vehicle ahead in the lane.
- A VANET can help disseminate geographical information to the driver as he continues to drive. For example, the driver would be notified of the nearby food malls or petrol refilling stations, map display, etc.
- Drivers may have the opportunity to engage in other leisurely tasks, such as VoIP with family, watch news highlights, listen to series of media files known as podcasts, or even carry out some business activities such as participate in an office video conference session.

10. Explain the various Security and attacks on VANET.(May/June 2016)

Security Issues in a MANET

- MANETS are fundamentally different from both wired networks and infrastructure-based wireless networks.
- The nature of MANETs not only introduces new security concerns but also exacerbates the problem of detecting and preventing anomalous behaviour.
- In a wired network or in an infrastructure-based wireless network, an intruder is usually a host that is outside the network and therefore could be controlled through a firewall and subjected to access control and authentication.

- In a MANET, on the other hand, an intruder is part of the network, and therefore much more difficult to detect and isolate.
- Dynamic topological changes and the inherent wireless communications in a MANET, make it vulnerable to different types of attacks.
- At the physical layer, an intruder can easily cause jamming or overload the available network resources beyond their capacities, thereby effectively paralysing it.
- Wireless links can get jammed and the batteries at the nodes can get depleted by such overloading, causing breakdowns of the network.
- Attackers can also disturb the normal operation of routing protocols by modifying the headers of packets.
- The intruder may insert spurious information while routing packets, causing erroneous routing table updates and thereby leading to frequent misroutings.

A few important characteristics of ad hoc networks that can be exploited to cause security vulnerabilities are the following:

Lack of physical boundary:

Each mobile node functions as a router and forwards packets from other nodes. As a result, network boundaries become blurred. The distinction between nodes that are internal or external to a network becomes meaningless, making it difficult to deploy firewalls or monitor the incoming traffic.

Low power RF transmissions:

It is possible for a malicious node to continuously transmit and monopolise the medium and cause its neighbouring nodes to wait endlessly for transmitting their messages. Also, signal jamming can lead to a denial-of-service (DoS) attack.

Limited computational capabilities:

Nodes in an ad hoc network usually have limited computational capabilities. It therefore becomes difficult to deploy compute-intensive security solutions such as setting up a public-key cryptosystem. Inability to encrypt messages invites a host of security attacks such as spoofing as well as several forms of routing attacks.

Limited power supply:

Since nodes normally rely on battery power, an attacker might attempt to exhaust batteries by causing unnecessary transmissions to take place or might cause excessive computations to be carried out by the nodes.

Characteristics of secure ad hoc networks

A secure ad hoc network should have the following characteristics:

Availability: It should be able to survive denial-of-service (DoS) attacks.

Confidentiality: It should protect confidentiality of information by preventing its access by unauthorized users.

Integrity: It should guarantee that no transferred message has been tampered with.

Authentication: It should help a node to obtain guarantee about the true identity of a peer node.

Non-repudiation: It should ensure that a node having sent a message, cannot deny it.

Attacks on Ad Hoc Networks

MANET can be classified into two types:

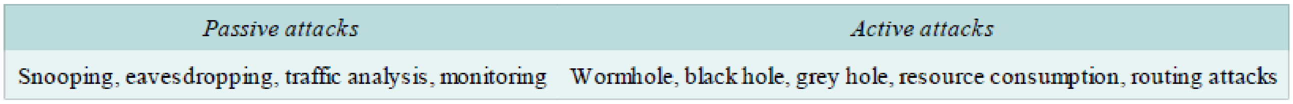
1. Passive attack
2. Active attack

Passive attacks target to monitor and steal the data exchanged in the network, without disrupting the network operations. It becomes very difficult to identify these attacks since these do not have any perceivable symptoms. These attacks can be reduced by using suitable ***encryption techniques.***

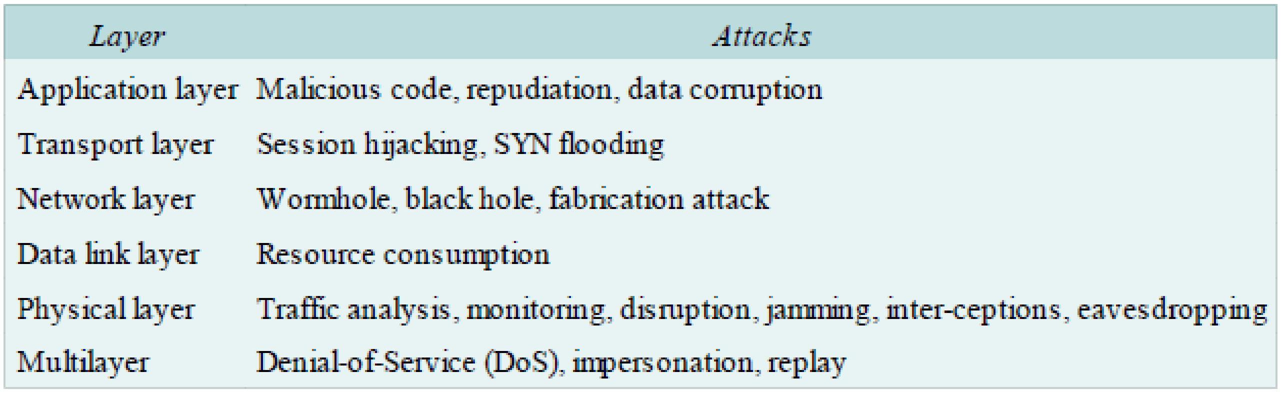
An active attack, is destructive and disturbs the normal functionality of the network.

Each attack can be considered to be exploiting the vulnerabilities at one or more layers of the MANET protocol stack while most attacks target certain security vulnerabilities at specific protocol layers. The multilayer attacks are those that exploit the vulnerabilities existing at more than one protocol layer.

TABLE 7.2 Passive and Active Attacks in a MANET



Passive attacks	*Active attacks*
Snooping, eavesdropping, traffic analysis, monitoring	Wormhole, black hole, grey hole, resource consumption, routing attacks



Layer	Attacks
Application layer	Malicious code, repudiation, data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, black hole, fabrication attack
Data link layer	Resource consumption
Physical layer	Traffic analysis, monitoring, disruption, jamming, inter-ceptions, eavesdropping
Multilayer	Denial-of-Service (DoS), impersonation, replay

Table – Attacks at Different Layers in MANET protocol.

The important types of security attacks in the following.

Routing loop

By sending tampered routing packets, an attacker can create a routing loop. This will result in data packets being sent around endlessly, consuming bandwidth and causing dissipation of power for a number of nodes. In this attack, the packets are prevented from reaching their intended recipients and thus it can be considered to be a type of denial-of-service (DoS) attack.

Malicious code attacks

A malicious code can be a virus, worm, spyware, or a Trojan. In a MANET, an attacker can propagate malicious code and can slow down the nodes, overload the network, or even crash the nodes.

Repudiation attack

Repudiation attack refers to the denial of participation in a communication. In this attack, a malicious user can deny a credit card or bank transaction.

SYN flooding attack

An attacker creates a large number of half-opened TCT connections with the victim nodes by sending a large number of SYN packets to them. This causes the TCP connection tables of the victim nodes to overflow.

Session hijacking

The attacker can spoof the IP address of a node that has just started a session and hijack the session from the victim and perform a DoS attack.

Fabrication attack

In AODV routing, when a node detects a broken link while forwarding a packet (possibly because the next hop node has either moved or has shut down), it sends a route error message towards the packet sender. In the fabrication attack, a malicious node sends a false route error message to the packet sender, even when the next hop link is not broken.

Black hole

A node can set up a route to some destination via itself, and when the actual data packets are received from other nodes, these are simply dropped. This node forms a black hole, to which data packets enter but never leave.

Grey hole

The attacker selectively drops some kinds of packets that pass through it but not the others. For example, the attacker might forward routing packets but not the data packets. This type of attack is more difficult to detect compared to a black hole attack.

Partitioning

The attacker partitions a network by causing some nodes to split up from the other nodes. That is, one set of nodes is not able to communicate with the other set of nodes. By analysing the network topology the attacker can choose to make the partitioning between the set of nodes that causes the most harm to the system. This attack can be accomplished in many ways, such as by tampering routing packets as in the previous attacks. It can also be launched through some physical attack such as radio jamming.

Blacklist

This attack tries to exploit a loophole in security mechanisms. Some ad hoc routing protocols try to tackle this security problem by keeping a list of perceived malicious nodes. Each node has a blacklist of, what it thinks, bad nodes and thereby avoids using them when setting up routing paths.

An attacker might try to get a good node blacklisted, causing the other good nodes to add this node to their respective blacklists and so avoid it.

Wormhole

In a wormhole attack, a direct link (tunnel) between the two nodes is established. This is referred to as *wormhole link*. The direct link can be established by making use of a wired line, a long-range wireless transmission, or an optical link.

Through the wormhole link, one node eavesdrops messages at one end, and tunnells them through the wormhole link to the other node which then replays them. The tunnel essentially emulates a shorter route through the network and so naive nodes prefer to use it rather than the alternative longer routes.

Once a wormhole is established, a malicious node can use it for traffic analysis or make a denial-of-service attack by dropping certain data or control packets. When this attack targets specifically the ***routing control packets***, the nodes that are close to the attackers are shielded from any alternative routes with more than one or two hops to the remote location.

Dropping routing traffic

It is essential that in an ad hoc network, all nodes participate in the routing process. However, it is possible that a node may act selfishly and process only the routing information that is related to itself either maliciously or to conserve energy. This behaviour/attack can create network instability or can even segment the network.

Security Attack Countermeasures

The cryptographic techniques are powerful techniques for ensuring confidentiality, authentication, integrity, and non-repudiation, these are ineffective against jamming. Spread spectrum technology such as frequency hopping is a promising countermeasure against the signal jamming type of attacks. In this technique, the transmission frequency changes randomly. Directional antennae can be deployed as a countermeasure against signal jamming.

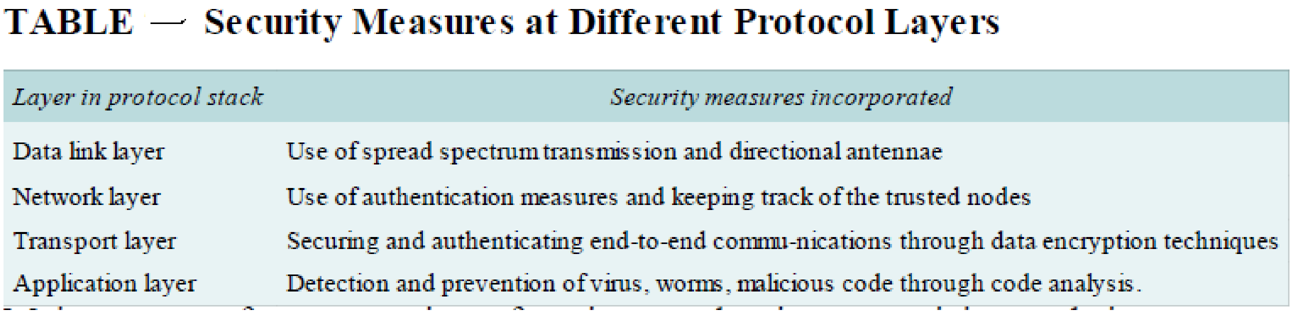


TABLE — Security Measures at Different Protocol Layers

Layer in protocol stack	*Security measures incorporated*
Data link layer	Use of spread spectrum transmission and directional antennae
Network layer	Use of authentication measures and keeping track of the trusted nodes
Transport layer	Securing and authenticating end-to-end commu-nications through data encryption techniques
Application layer	Detection and prevention of virus, worms, malicious code through code analysis.

Maintenance of a trust rating of various nodes is a promising technique to overcome many of the routing attacks. In this technique, every node maintains a trust rating of various nodes and packet transmission is carried out using a selective flooding technique.

University Questions

May/June 2015

Part A

1. List the characteristics of MANETs ? (Q.No:3)
2. Compare MANET Vs VANET.(Q.No:21)

Part B

(a) (i) Explain characteristics, applications of MANET? (Q.No:2)

(ii) Explain DSR Routing protocol in detail? (Q.No:7)

(Or)

(b) (i) Draw and explain the architecture of VANET? (Q.No:9)

(ii) Explain the various security and attacks on VANET? (Q.No:10)

Nov/Dec 2016

Part A

1. What is multicasting? (Q.No:23)
2. Compare and contrast MANET Vs VANET? (Q.No:21)

Part B

(a) Explain the Traditional Routing Protocols.(Q.No:4)

(Or)

(b) (i) What are Multicast routing protocols. (Q.No:8)

(ii) What are reactive and proactive protocols? Specify its advantages and disadvantages. (Q.No:5)

UNIT III MOBILE TELECOMMUNICATION SYSTEM

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

2 Marks

1) Write about GSM?

GSM (Global System for Mobile Communications) is at present being used in India. It is possibly the most successful digital mobile system to have ever been used till now. **An important characteristic of the GSM system is** that it provides **data services** in addition to **voice services**, and yet is compatible to 1G systems.

2) Listout GSM radio frequencies?

- operate either in the 900 MHz or in the 1800 MHz frequency bands.
- 850 MHz and 1900 MHz bands
- 400 MHz and 450 MHz frequency b
- uplink frequency band is 890–915 MHz, and the downlink frequency band is 935–960 MHz

1. Listout GSM services?

(i) Bearer services
(ii) Teleservices
(iii) Supplementary services

2. Define Bearer services?

Bearer services give the subscribers the capability **to send and receive data to/from remote computers or mobile phones**. For this reason, **bearer services are also known as data services**

3. Listout some of Teleservices ?

1) Telephony
2) Emergency number
3) Short message services
4) Fax

4. What are all the radio frequency elements compresed by RSS?

This subsystem **comprises** all the radio specific entities. That is,

i. The mobile stations,
ii. The base station subsystems
iii. The base transceiver station
iv. And the base station controller

5. Write short notes about SIM card?

The subscriber identity module (SIM)

✓ The SIM is a removable smart card.
✓ a SIM card is a very important component of a GSM network
✓ It contains all the subscription information of a subscriber and holds the key information that activates the

phone after it is powered on.

- ✓ Identification information is stored in the SIM card’s protected memory (ROM) that is not accessible or modifiable by the customer.
- ✓ The SIM card contains many other identifiers and tables such as card type, serial number, a list of subscribed services, and a Personal Identity Number (PIN).

6. Define Base Station Subsystem ?
(BSS):

- ✓ A GSM network comprises many BSSs. Each BSS consists of **A Base Station Controller (BSC)** and Several **Base Transceiver Stations (BTSs).**
- ✓ A BSS performs all functions necessary to **maintain radio connections to an MS**, as well **as does coding/decoding of voice**.

7. Define Base Transceiver Station ?
(BTS):

A BTS **comprises all radio equipment** such as antenna, signal processors and amplifiers that are necessary for radio transmission.

- o It **encodes the received signal**,
- o **modulates it on a carrier wave,**
- o **and feeds the RF signals to the antenna**.
- o **It communicates with both the mobile station and the BSC**.

8. Define Base Station Controller ?
(BSC):

A BSC manages the radio resource of the BTSs in the sense that **it assigns frequency and time slots for all MSs in the area**. It also manages the handoff from one BTS to another within the BSS. The BSC also multiplexes the radio channels onto the fixed network connection to the Mobile Switching Centre (MSC).

9. Define Network and switching subsystem ?
(NSS)

This subsystem forms the heart of the GSM system. It connects the wireless networks to the standard public networks and carries out usage-based charging, accounting, and also handles roaming. NSS consists of a switching centre and several databases as described below.

10. Define Mobile Switching Center?
(MSC):

An MSC can be considered to form the heart of a GSM network. An MSC sets up connections to other MSCs and to other networks such as Public Data Network (PDN). An MSC is responsible for the connection setup, connection release, and call handoff to other MSCs. A Gateway MSC (GMSC) is responsible for gateway functions, while a customer roams to other networks. It also performs certain other supplementary services such as call forwarding, multiparty calls, etc.

11. Define Home Location Registers ?
(HLRs):

A HLR stores in a database important information that is specific to each subscriber. The information contains subscriber’s IMSI, pre/post paid, user’s current location, etc.

12. Define Visitor Location Register ?

(VLR):

It is essentially a temporary database that is updated whenever a new MS enters its area by roaming. The information is obtained from the corresponding HLR database. The function of the VLR is to reduce the number of queries to the HLR and make the user feel as if he were in his home network.

13. Define Operation subsystem (OSS)?

The operation subsystem contains all the functions necessary for network operation and maintenance. **It consists of the following:**

- **Operation and Maintenance Centre (OMC):** It supervises all other network entities. Its functions are traffic monitoring, subscribers, security management and accounting billing.
- **Authentication Centre** (**AuC**)**:** It protects against intruders targeting the air interface. The AuC stores information concerned with security features such as user authentication and encryption. The AuC is related to the HLR.
- **Equipment Identity Register (EIR):** It is essentially a database that is used to track handsets using the IMEI. It helps to block calls from stolen, unauthorized, or defective mobiles.

14. Listout 3 leves of GSM Security?

- Operator's level,
- Customer's level and
- System level.

15. Define General Packet Radio Service (GPRS)

It transfers data packets from GSM mobile stations to external packet data networks (PDNs). Packets can be directly routed from the GPRS mobile stations to packet switched networks making it easy to connect to the Internet.

16. Define Point-to-Point (PTP) service?

- **The PTP service** is between two users and can either be connectionless or connection-oriented.

17. Define Point-to-Multipoint (PTM) service?

- **The PTM** is a data transfer service from one user to multiple users.
  - ✓ Again, **there are two types of PTM services**.
  - ✓ **One is multicast PTM** where the data packets are broadcast in a certain area
  - ✓ and the **other is group call PTM** where the data packets are addressed to a group of users.

18. Define GSN?

A GSN is essentially a router. All GSNs are integrated into a standard GSM architecture.

19. Define GGSN?

The GGSN is the interworking unit between the GPRS network and the external packet data network (PDN). The GGSN **contains routing information for** GPRS users, performs address connection and tunnells data to a user through encapsulation.

20. Define SGSN?

As shown in Fig. 2.10, **SGSN (Serving GPRS Support Node)** helps support MS. The SGSN is connected to BSC through frame relay and it is at the same hierarchy level as the

21. Dissimilarities between UTMS networks?

1) Higher speech quality
2) Higher data rate
3) Virtual home environment

22. Define User Equipment?

(UE):

The User Equipment (UE) is the name by which a cell phone is referred to. The new name was chosen because of the considerably greater functionality that the UE incorporates compared to a cell phone. It can be thought of as both a mobile phone used for talking and a data terminal attached to a computer with no voice capability.

23. Define Radio Network Subsystem?

(RNS):

The RNS is the equivalent of the Base Station Subsystem (BSS) in GSM. It provides and manages the wireless interface for the overall network.

24. Define Core Network?

The core network is the equivalent of the GSM Network Switching Subsystem (NSS).

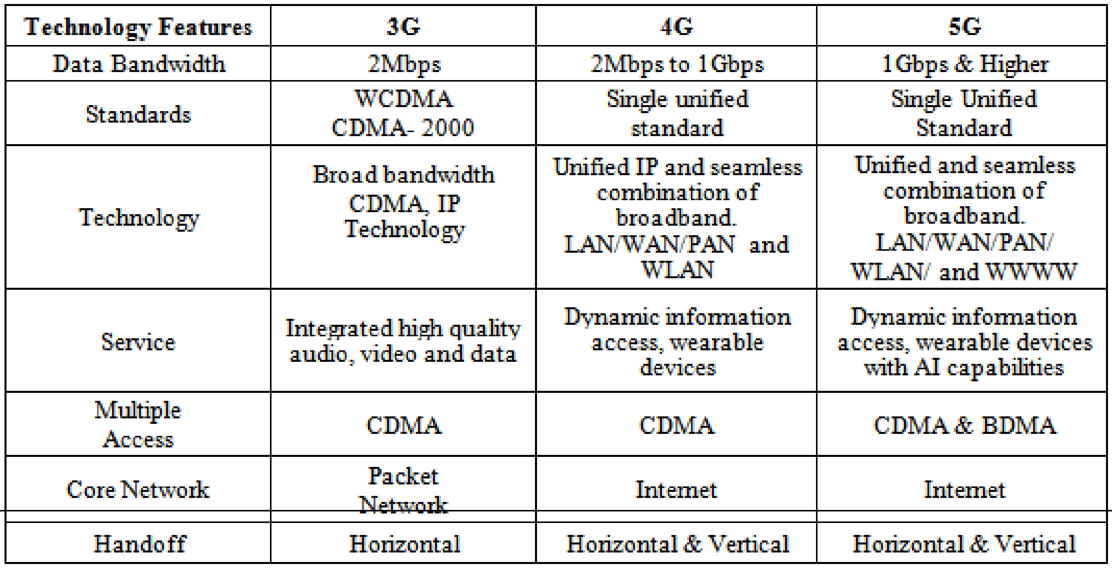
25. List the 3 important features of GSM security. (May/June 2015)

1) Authentication
2) Confidentiality
3) Anonymity(unknown or unacknowledged)

26. What are the main elements of UMTS. (May/June 2015)

1) User Equipment (UE):
2) Radio Network Subsystem (RNS)
3) Core Network

27. Difference between 1g,2g,3g,4g,5g?



Technology Features	3G	4G	5G
Data Bandwidth	2Mbps	2Mbps to 1Gbps	1Gbps & Higher
Standards	WCDMA CDMA- 2000	Single unified standard	Single Unified Standard
Technology	Broad bandwidth CDMA, IP Technology	Unified IP and seamless combination of broadband. LAN/WAN/PAN and WLAN	Unified and seamless combination of broadband. LAN/WAN/PAN/ WLAN/ and WWWW
Service	Integrated high quality audio, video and data	Dynamic information access, wearable devices	Dynamic information access, wearable devices with AI capabilities
Multiple Access	CDMA	CDMA	CDMA & BDMA
Core Network	Packet Network	Internet	Internet
Handoff	Horizontal	Horizontal & Vertical	Horizontal & Vertical

28. Write about the supplementry services in GSM? Nov/Dec 2016

Supplementary services

GSM provides certain supplementary services such as user identification, call redirection, and forwarding of ongoing calls. In addition, standard ISDN features such as ‘close user groups and ‘multiparty’ communication are available.

16 Marks

1) Explain detail about Global System for Mobile Communications (GSM) with neat diagram? (May/June 2015) Nov/Dec 2016

GSM :

(Global System for Mobile Communications) is at present being used in India. It is possibly the most successful digital mobile system to have ever been used till now

. **An important characteristic of the GSM system is** that it provides **data services** in addition to **voice services**, and yet is compatible to 1G systems.

GSM networks operate in **four different radio frequencies**.

- Most GSM networks **operate either in the 900 MHz or in the 1800 MHz** frequency bands.
- Some countries in the American continent (especially the USA and Canada) use the **850 MHz and 1900 MHz** bands because the 900 MHz and 1800 MHz frequency bands are already allocated for other purposes.
- The relatively rarely used **400 MHz and 450 MHz** frequency bands are assigned in some countries, notably Scandinavia where these frequencies were previously used for the first generation systems.
- In the 900 MHz band, the **uplink frequency band is 890–915 MHz**, and the **downlink frequency band is 935–960 MHz**.

1) GSM Services

GSM provides three main categories of services. These are:

(i) Bearer services
(ii) Teleservices
(iii) Supplementary services

i) Bearer services

Bearer services give the subscribers the capability **to send and receive data to/from remote computers or mobile phones**. For this reason, **Bearer services are also known as Data services (see Box 2.1)**.

These services also enable the transparent transmission of data between GSM and other networks like PSTN, ISDN, etc. at rates from 300 bps to 9600 bps.

These services are **implemented on the lower-three layers of the OSI reference model**. Besides supporting SMS, e-mail, voice mailbox, and Internet access, this service provides the users with the capability to execute remote applications. **GSM supports data transfer rates of up to 9.6 kbps.**

BOX 2.1 GSM bearer services

The GSM data services are named *bearer* services. **Consider the following example:** Suppose a customer requires to send a data file such as a picture to a computer at the office that is connected to a public telephone network.

In this example, the bearer service provides 9.6 kbps circuit switched data transfer. The handset dials the office computer telephone number and establishes a connection with it via the modem. When the office computer modem accepts the call, the customer's handset begins to send data directly on the telephone line channel at 9.6 kbps.

Bearer services permit **either transparent or non-transparent**, **and either synchronous or asynchronous** modes of data transmission.

<u>The transparent bearer services:</u>

- ✓ The transparent bearer services use the functions of the physical layer of transmission of data leading to constant delay and throughput if no transmission errors occur. There is a mechanism called **FEC (Forward Error Correction)** to increase the quality of data transmission.

<u>The non-transparent bearer services:</u>

- ✓ The non-transparent bearer services use protocols of the second and third layers to implement error correction and flow control.

They use transparent bearer services in addition to a Radio Link Protocol (RLP). This protocol comprises mechanisms of high level data link control.

ii) <u>Teleservices</u>

GSM provides **both the voice-oriented teleservices and the non-voice teleservices**, as discussed below.

<u>Telephony:</u>

The main goal of GSM was to provide high quality digital voice transmission, offering the bandwidth of 3.1 kHz of analog phone systems. Special codecs(**a device or program that compresses data to enable faster transmission and decompresses received data.)** are used for voice transmission, while other codecs are used for the transmission of analog data for communication with traditional computer modems used in fax machines.

<u>Emergency number</u>:

The same number is used throughout an area. This service is free of cost and mandatorily provided by all service providers. This connection will automatically be set up with the closest emergency centre.

<u>Short message services:</u>

This service offers transmission of text messages of sizes up to 160 characters. SMS services use the signalling channels, making possible the duplex system of the sending and receiving the SMSs messages.

Fax: In this service, using modems fax data is transmitted as digital data over the analog telephone network according to the ITU-T Standards T.4 and T.30.

iii) Supplementary services

GSM provides certain supplementary services such as user identification, call redirection, and forwarding of ongoing calls. In addition, standard ISDN features such as ‘close user groups and ‘multiparty’ communication are available.

2) System Architecture of GSM

A GSM system consists of three main subsystems:

(i) Radio Subsystem (RSS)

(ii) Networking and Switching Subsystem (NSS)

(iii) Operation Subsystem (OSS)

A schematic of the functional architecture of a GSM system is shown in Fig. 2.9. The different components of this architecture are briefly explained in the following.

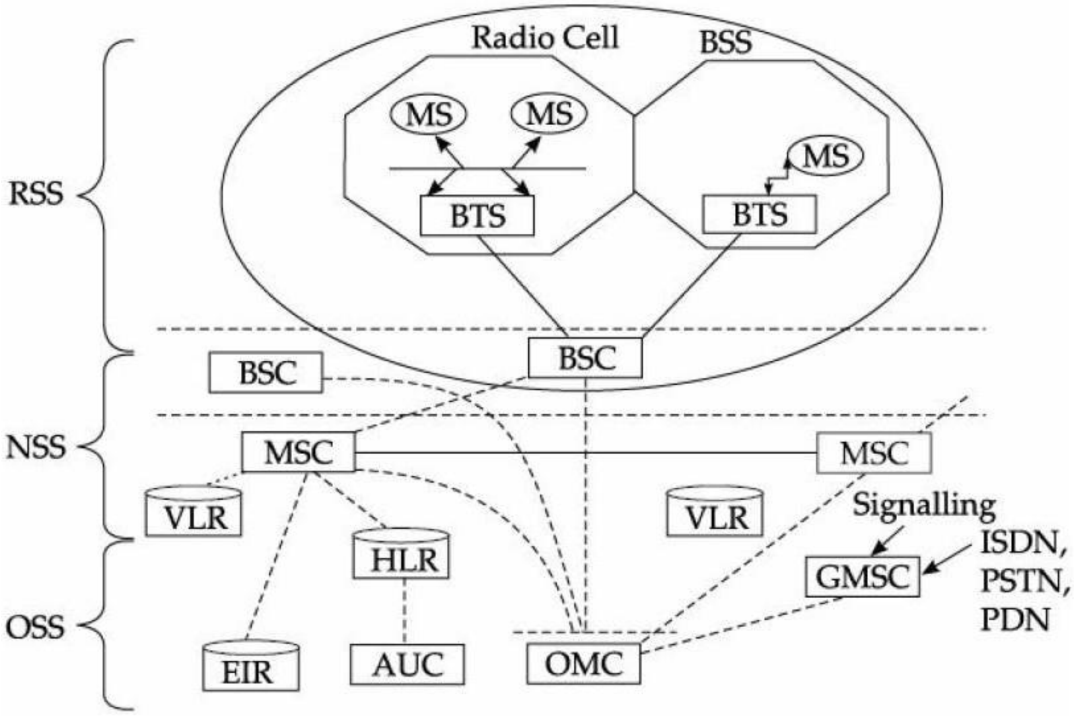


Figure 2.9 *Functional architecture of a GSM system.*

Radio subsystem (RSS)

This subsystem **comprises** all the radio specific entities. That is,

i) **The mobile stations,**
ii) **The base station subsystems,**
iii) **The base transceiver station**
iv) **And the base station controller.**

the important components of **the radio subsystem** in the following:

Mobile Station (Ms):

A mobile station (MS) or cell phone contains **two major components**:

- **a.** The subscriber identity module **(SIM)**
- **b.** And the **Mobile Device.**

a) The subscriber identity module (SIM)

- ✓ The SIM is a removable smart card.
- ✓ Each mobile device has a unique identifier that is known as its **IMEI (International Mobile Equipment Identity)**.
- ✓ Apart from the telephone interface, an **MS** also offers other types of interfaces to the users such as USB, Bluetooth, etc.
- ✓ Despite its small size, **a SIM card is a very important component of a GSM network**.
- ✓ It contains all the **subscription information of a subscriber** and holds **the key information that activates the phone** after it is powered on.
- ✓ It contains **a microcontroller** to primarily **store and retrieve data from the flash storage** on the SIM.
- ✓ **Identification information is stored in the SIM card's protected memory (ROM)** that is not accessible or modifiable by the customer.
- ✓ The SIM card contains many other identifiers and tables such as card type, serial number, a list of subscribed services, and a Personal Identity Number (PIN).

b) The Mobile Device

- ✓ **Additional flash memory** is included in the mobile device to allow storage of other information such as addresses, pictures, audio and video clips, and short messages.

Base Station Subsystem (BSS):

- ✓ A GSM network comprises many BSSs. Each BSS consists of **A Base Station Controller (BSC)** and Several **Base Transceiver Stations (BTSs).**
- ✓ A BSS performs all functions necessary to **maintain radio connections to an MS**, as well **as does coding/decoding of voice**.

Base Transceiver Station (BTS):

A BTS **comprises all radio equipment** such as antenna, signal processors and amplifiers that are necessary for radio transmission.

- o It **encodes the received signal**,
- o **modulates it on a carrier wave,**
- o **and feeds the RF signals to the antenna**.
- o **It communicates with both the mobile station and the BSC**.

Base Station Controller (BSC):

A BSC manages the radio resource of the BTSs in the sense that **it assigns frequency and time slots for all MSs in the area**. It also manages the handoff from one BTS to another within the BSS. The BSC also multiplexes the radio channels onto the fixed network connection to the Mobile Switching Centre (MSC).

Network and switching subsystem (NSS)

This subsystem forms the heart of the GSM system. It connects the wireless networks to the standard public networks and carries out usage-based charging, accounting, and also handles roaming. NSS consists of a switching centre and several databases as described below.

Mobile Switching Center (MSC):

An MSC can be considered to form the heart of a GSM network. An MSC sets up connections to other MSCs and to other networks such as Public Data Network (PDN). An MSC is responsible for the connection setup, connection release, and call handoff to other MSCs. A Gateway MSC (GMSC) is responsible for gateway functions, while a customer roams to other networks. It also performs certain other supplementary services such as call forwarding, multiparty calls, etc.

Home Location Registers (HLRs): A HLR stores in a database important information that is specific to each subscriber. The information contains subscriber's IMSI, pre/post paid, user's current location, etc.

Visitor Location Register (VLR): It is essentially a temporary database that is updated whenever a new MS enters its area by roaming. The information is obtained from the corresponding HLR database. The function of the VLR is to reduce the number of queries to the HLR and make the user feel as if he were in his home network.

Operation subsystem (OSS)

The operation subsystem contains all the functions necessary for network operation and maintenance. **It consists of the following:**

- **Operation and Maintenance Centre (OMC):** It supervises all other network entities. Its functions are traffic monitoring, subscribers, security management and accounting billing.
- **Authentication Centre** (**AuC**)**:** It protects against intruders targeting the air interface. The AuC stores information concerned with security features such as user authentication and encryption. The AuC is related to the HLR.
- **Equipment Identity Register (EIR):** It is essentially a database that is used to track handsets using the IMEI. It helps to block calls from stolen, unauthorized, or defective mobiles.

3) GSM Security

Security in GSM is broadly supported **at three levels:**

- **Operator's level,**
- **Customer's level and**
- **System level.**

These three levels help oversee aspects such as correct billing to the customer, avoiding fraud, protecting services, and ensuring anonymity**. The following are a few important features associated with providing security in GSM networks**.

Authentication

The purpose of authentication is to protect the network against unauthorized use. In the GSM context, it helps protect the GSM subscribers by denying the possibility for intruders to impersonate authorized users.

- ✓ A GSM network operator can verify the identity of the subscriber, making it highly improbable to clone someone else's mobile phone identity.
- ✓ Authentication can be achieved in a simple way by using a password such as Personal Identification Number (PIN). This method is not very secure in GSM networks as an attacker can "listen" the PIN and easily break the code.

Confidentiality

A GSM network protects voice, data and sensitive signalling information (e.g. dialed digits) against eavesdropping(**secretly listen to a conversation**) on the radio path.

Confidentiality of subscriber-dialled information in the GSM network is achieved by using encryption techniques prescribed by the GSM designers. Data on the radio path is encrypted between the Mobile Equipment (ME) and the BTS which protects user traffic and sensitive signaling data against eavesdropping.

Anonymity(unknown or unacknowledged)

A GSM network protects against someone tracking the location of a user or identifying calls made to (or from) the user by eavesdropping on the radio path.

The anonymity of the subscriber on the radio access link in the GSM network is achieved by allocating Temporary Mobile Subscriber Identity (TMSIs) instead of permanent identities.

This helps to protect against tracking a user's location and obtaining information about a user's calling pattern.

2) Explain in detail about General Packet Radio Service (GPRS) with architecture? (May/June 2015)

General Packet Radio Service (GPRS)

GPRS when integrated with GSM, significantly improves and simplifies Internet access. It transfers data packets from GSM mobile stations to external packet data networks (PDNs). Packets can be directly routed from the GPRS mobile stations to packet switched networks making it easy to connect to the Internet.

GSM uses a billing system based on the time (duration) of connection, whereas GPRS uses a billing system based on the amount of transmitted data rather than the duration of the connection. So, users can remain continuously connected to the system, and yet get charged only for the amount of transmitted data.

1. GPRS Services

GPRS offers end-to-end packet-switched data transfer services which can be categorized into the following two types:

i) Point-to-Point (PTP) service

- ✓ **The PTP service** is between two users and can either be connectionless or connection-oriented.

(ii) Point-to-Multipoint (PTM) service.

- ✓ **The PTM** is a data transfer service from one user to multiple users.
- ✓ Again, **there are two types of PTM services**.
  - **One is multicast PTM** where the data packets are broadcast in a certain area
  - and the **other is group call PTM** where the data packets are addressed to a group of users.

2. GPRS Architecture

GPRS architecture introduces **two new network elements**, called

- **GPRS Support Node (GSN) and**
- **The Gateway GPRS Support Node (GGSN).**

GSN:

A GSN is essentially a router. All GSNs are integrated into a standard GSM architecture.

GGSN:

The GGSN is the interworking unit between the GPRS network and the external packet data network (PDN). The GGSN **contains routing information for** GPRS users, performs address connection and tunnells data to a user through encapsulation.

In Fig. 2.10, the GGSN is connected to an external network and it transfers packets to the SGSN through an IP-based GPRS backbone network.

SGSN:

As shown in Fig. 2.10, **SGSN (Serving GPRS Support Node)** helps support MS. The SGSN is connected to BSC through frame relay and it is at the same hierarchy level as the MSC. The GPRS Register (GR) is a part of HLR which stores all the relevant GPRS data.

In a part of HLR which stores all the relevant data of GPRS in a mobile IP network, GGSN and SGSNs can be compared with home agent and foreign agent respectively. The data packets are transmitted to the BSS and finally to the MS through the GGSN and SGSN.

The MSC as we have already discussed is responsible for data transport in the traditional circuit-switched GSM.

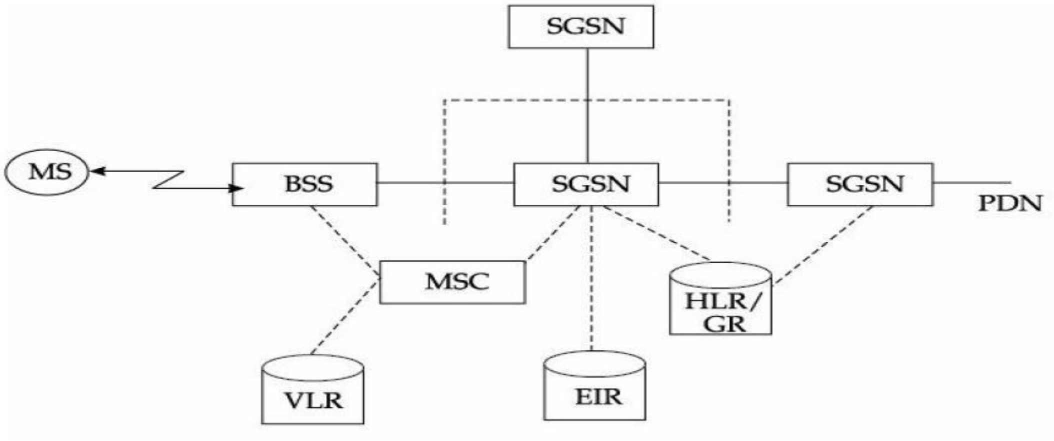


Figure 2.10 *GPRS architecture reference model.*

3) Explain in detail about Universal Mobile Telecommunications System (UMTS) and its dissimilarity? (May/June 2015) Nov/Dec 2016

Universal Mobile Telecommunications System (UMTS)

CDMA2000 and UMTS were developed separately and **are two separate ITU(International Telecommunication Union Governmental) approved 3G standards.** In these networks, coverage is provided by a combination of various cell sizes, ranging from "in building" pico cells to global cells provided by satellites, giving service to the remote regions of the world.

The UMTS was **developed mainly for countries with GSM networks**, and it is expected that **all GSM networks will be upgraded to UMTS networks**. Because it is a new technology, a whole new radio access network has to be built. **An important advantage of UMTS is that it gives significantly enhanced capacities to operators.**

The UMTS specification has been designed so that the UMTS systems are compatible with GSM networks. Therefore, the UMTS networks can easily work with any existing GSM/GPRS network. The UMTS systems use different frequency bands, so the BTSs do not interfere with each other.

The dissimilarities between these networks, The UMTS networks are different from the 2G networks in the following respects:

- ***Higher speech quality:*** In addition to speech traffic, the UMTS supports the advanced data and information services and can be called a true multimedia network.
- ***Higher data rate:*** The UMTS supports 2 Mbps data rate, which is much higher than that supported by the 2G mobile systems.
- ***Virtual home environment (VHE):*** A user roaming from his network to other UMTS networks will not feel any discontinuity or service difference, thus giving a "feeling" of being in the home network. In contrast, in a 2G network, a user is registered to a visitor location and is also charged a roaming overhead.

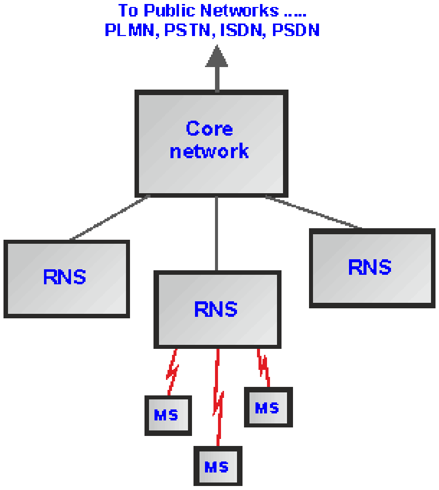
UMTS Network Architecture

The UMTS network architecture can **be divided into three main elements**:

User Equipment (UE): The User Equipment (UE) is the name by which a cell phone is referred to. The new name was chosen because of the considerably greater functionality that the UE incorporates compared to a cell phone. It can be thought of as both a mobile phone used for talking and a data terminal attached to a computer with no voice capability.

Radio Network Subsystem (RNS): The RNS is the equivalent of the Base Station Subsystem (BSS) in GSM. It provides and manages the wireless interface for the overall network.

Core Network: The core network is the equivalent of the GSM Network Switching Subsystem (NSS). It is the equivalent of the GSM Network Switching Subsystem or NSS.



User Equipment, UE

The USER Equipment or UE is a major element of the overall 3G UMTS network architecture. There are a number of elements within the UE that can be described separately:

- **UE RF circuitry:** The RF areas handle all elements of the signal, both for the receiver and for the transmitter. One of the major challenges for the RF power amplifier was to reduce the power consumption.

- **Baseband processing:** The base-band signal processing consists mainly of digital circuitry. This is considerably more complicated than that used in phones for previous generations. Again this has been optimised to reduce the current consumption as far as possible.

- **Battery:** While current consumption has been minimised as far as possible within the circuitry of the phone, there has been an increase in current drain on the battery. With users expecting the same lifetime between charging batteries as experienced on the previous generation phones, this has necessitated the use of new and improved battery technology.

- **Universal Subscriber Identity Module, USIM:** The UE also contains a SIM card, although in the case of UMTS it is termed a USIM (Universal Subscriber Identity Module). This is a more advanced version of the SIM card used in GSM and other systems, but embodies the same types of information. It contains the International Mobile Subscriber Identity number (IMSI) as well as the Mobile Station International ISDN Number (MSISDN). Other information that the USIM holds includes the preferred language to enable the correct language information to be displayed, especially when roaming, and a list of preferred and prohibited Public Land Mobile Networks (PLMN).

- The USIM also contains a short message storage area that allows messages to stay with the user even when the phone is changed. Similarly "phone book" numbers and call information of the numbers of incoming and outgoing calls are stored.

UMTS Radio Network Subsystem

The overall radio access network, i.e. collectively all the Radio Network Subsystem is known as the

UTRAN UMTS Radio Access Network.The radio network subsystem is also known as the UMTS Radio Access Network or UTRAN

UMTS Core Network

The UMTS core network may be split into two different areas:

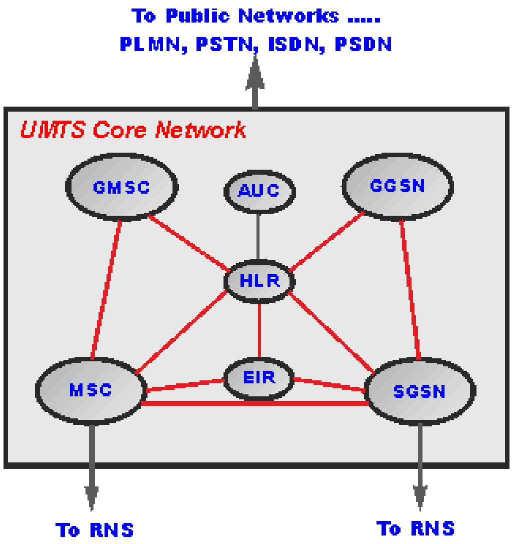
- **Circuit switched elements:** These elements are primarily based on the GSM network entities and carry data in a circuit switched manner, i.e. a permanent channel for the duration of the call.

- **Packet switched elements:** These network entities are designed to carry packet data. This enables much higher network usage as the capacity can be shared and data is carried as packets which are routed according to their destination.

Circuit switched elements

The circuit switched elements of the UMTS core network architecture include the following network entities:

- **Mobile switching centre (MSC):** This is essentially the same as that within GSM, and it manages the circuit switched calls under way.
- **Gateway MSC (GMSC):** This is effectively the interface to the external networks.



Packet switched elements

The packet switched elements of the 3G UMTS core network architecture include the following network entities:

- **Serving GPRS Support Node (SGSN):** The SGSN provides a number of functions within the UMTS network architecture.
  - **Mobility management**
  - **Session management**
  - **Interaction with other areas of the network:**
  - **Billing**

- **Gateway GPRS Support Node (GGSN):**

  Like the SGSN, this entity was also first introduced into the GPRS network. The Gateway GPRS Support Node (GGSN) is the central element within the UMTS packet switched network. It handles inter-working between the UMTS packet switched network and external packet switched networks, and can be considered as a very sophisticated router. In operation, when the GGSN receives data addressed to a specific user, it checks if the user is active and then forwards the data to the SGSN serving the particular UE.

<u>Shared elements</u>

The shared elements of the 3G UMTS core network architecture include the following network entities:

- **Home location register (HLR)**
- **Equipment identity register (EIR)**
- **Authentication centre (AuC**)

4) Explain in detail of 1G,2G,2.5G,3G,4G and 5G ? <u>Nov/Dec 2016</u>

WHAT IS WIRELESS ?

The word wireless is dictionary defined "having no wires ". In networking terminology, wireless is the term used to describe any computer network where there is no physical wired connection between sender and receiver, but rather the network is connected by radio waves and or microwaves to maintain communications. Wireless networking utilizes specific equipment such as NICs and Routers in place of wires (copper or optical fibre).

<u>1G TECHNOLOGY</u>

✓ 1G refers to the first generation of wireless telephone technology, mobile telecommunications which was first introduced in 1980s and completed in early 1990s.
✓ IPs Speed was upto 2.4kbps.
✓ It allows the voice calls in 1 country.
✓ 1G network use Analog Signal.
✓ AMPS was first launched in USA in 1G mobile systems

<u>DRA WBACKS OF 1G</u>

- Poor Voice Quality
- Poor Battery Life
- Large Phone Size
- No Security
- Limited Capacity
- Poor Han doff Reliability

1G Wireless System

<u>2G TECHNOLOGY</u>

✓ refers to the 2^{nd} generation which is based on GSM.
✓ It was launched in Finland in the year 1991.
✓ 2G network use digital signals.
✓ IFs data speed was upto 64kbps.

Features Includes:

- ✓ It enables services such as text messages**,** picture messages and MMS (multi media message).
- ✓ It provides better quality and capacity.

DRA WBACKS OF 2G

- ✓ 2G requires strong digital signals to help mobile phones work. If there is no network coverage in any specific area**,** digital signals would weak.
- ✓ These systems are unable to handle complex data such as Videos.

G is a technology

- ✓ 2.5G is a technology between the second (2G) and third (3G) generation of mobile telephony.
- ✓ 2.5G is sometimes described as 2G Cellular Technology combined with GPRS.

Features Includes:

- ✓ Phone Calls
- ✓ Send/Receive E-mail Messages Web Browsing
- ✓ Speed: 64-144 kbps
- ✓ Camera Phones
- ✓ Take a time of 6-9 mins, to download a 3 mins. Mp3 song

3G is a technology

- ✓ 3G technology refer to third generation which was introduced in year 2000s.
- ✓ Data Transmission speed increased from 144kbps- 2Mbps.
- ✓ Typically called Smart Phones and features increased its bandwidth and data transfer rates to accommodate web-based applications and audio and video files.

Features Includes:

- □ Providing Faster Communication
- □ Send/Receive Large Entail Messages
- □ High Speed Web /More Security
- □ Video Conferencing / 3D Gaming
- □ TV Streaming/Mobile TV/ Phone Calls Large Capacities and Broadband Capabilities
- □ 11 sec -1.5 min. time to download a 3 min Mp3 song.

4G is a technology

- ✓ 4G technology refer to or short name of fourth Generation which was started from late 2000s.
- ✓ A Capable of providing 100Mbps - lGbps speed.
- ✓ One of the basic term used to describe 4G is MAGIC.
    - o Mobile Multimedia

- o Anytime Anywhere
- o Global Mobility Support
- o Integrated Wireless Solution
- o Customized Personal Services

Also known as Mobile Broadband Everywhere.

4G (Anytime, Anywhere) Advantage

- ✓ The next generations of wireless technology that promises higher data rates and expanded multimedia services.
- ✓ Capable to provide speed lOOMbps-IGbps.
- ✓ High QOS and High Security
- ✓ Provide any kind of service at any time as per user requirements, anywhere.

Features Includes:

- □ *More Security*
- □ *High Speed*
- □ *High Capacity*
- □ *Low Cost Per-bit etc.*

DRA WBACKS OF 4G

- □ Battery uses is more
- □ Hard to implement
- □ Need complicated hardware
- □ Expensive equipment required to implement next generation network.

5G is a technology

- ✓ 5G technology refer to short name of fifth Generation which was started from late 2010s.
- ✓ Complete wireless communication with almost no limitations.
- ✓ It is highly supportable to WWWW Wireless World Wide Web).

Benifits of 5G:

- ♦ High Speedy High Capacity
- ♦ 5(7 technology providing large broadcasting of data in Gbps.
- ♦ Multi - Media Newspapers, watch T. Vpro, clarity as to that of an HD Quality.
- ♦ Faster data transmission that of the previous generations.
- ♦ Large Phone Memory, Dialing Speedy clarity in Audio/Video.
- ♦ Support interactive multimedia, voice, streaming video, Internet and other
- ♦ 5G is More Effective and More Attractive.

Anna University Questions

May/June 2015

Part A

1. List the 3 important features of GSM security. **[page:5 ,Q.no:25]**
2. What are the main elements of UMTS. **[page:5 ,Q.no:26]**

Nov/Dec 2016

3. Write about the supplementry services in GSM? **[page:5 ,Q.no:28]**

Part B

13.(a) (i)Describe GSM architecture and its services in detail. (8) **[page:6 ,Q.no:1]**

(ii)Explain GSM Authentication and Security.(8) **[page: ,Q.no:1]**

OR

(b) (i)Explain GPRS and its Protocol architecture. (8) **[page:11 ,Q.no:2]**

(ii)Explain in detail about UMTS architecture.(8) **[page:13 ,Q.no:3]**

Nov/Dec 2016

13.(a) (i)What are the functions of authentication and encryption in GSM? How is system security maintained. (8) **[page:6 ,Q.no:1]**

(ii)Explain in detail about the handovers of GSM.(8) **[page:6 ,Q.no:1]**

OR

(b) (i)Explain the functions of GPRS protocol stack with a diagram. (8) **[page:11 ,Q.no:2]**

(ii)Explain in detail about UMTS architecture.(8) **[page:13 ,Q.no:3]**

IT6601 MOBILE COMPUTING

UNIT I INTRODUCTION 9

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

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.

UNIT III MOBILE TELECOMMUNICATION SYSTEM 9

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

UNIT IV MOBILE AD-HOC NETWORKS 9

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.

UNIT V MOBILE PLATFORMS AND APPLICATIONS 9

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

TOTAL: 45 PERIODS

TEXT BOOK:

1. Prasant Kumar Pattnaik, Rajib Mall, “Fundamentals of Mobile Computing”, PHI Learning Pvt. Ltd, New Delhi – 2012.

REFERENCES:

1. Jochen H. Schller, “Mobile Communications”, Second Edition, Pearson Education, New Delhi, 2007.
2. Dharma Prakash Agarval, Qing and An Zeng, "Introduction to Wireless and Mobile systems", Thomson Asia Pvt Ltd, 2005.
3. Uwe Hansmann, Lothar Merk, Martin S. Nicklons and Thomas Stober, “Principles of Mobile Computing”, Springer, 2003.
4. William.C.Y.Lee,“Mobile Cellular Telecommunications-Analog and Digital Systems”, Second Edition,Tata Mc Graw Hill Edition ,2006.
5. C.K.Toh, “AdHoc Mobile Wireless Networks”, First Edition, Pearson Education, 2002.
6. Android Developers : http://developer.android.com/index.html
7. Apple Developer : https://developer.apple.com/

UNIT I: INTRODUCTION

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.

2 Marks

1) What Is Mobile Computing?

Mobile computing **(sometimes called ubiquitous computing and also at times called nomadic computing)** is widely described as the ability to compute remotely while on the move. This is a new and fast emerging discipline that has made it possible for people to access information from anywhere and at anytime.

Mobile computing as encompassing two separate and distinct concepts:

- Mobility and Computing.

2) Define computing?

Computing denotes the capability to automatically carry out certain processing related to service invocations on a remote computer.

3) Define Mobility?

Mobility, on the other hand, provides the capability to change location while communicating to invoke computing services at some remote computers.

4) What is main advantage and Disadvantage of mobile computing?(May/june 2015)

Advantage:-

✓ The tremendous **flexibility** it provides to the users.

✓ The user need not be tethered to the chair in front of his desktop, but **can move locally or even to far away places** and at the same time achieve what used to be performed while sitting in front of a desktop.

- Location Flexibility
- Saves Time
- Enhanced Productivity
- Ease of Research
- Entertainment
- Streamlining of Business Processes

Disadvantages:–

- quality of connectivity
- security concerns
- Power Consumption

5) Distinguish Mobile Computing vs. Wireless Networking

Mobile Computing	**Wireless Networking**
✓ accessing information and remote computational services while on the move ✓ That **mobile computing is based on wireless networking** and helps one to invoke computing services on remote servers while on the move	✓ provides the basic communication infrastructure necessary to make this possible. ✓ **wireless networking is an important ingredient of mobile computing**

6) List out various forms of Wireless networks?

Wireless networks appear in various forms such as

- WLANs (Wireless LANs),
- Mobile Cellular Networks,
- Personal Area Networks (Pans),
- And Ad Hoc Networks, etc.

7) What are the two basic types of wireless network?

Wireless networks can be classified into two basic types.

1. One is an extension of **wired networks**. It uses fixed infrastructures such as
2. The other type of **wireless network is an ad hoc network**

8) List out types of computer network?

Several types of computer networks are in use today.

1. Controller AreaNetworks (CANs)
2. Local Area Networks (LANs)
3. and Internetworks.

9) Define CAN?

A Controller Area Network (CAN) is essentially a very small network that is typically used to connect the different components of an embedded controller.

The end-to-end length of a CAN is usually less than 50 metres. Since the propagation time of a CAN is very small, it behaves more like alocal bus in a computer.

10) Define LANs?

A Local Area Network (LAN) is typically deployed in a building or a campus and is usually privately owned.

For example, a LAN can be used to connect a number of computers within an organization to share data and other resources such as files, printers, FAX services, etc. LANs typically operate at data rates exceeding 10 Mbps and many present-day LANs (gigabit Ethernets) operate at 1 Gbps.

11) Define Internetwork?

Several LANs can be interconnected using switches to realize internetworks or internet in short. In an internet, a node in a LAN communicates with a node in another LAN using packet switching.

12) Listout Component of wireless System?

A wireless communication system is built from various types of basic components. The following are some of these basic types of components.

- ✓ ***Transmitter***
- ✓ ***Receiver***
- ✓ ***Antenna***
- ✓ ***Filters***
- ✓ ***Amplifiers***
- ✓ ***Mixers***

13) Write short notes about WLANs?

Wireless Local Area

Networks (WLANs) provide connectivity between computers over short distances using the wireless medium.

Typical indoor applications of WLANs may be in educational institutes, office buildings and factories where the required coverage distances are usually restricted to less than a few hundred feet.

14) Brief about Access point ?

Access point: It is a radio receiver/transmitter (also called transceiver) that connects to the wired network. These are typically mounted on the roofs at different locations of a building.

You can spot them if you carefully observe the roof of a building having wireless LAN. The transceiver exchanges signals with the wireless LAN card in desktop or notebook PCs.

A single access point can support a small group of users. It is connected to a wired network through cables and provides the connectivity between wireless devices and the wired network.

15) Write short notes about Wireless LAN cards ?

Wireless LAN cards*:* End-users access the WLAN through WLAN adapters (wireless network interface cards) in their hand-helds. The LAN card used to be mounted on the motherboard of a computer. Now, it is inbuilt into the motherboards.

16) Define Bridge?

Bridge*:* It is used for connecting two LANs that may be in two different buildings or on two separate floors within the same building.

17) Write Advantages of Wireless LANs over Wired LANs?

Advantages of Wireless LANs over Wired LANs

1. Mobility- users get information at any place
2. Simplicity and speedy deployment
3. Flexibility: Wireless technology allows the network to be accessible where wiring is difficult to lay
4. Cost effectiveness

18) Write Bluetooth technology?

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHFradio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices, and building personal area networks (PANs)

19) Define PANs?

A personal area network (PAN) is a computer network used for data transmission among devices such as computers,telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication)

20) What is piconet?

A **piconet** is a computer network which links a wireless user group of devices using Bluetooth technology protocols. A piconet consists of two or more devices occupying the same physical channel (synchronized to a common clock and hopping sequence). It allows one *master* device to interconnect with up to seven active *slave* devices.

21) What will the master and slave?

Master/slave is a model of communication where one device or process has unidirectional control over one or more other devices. In some systems a master is selected from a group of eligible devices, with the other devices acting in the role of slaves.

22) Describe Mobile ad hoc network?

An ad hoc network is also known as a **Mobile Ad hoc Network(MANET)**. It is a collection of mobile nodes that form a network on the fly without requiring the support of any fixed infrastructure.Wireless sensor networks are a special type of wireless ad hoc networks.

23) Lisout the Chracteristic of Mobile computing?

Characteristics of Mobile Computing

- Ubiquity
- Location awareness
- Adaptation
- Broadcast

24) Listout the three tiers of a mobile computing application?

Presentation (Tier-1)
Application (Tier-2)
Data (Tier-3)

25) Write about MAC protocol?

MAC protocol is to enforce discipline in the access of a shared channel when multiple nodes contend to access that channel. At the same time, two other objectives of any MAC protocol are maximization of the utilization of the channel and minimization of average latency of transmission.

However, a MAC protocol must be fair and ensure that no node has to wait for an unduly(தேவையில்லாமல்) long time, before it is allowed to transmit.

26) Write some of issues of MAC protocol?

- Hidden Terminal Problems
- Exposed Terminal Problems

27) List out classification of MAC protocol?

(i) Fixed assignment schemes-
(ii) Random assignment schemes
(iii) Reservation-based schemes

28) Define fixed assignment schemes ?

In fixed assignment schemes, the resources required for a call are assigned for the entire duration of the call.

29) Define random assignment schemes ?

In random assignment schemes are comparable to the connection-less packet-switching schemes. In this, no resource reservations are made, the nodes simply start to transmit as soon as they have a packet to send.

30) Define reservation assignment schemes ?

In the reservation schemes, a node makes explicit reservation of the channel for an entire call before transmitting. This is analogous to a connection-based packet-switching scheme.

31) Explain hidden and exposed terminal problems in infrastructure-less network.<u>(May/June 2015)</u>

✓ The hidden terminal analogy is described as follows:

- Terminal A sends data to B, terminal C cannot hear A
- Terminal C wants to send data to B, terminal C senses a "free"' medium (CS fails) and starts transmitting
- Collision at B occurs, A cannot detect this collision (CD fails) and continues with its transmission to B
- Terminal A is "hidden" from C and vice versa.

✓ The exposed terminal analogy is described as follows:

- B sends to A, C wants to send to another terminal D not A or B
- C senses the carrier and detects that the carrier is busy.
- C postpones its transmission until it detects the medium as being idle again
- But A is outside radio range of C, waiting is not necessary
- C is “exposed" to B

32) What are the limitations of Mobile Computing? (Nov/Dec 2016)

- ✓ Insufficient bandwidth
- ✓ Security standards
- ✓ Power consumption
- ✓ Transmission interferences
- ✓ Potential health hazards
- ✓ Human interface with device

33) What are the different Random Assignment Scheme in MAC? (Nov/Dec 2016)

i) ALOHA

ii) Slotted ALOHA

iii) CSMA

iv) CSMA/CD

v) CSMA/CA

16 Marks

1) What Is Mobile Computing?(4 marks)

Mobile computing **(sometimes called ubiquitous computing and also at times called nomadic computing)** is widely described as the ability to compute remotely while on the move. This is a new and fast emerging discipline that has made it possible for people to access information from anywhere and at anytime.

Mobile computing as encompassing two separate and distinct concepts:

- Mobility and Computing.

Computing denotes the capability to automatically carry out certain processing related to service invocations on a remote computer.

Mobility, on the other hand, provides the capability to change location while communicating to invoke computing services at some remote computers.

The main advantage of this type of mobile computing is :

- The tremendous flexibility it provides to the users.
- The user need not be tethered to the chair in front of his desktop, but can move locally or even to far away places and at the same time achieve what used to be performed while sitting in front of a desktop.

2) Compare Mobile Computing vs. Wireless Networking

Distinguish Between Mobile Computing And Wireless Networking:

- ✓ While **mobile computing** essentially denotes accessing information and remote computational services while on the move
- ✓ **wireless networking** provides the basic communication infrastructure necessary to make this possible.
- ✓ That **mobile computing is based on wireless networking** and helps one to invoke computing services on remote servers while on the move: be it be office, home, conference, hotel, and so on.
- ✓ It should be clear **that wireless networking is an important ingredient of mobile computing,** but forms only one of the necessary ingredients of mobile computing.
- ✓ Mobile computing also requires the applications themselves— their design and development, and the hardware at the client and server sides.
- ✓ Wireless networking is increasingly replacing traditional networks because of the low setup time and low initial investment required to set up the wireless network.

WIRELESS NETWORKS

Wireless networks appear in various forms such as

- WLANs (Wireless LANs),
- Mobile Cellular Networks,
- Personal Area Networks (Pans),
- And Ad Hoc Networks, etc.

Wireless networks can be **classified into two basic types.**

1. One is an extension of **wired networks**. It uses **fixed infrastructures** such as

   ✓ Base stations to provide essentially single hop wireless communication with a wired network as illustrated in Fig. 2.1 A two-hop **wireless cellular communication** with another mobile.

2. The **other type** of wireless network is an **ad hoc network**. An ad hoc network does not use any fixed infrastructure and is based on multi-hop wireless communication as shown in Fig. 2.2.

✓ **One popular example of a fixed infrastructure wireless network is a Wireless LAN** (WLAN) that implements the IEEE 802.11 protocol.

Access Point:

✓ Observe from Fig. 2.1 that only the last **hop**(data packets pass quickly from one place to another) is through the wireless medium.

✓ **An access point (AP)** provides the last hop connectivity of the mobile nodes to a wired network.

✓ All communication goes through APs which perform bridging between the wireless and the wired mediums. A station must be recognized by an AP to be able to connect to the network.

✓ The AP may require authentication and this in turn is used as the basic means to keep out the unauthorized users.

✓ In an infrastructureless network, the communication between hosts occurs directly or via a few intermediate nodes that form the hops.

For example, station A in **Fig. 2.2** can communicate with station C using either the hops A–B, B– C or A–D, D–C. * A network bridge connects multiple network segments at the data link layer (Layer 2) of the OSI reference model.

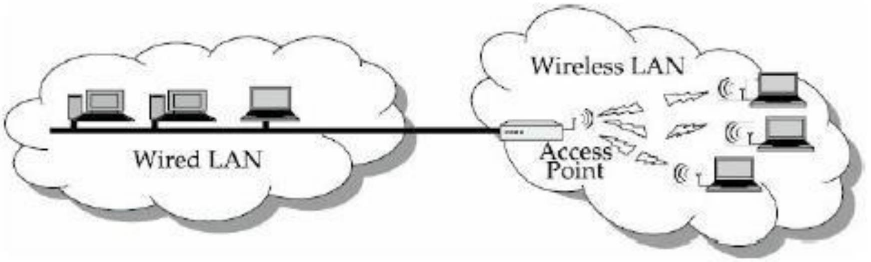


Figure 2.1 Wireless network based on fixed infrastructures.

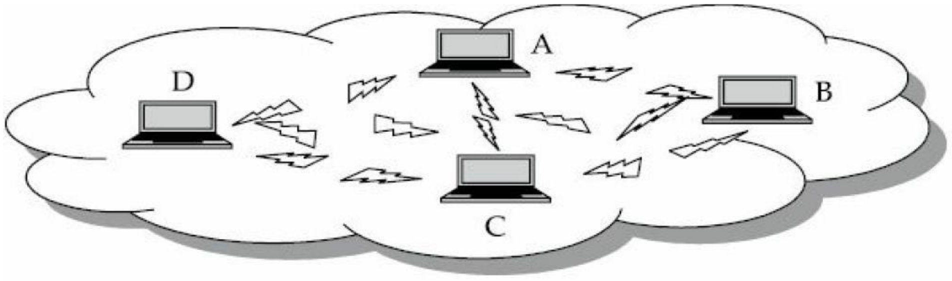


Figure 2.2 *Wireless network having no fixed infrastructures.*

Recent Development

Bluetooth

A recent development wireless networking of various types of devices using the **Bluetooth technology**

- ✓ A **Bluetooth** device uses radio waves instead of wires or cables to connect to a phone or computer.
- ✓ The Bluetooth technology can also be used to establish direct wireless connection of cell phones with devices such as printers, cameras, scanners, laptop and desk computers.
- ✓ Bluetooth is gradually replacing cables and infrared as the dominant way of exchanging information between devices.
- ✓ One of the objectives of the Bluetooth technology is to enable users to easily connect to a wide range of personal computing and telecommunication devices, without the need to buy, carry, or lay out cables.
- ✓ In fact, the Bluetooth technology enables setting up of personal area networks (PANs) known as **piconets** and ad hoc networks known as **scatternets**. It provides opportunities for rapid deployment of ad hoc connections, and the possibility of automatic, transparent connections between devices. It promises to eliminate the need to purchase additional or proprietary cabling and configuration exercises needed to connect the individual devices.

Ad Hoc Network

- ✓ An ad hoc network is also known as a **Mobile Ad hoc Network(MANET)**. It is a collection of mobile nodes that form a network on the fly without requiring the support of any fixed infrastructure.
- ✓ Wireless sensor networks are a special type of wireless ad hoc networks.

3) Explain in detail of Mobile Computing Applications? (4 marks) Nov/Dec 2016

Mobile Computing Applications

✓ Mobile computing technology makes **it possible for people to send or extract information while on the move.**

For example, a stock broker travelling in a car may wish to issue stock transaction orders from a mobile phone or to receive share price quotations.

- Emergency services
- Stock information
- Credit card verification
- Electronic mail paging
- Vehicles- transmission of news,road condition
- Entertainment – Games

Positive Points

It ease of deployment and scalability are two important positive points in favour of data transmissions over the wireless medium.

Difficult

But When data is being transmitted on air, all the wireless devices present in the transmission range can receive the data. This, therefore, opens up very difficult security issues that must be overcome to ensure privacy of data.

4) Detail about Characteristics of Mobile Computing? (May/June 2015)

Characteristics of Mobile Computing

✓ A **computing environment** is said to be **"mobile",** when either the sender or the receiver of information can be on the move while transmitting or receiving information.

✓ The following are some of the important characteristics of a mobile computing environment.
Ubiquity: The dictionary **meaning of ubiquity is present everywhere**. In the context of mobile computing, ubiquity means the ability of a user to perform computations from anywhere and at anytime.

For example, a business executive can receive business notifications and issue business transactions as long he is in the wireless coverage area.

Location awareness: A hand-held device equipped with global positioning system (GPS) can transparently provide information about the current location of a user to a tracking station. Many applications, ranging from strategic to personalized services, require or get value additions by location-based services

For example, a person travelling by road in a car, may need to find out a car maintenance service that may be available nearby. He can easily locate such a service through mobile computing where an application may show the nearby maintenance shop.

A few other example applications include traffic control, fleet management and emergency services.

1. In a traffic control application, the density of traffic along various roads can be dynamically monitored, and traffic can be directed appropriately to reduce congestions.
2. In a fleet management application, the manager of a transport company can have up-to-date information regarding the position of its fleet of vehicles, thus enabling him to plan accurately and provide accurate information to customers regarding the state of their consignments.
3. Location awareness can also make emergency services more effective by automatically directing the emergency service vehicles to the site of the call.

Adaptation: Adaptation in the context of mobile computing implies the ability of a system to adjust to bandwidth fluctuation without inconveniencing the user. In a mobile computing environment, adaptation is crucial because of intermittent disconnections and bandwidth fluctuations that can arise due to a number of factors such as handoff, obstacles, environmental noise, etc.

Broadcast: Due to the broadcast nature of the underlying communication network of a mobile computing environment, efficient delivery of data can be made simultaneously to hundreds of mobile users.

For example, all users at a specific location, such as those near a railway station, may be sent advertising information by a taxi service operator.

Personalization: Services in a mobile environment can be easily personalized according to a user's profile. This is required to let the users easily avail information with their hand-held devices.

For example, a mobile user may need only a certain type of information from specific sources. This can be easily done through personalization.

5) Explain in detail of Structure of Mobile Computing Application? (May/June 2015)

Structure of Mobile Computing Application

A mobile computing application is usually structured in terms of the functionalities implemented.

- ✓ The simple three-tier structure of a mobile computing application is depicted in Fig. 2.3.
- ✓ Figure 2.4 shows a specific scenario of the types of functionalities provided by each tier.
- ✓ As shown in these figures, the three tiers are named presentation tier, application tier and data tier.
- ✓ We now briefly explain the roles of the three tiers of a mobile computing application.

1. Presentation (Tier-1)
2. Application (Tier-2)
3. Data (Tier-3)

Figure 2.3 The three tier structure of a mobile computing application.

Presentation tier

- ✓ The topmost level of a mobile computing application concerns the user interface. A good user interface facilitates the users to issue requests and to present the results to the them meaningfully.
- ✓ Obviously, the programs at this layer run on the client's computer. This layer usually includes web browsers and customized client programs for dissemination of information and for collection of data from the user.

Application tier

- ✓ This layer has the vital responsibility of making logical decisions and performing calculations. It also moves and processes data between the presentation and data layers.
- ✓ We can consider the middle tier to be like an "engine" of an automobile. It performs the processing of user input, obtaining information and then making decisions.
- ✓ This layer is implemented using technology like Java, .NET services, cold fusion, etc.
- ✓ The implementation of this layer and the functionality provided by this layer should be database independent.
- ✓ This layer of functionalities is usually implemented on a fixed server.

Data tier

- ✓ The data tier is responsible for providing the basic facilities of data storage, access, and manipulation. Often this layer contains a database. The information is stored and retrieved from this database.
- ✓ But, when only small amounts of data need to be stored, a file system can be used.
- ✓ This layer is also implemented on a fixed server.

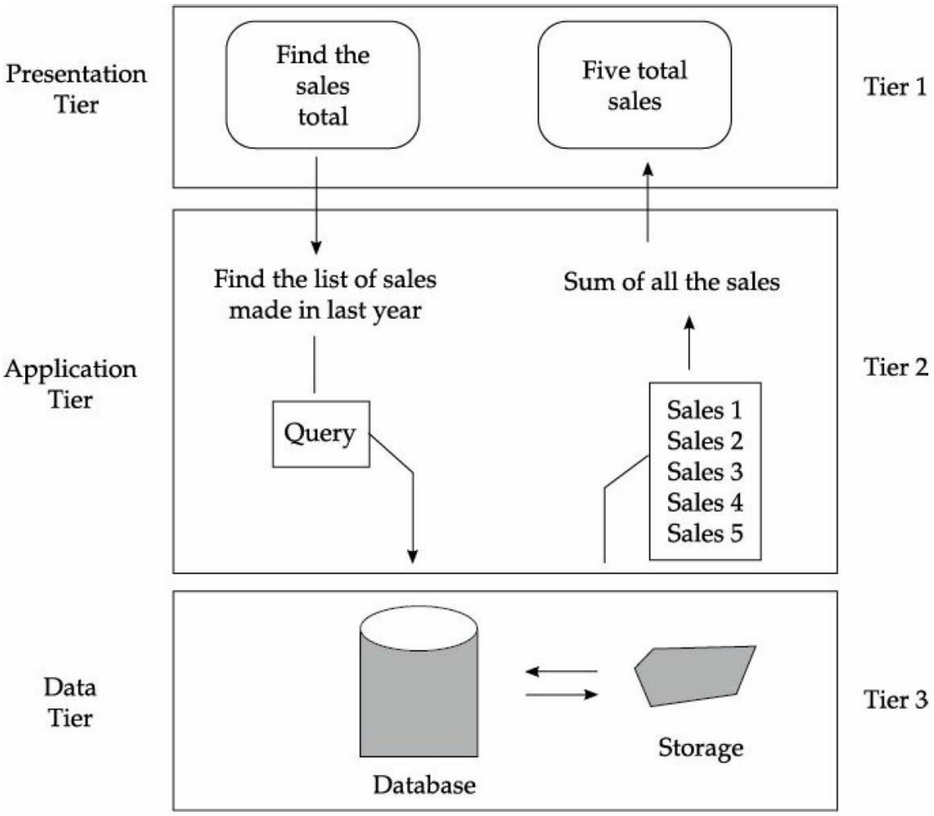


Figure 2.4 Functionalities provided by each tier structure of a mobile computing application.

6) Explain in detail about MAC Protocols and its properties?

<u>MAC Protocols</u>

In a wireless network, multiple nodes may contend to transmit on the same shared channel at the same time. In this situation, the transmitted data would get garbled(சிேறுண்டு) unless a suitable medium access arbitration scheme is deployed.

- ✓ Usually, it is the responsibility of the **medium access control (MAC)** protocol to **perform this task.**
- ✓ The MAC protocol is a sublayer of the data link layer protocol and it directly invokes the physical layer protocol.
- ✓ The primary responsibility of a MAC protocol is to enforce discipline in the access of a shared channel when multiple nodes contend to access that channel. At the same time, two other objectives of any MAC protocol are maximization of the utilization of the channel and minimization of average latency of transmission. However, a MAC protocol must be fair and ensure that no node has to wait for an unduly long time, before it is allowed to transmit.

Properties Required of MAC Protocols

✓ In a general sense a good MAC protocol needs to possess the following features
:

- It should implement some rules that help to enforce discipline when multiple nodes contend for a shared channel.
- It should help maximize the utilization of the channel.
- Channel allocation needs to be fair. No node should be discriminated against at any time and made to wait for an unduly long time for transmission.
- It should be capable of supporting several types of traffic having different maximum and average bit rates.
- It should be robust in the face of equipment failures and changing network conditions.

7) Write in detail of Wireless MAC Protocols: Some Issues

Wireless MAC Protocols: Some Issues

✓ A MAC protocol in a wireless medium is much more complex than its wired counterpart.
✓ First, a collision(தமாே◌ல்) detection scheme is difficult to implement in a wireless environment, since collisions are hard to be detected by the transmitting nodes.
✓ Also, in infrastructure-less networks, the issue of hidden and exposed(வைளிப்படும்) terminals make a MAC protocol extremely inefficient unless special care is taken to overcome these problems.

The Hidden and Exposed Terminal Problems in an Infrastructure-less Network

- The **Hidden Terminal problem arises** when at least three nodes (A, B, and C), as shown in Fig. 3.1, communicate among each other.

✓ As shown in this figure, B is in the radio range of A, and B is also within the radio range of C. However, the nodes A and C are not in the radio range of each other.
✓ **Note** that if both A and C start to transmit to B at the same time, the data received at node B would get garbled.
✓ Such a situation can arise because A and C are "hidden" from each other, because they are outside each other's transmission range. In this situation, when one node starts to sense the medium before transmission, it cannot sense that the other node is also transmitting. This creates a very difficult and important arbitration problem that a MAC protocol needs to resolve.

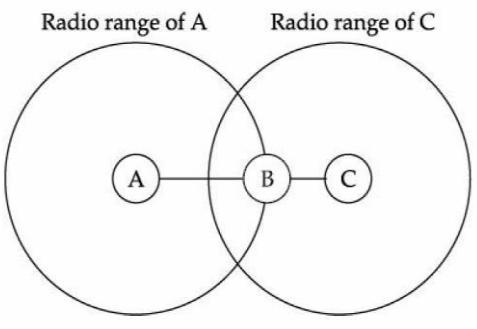


Figure 3.1 Hidden terminal problem.

- A related **problem called <u>Exposed Terminal</u>** could arise in a scenario such as that depicted in Fig. 3.2.

✓ MAC protocols usually inhibit(ே◌டுக்கும்) transmission when transmission from another terminal is detected.

✓ As a result, node A will not be able to transmit to any node when B is transmitting to C.

✓ On the other hand, had A transmitted to D, it would have been received correctly by D and B’s transmission would have also been correctly received at C.

✓ The problem arose only because A and B are within each other’s transmission range, though the destination nodes are in the transmission range of only one of the nodes.

✓ In other words, the problem occurs because A is exposed to B’s transmission.

The overall effect of **this problem is** that it leads to **inefficient spectrum usage** as well as **unnecessary transmission delays** unless these are carefully **addressed by a wireless MAC protocol**.

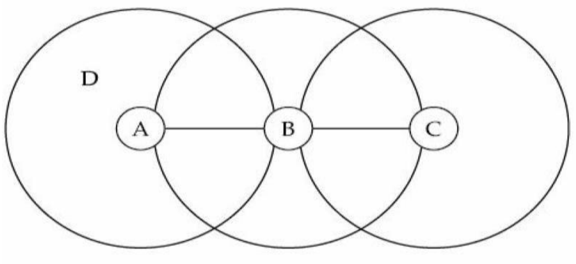


Figure 3.2 Exposed terminal problem.

8) Explain about A Taxonomy of MAC Protocols ?(May/June 2015) (Nov/Dec 2016)

<u>A Taxonomy of MAC Protocols</u>

A large number of MAC protocols have been proposed. These MAC protocols can be broadly divided into the following three categories:

(i) Fixed assignment schemes- are usually **called circuit-switched schemes**
(ii) Random assignment schemes
(iii) Reservation-based schemes are **called packet-switched schemes**

i. **In fixed assignment schemes**, the resources required for a call are assigned for the entire duration of the call.

ii. **In random assignment schemes** are comparable to the connection-less packet-switching schemes. In this, no resource reservations are made, the nodes simply start to transmit as soon as they have a packet to send.

iii. **In the reservation schemes**, a node makes explicit reservation of the channel for an entire call before transmitting. This is analogous to a connection-based packet-switching scheme.

The reservation-based MAC schemes are suitable to handle calls with widely varying traffic characteristics.

I) Fixed Assignment Schemes

A few important categories of fixed assignment MAC protocols are the following:

1. Frequency Division Multiple Access (FDMA)
2. Time Division Multiple Access (TDMA)
3. Code Division Multiple Access (CDMA)

We briefly discuss these techniques in the following subsections.

BOX 3.1 An analogy to the fixed assignment solution to the multiple access issues of a shared medium

An analogy may be drawn to the fixed assignment solution to the multiple access issues of a shared medium in the following way: Consider a students' common room (channel) in which many students want to communicate with each other. If the students want to avoid cross-talk in the ongoing process, then either the students could take turns in speaking (i.e. time division), or they could speak at different pitches (i.e. frequency division), or they could speak in different languages (i.e. code division). The last analogy captures the essence of CDMA, when the students who are speaking the same language understand each other, but the rest of the students cannot. In CDMA, each communicating pair shares a decryption code using which lets them understand only the communication between them. In this case many codes occupy the same channel, but only the users who share a specific code will be able to understand each other.

1) Frequency Division Multiple Access (FDMA)

- ✓ In FDMA, the available bandwidth (frequency range) is divided into many narrower frequency bands called channels. Figure 3.3 shows a division of the existing bandwidth into many channels (showns as Ch 1, Ch 2, etc.).

- ✓ For full duplex communication to take place, each user is allocated a forward link (channel) for communicating from it (mobile handset) to the base station (BS), and a reverse channel for communicating from the BS to it. Thus, each user making a call is allocated two unique frequency bands (channels), one for transmitting and the other for receiving signals during the call. Obviously, when a call is underway, no other user would be allocated the same frequency band to make a call. Unused transmission time in a frequency band that occurs when the allocated caller pauses between transmissions, or when no user is allocated a band, goes idle and is wasted. FDMA, therefore, does not achieve a high channel utilization.

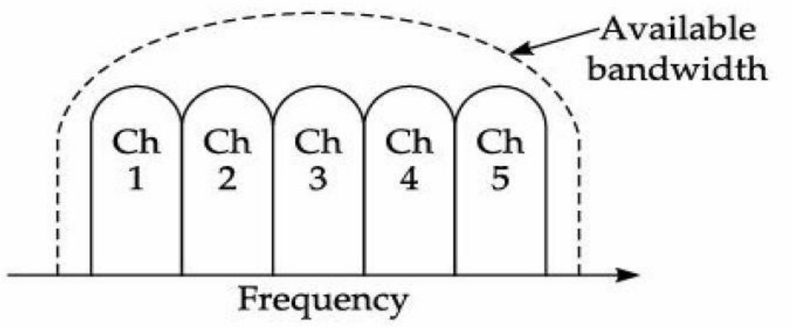


Figure3.3 Channels in Frequency Division Multiple Access (FDMA) scheme.

2) **Time Division Multiple Access (TDMA)**

- ✓ TDMA is an access method in which multiple nodes are allotted different time slots to access the same physical channel. That is, the timeline is divided into fixed-sized time slots and these are divided among multiple nodes who can transmit.
- ✓ Note that in this case, all sources use the same channel, but take turns in transmitting. Figure 3.4 shows the situation where time slots are allocated to users in a round robin manner, with each user being assigned one time slot per frame. See Box 3.2. Obviously, unused time slots go idle, leading to low channel utilization.

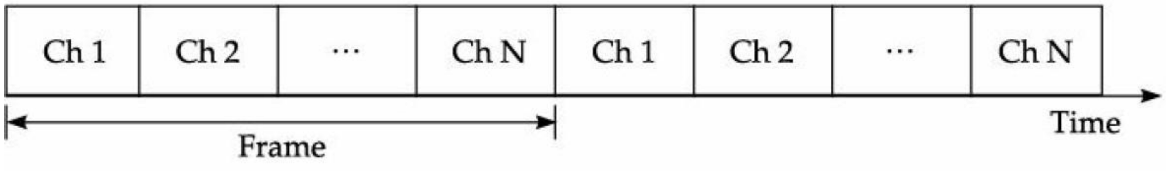


Figure 3.4 Channels in Time Division Multiple Access (TDMA) scheme.

BOX 3.2 TDMA scheme
In TDMA, each user of the channel owns the channel for exclusive use for one time slot at a time in a round robin fashion.

3) **Code Division Multiple Access (CDMA)**

- ✓ In CDMA, multiple users are allotted different codes that consist of sequences of 0 and 1 to access the same channel. As shown in Fig. 3.5, a special coding scheme is used that allows signals from multiple users to be multiplexed over the same physical channel. As shown in the figure, three different users who have been assigned separate codes are multiplexed on the same physical channel.

✓ In the following, we elaborate the CDMA technology. In CDMA, multiple users use the same frequency at the same time and no time scheduling is applied. All the senders send signals simultaneously through a common medium. The bandwidth of this medium is much larger than the space that would be allocated to each packet transmission during FDMA and the signals can be distinguished from each other by means of a special coding scheme that is used. This is done with the help of a frequency spreading code known as the *m*-bit pseudo-noise (PN) code sequence.

BOX 3.3 How to distinguish transmission from different nodes

Two vectors are said to be orthogonal if their inner product = 0. Let **p** and **q** be two vectors and suppose **p** = (2, 5, 0) and **q** = (0, 0, 17), then the inner

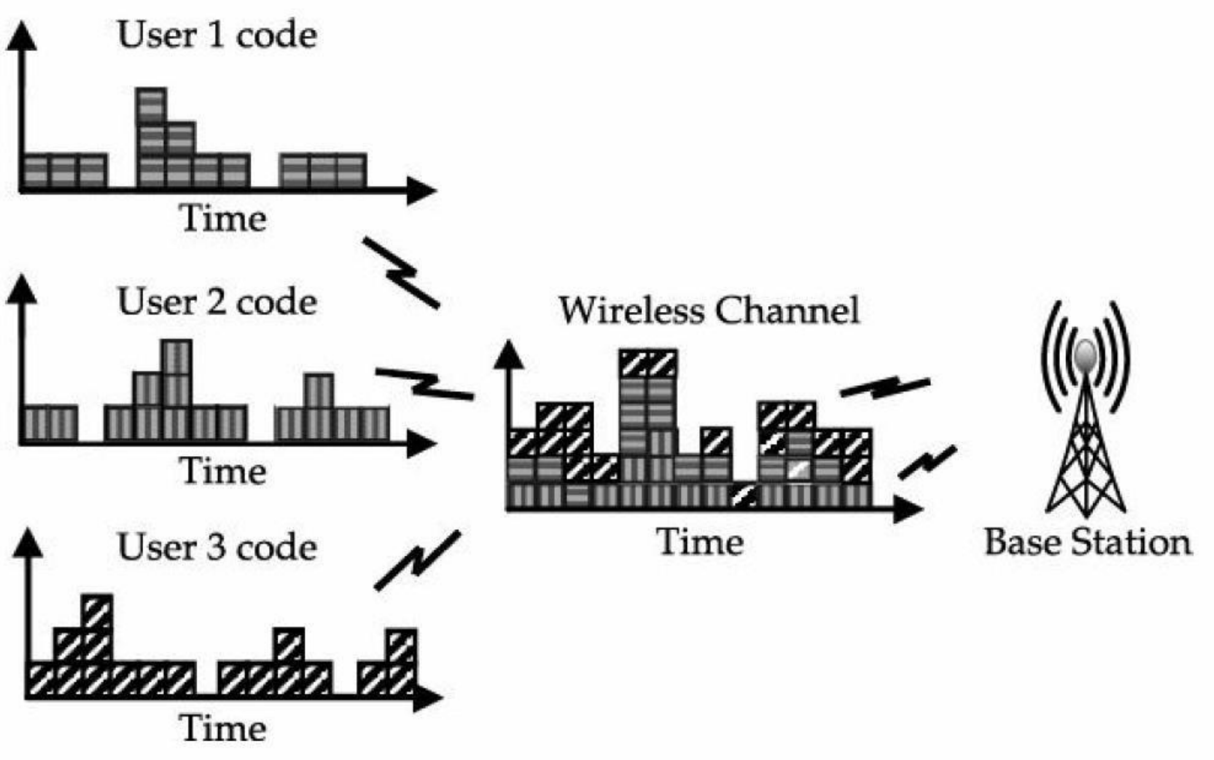


Figure 3.5 *Schematic of operation of Code Division Multiple Access (CDMA).*

✓ Using *m* bits, 2*m* – 1 different codes can be obtained. From these codes, each user will use only one code.

✓ It is possible to distinguish transmissions from different nodes by ensuring some properties on the codes.

✓ A code for a user should be orthogonal (that is, non-interfering) to the codes assigned to other nodes. **The term “orthogonal” means that the vector inner product is zero**, and good autocorrelation (இரண்டு (அ) அேற்கு தமற்பட்ட வபாருள்களுக்கு வோடர்பு ஏற்படுத்ே◌ல்) uses the bipolar notation where a code sequence of binary 0 is represented as –1 and binary 1 is represented as +1.

✓ **See Box 3.3.** On the receiving end, only the same PN sequence is able to demodulate the signal to successfully convert the input data.

BOX 3.4 Pseudorandom sequence generator

To generate a series of pseudorandom numbers, a seed (or starting point) is required. Based on the selected seed, the next number can be generated using a deterministic mathematical transformation or can be generated probabilistically. In CDMA, a code actually denotes a starting point (seed) for a pseudorandom sequence generator (PRSG). PRSG generates a series of bits at a frequency which is much higher than the actual user data (such as digitized voice). These bits are XORd with the user data and subsequently the results are transmitted. This occurs in the case of multiple transmitters.

If someone listens to this signal with the help of a suitable wideband receiver, the person will hear something similar to what is produced by random noise. All the other users who are on the same frequency will send a similar signal, but with a different PRSG seed. So these apparent random noises will all coexist in the same band of frequencies, but would not interfere with each other. This is due to the reason that the exact frequency of any transmitter at any instant (which is in effect determined by the seed) is almost always unique. Error correction takes care of occasional bit errors.

The receiver is aware of the PRSG starting point for each transmitter. It hears just one of the transmitters by correlating the noise it receives, against its own PRSG, which is also running with the same seed. It is slightly similar to FDMA in this sense, but the difference is that the transmitters do not stay on one frequency. They hop around many times per bit of user data. The pseudorandom sequence determines this hopping, rather than a fixed assignment to each transmitter.

For simplicity, we assume

1. that all nodes transmit on the same frequency at the same time using the entire bandwidth of the transmission channel.
2. Each sender has a unique random number key, and the sender XORs the signal with this random number key.
3. The receiver can “tune” into this signal if it knows the pseudorandom number.

4. **Consider an example**,
   a. where X, Y are the transmitters and Z is a receiver.

   b. Sender X_data = 1 and X_Key = (010011). Its autocorrelation representation is (–1, +1, –1, –, +1, +1). The signal to be calculated at sender X is Xs = X_data □ X_key = +1□X_key = (–1, +1, –1, –1, +1, +1). Similarly, sender Y_data = 0 and Y_key = (110101) and the signal to be sent at Y is Ys = –1□Y_key = –1 (□+1, +1, –1, +1, –1, +1) = (–1, –1, +1, –1, +1, –1).

   c. The signal received by receiver Z is Xs + Ys = (–1, +1, –1, –1, +1, +1) + (–1, –1, +1, –1, +1, –1) = (–2, 0, 0, –2, +2, 0). At the receiver, in order to receive the data sent by sender X, the signal Z is dispread.

   d. So now if Z wants to get information of sender X data, then Z □X_key = (–2, 0, 0, –2, +2, 0) (□–1, +1, –1, –1, +1, +1) = 2 + 0 + 0 + 2 + 2 + 0 = 6 > 0 (positive), that is the original bit was a 1. Similarly, the information of sender Y data may be obtained as Z □Y_key = (–2, 0, 0, –2, +2, 0) □(+

1, +1, –1, +1, –1, +1) = –2 + 0 + 0 – 2 – 2 + 0 = – 6 < 0 (negative). So the Y data original bit was a 0.

II) **Random Assignment Schemes**

There are a number of random assignment schemes that are used in MAC protocols. A few importantones are the following:

vi) ALOHA
vii) Slotted ALOHA
viii) CSMA
ix) CSMA/CD
x) CSMA/CA

i) **ALOHA Scheme**

✓ It is a simple communication scheme, the basic (also called pure) ALOHA scheme, is a simple protocol. If a node has data to send, it begins to transmit.

✓ **Note that the first step implies** that Pure ALOHA does not check whether the channel is busy before transmitting.

- If the frame successfully reaches the destination (receiver), the next frame is sent.
- If the frame fails to be received at the destination, it is sent again.

✓ **The simple ALOHA scheme works acceptably**,

- when the chances of contention are small (i.e., when a small number of senders send data infrequently).
- However, the collisions can become **unacceptably** high if the number of contenders for transmission is high.

✓ An **improvement** over the pure **ALOHA scheme is the slotted ALOHA.**

- In the slotted ALOHA scheme, the chances of collisions are attempted to be reduced by enforcing the following restrictions.
- The time is divided into equal-sized slots in which a packet can be sent.
- Thus, the size of the packet is restricted. A node wanting to send a packet, can start to do so only at the beginning of a slot.
- The slotted ALOHA system employs beacon(எச்சரிக்கும்) signals that are sent at precise intervals that mark the beginning of a slot, at which point the nodes having data to send can start to transmit.

- Again, this protocol does not work very well if the number of stations contending to send data is high. **In such cases, the CSMA scheme (described next) works better.**

ii) <u>The CSMA Scheme</u>

✓ A popular MAC arbitration technique is the Carrier Sense Multiple Access (CSMA).
✓ In this technique, a node senses the medium before starting to transmit.
✓ If it senses that some transmission is already underway, it defers its transmission.

Two popular extensions of the basic CSMA technique are

- The collision detection (csma/cd)
- And the collision avoidance (CSMA/CA) techniques.

Unlike that in a wired network, in a wireless network the CSMA/CD technique does not work very well.

- In the CSMA/CD technique, the sender starts to transmit if it senses the channel to be free. But, even if it senses the channel to be free, there can be a collision (why?) during transmission.
- In a **wired network**, the implementation of a **collision detection scheme is simple**.
- However, in a **wireless network** it is very **difficult** for a transmitting node to **detect a collision**, since any received signal from other nodes would be too feeble compared to its own signal and can easily be masked by noise.
- As a result, a transmitting node would continue to transmit the frame, and only the destination node would notice the corrupted frame after it computes the checksum. This leads to retransmissions and severe wastage of channel utilization.
- **In contrast**, in a **wired network when a node detects a collision**, it immediately stops transmitting, thereby minimizing channel wastage.
- **In a wireless network, a collision avoidance scheme works much better** compared to a collision detection-based scheme.
- A collision avoidance scheme is based on the idea that it is necessary to prevent collisions at the moment they are most likely to occur, that is, when the bus is released after a packet transmission.

✓ **We explain the reason for this in the following.**

During the time a node is transmitting on the channel, several nodes might be wanting to transmit. These nodes would be monitoring the channel and waiting for it to become free. The moment the transmitting node completes its transmission, these waiting nodes would sense the channel to be free, and would all start transmitting at the same time.

To overcome such collisions, in the collision avoidance scheme, all nodes are forced to wait for a random time and then sense the medium again, before starting their transmission. If the medium is sensed to be busy, a node waiting to transmit waits for a further random amount of time and so on. Thus, the chance of two nodes starting to transmit at the same time would be greatly reduced.

III) <u>Reservation-based Schemes</u>

- ✓ A basic form of the reservation scheme is the RTS/CTS scheme.
- ✓ In an RTS/CTS scheme, a sender transmits an RTS (Ready to Send) packet to the receiver before the actual data transmission. On receiving this, the receiver sends a CTS (Clear to Send) packet, and the actual data transfer commences only after that.
- ✓ When the other nodes sharing the medium sense the CTS packet, they refrain from transmitting until the transmission from the sending node is complete.
- ✓ In a contention-based MAC protocol, a node wanting to send a message first reserves the medium by using an appropriate control message.

For example, reservation of the medium can be achieved by transmitting a “Ready To Send” (RTS) message and the corresponding destination node accepting this request answers with a “Clear To Send” (CTS) message. Every node that hears the RTS and CTS messages defers its transmission during the specified time period in order to avoid a collision.

A few examples of RTS-CTS based MAC protocols are MACA, MACAW, MACA-BI, PAMAS, DBTMA, MARCH, S-MAC protocols which have specifically been designed for sensor networks. In the following, we discuss MACA as a representative protocol belonging to this category of protocols.

MACA:

MACA stands for Multiple Access Collision Avoidance. MACA solves the hidden/exposed terminal problems by regulating the transmitter power. A node running MACA requests to use the medium by sending an RTS to the receiver. Since radio signals propagate omni-directionally(ைட்டத்ேிவச), every terminal within the sender’s radio range will hear this and then refrain from transmitting. As soon as the receiver is ready to receive data, it responds with a CTS.

Figure 3.6 schematically shows how MACA avoids the hidden terminal problem. Before the start of its transmission, it sends a Request To Send (RTS). B receives the RTS that contains the sender’s name and the receiver’s name, as well as the length of the future transmission**.** In response to the RTS, an acknowledgment from B is triggered indicating Clear To Send (CTS). The CTS contains the names of the sender and receiver, and the length of the planned transmission. This CTS is heard by C and the medium is reserved for use by A for the duration of the transmission.

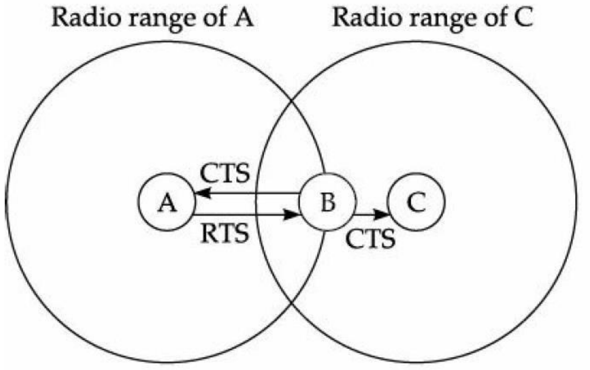


Figure 3.6 Hidden terminal solution in MACA.

On receipt of a CTS from B, C refrains from transmitting anything for the time indicated in the CTS. Thus a collision cannot occur at B during data transmission, and the hidden terminal problem is solved.

Though this is a collision avoidance protocol, a collision can occur during the sending of an RTS.Both A and C could send an RTS at same time. But an RTS occurs over a very small duration compared to the duration of data transmission. Thus the probability of collision remains much less. B resolves this contention problem by acknowledging only one station in the CTS. No transmission occurs without an appropriate CTS.

Figure 3.7 schematically shows how the exposed terminal problem is solved in MACA. Assume that
B needs to transmit to A. B has to transmit an RTS first as shown in Fig. 3.7. The RTS would contain
the names of the receiver (A) and the sender (B). C does not act in response to this message as it is not the receiver, but A responds with a CTS. C does not receive this CTS and concludes that A is outside the detection range. Thus C can start its transmission assuming that no collision would occur at A.

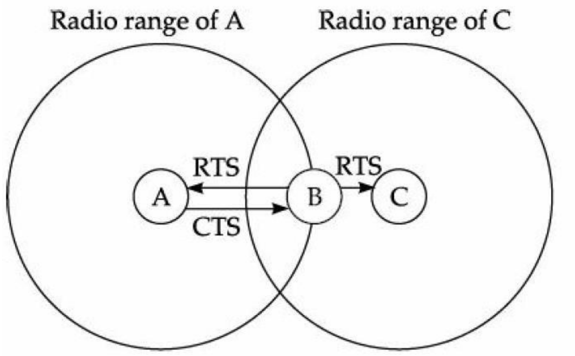


Figure 3.7 Exposed terminal solution in MACA.

Anna University Questions

May/June 2015

Part A

1. List the advantages of mobile computing. **[page:2 ,Q.no:4]**
2. Explain hidden and exposed terminal problems in infrastructure-less network. **[page:7 ,Q.no:31]**

Nov/Dec 2016

3. What are the limitations of Mobile Computing? **[page:8 ,Q.no:32]**
4. What are the different Random Assignment Scheme in MAC? **[page:8 ,Q.no:33]**

Part B

11.(a) (i)Explain the characteristics of Mobile computing. (8) **[page:12 ,Q.no:4]**

(ii)Explain the structure of Mobile Computing Application. (8) **[page:14 ,Q.no:5]**

OR

(b) Explain the various taxonomy of MAC protocols in detail. (16) **[page:17 ,Q.no:8]**

Nov/Dec 2016

11. (a) Differentiate between FDMA,TDMAand CDMA(16) **[page:16 ,Q.no:8]**

OR

(b) i) Explain the Distinguishng features of various generations of wireless networks? (8) **[Unit III page:17 ,Q.no:4]**

ii) Describe the applications of mobile computing?(8) **[page:12 ,Q.no:3]**

UNIT II
MOBILE INTERNET PROTOCOL AND TRANSPORT LAYER

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.

PART - A

1. Define Tunnelling with its functions?

- The packet is forwarded by the home agent to the foreign agent. When the packet comes to the foreign agent (care-of-address), it delivers the packet to the mobile node. This process is called ***tunnelling.***

- Tunnelling has two primary functions:
    1. Encapsulation of the data packet to reach the tunnel endpoint,
    2. Decapsulation when the packet is delivered at that endpoint.

2. Define Care-Of-Address (COA) with its types? (Nov/Dec 2016)

- ***Care-of-Address (COA):*** It is the address that is used to identify the present location of a foreign agent. The packets sent to the MN are delivered to COA.

- The COA can be any of the following two types:

  (a) ***Foreign agent COA:*** The COA is an IP address of foreign agent (FA).
  (b) ***Co-located COA:*** When the mobile node (MN) acquires a temporary IP address, that address acts as the COA.

3. Define Agent Discovery and its discovery methods?

- ***Agent Discovery:*** During call establishment it is necessary for a mobile node to determine its foreign agent. This task is referred to as ***agent discovery.***

- The following two discovery methods are popularly used:
  (1) Agent advertisement, and

  (2) Agent solicitation.

4. Describe some of the features of Mobile IP

- ***Transparency:*** The IP address is to be managed transparently and there should not be any effect of mobility on any ongoing communication.

- ***Compatibility:*** Mobile IP should be compatible with the existing Internet protocols.

- ***Security:*** Mobile IP should, as far as possible, provide users with secure communications over the Internet.

- ***Efficiency and Scalability:*** In the event of worldwide support, there can be a large number of mobile systems in the whole Internet. It should also be scalable to support billions of moving hosts worldwide.

5. What are the key mechanisms followed by Mobile IP?

- Mobile IP is associated with the following three basic mechanisms:
    1. Discovering the care-of-address
    2. Registering the care-of-address
    3. Tunnelling to the care-of-address

6. Define DHCP? (May/June 2016)

- DHCP was developed based on bootstrap protocol (BOOTP). DHCP provides several types of information to a user including its IP address. To manage dynamic configuration information and dynamic IP addresses, IETF standardized an extension to BOOTP known as dynamic host configuration protocol (DHCP).

- The DHCP client and server work together to handle the roaming status and to assign IP address on a new network efficiently. The DHCP server allocates an IP address from a pool of IP addresses to a client.

7. What Are The Common TCP/IP Application Protocols?

- DHCP - dynamic host configuration protocol
- DNS - Domain Name System
- FTP – File Transfer Protocol
- HTTP – HyperText Transfer Protocol
- IMAP – Internet Message Access Protocol
- NFS – Network File System
- NNTP - Network News Transfer Protocol
- NTP - Network Time Protocol
- POP – Post Office Protocols
- SMTP – Simple Mail Transfer Protocol
- SNMP - Simple Network Management Protocol

8. What is TCP?

- On the sending side, TCP is responsible for breaking a message into small parts, adding sequence numbers and certain other information and after this, making them known as segments. TCP passes the segments to the lower layer protocol for transmission over the network.

- While at the receiver's end, TCP assembles the segments when they arrive and reconstructs the message. TCP is a reliable protocol. Whenever a packet is lost or corrupted during transmission, TCP detects it and requests the sender for retransmission. Thus, retransmission is used as the primary mechanism by TCP for reliable data delivery to the destination.

9. What is IP?

- ***IP** (Internet Protocol):* At the host machine of an application sending a message, IP is responsible for constructing packets (also called datagrams) from the segments it receives from the transport layer protocol by adding the destination host address and then passes these on to the lower layer protocol for transmitting. On the receiver's side, it deconstructs the segments and then passes these to the transport layer protocol.

10. What is IPv6?

IP Version 6 (**IPv6**) is the newest version of IP, sometimes called **IPng** for "IP, Next Generation". IPv6 is fairly well defined but is not yet widely deployed.

The main differences between IPv6 and the current widely-deployed version of IP (which is IPv4) are:

- IPv6 uses larger addresses (128 bits instead of 32 bits in IPv4) and so can support many more devices on the network, and
- IPv6 includes features like authentication and multicasting that had been bolted on to IPv4 in a piecemeal fashion over the years.

11. What is IPsec?

- Internet Protocol Security (**IPsec**) is a protocol suite for secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.

12. Does IP Protect Data On The Network?

- IP itself does not guarantee to deliver data correctly. It leaves all issues of data protection to the transport protocol. Both TCP and UDP have mechanisms that guarantee that the data they deliver to an application is correct.

- IP does try to protect the packet's IP header, the relatively small part of each packet that controls how the packet is moved through the network. It does this by calculating a checksum on the header fields and including that checksum in the transmitted packet.

- The receiver verifies the IP header checksum before processing the packet. Packets whose checksums no longer match have been damaged in some way and are simply discarded.

- The IP checksum is discussed in detail in RFC 1071, which also includes sample code for calculating the checksum. The same checksum algorithm is used by TCP and UDP, although they include the data portion of the packet (not just the header) in their calculations.

13. What is ARP?

- Address Resolution Protocol (**ARP**) is a mechanism that can be used by IP to find the link-layer station address that corresponds to a particular IP address. ARP sends broadcast frames to obtain this information dynamically, so it can only be used on media that support broadcast frames. Most LAN's (including Ethernet, FDDI, and Token Ring) have a broadcast capability and ARP is used when IP is running on those media. ARP is defined in RFC 826.

14. Name two sub layers of data link layer.

- In Data link layer we are having 2 types of sub layers:
  1. **Logical Link Control (LLC)** - Maintains the Link between two computers by establishing Service Access point (SAPs) which are a series of interface points.
  2. **Media Access Control (MAC)** -Use to coordinate the sending of data between computers. If you hear MAC Address of a network card, they are referring to the hardware address of the card (48 bit).

15. What are the difference between TCP and UDP?

TCP	***UDP***
Connection oriented protocol	Connection less protocol
TCP is network friendly	UDP is not network friendly
TCP guarantees in-order delivery reliable data transmission using Retransmission techniques.	Does not pull back in case of congestion to send packets in to an already congested network.

16. Differentiate between TCP/IP and OSI Model?

OSI(Open System Interconnection)	**TCP/IP(Transmission Control Protocol / Internet Protocol)**
1. OSI provides layer functioning and also defines functions of all the layers.	1. TCP/IP model is more based on protocols and protocols are not flexible with other layers.
2. In OSI model the transport layer guarantees the delivery of packets	2. In TCP/IP model the transport layer does not guarantees delivery of packets.
3. Follows horizontal approach	3. Follows vertical approach.
4. OSI model has a separate presentation layer	4. TCP/IP does not have a separate presentation layer
5. OSI is a general model.	5. TCP/IP model cannot be used in any other application.

17. What is the port number of Telnet and DNS?

1. Telnet uses TCP and the port no is 23.
2. DNS uses both TCP and UDP, port no is 53

18. Name any 4 Example of Application layer?

- ***Simple Mail Transfer Protocol (SMTP):*** It provides an ‘electronic mail’ function, that is used for transferring messages between different hosts.
- ***File Transfer Protocol (FTP):*** FTP is mainly used for transferring files from one host to another based on a user command. FTP allows both binary and text file transfers. Each FTP connection opens two TCP connections, one for data transfer and the other for transfer of control commands such as put, get, etc.
- ***TELNET:*** This application layer protocol lets users use a remote log-on facility, using which a user can log-on to a remote system. Both FTP and TELNET make use of the TCP layer. TCP forwards

these data over the network by invoking the IP layer and the IP layer in turn invokes the like layer protocol.

- **Hypertext Transfer Protocol (HTTP)** – To transfers files that make up pages on the World Wide Web.

19. Different Applications of TCP and UDP

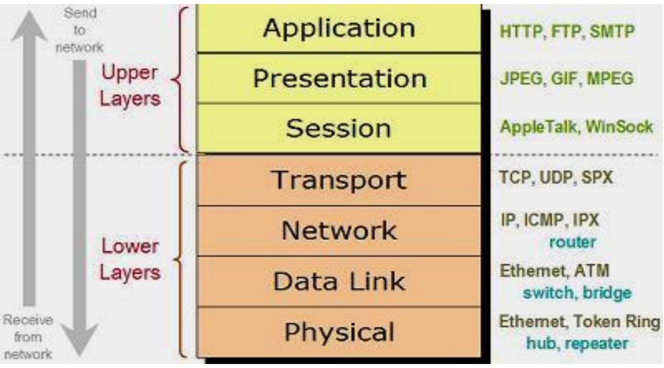
- Web browsing, email and file transfer are common applications that make use of TCP. TCP is used to control segment size, rate of data exchange, flow control and network congestion. TCP is preferred where error correction facilities are required at network interface level. UDP is largely used by time sensitive applications as well as by servers that answer small queries from huge number of clients.
- UDP is compatible with packet broadcast - sending to all on a network and multicasting – sending to all subscribers. UDP is commonly used in Domain Name System, Voice over IP, Trivial File Transfer Protocol and online games.

20. What are the various types of flow control used in congestion avoidance?

Three types of flow control are buffering, windowing & congestion avoidance:

- **Buffering**: If a device receives packets too quickly for it to handle then it can store them in a memory section called a buffer and proceed them later.
- **Windowing**: a window is the quantity of data segments that the transmitting device is allowed to send without receiving an acknowledgment for them.
- **Congestion avoidance**: lower-priority traffic can be discarded when the network is overloaded → minimize delays.

21. Draw the Architecture of OSI Reference Model?



22. What is the Protocol Data Unit (PDU) employed at the each lower layer?

The Transport layer packages data into **segments** for use by the Network layer.

- The Network layer packages data into **packets** for use by the Data Link layer. (Internet Protocol, for example, functions with IP packets.)
- The Data Link layer packages data into **frames** for use by the physical layer. This layer consists of two sublayers for Logical Link Control (LCC) and Media Access Control (MAC).
- The Physical layer organizes data into **bits,** a bitstream for transmission over the physical network media.

23. Which layers perform error detection and recovery functions?

- The **Data Link** layer performs error detection on incoming packets. Networks often use cyclic redundancy check (CRC) algorithms to find corrupted data at this level.
- The **Transport** layer handles error recovery. It ultimately ensures data are received in order and free of corruption.

24. What are the two functions of the transport layer in the internet?

- The two functions of the transport layer in the internet are check summing over user data and multiplexing / demultiplexing of data from applications.

25. Write short notes on benefits of OSI Model?

- By separating the network communications into logical smaller pieces, the OSI model simplifies how network protocols are designed. The OSI model was designed to ensure different types of equipment (such as network adapters, hubs, and routers) would all be compatible even if built by different manufacturers.

- A product from one network equipment vendor that implements OSI Layer 2 functionality, for example, will be much more likely to interoperate with another vendor's OSI Layer 3 product because both vendors are following the same model.

- The OSI model also makes network designs more extensible as new protocols and other network services are generally easier to add to a layered architecture than to a monolithic one.

26. What is called the exponential growth of the congestion window?

- The sender always calculates congestion window for a window start size of the congestion window is one segment. Sender sends one packet and waits for acknowledgement. If acknowledgements arise it raises the level of congestion window by one.

- If sender sends two packets if acknowledgement arises it raises the level of congestion window by two. This scheme raises the level of congestion window every time the acknowledge come back, which takes roundtrip time (RTT).This is called the exponential growth of the congestion window.

27. What are the advantages of I-TCP?

- I-TCP does not require any changes in the TCP protocol as used by the hosts in the fixed network or other hosts in a wireless network that do not use this optimization.
- Without partitioning retransmission of lost packets would take place between mobile host and correspondent host across the whole network.
- Optimization of new mechanisms is quite simple to be done in I-TCP as they only cover a single hop.
- The short delay between the mobile host and foreign agent can be determined and is independent of other traffic streams. Therefore an optimized TCP can use precise time-outs to guarantee retransmission as fast as possible.

- Partitioning into two connections also allows the use of a different transport layer protocol between the foreign agent and the mobile host or the use of compressed headers etc. The foreign agent can act as a gateway to translate between different protocols.

28. What are the Disadvantages of I-TCP?

- The loss of the end to end semantics of TCP cause problems if the foreign agent portioning the TCP connection crashes.
- An increased handover latency is more problematic in practical use.
- The foreign agent must be a trusted entity because the TCP connections end at this point.

29. How does data transmission takes place?

- Data transmission takes place using network adapters, fibre optics, copper wires, special hardware for routers etc.

30. What is mean by Slow Start?

- TCP's reaction to a missing acknowledgement is quite drastic, but necessary to get rid of congestion fast enough. The behaviour TCP shows after the detection of cogestion is called slowstart.

31. What are Advantage and Disadvantage of MobileTCP?

Advantage:

- M-TCP maintains the TCP end-to-end semantic. The SH does not send any ACK itself but forwards the ACKs from the MH.
- If the MH is disconnected, M_TCP avoids useless retransmissions, slow starts or breaking connections by simply shrinking the sender's window to 0;
- Since M-TCP does not buffer data in the SH as I-TCP does, it is not necessary to forward buffers to a new SH.
- Lost packets will be automatically retransmitted to the new SH.

Disadvantage:

- As the SH does not act as proxy as in I-TCP, packet loss on the wireless link due to bit errors is propagated to the sender.
- M-TCP assumes low bit error rates, which is not always a valid assumption. ii. A modified TCP on the wireless link not only requires modification to the MH protocol software but also new network elements like the bandwidth manager.

32. What is Fast retransmit?

- In TCP, a receiver sends acknowledgements only if it receive any packets from the sender. Thus receiving acknowledgements from a receiver shows additionally that the receiver continuously receives something from the sender. Therefore, the gap in the packet stream is not due to severe congestion, but a simple packet loss due to a transmission error. The sender can now retransmit the missing packets before the timer expires. This behaviour is called fast retransmit.

33. What is fast recovery?

- The receipt of acknowledgement shows that there is no congestion justifying a slow start. The sender can continue with the current congestion window. The sender performs a fast recovery from the packet loss. This mechanism can improve the efficiency of TCP dramatically.

34. What is HTTP?

- The Hypertext transfer protocol is a stateless, lightweight, application level protocol for data transfer between servers and clients. An HTTP transaction consists of an HTTP request issued by a client and an HTTP response from the server. Stateless means that all HTTP transactions independent of each other.

35. What are the four additional messages in optimized mobile IP Protocol?

- Binding request
- Binding update
- Binding acknowledgement
- Binding warning

36. State some of the classical solutions to improve the efficiency of TCP in wireless?

1) Indirect TCP (I-TCP)
2) Snooping TCP
3) Mobile TCP (M-TCP)
4) Fast retransmit/font recovery
5) Transmission/time –out freezing
6) Selective retransmission
7) Transaction oriented TCP.

37. What is congestion & how it is identified in TCP?

- When there is a temporary overload at some point in the transmission path it is referred to as congestion. Congestion result in packet loss. If acknowledgement does not arrive in time or if any acknowledgement is missing, TCP assumes network congestion.

38. How congestion is controlled in TCP?

- TCP shows a behavior after congestion is called slow start. The sender has a congestion window & congestion threshold for receiver. For each acknowledgement the window size is increased exponentially until the congestion threshold & then it increases linearly (by 1). When congestion occurs the threshold is reduced to half its current size.

39. State whether standard TCP alone support mobile users or wireless links and why?

- No, standard TCP alone cannot support wireless links because wireless links have much higher error rates compared to wired links. The link layer may try to correct errors which results in higher delays and mobility (Handover between access points) may result in packet loss. In both cases standard TCP goes into slow start state.

40. What are the steps to be taken by I-TCP when hand over take place?

1) The old proxy must forward buffered data to new proxy

2) After registration with new foreign agent, the new foreign agent informs the old one about its location to enable packet forwarding.

3) The sockets of proxy must mitigate to the new foreign agent located in the access point.

41. Explain the three types of addresses in TCP/IP?

- Three types of addresses are used by systems using the TC P/IP protocol: the physical address, the internetwork address (IP address), and the port address. The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN. The IP address uniquely defines a host on the Internet. The port address identifies a process on a host.

42. What is encapsulation in Mobile IP? (May/June 2016)

- Tunnelling establishes a virtual pipe for the packets available between a tunnel entry and an endpoint.
- Tunnelling is the process of sending a packet via a tunnel and it is achieved by a mechanism called **encapsulation**. Encapsulation refers to arranging a packet header and data in the data part of the new packet.
- Encapsulation also describes the process of placing an IP datagram inside a network packet or frame

43. Illustrate the use of BOOTP protocol? (Nov/Dec 2015)

- The BOOTP protocol is used for booting (starting) computers from the network. These are popularly used in case of diskless computers. Whenever a client requests an IP address from the server machine, BOOTP searches a table which matches to its physical address.

PART-B

1. What is mobile IP? Explain various entities and terminologies used in Mobile Systems. (Or) Explain the services of Mobile IP and describe the tunneling process?

Mobile Internet Protocol

- The Internet is built on top of a collection of protocols, called the TCP/IP protocol suite. Transmission Control Protocol (TCP) and Internet Protocol (IP) are the core protocols in this suite.

- IP is responsible for routing a packet to any host, connected to the Internet, uniquely identified by an assigned IP address. This raises one of the most vexing issues caused by host mobility. In the traditional IP addressing scheme, each LAN is assigned an address.

- The nodes in the LAN are assigned an address based on the LAN address. In the traditional IP addressing scheme, when a host moves to a different location, it may move to another network. As a result, it needs to change its IP address. This is an unworkable proposition for routing messages to a host, as it would keep changing its address as it moves from one network to another.

- Mobile Internet Protocol (Mobile IP) was proposed by the Internet Engineering Task Force (IETF). The mobile IP allows mobile computers to stay connected to the Internet regardless of their location and without changing their IP address.

- Mobile IP is a standard protocol that extends the Internet Protocol by making mobility transparent to applications and to higher level protocols like TCP.

- Every mobile user likes to have continuous network connectivity irrespective of its physical location. The traditional IP does not support user mobility. Mobile IP was created by extending IP to enable users to keep the same IP address while travelling to a different network.

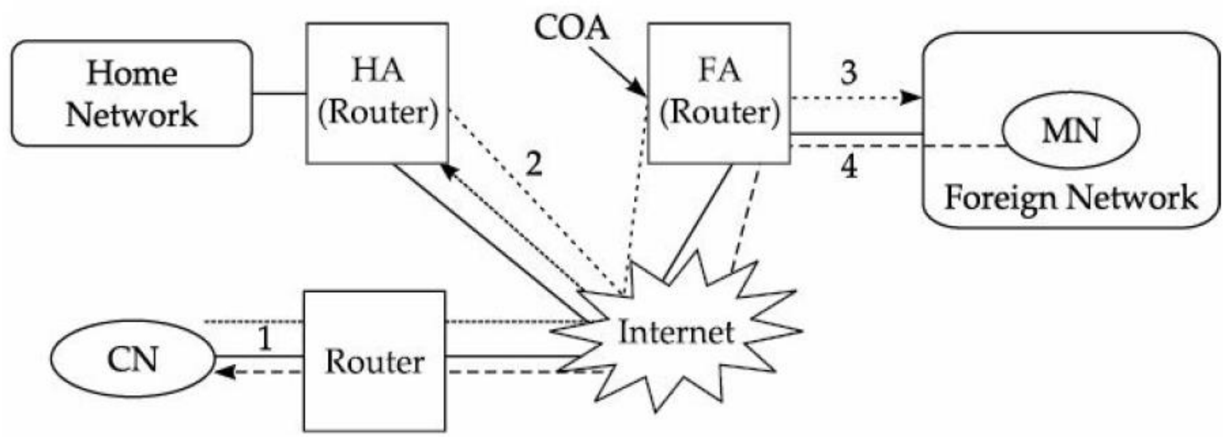


Figure 2.1 *Packet delivery to and from a mobile node.*

- Figure 2.1 shows , a correspondent node (CN) is connected via a router to the Internet, and the home network and the foreign network are also connected via a router, i.e. the home agent (HA) and foreign agent (FA), respectively, to the Internet.

- Therefore, home agent (HA) is implemented on the router connecting the home network with the Internet, a foreign agent (FA) is also implemented on the router connecting the foreign network with the Internet.

- The tunnel for the packets towards the mobile node starts at the home agent and ends at the foreign agent, again here the foreign agent has the care-of-address (COA).

Packet Delivery

- The corresponding node (CN) wants to send an IP packet to a mobile node. CN sends the packet to the IP address of the mobile node as shown in step 1 of Fig. 2.1.

- The IP address of the MN is the destination address, whereas the address of CN is the source address. The packet is passed to the Internet that does not have any information about the MN’s current location. So the Internet routes the packet to the router of the MN’s home network.

- The home agent examines the packet to determine whether the MN is present in its current home network or not. In case that MN is not present, then the packet is encapsulated by a new header that is placed in front of the existing IP header.

- The encapsulated packet is tunnelled to the COA, which act as the new destination address and the HA acts as the source address of the packet as shown in step 2 of Fig. 2.1

- The encapsulated packet is routed to the foreign agent which performs decapsulation to remove the additional header and forwards the decapsulated packet to the MN, which is the actual destination, as specified by the source node (CN), shown in step 3 of Fig. 2.1.

- The MN after receiving the packet from CN, forwards a reply packet to the CN by specifying its own IP address along with the address of the CN as shown in step 4 of Fig. 2.1. The MN's IP address acts as the source address and the CN's IP address acts as the destination address. The packet is routed to the FA. After receiving the packet, FA forwards the packet to CN.

Terminologies—Mobile IP

Mobile Node (MN)*:* A mobile node is a hand - held equipment with roaming capabilities. It can be a cell phone, personal digital assistant, laptop, etc.

Home Network: The home network of a mobile device is the network within which the device receives its identifying IP address (home address). In other words, a home network is a subnet to which a mobile node belongs to as per its assigned IP address. Within the home network, there is no need of mobile IP.

Home Address (HA)*:* The home address of a mobile device is the IP address assigned to the device within its home network. The IP address on the current network is known as home address.

Foreign Agent (FA): The foreign agent is a router in a foreign network that functions as the point of attachment for a mobile node when it roams to the foreign network. The packets from the home agent are sent to the foreign node which delivers it to the mobile node.

Foreign Network (FN)*:* The foreign network is the current subnet to which the mobile node is visiting. It is different from home network. In other words, a foreign network is the network in which a mobile node is operating when away from its home network.

Correspondent Node (CN): The home agent is a router on the home network serving as the anchor point for communication with the mobile node. It tunnells packets from a device on the Internet, called a correspondent node (CN), to the roaming mobile node.

Care-of-Address (COA): It is the address that is used to identify the present location of a foreign agent. The packets sent to the MN are delivered to COA.

The COA can be any of the following two types:

(a) ***Foreign agent COA:*** The COA is an IP address of foreign agent (FA).

(b) ***Co-located COA:*** When the mobile node (MN) acquires a temporary IP address, that address acts as the COA.

Note: The co-located address (temporary IP address) can be acquired using services like dynamic host configuration protocol (DHCP).

Home Agent (HA): It is located in home network and it provides several services for the MN. HA maintains a location registry. The location registry keeps track of the node locations using the current care-of-address of the MN.

Agent Discovery: During call establishment it is necessary for a mobile node to determine its foreign agent. This task is referred to as ***agent discovery.***

The following two discovery methods are popularly used:

(1) Agent advertisement, and
(2) Agent solicitation.

1. ***Agent advertisement:*** Generally the foreign and the home agents advertise their presence through periodic agent advertisement messages.

An agent advertisement message, lists one or more care-of-addresses and a flag indicating whether it is a home agent or a foreign agent. Agent advertisement is a popularly used method in agent discovery.

2. ***Agent solicitation:*** In case a mobile node (MN) does not receive any COA, then the MN should send an agent solicitation message. But it is important to monitor that these agent solicitation messages do not flood the network.

A mobile node can usually send up to three solicitation messages (one per second) as soon as it enters a new network. The basic purpose of the solicitation messages sent by a mobile node (MN) is to search for a foreign agent (FA).

If an MN does not receive any address in response to its solicitation messages, then to avoid network flooding, the MN should exponentially reduce the rate of sending the solicitation messages.

Tunnelling and encapsulation

- Tunnelling establishes a ***virtual pipe*** for the packets available between a tunnel entry and an endpoint.
- Tunnelling is the process of sending a packet via a tunnel and it is achieved by a mechanism called **encapsulation**.
- Encapsulation refers to arranging a packet header and data in the data part of the new packet.
- Disassembling the data part of an encapsulated packet is called **decapsulation**.

2. Answer the following with respect to missing and duplicate segments in TCP operation.

(a) What can cause segments to be missed at the receiver-end and also cause duplicate segments to arise? Explain your answer using a suitable scenario of operation.

(b) How exactly is a missing segment detected in TCP? Explain the specific actions that take place when a missing segment is detected.

Overview of Mobile IP

The goal of mobile IP is to enable packet transmission efficiently without any packet loss and disruptions in the presence of host and/or destination mobility.

Scenario

- Suppose a person working as a business development executive for a company needs to take care of many regional offices in India and abroad. His home office is in Delhi where he spends about 40% of his time. The rest of the time he spends between the other offices, say, Kolkata, Mumbai, Chennai, Kathamandu and Singapore.

- A problem that arises in this context is: how does he make arrangements so that he would continue to receive postal mails regardless of his location? If we can answer this, we can easily understand how IP works in the context of a mobile device.

- There are two broad categories of solutions to this problem being faced by the business executive: (i) address changing, (ii) decoupling mail routing from his address. It would be difficult for the business development executive to inform about his changed address to all those who are likely to write letters to him each time he moves. Also, by the time, he would have informed everyone about his new address, it would have become time for the address to change again. And he certainly cannot decouple the routing of mail from his address, unless he has set up his own personal postal system.

- Solution is mail forwarding. He leaves Delhi for Singapore for a couple of months. He will inform the Delhi post office that he will be in Singapore. The Delhi post office would intercept his mails headed for his normal Delhi address, relabel them, and forward them to Singapore.

- Depending on where he is staying, this mail might be redirected either straight to a new address in Singapore, or to a Singapore post office where he can pick it up. If he leaves Singapore to go to another city, say, Kathamandu, he would just call the Delhi post office and tell them about his new location. When he gets back to home office, he will cancel the forwarding arrangement and get his mail as usual.

- The mobile node is normally resident on its home network, which is the one indicated by the network ID in its IP address. Devices on the internetwork always route using this address, so the pieces of "mail" (datagrams) always arrive at a router at the device's "home". When the device "travels" to another network, the home router ("post office") intercepts these datagrams and forwards them to the device's current address.

- It may send the datagrams straight to the device using a new, temporary address, or it may send them to a router on the device's current network (the "other post office", Singapore) for final delivery. The mobile node's home router serves as the home agent and the router in Singapore as the foreign agent. The mobile has been assigned a temporary "care-of address" to use in Singapore (which in this case is a co-located care-of-address). As per mobile IP terminology, the home agent tunnells the packet to the COA.

Advantages

- Simple mechanism to understand and implement.
- This scheme is transparent to everyone sending mails

Disadvantages

- To keep communicating with his home post office each time he moves.
- Every piece of mail has to be sent through the system twice—first to Delhi and then to wherever he moves, which is inefficient and delay in delivering and also loads the postal system.

3. Explain about the key mechanism in Mobile IP? (Nov/Dec 2016)

Key Mechanism in Mobile IP

Mobile IP is associated with the following three basic mechanisms:

- Discovering the care-of-address
- Registering the care-of-address
- Tunnelling to the care-of-address

The specific protocols used by the basic mechanisms have also been shown. Observe that the registration process works over UDP and the discovery protocol over ICMP.

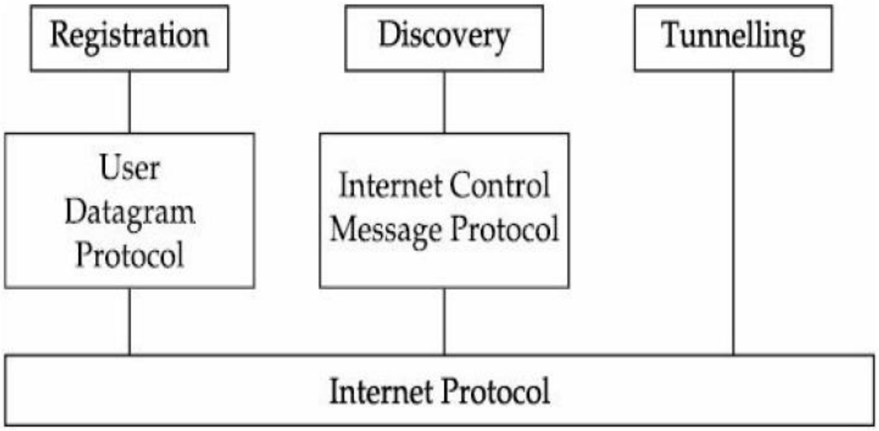


Figure 4.2 *A schematic model of Mobile IP.*

Discovering the care-of-address

Each mobile node uses a discovery protocol to identify the respective home and foreign agents.

The discovery of the care-of-address consists of four important steps.

1. Mobile agents advertise their presence by periodically broadcasting the ***agent advertisement*** messages.

2. The mobile node receiving the ***agent advertisement*** message observes whether the message is from its own home agent and determines whether it is on the home network or on a foreign network.

3. If a mobile node does not wish to wait for the periodic advertisement, it can send out ***agent solicitation*** messages that will be responded to by a mobility agent.

4. The process of ***agent advertisements, involves the following activities:***

- Foreign agents send messages to advertise the available care-of-addresses.
- Home agents send advertisements to make themselves known.
- Mobile hosts can issue agent solicitations to actively seek information.

- If a mobile host has not heard from the foreign agent to which its current care-of-address belongs, it takes up another care-of-address.

Registering the care-of-address

- If a mobile node discovers that it is on the home network, it operates without requiring any mobility services.
- If a mobile node obtains a care-of-address from a foreign agent, then this address should be registered with the home agent.
- The mobile node sends a request for registration to its home agent along with the 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.
- The mobile node makes use of the registration procedure to intimate the care-of-address to a home agent.

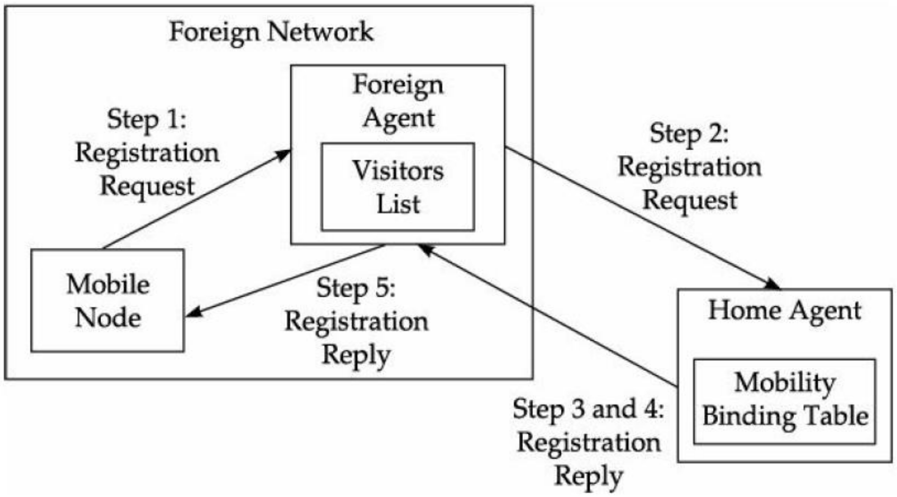

Foreign Network
Foreign Agent
Visitors List
Step 1: Registration Request
Step 2: Registration Request
Mobile Node
Step 5: Registration Reply
Home Agent
Mobility Binding Table
Step 3 and 4: Registration Reply

Figure 4.3 *Registration process in Mobile IP.*

The registration process consists of the following steps:

1. If the mobile node is on a new network, it registers with the foreign agent by sending a ***registration request*** message which includes the permanent IP address of the mobile host and the IP address of its home agent.

2. The foreign agent in turn performs the registration process on behalf of the mobile host by sending a Registration Request containing the permanent IP address of the mobile node and the IP address of the foreign agent to the home agent.

3. When the home agent receives the Registration Request, it updates the mobility binding by associating the care-of-address of the mobile node with its home address.

4. The home agent then sends an acknowledgement to the foreign agent.

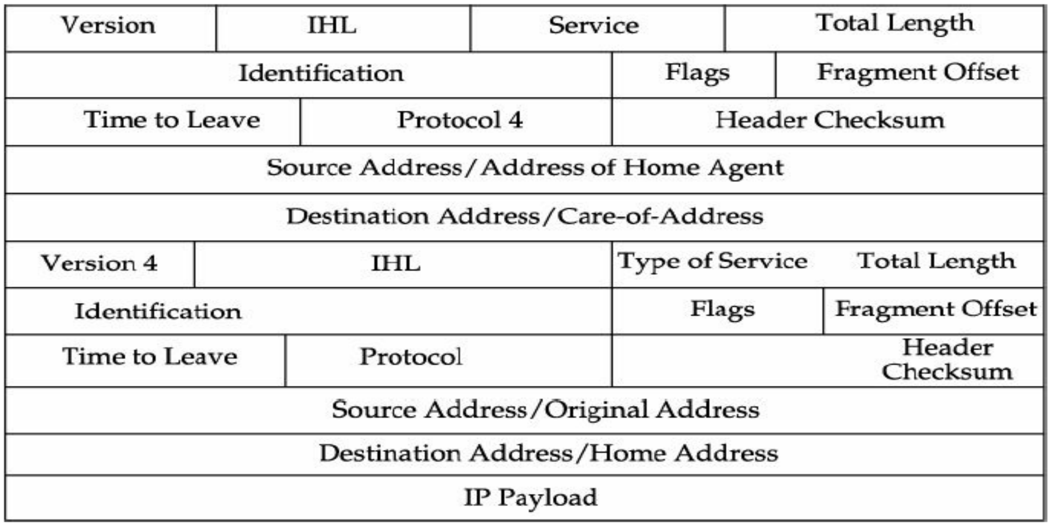
5. The foreign agent in turn updates its visitors list by inserting the entry for the mobile node and relays the reply to the mobile node.

Tunnelling to the care-of-address - Tunnelling takes place to forward an IP datagram from the home agent to a care-of-address.

This involves carrying out the following steps:

- When a home agent receives a packet addressed to a mobile host, it forwards the packet to the care-of-address using IP-within-IP (encapsulation).
- Using IP-within-IP, the home agent inserts a new IP header in front of the IP header of any datagram.
- Destination address is set to the care-of-address.
- Source address is set to the home agent’s address.
- After stripping out the first header, IP processes the packet again.

The tunnelling operation in mobile IP and IP-within-IP encapsulation (embedding) are shown in Fig. 4.4.



Version	IHL	Service	Total Length
Identification		Flags	Fragment Offset
Time to Leave	Protocol 4	Header Checksum	
Source Address/Address of Home Agent			
Destination Address/Care-of-Address			
Version 4	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
Time to Leave	Protocol	Header Checksum	
Source Address/Original Address			
Destination Address/Home Address			
IP Payload			

Figure 4.4 *IP encapsulation in mobile IP.*

4. Discuss how optimization in achieved in mobile IP?

Route Optimization

In the mobile IP protocol, all the data packets to the mobile node go through the home agent. Because of this there will be heavy traffic between HA and CN in the network, causing latency to increase.

The association of the home address with a care-of-address is called ***binding.***

Therefore, the following route optimization needs to be carried out to overcome this problem.

- Enable direct notification of the corresponding host
- Direct tunnelling from the corresponding host to the mobile host
- Binding cache maintained at the corresponding host

TABLE - Messages Transmitted in Optimized Mobile IP

Message type	***Description***

Binding request	If a node wants to know the current location of a mobile node (MN), it sends a request to home agent (HA).
Binding acknowledgement	On request, the node will return an acknowledgement message after getting the binding update message.
Binding update	This is a message sent by HA to CN mentioning the correct location of MN. The message contains the fixed IP address of the mobile node and the care-of-address. The binding update can request for an acknowledgement.
Binding warning	If a node decapsulates a packet for a mobile node (MN), but it is not the current foreign agent (FA), then this node sends a binding warning to the home agent (HA) of the mobile node (MN).

5. With a diagram explain DHCP and its protocol architecture? (May/June 2016)

Dynamic Host Configuration Protocol (DHCP)

- DHCP was developed based on bootstrap protocol (BOOTP). DHCP provides several types of information to a user including its IP address. To manage dynamic configuration information and dynamic IP addresses, IETF standardized an extension to BOOTP known as dynamic host configuration protocol (DHCP).

- The DHCP client and server work together to handle the roaming status and to assign IP address on a new network efficiently. The DHCP server allocates an IP address from a pool of IP addresses to a client.

- The BOOTP protocol is used for booting (starting) computers from the network. These are popularly used in case of diskless computers. Whenever a client requests an IP address from the server machine, BOOTP searches a table which matches to its physical address.

Benefits of DHCP

- **Reliable IP address configuration.** DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time.

- **Reduced network administration.** DHCP includes the following features to reduce network administration:

  - Centralized and automated TCP/IP configuration.
  - The ability to define TCP/IP configurations from a central location.
  - The ability to assign a full range of additional TCP/IP configuration values by means of DHCP options.
  - The efficient handling of IP address changes for clients that must be updated frequently, such as those for portable computers that move to different locations on a wireless network.
  - The forwarding of initial DHCP messages by using a DHCP relay agent, thus eliminating the need to have a DHCP server on every subnet.

Why use DHCP

- Every device on a TCP/IP-based network must have a unique unicast IP address to access the network and its resources. Without DHCP, IP addresses must be configured manually for new computers or computers that are moved from one subnet to another, and manually reclaimed for computers that are removed from the network.
-
- DHCP enables this entire process to be automated and managed centrally. The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it starts up on the network. Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.
-
- The network administrator establishes DHCP servers that maintain TCP/IP configuration information and provide address configuration to DHCP-enabled clients in the form of a lease offer.
- The DHCP server stores the configuration information in a database, which includes:

    - Valid TCP/IP configuration parameters for all clients on the network.
    - Valid IP addresses, maintained in a pool for assignment to clients, as well as excluded addresses.
    - Reserved IP addresses associated with particular DHCP clients. This allows consistent assignment of a single IP address to a single DHCP client.
    - The lease duration, or the length of time for which the IP address can be used before a lease renewal is required.

A DHCP-enabled client, upon accepting a lease offer, receives:

- A valid IP address for the subnet to which it is connecting.
- Requested DHCP options, which are additional parameters that a DHCP server is configured to assign to clients. Some examples of DHCP options are Router (default gateway), DNS Servers, and DNS Domain Name. For a full list of DHCP options, see "DHCP Tools and Settings."

Significance of Dynamic Host Configuration Protocol

DHCP is an extension to the BOOTP and compatible with it. For example, if a host is running BOOTP, it can also request configuration (static configuration) from a DHCP server node.

To provide temporary IP addresses whenever a host moves from one network to another network.

DHCP supports the following three important mechanisms for IP address allocation:

Automatic allocation: In automatic allocation, DHCP assigns a permanent IP address to a particular client.

Dynamic allocation: In dynamic allocation, DHCP assigns IP address to a client for a specific period of time.

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

Mobile Transport Layer

- In mobile computing applications, Transmission Control Protocol (TCP) is possibly the most popular transport layer protocol. In fact, TCP is the ***de facto*** standard transport layer protocol for applications that require guaranteed message delivery.

- TCP is a connection-oriented protocol. UDP (User Datagram Protocol), on the other hand, is a connectionless protocol in the TCP/IP protocol suite and does not guarantee reliable data delivery. However, when the traditional TCP is used in mobile computing networks, it operates in a highly inefficient and unsatisfactory manner.

- TCP needs several special adaptations to make it suitable for use in wireless networks.

6. Explain the following terms associated with TCP/IP stack: (a) IP, (b) HTTP, (c) SMTP, (d) MIME, (e) FTP, (f) SNMP, (g) ICMP, (h) ARP, (i) RARP, (j) DNS, (k) IP Addresses, (l) IGMP

Overview of TCP/IP

The TCP/IP protocol suite was developed by DARPA in 1969 to provide seamless communication services across an internetwork consisting of a large number of different networks. The TCP/IP protocol suite is a collection of a large number of protocols.

Two most important protocols

1. Transmission Control Protocol (TCP)
2. Internet Protocol (IP).

TCP/IP protocol stack consists of four layers of protocols.

1. Application layer,
2. Transport layer,
3. Internet layer, and
4. Network interface layer.

TCP/IP does not define any specific protocol for the network interface layer, but allows any of the standard protocols to be used at this layer.

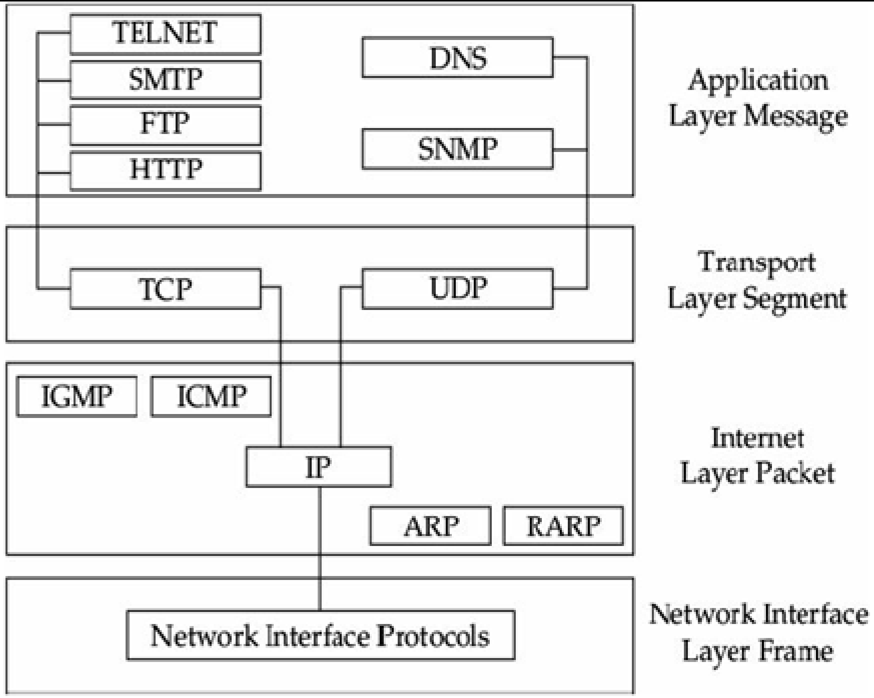


Figure 5.1 *TCP/IP protocol stack*

- The application programmers and end-users are mainly concerned with the application layer protocols. The application layer protocols, in turn, make use of the services provided by the lower layer protocols.

- An application layer protocol requiring ***to send a message to another application*** makes use of a transport layer protocol and passes it with the message to be transmitted.

- The specific transport layer protocol converts the message into small parts and attaches certain information to it. The transport layer protocol first converts a ***message into segments*** and passes these segments to the Internet layer protocol (IP).

- The IP layer protocol attaches certain information to the segments such as the destination host address to form ***packets***. We can say that a TCP segment is carried in one or more IP packets.

- The IP passes on the packets to the network interface layer protocol, which in turn converts them ***to frames*** by adding certain additional information to the packets such as checksum and then transmits them on the network.

- The reverse operation takes place when a frame arrives at a host. The network interface layer protocol removes the information added by the corresponding network interface layer protocol at the sender-end and passes on the packet to the IP layer.

- The IP layer protocol at the destination removes the information added by the IP layer at the sender's end and gets back the segments and passes these to the transport layer protocol. The transport layer protocol at the receiver strips the information added by ***the transport layer protocol at the sender, reconstructs the message and sends it to the application layer.***

- Note that the application layer deals with messages; the transport layer deals with segments; the internet layer deals with packets; and the data link layer deals with frames.

- Over the last two decades, the Internet has seen almost exponential growth and now the Internet applications have become ubiquitous. The Internet-based applications are developed predominantly by using the client-server paradigm.

- In a typical Internet-based application deployment scenario, the server is an application providing certain services and a client that typically runs on a web browser, is primarily the requester of services. TCP has now become the *de facto* transport layer protocol for client-server communications.

Terminologies of TCP/IP

TCP *(Transmission Control Protocol):* On the sending side, TCP is responsible for breaking a message into small parts, adding sequence numbers and certain other information and after this, making them known as segments. TCP passes the segments to the lower layer protocol for transmission over the network.

While at the receiver's end, TCP assembles the segments when they arrive and reconstructs the message. TCP is a reliable protocol. Whenever a packet is lost or corrupted during transmission, TCP detects it and requests the sender for retransmission. Thus, retransmission is used as the primary mechanism by TCP for ***reliable data delivery*** to the destination.

IP *(Internet Protocol):* At the host machine of an application sending a message, IP is responsible for constructing packets (also called datagrams) from the segments it receives from the transport layer protocol by adding the destination host address and then passes these on to the lower layer protocol for transmitting. On the receiver's side, it deconstructs the segments and then passes these to the transport layer protocol.

HTTP *(Hyper Text Transfer Protocol):* The HTTP protocol is used for communications between a web server and the client-side application running on a web browser.

SMTP *(Simple Mail Transfer Protocol):* The SMTP protocol is used for sending and receiving emails by a mail client.

MIME *(Multipurpose Internet Mail Extensions):* The MIME protocol lets the SMTP encode multimedia files such as voice, picture, and binary data in e-mails and transmit them across TCP/IP networks. SMTP has been designed to handle only the text contents in e-mails. MIME helps e-mails to include non-text contents such as picture, voice, and binary data files by encoding the binary data in the ASCII text format.

FTP *(File Transfer Protocol):* The FTP protocol is used to transfer files between the computers.

SNMP *(Simple Network Management Protocol):* The SNMP protocol is used for administration and management of computer networks. The network manager uses tools based on this protocol to monitor network performance.

ICMP *(Internet Control Message Protocol):* The ICMP protocol runs on all hosts and routers and is mainly used for reporting errors such as a non-reachable host.

ARP *(Address Resolution Protocol):* The ARP protocol is used by IP to find the hardware address (also called the physical address) of a computer based on its IP address. The hardware (physical) address is stored in the ROM (Read Only Memory) of the computer's network interface card. It is also known as MAC (Media Access Control) address and also as an Ethernet hardware address (EHA).

RARP *(Reverse Address Resolution Protocol):* The RARP protocol is used by IP to find the IP address based on the physical (MAC address) address of a computer.

BOOTP *(Boot Protocol):* The BOOTP protocol is used for booting (starting) a diskless computer over a network. Since a diskless computer does not store the operating system program in its permanent memory, the BOOTP protocol helps to download and boot over a network, using the operating system files stored on a server located in the network.

Routers: A router is responsible for ***routing*** the packets that it receives to their destinations based on their IP addresses, possibly via other routers.

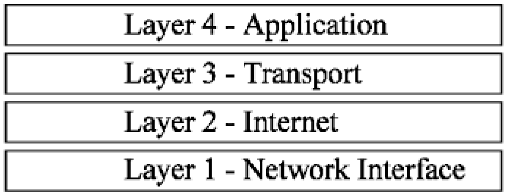
DNS: It stands for **D**omain **N**ame **S**ystem (or **S**ervice or **S**erver). It is a software service available on the Internet that is responsible for translating domain names into IP addresses. We use domain names while accessing any website since these are alphabetic character strings that are much easier to remember compared to the conventional IP address specification using dot-separated numerical values.

Of course, when we specify a website (URL) using its domain name, a DNS service hosted on the Internet translates the domain name into the corresponding IP address, since, after all, the Internet works using IP addresses. For example, the domain name *www.iitkgp.ernet.in* might get translated by the DNS to *144.16.192.245.*

IP Addresses: Each computer must have an IP address before it can be meaningfully connected to the Internet. A packet gets routed to its destination based on its IP address.

IGMP *(Internet Group Management Protocol)**:*** The IGMP protocol is used by hosts to exchange information with their local routers to set up multicast groups. A setup of multicast groups allows efficient communication, especially for video streams and certain gaming applications. The routers also use the IGMP to check whether the members of a known group are active or not.

7. With a neat diagram explain the architecture of TCP/IP? (May/June 2016)



Layer 4 - Application

Layer 3 - Transport

Layer 2 - Internet

Layer 1 - Network Interface

Figure 5.2 *TCP/IP protocol layers.*

Application layer: The protocols are used by applications to establish communication with other applications which may possibly be running on separate hosts.

The most widely known Application layer protocols help users exchange information:

- The Hypertext Transfer Protocol (HTTP) transfers files that make up pages on the World Wide Web.
- The File Transfer Protocol (FTP) transfers individual files, typically for an interactive user session.
- The Simple Mail Transfer Protocol (SMTP) transfers mail messages and attachments.
- The Domain Name System (DNS) protocol resolves a host name, such as www.microsoft.com, to an IP address and copies name information between DNS servers.

- The Routing Information Protocol (RIP) is a protocol that routers use to exchange routing information on an IP network.
- The Simple Network Management Protocol (SNMP) collects and exchanges network management information between a network management console and network devices such as routers, bridges, and servers.

Transport layer: It provides reliable end-to-end data transfer services. The term end-to-end means that the end points of a communication link are applications or processes. Therefore, sometimes protocols at this layer are also referred to as host-to-host protocols. Remember that there can be several applications or processes running on a host.

Thus, to identify the end point, it is not only the computer that needs to be identified, but also the exact process or application that would receive the message needs to be identified. An application or a process specifies a port number on which it would receive a message.

Once a message reaches a host, it is demultiplexed using the port number at the transport layer for delivery to the appropriate application. The transport layer provides its services by making use of the services of its lower layer protocols. This layer includes both connection-oriented (TCP) and connectionless (UDP) protocols.

Internet layer: The Internet layer packs data into data packets that are technically known as IP datagrams. Each IP datagram contains source and destination address (also called IP address) information that is used to forward the datagrams between hosts and across networks. The Internet layer is also responsible for routing of IP datagrams. In a nutshell, this layer manages addressing of packets and delivery of packets between networks using the IP address.

The core protocols for the IPv4 Internet layer consist of the following:

- The Address Resolution Protocol (ARP) resolves the Internet layer address to a Network Interface layer address such as a hardware address.
- The Internet Protocol (IP) is a routable protocol that addresses, routes, fragments, and reassembles packets.
- The Internet Control Message Protocol (ICMP) reports errors and other information to help you diagnose unsuccessful packet delivery.
- The Internet Group Management Protocol (IGMP) manages IP multicast groups.

Network access layer: The functions of this protocol layer include encoding data and transmitting at the signalling determined by the physical layer. It also provides error detection and packet framing functionalities. The data link layer protocols help deliver data packets by making use of physical layer protocols. A few popular data link layer protocols are Ethernet, Token Ring, FDDI, and X.25.

Ethernet is possibly the most common data link layer protocol. The physical layer defines how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface with a network medium, such as coaxial cable, optical fibre, or twisted pair of copper wires.

8. How data are transmitted from client to server? Explain the operation of TCP with its header format?

An Overview of the Operation of TCP

- When a client-server application runs on hosts that are wide apart, data transmission between the client and the server may span multiple networks. These networks are called ***sub-networks***. For data routing, the Internet Protocol (IP) requires that each host in the network should have a unique address.

- Identification of hosts is not enough for data delivery, the packets must be forwarded to the exact application (or to a process in an application) requiring the packet. Within each host, every process is identified by a port number based on which the TCP can deliver data/information to each relevant process.

- A host can run many client and server applications. Therefore, these different applications can send/receive data concurrently and independently.

- As a result, data sent by different applications need to be ***multiplexed*** together, before these are sent on the network. Similarly, the TCP receives segments that may correspond to different applications running on a host.

- Therefore, on receiving a segment from its lower layer, TCP has to decide as to which application is the recipient. This is called ***demultiplexing***. TCP performs multiplexing and demultiplexing by using ***port*** numbers.

- Usually a message in the form of a block of data is passed to TCP by the sending application. The TCP breaks it into many small parts and attaches certain control information (called TCP header) to each small part. Each small part of the data along with the TCP header is called a segment.

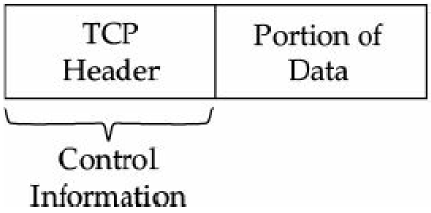
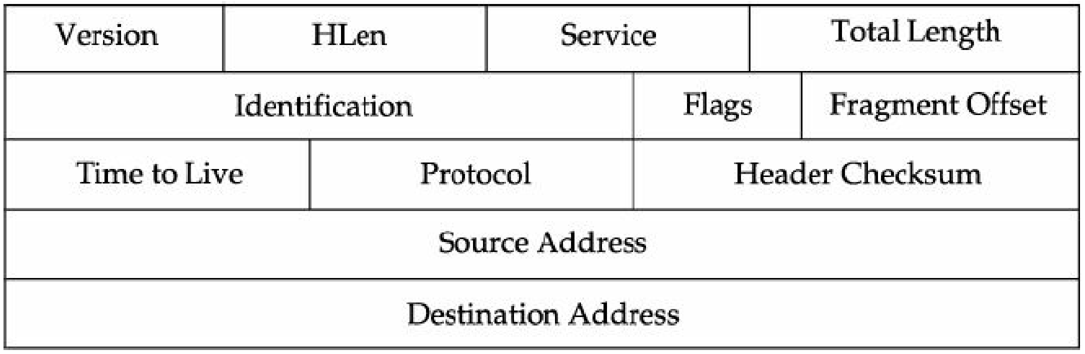


Figure 5.3 *The structure of a TCP segment.*

The TCP header includes several items of information including the following:
(i) Destination Port
(ii) Checksum
(iii) Sequence number

IP datagram

An IP packet is also called a datagram. A datagram is of variable length which can be up to 65,536 bytes. It has two fields, namely header and data.



<table>
<tr><td>Version</td><td colspan="2">HLen</td><td colspan="2">Service</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="4">Identification</td><td colspan="2">Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td colspan="2">Protocol</td><td colspan="3">Header Checksum</td></tr>
<tr><td colspan="7">Source Address</td></tr>
<tr><td colspan="7">Destination Address</td></tr>
</table>

Figure 5.4 *IP datagram structure.*

Important fields of an IP datagram

Version (Ver): The IP version number is defined in this field, e.g. IPV4 or IPV6.

Header length (Hlen): It defines the header length as multiples of four bytes.

Service type: It has bits that define the priority of the datagram itself.

Total length: This field is allotted 16 bits to define the length of IP datagram.

Identification: It is mainly used to identify fragmentation that belongs to different networks. 16 bits are allotted for this job.

Flags: It deals with fragmentation of the data.

Fragmentation offset: It is a pointer to the offset of the data in the original datagram.

Time to live: This field is used to define the total number of hops that a datagram has to travel before discarding the operation.

Protocol: This field has 16-bits. It defines which upper layer protocol data is encapsulated at that time, for example TCP or UDP or ICMP, etc.

Header checksum: It has a 16-bit field to check the integrity of the packets.

Source address: It is a four byte (4 □ 8 = 32) internet address to define the original source.

Destination address: It is a four byte (4 □ 8 = 32) internet address to identify the destination of datagram. The IP datagrams are sent to the link layer and become ready for transmission to the first sub-network in the path to its destination. The IP datagrams are also called packets.

Port address

In a client-server application, often the client and server programs are located on different host machines. The client program usually uses a temporary port number and the server program uses a well-known (or permanent) port number. These port numbers are used for identification of the application.

Protocol	*Port*
TELNET	23

SMTP	25
RPC	111
DNS	53

TABLE 5.1 A Few Commonly Used Well-known Port Numbers

Data encapsulation

When the TCP segments are handed over to Internet Protocol (IP layer), this layer appends an IP header containing the relevant control information. A segment after this additional control data is added, is called an IP datagram (see Fig. 5.4). The network access layer also appends its own header and now the segment becomes known as a frame/packet.

The packet header includes important information such as the following:

(i) Facilities requests (such as priority)

(ii) Destination sub-network address

Application Layer Protocols of TCP

Simple Mail Transfer Protocol (SMTP): It provides an 'electronic mail' function, that is used for transferring messages between different hosts. Originally, SMTP could handle text messages only. ***MIME*** helps transmit multimedia data within an e-mail by encoding the binary multimedia data in the ASCII format.

File Transfer Protocol (FTP): FTP is mainly used for transferring files from one host to another based on a user command. FTP allows both binary and text file transfers. Each FTP connection opens two TCP connections, one for data transfer and the other for transfer of control commands such as put, get, etc.

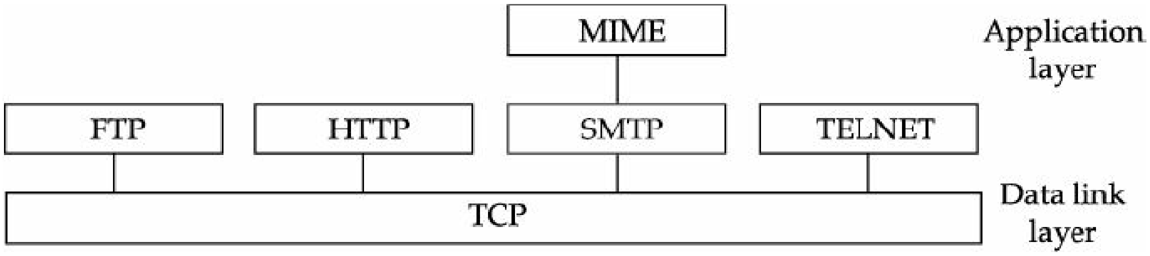


Figure 5.5 *Application layer protocols in TCP/IP protocol suite.*

TELNET: This application layer protocol lets users use a remote log-on facility, using which a user can log-on to a remote system. Both FTP and TELNET make use of the TCP layer. TCP forwards these data over the network by invoking the IP layer and the IP layer in turn invokes the like layer protocol.

The users and applications use sftp (secure ftp) and ssh (secure shell) protocols. These protocols essentially serve to encrypt before passing the data on to the TCP layer. These protocols also perform decryption after receiving the data.

9. What are the main differences between TCP/IP versus ISO/OSI Model?

TCP/IP versus ISO/OSI Model

OSI(Open System Interconnection)	**TCP/IP(Transmission Control Protocol / Internet Protocol)**

1. OSI provides layer functioning and also defines functions of all the layers.	1. TCP/IP model is more based on protocols and protocols are not flexible with other layers.
2. In OSI model the transport layer guarantees the delivery of packets	2. In TCP/IP model the transport layer does not guarantees delivery of packets.
3. Follows horizontal approach	3. Follows vertical approach.
4. OSI model has a separate presentation layer	4. TCP/IP does not have a separate presentation layer
5. OSI is a general model.	5. TCP/IP model cannot be used in any other application.
6. Network layer of OSI model provide both connection oriented and connectionless service.	6. The Network layer in TCP/IP model provides connectionless service.
7. OSI model has a problem of fitting the protocols in the model	7. TCP/IP model does not fit any protocol
8. Protocols are hidden in OSI model and are easily replaced as the technology changes.	8. In TCP/IP replacing protocol is not easy.
9. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them.	9. In TCP/IP it is not clearly separated its services, interfaces and protocols.
10. It has 7 layers	10. It has 4 layers
11. The OSI model define specific Data link layer and Physical layer.	11. The network access layer encompasses the Data link and physical layers.

10. Give the comparison of various TCP advantages and disadvantages in wireless networking. (Nov/Dec 2016)

Adaptation of TCP Window

- The TCP primarily deploys a flow control technique to control congestion in a network. Traffic congestion occurs when the rate at which data is injected by a host into the network exceeds the rate at which data can be delivered to the network.

- A ***flow control technique*** helps adapt the rate of data transmission by the TCP at the sending host end. The flow control technique helps to prevent the build-up of congestion in the network and at the same time helps to prevent buffer overrun at the slow receivers.

- If data transmissions occur at a much faster rate than what the network infrastructure can comfortably support, then data packets get built up at the routers. When the ***buffers at routers start to overflow, the packets start getting lost.***

- Additionally, if data transmissions by a sender take place at a much faster rate than what a slower receiver can handle, then the receiver's buffer starts to get flooded and hence the packets get lost.

- TCP handles both these causes of ***packet loss*** by reducing the rate at which data is transmitted at the sender's end. Thus, a receiver uses the flow control mechanism to restrict how fast a sender can transmit.

- To provide an acceptably fast data transmission service, once congestion disappears the transmission rate at the sender's end needs to be increased to a suitable value.

- Thus a flow control technique helps TCP dynamically adjust the transmission rate at the sender’s end, ***reducing the transmission rate as*** congestion starts to develop and increasing it as congestion starts to disappear.

- The flow control mechanism deployed by TCP (called the sliding window protocol) is primarily based on the concepts of congestion window and advertised window.

- When a sender starts to send data packets, the receiver indicates an advertised window (or receiver window) to the sender while sending acknowledgements. The advertised window is usually set equal to the size of the receive buffer at the receiver.

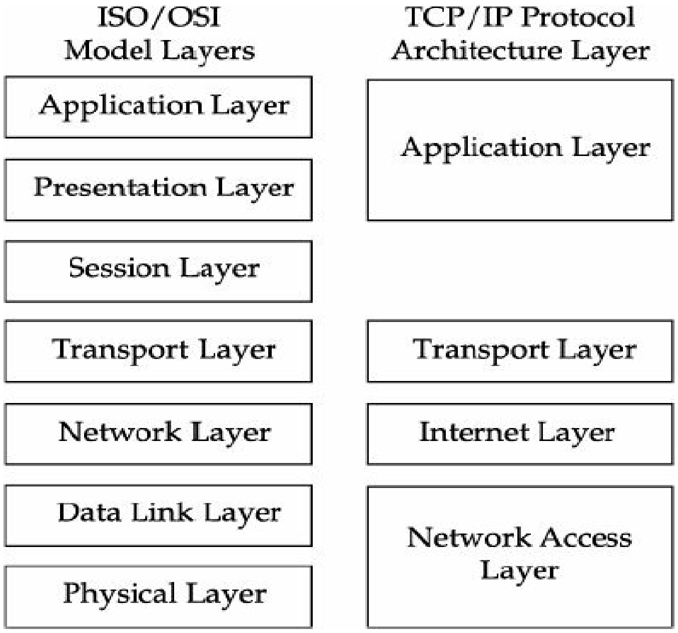


Figure 5.6 *A comparison of TCP/IP and ISO/OSI models.*

- The sender uses the advertised window size obtained from the receiver to determine the maximum amount of data that it can transmit to the receiver without causing **buffer overflow at the receiver.** In other words, to prevent buffer overflow at the receiver, the data packets transmitted by a sender **without having received acknowledgments** for them should not exceed the size of the buffer available at the receiving end.

- For each segment sent, a sending host expects to receive an acknowledgment. A ***congestion window*** indicates the maximum number of segments that can be outstanding without the receipt of the corresponding acknowledgement before the TCP at the sender’s end pauses transmitting and waits for an acknowledgement to arrive.

- The TCP at a sender’s end pauses if the number of segments for which the acknowledgement is outstanding becomes equal to the congestion window. A sender sets the congestion window size to 1 and keeps on increasing it until duplicate acknowledgements are received or until the number of outstanding packets becomes equal to the size of the advertised window.

- Upon receipt of an acknowledgement, TCP detects packet loss using ***Retransmission timeout*** (RTO) and duplicate acknowledgements. After transmitting a segment, a TCP sender sets the retransmission timer for only one packet. If an acknowledgement for the packet is not received before the timer goes off, the packet is assumed to be lost. RTO is dynamically calculated. Timeouts can take too long.

- Again the TCP sender assumes that a packet loss has occurred if it receives three duplicate acknowledgements consecutively. In TCP, when a receiver does not get a packet that it expects in a sequence but gets an out of order packet, it considers that the expected packet might have got lost and it indicates this to the sender by transmitting an acknowledgment for the last packet that was received in order. Thus, three duplicate acknowledgement are also generated if a packet is delivered at least three places beyond its in-sequence location.

- In wired networks, packet losses primarily occur on account of congestions encountered in the transmission path. However, in a wireless environment packet losses can also occur due to mobility and channel errors. In wired networks, bit errors are rare.

- Noise can cause intermittent bit errors. Further, there can be intermittent disconnections due to fading and also due to obstructions that may be encountered by a mobile host.

- Further, packets may get lost during handoff. An intermittent disconnection may cause the TCP at the sender's end to time out for an acknowledgement and cause it to retransmit. This would cause unnecessary retransmissions to occur, even though the packet may be buffered at a router.

11. Explain the various improvements in TCP performance with diagram (8) (May/June 2016)

Traditional Networks

- Congestion control is primarily achieved by reducing the transmission window, which in turn results in slower data transfer. The important mechanisms used by TCP for improving (tcp-reno model) performance are given below.

Slow start

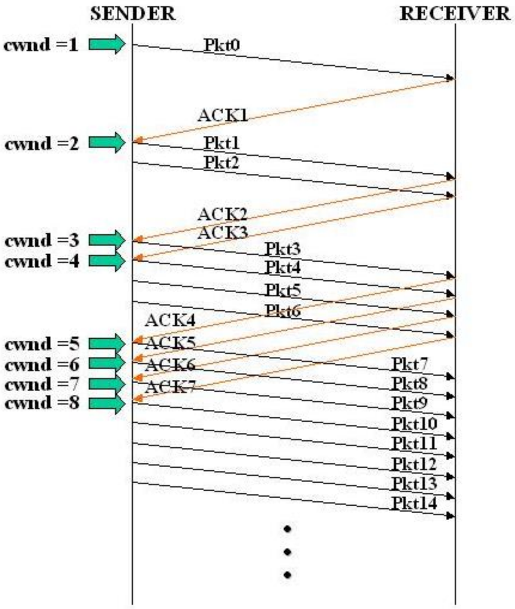
- The slow-start mechanism is used when a TCP session is started. Instead of starting transmission at a ***fixed transmission window size***, the transmission is started at the lowest window size and then doubled after each successful transmission. The rate of doubling is tied to the rate at which acknowledgements come back. Thus, the ***doubling of window size*** occurs at every round trip time (RTT).

- RTT is the time that ***elapses between a segment is transmitted by a sender and the corresponding acknowledgement is received.*** If congestion is detected (indicated by duplicate acknowledgements), the transmission window size is reduced to half of its current size and the congestion avoidance process starts. This mechanism of ***rate doubling and reduction to half*** the previous value is nothing but ***a binary search technique*** deployed to determine the 'right' transmission window size.

- The slow-start process begins by the sender setting the transmission window size to one, i.e., transmiting one segment to the receiver. The sender does not transmit the next segment until it receives an acknowledgement for the previous segment. Once the acknowledgement is received, the sender becomes sure that the congestion window (network capacity) is at least one segment.

- To determine the exact congestion window size, the sender doubles the transmission window size. It transmits two segments and after arrival of the two corresponding acknowledgements, it again ***increases the transmission window size by two and sets it equal to four,*** and so on.

- Increments that occur to the size of the congestion window are, thus, exponential. A congestion window is doubled every time the acknowledgements arrive smoothly. This exponential growth of congestion window stops at the congestion threshold.



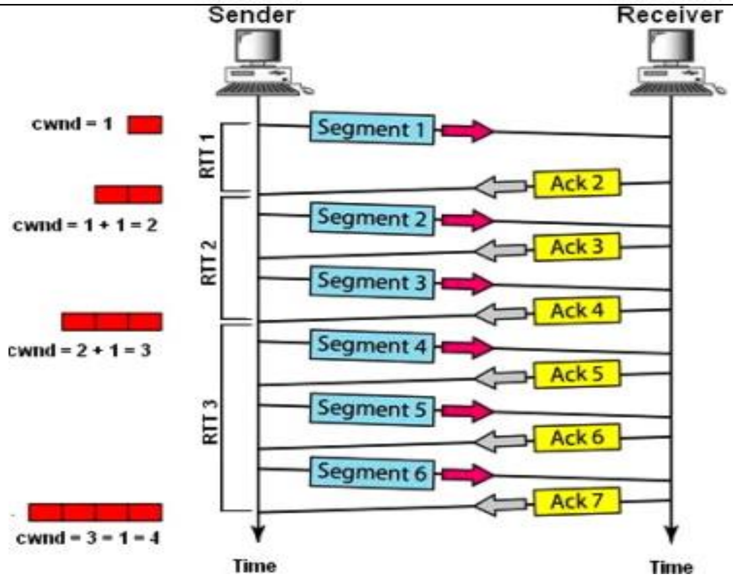
Congestion avoidance

- The congestion avoidance algorithm starts where the slow start stops. Once the congestion window reaches the congestion threshold level, then after that ***if an acknowledgement is received the window size is increased linearly,*** i.e., the window size doubling is avoided.

- The TCP increases its transmission rate linearly by adding one additional packet to its window at each transmission time.

- If congestion is detected at any point, the TCP reduces its transmission rate to half the previous value. Thus the TCP seesaws its way to the right transmission rate.

- This scheme is ***less aggressive*** than the slow-start phase (note the linear increase against the exponential growth in slow start).



Fast Retransmit/ Fast Recovery:

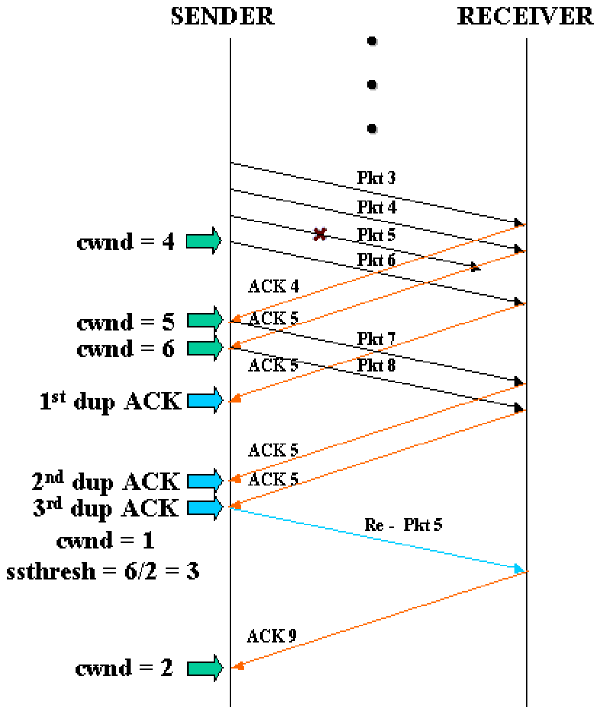
- Usually, a sender initiates a timer after transmitting a packet and sets the timeout value (RTO). RTO is calculated based on RTT. The sender waits for an acknowledgement of a transmitted packet from the receiver until the timer expires. When the timer expires, it retransmits the packet. This mechanism is called fast retransmission.
-
- The retransmission istriggered by the receipt of ***three duplicate copies*** of an acknowledgement for a packet received from the sender. Since duplicate acknowledgements also arise when a segment is received out of order, the sender waits for three copies of acknowledgements for the same packet.

- This is taken by the sender as the confirmed indication of a missed packet for starting to retransmit the particular packet. When retransmission occurs, the ***congestion window size is reduced by half.*** For example, if the current congestion window size is four segments, then it is set to two segments.

- Once the lost segment has been retransmitted, TCP tries to maintain the current data transmission rate by not going back to slow start. This is called fast recovery.

- In fast recovery, the congestion window size is incremented by three since the retransmission occurred after the third duplicate acknowledgement. This is construed to be the indication that three packets would have been successfully buffered at the receiver end.

- Thus, in fast recovery, compensation for the segments that have already been received by the receiver is carried out. If the acknowledgements are received smoothly, it is considered to be the indication that there is no congestion.



12. State some of the classical solutions to improve the efficiency of TCP in wireless?

1) Indirect TCP (I-TCP) , 2) Snooping TCP (S-TCP) , 3) Mobile TCP (M-TCP) ,
4) Fast retransmission/fast recovery, 5) Freeze TCP (F-TCP)

TCP in Mobile Networks

- The performance of TCP for wired networks are significantly different from wireless mobile networks. The main differences are much lower bandwidth, bandwidth fluctuations with time and also as a mobile host moves, higher delay, intermittent disconnections, high bit error rate, and poor link reliability.

- The traditional TCP are not valid in mobile (wireless) environments. This leads to poor performance of TCP in mixed wired-wireless environments.

Indirect TCP (I-TCP)

- It segments the connection between the fixed host and the mobile host into two different connections: the wired part and the wireless part (Fig. 5.7). The wired connection exists between the fixed host (FH) and the base station (BS) and the wireless part connection exists between the BS and the mobile host (MH).

- Thus, the base station maintains two separate TCP connections: one over the fixed network and the other over the wireless link. The wireless link usually has poor quality communication, but it gets hidden from the fixed network at the BS. When a packet is sent by FH to MH, the packet is received by BS first and then BS transmits it to the MH over the wireless link.

- If the mobile host moves out of the current BS region, the whole connection information and responsibilities that are with the current BS are transferred to the new BS.

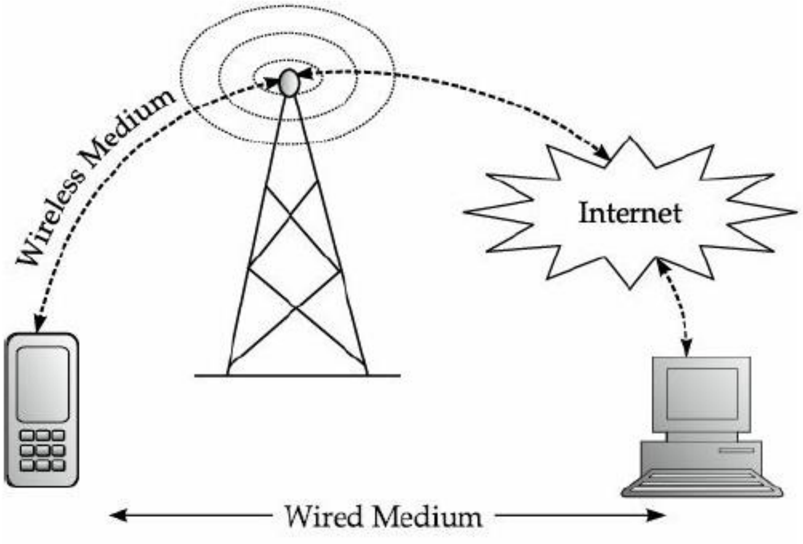


Figure 5.7 *A schematic of working of indirect-TCP.*

- ***Advantage:*** The Indirect-TCP does not need any changes to be made to the standard TCP protocol. By partitioning a TCP connection into two connections in I-TCP, the transmission errors in the wireless part would not propagate into the fixed network, thereby effectively achieving an increase in bandwidth over the fixed network.

- ***Disadvantage:*** The Indirect-TCP does not maintain the semantics of TCP as the FH gets the acknowledgement before the packet is delivered at MH. I-TCP does not maintain the end-to-end semantics of TCP and assumes that the application layer would ensure reliability.

Fast retransmission

- This approach was suggested to overcome the delay in transmissions caused due to intermittent disconnections such as those that occurs when a mobile host (MH) moves to a foreign agent (FA) during a TCP communication.

- The TCP transmission behavior after a disruption depends on its duration. The extremely short disruptions (lasting for a time much less than RTO) would appears as short bursts of packet losses.

- The TCP retransmits those packets for which the timeout occurs and recovers them without slow-start. However, for long disruptions (lasting for a time much greater than RTO), TCP resorts to slow-start. This results in inefficiency.

- A mobile host registers at a foreign agent, it starts sending duplicate acknowledgements. As is standard with TCP, three consecutive acknowledgements for the same TCP segment are inferred as a packet loss by the host-end TCP, and it is also inferred that the connection is live, thereby causing the fast retransmit behavior of TCP.

- ***Advantage*** - It reduces the time for the MH to get reconnected, otherwise FH would wait for RTO unnecessarily.

- The ***disadvantage*** of this approach is that it does not propose a general approach for TCP communication in mobile wireless networks. For example, it does not address the specific error characteristics of the wireless medium.

Snooping TCP (S-TCP)

- TCP performance improves by modifying the software at the base station while preserving the end-to-end TCP semantic. The modified software at the base station is known as ***snoop.***

- It monitors every packet that passes through the TCP connection in both directions, that is from MH to FH and vice versa.

- It buffers the TCP segments close to the MH. When congestion is detected during sending of packets from the FH to MH in the form of a ***duplicate acknowledgement or the timeout***, it locally retransmits the packets to MH if it has buffered the packet and hides the duplicate acknowledgement.

- An advantage of snooping TCP is that it maintains the TCP semantics by hiding the duplicate acknowledgements for the lost TCP segment and resends the packets locally. However, it also suffers from higher overheads incurred when MH moves from its current BS to a new BS, the packet buffered at the current BS need not be transferred to the new BS.

Mobile TCP (M-TCP)

- In mobile wireless networks, users would badly suffer from unacceptable delays in TCP communications and frequent disconnections caused by events such as signal fades, lack of bandwidth, handoff, unless these are explicitly handled by the protocol.

- The M-TCP protocol tries to avoid the sender window from shrinking or reverting to slow-start when bit errors cause a packet loss, as is attempted in I-TCP and snooping TCP.

- TCP connection between the fixed host and the mobile host is segmented into wired and wireless parts—the wired part connection between the fixed host (FH) and the supervisory host (SH) and the wireless part connection between the SH and the mobile host (MH).

- The SH supervises all the packets transmitted to MH and the acknowledgements sent by MH. It is also used as an interface between FH and MH and vice versa.

- When a packet is sent to FH by MH using SH, the wired part uses the normal unmodified TCP and the wireless part uses the modified version of TCP known as M-TCP to deliver data to MH.

- This packet is acknowledged only when the MH receives the packet. Thus, it maintains the TCP semantics, unlike the I-TCP.

- In case the acknowledgement is not received by FH, SH decides that MH is disconnected and sets the sender FH window size to zero. This ***prevents retransmission***. When SH notices that the MH is connected, it sets the full windows size of the sender FH.

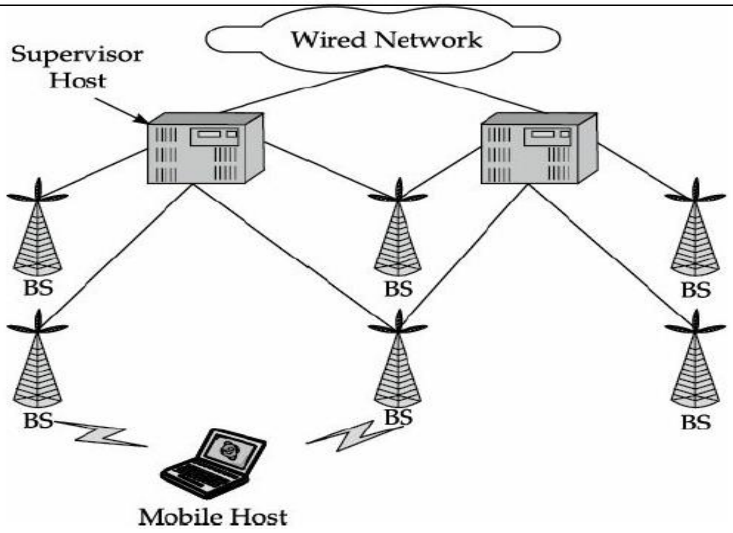


Figure 5.8 *A schematic of operation of the M-TCP protocol.*

- When MH moves from its current SH region to a new SH region, a state transfer take places, so that the new SH can maintain TCP connection between FH and MH.

Freeze-TCP

- The basic idea in this scheme is to "freeze" the TCP senders' streams, little before a disconnection is to occur. This is done by artificially sending a "Zero Windows Advertisement" informing the sender that the receiver cannot receive data at the moment. When the sender resumes its connectivity, the receiver can ***unfreeze the sender*** by sending the value of its actual receive window.

- ***Advantage:*** To avoid the slow-start period upon re-establishment of connectivity. It does not require the involvement of the intermediate nodes and hence it can be used if the IP payload is encrypted. Freeze-TCP use in Virtual Private Networks (VPNs).

TABLE - A Comparative Study of a few Important Protocols for Mobile Applications

TCP approach	*Mechanism used*	*Merits*	*Demerits*
Indirect TCP (I-TCP)	Segments the TCP connection into two	Simple • Isolation of wire and wireless links is possible	• Loss of the TCP semantics • Security problem
Snooping TCP (S-TCP)	Snooping of data and acknowledgements	• Transparency • MCA interaction	• Inadequate isolation of the wireless links • Security problem
Mobile TCP (M-TCP)	The segmented TCP connection can choke the sender through window sizes	• End-to-end segment is maintained • Handles frequent disconnections	• Poor isolation wireless links • Security Problem
Fast retransmission Fast recovery	It avoids slow-start after any roaming	Simple More efficient	Not transparent Mixed layers
Freeze-TCP	It freezes the TCP, later it resumes the TCP after reconnection	Works even when there are long interruptions	• Changes in TCP • MAC dependent

TCP in Multi-hop Wireless Networks

- The TCP-F (TCP feedback) protocol has been proposed for extending TCP to multiple-hop networks. In a mobile ad hoc network, a sender MH sends a packet to destination MH through the intermediate MH, since all the nodes of networks are MH.

- The MHs are free to move arbitrarily which changes the network topology unpredictably. If the normal TCP runs over in this network, there may be significant performance degradation at the transport layer. This happens because the normal TCP is unable to distinguish between packet loss resulting from link failure and packet loss due to congestion on the network. As a result, the normal TCP invokes the congestion control mechanism, even if a packet loss occurs due to link failure.

- When this happens, TCP waits for a longer time to retransmit the lost packet and this slows down the rate of transmission. The TCP-F addresses the problem caused by link failure due to mobility by performing a freezing action and limiting the re-transmissions.

- For simplicity, consider that a source MH is sending packets to a destination MH. As soon as an intermediate MH detects the disruption of route due to mobility of MH along that route, it sends a route failure notification (RFN) packet to the source MH and records that event.

- Each intermediate MH that receives the RFN packet invalidates the particular route and prevents the incoming packets intended for the destination MH passing through that route. If the intermediate node MH knows of an alternate route to destination MH, this alternative route can now be used to support further communication and the RFN is discarded.

- MH propagates the RFN towards the source MH. On receiving the RFN, the source MH completely stops sending further packets (new or retransmission), then it marks all its existing timers as invalid and freezes the send windows. The source MH remains in this state until it is notified of the restoration of the route through route re-establishment notification (RRN) packets.

13. Explain IP-in-IP, Minimal IP and GRE encapsulation methods.(May/June 2016)

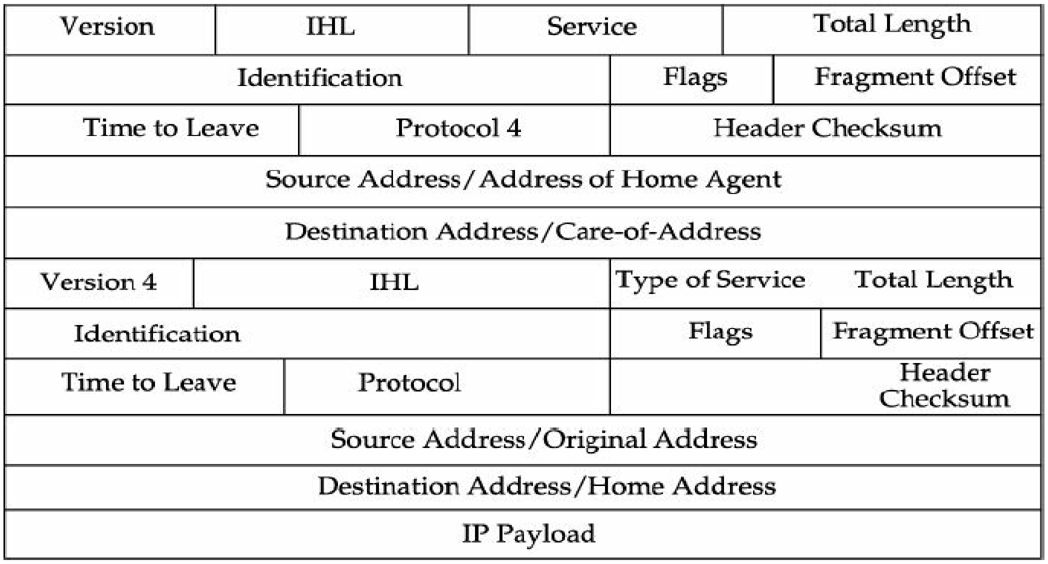
Tunnelling to the care-of-address

Tunnelling takes place to forward an IP datagram from the home agent to a care-of-address.

This involves carrying out the following steps:

- When a home agent receives a packet addressed to a mobile host, it forwards the packet to the care-of-address using IP-within-IP (encapsulation).
- Using IP-within-IP, the home agent inserts a new IP header in front of the IP header of any datagram.
- Destination address is set to the care-of-address.
- Source address is set to the home agent’s address.
- After stripping out the first header, IP processes the packet again.

The tunnelling operation in mobile IP and IP-within-IP encapsulation (embedding) are shown in Fig. 4.4.



Version	IHL	Service	Total Length
Identification		Flags	Fragment Offset
Time to Leave	Protocol 4	Header Checksum	
Source Address/Address of Home Agent			
Destination Address/Care-of-Address			
Version 4	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
Time to Leave	Protocol		Header Checksum
Source Address/Original Address			
Destination Address/Home Address			
IP Payload			

Figure 4.4 *IP encapsulation in mobile IP.*

Generic Routing Encapsulation (GRE)

GRE was developed as a tunneling tool meant to carry any OSI Layer 3 protocol over an IP network. In essence, GRE creates a private point-to-point connection like that of a virtual private network (VPN).

GRE works by encapsulating a payload - that is, an inner packet that needs to be delivered to a destination network -- inside an outer IP packet. GRE tunnel endpoints send payloads through GRE tunnels by routing encapsulated packets through intervening IP networks. Other IP routers along the way do not parse the payload (the inner packet); they only parse the outer IP packet as they forward it towards the GRE tunnel endpoint. Upon reaching the tunnel endpoint, GRE encapsulation is removed and the payload is forwarded along to its ultimate destination.

In contrast to IP-to-IP tunneling, GRE tunneling can transport multicast and IPv6 traffic between networks. Advantages of GRE tunnels include the following:

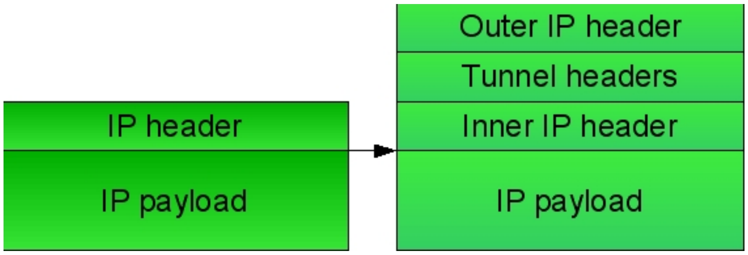
- GRE tunnels encase multiple protocols over a single-protocol backbone.
- GRE tunnels provide workarounds for networks with limited hops.
- GRE tunnels connect discontinuous sub-networks.
- GRE tunnels allow VPNs across wide area networks (WANs).

While GRE provides a stateless, private connection, it is not considered a secure protocol because it does not use encryption like the IP Security (IPsec) Encapsulating Security Payload (ESP), defined by RFC 2406.

Minimal IP

A minimal forwarding header is defined for datagrams which are not fragmented prior to encapsulating. Use of this encapsulating method is optional. Minimal encapsulation must not be used when an original datagram is already fragmented, since there is no room in the inner header to store fragmentation information.

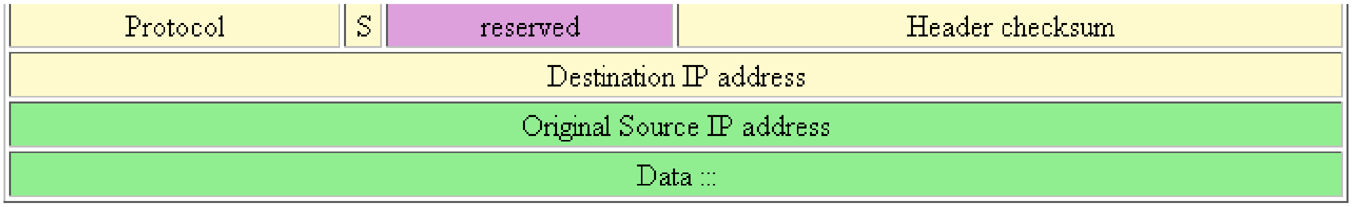
The minimal encapsulation process produces a datagram structured as shown below; the IP header of the original datagram is modified, then followed by the minimal forwarding header, followed by the unmodified IP payload of the original datagram.



Encapsulation is performed as follows.

The protocol field in the IP header is replaced by protocol number 55 for the minimal encapsulation protocol. The destination field in the IP header is replaced by the care-of address of the mobile node. If the encapsulating agent is not the original source of the datagram, the source field in the IP header is replaced by the IP address of the encapsulating agent.

When decapsulating a datagram, the fields in the forwarding header are restored to the IP header, and the forwarding header is removed from the datagram.



Protocol	S	reserved	Header checksum
Destination IP address			
Original Source IP address			
Data :::			

Protocol - Copied from the protocol field in the original IP header.

Source - Source field present bit, which indicates whether the Original
Source Address field is present.
0 not present.
1 present.

Reserved - Sent as zero; ignored on reception.

Header Checksum - The 16-bit one's complement of the one's complement sum of the encapsulation header. For computing the checksum, the checksum field is set to 0.

Original Destination Address - Copied from the destination field in the original IP header.

Original Source Address - Copied from the source field in the original IP header. Present only if the S-bit is set.

The encapsulating agent is free to use existing IP mechanisms appropriate for delivery of the encapsulated payload to the tunnel endpoint. In particular, this means that use of IP options and fragmentation are allowed, unless the "Don't Fragment" bit is set in the inner IP header.

<u>University Questions</u>

May/June 2015

Part A

1. Define DHCP? (Q.No:6)
2. What is encapsulation in Mobile IP? (Q.No:42)

Part B

(a) (i) With a diagram explain DHCP and its protocol architecture? (Q.No:5)

(ii) Explain IP-in-IP, Minimal IP and GRE encapsulation methods.(Q.No:13)

(Or)

(b) (i) With a neat diagram explain the architecture of TCP/IP? (Q.No:7)

(ii) Explain the various improvements in TCP performance with diagram (8)? (Q.No:11)

Nov/Dec 2016

Part A

1. Define COA? (Q.No:2)
2. Illustrate the use of BOOTP protocol? (Q.No:43)

Part B

(a) Explain about the key mechanism in Mobile IP? (Q.No:3)

(Or)

Give the comparison of various TCP advantages and Disadvantages wireless networking. (Q.No:10)