Q.52 HLR keeps the _____ of each mobile that belongs to the MSC to which it is interacting.

[a] last location [b] first location
[c] current location [d] none of these [Ans. : c]

Q.53 HLR performs the functions such as _____ to subscribers at their current locations by using user profile information

[a] delivery of calls [b] information and messages
[c] both a & b [d] none of these [Ans. : c]

Q.54 HLR maintains user information in the form of _____ .

[a] static information [b] dynamic information
[c] both a & b [d] none of these [Ans. : c]

Q.55 The static information is the _____ .

[a] international mobile subscriber identity
[b] service subscription information authentication key
[c] all of these [d] account status [Ans. : d]

Q.56 The dynamic information is the _____ area of the mobile subscriber which is the identity of the currently serving VLR.

[a] last location [b] first location
[c] current location [d] none of these [Ans. : c]

Q.57 The HLR handles SS7 transactions with both _____ .

[a] MSCs [b] VLR nodes
[c] both a & b [d] none of these [Ans. : c]

Q.58 VLR main tasks are association with _____ .

[a] MSC [b] IMSI
[c] TMSI [d] roaming
[e] all of these [Ans. : e]

6 Recent Trends

Syllabus

Introduction to Wi-Fi, WiMAX, ZigBee Networks, Software Defined Radio, UWB Radio, Wireless Adhoc Network and Mobile Portability, Security issues and challenges in a Wireless network.

Contents

6.1	Wi-Fi		
6.2	WiMAX	Summer-12,15,16, Winter-12,13,	Marks 7
6.3	ZigBee	Winter-14, Summer-16,	Marks 7
6.4	Software Defined Radio (SDR)	Summer-16,	Marks 7
6.5	UWB Radio	Winter-14,	Marks 7
6.6	Wireless Adhoc Networks		
6.7	Mobile Number Portability	Summer-16,	Marks 7
6.8	Security in Wireless Network		
6.9	Multiple Choice Questions		

6.1 Wi-Fi

- The term Wi-Fi refers to a wireless local area network (WLAN) which is basically an alternative to a wired LAN. WiFi is a technology that allows for networking capabilities without physical cables.
- For a connection to be made over WiFi there must be-
  1. WiFi Access Point
     i. Modem ii. Routers
  2. WiFi Client
     i. Computers ii. Laptops iii. Mobile Phones / Tablet
     iv. Printers
- Wi-Fi allows users to connect various devices to a broadband connection via a wireless router. The broadband connection itself is not wireless, it is the wireless router that converts the internet data it receives from your phone line into radio signals.
- The number 802.11 is a common set of standards for wireless local area network connectivity. These standards allow your devices/computers and your wireless router to communicate using the same language.

6.1.1 WiFi Data Rate

- Normally "b/g" or the letter "n" appears after the number, these letters relate to the version and speed of the standard.

802.11b	11Mbps
802.11g	54Mbps
802.11n	300Mbps

6.1.2 WiFi Connection Schematic

- A WiFi Access Point will broadcast a Network Name (SSID) for Clients to connect. WiFi Access Points can be password protected to increase security of your network and is recommended. (See Fig. 6.1.1 on next page)

6.1.3 Wifi Range

- The 802.11a Wireless Router Range with WiFi technology has an approximate indoor wifi range of 115ft and 390ft outdoors in best weather conditions.

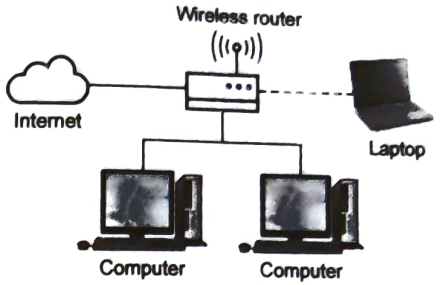

Fig. 6.1.1 WiFi

- Wireless 802.11b/g wifi technology can travel 125ft indoors and can reach out to 460ft outdoors with a clear line of sight.
- The 802.11n wifi technology signals have greater range due the advanced MIMO antenna technology allowing it to penetrate indoors up to 230ft and extend outdoors to a wifi range of 820ft in the best working environment.

Network Standard	Frequency Range	Bandwidth	MIMO Streams	Indoor Range	Outdoor Range
802.11A	5GHz	20MHz	1	115ft	390ft
802.11B	2.4GHz	20MHz	1	125ft	460ft
802.11G	2.4GHz	20MHz	1	125ft	460ft
802.11N	2.4GHz/5GHz	20MHz/40MHz	4	230ft	820ft

6.1.4 WiFi Security

- WEP was the first layer of protection that wireless routers would use to encrypt the channel of communication that devices would use to talk to the router's base station. Widely known to be hackable and the least secure, it's not recommended you use WEP anymore unless you have a very specific reason for turning it on.
- The newest standard called WPA2-PSK is uncrackable, using something known as the Temporal Key Integrity Protocol. This protocol makes sure that every device is handed its very own, pre-encrypted key that can't be hijacked or stolen by any man-in-the-middle attacks that might attempt to impersonate a new user on the network.
- WPA2-PSK protects the password that you create when you first create your wireless network, a specific string of anywhere from 8 to 63 unique characters. Without this, it would be simple for anyone with an iPhone to simply walk by, pick up your signal, and have access to all the devices and computers currently attached to the network at once.

GTU : Summer-12,15,16, Winter-12, 13

6.2 WiMAX

- Towards convergence of voice data and video IEEE 802 committee has introduced 802.16 standards for wireless broadband or wireless MAN (Metropolitan Area Network) or Wireless Microwave Access (WiMAX).
- WiMAX is an acronym meaning "Worldwide Interoperability for Microwave Access.
- The IEEE 802.6 standard offers an alternative to high bandwidth wired access networks like fiber optic, cable modems and DSL. It provides network access to buildings through exterior antennas communicating with radio base stations. Networks can be created just by deploying a small number of base stations on buildings to create high capacity wireless access systems.
- In Wireless MAN the traffic movement between subscribers and core network involves following steps:
  1. Subscriber sends wireless traffic at speeds ranging from 2M to 155 M bit/sec from a fixed antenna on a building.
  2. The base station receives transmissions from multiple sites and sends traffic over wireless or wired links to switching center by using 802.16 protocol.
  3. The switching center sends traffic to an Internet Service Provider (ISP) or the public switched telephone network.

Sub-standards of IEEE 802.16

Standard	Description
IEEE 802.16.1	Air interface for 10 to 66 GHz
IEEE 802.16.2	Coexistence of broadband wireless access systems
IEEE 802.16.3	Air interface for licensed frequencies, 2 to 11 GHz

- Different IEEE 802.16 Standards and its scope is summarized in Table 6.2.1

Standard	Scope
IEEE 802.16	Medium access control (MAC) : one common MAC for wireless MAN standards Physical layer : 10 to 66 GHz
IEEE 802.16a	MAC modifications to 802.16.1 Physical layer : 2 to 11 GHz
IEEE 802.16c	Detailed System Profiles for 10-66 GHz
IEEE 802.16e	Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands
IEEE 802.16.2	Coexistence of Fixed Broadband Wireless Access Systems

Table 6.2.1

6.2.1 IEEE 802.16 Architecture

- The 802.16 standards are organized into three layer architecture.
  1. Physical Layer
  2. MAC Layer
  3. Convergence Layer

Physical Layer

- Physical layer specifies the frequency band, modulation scheme, and error coding techniques, synchronization between transmitter and receiver data rate and the multiplexing structure.
- Both TDD and FDD alternatives support adaptive bursts profiles in which modulation and coding options may be dynamically assigned on a burst-by-burst basis.

MAC Layer

- The MAC layer is designed for point-to-multipoint broadband access.
- The MAC layer is responsible for transmitting data in frames and controlling access to shared wireless medium.
- The MAC protocol defines how and when a base station or subscriber station may initiate transmission on the channel.
- MAC protocol addresses the need for very high bit rates, both uplink (to base station) and down link (from base station).
- MAC protocol is equipped to accommodate services like multimedia and voice.

Convergence Layer

- Convergence layer provides functions specific to the service being provided.
- For IEEE 802 .16.1, bearer services include digital audio/video multicast, digital telephony, ATM, Internet access, wireless trunks in telephone networks and frame relay.

University Questions

1. *Differentiate the WiMAX and WiFi technologies.* GTU : Summer-12, Marks 6
2. *What is WiMax ? How is it different from WiFi ?* GTU : Winter-12, Marks 3
3. *Explain WiMax* GTU : Winter-13, Marks 3
4. *Compare Wi-Fi and Wi-MAX system parameters.* GTU : Summer-15, Marks 7
5. *Compare Wi Fi and Wi Max technologies.* GTU : Summer-16, Marks 7

6.3 ZigBee

- ZigBee is an emerging wireless technology for low-power, low data rate and short range communications between wireless nodes, which is showing a promising future.
- ZigBee is the name given to a specific suite of high level communication protocols using low power digital radios, based on the IEEE 802.15.4 standard for Wireless Personal Area Networks (WPANs).
- ZigBee is a wireless networking standard that is aimed at remote control and sensor applications which is suitable for operation in harsh radio environments and in isolated locations.
- ZigBee, is intended to serve a set of industrial, residential and medical applications with very low power consumption and cost requirement and with much lower requirements in terms of data rate and performance.
- A ZigBee network links a number of electronic devices (nodes). Each node in the network forms part of the transmission chain, receiving messages, deciding if the messages are for local use, and re-transmitting them to other nodes in the network if not.
- A common use of ZigBee is to form 'sensor area networks'. For example in a factory environment many ZigBee nodes can be quickly installed to provide complete low power wireless coverage of the many sensors needed in a factory for fire and burglar alarm systems.

6.3.1 Features of ZigBee

1. Extremely low cost
2. High reliability data transfer
3. very long battery life
4. high security
5. self-healing properties
6. large number of nodes supported
7. ease of deployment
8. guaranteed delivery
9. route optimisation

6.3.2 Frequency Bands

- ZigBee is ideal for wireless sensor networks mainly because of the implementation of a low-power physical layer (PHY). In this design, ZigBee is allowed to operate at

three unlicensed ISM bands: 868 MHz (Europe), 915 MHz (North America), and 2.4 GHz (Worldwide).

Band	Coverage	Data rate	Channels
2.4 GHz ISM	Worldwide	250kbps	16
915 MHz ISM	America	40kbps	10
868 MHz	Europe	20kbps	1

Fig. 6.3.1

6.3.3 ZigBee Protocol Outline

- Computer and computer-related networking is often simplified by using the OSI (Open System Interconnection) model. This divides the tasks involved with moving information between networked devices into smaller, more manageable groups.
- Each layer of the model is responsible for one of these task groups. Each layer is reasonably self-contained so that the tasks assigned to each layer can be implemented independently of other layers. This enables the solutions offered by one layer to be updated without adversely affecting the other layers.
- Fig. 6.3.2 shows the seven layers of the full OSI model. It shows that these layers can be grouped into two areas of action, application issues, which are usually implemented in software, and data-transfer issues, which are realised in hardware and software. The latter includes the Network layer, which deals with planning the route that the data will take between source and destination devices, the Data-link layer, which controls when a device can transmit over the medium being used (copper cable, air, glass fibre etc., and the Physical layer, which includes the electrical and signalling standards used by the transmission.

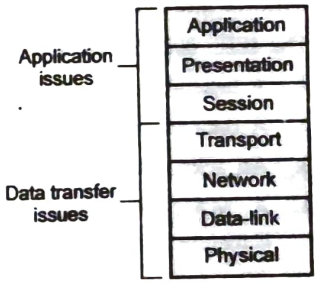

Fig. 6.3.2 Grouping of OSI layers

- The ZigBee protocol can be viewed as three separate layers, each with its own specific functions. The Application layer and some of the functions of the ZigBee Stack layer are usually controlled by a microcontroller, such as a PIC chip. In a typical system, the IC contains circuitry to meet the requirements of the physical layer (PHY) and a portion of the media access controller (hardware-MAC). The

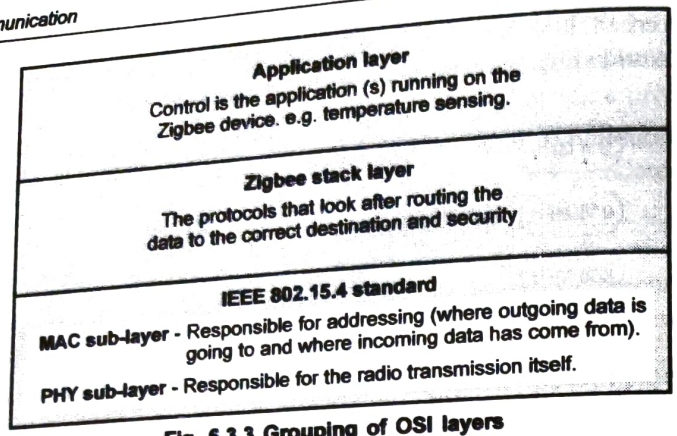

Fig. 6.3.3 Grouping of OSI layers

remaining MAC functions (software-MAC) may also be executed on the microcontroller.

6.3.4 Frame Structure

- The frame structures have been designed to keep the complexity to a minimum while at the same time making them sufficiently robust for transmission on a noisy channel. Each successive protocol layer adds to the structure with layer-specific headers and footers.
- The IEEE 802.15.4 MAC defines four frame structures:
  1. A beacon frame, used by a coordinator to transmit beacons.
  2. A data frame, used for all transfers of data.
  3. An acknowledgment frame, used for confirming successful frame reception.
  4. A MAC command frame, used for handling all MAC peer entity control transfers.
- The data frame is illustrated in Fig. 6.3.4.
- The Physical Protocol Data Unit is the total information sent over the air. As shown in the illustration above the Physical layer adds the following overhead:

Preamble Sequence	4 Octets
Start of Frame Delimiter	1 Octet
Frame Length	1 Octet

- The MAC adds the following overhead:

Frame Control	2 Octets
Data Sequence Number	1 Octet
Address Information	4 - 20 Octets
Frame Check Sequence	2 Octets

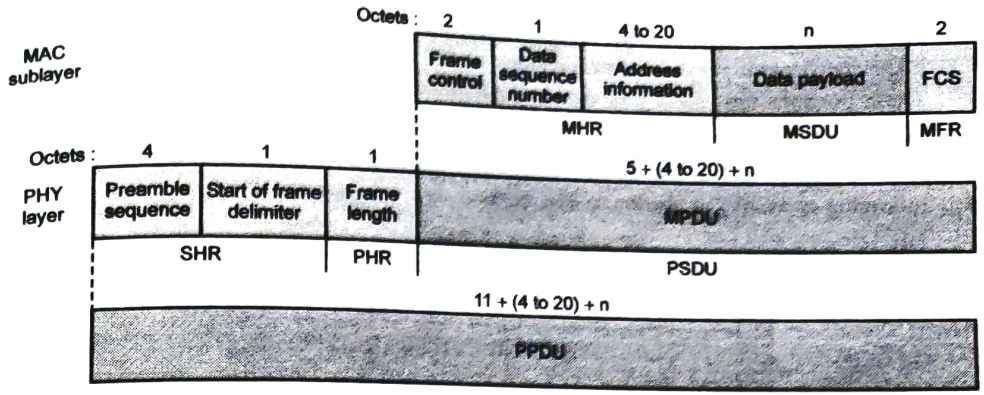

Fig. 6.3.4 Data frame

- Total overhead for a single packet is therefore 15 -31 octets (120 bits); depending upon the addressing scheme used (short or 64 bit addresses). These numbers do not include any security overhead.

6.3.5 Super Frame Structure

- The LR-WPAN standard allows the optional use of a superframe structure. The format of the superframe is defined by the coordinator.

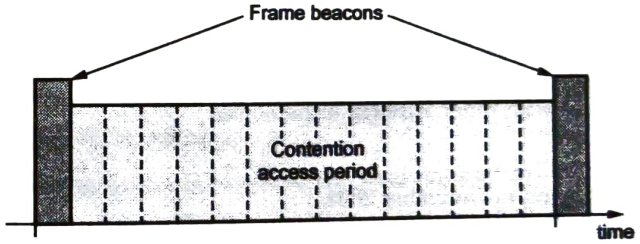

Fig. 6.3.5 Superframe

- The superframe is bounded by network beacons, is sent by the coordinator and is divided into 16 equally sized slots. The beacon frame is transmitted in the first slot of each superframe.
- If a coordinator does not wish to use a superframe structure it may turn off the beacon transmissions. The beacons are used to synchronize the attached devices, to identify the PAN, and to describe the structure of the superframes. Any device wishing to communicate during the contention access period (CAP) between two beacons shall compete with other devices using a slotted CSMA-CA mechanism. All transactions shall be completed by the time of the next network beacon.

- For low latency applications or applications requiring specific data bandwidth, the PAN coordinator may dedicate portions of the active superframe to that application. These portions are called **guaranteed time slots (GTSs)**.
- The guaranteed time slots comprise the contention free period (CFP), which always appears at the end of the active superframe starting at a slot boundary immediately following the CAP, as shown in Fig. 6.3.6.

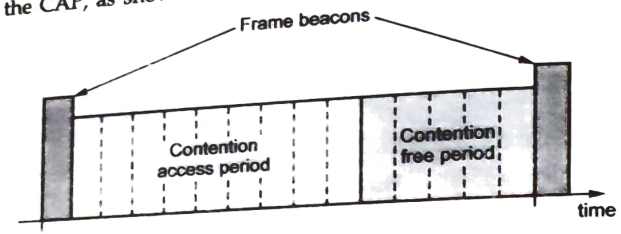

Fig. 6.3.6

- The PAN coordinator may allocate up to seven of these GTSs and a GTS may occupy more than one slot period. However, a sufficient portion of the CAP shall remain for contention based access of other networked devices or new devices wishing to join the network. All contention based transactions shall be complete before the CFP begins. Also each device transmitting in a GTS shall ensure that its transaction is complete before the time of the next GTS or the end of the CFP.

6.3.6 Comparison of Wireless Technologies

- Comparing ZigBee with other wireless technologies :

ZigBee :

- Was formally adopted in December 2004.
- is targeting control applications in industry, which do not require high data raes, but must have low power demand, low cost and offer ease of use (remote controls, home automation, etc.)
- offers data rates of 250 Kbits at 2.4 GHz, 40 kpbs at 915 MHz and 20 Kpbs at 868 MHz with a range of 10-100 m;
- currently offers three levels of security.
- costs around half that of Bluetooth;
- can network up to 256 devices;
- has power requirements much less than Bluetooth;
- uses star, tree or mesh topology.

Blue tooth

- is designed for voice and higher data-rate applications;
- also operates in the 2.4 GHz spectrum :
- operates typica)ly over a distance of 10 metres;
- allows for three modes of security;
- has a ra.nge of ~10 metres;
- has povver requirements of ~40 to 100 mW per device;
- can network up to 8 devices .;

Ultra-Wideband (UWB):

- transmits digital data over a wide frequency spectrum using very low power;
- can transmit data at very high rates (for wireless local area network applications) over distances of up to 10 m;
- has two competing UWB standards currently - one based on direct sequence spread spectrum techniques, (DS-UWB), the other based on Multi-band Orthogonal Frequency Division Modulation (OFDM), with each standard offering data rates around 500 Mbps at a range of 2 metres;
- has povver demands typically twice that of Bluetooth;
- is typically twice as expensive as Bluetooth implementations.

WI-FI (IEEE 802.11. x technologies)

- is typically three times more expensive than Blue tooth implementations;
- uses around five times the power consumption of Bluetooth devices;
- is certified by the Wi-Fi Alliance;
- 802.11a uses OFDM, in the 5GHz bandwith data rates up to 54Mbps;
- 802.11 b uses DSSS, in the 2.4GHz bandwith data rates up to 11 Mbps;
- 802.11g uses OFDM, in the 2.4GHz -bandwith data rates up to 54Mbps;
- 802.1 1 n is likely to operate in the 5GHz bandwith data rates over 100Mbps.

WiMAX (Worldwide Interoperability for Microwave Access)

- is a wireless metropolitan area ner.vork technology;
- has a range of 50 km with data rates of 70 Mbps;
- operates in the 10-66 GHz frequency bands, but requires line of sight;
- supports vehicle mobility of 20 to 100+ km/hr; .
- was created to compete with DSL and cable modem access for rural, hard-to-wire areas.

	ZigBee	Bluetooth	802.11a	802.11b	802.11g	802.11n	UWB
Throughput in Mbps	0.03	1-3	54	11	54	200	200
Max. range in m	30	10	45	60	60	150	10
Power in mW	30	100	1500	750	1000	2000	400
Bandwidth in MHz	0.3	1	20	22	20	40	500

University Questions

1. *Explain the salient features of ZigBee networks.* **GTU : Winter-14, Marks 7**
2. *What is ZigBee? Explain in details ZigBee networks.* **GTU : Summer-16, Marks 7**

6.4 Software Defined Radio (SDR)

GTU : Summer-16

- Software-Defined Radio is basically a wireless communication device where the transmitter and receiver operations are changed or modified by software alone without making any (physical) changes to the hardware. So the functions of the radio can be completely (re)configured with the software, eliminating the need to make any changes to the hardware which can be expensive and time-consuming.
- Software Defined Radio (SDR) is defined as "Radio in which some or all of the physical layer functions are software defined".
- SDR defines a collection of hardware and software technologies where some or all of the radios operating functions (also referred to as physical layer processing) are implemented through modifiable software or firmware operating on programmable processing technologies.
- It is a radio that has the ability to be transformed through the use of software or re-definable logic. They have the ability to go beyond simple single channel, single mode transceiver technology with the ability to change modes arbitrarily because the channel bandwidth, rate, and modulation are all flexibly determined through software. It takes an AM/FM modulated signal from a common RF front end, down convert to baseband frequency and then demodulates it.
- Software Defined Radio (SDR) is a new digital technology wherein radio functions are implemented by signal- processing software running on generic hardware platforms. This makes the system very flexible and adaptive, and thus promises to solve the many problems faced by traditional hardware based radio systems.

Definition by SDR forum

According to SDR forum, "Software Defined Radio (SDR) are Radios that provide software control of a variety of modulation techniques wide and narrowband operation, communication security function and waveform requirements of current and evolving standards over a broad frequency range [SDR forum]"

Concept of SDR

- The primary goal of SDR is to replace as many analog components and hardwired digital VLSI devices of the transmitter-receiver as possible with programmable devices. This include:
  1. Air interface
  2. Modulation and coding schemes
  3. Data converters (ADC/DAC)
- The ultimate goal in radio transceiver design is to implement all transceiver functions in software. This idea is shown in the following Fig. 6.4.1.

Fig. 6.4.1 Typical software-defined radio architecture

- The SDR concept promises the main solution of supporting a multitude of wireless communication services in a single infrastructure design. The need to communicate with people using different types of equipment can only be solved using software programmable radios because of its flexible architecture.
- The key components of SDR architecture are as follows :
  1. Intelligent antenna,
  2. Programmable RF modules,
  3. Digital-to-Analog (DAC) and Analog-to-Digital Converters (ADC),
  4. Digital Signal Processing Techniques
  5. Interconnect Technologies

University Question

1. *Write a short note on software defined radio* **GTU : Summer-16, Marks 7**

GTU : Winter-14

6.5 UWB Radio

- Ultra-wideband radio technology uses extremely short or narrow pulses (sub-nanosecond) with a correspondingly ultra-wideband frequency spectrum to transmit information (data) over relatively short distances (meters).

- The typical type of radio pulse used by UWB is a short sub-nanosecond pulse.
- UWB radio technology is most suited for short range applications i.e. 1 to 10 meters and it support high data rate 100 to 500 Mbps.
- The first definition for a UWB signal was based on the fractional bandwidth $B_{f,3dB}$ of the signal.

The fractional bandwidth is defined as

$$G_{f,3dB} = 2\frac{f_H - f_L}{f_H + f_L}$$

Where, f_L and f_H are respectively the lower and the higher – 3 dB point in a spectrum

Key Benefits of UWB

- UWB has a number of advantages that makes it attractive for consumer communication applications. In particular, UWB systems -
  1. provide high data rates
  2. have very good time domain resolution allowing for ranging and communication at the same time
  3. have immunity to multipath and interference
  4. have potentially low complexity and low equipment cost.

6.5.1 UWB Transceiver Architecture

- UWB technology comes up with increased use for high-speed short range wireless communications, ranging and ad hoc networking.
- There are two competing technologies for UWB wireless communications;
  1. Impulse Radio (IR) and
  2. Multi-band OFDM (MB-OFDM).
- The IR UWB technology is also known as carrier-less technology, because in which the modulated base-band signal is directly transmitted through the antenna into air.
- In this transmission is done with very short pulses with relatively low energy . This attribute reduces the complexity of transceiver architecture.
- Due to low power emission requirement in IR-UWB transceiver naturally reduces the design of antenna predrivers on transmitter side. This feature of IR-UWB is quite opposite to narrowband transceiver where high power; Power Amplifiers are needed to launch the signal with sufficient power to the antenna time hoping impulse radio was introduced as a carrierless modulation scheme, where no up/down conversion of the transmitted/ received signal is required for the transceiver circuitry.

- Whereas in another technology of the UWB i.e. MB-OFDM (Multi-band Orthogonal Frequency Division Multiplexing); the UWB frequency spectrum divided into multiple non-overlapping bands and for each band transmission is OFDM.
- In MB-OFDM the spectrum is divided into several sub-bands with a 10 dB bandwidth of at least 500 MHz. This information is then interleaved across sub-bands and then transmitted through multi-carrier (OFDM) technique.

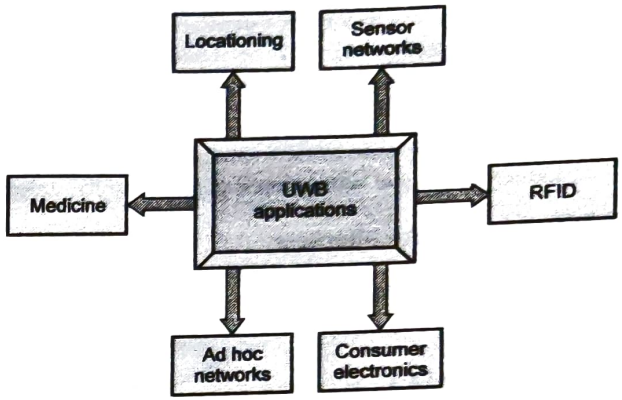

Fig. 6.5.1 Idealized received UWB pulse shape

6.5.2 Transmitter Architecture

- Impulse radio (IR) is also a form of spectrum spreading. IR transmits base band pulses of very short duration, typically on the order of nanosecond or sub-nanosecond.
- In IR scheme there is great reduction in transceiver complexity as well as in overall power consumption because it does not require sinusoidal carriers or any IF processing. Fig. 6.5.2 shows the block diagram of the IR transmitter.
- In IR because of narrowness of the transmitted pulses it has a fine time resolution. This is the most attractive characteristics of IR-UWB which makes impulse-based UWB a prominent andidate technology for indoor positioning.
- The transmitted pulses are produced as modulated pulses with the variable delay. Hence in IR, every symbol is repeatedly transmitted with a low duty cycle over a

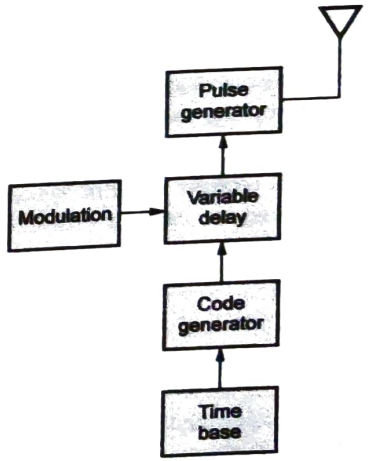

Fig. 6.5.2 Block diagram of IR transmitter

large number of frames with one pulse per frame to gather adequate symbol energy while maintaining low power density.

- Due to impulsive nature of the IR transmission, the multiuser interference may substantially differ from the continuous transmission. This again allows low transmit power when compared to continuous transmission systems. The design of antenna pre-drivers is unwinds on the transmitter side due to low-power emission requirement.
- This is quite opposite to narrowband transceivers. Where high power PAs is needed to launch the signal with sufficient power to the antenna.

6.5.3 Receiver Architecture

- In the receiver architecture analog-to-digital converter (ADC) is inserted just after a low-noise amplifier (LNA) and variable-gain amplifier (VGA), to carry out much of the signal processing in the digital domain. The ADC for such system should operate at extremely high sampling rate of at least 15 G samples/sec with resolution of 4 to 6 bits. Fig. 6.5.3 shows the block diagram of the IR-UWB receiver.

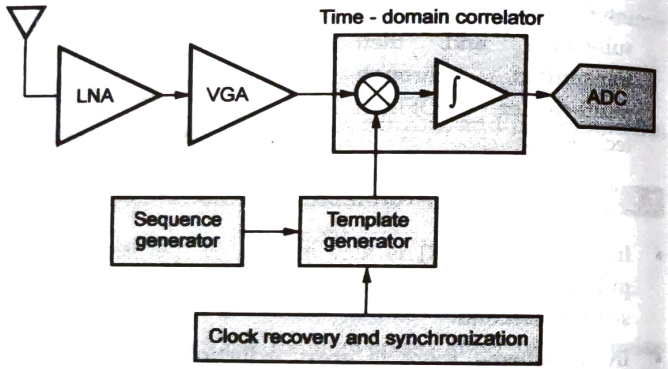

Fig. 6.5.3 Block diagram of an IR-UWB receiver with a time domain correlator

- In the IR receiver some of signal processing is carried out in the analog domain; this is achieved by using a time-integrating analog correlator. This correlator is placed after LNA/VGA and before the ADC.
- The analog correlator consists of a wideband multiplier followed by an integrator. The correlator or multiplier having two inputs first is the input signals and second the template generated by the pulse generator.
- The output of multiplier which is nothing but the product of these two signals is further integrated to produce a robust signal level with relatively low frequency content. Furthermore the receiver needs a precise pulse generator, which provides periodic timing signals at the receiver.

- A series of template pulses are ideally synchronized with the sequence of all the possible transmitted signals which is triggered by the coded timing signal. The correlator then converts the received RF signal to baseband for detection.
- Consequently when the received signal and the reference pulse are synchronized in phase, a peak emerges at the output of correlator.

6.5.4 Applications of UWB

1. UWB application in WSN:
   a) Monitoring Factory Systems and Devices.
   b) WPAN Security
   c) UWB link functions as a cable replacement
2. UWB application in tracking and positioning:
   a. High Accuracy Position and Attitude Integrati :g UWB and MEMS for Indoor Positioning.
   b. High Accuracy Positioning in Hazardous Environments.
3. UWB application in active RFID:
   a. Indoor Real Time Location with Active RFID - System Precision and Possible Applications.
   b. Understanding the Benefits of Active RFID for Asset Tracking
   c. Implementation Example of Active UWB
4. Other applications:
   a. Real-Time Locating Systems in Agriculture: Technical Possibilities and Limitations
   b. Ultra wide band (UWB) of optical fiber Raman amplifiers in advanced optical communication networks.

6.5.5 Advantages, Disadvantages and Applications of UWB Waveform Properties

UWB Property	Advantages	Disadvantages	Applications
Very wide fractional and absolute RF bandwidth	• High rate communications • Potential for processing gain. • Low frequenies penetrate walls, ground.	• Potential interference to existing system. • Potential interference from existing systems.	• High-rate WPAN • Low-power, stealthy comms • Indoor localization • Multiple access.

UWB Property	Advantages	Disadvantages	Applications
Very short pulses	• Direct resolvability of discrete multipath components. • Diversity gair.	• Large number of multipaths • Long synchronization times	• Low-power combined communications and localization.
Persistence of multipath reflections	• Low fade margins • Low power	• Scatter in angle of arrival	• NLOS communications indoors and on ship
Carrierless transmission	• Hardware simplicity • Small hardware	• Inapplicability of super resolution beamforming	• Smart sensor networks.

University Question

1. *Explain in detail about architecture of UWB radio and its applications.*

GTU : Winter-14, Marks 7

6.6 Wireless Adhoc 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 / Need 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 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

6.7 Mobile Number Portability

GTU : Summer-16

- The term "Mobile Number Portability (MNP)" refers to facilities enabling a customer to change his mobile network operator and/or service provider while retaining his existing mobile number.
- **MNP is** defined as the process enabling a mobile subscriber to move from a network operator to another network operator without changing his mobile number. The change of network operator may or may not imply a change of service provider.
- MNP does not include Service Portability, which refers to the possibility of moving from one service to another service while retaining the same mobile number.
- In the case of MNP the customer changes network operator and/or service provider while keeping the same number for the provision of the same service. However in the process of changing network operator and/or service provider the customer may lose supplementary services related to the basic service.
- International Mobile Subscriber Identities (IMSIs), which are used by mobile networks for the identification of mobile users and terminals, are not portable. A change of mobile network operator necessitates a change in the IMSI and in the SIM (Subscriber Interface Module) card.

6.7.1 Types of Number Portability

- There are three types of number portability.

1. Location portability

- A subscriber may move from one location to another location without changing his or her telephone number.

2. Service portability

- A subscriber may keep the same telephone number when changing the telecommunication services.

3. Operator portability

- A subscriber may switch operators or service providers without changing his or her telephone number.

6.7.2 Fixed Network Number Portability

- Fixed Network number Portability (FNP) is the ability of subscribers to switch between fixed line voice service providers without the need to change the telephone numbers.

- Fixed network number portability can be implemented by four ways.
  1. Call forwarding
  2. Call drop back
  3. Query on release
  4. All call query

Standard terminologies :

1. **Donor operator**- Means an operator from whose network the subscriber is porting out.
2. **Recipient operator**- Means an Operator who will be providing mobile service to the subscriber after porting.
3. **Signalling path**- Dotted line
4. **Solid line**-Trunk Setup path

6.7.2.1 Call Forwarding

- The call forwarding process takes two steps to complete the process. Fig. 6.7.1 shows this process.

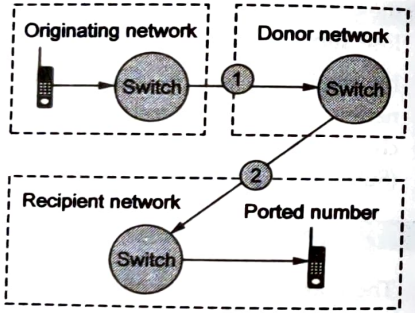

Fig. 6.7.1 Call forwarding

Step-1

- The originating network switch routes the call to the donor network switch according to the dialled telephone number.
- A solid arrow between two switches represents a trunk set up by using an ISDN (Integrated Services Digital Network) User Part or ISUP (part of SS7) Initial Address Message (IAM).

Step-2

- If the dialled number has been ported, the donor network switch forwards the call to the recipient network switch.
- For a non ported number, the recipient switch is the donor network switch in this step, and no forwarding action is performed.

6.7.2.2 Call Drop-back

- The call drop-back process takes two steps to complete the process. Fig. 6.7.2 shows this process.

Step-1

- The originating switch queries the donor network switch to obtain the routing information of the recipient network switch. In Fig. 6.7.2 dashed arrows represent transaction capabilities application part of the SS7 protocol (TCAP) signaling message exchange without involving trunk setup.

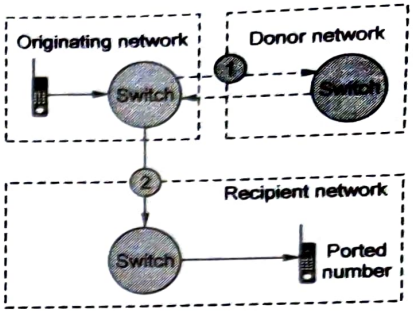

Fig. 6.7.2 Call drop-back

Step-2

- The originating switch sets up the trunk to the recipient switch based on the obtained routing information.

6.7.2.3 Query on Release

- The query on release process takes three steps to complete the process. Fig. 6.7.3 shows this process.

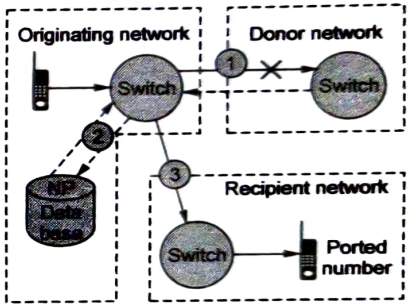

Fig. 6.7.3 Query on release

Step-1

- As in call forwarding, the originating network switch sets up the trunk to the donor network switch using an ISDN (Integrated Services Digital Network) User Part or ISUP (a part of the Signaling System No. 7) IAM message.
- If the dialled number has been ported, the donor network switch replies with an SS7 ISUP Release Message (REL) with the QoR cause value.

Step-2

- When the donor network switch receives the REL message, the trunk to the donor network switch is released.
- Since the QoR cause value indicates that the called party number is ported, the originating network switch sends an SS7 TCAP message to query the number portability database for the routing address of the recipient network switch.

Step-3

- The originating network switch sets up the trunk to the recipient network switch based on the obtained routing information.

6.7.2.4 All Call Carry

- The all call query process takes two steps to complete the process. Fig. 6.7.4 shows this process

Step-1

- The originating network switch sends an SS7 TCAP message to query the number portability database for the routing address of the recipient network switch.

Step-2

- The originating network switch sets up the trunk to the recipient network switch based on the obtained routing information.

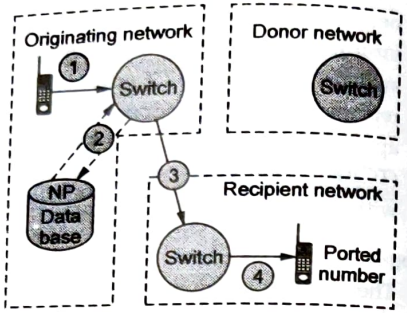

Fig. 6.7.4 All call carry

6.7.2.5 Comparison of Number Portability Solution

Number portability solution	Routing independence	Extra call setup cost	Initial system setup cost
Call forwarding	Low	pc_t	Low
Call drop-back	Medium	c_s	Medium
Query-on-release	Medium	$p(c_s + c_d)$	High
All-call-query	High	c_s	High

6.7.3 Number Portability for Mobile Networks

- When a mobile user switches operators and when mobile number portability is introduced, the mobile user keeps the MSISDN while being issued a new IMSI.
- The impact of number portability on mobile network:
  1. **Location update** : The assignment of a new IMSI is not affected by the introduction of number portability.
  2. **Mobile call origination** : To originate a call to a ported number, the MSC needs to be equipped with a routing mechanism.
  3. **Mobile call termination** : To deliver or terminate a call to a ported mobile number, the standard mobile call termination procedure is modified to accommodate the portability mechanism

University Question

1. *Write a short note on mobile portability.* **GTU : Summer-16, Marks 7**

6.8 Security in Wireless Network

6.8.1 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.

6.9 Multiple Choice Questions

WiFi/Wireless LAN

Q.1 Wireless networking, or Wi-Fi, can be used to connect computers in a home, and many cities are using the technology to offer free or low-cost Internet access to residents. What's another name for Wi-Fi ?

a 801.12 networking
b 801.22 networking
c 802.11 networking
d None of the above

[Ans. : c]

Q.2 A wireless network uses ___ waves to transmit signals.

[a] mechanical [b] radio [c] sound [d] all of the above

[Ans. : b]

Q.3 What is the access point (AP) in wireless LAN ?

[a] device that allows wireless devices to connect to a wired network

[b] wireless devices itself [c] both (a) and (b)

[d] none of the mentioned **[Ans. : a]**

Q.4 In wireless ad-hoc network _____.

[a] access point is not required [b] access point is must

[c] nodes are not required [d] none of the mentioned **[Ans. : a]**

Q.5 Which multiple access technique is used by IEEE 802.11 standard for wireless LAN ?

[a] CDMA [b] CSMA/CA [c] ALOHA [d] none of the mentioned

[Ans. : b]

Q.6 In wireless network an extended service set is a set of _____.

[a] connected basic service sets [b] all stations

[c] all access points [d] none of the mentioned **[Ans. : a]**

Q.7 IEEE 802.11 have three types of _____.

[a] frames [b] fields [c] signals [d] sequences **[Ans. : a]**

Q.8 Mostly _____ is used in wireless LAN.

[a] time division multiplexing [b] orthogonal frequency division multiplexing

[c] space division multiplexing [d] none of the mentioned **[Ans. : b]**

WiMAX

Q.1 WiMAX stands for _____.

[a] wireless maximum communication

[b] worldwide interoperability for microwave access

[c] worldwide international standard for microwave access

[d] none of the mentioned

[Ans. : b]

Q.2 WiMAX provides _____.

[a] simplex communication [b] half duplex communication

[c] full duplex communication [d] none of the mentioned **[Ans. : c]**

Q.3 WiMAX uses the _____.

[a] orthogonal frequency division multiplexing

[b] time division multiplexing

[c] space division multiplexing

[d] all of the mentioned **[Ans. : a]**

Q.4 Which one of the following modulation scheme is supported by WiMAX ?

[a] binary phase shift keying modulation

[b] quadrature phase shift keying modulation

[c] quadrature amplitude modulation

[d] all of the mentioned **[Ans . : d]**

Q.5 WiMAX MAC layer provides an interface between _____.

[a] higher transport layers and physical layer

[b] application layer and network layer

[c] data link layer and network layer

[d] none of the mentioned **[Ans. : a]**

Q.6 For encryption, WiMAX supports _____.

[a] advanced encryption standard [b] triple data encryption standard

[c] both (a) and (b) [d] none of the mentioned **[Ans. : c]**

Q.7 WiMAX provides _____.

[a] VoIP services [b] IPTV services [c] both (a) and (b)

[d] none of the mentioned **[Ans. : c]**

Q.8 Devices that provide the connectivity to a WiMAX network are known as _____.

[a] subscriber stations [b] base stations

[c] gateway [d] none of the mentioned **[Ans. : a]**