Unit III

3 Generations of Mobile Communication Technologies

Syllabus

First Generation Wireless Networks, Second Generation (2G) Wireless Cellular Networks, Major 2G standards, 2.5G Wireless Networks, Third Generation 3G Wireless Networks, Fourth Generation 4G wireless networks, Fifth Generation 5G wireless networks.

Contents

3.1 First Generation Wireless Networks

- The first analog, voice oriented cellular telephone system launched during 1970s and 1980s is referred to as first generation or 1G cellular technology.
- The first generation cellular system used analog frequency modulation schemes for transmission with two isolated bands downlink (from base station to mobile) and uplink (from mobile to base station) transmission. It uses Frequency Division Multiplexing (FDM) to increase system capacity.
- Different 1G cellular technologies are :
  1. Advanced Mobile Phone System (AMPS)
  2. Total Access Communication System (TACS)
  3. Nordic Mobile Telephone (NMT - 450)
  4. Nippon Telegraph and Telephone (NTT)
  5. Japanese TACS (JTACS)
- Table 3.1.1 summarizes different 1G analog cellular systems.

Standard	Forward band (MHz)	Reverse band (MHz)	Channel spacing (kHz)	Region	Comments
AMPS	824 - 849	869 - 894	30	United States	Also in Australia, Southeast Asia, Africa
TACS	890 - 915	935 - 960	25	EU	Later, bands were allocated to GSM
E-TACS	872 - 905	917 - 950	25	UK	
NMT 450	453 - 457.5	463 - 467.5	25	EU	
NMT 900	890 - 915	935 - 960	12.5	EU	Freq. overlapping; also in Africa and southeast Asia
C-450	450 - 455.74	460 - 465.74	10	Germany, Portugal	
RMTS	450 - 455	460 - 465	25	Italy	

Standard	Forward band (MHz)	Reverse band (MHz)	Channel spacing (kHz)	Region	Comments
Radiocom 2000	192.5 - 199.5	200.5 - 207.5	12.5	France	
	215.5 - 233.5	207.5 - 215.5			
	165.2 - 168.4	169.8 - 173			
	414.8 - 418	424.8 - 428			
NTT	925 - 940	870 - 885	25/6.25	Japan	First band is nationwide, others regional
	915 - 918.5	860 - 863.5	6.25		
	922 - 925	867 - 870	6.25		
JTACS/NTACS	915 - 925	860 - 870	25/12.5	Japan	All are regional
	898 - 901	843 - 846	25/12.5		
	918.5 - 922	863.5 - 867	12.5		

Table 3.1.1 : Existing 1G analog cellular systems

3.1.1 AMPS

- Due to increasing demand of mobile users, the available channels are not enough to accomodate new users. The solution can not be simply to assign new frequencies as the spectrum space for new approach to mobile telephony was needed. Hence a system called Advanced Mobile Telephone System (AMPS) was deployed in 1983 in Chicago.
- AMPS uses cellular concept based on many repeaters. The cellular radio technology was more efficient and can provide high quality mobile service to maximum subscribers.
- A total 40 MHz of spectrum bandwidth is 800 MHz band was allocated to AMPS. The AMPS uses seven cells reuse pattern with provisions for sectoring and cell splitting to increase capacity. There are many repeaters responsible for coverage in a cell. The cell shapes are hexagonal ideally as shown in Fig. 3.1.1.

Fig. 3.1.1 : Cell structure

- All the cell sites are interconnected by fiber optics or microwave link to Mobile Telephone Switching Office (MTSO) or Mobile Switching Center (MSC). All the calls are routed through cell center and MTSO. No mobile users are directly connected.
- Each cell site transmitter operates at comparatively low power frequency reuse is possible after some distance. The available bandwidth is divided amongs the cells.

3.1.2 Cellular Carriers and Frequencies

- Each carrier has 395 duplex voice channels and 21 control channels to setup calls and administer housekeeping activities like registration and paging. For voice modulation narrowband analog FM is used with maximum frequency deviation of 12 kHz and channel spacing of 30 kHz.
- Two carriers are used known as A and B carrier. A represents non-wireline carrier and B is for wire line carrier. Each carriers are assigned 832 frequencies (790 voice and 42 data). A pair of frequency is used to create one channel. Transmission from base to mobile is called as **forward channel** and transmission from mobile to base is called as **reverse channel.**
- In North American system, reverse channel transmission uses frequency in range of 824 MHz to 849 MHz and forward channel transmission uses frequency in the range of 869 MHz to 894 MHz.

3.1.3 Channel Allocation

- The control channels are used to allocate voice channels to the user. After dialling a telephone number and then pressing send button, the phone scans all the control channel frequencies for a strongest signal. The cell phone transmits its corresponding control channel and once the call is established the cell sites assigns it a clear voice channel.
- During conversation, the adjacent cell monitors the signal strength, when signal strength is greater in an adjacent cell, the call is transferred to that cell. This process is called **handoff.** Thus handoff requires a change in frequency for mobile phone.

3.1.4 AMPS Operation for Mobile Originated Calls

- It is a mobile to land call. If a mobile subscriber wants to make a call, there is exchange of several messages over the control channels such as :
  1. Handshaking operations
  2. Signaling operations
  3. Service requests

- Fig. 3.1.2 shows steps involved in mobile originated calls.

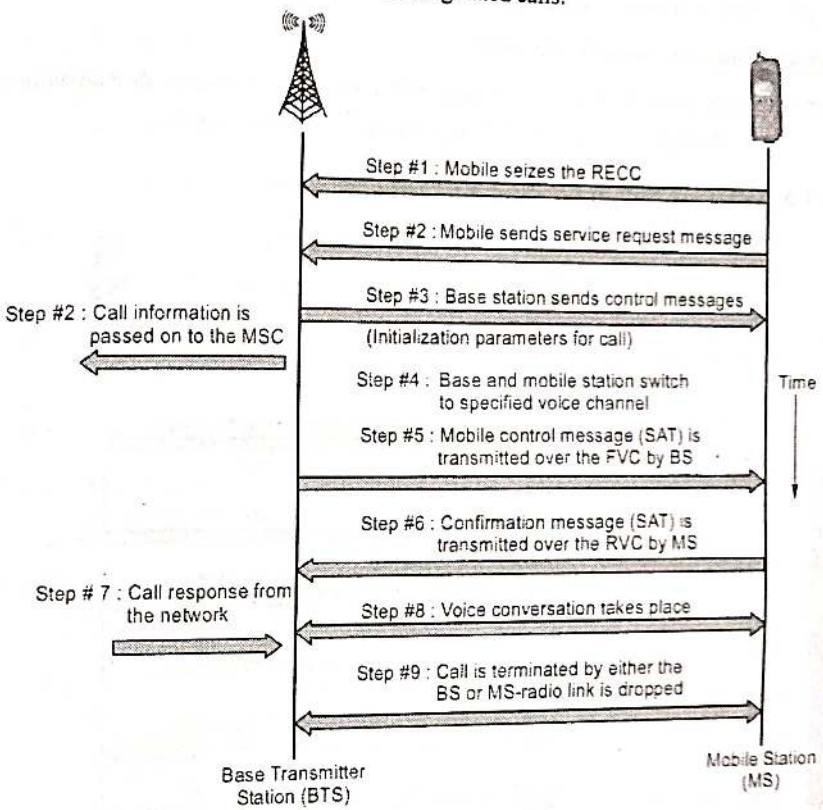

Fig. 3.1.2 : AMPS mobile originated calls

Step 1 : Mobile seizes to Reverse Control Channel (RECC).

Step 2 : Once mobile seizes the RECC, it starts transmitting service request message to base station over RECC.

Step 3 : On granting the service request it sends initial voice channel designation message.

Step 4 : Base and mobile stations switched their communication to the voice channel specified.

Step 5 : The base station sends a mobile control message over Forward Voice Channel (FVC) with Supervisory Audio Tones (SAT).

Step 6 : Mobile station sends transmits confirmation message (SAT) over Reverse Voice Channel (RVC).

Step 7 : Mobile station awaits completion of call with response from network.

Step 8 : Voice conversation takes place.

Step 9 : Either base station sends a release order message or mobile sends a signalling tone at which point the BS and MS drop the voice channel radio link.

3.1.5 AMPS Operation for Mobile Terminated Calls

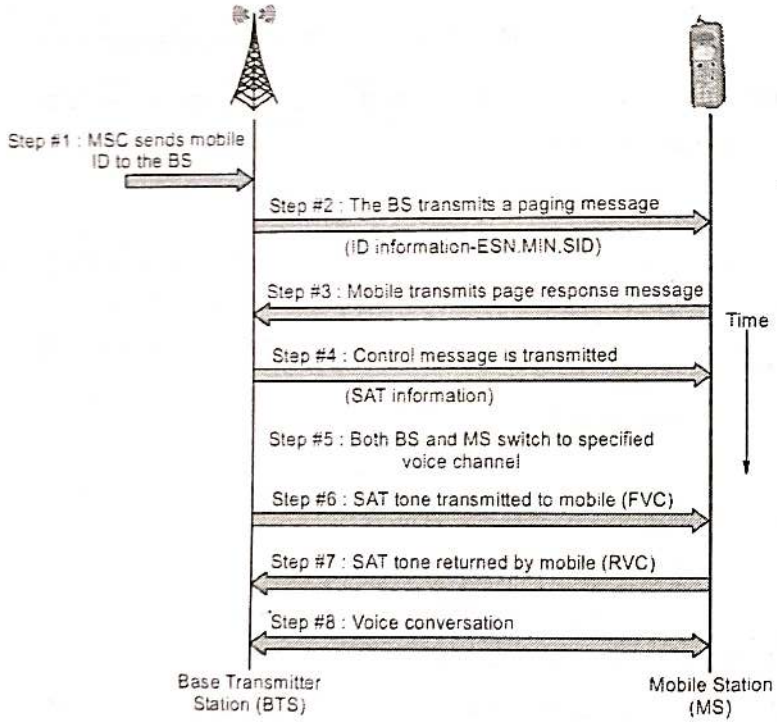

Fig. 3.1.3 : AMPS mobile terminated calls

- The mobile terminated calls are land-to-mobile and mobile-to-mobile calls. Various phases involved in mobile terminated calls are :
  1. Paging
  2. ID information exchange
  3. Signaling
  4. Control messages

- Fig. 3.1.3 shows steps involved in mobile terminated calls.

Step 1 : The Main Switching Centre (MSC) sends ID of Mobile Station (MS) to Base Station (BS).

Step 2 : The Base Station (BS) transmits a paging message along with ID information ESN, MIN, SID.

Step 3 : The Mobile Station (MS) responds to the page by returning ID over Reverse Control Channel (RECC).

Step 4 : Control message is sent by Base Station (BS) over Forward Control Channel (FOCC).

Step 5 : Both Base Station (BS) and Mobile Station (MS) switch to voice channel.

Step 6 : Supervisory Audio Tones (SAT) transmitted to Mobile Station (MS) over Forward Voice Channel (FVC).

Step 7 : Supervisory Audio Tones (SAT) returned by Mobile Station (MS) over Reverse Voice Channel (RVC).

Step 8 : After last handshake signal, the traffic channel is opened to conversation between Base Station (BS) and Mobile Station (MS).

3.1.6 AMPS Hand-off Operation

- The hand-off operations occur in a cellular system when Mobile Station (MS) to another cell.
- The hand-off operation in AMPS involves following :
  1. Handshaking operations
  2. Signal strength measurements
  3. MSC operations during hand-off
  4. Confirmation messages.
- Fig. 3.1.4 illustrates various control messages sequence of hand-off operation in AMPS system. (Refer Fig. 3.1.4 on next page)

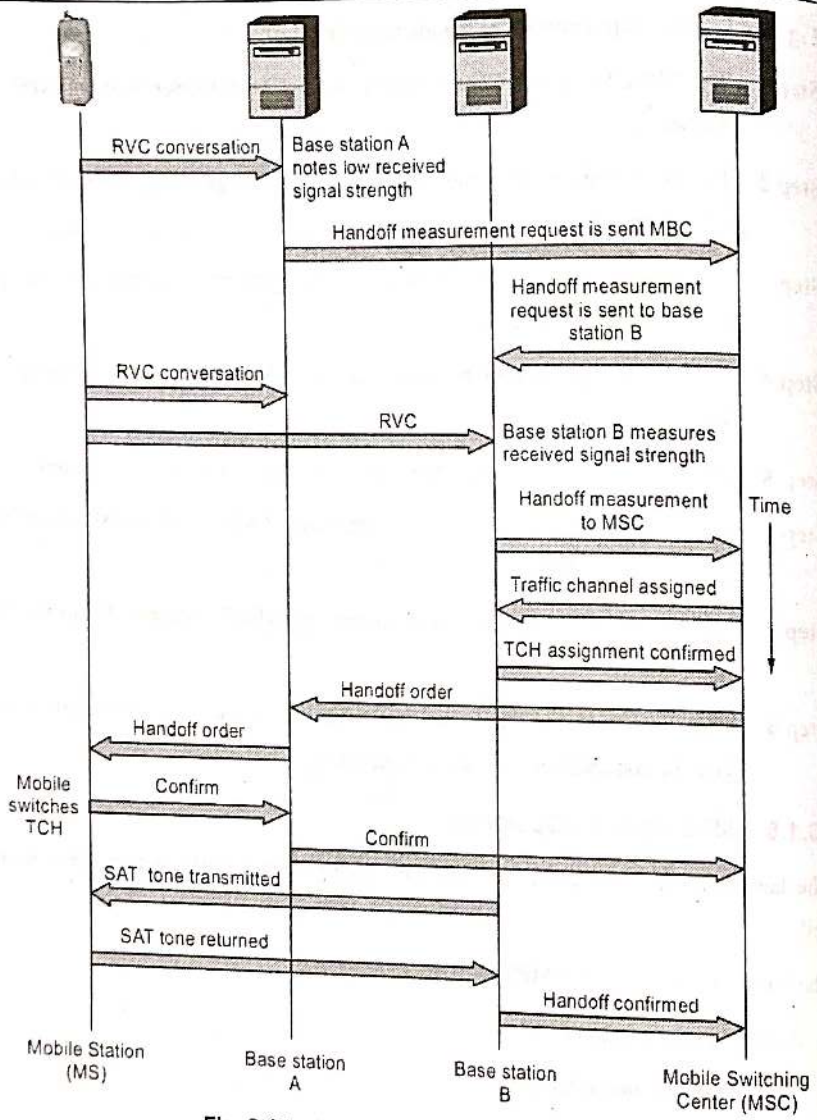

Fig. 3.1.4 : Hand-off operation in AMPS

3.2 Second Generation (2G) Wireless Cellular Networks

- 2G standards rely on digital formats TDMA/FDD and CDMA/FDD multiple access techniques (FDD - Frequency Division Duplexing). 2G cellular systems provide more facilities and attractive features than 1G systems.

- Features of 2G cellular systems are :
  1. Better speech quality.
  2. High speed data application.
  3. Efficient spectrum utilization.
  4. Supports multiple users.
- Different 2G cellular technologies are :

A] TDMA :

1. Interim Standard - 136 (IS - 136)
2. Global System for Mobile (GSM)
3. Pacific Digital Cellular (PDC).

B] CDMA :

1. Interim Standard - 95 (CDMA - one)

- Table 3.2.1 summarizes major 2G digital cellular standards.

System	GSM	IS-54	JOC	IS-95
Region	Europe / Asia	United States	Japan	United States/Asia
Access method	TDMA/FDD	TDMA/FDD	TDMA/FDD	CDMA/FDD
Modulation scheme	GMSK	$\pi/4$ - DQPSK	$\pi/4$ - DQPSK	SQPSK/QPSK
Frequency band (MHz)	935 - 960	869 - 894	810 - 826	869 - 894
	890 - 915	824 - 849	940 - 956	824 - 849
			1,477 - 1,489	
			1,429 - 1,441	
			1,501 - 1,513	
			1,453 - 1,465	
Carrier spacing (kHz)	200	30	25	1,250
Bearer channels/carrier	8	3	3	Variable
Channel bit rate (kbps)	270.833	48.6	42	1,228.8
Speech coding	13 kbps	8 kbps	8 kbps	1 - 8 kbps (variable)
Frame-duration (ms)	4.615	40	20	20

Table 3.2.1 : 2G digital cellular standards

3.3 2.5G Cellular System

- 2.5G is an upgradation of existing 2G cellular system without any additional frequency spectrum and change in technology.
- Different 2.5G cellular system standards include :
  1. CDPD (Cellular Digital Packet Data)
  2. HSCSD (High Speed Circuit Switched Data)
  3. GPRS (General Packet Radio Service).

3.3.1 Mobile Data Services

- Various mobile data services technologies are : ARDIS, Mobitex, CDPD, TETRA, GPRS and Metricom. Table 3.3.1 compares different parameters of these technologies.

System	ARDIS	Mobitex	CDPD	TETRA	GPRS	Metricom
Frequency band (MHz)	800 bands 45 kHz	935 - 940 896 - 961	869 - 894 824 - 849	380 - 383 390 - 393	890 - 915 935 - 960	902 - 928 ISM bands
Channel bit rate (kbps)	19.2	8.0	19.2	36	200	100
RF channel spacing	25 kHz	12.5 kHz	30 kHz	25 kHz	200 kHz	160 kHz
Channel access / Multiuser access	FDMA / DSMA	FDMA / Dynamic S-ALOHA	FDMA / DSMA	FDMA / DSMA	FDMA / TDMA / Reservn.	FHSS / BTMA
Modulation technique	4-FSK	GMSK	GMSK	$\pi/4$-QPSK	GMSK	GMSK

Table 3.3.1

3.4 3G Cellular System

- 3G is a cellular system that supports higher data services, advanced multimedia services and global roaming. The 3G system ensures an efficient wireless access with high performance quality by using intelligent new protocols.
- Different 3G cellular system standards include :
  1. IMT 2000 and UMTS 2. CDMA 2000.

3.5 4G Cellular System

- The goal of 4G cellular system is convergence of wireless mobile with wireless access communication technologies. A new converged system will be an improvement in bandwidth efficiency, dynamic bandwidth allocation, quality of service and security.
- The 4G cellular system will require an all IP architecture and connectivity for any one, any where and at all the time. The expected data rate is above 20 Mbps which can match wireless ATM speed.

3.5.1 Characteristics of 4G

1. Fully converged services

- A wide range of services will be available to the mobile user conveniently and securely via the 4G Core Network. Personal communications, information systems and entertainment will seem to be merged into a seamless pool of content.

2. Ubiquitous mobile access

- 4G aims to provide access to multimedia services anytime anywhere. Devices will not simply rely on cellular reception. Improved radio access technology as well as integration of all types of communication networks allows for virtually constant connectivity to the 4G core backbone. Mobile handsets will be intelligent and software-reconfigurable on the fly to allow them to interface with different types of networks on the move. Also, there will be full cross compatibility on a world-wide scale since each type of network has a gateway to the IP backbone.

3. Software dependency

- Advanced software systems are employed for all purposes - network operation, service provision, interfacing and integration, etc. Not only the Core Network but the mobile devices will be highly intelligent as well as re-configurable via software.

4. Diverse user devices

- A defining feature of 4G will be the proliferation of a vast array of devices that are capable of accessing the 4G backbone. Wireless capabilities will be embedded into devices that we wouldn't even consider today. Not only personal devices like phones, PDAs, laptops, etc. but also sensors, embedded controllers and other specialised equipment. The point behind this is to allow them to autonomously communicate with each other. By building in sophisticated software, they will be able to automatically initiate timely actions. 2G enabled mobile person-to-person communications while 3G is opening the door to person-to-machine communication with mobile Internet. 4G introduces another dimension with machine-to-machine communication.

5. Autonomous networks

- While user devices are highly intelligent, the core network will also be very sophisticated. It will be capable of managing itself and dynamically adapting to changing network conditions and user preferences for seamless communication. Apart from evolved mobility management, connection control, hand-over mechanisms, etc, dynamic bandwidth allocation will make far more efficient use of the available radio spectrum.

3.5.2 Comparison of 1G, 2G, 3G and 4G System

Technology/Features	1G	2G/2.5G	3G	4G
Start/Deployment	1970/1984	1980/1999	1990/2002	2000/2010
Data bandwidth	2 kbps	14.4-64 kbps	2 Mbps	200 Mbps to 1 Gbps for low mobility
Standards	AMPS	2G : TDMA, CDMA, GSM 2.5G : GPRS. EDGE , 1xRTT	WCDMA, CDMA-2000	Single unified standard
Technology	Analog cellular technology	Digital cellular technology	Broadband width CDMA, IP technology	Unified IP and seamless combination of broadband LAN/WAN/ PAN and WLAN
Service	Mobile telephony (voice)	2G : Digital voice, short messaging 2.5G : Higher capacity packetized data	Integrated high quality audio, video and data	Dynamic information access wearable devices

Technology/Features	1G	2G/2.5G	3G	4G
Multiplexing	FDMA	TDMA, CDMA	CDMA	CDMA
Switching	Circuit	2G : Circuit 2.5G : Circuit for access network and air interface; packet for core network and data	Packet except circuit for air interface	All packet
Core network	PSTN	PSTN	Packet network	Internet

3.6 Fifth Generation 5G Wireless Networks

- 5G isn't just an incremental improvement over 4G - it's the next major evolution of mobile communication technology with performance improvements of several orders of magnitude over today's networks.
- 5G does not replace 4G, it simply enables a huge diversity of tasks that 4G cannot perform.
- 4G will continue to advance in parallel with 5G, as the network to support more routine tasks.
- 5G will enable services yet to be imagined, in a world where national economies are driven by sophisticated communications networks.

3.6.1 Features of 5G

- Immersive 5G services : Virtual Reality/Augmented Reality (VR/AR), massive contents streaming.
- Intelligent 5G services : User-centric computing, crowded area services.
- Omnipresent 5G services : Internet of things.
- Autonomous 5G services : Smart transportation, drones, robots.
- Public 5G services : Disaster monitoring, private security/public safety, emergency services.

3.6.2 Comparison of 4G and 5G

- Fig. 3.6.1 shows comparison of 4G and 5G and Table 3.6.1 show comparison.

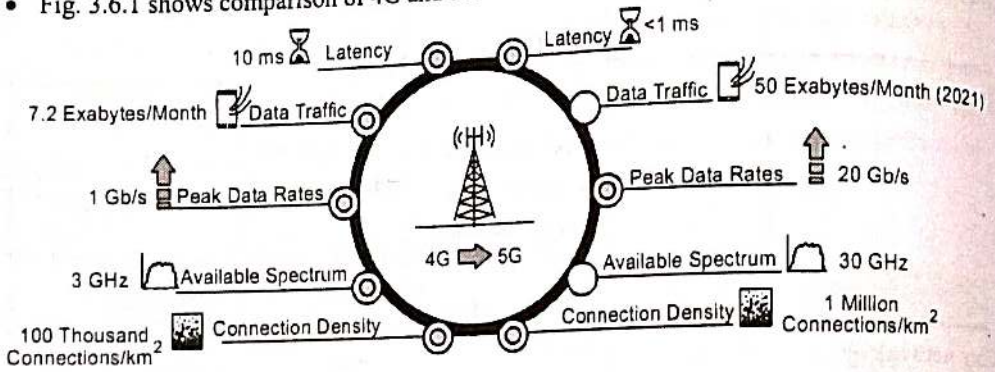

Fig. 3.6.1 : Comparing 4G and 5G

Parameters	4G	5G
Latency	10 ms	Less than 1 ms
Peak data rates	1 Gbps	20 Gbps
Number of mobile connections	8 bilion (2016)	11 bilion (2021)
Channel bandwidth	20 MHz	100 MHz below 6 GHz
	200 kHz (for Cat-NB 1 loT	400 MHz above 6 GHz.
Frequency band	600 MHz to 5.925 GHz	600 MHz-mm Wave (for example 28 GHz 39 GHz and onword to 80 GHz.
Uplink waveform	Single-camer frequency division multiple access (SC-FDMA)	Option for cyclic prefix orthogonal frequency division multiplexing (CP-OFDM)
User Equipment (UE) transmitted power	+23 decibel-miliwatts (dBm) except 2.5 GHz time-division duplexing (TDD) Band 41 where + 26 dBm, HPUE is allowed loT haa a lower power-class at + 20 dBm.	+26 dBm for less than 6 GHz 5G bands at and above 2.5 GHz.

Table 3.6.1

3.6.3 Opportunities and Requirements of 5G

1. **Enhanced Mobile Broadband (eMBB)** requiring hundreds of megahertz (MHz) of channel bandwidth using new frequencies for mobile wireless - from 2.5 gigahertz (GHz) for 4G LTE Pro and 3.5 GHz for 5G, to tens of gigahertz and beyond into the millimeter wave (mmWave) spectrum.
2. **Ultra efficient** for streaming data, taking full advantage of **Carrier Aggregation (CA)** and massive Multiple Input/Multiple Output (MIMO).
3. **Fixed wireless,** giving more choices to get 20 gigabit per second (Gbps) connections to your home and business.
4. **Wireless infrastructure,** using beam steering and **high-power Gallium Nitride (GaN),** ideally suited to adaptive-array steerable antennas.
5. **Low latency** for real-time connections enabling **autonomous vehicles** and Augmented Reality/Virtual Reality (AR/VR).
6. **Internet of Things (IoT)** connecting more than a trillion devices to the Internet in the next ten years with extremely low data rates, battery life greater than ten years and the longest possible communication range.

Technical requirements for 5G core networks

- The core network requirements are described in three aspects to support various 5G services.
  1. Functional requirements (F),
  2. Architectural requirements (A)
  3. Operational requirements (O).
- Table 3.6.2 shows technical requirements of 5G network and its brief description.

	Technical Requirement	Brief Description
F1	Seamless mobility	Shall support seamless mobility regardless of the cell types and RATs where the macro-cell BSs, small-cell BSs, WLANAPs. and relay stations are mixed and overlapped.
F2	Wired/wireless terminal switching	Shall support terminal and/or session mobility to provide fast handover between wireless and wired terminals

	Technical Requirement	Brief Description
F3	Context-aware best connection	Shall utilize the various context information (device, user, environment, network) to provide always best connection / service.
F4	Single ID for multiple access	Shall recognize a mobile terminal as a single entity regardless of its access network.
A1	Distributed architecture	Shall support the distributed network architecture to accommodate anticipated 1000 times of traffic.
A2	Lightweight signaling	Shall have lightweight signaling to support a variety of terminals such as massive MTC terminal.
A3	Multiple RAT inter working	Shall have architecture to support 'Flow over Multi-RAT' to provide the high volume service with low cost and guarantee the service continuity in spite of the bandwidth deficiency in a wireless access.
A4	Fine-grained location tracking	Shall have function to trace the mobile terminal location in a fine granularity in order to provide advanced location based service.
01	Flexible reconfiguration and upgrade	Shall provide virtualization environment and support to reconfigure and upgrade the core network at low cost without changing the physical network infrastructure.
02	Network on-demand	Shall be able to build the network based on the QoS/QoE, charging and service characteristics.

RATs (radio access technologies)

Table 3.6.2

3.6.4 5G Core Network Architecture

- Fig. 3.6.2 shows a software-centric 5G core and access network architecture designed to support various 5G mobile services.
- The fronthaul and the backhaul represent the interface between Access Units (AUs) and the edge cloud and the interface between the edge cloud and the core cloud, respectively.
- The AU-Cloud Unit (CU) configuration is similar to the conventional Radio Unit-Digital Unit (RU-DU) configuration of a Cloud Radio Access Network (C-RAN) in the 3GPP-LTE system.

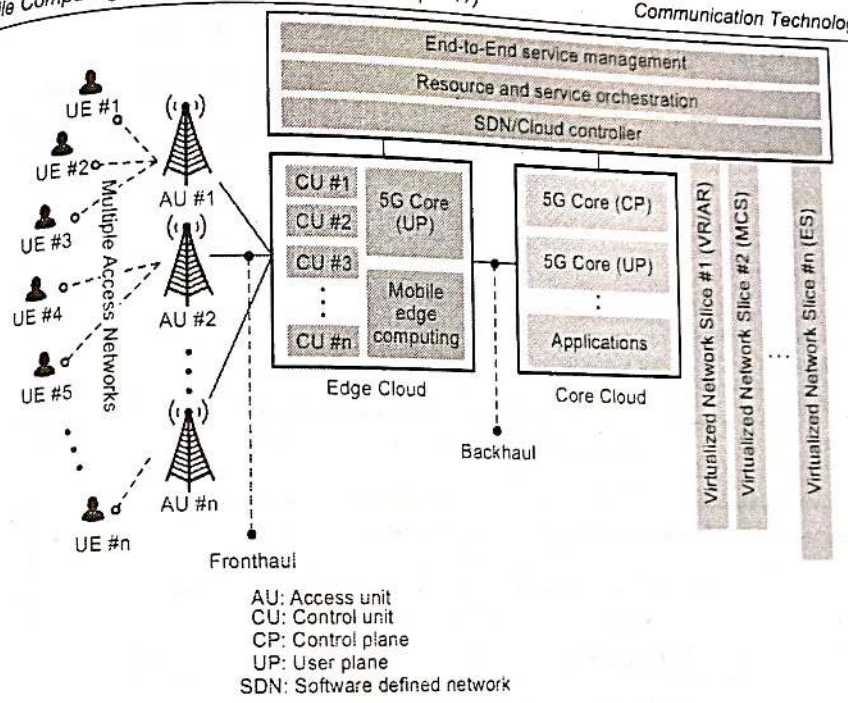

Fig. 3.6.2 : Software-centric 5G core and access network architecture

- The legacy RUs are remote RF units located at cell-sites and centralized DUs are connected with these RUs and have relatively heavy functionalities regarding the Medium Access Control (MAC) layer, Radio Link Control (RLC) layer and the Packet Data Convergence Protocol (PDCP) layer, compared with RUs.
- Because the fronthaul data overhead between RUs and DUs is predicted to increase explosively, several functionalities of DUs will be moved into RUs at cell-sites.
- Therefore, this modified cell-site unit in the 5G core network the AU and CUs can be considered as the lightweight DUs.
- The Mobile Edge Computing (MEC) entity in the edge cloud provides application developers and content providers with cloud computing capabilities and a 5G service environment at the edge of the 5G mobile networks.
- The MEC technology is leveraged to support ultra-low latency and high-bandwidth services.
- In the 5G core network architecture, the separation of the Control Plane (CP) and the User Plane (UP) is one of the most important features in order to increase operational efficiency, as well as to improve network simplicity and flexibility.

Relationship between 5G services and 5G core network requirements

- Table 3.6.3 shows the relation between 5G services and 5G core network requirement.

Service Category		F1	F2	F3	F4	A1	A2	A3	A4	01	02
Innersive 5G Service	Virtual Reality and Augmented Reality	✓	✓	✓						✓	✓
	Massive Contents Streaming	✓	✓			✓				✓	✓
Intelligent 5G Service	User Centric Computing		✓	✓						✓	✓
	Growded Area service	✓		✓		✓				✓	✓
Ommipresent 5G Service	Internet of Things.		✓	✓		✓	✓			✓	✓
Autonomous 5G Service	Smart Transportation	✓	✓	✓	✓				✓	✓	✓
	Smart Drone	✓		✓					✓	✓	✓
	Smart Robot			✓			✓	✓		✓	✓
Public 5G Service	Disaster Monitoring			✓				✓	✓	✓	✓
	Private Safety and Public Security			✓				✓	✓	✓	✓
	Emergency Service	✓		✓				✓	✓	✓	✓

Table 3.6.3

3.6.5 Disruptive Technologies for 5G

- Five technologies for 5G that could lead to both architectural and component disruptions:
  1) Device-centric architectures,
  2) Millimeter wave;
  3) Massive MIMO;
  4) Smarter devices; and
  5) Native support for machine - to - machine communications.

- The key ideas for each technology are described, along with their potential impact on 5G and the research challenges that remain.

1) **Device-centric architectures :** The base - station - centric architecture of cellular systems may change in 5G. It may be time to reconsider such concepts as uplink and downlink, as well as control and data channels. 5G systems will use nodes on an ad hoc basis.

2) **Millimeter wave (mmWave) :** While spectrum has become scarce at microwave frequencies, it is plentiful in the mmWave region. Such a spectrum "el Dorado" has led to an mmWave "gold rush". Although far from being fully understood, mmWave technologies have already been standardized for short-range services (IEEE 802.11ad) and deployed for niche applications such as small-cell backhaul.

3) **Massive MIMO :** Massive multiple-input multiple-output (MIMO) proposes using a very large number of antennas to spatially multiplex data. Massive MIMO may require major architectural changes, particularly in the design of macro base stations and it may also lead to new types of deployments.

4) **Smarter devices :** 2G-3G-4G cellular networks were built under the design premise of having complete control at the infrastructure side. The proposal is for 5G systems to drop this design assumption and exploit intelligence at the device side within different layers of the software protocol stack. For example, one could allow device-to-device (D2D) connectivity or exploit smart caching at the mobile smart-phone side. While this design philosophy mainly requires a change at the node level (component change), it also has implications at the architectural level.

5) **Native support for Machine-to-Machine (M2M) communication :** A native inclusion of M2M communication in 5G has three main requirements : Support of a massive number of low-data-rate devices, sustaining a minimal data rate in virtually all circumstances and very-low-latency data transfer. Addressing these requirements in 5G requires new methods and ideas at both the component and architectural levels.

❑❑❑

Unit IV

4 Mobile Network Layer

Syllabus

Mobile IP : Goals, assumptions and requirements, Entities and Terminology, IP packet delivery, Agent advertisement and discovery, Registration, Tunnelling and Encapsulation, Optimizations, Reverse tunnelling,

IPv6 : DHCP, **AdHoc networks :** Routing, Proactive protocol-DSDV, **Reactive Routing Protocols :** DSR, AODV, Hybrid routing –ZRP, **Multicast Routing :** ODMRP, Vehicular Ad Hoc networks (VANET) MANET Vs VANET Security.

Contents

4.1 Mobile IP

- Mobile IP provides network layer mobility.
- When user is mobile using laptop with Wi-Fi, the IP address changes with user movement, forcing to terminate connection. This situation of mobility with data connection alive is handled by mobile IP technology. Mobile IP provides seamless roaming.
- The mobile IP signifies that, while a user is connected to applications across the internet and the user's point of attachment changes dynamically, all connections are maintained despite the changes in underlying network properties.
- Mobile IP extends the home network over the entire Internet.
- Mobile IP allows the mobile node to use two IP addresses called home address and care of address. The home address is static and known to everybody as the identity of the host. The care of address changes at each new point of attachment.

4.1.1 Goals of Routing Protocol and Mobile IP

[A] Goals of routing protocol -

- Important goals of routing protocol are -
  1. Decrease routing-related overhead
  2. Find short routes
  3. Find stable routes (despite mobility)

[B] Goal of mobile IP

- Supporting end-system mobility while maintaining scalability, efficiency and compatibility in all respects with existing systems.

4.1.2 Requirements of Mobile IP

- Some of common requirements of mobile IP are-

1. Compatibility

- Mobile IP must not require special media or MAC / LLC protocols, so it must use the same interfaces and mechanisms to access the lower layers.
- No changes to current end - systems and routers required.
- Mobile end - systems can communicate with fixed systems.

2. Transparency

- Mobility should remain invisible for many higher layer protocols and applications.
- Higher layers should continue to work even if the mobile computer has changed its point of attachment to the network.

3. Efficiency and scalability

- Only little additional messages to the mobile system required (connection typically via a low bandwidth radio link)
- World - wide support of a large number of mobile systems.

4. Security

- Authentication of all registration messages.

4.1.3 Entities and Terminology

1. Mobile Node (MN)

- A system (node) that can change the point of connection to the network without changing its IP address is referred as **Mobile Node (MN)**.

2. Home Agent (HA)

- **Home Agent (HA)** is system in the home network of the MN, typically a router.
- Home agent (HA) registers the location of the MN, tunnels IP datagrams to the Care-of Address (COA).

3. Foreign Agent (FA)

- **Foreign Agent (FA)** is system in the current foreign network of the MN, typically a router.
- Foreign Agent (FA) forwards the tunneled datagrams to the MN, typically also the default router for the MN.

4. Care-of Address (COA)

- **Care-of Address (COA)** is address of the current tunnel end-point for the MN (at FA or MN).
- **Care-of Address (COA)** provides actual location of the MN from an IP point of view

5. Correspondent Node (CN) is communication partner.

4.1.4 Features of Mobile IP

1. Mobile IP allows a host to be reachable at the same address, even as it changes its location.
2. Mobile IP makes it seem as one network extends over the entire Internet.
3. Mobile IP provides continuous connectivity, seamless roaming even while network applications are running.
4. Mobile IP is fully transparent to the user.

Review Questions

1. Define the following mobile IP terms :
   a. Mobile Node b. Foreign Agent
   c. Foreign Network d. Home Network e. Home agent
2. Explain the desirable features of Mobile IP.
3. Define binding. Explain the messages transmitted in Optimized mobile IP.
4. What is mobile IP ?

4.2 IP Packet Delivery

- Suppose a mobile node (A) wants to connect to another host (server X). Fig. 4.2.1 Illustrates the working of mobile IP.

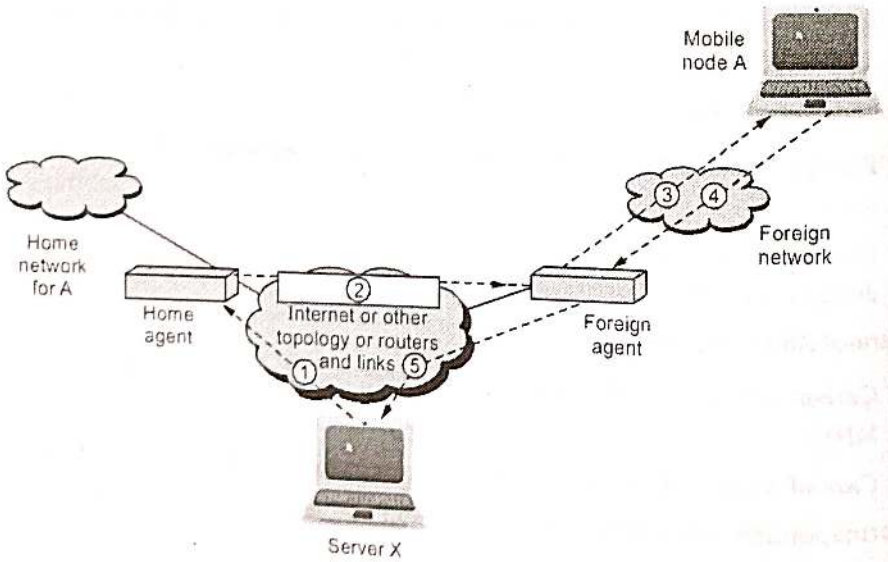

Fig. 4.2.1 : Mobile IP

- Host (server X) wants to transmit an IP datagram to mobile node A. The home address of A is known to X. The host X does not know whether A is in home network or any other network. Therefore, host X sends the packet to A with A's home address as the destination IP address in the IP header.
- The IP datagram is routed to A's home network. At A's home network, the incoming IP datagram is intercepted by home agent. The home agent discovers that A is in a foreign network. A care of address is allocated to A by the foreign network and available with the home agent.
- The home agent encapsulates the entire datagram inside a new IP datagram, with A's care of address in the IP header. This new datagram with the care of address as the destination address is retransmitted by the home agent.
- The incoming IP datagram is intercepted by the foreign agent at foreign network. The foreign agent is the counterpart of the home agent in the foreign network.
- The foreign agent strips off the outer IP header and delivers the original datagram to A. The mobile node A intends to respond to this message and sends traffic to X. The IP datagram from A to X travels directly across the network, using X's IP address as the destination address.
- To support the entire operation, the mobile IP should have three basic qualities -
  1. **Discovery :** The mobile node uses a discovery procedure to identify prospective home agents and foreign agents.
  2. **Registration :** A mobile node uses a registration procedure to inform its home agent of its care-of- address.
  3. **Tunnelling :** Tunnelling procedure is used to forward IP datagrams from a home address to a care of address.

Review Question

1. Discuss the process of packet delivery by suitable example.

4.3 Key Mechanism in Mobile IP

- Home agents and foreign agents advertise their presence on any attached links by periodically multicasting or broadcasting special mobile IP messages called agent advertisements.
- Mobile nodes listen to these agent advertisements and examine their contents to determine whether they are connected to their home link or a foreign link.
- A mobile node connected to a foreign link acquires a care-of address. A foreign agent care-of address can be read from one of the fields within the foreign agent's agent advertisement.
- A collocated care-of address must be acquired by some assignment procedure, such as Dynamic Host Configuration Protocol (DHCP), the Point-to-Point protocol's IP Control Protocol (IPCP) or manual configuration.
- The mobile IP Registers the care-of address acquired previously with its home agent, using a message-exchange defined by Mobile IP. It asks for service from a foreign agent, if one is present on the link. In order to prevent Denial-of-Service attacks, the registration messages are required to be authenticated.
- The home agent or some other router on the home link advertises reachability to the network-prefix of the mobile node's home address, thus attracting packets that are destined to the mobile node's home address.
- The home agent intercepts these packets and tunnels them to the care-of address that the mobile node registered previously.
- At the care-of address - at either the foreign agent or one of the interfaces of the mobile node itself - the original packet is extracted from the tunnel and then delivered to the mobile node.
- In the reverse direction, packets sent by the mobile node are routed directly to their destination, without any need for tunneling. The Foreign Agent serves as a default router for all packets generated by visiting node.

4.3.1 Agent Advertisement and Discovery

- One initial problem of an MN after moving is how to find a foreign agent.
- To communicate with a remote host, a mobile host goes through three phases : Agent discovery, registration and data transfer.

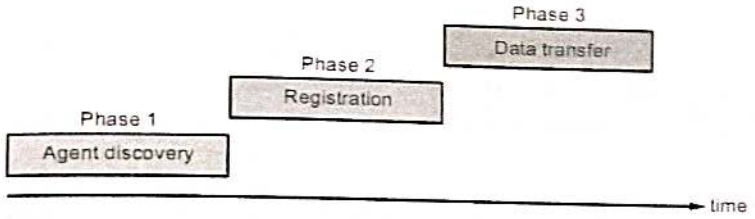

Fig. 4.3.1 : Three phases of mobile host

4.3.2 Route Optimization

- **Triangle routing :** It is tunneling in its simplest form has all packets go to home network (HA) and then sent to MN via a tunnel.
- This involves two IP routes that need to be set-up, one original and the second the tunnel route. It causes unnecessary network overhead and adds to the latency.
- **Route optimization :** Allows the correspondent node to learn the current location of the MN and tunnel its own packets directly.
- Problems arise with :
  1. **Mobility :** Correspondent node has to update/maintain its cache.
  2. **Authentication :** HA has to communicate with the correspondent node to do authentication, i.e., security association is with HA not with MN.

Review Questions

1. Explain the agent discovery methods.
2. Explain agent advertisement.
3. Explain agent solicitation.
4. Give a brief account of route optimization in mobile IP.

4.4 Tunnelling and Encapsulation

- In mobile IP, IP - within - IP encapsulation is used i.e. home agent adds a new IP header called tunnel header. Once a mobile node on a foreign network has completed a successful registration with its home agent, the Mobile IP datagram forwarding process is activated. The home agent will intercept datagrams intended for the mobile node as they are routed to its home network and forward them to the mobile node. This is done by encapsulating the datagrams and then sending them to the node's care-of address.

- Fig. 4.4.1 illustrates tunnelling.

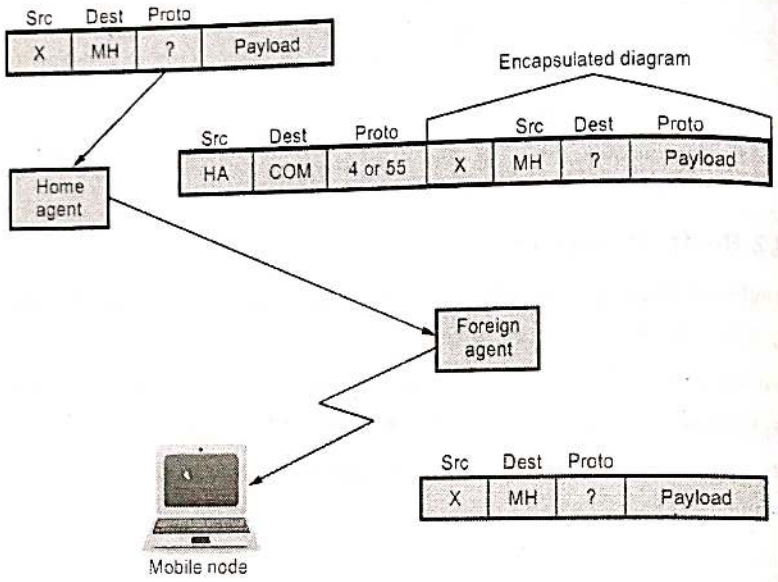

Fig. 4.4.1 : Tunnelling

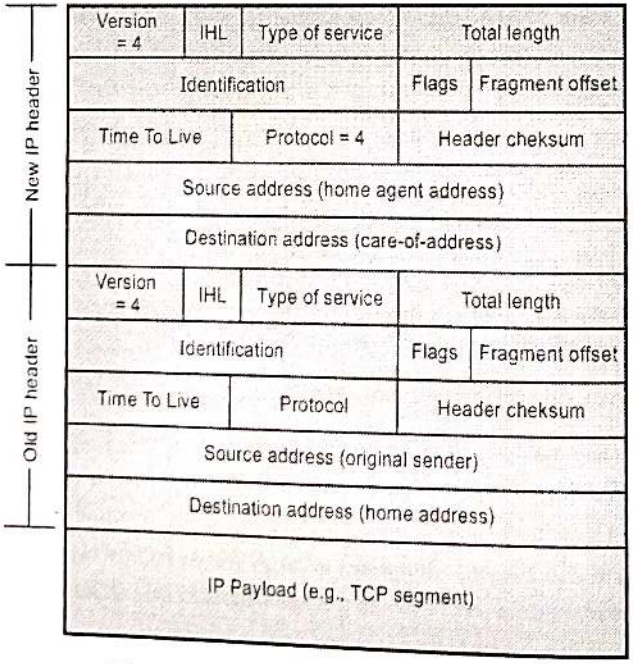

Fig. 4.4.2 : Encapsulation in mobile IP

- Encapsulation is required because each datagram intercepted and forwarded needs to be resent over the network to the device's care-of address. The encapsulation process creates a logical construct called a tunnel between the device that encapsulates and the one that decapsulates.
- The default encapsulation process used in mobile IP is called IP Encapsulation within IP, defined in RFC 2003 and commonly abbreviated IP-in-IP. It is a relatively simple method that describes how to take an IP datagram and make it the payload of another IP datagram.

Review Questions

1. Write short notes on the following :
   a. Correspondent node b. Care-of-Address
   c. Agent Discovery d. Tunnelling and Encapsulation
2. Define tunnelling process.

4.5 IPv6

- Internet Protocol Version 6 (IPv6) is the latest version of the Internet Protocol after IPv4.
- IPv6 includes the features of IPv4 but the significance is address configuration and neighbor discovery. Ipv6 expects all nodes to implement strong encryption and authentication features. Supports mobility at greater extent.
- IPv6 communication protocol provides identification and local systems for computers on the network and routes communications on the Internet. Each device that uses the Internet is identified by its own IP address so that Internet communication can work properly.

Features of IPv6

1. IPv6 provides a simplified and enhanced packet header to allow for more efficient routing.
2. IPv6 improves support for mobile phones and other mobile computing devices.
3. IPv6 enforces increased, mandatory data security through IPsec (which was originally designed for it).
4. IPv6 provides more extensive quality-of-service (QoS) support.
5. IPv6 addresses consist of 128 bits, which allows approximately 3.4×10^{38} addresses.
6. IPv6 uses eight sets of four hexadecimal digits (separated by colons).
7. IPv6 does not support broadcast addresses, but instead uses multicast addresses for broadcast. In addition, IPv6 defines a new type of address called anycast.

4.6 DHCP : Dynamic Host Configuration Protocol

Introduction and working

- When a computer comes online on a network, it requires and IP (unique identification number) address, saving an IP specific computer even when it is not online is infeasible, what we can do is, dynamically assign it IP from a Pool of IPs available when it requires or when it comes online.
- If a new computer is connected to a network, DHCP provide it with all necessary information for full system integration into the network.
- DHCP dynamic host configuration protocol forward the packets for configuration of IP address in the network.
- Dynamic Host Configuration Protocol (DHCP) is a client/server protocol used to enable clients to obtain configuration information for operation in an IP network.
- The DHCP dynamic host configuration protocol is reliable so if any new device connected in the network, it will automatically got the IP address for communication with the network ID.
- A standard DHCP table is maintained by the DHCP servers for all connected devices in the network.
- DHCP protocol assign the IP address to host dynamically which lie in the network.
- DHCPv6 do the same thing in the network the difference is of the address scheme only.
- In configuration of IPv6 addresses from DHCPv6 the RS (Router Solicitation) and RA (Router Advertisement) happens firstly as in stateless auto-configuration.
- If router available then the IPv6 address auto-configured automatically.
- If router not available in the network then DHCPv6 solicite message broadcasted by the DHCP server to all clients in the network.
- So in both case the host got the prefix ID of the IPv6 address. The IPv6 address auto-configured by adding the 64 bit interface ID with it.
- When DHCPv6 is employed for address configuration, the DHCPv6 server typically maintains a log of IPv6 address leases. This means that in the event a host is compromised (e.g. by malware) and such behavior is detected, it is trivial to correlate the malicious activity to the infected node.

Functions of DHCP

- DHCP supplies systems with all necessary information, such as IP address, DNS server address, domain name, subnet mask, default router etc.
- DHCP enables automatic integration of systems into an intranet or the internet, can be used to acquire a COA for Mobile IP.

Applications of DHCP

1. Simplification of installation and maintenance of networked computers
2. Supplies systems with all necessary information, such as IP address, DNS server address, domain name, subnet mask, default router etc.
3. Enables automatic integration of systems into an intranet or the internet.

4.6.1 DHCP Address Assignment and Allocation Mechanisms

- The two main functions of the Dynamic Host Configuration Protocol are :
  1. To provide a mechanism for assigning addresses to hosts and
  2. A method by which clients can request addresses and other configuration data from servers.
- Providing an IP address to a client is the most fundamental configuration task performed by a host configuration protocol.
- To provide flexibility for configuring addresses on different types of clients, the DHCP standard supports three different IP address allocation mechanisms:

1. Manual allocation :

- A particular IP address is pre-allocated to a single device by an administrator. DHCP only communicates the IP address to the device.
- Manual allocation allows DHCP to be used to eliminate the error-prone process of manually configuring hosts with IP addresses in environments where (for whatever reasons) it is desirable to manage IP address assignment outside of the DHCP mechanisms.

2. Automatic allocation

- DHCP automatically assigns an IP address permanently to a device, selecting it from a pool of available addresses.
- DHCP gives a host a permanent network address but still do it automatically, without human interference.

3. Dynamic allocation :

- DHCP assigns an IP address from a pool of addresses for a limited period of time chosen by the server or until the client tells the DHCP server that it no longer needs the address.
- Dynamic allocation is the only one of the three mechanisms that allows automatic reuse of an address that is no longer needed by the client to which it was assigned.
- Thus, dynamic allocation is particularly useful for assigning an address to a client that will be connected to the network only temporarily or for sharing a limited pool of IP addresses among a group of clients that do not need permanent IP addresses.
- Dynamic allocation may also be a good choice for assigning an IP address to a new client being permanently connected to a network where IP addresses are sufficiently scarce that it is important to reclaim them when old clients are retired.

Review Questions

1. Explain three important mechanisms for IP address allocation by DHCP.
2. State some applications of DHCP.

4.7 Ad-Hoc Networks

- Ad-hoc networks are used in many applications such as :
  1. Personal area networking e.g.- cell phone, laptop, earphone etc.
  2. Military applications.
  3. Civilian environment like - taxi cab network, sports stadium, boats, small aircrafts.
  4. Emergency operations such as search and rescue, policing and fighting.

Advantages of ad-hoc networks

1. No infrastructure needed.
2. It can be deployed quickly, where there is no wireless communication infrastructure present.
3. It can act as extension to existing networks to enhance coverage.
4. Ad-hoc networks are cost effective.

Ad-hoc network constraints

- Various constraints of ad-hoc networks are :
  1. Dynamic topologies
  2. Bandwidth requirements
  3. Limitations of transmitting power
  4. No QoS preservation
  5. Limited physical security

Review Questions

1. Briefly describe the following networks : Ad hoc network.
2. What is Adhoc network ?
3. Write a brief note on Adhoc networks.
4. Write a note on Adhoc networks.
5. Explain wireless networks and Adhoc networks.

4.8 Routing

- Routing is the act of moving information across the network from a source to a destination. It is also referred as the process of choosing a path over which the packets are sent.
- The routing process usually directs forwarding on the basis of routing tables which maintain a record of the routes to various network destinations.
- Mobile Ad-hoc networks are self-organizing and self-configuring multihop wireless networks, where the structure of the network changes dynamically. This is mainly due to the mobility of the nodes.
- In an ad-hoc network, a destination node might be out of range of a source node transmitting packets.
- Routing is needed to find a path between source and destination and to forward the packets appropriately.

Problems in routing with mobile ad hoc networks

- In the case of ad-hoc networks, each node must be able to forward data for other nodes. This creates many additional problems -
  i) **Asymmetric links :** Most of the wired networks rely on the symmetric links which are always fixed. But this is not a case with ad-hoc networks as the nodes are mobile and constantly changing their position within network.

ii) **Routing overhead :** In wireless ad hoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.

iii) **Interference :** This is the major problem with mobile ad-hoc networks as links come and go depending on the transmission characteristics, one transmission might interfere with another one and node might overhear transmissions of other nodes and can corrupt the total transmission.

iv) **Dynamic topology :** Since the topology is not constant; so the mobile node might move or medium characteristics might change. In ad-hoc networks, routing tables must somehow reflect these changes in topology and routing algorithms have to be adapted. For example in a fixed network routing table updating takes place for every 30 sec. This updating frequency might be very low for ad-hoc networks.

4.8.1 Ad-hoc On-demand Distance Vector (AODV) Protocol

- Ad-hoc on demand distance vector routing (AODV) is a stateless on-demand routing protocol. Two major functions of AODV protocols are: route discovery and route maintenance. The performance of protocol is improved by keeping the routing information in each node.
- AODV is a distance vector routing protocol, which means routing decisions will be taken depending on the number of hops to destination. A particularity of this network is to support both multicast and unicast routing.

4.8.1.1 Algorithm

- When a route is needed to some destination, the protocol starts route discovery. Then the source node sends route request message (RREQ) to its neighboring nodes (flooding). And if those nodes do not have any information about the destination node, they will send the message to all its neighboring nodes and so on.
- If any neighbor node has the information about the destination node, the node sends route reply message to the route request message initiator. The path is recorded in the intermediate nodes. This path identifies the route and is called the reverse path.
- Since each node forwards route request message to all of its neighbors, more than one copy of the original route request message can arrive at a node. A unique ID is assigned, when a route request message is created. When a node received, it will check this ID and the address of the initiator and discarded the message if it had already processed that request.

- Node that has information about the path to the destination sends route reply message to the neighbor from which it has received route request message. This neighbor does the same. Due to the reverse path it can be possible. Then the route reply (RREP) message travels back using reverse path. When a route reply message reaches the initiator the route is ready and the initiator can start sending data packets.
- When a node detects the link failure to its next hop, it propagates a link failure notification message, Route-Error (RERR) to each of its active upstream neighbours to inform them to erase that part of the route. These nodes in turn propagate the link failure notification message to their upstream neighbours and so on, until the source node is reached.
- When the source node receives the link failure notification message, it will re-initiate a route discovery for the destination if a route is still needed. A new destination sequence number is used to prevent routing loops formed by the entangling of stale and newly established paths.
- AODV saves bandwidth and performs well in a large MANET since a data packet does not carry the whole path information.

4.8.1.2 Route Maintenance

- Another part of this algorithm is the **route maintenance.**
- While a neighbour is no longer available, if it was a hop for a route, this route is not valid anymore.
- AODV uses HELLO packets on a regular basis to check if they are active neighbours. Active neighbours are the ones used during a previous route discovery process. If there is no response to the HELLO packet sent to a node, then, the originator deletes all associated routes in its routing table.
- HELLO packets are similar to ping requests. While transmitting, if a link is broken (a station did not receive acknowledgment from the layer 2), a ROUTE ERROR packet is unicast to all previous forwarders and to the sender of the packet.

4.8.1.3 Characteristics of AODV

1. AODV support unicast, broadcast and multicast communication.
2. AODV performs on-demand route establishment with small delay.
3. Multicast trees connecting group members maintained for lifetime of multicast group.
4. Link breakages in active routes efficiently repaired.
5. All routes are loop-free through use of sequence numbers.

6. Use of Sequence numbers to track accuracy of information.
7. Only keeps track of next hop for a route instead of the entire route.
8. Use of periodic HELLO messages to track neighbors.

4.8.1.4 Advantages and Disadvantages of AODV

- The main advantage of AODV protocol is that routes are established on demand and destination sequence numbers are used to find the latest route to the destination. The connection setup delay is lower.
- One of the disadvantages of AODV protocol is that intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries. Also multiple RouteReply packets in response to a single RouteRequest packet can lead to heavy control overhead.
- Another disadvantage of AODV is that the periodic beaconing leads to unnecessary bandwidth consumption.

4.8.2 Destination-Sequenced Distance-Vector (DSDV) Protocol

- DSDV was one of the first proactive routing protocols available for Ad-hoc networks.

4.8.2.1 Algorithm

- DSDV is based on the Bellman-Ford algorithm.
- With DSDV, each routing table will contain all available destinations, with the associated next hop, the associated metric (numbers of hops) and a sequence number originated by the destination node.
- Tables are updated in the topology per exchange between nodes.
- Each node will broadcast to its neighbors entries in its table. This exchange of entries can be made by dumping the whole routing table or by performing an incremental update, that means exchanging just recently updated routes.
- Nodes who receive this data can then update their tables if they received a better route or a new one.
- Updates are performed on a regular basis and are instantly scheduled if a new event is detected in the topology.
- If there are frequent changes in topology, full table exchange will be preferred whereas in a stable topology, incremental updates will cause less traffic.

- The route selection is performed on the metric and sequence number criteria. The sequence number is a time indication sent by the destination node. It allows the table update process, as if two identical routes are known, the one with the best sequence number is kept and used, while the other is destroyed (considered as a stale entry).

4.8.2.2 Advantages and Disadvantages of DSDV

Advantages

1. DSDV was one of the early algorithms available. It is quite suitable for creating ad hoc networks with small number of nodes. Since no formal specification of this algorithm is present there is no commercial implementation of this algorithm.
2. DSDV guarantees for loop free path.

Disadvantages

1. DSDV requires a regular update of its routing tables, which uses up battery power and a small amount of bandwidth even when the network is idle.
2. Whenever the topology of the network changes, a new sequence number is necessary before the network re-converges; thus, DSDV is not suitable for highly dynamic networks.

4.8.3 Dynamic Source Routing (DSR)

- The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes.
- DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration.
- It is a reactive protocol and all aspects of the protocol operate entirely on-demand basis.
- DSR protocol uses the concept of source routing approach (every data packet carries the whole path information in its header) to forward packets.
- The protocol is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance". DSR requires each node to maintain a route cache of all known self to destination pairs. If a node has a packet to send, it attempts to use this cache to deliver the packet.
- In source routing technique the sender of a packet determines the complete sequence of nodes through which, the packets are forwarded. Otherwise, it will initiate a route discovery phase by flooding a Route REQuest (RREQ) message.

- The RREQ message carries the sequence of hops it passed through in the message header. Any nodes that have received the same RREQ message will not broadcast it again.
- Once an RREQ message reaches the destination node, the destination node will reply with a Route REPly (RREP) packet to the source. The RREP packet will carry the path information obtained from the RREQ packet.
- When the RREP packet traverses backward to the source, the source and all traversed nodes will know the route to the destination. Each node uses a route cache to record the complete route to desired destinations.
- The advantage of source routing is: intermediate nodes do not need to maintain up to date routing information in order to route the packets they forward.
- Route failure is detected by the failure of message transmissions. Such a failure will initiate a route error message to the source. When the source and the intermediate nodes receive the error message, they will erase all the paths that use the broken link from their route cache.
- If the destination does not exist in the cache, then a route discovery phase is initiated to discover a route to destination, by sending a route request (RREQ). The RREQ request includes the destination address, source address and a unique identification number.
- If a route is available from the route cache but is not valid any more, a route maintenance procedure may be initiated.
- A node processes the route request packet only if it has not previously processes the packet and its address is not present in the route cache.
- A route reply is generated by the destination or by any of the intermediate nodes when it knows about how to reach the destination.

4.8.3.1 Advantages and Disadvantages of DSR

Advantages

1. DSR uses a reactive approach which eliminates the need to periodically flood the network with table update messages which are required in a table-driven approach. The intermediate nodes also utilize the route cache information efficiently to reduce the control overhead.
2. DSR is simple and loop-free.

Disadvantages

1. The disadvantage of DSR is that the route maintenance mechanism does not locally repair a broken down link.
2. The connection setup delay is higher than in table-driven protocols. Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility.
3. Considerable routing overhead is involved due to the source-routing mechanism employed in DSR. This routing overhead is directly proportional to the path length.
4. The loop free feature may waste bandwidth if every data packet carries the entire path information.

4.9 Mobile Ad-hoc Network (MANET)

- A network in which the locations of the switches, hubs or routers can be mobile is referred to **Mobile Ad-hoc Network** or **MANET**.
- In MANET, the number of routers available at an instant can increase or decrease and the available routing paths can change.
- The mobile devices or wireless sensors as well as the access-points can have switches or routers. Each mobile device or sensor functions as a node with a switch or router.
- An important characteristic of ad-hoc network architecture is that they are self-organizing i.e. its organization can change due to movement of a device or sensor.

Example of MANET :

1. A bluetooth-enabled mobile device, a bluetooth-enabled computer and Internet with Wi-Fi connection at home.
2. Through intermediate nodes Wi-Fi, Internet and office computer, an ad-hoc network establishment between the mobile device at home and printer at office when the user carrying the device moves from office to home and handheld PDA mobile device reaches near the home computer.
3. When the user of same mobile device goes to an airport with Wi-Fi connectivity, a MANET again established with the office printer.

- Fig. 4.9.1 shows typical schematic of MANET.

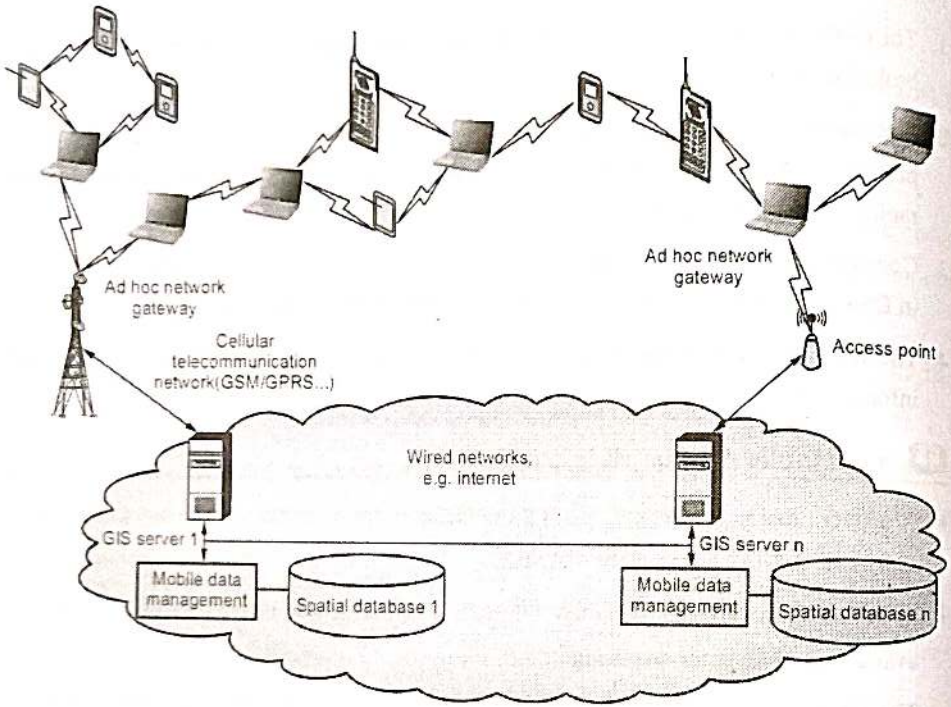

Fig. 4.9.1 : MANET schematic

4.9.1 Characteristics of MANET

- Important characteristics of **MANET are as under** :

1. **Seamless interaction** and ubiquitous mobile computing environment.
2. **Seamless connectivity** maintained between the devices when they move with the nearby wireless nodes, sensor nodes and embedded devices in automobiles.
3. One of the important characteristics of a MANET node is **neighbour discovery**.
4. **Data routing abilities** - Data can be routed from a source node to a neighbouring node.
5. Flexible network architecture and variable routing paths to provide communication in case of the limited wireless connectivity range and resource constraints.
6. **Flexibility** - It enables fast establishment of networks.

7. **Easy establishment** - When a new network is to be established, the only requirement is to provide a new set of nodes with limited wireless communication range.
8. **Computations decentralization** - Independent computational, switching (or routing) and communication capabilities.

4.9.2 Constraints / Limitations of MANET

1. A node has limited capability; i.e. it can connect only to the nodes which are nearby and thus consumes limited power.
2. Limited wireless connectivity range - require that a node should move in the vicinity of at least one nearby node within the wireless communication range, else the node should be provided with the access-point of wired communication.
3. Weak connectivity and remote server latency.
4. Unreliable links to base station or gateway - failure of an intermediate node results in greater latency in communicating with the remote server.
5. Resource constraints - limited bandwidth available between two intermediate nodes.
6. Node may have limited power and thus computations need to be energy-efficient.
7. Only selected access-points provided for connection to other networks or other MANETs.

4.9.3 Routing in MANET

- Important routing protocols for MANETs :

1. Ad hoc On-demand Distance Vector (AODV) protocol,
2. Destination-Sequenced Distance-Vector (DSDV) protocol,
3. Dynamic Source Routing (DSR)

4.9.4 Security Attacks on MANET

- Security attacks on protocol layers are listed here :

Physical layer attacks

1. Eavesdropping
2. Jamming

Link layer attacks

1. Disruption on MAC

Network layer attacks

1. Wormwhole attack,
2. Black whole attack,
3. Flooding attack,
4. Resource consumption attack,
5. Location disclosure attack

Transport layer attacks

1. Session hijacking,
2. SYN flooding

Application layer

1. Repudiation attack,
2. Data corruption

Review Questions

1. Define MANET (Mobile Ad Hoc Network).Explain the schematic model of a MANET.
2. Compare the MANET routing strategies with the routing strategies of traditional networks.
3. List the characteristics of MANETs.
4. List the MANET operational constraints.
5. Describe the applications of MANETs.
6. Define routing. List out the problems arises in MANET by routing.
7. Write a short note on characteristics of secure MANET.
8. Explain the characteristics of MANET that can be exploited to cause security vulnerabilities.
9. Explain the characteristics of MANETs.
10. Explain the important design constraints (issues) on a MANET.
11. Explain security issues in a MANET.
12. Write a note on MANET.
13. Describe the features of mobile Adhoc network.
14. What is mobile adhoc network ? Write down the challenges for designing a good wireless network.

4.10 Hybrid Algorithms

- Maintain routes to nearby nodes even if they are not needed and maintain routes to far away nodes only when needed. Example is Zone Routing Protocol(ZRP).
- Nodes within a certain distance from the node concerned or within a particular geographical region are said to be within the routing zone of the given node.
- For routing within this zone, a table- driven approach is used. For nodes that are located beyond this zone is on-demand approach is used

4.10.1 Zone Routing Protocol (ZRP)

- ZRP is either a proactive or reactive protocol. It is a hybrid routing protocol. It combines the advantages from proactive and reactive routing.
- ZRP divides its network in different zones.
- Each node may be within multiple overlapping zones and each zone may be of a different size.

4.11 VANET (Vehicular Network)

- Vehicle ad-hoc networks (VANETs) are promising technology for increasing the efficiency and security of the transportation systems.
- Vehicles connected to each others through an adhoc formation form a wireless network is called "vehicular adhoc network (VANET)".
- Vehicular adhoc networks are subgroup of mobile adhoc networks (MANETs).
- VANETs consists of network entities, mainly including vehicles and Road Side infrastructure Units (RSUs).
- The communications in VANET are classified into three categories :
  1. The communications between vehicles (V2V or Vehicle-to-Vehicle communication).
  2. The communications between one vehicle and RSUs (V2R).
  3. The broadcast of the vehicles.

- Fig. 4.11.1 shows architecture of VANET.

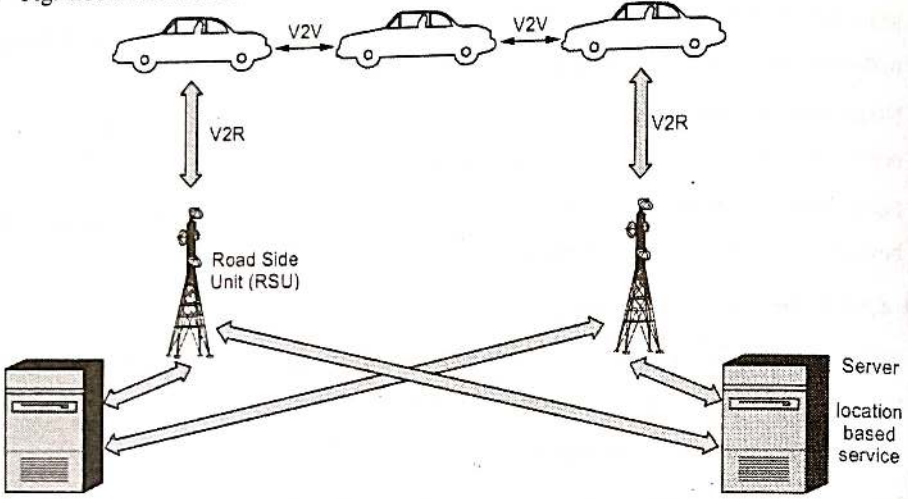

Fig. 4.11.1 : Architecture of VANET

- VANETs can be applied in electronic toll system collection and broadcast of traffic information; access to roadside devices.
- Every participating car is a wireless router or node. The range of connection is approximately 100 to 300 m. Cars / Vehicles may fall out of the signal range and drop out of the network.
- Every node is aware of its location, speed and moving direction.

Characteristics of VANET

1. High mobility at nodes.
2. Rapidly changing network topology.
3. Unbound network size.
4. Potential support from infrastructure
5. Real-time data exchange.
6. Crucial effect of security and privacy
7. Multihop wireless network.

Challenges in VANET

1. Mobility
2. Volatility
3. Privacy and authentication
4. Privacy and liability

5. Network scalability
6. Routing
7. Security

Security requirements in VANET

1. Message authentication and integrity
2. Message non-repudiation
3. Node authentication
4. Access control
5. Message confidentiality
6. Availability
7. Accomotability
8. Privacy protection

VANET models

- Various mobility models are -
  1. Survey models
  2. Event driven models
  3. Software oriented models
  4. Synthetic models

4.11.1 Comparison of MANET and VANET

Ad-Hoc network types / Criteria	VANET	MANET
Node mobility	Medium compactness	Low compactness
Mobility model	Steady	Arbitrary
Node density	Medium thickness	Low thickness
Topology change	Average speed	Slow and steady
Radio propagation model	Close to ground, LoS is not accessible for all cases	Very close to ground, LoS is not accessible for all cases
Power consumption and network lifetime	Not needed	Need of energy efcient protocols
Computational power	Average	Limited
Localization	GPS, AGPS, DGPS	GPS

Review Questions

1. Explain VANET and few important applications of it.
2. Compare MANET and VANET.

❑❑❑

Unit V

5 Mobile Transport Layer

Syllabus

Traditional TCP : Congestion control, Slow start, Fast retransmit/fast recovery, Implications on mobility; Indirect TCP, Snooping TCP, Mobile TCP, Fast retransmit/fast recovery, Transmission/time-out freezing, Selective retransmission, Transaction oriented TCP.

Support for Mobility : File systems : Consistency, Examples.

World Wide Web : Hypertext transfer protocol, Hypertext markup language, some approaches that might help wireless access, System architectures.

Wireless application protocol : Architecture, Wireless datagram protocol, Wireless transport layer security, Wireless transaction protocol, Wireless session protocol, Wireless application environment, Wireless markup language, WML script, Wireless telephony application, Examples Stacks with WAP, Mobile databases, Mobile agents.

Contents

5.1 Traditional TCP

- The Transmission Control Protocol (TCP) is one of the core protocols of the Internet Protocol suite referred to as TCP/IP. TCP is reliable, guarantees in-order delivery of data and incorporates congestion control and flow control mechanisms.
- TCP supports many of the internet's most popular application protocols and resulting applications, including the World Wide Web, e-mail, File Transfer Protocol and Secure Shell. In the Internet protocol suite, TCP is the intermediate layer between the Internet layer and application layer.

5.1.1 Problems with Traditional TCP in Wireless Environments

1. Slow start mechanism in fixed networks decreases the efficiency of TCP if used with mobile receivers or senders.
2. Error rates on wireless links are orders of magnitude higher compared to fixed fiber or copper links. This makes compensation for packet loss by TCP quite difficult.
3. Mobility itself can cause packet loss. There are many situations where a soft handover from one access point to another is not possible for a mobile end-system.
4. Standard TCP reacts with slow start if acknowledgements are missing, which does not help in the case of transmission errors over wireless links and which does not really help during handover. This behaviour results in a severe performance degradation of an unchanged TCP if used together with wireless links or mobile nodes.

5.1.2 Congestion Control

- Traditional TCP suffers from problem of -
  1. Packet loss in fixed networks typically due to (temporary) overload situations.
  2. Router have to discard packets as soon as the buffers are full.
  3. TCP recognizes congestion only indirect via missing acknowledgements, retransmissions unwise, they would only contribute to the congestion and make it even worse.
- When too many packets rushing to a node or a part of network, the network performance degrades and this situation is called as congestion.
- TCP has three congestion control methods :

  1. Additive increase 2. Slow start 3. Retransmit

5.1.3 Slow Start

- Slow-start is part of the congestion control strategy used by TCP, the data transmission protocol used by many internet applications.
- Slow-start is used in conjunction with other algorithms to avoid sending more data than the network is capable of transmitting, that is, to avoid causing network congestion.
- Steps in slow start congestion control mechanism are -
  1. Sender calculates a congestion window for a receiver.
  2. Start with a congestion window size equal to one segment.
  3. Exponential increase of the congestion window up to the congestion threshold, then linear increase.
  4. Missing acknowledgement causes the reduction of the congestion threshold to one half of the current congestion window.
  5. Congestion window starts again with one segment.

5.1.4 Fast Retransmit and Fast Recovery

- Fast re-transmit and fast recovery have been designed to speed up the recovery of the connection, without compromising its congestion avoidance characteristics.

Fast retransmit

- Fast retransmit is a heuristic that sometimes triggers the retransmission of a dropped packet sooner than the regular timeout mechanism. This mechanism does not replace regular timeouts.
- The congestion window is dropped down to 1 each time network congestion is detected. Thus, it takes an amount of time to reach high link utilization as before.
- Important steps in fast retransmit mechanism of congestion control are -
  1. TCP sends an acknowledgement only after receiving a packet.
  2. If a sender receives several acknowledgements for the same packet, this is due to a gap in received packets at the receiver.
  3. However, the receiver got all packets up to the gap and is actually receiving packets.
  4. Therefore, packet loss is not due to congestion, continue with current congestion window (do not use slow-start).

Fast recovery

- The receipt of acknowledgements shows that there is no congestion to justify 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.

5.1.5 Implications on Mobility

- TCP assumes congestion if packets are dropped. TCP concludes a congestion situation from a missing acknowledgement.
- Often packet loss due to transmission errors, also mobility can cause packet loss, if e.g. a mobile node roams from one access point (e.g. foreign agent in Mobile IP) to another while packets in transit to the old access point and forwarding is not possible.
- The performance of an unchanged TCP degrades severely.
- TCP cannot be changed fundamentally due to large installed base in the fixed network, TCP for mobility has to remain compatible.

5.2 Indirect TCP

- Indirect TCP segments a TCP connection into a fixed part and a wireless part. Fig. 5.2.1 illustrates an example with a mobile host connected via a wireless link and an access point to the 'wired' internet where the correspondent host resides.

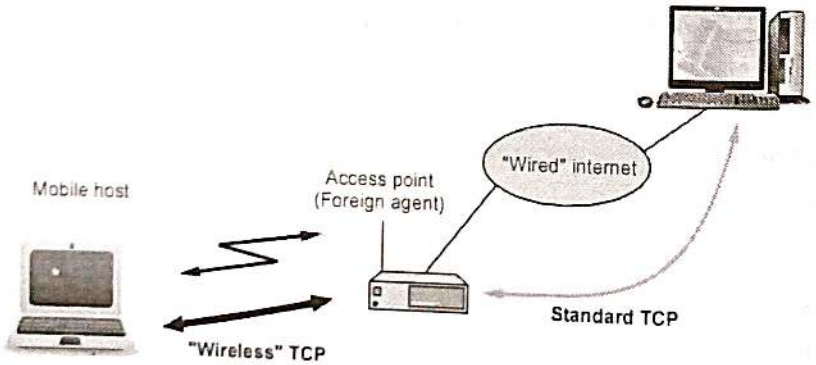

Fig. 5.2.1

- Standard TCP is used between the fixed computer and the access point. No computer in the internet recognizes any changes to TCP. Instead of the mobile host, the access point now terminates the standard TCP connection, acting as a proxy. This means that the access point is now seen as the mobile host for the fixed host and as the fixed host for the mobile host. Between the access point and the mobile host, a special TCP, adapted to wireless links, is used.
- However, changing TCP for the wireless link is not a requirement. A suitable place for segmenting the connection is at the foreign agent as it not only controls the mobility of the mobile host anyway and can also hand over the connection to the next foreign agent when the mobile host moves on.
- The foreign agent acts as a proxy and relays all data in both directions. If CH (Correspondent Host) sends a packet to the Mobile Host (MH), the Foreign Agent (FA) acknowledges it and forwards it to the MH. MH acknowledges on successful reception, but this is only used by the FA.
- If a packet is lost on the wireless link, CH doesn't observe it and FA tries to retransmit it locally to maintain reliable data transport. If the MH sends a packet, the FA acknowledges it and forwards it to CH. If the packet is lost on the wireless link, the mobile hosts notice this much faster due to the lower round trip time and can directly retransmit the packet. Packet loss in the wired network is handled by the foreign agent.
- Socket and state migration after handover of a mobile host is shown in Fig. 5.2.2.

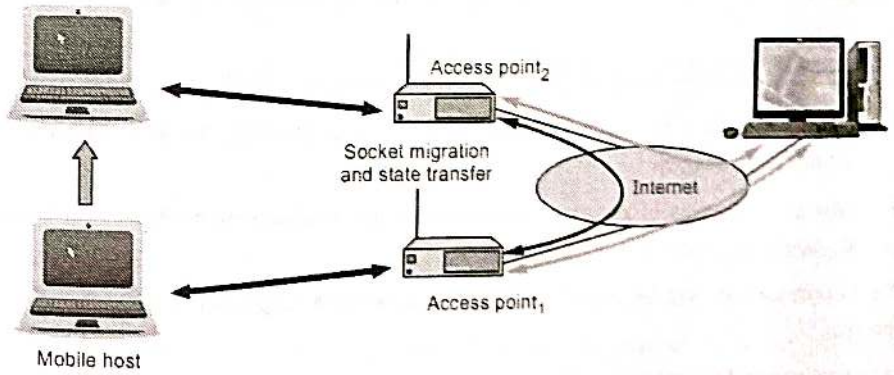

Fig. 5.2.2

- During handover, the buffered packets, as well as the system state (packet sequence number, acknowledgements, ports, etc.), must migrate to the new agent. No new connection may be established for the mobile host and the correspondent host must not see any changes in connection state.

- Packet delivery in I-TCP is shown in Fig. 5.2.3.

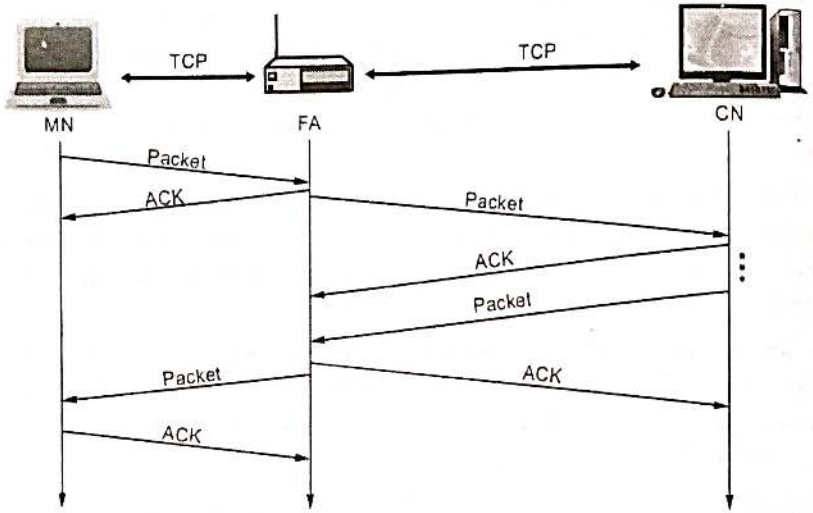

Fig. 5.2.3

Advantages of indirect TCP

1. No changes in the fixed network necessary, no changes for the hosts (TCP protocol) necessary, all current optimizations to TCP still work.
2. Simple to control, mobile TCP is used only for one hop between, e.g., a foreign agent and mobile host -
   a. Transmission errors on the wireless link do not propagate into the fixed network.
   b. Therefore, a very fast retransmission of packets is possible, the short delay on the mobile hop is known.
3. It is always dangerous to introduce new mechanisms in a huge network without knowing exactly how they behave.
4. New optimizations can be tested at the last hop, without jeopardizing the stability of the internet.
5. It is easy to use different protocols for wired and wireless networks.

Disadvantages of indirect TCP

1. Loss of end-to-end semantics - an acknowledgement to a sender no longer means that a receiver really has received a packet, foreign agents might crash.

2. Higher latency possible - due to buffering of data within the foreign agent and forwarding to a new foreign agent.
3. Security issue - The foreign agent must be a trusted entity.

5.2.1 Snooping TCP

- The main drawback of Indirect TCP is the segmentation of the single TCP connection into two TCP connections, which loses the original end-to-end TCP semantic.
- A new enhancement, which leaves the TCP connection intact and is completely transparent, is Snooping TCP. The main function is to buffer data close to the mobile host to perform fast local retransmission in case of packet loss.
- Fig. 5.2.4 shows snooping TCP as a transparent TCP extension.

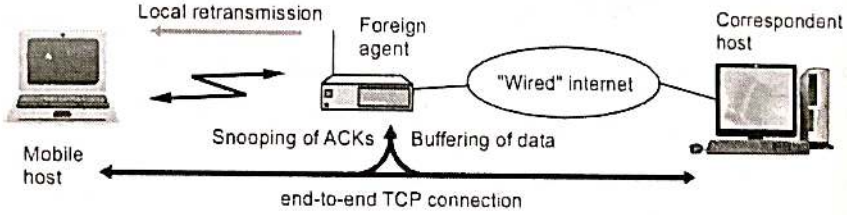

Fig. 5.2.4

- The foreign agent buffers all packets with destination mobile host and additionally 'snoops' the packet flow in both directions to recognize acknowledgements. The foreign agent buffers every packet until it receives an acknowledgement from the mobile host.
- If the FA does not receive an acknowledgement from the mobile host within a certain amount of time, either the packet or the acknowledgement has been lost. Alternatively, the foreign agent could receive a duplicate ACK which also shows the loss of a packet. Now, the FA retransmits the packet directly from the buffer thus performing a faster retransmission compared to the CH.
- For transparency, the FA does not acknowledge data to the CH, which would violate end-to-end semantic in case of a FA failure.
- The foreign agent can filter the duplicate acknowledgements to avoid unnecessary retransmissions of data from the correspondent host. If the foreign agent now crashes, the time-out of the correspondent host still works and triggers a retransmission.
- The foreign agent may discard duplicates of packets already retransmitted locally and acknowledged by the mobile host. This avoids unnecessary traffic on the wireless link.

- Fig. 5.2.5 shows snooping TCP packet delivery timing diagram.

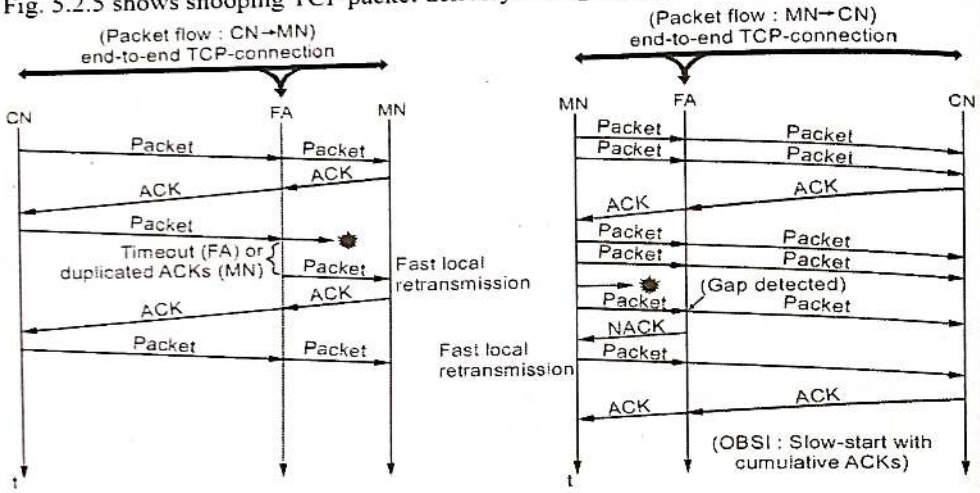

Fig. 5.2.5

- For data transfer from the mobile host with **destination correspondent host**, the FA snoops into the packet stream to detect gaps in the sequence numbers of TCP.
- As soon as the foreign agent detects a missing packet, it returns a Negative Acknowledgement (NACK) to the mobile host. The mobile host can now retransmit the missing packet immediately. Reordering of packets is done automatically at the correspondent host by TCP.

Advantages of snooping TCP

1. The end-to-end TCP semantic is preserved.
2. Most of the enhancements are done in the foreign agent itself which keeps correspondent host unchanged.
3. Handover of state is not required as soon as the mobile host moves to another foreign agent. Eventhough packets are present in the buffer, time out at the CH occurs and the packets are transmitted to the new COA.
4. No problem arises if the new foreign agent uses the enhancement or not. If not, the approach automatically falls back to the standard solution.

Disadvantages of snooping TCP

1. Snooping TCP does not isolate the behaviour of the wireless link as well as I-TCP. Transmission errors may propagate till CH.
2. Using negative acknowledgements between the foreign agent and the mobile host assumes additional mechanisms on the mobile host. This approach is no longer transparent for arbitrary mobile hosts.
3. Snooping and buffering data may be useless if certain encryption schemes are applied end-to-end between the correspondent host and mobile host.
4. If encryption is used above the transport layer, (such as SSL/TLS), snooping TCP can be used.

5.2.2 Mobile TCP

- When a mobile host gets disconnected, both I-TCP and Snooping TCP does not help much. The **M-TCP (Mobile TCP)** approach has the same goals as I-TCP and snooping TCP i.e. to prevent the sender window from shrinking if bit errors or disconnection but not congestion cause current problems.
- M-TCP helps to improve overall throughput, to lower the delay, to maintain end-to-end semantics of TCP and to provide a more efficient handover. M-TCP is especially adapted to the problems arising from lengthy or frequent disconnections.
- M-TCP splits the TCP connection into two parts as I-TCP does. An unmodified TCP is used on the standard host-**Supervisory Host (SH)** connection, while an optimized TCP is used on the SH-MH connection.
- The SH monitors all packets sent to the MH and ACKs returned from the MH. If the SH does not receive an ACK for sometime, it assumes that the MH is disconnected. It then chokes the sender by setting the sender's window size to 0. Setting the window size to 0 forces the sender to go into **persistent mode**, i.e., the state of the sender will not change no matter how long the receiver is disconnected.
- This means that the sender will not try to retransmit data. As soon as the SH (either the old SH or a new SH) detects connectivity again, it reopens the window of the sender to the old value. The sender can continue sending at full speed. This mechanism does not require changes to the sender's TCP.
- The wireless side uses an adapted TCP that can recover from packet loss much faster. This modified TCP does not use slow start, thus, M-TCP needs a **bandwidth manager** to implement fair sharing over the wireless link.

Advantages of M-TCP

1. It maintains the TCP end-to-end semantics. The SH does not send any ACK itself but forwards the ACKs from the MH.
2. If the MH is disconnected, it avoids useless retransmissions, slow starts or breaking connections by simply shrinking the sender's window to 0.
3. As no buffering is done as in I-TCP, there is no need to forward buffers to a new SH. Lost packets will be automatically retransmitted to the SH.

Disadvantages of M-TCP

1. 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.
2. A modified TCP on the wireless link not only requires modifications to the MH protocol software but also new network elements like the bandwidth manager.

Comparison of various approach of TCP for mobility

Approach	Mechanism	Advantages	Disadvantages
Indirect TCP	Splits TCP connection into two connections.	Isolation of wireless link, simple.	Loss of TCP semantics higher latency at handover.
Snooping TCP	"Snoops" data and acknowledgements, local retransmission.	Transparent for end-to-end connection, MAC integration possible.	Problematic with encryption, bad isolation of wireless link.
M-TCP	Splits TCP connection, chokes sender via window size.	Maintains end-to-end semantics, handles long term and frequent disconnections.	Bad isolation of wireless link, processing overlead due to bandwidth management.

Review Questions

1. Explain about indirect and snooping TCP. Also give any two advantages of mobile TCP.
2. Explain the indirect and snooping TCP.
3. Explain classical TCP improvements and snooping TCP.
4. Distinguish between traditional TCP and wireless TCP.

5.3 Support for Mobility : File System

- Mobility is the ability to move or be moved freely and easily. Mobility means the movement of individuals from a one place or position to another, ensuring that their independence is maintained e.g. moving from a wheelchair to a bed or transferring from the bed to a chair as well as bed mobility - changing positions from one to another.
- Motivation for mobility is efficient and transparent access to shared files within a mobile environment while maintaining data consistency.

Mobility problems

- Most severely faced problems for support of mobility are -
  1. Limited resources of mobile computers (memory, CPU, ...).
  2. Low bandwidth, variable bandwidth, temporary disconnection.
  3. High heterogeneity of hardware and software components (no standard PC architecture).
  4. Wireless network resources and mobile computer are not very reliable.
  5. Standard file systems (e.g., NFS, network file system) are very inefficient, almost unusable.
  6. Problem of distributed, loosely coupled systems.
  7. Weak consistency.
  8. Conflict detection.

Database systems in mobile environments

- Database systems in mobile environments include :
  1. Request processing
  2. Replication management
  3. Location management
  4. Transaction processing

5.4 World Wide Web

- World-Wide Web (also called WWW or W3) is a hypertext-based information system. Any word in a hypertext document can be specified as a pointer to a different hypertext document where more information pertaining to that word can be found.
- The reader can open the second document by selecting the word (using different methods depending on the interface; in a mouse based system, a user would probably place the mouse over the word and click the mouse button); only the part of the linked document which contains relevant information will be displayed.

- Web consists of three key components :
  1. **HTML - (Hypertext Markup Language) :** This is a standard markup language used to create web pages.
  2. **URL - (Uniform Resource Locator) :** This is the understandable form of a web address which is used to identify a resource.
  3. **HTTP - (Hyper Text Transfer Protocol) :** This protocol is stateless and acts as the foundation of the Web.

Hypertext

- Hypertext is text which is not constrained to be linear. Hypertext is text which contains "links" to other texts.
- HyperMedia is a term used for hypertext which is not constrained to be text: it can include graphics, video and sound.

HTTP

- The Hypertext Transfer Protocol (HTTP) is the foundation of the World Wide Web and is used to load web pages using hypertext links.
- HTTP is an application layer protocol designed to transfer information between networked devices and runs on top of other layers of the network protocol stack.
- A typical flow over HTTP involves a client machine making a request to a server, which then sends a response message.

HTTP request

- An HTTP request is the way internet communications platforms such as web browsers ask for the information they need to load a website.
- Each HTTP request made across the Internet carries with it a series of encoded data that carries different types of information.
- A typical HTTP request contains :
  1. HTTP version type
  2. A URL
  3. An HTTP method
  4. HTTP request headers
  5. Optional HTTP body.

HTTP response

- An HTTP response is what web clients (often browsers) receive from an Internet server in answer to an HTTP request.
- These responses communicate valuable information based on what was asked for in the HTTP request.
- A typical HTTP response contains :
  1. An HTTP status code
  2. HTTP response headers
  3. Optional HTTP body

HTML

- HTML stands for HyperText Markup Language. It is a standard markup language for web page creation.
- HTML allows the creation and structure of sections, paragraphs and links using HTML elements (the building blocks of a web page) such as tags and attributes.
- HTML has a lot of use cases, namely :
  1. **Web development :** Developers use HTML code to design how a browser displays web page elements, such as text, hyperlinks and media files.
  2. **Internet navigation :** Users can easily navigate and insert links between related pages and websites as HTML is heavily used to embed hyperlinks.
  3. **Web documentation :** HTML makes it possible to organize and format documents, similarly to Microsoft Word.

5.5 WAP (Wireless Application Protocol)

- WAP stands for Wireless Application Protocol. WAP is an application communication protocol.WAP is used to access services and information.
- WAP is a "standard" created by wireless and Internet companies to enable Internet access from a cellular phone.
- WAP is designed to access to Internet and advanced telephony services from mobile phone users.
- WAP uses mark-up language (WML) not HTML.
- WAP can be used from variety of 2G and 3G networks such as GSM-900,GSM-1800,GSM-1900,CDMA IS-95,cdma-2000,TDMA IS-136,i-mode,3G systems : IMT-2000,UMTS,W-CDMA. GPRS and 3G are more suited for these applications.

5.5.1 Requirements of WAP

- Following are WAP architecture requirements :
  1. The architecture should have leverage existing standards whenever possible.
  2. WAP define a layered, scalable and extensible architecture.
  3. WAP architecture must support as many wireless networks as possible.
  4. Optimization for narrow band bearer with high latency.
  5. Optimize for efficient use of device resources.
  6. Provide support for secure application and communication.

5.5.2 WAP Protocol Stack

- WAP is designed in a layered fashion so that it can be extensible, flexible and scalable. As a result, the WAP protocol stack is divided into five layers :
  1. Wireless Application Environment (WAE)
  2. Wireless Session Protocol (WSP)
  3. Wireless Transaction Protocol (WTP)
  4. Wireless Transport Layer Security (WTLS)
  5. Wireless Datagram Protocols (WDP)

5.5.2.1 Wireless Application Environment (WAE)

- This layer is of most interest to content developers because it contains, among other things, device specifications and the content development programming languages, WML and WMLScript.
- WAE architecture allows all content and services to be hosted on standard Web servers when all content is located using WWW standard URLs.
- The application environment of WAE consists of :
  1. User agent : Browser or client program.
  2. WML : Wireless Markup Language is a lightweight markup language optimized for use in wireless devices.
  3. WMLScript : Lightweight client side scripting language.
  4. Wireless Telephony Application : Telephony services and programming interfaces.
  5. WAP Push Architecture : Mechanism to allow origin servers to deliver content to terminal.
  6. Content formats : Set of data formats.

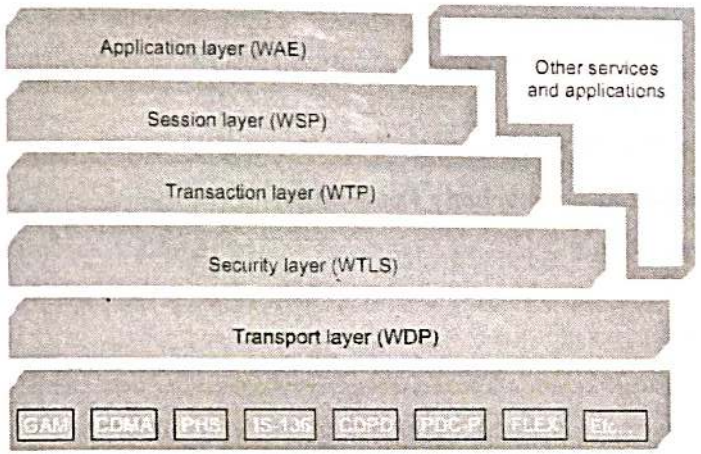

Fig. 5.5.1

5.5.2.2 Wireless Session Protocol (WSP)

- Wireless Session Protocol (WSP). Unlike HTTP, WSP has been designed by the WAP Forum to provide fast connection suspension and reconnection.
- WSP provides a consistent interface between two session services like client and server.
- WSP offers both connection oriented and connectionless service.

5.5.2.3 Wireless Transaction Protocol (WTP)

- Wireless Transaction Protocol (WTP) runs on top of a datagram service such as User Datagram Protocol (UDP) and is part of the standard suite of TCP/IP protocols used to provide a simplified protocol suitable for low bandwidth wireless stations.
- WTP supports class of transaction service, optional user-to-user reliability, PDU concatenation and asynchronous transaction.

5.5.2.4 Wireless Transport Layer Security (WTLS)

- WTLS incorporates security features that are based upon the established Transport Layer Security (TLS) protocol standard. It includes data integrity checks, privacy, service denial and authentication services.
- WTLS provides data integrity, privacy, authentication, denial of service protection.

5.5.2.5 Wireless Datagram Protocol (WDP)

- The WDP is transport layer protocol in WAP architecture. WDP operates above data capable bearer services supported by various network type general transport service.

- The WDP allows WAP to be bearer-independent by adapting the transport layer of the underlying bearer. The WDP presents a consistent data format to the higher layers of the WAP protocol stack, thereby offering the advantage of bearer independence to application developers.

5.5.3 WTA (Wireless Telephony Application)

- The WTA allows WAP applications to control various telephony applications, such as making calls, answering calls, putting calls on hold or forwarding them. It allows WAP WTA-enabled cell phones to have integrated voice and data services.
- The WTA framework supports Wireless Telephony Applications that interface with the in-device telephony related functions and the network telephony infrastructure.
- WTA offers transaction support, adding reliability to the datagram service provided by WDP. It is a light weight transaction-oriented protocol.
- Three classes of transaction services -
  1. Unreliable one-way requests
  2. Reliable one-way requests
  3. Reliable two-way request-reply transactions
- The WTA framework extends the WAE framework by adding :
  i) An interface from WML and WMLScript to a specific set of local, telephony related, functions in the client. This interface is called the "Wireless Telephony Application Interface" [WTAI].
  ii) Network event handling. This means that events originating from the mobile network could be detected by the WTA user-agent and actions in response to the events could be defined.
  iii) A repository, which is a storage container, used by the WTA user-agent, that persistently stores content that executes WTA services. The purpose of the repository is to fulfil the real-time requirements that are placed on the execution of WTA services.
  iv) A model for WTA user-agent state and WTA context management.
  v) A MANDATORY security model.

5.5.4 WTA Architecture

- WTA is an application framework for telephony services. The WTA user-agent essentially is a user-agent similar to the standard WML user-agent with the addition of capabilities for interfacing with mobile network services available to a mobile telephony device, e.g. setting up and receiving phone calls.
- The Fig. 5.5.2 shows describes one possible configuration of the WTA framework. However, this specification solely defines the components contained in the client.

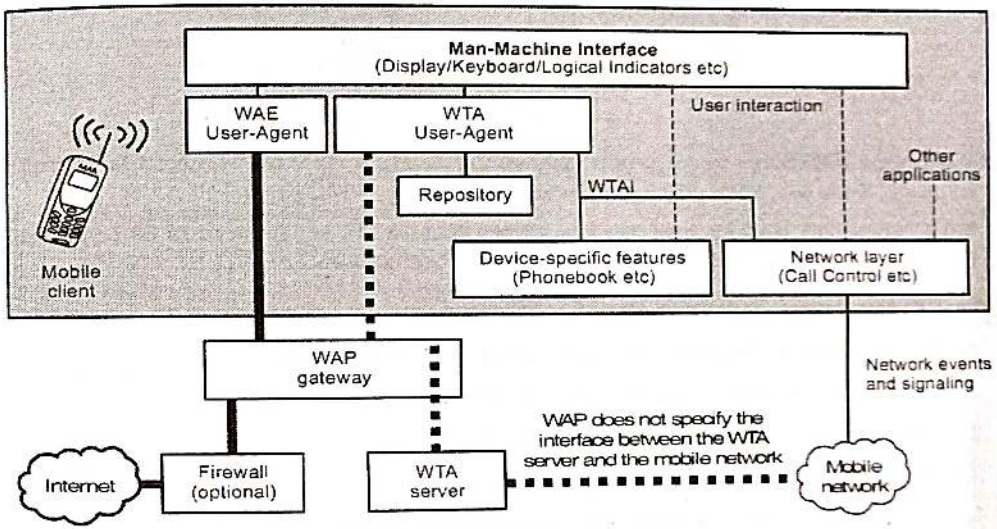

Fig. 5.5.2 : WTA architecture

5.5.5 WML

- WML stands for Wireless Markup Language. It is a mark-up language inherited from HTML, but WML is based on XML, so it is much stricter than HTML.
- WML is used to create pages that can be displayed in a WAP browser. Pages in WML are called DECKS. Decks are constructed as a set of CARDS.
- WML is Tag-based browsing language. WML performs operation of :
  - Screen management (text, images)
  - Data input (text, selection lists, etc.)
  - Hyperlinks and navigation support

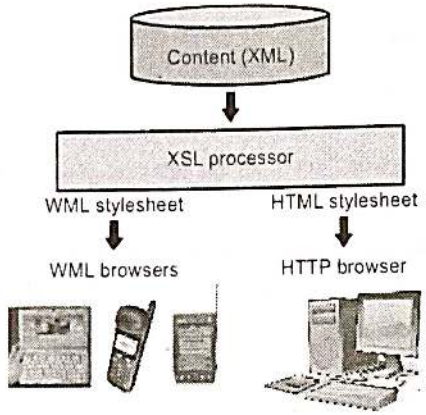

Fig. 5.5.3 : WML

- WML uses WMLScript to run simple code on the client. WMLScript is a light JavaScript language. However, WML scripts are not embedded in the WML pages.
- WML pages only contains references to script URLs. WML scripts need to be compiled into byte code on a server before they can run in a WAP browser.

5.5.6 Advantage of WMLScript over WML

- WMLScript provides following advantages to application developer.
  1. Local validation of user input before it is sent to the content server.
  2. Access device resources, functions and peripherals.
  3. Interact with users without reference to origin server.
  4. WMLScript is based on industry standard JavaScript solution.
  5. WMLScript adds power of procedural logic to WML.
  6. WMLScript may be invoked in response to certain event.
  7. WMLScript is fully integrated with the WML browser.

5.5.7 WAP Gateway

- WAP gateway acts as a middleware which performs coding and encoding between cellular device and the web server.
- WAP gateway can be located either in a telecom network or within a computer data network (ISP).
- WAP gateway implements a WAP protocol stack. It performs protocol translation between phone and server.

- WAP gateway compresses WML pages to save bandwidth.
- WAP gateway performs user authentication and billing. Architecture of WAP gateway is shown in Fig. 5.5.4.

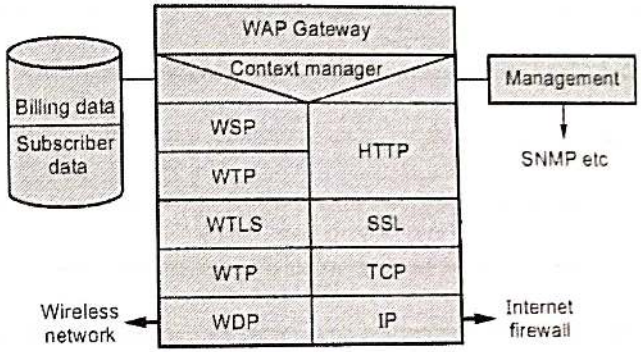

Fig. 5.5.4 : WAP gateway architecture

- External interfaces to WAP gateways are :
  a) SMS center using protocols.
  b) HTTP servers to fetch WML pages.
  c) WAP devices using WAP protocol stack.

Functions of WAP Gateway

1. Implementation WAP protocol stack.
2. Protocol translation between mobile handset and server.
3. Compress WML pages to save bandwidth.
4. User authentication and billing.

Review Questions

1. State the requirements of WAP and explain different layers of WAP. What are the advantages of WML script over WML ?
2. What is a WAP gateway ? What are its functions ?
3. Describe the WAP protocol stack. What are the functions of different layers in this protocol stack ?
4. Describe the WAP protocol stack while enumerating the functions of different layers.
5. Explain WAP.

❑❑❑

Unit VI

6 Mobile Platforms and Applications

Syllabus

Mobile Device Operating Systems, Special Constrains and Requirements, Commercial Mobile Operating Systems.

Software Development Kit : Ios, Android, Blackberry, Windows Phone,

M Commerce, Structure, Pros and Cons, Mobile Payment System, Security Issues.

Contents

6.1 Operating System

- The Operating System (OS) is a master control program for a device. It manages all software and hardware resources.
- The operating system controls, allocates, frees and modifies the memory by increasing or decreasing it.
- The operating system also manages files, disks and security, provides device drivers and GUIs for desktop or mobile computer, other functions and applications.
- The OS enables the assignment of priorities for requests to the system and controls IO devices and network.

6.1.1 Basic Functions of OS

- OS provide functions to perform following actions :
  1. Task management - Task creation, blocking, running, delaying, suspending, resuming.
  2. Memory management - Allocation, freeing and de-allocation.
  3. Device management - configuration, initiation, registration, reading, listening, writing, deregistration.
  4. File management - Creating, opening, closing, read, write and delete.
  5. Database connectivity - Sending queries, appending, deleting or modifying.
  6. I/O devices subsystems management - Display, printer, USB ports, SD/micro SD card.
  7. Network subsystem management - Ethernet, Internet, Wi-fi.

6.2 Mobile OS

- The Operating System (OS) is a master control program for a device. It manages all software and hardware resources.
- The operating system controls, allocates, frees and modifies the memory by increasing or decreasing it.
- The operating system also manages files, disks and security, provides device drivers and GUIs for desktop or mobile computer, other functions and applications.
- A **mobile OS** is a software platform on top of which other programs called application programs, can run on mobile devices such as PDA, cellular phones, smart phone and etc.
- The OS enables the assignment of priorities for requests to the system and controls I/O devices and network.

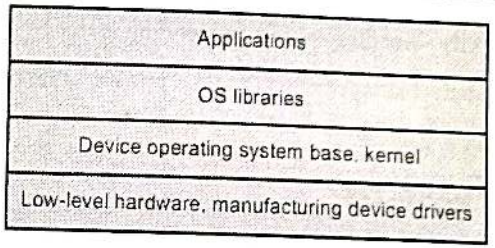

Fig. 6.2.1 : Mobile OS

- Mobile OS enables running of application tasks taking into account such constraints of hardware and network.
- Mobile OS enables a programmer to develop application without considering the specifications, drivers and functionalities of the hardware of the system.
- It enables an application to run by simply abstracting the mobile system hardware.
- Mobile OS enables the programmer to abstract the devices such that the application need not know full details of the font and font size of the mobile device display.

Mobile OS Examples

- There are many mobile operating systems. The followings demonstrate the most important ones :
  1. Java ME Platform
  2. Palm OS
  3. Symbian OS
  4. Windows Mobile OS
  5. BlackBerry OS
  6. iPhone OS - Google Android Platform

6.2.1 Basic Functions of OS

- OS provide functions to perform following actions :
  1. Task management - Task creation, blocking, running, delaying, suspending, resuming.
  2. Memory management - Allocation, freeing and de-allocation.
  3. Device management - configuration, initiation, registration, reading, listening, writing, deregistration.
  4. File management - Creating, opening, closing, read, write and delete.

5. Database connectivity - Sending queries, appending, deleting or modifying.
6. I/O devices subsystems management - Display, printer, USB ports, SD/micro SD card.
7. Network subsystem management - Ethernet, Internet, Wi-fi.

6.2.2 Features of Mobile OS

1. **Multitasking** - The OS handles multitasking in the way that it can handle multiple operations/executes multiple programs at a time.
2. **Scheduling** - Schedulers are special system software which handle process scheduling in various ways. Their main task is to select the jobs to be submitted into the system and to decide which process to run.
3. **Memory allocation** - The main memory must accommodate both the operating system and the various user processes. We therefore need to allocate different parts of the main memory in the most efficient way possible.
4. **File system interface** - A frequent use of streams is to communicate with a file system to which groups of data (files) can be written and from which files can be retrieved.
5. **Keypad interface** - Provides efficient keyboard interface.
6. **I/O interface** - Multiformat I/O interface.
7. **Protection and security** - The security functionality includes protected communications to and between elements; administrative access and its configuration capabilities; system monitoring for detection of security relevant events; and the ability to verify the source of updates.
8. **Multimedia feature** - A mobile OS manages mobile multimedia functions.

6.2.3 Special Constraints and Requirements of Mobile OS

- Design and capabilities of a mobile OS (Operating System) is very different than a general purpose OS running on desktop machines.
- There are special constrains under which the operating system of a mobile device to operate.

A] Physical Contraints

1. Limited memory
2. Limited screen size
3. Miniature keyboard
4. Limited processing power
5. Limited battery power

B] Working in Uncertainty

1. Limited and fluctuating of the wireless medium.
2. OS need to provide robust methods for handling connections and coping with service interruptions and ad hoc attempts to communicate.
3. Network signal come and go
4. Other devices appear and disappear

Special service Requirements of Mobile OS

1. Support for specific communication protocols
2. Support for a variety of input mechanism
3. Compliance with open standard
4. Extensive library support

Review Questions

1. 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.
2. List and explain the special constraints of mobile OS.

6.3 Microkernel OS

- A multi-server design divides the OS functionality into several independent user-level processes. The ability of each single process is also tightly controlled. Kernel only maintains minimum set of basic functionality that cannot be done in user space. This type of design is called **microkernel**.
- The microkernel implements essential core-operating system functions. The functions typically encompass process management, inter-process communication, address space management and hardware abstraction.
- The structure of a microkernel-supported multi-server design is illustrated in Fig. 6.3.1.

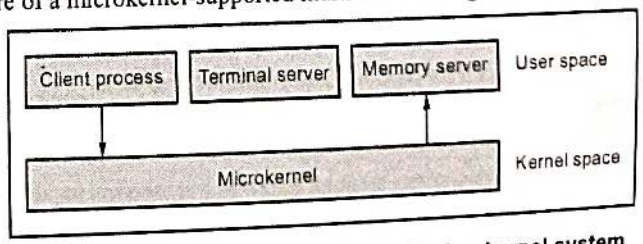

Fig. 6.3.1 : Structure of a multi-server microkernel system

- Microkernels and their user environments are most often implemented in the C or C++ programming languages with a little bit of assembly, but other implementation languages are possible too.
- A microkernel is a tiny operating system core that provides the foundation for modular and portable extensions.
- A microkernel with a small privileged core surrounded by user-mode services, would deliver unprecedented modularity, flexibility and portability. Thus OS designed using microkernel technology has the following relation :

  OS = Microkernel + User subsystems (Servers)
- Microkernel does not necessarily mean small system. The appendage 'micro' suggests that kernel providing only a minimal function that allows user-level system processes to perform OS services efficiently.

6.3.1 Features of Microkernel

- The most important characteristics or features of microkernel are listed below :

1. Code management is much easier.
2. Better expansion of functionality.
3. Microkernel is compact and modular.
4. Microkernel is flexible.
5. Traditional services of OS have become peripheral.
6. Improved reliability
7. Vertical style access instead of horizontal
8. Message passing facilities
9. Leads to a distributed computing model (Transparent local or remote services)
10. Subsystems of microkernel are - POSIX, database, file, Network server, etc.
11. Monolithic application performance competence.
12. Microkernel is foundations for modular and portable extensions

Review Question

1. Define microkernel OS. Give some reasons to prefer microkernel for developing mobile OS.

6.4 Commercial Mobile Operating Systems

6.4.1 Windows CE

- Windows CE is a 32-bit multitasking, multithreading OS developed by Microsoft for mobile devices. Although Microsoft does not explain the "CE," it is reported to have originally stood for "Consumer Electronics.
- Windows CE can be customized for each specific hardware and processor in order to fine-tune the performance.
- Windows CE is compatible with a variety of processor architectures.
- Windows CE performance can be very finely tuned for a specific set of hardware.
- The major versions of WinCE include :

1. WinCE 1.0 - First release, used on a few Palmtop devices.
2. WinCE 2.0 - First commercially successful version used on Palmtop units
3. WinCE 2.11 - Last version 2 product, widely used.
4. WinCE 3.0 - Stable version used on Pocket PC 2000 and 2002 PDAs and Handheld PC 2000 Palmtop units
5. WinCE 4.0, 4.1 - Used in various embedded devices like DoTel 300 PDA or Sigmarion 3 palmtop, never used in Windows Mobile platform release
6. WinCE 4.2 - Windows Mobile 2003, 2003SE. (CE.NET)
7. WinCE 5.0 - Windows Mobile 5.0, 6.0 (CE 5.0)
8. WinCE 6.0 - Windows Mobile 7.0 (unconfirmed), Zune HD

6.4.2 iOS

- **iOS (iPhone OS)** is a mobile operating system developed by Apple Inc. and distributed exclusively for Apple hardware. It was originally released in 2007.
- iOS is the operating system presently used in many mobile devices, including the iPhone, iPad and iPod touch.

Main features of iOS

Programmed in	: C, C++, Objective-C and Swift
OS family	: OS X, UNIX
Initial release	: June 29,2007

Kernel type : Hybrid (XNU)

Default user Interface : Cocoa touch (multi-touch, GUI)

Kernel Type : Hybrid Kernel Architecture

6.4.2.1 Architecture of iOS

- iOS architecture consists of four abstraction levels :
  1. Cocoa touch layer
  2. Media layer
  3. Core Services layer and
  4. Core OS layer
- Fig. 6.4.1 shows architecture of iOS.

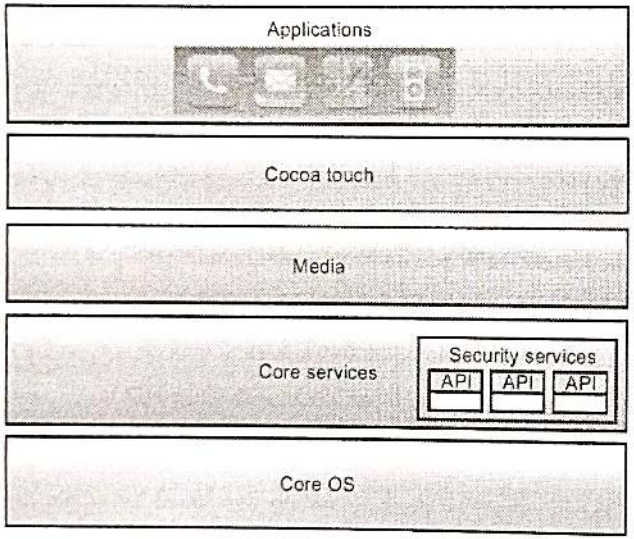

Fig. 6.4.1 : iOS architecture

- At the highest level, iOS acts as an intermediary between the underlying hardware and the apps that appear on the screen. The apps you create rarely talk to the underlying hardware directly. Instead, apps communicate with the hardware through a set of well-defined system interfaces that protect your app from hardware changes.
- The Kernel in iOS is based on same variant of the basic mach Kernel that is found in MAC OSX.

1. Cocoa Touch Layer

- The Cocoa Touch layer contains the key frameworks for building iOS applications. This layer defines the basic application infrastructure and support for key technologies such as multitasking, touch-based input, push notifications and many high-level system services. High level features such as storyboards, Document support, Multitasking, Printing, Data Protection, Apple push notifications service and File sharing are supported by Cocoa touch layer.
- There are so many Cocoa touch layer frameworks, they are :

Address Book UI Framework -

- The Address Book UI framework (AddressBookUI.framework) is an Objective-C programming interface that you use to display standard system inter-faces for creating new contacts and for editing and selecting existing contacts.

Game Kit Framework -

- Introduced in iOS 3.0, the Game Kit framework (GameKit.framework) lets you add peer-to-peer network capabilities to your applications. Specifically, this framework provides support for peer-to-peer connectivity and in-game voice features.

Twitter Framework -

- Introduced in iOS 5, the Twitter framework (Twitter.framework) provides support for sending Twitter requests on behalf of the user and for composing and sending tweets.
- The Twitter framework also works in conjunction with the Accounts framework (Accounts.framework) to access the users account.

Map Kit Framework -

- Introduced in iOS 3.0, the Map Kit framework (MapKit.framework) provides a scrollable map interface that you can integrate into your existing view hierarchies. You can use this map to provide directions or highlight points of interest.
- Applications can programmatically set attributes of the map or let the user navigate the map freely. You can also annotate the map with custom images or content.

2. Media Layer

- The Media layer contains the graphics, audio and video technologies geared toward creating the best multimedia experience available on a mobile device.

Graphics Technologies

- High-quality graphics are an important part of all iOS applications. Core Graphics (also known as Quartz) handles native 2D vector and image-based rendering.
- Core Animation (part of the Quartz Core framework) provides advanced support for animating views and other content. Core Image provides advanced support for manipulating video and still images.

Audio Technologies

- The audio technologies available in iOS are designed to help you provide a rich audio experience for your users. This experience includes the ability to play high-quality audio, record high-quality audio and trigger the vibration feature on certain devices.
- The audio technologies in iOS support the following audio formats : AAC, Apple Lossless (ALAC), A-law, IMA/ADPCM (IMA4),Linear PCM, DVI/Intel IMA ADPCM, Microsoft GSM6.10.

Video Technologies

- Whether you are playing movie files from your application or streaming them from the network, iOS provides several technologies to play your video-based content. On devices with the appropriate video hardware, you can also use these technologies to capture video and incorporate it into your application.
- The video technologies in iOS support the playback of movie files with the .mov, .mp4, .m4v and .3gp filename extensions and using the following compression standards :
  1. H.264 video, up to 1.5 Mbps, 640 by 480 pixels, Low-Complexity version of the H.264 Baseline Profile with AAC-LC audio up to 160 Kbps, 48 kHz, stereo audio in .m4v, .mp4 and .mov file. formats.
  2. H.264 video, up to 768 Kbps, 320 by 240 pixels, Baseline Profile up to Level 1.3 with AAC-LC audio up to 160 Kbps, 48 kHz, stereo audio in .m4v, .mp4 and .mov file formats.
  3. MPEG-4 video, up to 2.5 Mbps, 640 by 480 pixels, Simple Profile with AAC-LC audio up to 160 Kbps, 48 kHz, stereo audio in .m4v, .mp4 and .mov file formats.

AirPlay

- AirPlay is a technology that lets your application stream audio to Apple TV and to third-party AirPlay speakers and receivers.
- AirPlay support is built in to the AV Foundation framework and the Core Audio family of frameworks.

- Any audio content you play using these frameworks is automatically made eligible for AirPlay distribution.
- Once the user chooses to play your audio using AirPlay, it is routed automatically by the system.

3. Core Services Layer

- The Core Services layer contains the fundamental system services that all applications use. Even if you do not use these services directly, many parts of the system are built on top of them.
- Some of the key technologies available in the Core Services layer are :

iCloud Storage -

- Introduced in iOS5, iCloud storage lets your application write user documents and data to a central location and access those items from all of a users computers and iOS devices.
- There are two ways that applications can take advantage of iCloud storage, each of which has a different intended usage :
  1. **iCloud document storage -** Use this feature to store user documents and data in the users iCloud account.
  2. **iCloud key -** Value data storage use this feature to share small amounts of data among instances of your application.

Accounts Framework -

- Introduced in iOS 5, the Accounts framework (Accounts.framework) provides a single sign-on model for certain user accounts.
- Single sign-on improves the user experience, because applications no longer need to prompt a user separately for login information related to an account.

Address Book Framework -

- The Address Book framework (AddressBook.framework) provides programmatic access to the contacts stored on a users device.

Core Data Framework -

- Introduced in iOS 3.0, the Core Data framework (Core-Data.framework) is a technology for managing the data model of a Model-View-Controller application.

4. Core OS Layer

- The core OS layer contains the low-level features that most other technologies are built upon. Even if you do not use these technologies directly in your applications, they are most likely being used by other frameworks.

Core Bluetooth -

- The Core Bluetooth framework (CoreBluetooth.framework) allows developers to interact specifically with Bluetooth Low-Energy ("LE") accessories.

External Accessory Framework -

- Introduced in iOS 3.0, the External Accessory frame-work (ExternalAccessory.framework) provides support for communicating with hardware accessories attached to an iOS-based device.
- Accessories can be connected through the 30-pin dock connector of a device or wirelessly using Bluetooth.

Security Framework -

- iOS also provides an explicit Security framework(Security framework) that you can use to guarantee the security of the data your application manages.
- This framework provides interfaces for managing certificates, public and private keys and trust policies.
- It supports the generation of cryptographically secure pseudorandom numbers. It also supports the storage of certificates and cryptographic keys in the keychain, which is a secure repository for sensitive user data.
- The Common Crypto library provides additional support for symmetric encryption, HMAC and digests.
- The digests feature provides functions that are essentially compatible with those in the OpenSSL library, which is not available in iOS.

6.4.3 Android OS

- Android is an open-source software development platform for creating mobile applications.
- Android is an open source software stack that includes :
  1. Operating system : Linux operating system kernel that provides low level interface with the hardware, memory management and process control.
  2. Middleware : A run time to execute Android applications.

  3. Key mobile applications : Email, SMS, PIM, web browser and etc.
  4. Along with API libraries for writing mobile applications : Including open-source libraries such as SQLite, WebKit and OpenGL ES.
- The components of the underlying OS are written in C or C++, user applications are built for Android in Java. Even the built-in applications are written in Java.
- An important feature of the Android platform is that there's no difference between the built-in applications and applications that is create with the Software Development Kit (SDK).
- Android is only a software. By leveraging its Linux kernel to interface with the hardware, Android runs on many different devices from multiple cell phone manufacturers. Developers write applications in Java.
- The Android software environment and hardware it runs on is shown in Fig. 6.4.2.

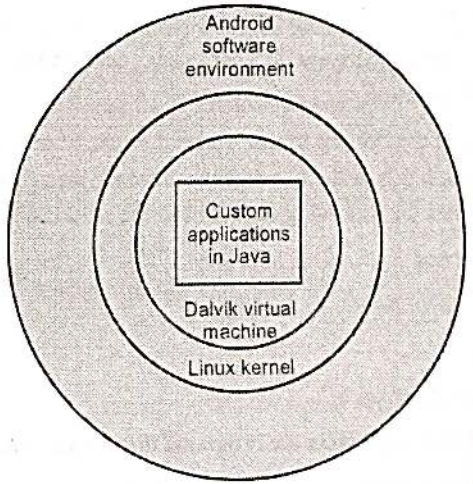

Fig. 6.4.2 : Android environment

6.4.3.1 Layers of Android

- Following are the different layers in the Android stack :
  1. Linux Kernel layer
  2. Native layer
  3. Application framework layer
  4. Applications layer

- Fig. 6.4.3 illustrates android stack.

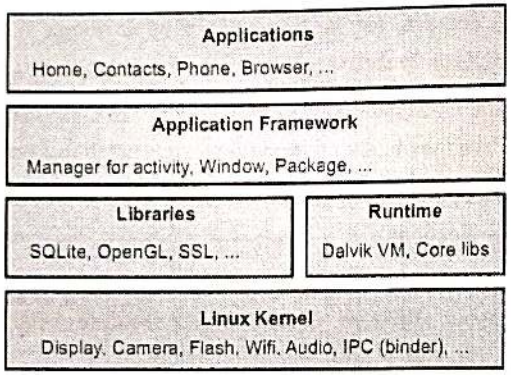

Fig. 6.4.3 : Android stack

1. The Linux kernel layer

- The Linux kernel includes drivers for hardware, networking, file system access and inter-process-communication.
- The Linux kernel is at the bottom of the Android stack. It never really interacts with the users and developers, but is at the heart of the whole system. Its importance stems from the fact that it provides the following functions in the Android system :
  a) Hardware abstraction
  b) Memory management programs
  c) Security settings
  d) Power management software
  e) Other hardware drivers (Drivers are programs that control hardware devices.)
  f) Support for shared libraries
  g) Network stack

2. Native code libraries layer

- The next layer in the Android architecture includes **Android's native libraries**. Libraries carry a set of instructions to guide the device in handling different types of data. For instance, the playback and recording of various audio and video formats is guided by the media framework library.
- The native libraries includes daemons and services (written in C or C++) like browser technology from WebKit, database support via SQLite, advanced graphics support (2D, 3D and animation from scalable games language), audio and video media support from PacketVideo's OpenCORE.

Android Runtime

- The Android runtime are written in Java and executing in Dalvik. The core Java packages used for a full-featured Java programming environment and the Dalvik VM, employs services of the Linux-based kernel to provide an environment to host Android applications.
- Dalvik is open-source software. It is the software responsible for running apps on Android devices.

3. Application framework layer

- An important block of application framework is application manager. The application managers include windows, contents, activities, telephony, location and notifications.

4. Application layer

- The applications are at the topmost layer of the Android stack. An average user of the Android device would mostly interact with this layer (for basic functions, such as making phone calls, accessing the Web browser etc.).
- The layers further down are accessed mostly by developers, programmers and the likes.
- Several standard applications come installed with every device, such as :
  a) SMS client app b) Dialer
  c) Web browser d) Contact manager

6.4.4 Palm OS

- Palm OS is an embedded operating system designed for ease of use with a touchscreen-based graphical user interface.
- It has been implemented on a wide variety of mobile devices such as smart phones, barcode readers and GPS devices.
- It is run on Arm architecture-based processors. It is designed as a 32-bit architecture.

6.4.4.1 Features of Palm OS

- The key features of Palm OS are :

1. A single-tasking OS :

- Palm OS Garnet (5.x) uses a kernel developed at Palm, but it does not expose tasks or threads to user applications. In fact, it is built with a set of threads that cannot be changed at run-time.

- Palm OS Cobalt (6.0 or higher) does support multiple threads but does not support creating additional processes by user applications.
- Palm OS has a preemptive multitasking kernel that provides basic tasks but it does not expose this feature to user applications.

2. Memory management :

- The memory, RAM and ROM, for each Palm reside on a memory module known as card. In other words, each memory card contains RAM, ROM or both.
- Palms can have no card, one card or multiple cards.

3. Expansion support :

- The expansion capability not only augments the memory and I/O, but also it facilitates data interchanges with other Palm devices and with other non-Palm devices such as digital cameras and digital audio players.
  a) Handwriting recognition input called Graffiti 2.
  b) HotSync technology for synchronization with PC computers
  c) Sound playback and record capabilities
  d) TCP/IP network access
  e) Support of serial port, USB, infrared, bluetooth and Wi-Fi connections
  f) Defined standard data format for PIM (Personal Information Management) applications to store calendar, address, task and note entries, accessible by third-party applications

4. Security model :

- Device can be locked by password, arbitrary application records can be made private.
- Palm OS Cobalt includes a certificate manager. The certificate manager handles X.509 certificates.

6.4.5 Symbian OS

- Symbian OS is 32 bit operating system, running on different flavors of ARM architecture.
- It is a multitasking operating system and very less dependence on peripherals.
- Kernel runs in the privileged mode and exports its service to user applications via user libraries.

6.4.5.1 Architecture of Symbian OS

- User libraries include networking, communication, I/O interfaces and etc.
- Access to these services and resources is coordinated through a client-server framework.
- Clients use the service APIs exposed by the server to communicate with the server.
- The client-server communication is conducted by the kernel.
- The Symbian OS architecture is shown in Fig. 6.4.4.

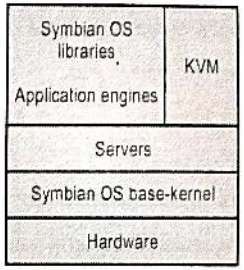

Fig. 6.4.4 : Symbian OS structure

6.4.5.2 Features of Symbian OS

1. **Symbian is real-time OS :** It has a real-time, multithreaded kernel.
2. **Data Caging :** Symbian OS allows applications to have their own private data partition. This feature allows for applications to guarantee a secure data store. It can be used for e-commerce applications, location aware applications and etc.
3. **Multimedia :** Symbian OS supports audio, video recording, playback and streaming and image conversion.
4. **Platform Security -** Symbian OS provides a security mechanism against malware.
   - It allows sensitive operations can be accessed by applications which have been certified by a signing authority.
   - In addition, it supports full encryption and certificate management, secure protocols (HTTPS, TLS and SSL) and WIM framework.
5. **Internationalization support :** Symbian OS supports unicode standard.
6. Symbian OS is **fully object-oriented and component- based.**
7. Optimized memory management.

8. **Client-server architecture :** Symbian OS provides simple and high-efficient inter-process communication. This feature also eases porting of code written for other platforms to Symbian OS.
9. **A Hardware Abstraction Layer (HAL) :** This layer provides a consistent interface to hardware and supports device-independency.

6.4.6 Blackberry OS

- Blackberry OS has a multitasking environment. It enables heavy use of input devices like trackball and scroll wheel. It does not support touchpad.
- Blackberry OS is an event-driven operating system.
- Blackberry smartphone's CPU architecture is based on ARM XScale. The other BlackBerry device has Intel-based processors.
- Blackberry OS supports multitasking and multithreading applications.
- Any application that wants to use certain BlackBerry functionality must be digitally signed.

6.4.6.1 Features of Blackberry OS

1. **Multitasking -** Blackberry OS employs co-operative multitasking so no application can pre-empt another application in mid-stream, unless that application explicitly yields control.
2. **Threads -** Foreground threads can be switched by applications requesting a new application to be replaced on the foreground by calling RimRequestForeground.
   - Communication between OS and threads is done by a messaging system.
   - Like event-driven systems, applications receive messages describing system events and associate parameters. Then, they post them to threads to process.
3. **Message Services -** BB OS is an event-driven OS. This means that BB applications receive all external notifications through events sent to the applications.
   - Applications process the events. Since the process is completed, they call the RIMGETMESSAGE function to receive the next event.
4. **Asynchronous Message Services -** For asynchronous communication (non-blocking send), applications send message to another application messages' queue by calling RimPostMessage. The destination receives messages. The sending process continues execution immediately after the call to RimPostMessage.
5. **Synchronous Message Services -** In synchronous communications (blocking send), applications send messages to other application's message queue by calling RimSendMessage and blocks the sending process until it receives responses from the destination.

6.4.7 Comparison of Features of Mobile OS

Sr. No.	Feature	Symbian	Android	iOS	Blackberry OS	Windows phone
1.	Multitasking	Full	Full	Optimized	Full	Optimized
2.	Notification LED	Yes	Yes	No	Yes, 7 colours	No
3.	Profiles	Yes	No	No	Yes	No
4.	Free turn-by-tune navigation	Yes	Limited to a few countries	No	No	In pipeline for Nokia phones
5.	Offline maps	Yes	No	No	No	In pipeline for Nokia phones
6.	Custom ring-tones	Yes	Yes	No	Yes	Limited
7.	Access to device filesystem	Yes	Yes	No	Yes	No

Review Questions

1. Write a short on the following commercial OS :
   a. Windows Mobile b. Palm OS
   c. Symbian OS d. Ios
   e. Android f. Kernel
   g. Blackberry OS
2. Comparison of features of various mobile OS.

6.5 Android Application Development

- Android applications are primarily written in the Java programming language.
- During development the developer creates the Android specific configuration files and writes the application logic in the Java programming language.
- The ADT or the Android studio tools convert these application files, transparently to the user, into an Android application.
- When developers trigger the deployment in their IDE, the whole Android application is compiled, packaged, deployed and started.

6.5.1 Conversion from Source Code to Android Application

- The Java source files are converted to Java class files by the Java compiler.
- The Android SDK contains a tool called dx which converts Java class files into a *.dex* (Dalvik Executable) file. All class files of the application are placed in this .dex file.
- During this conversion process redundant information in the class files are optimized in the *.dex* file. For example, if the same **String** is found in different class files, the *.dex* file contains only one reference of this **String**.
- These *.dex* files are therefore much smaller in size than the corresponding class files.
- The *.dex* file and the resources of an Android project, e.g., the images and XML files, are packed into an *.apk* (Android package) file. The program aapt (Android Asset Packaging Tool) performs this step.
- The resulting *.apk* file contains all necessary data to run the Android application and can be deployed to an Android device via the adb tool.

Review Questions

1. Define android and their applications.
2. Explain the components of android applications.

6.6 Software Development Kit (SDK)

- Various Android development tools are :

6.6.1 Android SDK

- The Android Software Development Kit (Android SDK) contains the necessary tools to create, compile and package Android applications. Most of these tools are command line based.
- The primary way to develop Android applications is based on the Java programming language.
- Android SDK can be freely downloaded from Android website.

6.6.2 Android Debug Bridge (ADB)

- The Android SDK contains the Android Debug Bridge (ADB), which is a tool that allows you to connect to a virtual or real Android device, for the purpose of managing the device or debugging your application.

6.6.3 Android Developer Tools and Android Studio

- Google provides two Integrated Development Environments (IDEs) to develop new applications.
- The Android Developer Tools (ADT) are based on the Eclipse IDE. ADT is a set of components (plug-ins), which extend the Eclipse IDE with Android development capabilities.
- Google also supports an IDE called Android Studio for creating Android applications. This IDE is based on the IntelliJ IDE.
- Both IDEs contain all required functionality to create, compile, debug and deploy Android applications. They also allow the developer to create and start virtual Android devices for testing.

6.6.4 Dalvik Virtual Machine (DVM)

- Android uses the Dalvik virtual machine with just-in-time compilation to run Dalvik byte code, which is usually translated from Java byte code.
- According to Google's Android documentation, the Dalvik VM is an interpreter-only virtual machine that executes files in the Dalvik Executable (.dex) format, a format that is optimized for efficient storage and memory-mappable execution.
- The virtual machine is register-based and it can run classes compiled by a Java language compiler that have been transformed into its native format.
- Currently Android versions use the Dalvik virtual machine. The latest Android versions introduced a new runtime the Android RunTime.

6.6.5 Android RunTime (ART)

- With Android 4.4, Google introduced the Android RunTime (ART) as optional runtime for Android 4.4. It is uses as default runtime for all Android versions after 4.4.
- ART uses Ahead of Time compilation. During the deployment process of an application on an Android device, the application code is translated into machine code. This result in approximately 30 % larger compiles code, but allows faster execution from the beginning of the application.
- This also saves battery life, as the compilation is only done once, during the first start of the application.

- The **dex2oat** tool takes the .dex file created by the Android tool change and compiles that into an Executable and Linkable Format (ELF file). This file contains the dex code, compiled native code and meta-data. Keeping the .dex code allows that existing tools still work.
- The garbage collection in ART has been optimized to reduce times in which the application freezes.

6.6.6 Features of SDK

- Important features of Android SDK are as under.

1. No licensing, distributions or development fees or release approval processes.
2. Full multimedia hardware control.
3. APIs for using sensor hardware including accelerometer and the compass.
4. APIs for location based services.
5. Android Inter-Process Communication (IPC).
6. Shared data storage.
7. Background applications and processes.
8. Home screen widgets, live folders.
9. HTML5 WebKit-based web browser.
10. GSM, EDGE and 3G networks for telephony and data transfer.
11. The Android SDK includes development tools which helps compile and debug any app.
12. Android emulator shows how app will look and behaviour on a real Android device.

Review Questions

1. Define Android SDK. Compare Java byte code with Android byte code.
2. Explain the features of SDK.

6.7 M Commerce

- Mobile commerce services are evolving rapidly in India due to the coming together of mobile service providers, banks and payment service providers to offer more products and secure transactions through mobile networks.
- While e-commerce is limited to PC users only, mobile commerce is open to almost everyone with a cellphone and mobile connection.

- Mobile commerce is expected to grow because the mobile usage and ownership penetration is more than 4 to 5 times than a PC and growing at a very fast rate. With mobile commerce offerings expanding, customers in India have the hand-held convenience of using their mobile phones for making payments for taxi fares and recharging prepaid phone cards.

Definitions of M-Commerce

1. Mobile commerce is the buying and selling of goods and services through wireless hand-held devices such as mobile phones, Personal Digital Assistants (PDAs), smartphones, handheld gaming devices and computers.
2. Mobile commerce is defined as any transaction with a monetary value that is conducted via a mobile telecommunications network.
3. Mobile commerce is about the purchase and sale of goods and services through the cellphone with the involvement of a financial institution.

Examples of M-Commerce

- Mobile commerce includes the following :

a) Travel and ticketing b) Movie ticketing

c) Bill payments to utility and service companies

d) Merchant and retail transactions

e) Money transfer

Advantages of M-Commerce over E-Commerce

- In comparison to e-commerce, m-commerce offers both advantages and disadvantages. The following list summarises the advantages of m-commerce :

1. **Ubiquity :** The use of wireless device enables the user to receive information and conduct transactions anywhere, at anytime.
2. **Accessibility :** Mobile device enables the user to be contacted at virtually any time and place. The user also has the choice to limit their accessibility to particular persons or times.
3. **Convenience :** The portability of the wireless device and its functions from storing data to access to information or persons.
4. **Localization :** The emergence of location-specific based applications will enable the user to receive relevant information on which to act.
5. **Instant connectivity (2.5G) :** Instant connectivity or "always on" is becoming more prevalent will the emergence of 3 G networks, GPRS or EDGE. Users of 3 G services will benefit from easier and faster access to the Internet.

6. **Personalization :** The combination of localization and personalization will create a new channel/business opportunity for reaching and attracting customers. Personalization will take the form of customized information, meeting the users' preferences, followed by payment mechanisms that allow for personal information to be stored, eliminating the need to enter credit card information for each transaction.
7. **Time sensitivity :** Access to real-time information such as a stock quote that can be acted upon immediately or a sale at a local boutique.
8. **Security :** Depending on the specific end user device, the device offers a certain level of inherent security.

6.7.1 B2C (Business to Customer) Applications

- In B2C commerce, commercial transactions are between organization and consumers directly who are the end-users of its products or services.
- The business-to-consumer, consumer concerns the use of Information and Communication Technology (ICT) to enable forms of cash and credit commerce between a company and its consumers.

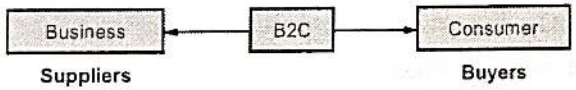

Fig. 6.7.1

- The examples of B2C commerce are :
  1. E-tailors : The companies offering multimedia website that provide shopping mall.
  2. Portal : Interactive order processing and secure electronic payment systems.
  3. Transaction broker/ market creator.

6.7.2 B2B (Business to Business) Commerce

- In B2B commerce, commercial transactions are between an organization and other organizations i.e. companies doing business with each other.
- The B2B commerce concerns the use of Information and Communication Technology (ICT) to enable terms of credit and repeat commerce between a company and its suppliers.

Fig. 6.7.2

- The examples of B2B commerce are :
  1. Many companies offering variety of marketing and product information on the world wide web.
  2. Market place /hub.
  3. B2B service provider.

6.7.3 M-Commerce Structure/Components

- A mobile commerce transaction may involve multiple network components such as location database, user preference database and multicast server. Also different transactions may require very different types and number of network components.

1. Extended SIM card

- It has a Public-Key Infrastructure (PKI) enabled smart card, an extended SIM card (ESIM) which is a modified and customized version of the current SIM card. Certificates and necessary public/private keys are stored in it. With PKI and secret keys, this infrastructure can ensure mutual authentication, confidentiality, integrity and non-repudiation in financial transactions.
- ESIM is issued by a mobile operator in association with the proposed identity provider (banks).

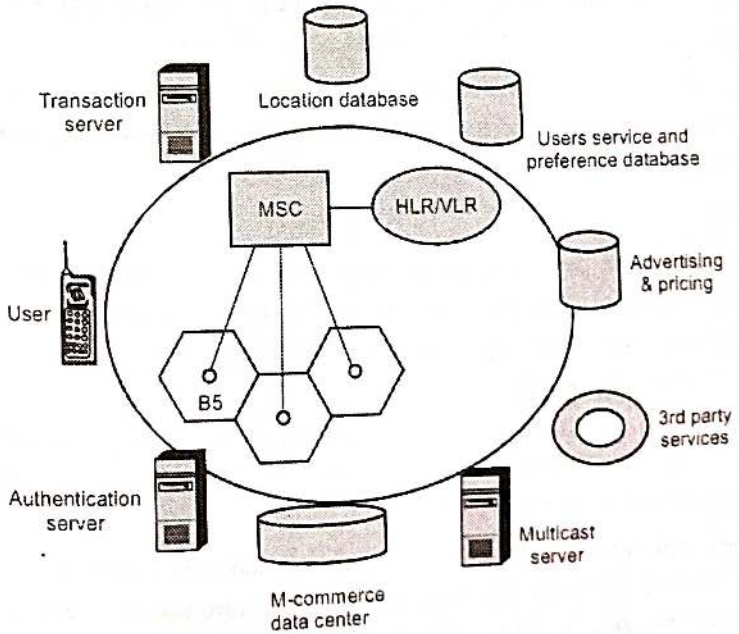

Fig. 6.7.3 : Components of M-commerce

- ESIM might have several modules; one provides the access to mobile operator's services and the other modules may act as the infrastructure of providing identity handling services. To activate the later requires an additional authentication mechanism using a separate PIN code and it holds the m-commerce mechanism.

2. NFC (Near Field Communication)

- NFC is a technology that offers short-range communication between two devices. Introduction of NFC adds intelligence and networking capabilities to the phone and creates many new opportunities like digital transactions in very good proximities. It can make mobile phone an ideal device for payments. Therefore, the proposed m-commerce mechanism decides NFC as the short range communication technology for local mobile payments.
- To establish secure channel between devices, various cryptographic protocols (RSA, 3DES, AES etc.) can be used. Almost all the trials in local payments are going on using NFC.

3. Mobile banking

- An ESIM will be issued to the user when registered for mobile banking. It contains the certificate to authenticate the user to banks. User can make account transfer, check the balance, view and pay the bills, order credit card to use from mobile phone, subscribe for digital cash and thereby load the mobile phone with it etc.
- Traditional SMS banking is also possible. Use can set various SMS alerts in the account and can make enquiries. Therefore, mobile banking is a way to realize payments ranging micro to macro remotely.

4. Credit card

- Most of the remote payment requires credit card but most mobile users do not own credit card. Number of people using mobile phones is increased many fold than the people having credit cards. These motivate including easy-to-use credit card solutions into the proposed mechanism.
- Upon registering for mobile banking user can also subscribe for credit card. Bank then issues a separate certificate to the user for using credit card facilities from mobile phone. The certificate will be stored in the SIM card.
- This credit card can be used both for local payment and remote payment in macro, mini and micro level. The major advantage of it is, credit card can also be used for macro-level remote payments without compromising user's security (besides local micro-level payment provisions).

5. Digital cash (DigiCash)

- Traditional physical cash provides the user a high degree of privacy, as it is not traceable to a single user. User expects the similar privacy provision in mobile commerce.
- The user receives an inactive digital wallet during subscription. Through online mobile banking, user can subscribe and thereby activate the wallet. Afterwards, user can load the cash in the digital form to this wallet from his/her bank account. This can be used for digital cash creation, negotiation and payment. The vendor's POS requires the similar digital cash handling capabilities.
- This is how the proposed mechanism ensures privacy and anonymity to a mobile user in m-commerce. The digital cash serves the local payment only.

6.7.4 M-Commerce Applications

- The general m-commerce applications are :

1. Mobile ticketing

- Tickets can be sent to mobile phones using a variety of technologies. Users are then able to use their tickets immediately by presenting their phones at the venue.
- Tickets can be booked and cancelled on the mobile with the help of simple application downloads or by accessing WAP portals of various Travel agents or direct service providers. Mobile ticketing for airports and train stations, for example, will not only streamline unexpected metropolitan traffic surges, but also help users remotely secure parking spots (even while in their vehicles) and greatly facilitate mass surveillance at transport hubs.

2. Mobile vouchers, coupons and loyalty cards

- Mobile ticketing technology can also be used for the distribution of vouchers, coupons and loyalty cards. The voucher, coupon or loyalty card is represented by a virtual token that is sent to the mobile phone. Presenting a mobile phone with one of these tokens at the point of sale allows the customer to receive the same benefits as another customer who has a loyalty card or other paper coupon/voucher.
- Mobile delivery enables :
  a) Economy of scale
  b) Quicker and easier delivery
  c) Effective target marketing

d) Privacy-friendly data mining on consumer behaviour.

e) Environment-friendly and resources-saving efficacy.

3. Content purchase and delivery

- Currently, mobile content purchase and delivery mainly consists of the sale of ring-tones, wallpapers and games for mobile phones. The convergence of mobile phones, mp3 players and video players into a single device will result in an increase in the purchase and delivery of full-length music tracks and video. Download speeds, if increased to 4G levels, will make it possible to buy a movie on a mobile device in a couple of seconds, while on the go.

4. Location-based services

- Unlike a home PC, the location of the mobile phone user is an important piece of information used during mobile commerce transactions. Knowing the location of the user allows for location based services such as :

  a) Local maps b) Local offers

  c) Local weather d) People tracking and monitoring.

5. Information services

- A wide variety of information services can be delivered to mobile phone users in much the same way as it is delivered to PCs. These services include :

  a) News services b) Stock data

  c) Sports results d) Financial records

  e) Traffic data and information.

- Particularly, more customized traffic information, based on users' travel patterns, will be multicast on a differentiated basis, instead of broadcasting the same news and data to all users. This type of multicasting will be suited for more bandwidth-intensive mobile equipment.

6. Mobile banking

- Banks and other financial institutions are exploring the use of mobile commerce to allow their customers to not only access account information, but also make transactions, e.g. purchasing stocks, remitting money, via mobile phones and other mobile equipment. This service is often referred to as mobile banking or M-banking.

- More negative issues like ID theft, phishing and pharming are lurking when it comes to mobile banking, particularly done on the mobile web. Net security technology free from redundancy and paradigm shifts away from mobile web-based banking will be an optimal solution to mobile banking in the near future.

7. Mobile brokerage

- Stock market services offered via mobile devices have also become more popular and are known as mobile brokerage. They allow the subscriber to react to market developments in a timely fashion and irrespective of their physical location.

8. Auctions

- Over the past three years mobile reverses action solutions have grown in popularity. Unlike traditional auctions, the reverse auction (or low-bid auction) bills the consumer's phone each time they place a bid. Many mobile PSMS commerce solutions rely on a one-time purchase or one-time subscription; however, reverse auctions are high return applications as they allow the consumer to transact over a long period of time.

9. Mobile purchase

- Mobile purchase allows customers to shop online at any time in any location. Customers can browse and order products while using a cheap, secure payment method. Instead of using paper catalogues, retailers can send customers a list of products that the customer would be interested in, directly to their mobile device or consumers can visit a mobile version of a retailer's ecommerce site.
- Additionally, retailers will also be able to track customers at all times and notify them of discounts at local stores that the customer would be interested in.

10. Mobile marketing and advertising

- Mobile marketing is an emerging concept, but the speed with which it's growing its roots is remarkable. Mobile marketing is highly responsive sort of marketing campaign, especially from brands' experience point of view. And almost all brands are getting higher campaign response rates.
- Corporations are now using m-commerce to expand everything from services to marketing and advertisement. Although there are currently very few regulations on the use and abuses of mobile commerce, this will change in the next few years. With the increased use of m-commerce comes increased security. Cell phone companies are now spending more money to protect their customers and their information from online intrusions and hackers.

6.7.5 Advantages and Disadvantages of M-Commerce

Advantages

- The advantages of m-commerce are :
  1. Providing wider reach
  2. Reducing transaction cost
  3. Streamline business processes
  4. Competitive pricing
  5. Reducing time to order
  6. Purely personal
  7. Secure
  8. Location and time independent

Disadvantages

- The disadvantages of m-commerce are :
  1. Technology constraints of mobile devices (memory, processing power, display capabilities, input methods).
  2. User interface is often difficult to learn how to use.
  3. Use of graphics limited
  4. WAP and SMS limited to small number of characters and text.
  5. Limited bandwidth.
  6. Small screens of most devices still limit types of file and data transfer.
  7. WAP and SMS limited to small number of characters and text.
  8. Cost of establishing mobile and wireless broadband Infrastructure.
  9. Mobile devices are more prone to theft and destruction.
  10. The communication over the air interface between mobile device and network introduces additional security threats.

Review Questions

1. Define M-commerce.
2. Explain B2C commerce.
3. Explain B2B commerce.

4. List the features required by a mobile device to potentiate M-commerce.
5. Describe the architecture of a M-commerce.
6. List the application of M-commerce and explain any one application.
7. Explain the pros (advantages) of M-commerce.
8. Discuss the pros and cons of M-commerce.
9. Discuss the cons (disadvantages) of M-commerce.

6.8 Mobile Payment System

- **Mobile payment** is also referred to as **mobile money, mobile money transfer** and **mobile wallet.**.
- Mobile payments are gaining popularity with consumers not only for their convenience but also for their security, because with many types of mobile PoS systems, credit card data is not saved on the merchant's PoS terminal.
- **Mobile payment** is a payment services operated under financial regulation and performed from a mobile device.
- **Mobile payment** (m-payment) is a Point-of-Sale (PoS) transaction made or received with a mobile device.

6.8.1 Types of Mobile Payment System

- A GSM mobile phone may send or receive information (mobile data service) through three possible channels - SMS, USSD or WAP/GPRS.
- There are a few different types of mobile payment systems that all work a bit differently.

1. Near Field Communication (NFC) :

- NFC is the fusion of contactless smartcard (RFID) and a mobile phone. The mobile phone can be used as a contactless card. NFC enabled phones can act as RFID tags or readers. This creates opportunity to make innovative applications especially in ticketing and couponing.
- NFC provides contactless, almost instantaneous transfer of data between devices. NFC is often used in "Tap and Go" payment methods, such as tapping the smartphone to a device reader.

2. Wireless Application Protocol (WAP)/GPRS :

- General Packet Radio Service (GPRS) is a mobile data service available to GSM users. GPRS provides packet-switched data for GSM networks. GPRS enables services such as Wireless Application Protocol (WAP) access, Multimedia Messaging Service (MMS) and for Internet communication services such as email and World Wide Web access in mobile phones.
- With WAP, the smartphone connects to the internet, then pays via an online payment system (such as Paypal or Google Wallet) or by entering credit card info through the merchant's website.

3. Short Messaging Service (SMS) payments :

- SMS can be used to provide information about the status of one's account with the bank (informational) or can be used to transmit payment instructions from the phone (transactional).
- SMS allows users to pay for goods and services via a text message sent from the phone. The cost of the item is then added to the user's monthly phone bill.

4. In-App Billing or Direct Mobile Billing :

- Most commonly used when purchasing an app from an online store or a game, this system charges the cost of the product to the monthly phone bill.

5. Mobile Wallet :

- A m-payment application software that resides on the mobile phone with details of the customer (and his or her bank account details or credit card information) which allows the customer to make payments using the mobile phone is called as a **mobile wallet**.
- Customers can multi-home with several debit or credit payment instruments in a single wallet. Several implementations of wallets that are company-specific are in use globally.

6. Unstructured Supplementary Services Delivery (USSD) :

- Unstructured Supplementary Service Data (USSD) is a technology unique to GSM. It is a capability built into the GSM standard for support of transmitting information over the signaling channels of the GSM network.
- USSD provides session-based communication, enabling a variety of applications. USSD is session oriented transaction-oriented technology while SMS is a store-and-forward technology.
- Turnaround response times for interactive applications are shorter for USSD than SMS.

6.8.2 Advantages of Mobile Payment System

- The major benefits of MPS as under :

1. Security :

- Mobile payments help to reduce the chances of stealing, hacking and other fraudulent activities as mobiles carry huge security features as the fingerprint scanner, pin, pattern code and many other options to make your payment safe and secure from misuse.

2. Reduces time :

- The speed at which m-payments are executed is acceptable to both customers and merchants.
- It reduces the time as it is faster than any other form of payments. The time savings can also increase profits by allowing you to put up more customers at the same time, especially for businesses with a busy scheduled during the day like a lunch rush at a restaurant.

3. Lower cost :

- Basic advantage is the **lower costs** of using a mobile card reader or barcode scanner than carrying a credit card terminal from a bank that also charges merchants/ retailers with a monthly fee and the transaction fees.

4. Involve customers :

- By offering a lot of mobile payment options to customers offline and online, helps to make the purchase process easier for them. This in turn increases the number returning customer and the conversion rates for the businesses.

6.8.3 Characteristics of Mobile Payment System

- Important characteristics of mobile payment system are :

1. **Simplicity and usability :** The m-payment application must be user friendly to the customer. The customer must also be able to personalize the application to suit his or her convenience.
2. **Universality :** M-payments service must provide for transactions between one customer to another customer (C2C) or from a business to a customer (B2C) or between businesses (B2B).
3. **Ubiquitous :** Highly ubiquitous. New payment products must work everywhere, all the time.

4. **Security and privacy :** Mobile payment system should be highly secure, foolproof, resistant to attacks from hackers and terrorists. This may be provided using public key infrastructure security, biometrics and passwords integrated into the mobile payment solution architectures.
5. **Cost :** The m-payments should not be costlier than existing payment mechanisms to the extent possible. A m-payment solution should compete with other modes of payment in terms of cost and convenience.
6. **Speed :** The settlement of m-payments must be instantaneous.

Review Questions

1. Define mobile payment systems.
2. Explain different M-payment mechanisms that exit at present.
3. Explain different M-payment schemes (mechanisms) that exist at present.
4. Discuss the different M-payment solution in a M-commerce.
5. Discuss a model of M-payment process.
6. List the characteristics of M-payment system.
7. Explain the properties (characteristics) of M-payment system.

6.9 Security Issues in Mobile Computing

- Security serves as a fundamental critical success factor in relation to mobile payment system. If the security is low or unacceptable, then the payment system should never be introduced.
- Security is regarded as a challenging issue for mobile payment that can be challenged during sensitive and confidential payment information handling and transmission.
- Cryptography is the study of mathematical techniques related to the aspects of information like confidentiality, message integrity, entity authentication etc.
- Cryptography provides the means to ensure that objectives of communicating parties are met.
- The security requirements for payment transaction include authentication, integrity of payment data, confidentiality, anti-replay protection, anonymity, privacy protection authorization and non-repudiation.

1. Authentication and Confidentiality

- **Confidentiality** is a protection against eavesdroppers who understand intercepted messages by keeping information secret from all but available for those who are authorized to see it.

- **Authentication** means prove the identity of someone claiming to be a particular party.
- The design of mobile payment schemes will be more focuses on authentication between payer and payee. Both authentication and confidentiality properties can be achieved by employing asymmetric encryption such as Public Key Infrastructure (PKI), Message Authentication Code (MAC), digital signature or symmetric encryption.

2. Integrity of Payment Data

- Integrity of payment data assures that the transaction data has not been changed or altered enroute by unauthorized or unknown means.
- Integrity protects against the threat of corruption or modification of information (either accidentally or intentionally).
- The security mechanism of payment schemes should be able to prevent and detect alterations of the payment data from engaging parties and attack from outsiders such eavesdroppers, attackers, etc. hashing algorithm, encryption or MAC can be applied to preserves the integrity of payment data.

3. Authorization

- Authorization is the function of specifying access rights to resources and it is very crucial for payment transaction.

4. Non-Repudiation

- Non-repudiation concerns about prevention of any deny for previous commitments or actions by the communicating parties and it works closely with authorization properties.
- The security mechanism should able to assure that payer must not be charged on the payment that he has never made.

5. Privacy Protection

- Privacy concerns exist wherever personally identifiable information is collected and stored - in digital form or otherwise.
- Improper or non-existent disclosure control can be the root cause for privacy issues. The privacy protection is includes identity privacy protection and transaction privacy transaction.
- The payment protocol should provide the privacy protection to payer.

6. Anti-Replay Protection

- Anti-replay protection ensures that if an attacker captures a message and transmits it again later; the receiver will not accept the message. This malicious activity known as man-in-the-middle attacks.

- The payment protocol should prevent an adversary from trying to intercepts an encrypted message and transmits it again.

7. Anonymity

- Anonymity refers to the personal identity or personally identifiable information of that person is being unknown.
- Payers may needs protect their identity from eavesdroppers and (optionally) from payee Financial Service Providers (FSPs) and Payment Service Providers (PSPs).

Review Question

1. Describe the security issues in M-commerce.

6.10 Security Requirements of Wireless Networks

- Wireless networks are inherently insecure compared to wired networks. Digital systems (TDMA and CDMA) are little difficult to tap as compared to analog systems.

Privacy requirements

- Encryption is used for providing privacy to wireless networks. Data Encryption Scheme (DES) with 56-bits keys is used. Two levels of privacy security for 56-bits keys are :

1. Level-0 : (None - with no privacy enabled)

- Level-0 privacy is when there is no encryption employed over the air so that anyone can tap into signal.
- Anyone with digital scanner can monitor calls.
- A "lack of privacy" indicator should be provided - a public trust issue.

2. Level-1 : (Equivalent to wireline)

- Level-1 privacy provides privacy equivalent to that of wireline telephone call.
- Used for routine every day calls.

3. Level-2 : (Commercially secure)

- For commercial applications, a much stronger encryption scheme with key size larger than 80 - bits is appropriate. This is referred to as Level-2 privacy.

4. Level 3 : (Military/Government secure)

- Non breakable.

❑❑❑