Wireless and Mobile Computing

UNIT-I

MOBILE COMMUNICATION

Mobile Communication is the use of technology that allows us to communicate with others in different locations without the use of any physical connection (wires or cables). Mobile communication makes our life easier, and it saves time and effort.

MOBILE COMPUTING

Mobile Computing is a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link.

The main concept involves −

- Mobile communication
- Mobile hardware
- Mobile software

MOBILE COMMUNICATION

The mobile communication in this case, refers to the infrastructure put in place to ensure that seamless and reliable communication goes on. These would include devices such as protocols, services, bandwidth, and portals necessary to facilitate and support the stated services. The data format is also defined at this stage. This ensures that there is no collision with other existing systems which offer the same service.

Mobile Hardware

Mobile hardware includes mobile devices or device components that receive or access the service of mobility. They would range from portable laptops, smartphones, tablet Pc's, Personal Digital Assistants.

These devices will have a receptor medium that is capable of sending and receiving signals. These devices are configured to operate in full- duplex, whereby they are capable of sending and receiving signals at the same time. They don't have to wait until one device has finished communicating for the other device to initiate communications.

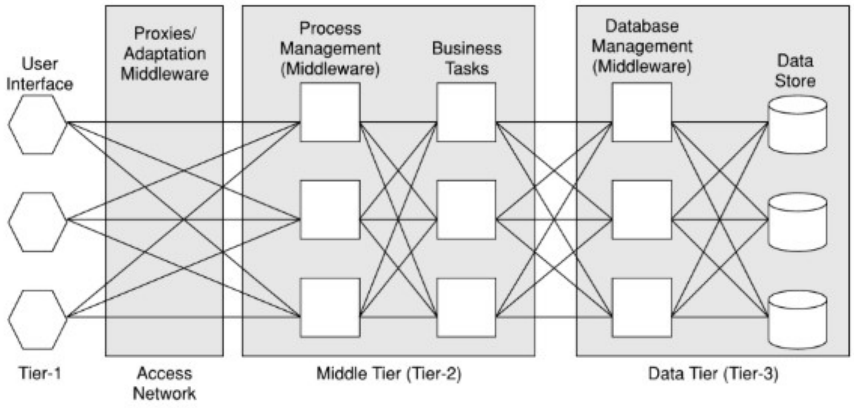
Mobile software

Mobile software is the actual program that runs on the mobile hardware. It deals with the characteristics and requirements of mobile applications. This is the engine of the mobile device. In other terms, it is the operating system of the appliance. It's the essential component that operates the mobile device.

MOBILE COMPUTING ARCHITECTURE

A 3-tier architecture is an application program that is organized into three major parts, comprising of:

- *Presentation*
- *Application tier (business logic)*
- *Data Access.*



Each tier is distributed to a different place or places in a network. These tiers do not necessarily correspond to physical locations on various computers on a network, but rather to logical layers of the application.

1. Presentation (Tier-1) (UI):

This is the user facing system in the first tier. This is the layer of agent application and systems. These applications run on the client device and offer all the user interfaces. This tier is responsible for presenting the information to the end user. Human generally use visual and audio means to receive information from machines (like mobile phones). In the case of the visual, the presentation of information will be through a screen.

2. Application (Tier-2):

The application tier or middle tier is the 'engine' of a presenting application. It performs the business logic of processing user input, obtaining data and making decisions. In certain cases, this layer will do the transcoding of data for appropriate rendering in the presentation tier.

A middleware framework is defined as a layer of software which sits in the middle between the operating system and the user facing software.

3. Data Access (Tier-3):

The data tier is used to store data needed by the application and acts as a repository for both temporary and permanent data. The data can be stored in any form of data store or database. These can range from sophisticated relational database to even simple text files. The data can also be stored in XML format for interoperability with other systems and data sources.

Mobile Devices

A mobile device is a handheld tablet or other device that is made for portability and is therefore both compact and lightweight. New data storage, processing and display technologies have allowed these small devices to do nearly anything that had previously been traditionally done with larger personal computers.

Mobile device is a general term for any handheld computer or smartphone. The term is interchangeable with 'handheld,' 'handheld device,' and 'handheld computer.' Tablets, e-readers, smartphones, PDAs and portable music players with smart capabilities are all mobile devices.

Laptops: Laptops are still the de facto portable computing device because they are designed to do everything a desktop PC can do, just from different locations. While laptops have the most computing power of the mobile

devices, and they are travel-friendly, they are the least portable of the mobile device options. Many people are starting to replace or supplement using regular laptops with smaller, more mobile devices.

Netbooks: For some people, even small laptops are too big. Netbooks have a more compact form factor, with 10-inch screen sizes or smaller and a weight of only 2 pounds. Netbooks are inexpensive, usually have long battery lives, and do the most common tasks — those that are least processor-intensive — that most of us use our computers for, like surfing the web, checking email, and using office productivity programs.

Smartphones: No matter what type of other mobile devices you have, it is almost certain that you have a smartphone. With their combination of internet and Wi-Fi access as well as cellular communication capabilities, smartphones are the devices driving mobility for both professional and consumer purposes. Android smartphones and iPhones in particular show rapid growth. With their small screen size and lack of hardware keyboards, smartphones are difficult to work from for extended periods.

Tablets: The tablet is less dependent on size or weight than on input. Tablets are computing devices that take input from a stylus, touchscreen or keyboard. Early tablet PCs championed by Microsoft used pen-based computing and ran a tablet-customized version of Windows XP. More recently, especially after Apple's introduction of the iPad, tablets are moving away from running the same operating systems as desktop and laptop PCs, running instead mobile operating systems like iOS and Android.

Ultra-Mobile PCs: For traditional computing in the smallest package, ultra-mobile PCs (UMPCs) may be the answer. UMPCs are mini computers or, to be more precise, mini tablets with touchscreen, stylus, and keyboard input options. With displays that are 7 inches and smaller and weighing less than 2 pounds, UMPCs are truly pocketable devices and offer traditional or full-fledged operating systems like Windows and Linux.

PDA's: Though PDAs are going out of favour because smartphones can do what PDAs do plus add telephony and data, PDA users still abound. Using a PDA has some advantages over smartphones. Many smartphones require, for example, a monthly data plan, whereas you can use a PDA at a Wi-Fi hotspot for free data connectivity. There's also a lot of business-oriented PDA software still available because the earliest PDA adopters were business users.

Characteristics of Mobile Devices

Mobile devices have similar characteristics. Among them are:

- Wi-Fi or cellular access to the internet
- A battery that powers the device for several hours
- A physical or onscreen keyboard for entering information
- Size and weight that allows it to be carried in one hand and manipulated with the other hand
- Touch-screen interface in almost all cases
- A virtual assistant, like Siri, Cortana or Google Assistant
- The ability to download data from the internet, including apps and books
- Wireless operation.

Mobile System Network

The mobile phone network enables wireless communication using mobile devices, such as mobile phones, smart phones or tablets. Mobile phone networks provide the necessary infrastructure and are operated by mobile phone providers. In addition to the access network, which establishes the wireless connection to the terminal devices by radio, a core network exists that connects the individual access points to each other. The core network ensures that mobile users can exchange information with those using other access networks or external networks. The main distinguishing factor between fixed and mobile networks is in the access network. The landline network also uses a similar or the same core network, but, as opposed to the mobile network, uses wired technologies in its access network.

To begin with, the mobile network was planned almost exclusively for voice communication, however, mobile data usage has become increasingly important over the years, especially with the advent of smart phones and tablets. This is also a major reason behind the rapid development of mobile communication standards. Whereas standards such as GPRS or EDGE only enable transmission speeds in the kilobits per second range, modern mobile networks, with 3G or 4G technology, such as UMTS and LTE, achieve bandwidths of many megabytes per second. The LTE standard allows transfer rates of more than 100 megabytes per second and, by using various different frequency ranges, can cover a large area around the radio mast.

Mobility Management

The main aim of mobility management is to track where the subscriber is allowing calls, SMS and other phone services to be delivered to them.

Mobile devices inform the cellular network, whenever it moves from one location area to another. Mobiles devices detects the location area codes. When a mobile find that the location area code is different from its last update, it performs another update by sending to the network, a location update request, together with its previous location, and its Temporary Mobile Subscriber Identity (TMSI) as well. Thus, a subscriber enjoys an uninterrupted access to the network.

Mobility management consists of two related functions: location management and call routing. Location management is the process of identifying the physical location of the user so that calls directed to that user can be routed to that location. Location management is also responsible for verifying the authenticity of users accessing the network. Routing consists of setting up a route through the network over which data directed to a particular user is sent, and dynamically reconfiguring the route as the user location changes. In cellular systems location management and routing are coordinated by the base stations or the central mobile telephone switching office (MTSO), whereas on the Internet these functions are handled by the Mobile Internetworking Routing Protocol (Mobile IP).

UMTS (Universal Mobile Telecommunications System) and GSM (Global System for Mobile Communications) are each made up of separate cells (base stations) that cover a specific geographical area. All base stations are integrated into one area, allowing a cellular network to cover a wider area (location area).

The location update procedure allows a mobile device to notify a cellular network when shifting between areas. When a mobile device recognizes that an area code differs from a previous update, the mobile device executes a location update, by sending a location request to its network, prior location and specific Temporary Mobile

Subscriber Identity (TMSI). A mobile device provides updated network location information for several reasons, including reselecting cell location coverage due to a faded signal.

Roaming is among the basic procedures of mobility management. It enables subscribers to use mobile services when moving outside of the geographical area of a specific network.

GSM Services

Teleservices

The abilities of a Bearer Service are used by a Teleservice to transport data. These services are further transited in the following ways:

Voice Calls:

The most basic Teleservice supported by GSM is telephony. This includes full-rate speech at 13 kbps and emergency calls, where the nearest emergency-service provider is notified by dialling three digits.

Videotext and Facsimile:

Another group of teleservices includes Videotext access, Teletex transmission, Facsimile alternate speech and Facsimile Group 3, Automatic Facsimile Group, 3 etc.

Short Text Messages:

Short Messaging Service (SMS) service is a text messaging service that allows sending and receiving text messages on your GSM mobile phone. In addition to simple text messages, other text data including news, sports, financial, language, and location-based data can also be transmitted.

Bearer Services

Data services or Bearer Services are used through a GSM phone. to receive and send data is the essential building block leading to widespread mobile Internet access and mobile data transfer. GSM currently has a data transfer rate of 9.6k. New developments that will push up data transfer rates for GSM users are HSCSD (high speed circuit switched data) and GPRS (general packet radio service) are now available.

Supplementary Services

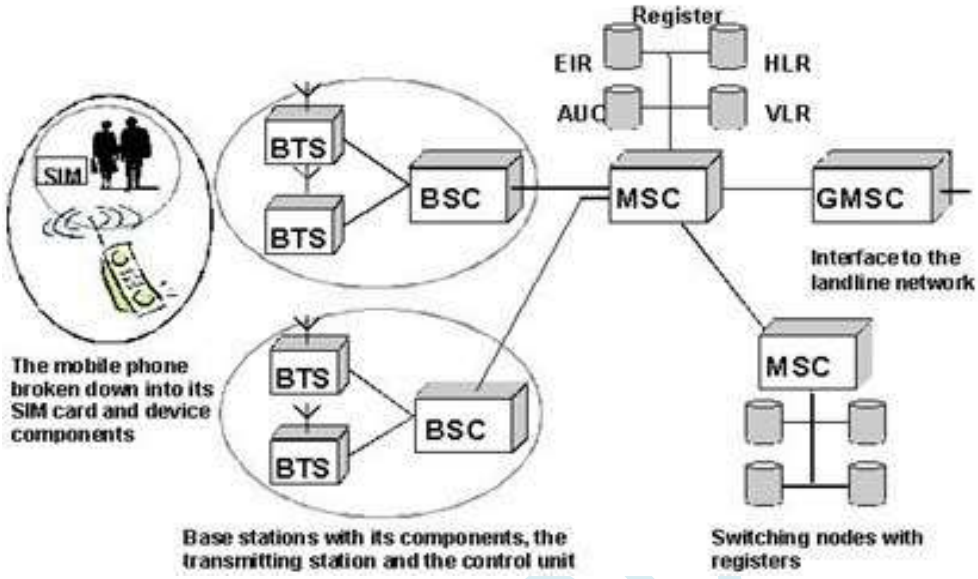
Supplementary services are additional services that are provided in addition to teleservices and bearer services. These services include caller identification, call forwarding, call waiting, multi-party conversations, and barring of outgoing (international) calls, among others.

GSM Architecture diagram

GSM (Global System for Mobile communication) is a digital mobile network that is widely used by mobile phone users in the world. GSM uses a variation of time division multiple access (TDMA) and is the most widely used of the three digital wireless telephony technologies: TDMA, GSM and code-division multiple access (CDMA). GSM digitizes and compresses data, then sends it down a channel with two other streams of

user data, each in its own time slot. It operates at either the 900 megahertz (MHz) or 1,800 MHz frequency band.

Here is the flow chart of GSM architecture:



GSM architecture and working

Followings are the main components of GSM architecture

Mobile Station (MS)

MS grant access to the GSM network. It is main component of GSM architecture. It contains the following two components.

1. Mobile Equipment (ME)
2. Subscriber Identity Module (SIM)

Mobile Equipment (ME)

There are number of mobile equipment being used for this architecture. These can be dispositive portable, mounted on vehicle, held in the hand. Every device has the sound only identified from a IMEI. These mobile devices are responsible for voice and data transmission simultaneously. It works at power level 0.8 – 20 W.

Subscriber Identity Module (SIM)

It permit the user whom it sends and who receives calls and to receive others of the subscribed services. It is main part of GSM architecture. Number details of definition of network like main Ki, algorithms kc, and A3, A5, and A8. A word of order or a PIN is protecting near. It can move of the telephone so that it is called by telephone and it contains the key information to activate the telephone.

Base Transceiver Station (BTS)

The station of receiving transmitter lowers code, calculates multiplex, modulates and introduces the signals of RF to the antenna. It makes the method of the frequency jump, communicates with the movable station and BSC. It consists of the units of receiving transmitter (TR). The LOW SULFUR CONTENT provides the insurance by radio of GSM in a cell. It implies the radio that it transmits and that receives equipment and the treatment of the signals associate in GSM architecture.

Base Station Controller (BSC)

The controller of basic station controls the resources by radio for the LOW SULFUR CONTENT. He assigns to the frequency and the sections of time for all the ` s of thousandth in his sector. He also directs the installation of call, functionality of adaptation. He provides to the delivery for each thousandth and the communication CAM and the LOW SULFUR CONTENT. BSC also provides the management of the resources by radio. It assigns and it releases to frequencies and sections of time for all the thousandth in his sector. One takes control frequencies between cells again.

Base Station Subsystem (BSS)

With air interface BSS provides MS and NSS (Network Station Subsystem). BSS consists of following elements.

- One or more BTS
- One BSC
- One TRAU (Transcoding Rate and Adaptation Unit)

Main Switching Center (MSC)

The center of main commutation is the heart of the net. The communication between the GSM and of other nets controls. Draft the function of system of call and the commutation, the advance of call, the information of invoicing and the collection of bases. It is also playing important role in GSM architecture.

Gateway Main Switching Center (GMSC)

It is a special kind of MSC that is used to route calls outside the mobile network. Whenever a call for a mobile subscriber comes from outside the mobile network, or the subscriber wants to make a call to somebody outside the mobile network the call is routed through the **GMSC**.

Home Location Register (HLR)

A HLR contains given customer as given of account, account position; the preferences customer, devices have undersigned with to the customer, the current situation of the customer, etc the data conserved in HLR for the several types of nets are similar but they differ in some details.

Visitor Location Register (VLR)

A VLR is a disc, similar to a HLR, that it is used by the nets you furnish to the profiles of taken of temporality for the customers (those are out of their central field). These data of VLR are low on the searched data customer of an HLR.

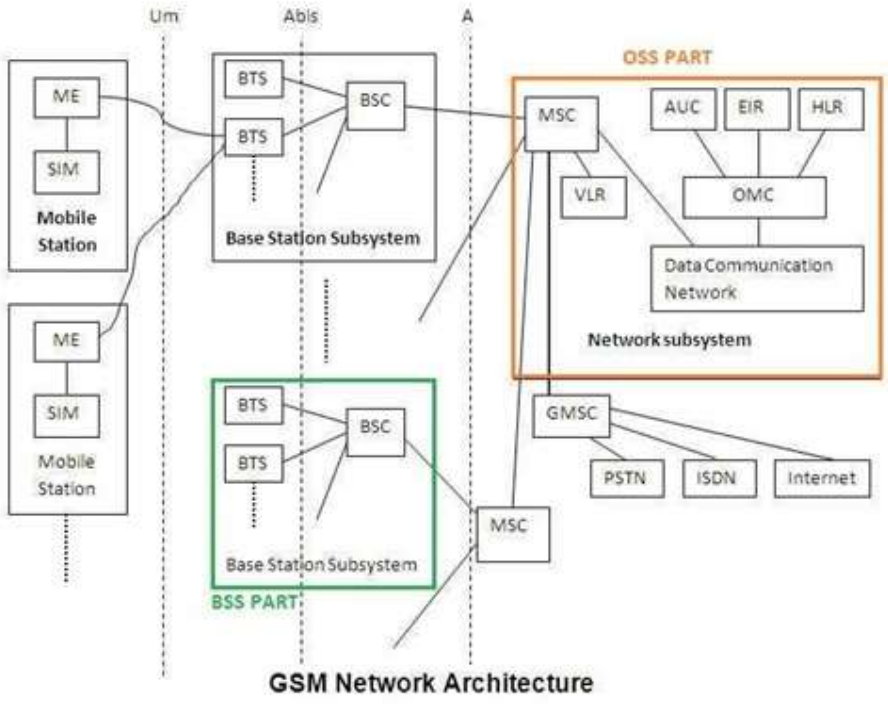
Authentication Center (AUC)

AUC look after not in favour of robber or thief during air interface. It keeps the authentication keys and granted the security triplets. It is normally linked with the HLR.

Equipment Identity Register (EIR)

GSM MS is possible to operate any valid GSM SIM. An opportunity exists for black market and stolen equipment. To combat this problem EIR is introduce and track such equipment.

Radio interfaces of GSM



GSM Network Architecture

In the Public Land Mobile Communication Network (PLMN), the MS is connected with the network via the radio channel. In this way, the subscribers can access the network and obtain communication services. To achieve the interworking between MS and BTS, a set of standards are needed for signal transmission through the radio channel. This set of specifications which related to the radio channel signal transmission, aim at Um interface.

The Um interface is a kind of radio interface. It is responsible for the communication between the mobile station and the BTS and provides the interworking link between the mobile station and GSM system. Its physical connection is achieved via the radio waves. The Um interface is the most important interface among all the interfaces in GSM system. First of all, the complete and normative Um interface realizes full compatibility between MS of different venders and different networks. That are fundamental conditions needed in global roaming of the GSM system; second, the radio interface determines the rate of frequency spectrum utilization of GSM system. The name “Um” is derived from the name of the interface between the client terminal and the network in ISDN, in which the “m” means “mobile”.

Protocols used in GSM

MS Protocols

Based on the interface, the GSM signalling protocol is assembled into three general layers:

- **Layer 1**: The physical layer. It uses the channel structures over the air interface.
- **Layer 2**: The data-link layer. Across the Um interface, the data-link layer is a modified version of the Link access protocol for the D channel (LAP-D) protocol used in ISDN, called Link access protocol on the Dm channel (LAP-Dm). Across the A interface, the Message Transfer Part (MTP), Layer 2 of SS7 is used.
- **Layer 3**: GSM signalling protocol's third layer is divided into three sublayers:
    - Radio Resource Management (RR),
    - Mobility Management (MM), and
    - Connection Management (CM).

MS to BTS Protocols

The RR layer is the lower layer that manages a link, both radio and fixed, between the MS and the MSC. For this formation, the main components involved are the MS, BSS, and MSC. The responsibility of the RR layer is to manage the RR-session, the time when a mobile is in a dedicated mode, and the radio channels including the allocation of dedicated channels.

The MM layer is stacked above the RR layer. It handles the functions that arise from the mobility of the subscriber, as well as the authentication and security aspects. Location management is concerned with the procedures that enable the system to know the current location of a powered-on MS so that incoming call routing can be completed.

The CM layer is the topmost layer of the GSM protocol stack. This layer is responsible for Call Control, Supplementary Service Management, and Short Message Service Management. Each of these services are treated as individual layer within the CM layer. Other functions of the CC sublayer include call establishment, selection of the type of service (including alternating between services during a call), and call release.

BSC Protocols

The BSC uses a different set of protocols after receiving the data from the BTS. The Abis interface is used between the BTS and BSC. At this level, the radio resources at the lower portion of Layer 3 are changed from the RR to the Base Transceiver Station Management (BTSM). The BTS management layer is a relay function at the BTS to the BSC.

The RR protocols are responsible for the allocation and reallocation of traffic channels between the MS and the BTS. These services include controlling the initial access to the system, paging for MT calls, the handover of calls between cell sites, power control, and call termination. The BSC still has some radio resource management in place for the frequency coordination, frequency allocation, and the management of the overall network layer for the Layer 2 interfaces.

To transit from the BSC to the MSC, the BSS mobile application part or the direct application part is used, and SS7 protocols is applied by the relay, so that the MTP 1-3 can be used as the prime architecture.

MSC Protocols

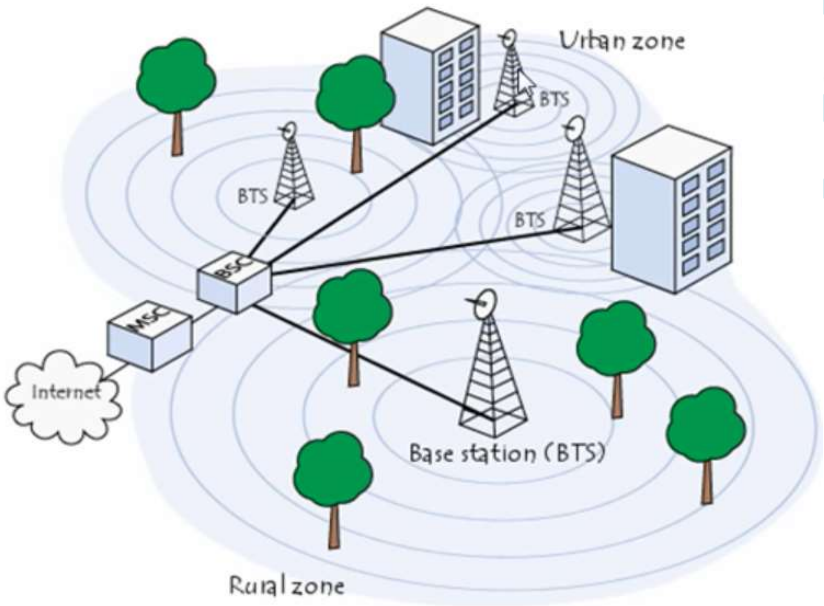
At the MSC, starting from the BSC, the information is mapped across the A interface to the MTP Layers 1 through 3. Here, Base Station System Management Application Part (BSS MAP) is said to be the equivalent set of radio resources. The relay process is finished by the layers that are stacked on top of Layer 3 protocols, they are BSS MAP/DTAP, MM, and CM. This completes the relay process. To find and connect to the users across the network, MSCs interact using the control-signalling network. Location registers are included in the MSC databases to assist in the role of determining how and whether connections are to be made to roaming users.

Each GSM MS user is given a HLR that in turn comprises of the user's location and subscribed services. VLR is a separate register that is used to track the location of a user. When the users move out of the HLR covered area, the VLR is notified by the MS to find the location of the user. The VLR in turn, with the help of the control network, signals the HLR of the MS's new location. With the help of location information contained in the user's HLR, the MT calls can be routed to the user.

UNIT-II

Cellular network and frequency reuse

A **Cellular Network** is a radio network distributed over land through cells where each cell includes a fixed location transceiver known as base station. These cells together provide radio coverage over larger geographical areas. User equipment (UE), such as mobile phones, is therefore able to communicate even if the equipment is Moving through cells during transmission. Cellular networks give subscribers advanced features over alternative solutions, including increased capacity, small battery power usage, a larger geographical coverage area and reduced interference from other signals. Popular cellular technologies include the Global System for Mobile Communication, general packet radio service, 3GSM and code division multiple access.



Frequency reuse is the process of using the same radio frequencies on radio transmitter sites within a geographic area that are separated by sufficient distance to cause minimal interference with each other. Frequency reuse allows for a dramatic increase in the number of customers that can be served (capacity) within a geographic area on a limited amount of radio spectrum (limited number of radio channels). Frequency reuse allows WiMAX system operators to reuse the same frequency at different cell sites within their system operating area.

The number of times a frequency can be reused is determined by the amount of interference a radio channel can tolerate from nearby transmitters that are operating on the same frequency (carrier to interference ratio).

More info: https://youtu.be/1JZG9x_VOwA

Handheld device

A handheld is any portable device that can be carried and held in one's palm. A handheld can be any computing or electronic device that is compact and portable enough to be held and used in one or both hands. A handheld may contain cellular communication, but this category can also include other computing devices.

Various popular handheld devices include:

- Notebook PC

- Ultra-Mobile PC
- Handheld PC
- Personal digital assistant/Enterprise digital assistant
- Graphing calculator
- Pocket computer (largely obsolete)
- Handheld game consoles

Limitation of mobile device

Wireless switching technology

Packet switching is the basic type of wireless switching technology. Packet-switched communication uses short bursts of information that use channels only for short periods of time. Wireless devices are ON with a specific address assigned to them. Data are sent to and from the address, routed using standardized protocol.

Packet switching is a more efficient system for transmitting data, because it shares spectrum and bandwidth. By only using bandwidth when data is transmitted and not holding a circuit open, many users can share capacity on a network more easily. Having an IP-type address for a device permits devices to act as part of the internet, sending and receiving information automatically using standard protocol.

Another switching technology is based on virtual circuits. A virtual circuit is a logical circuit created within a shared network between two network devices. Two types of virtual circuits exist: switched virtual circuits (SVC) and permanent virtual circuits (PVC).

SVCs are virtual circuits that are dynamically established on demand and terminated when transmission is complete. Communication over an SVC consists of three phases: circuit establishment, data transfer and circuit termination. The establishment phase involves creating the virtual circuit between the source and destination device. Data transfer involves transmitting data between the devices over the virtual circuit and the circuit termination phase involves tearing down the virtual circuit between the source and destination devices.

PVC is a permanently established virtual circuit that consists of one mode: data transfer. PVCs are used in situations in which data transfer between devices is constant. PVCs decrease the bandwidth use associated with the establishment and termination of virtual circuits, but they increase costs due to constant virtual circuit availability. PVCs are generally configured by the service provider when an order is placed for service.

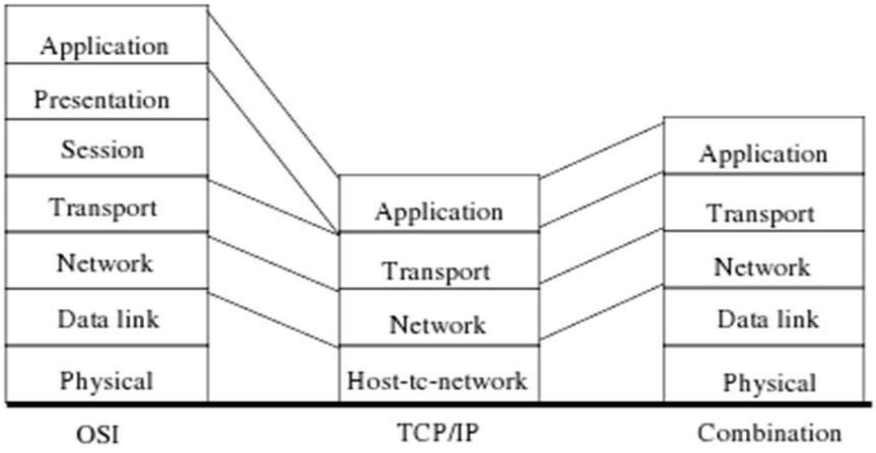
Wireless communication problem

The problems are namely, shared media, increased bit error rate (BER), lower radio transmission power, scattering, reflection, diffraction, multipath propagation, fading, path loss, radio frequency signal interference etc.

1. **Shared media:** The wireless media offers lower bandwidth inspite of the technologies coming up to support Mbps wireless networks. Therefore, the effective utilization of the bandwidth is necessary for wireless networks.
2. **Increased bit error rate (BER):** Wireless network media is more prone to errors due to obstacles coming in between the transmitter and the receiver and the interference caused by neighbouring transmitters. One can observe frequent disconnections causing loss of data and annoying the users especially in voice and video communication.
3. **Lower radio transmission power:** Mobile units are compact in size and work on battery with scarce energy resources. The mobile nodes limit transmission power to avoid interference. Signal strength decreases with inverse square of distance. Higher frequency usage increases attenuation and decreases range of communication.
4. **Scattering:** Scattering occurs when the material through which the wave travels has objects with dimensions that are small compared to the wavelength and where the number of obstacles per unit volume is large. Scattered waves are produced by rough surfaces, small objects or other irregularities in the channel.
5. **Reflection:** Reflection occurs when a propagating electromagnetic wave strikes an object which has very large dimensions compared to the wavelength of the propagating wave, for example, walls, furniture, building structure etc.
6. **Diffraction:** Diffraction occurs when the radio path between the transmitter and the receiver is obstructed by a surface that has sharp irregularities. The secondary waves resulting from the obstructing surface are present throughout the space and even behind the obstacle.
7. **Multipath propagation:** The multipath problem in mobile radio is caused by reflection and scattering from buildings, trees and other obstacles along the radio path. Radio waves arrive at a mobile receiver from many different directions, with different time delays.
8. **Fading:** Signal-fading phenomena can drastically affect the performance of a wireless communications system. Often caused by multipath conditions, fading can degrade the BER performance of a digital communications system, resulting in the data loss.
9. **Path loss:** Path loss between the transmitter and the receiver is a key consideration when designing a wireless network. Expected levels of path loss, based on the range between the transmitter and the receiver, provide valuable information when determining requirements for transmit power levels, receiver sensitivity and signal-to-noise ratio.
10. **RF signal interference:** The process of transmitting and receiving radio and laser signals through the air makes wireless systems vulnerable to atmospheric noise and transmissions from other systems. In addition, wireless networks can interfere with other nearby wireless networks and radio wave equipment.

Wireless network reference model

Several different but similar layered data architectures have been developed to allow reliable data transfer between different computer systems and between different networks. The seven-layer International Standards Organization (ISO) opens systems interconnect (OSI) reference model was first proposed around 1983 to allow connectivity between different computer systems. Prior to the OSI reference model, computer systems made by one manufacturer could not easily communicate with computer systems made by other manufacturers. The intent of the OSI reference model was to allow computer systems to successfully communicate with each other even though different vendors manufactured them.



The TCP/IP architecture is functionally equivalent to the OSI reference model. The major similarities and differences are as follows:

1. Both models have an application, a transport and a network/internet layer.
2. The TCP/IP model does not have a session layer or presentation layer.
3. Both models have a lower layer that connects the upper layers to actual physical network. In the OSI reference model, the lower layer is called the physical layer.

Virtually all the wireless equipment features that we use operate at the physical, data link, and network layer of the OSI and TCP/IP reference models.

1. **Application layer functions:** The application layer is where the end-user programs run. Some of the end user programs are remote login, mail transfer, file transfer, web browsers etc.
2. **Transport layer functions:** The transport layer's job is to provide reliable communications from application to application regardless of the lower-layer protocols and communication links.
3. **Network layer functions:** Network layer often performs routing of packets and internetworking of two or more networks. Packet routing typically goes from intermediate network to intermediate network before the packets finally arrive at their destination network.
4. **Data link layer functions:** The data link layer includes the logical link control sublayer and MAC layer. The data link layer normally performs a wide variety of functions, including segmentation the bit stream into frames, error handling, flow control, and access control.
5. **Physical layer functions:** The physical layer transports encapsulated data from the data link layer and transmits it wirelessly to the distant network. The wireless features and functionality take place at this layer.

Wireless networking issue

The challenge of wireless network is to overcome the harsh reality of wireless transmission and to provide mobility and multimedia services.

Traffic and resource allocation

Each accepted connection has a certain traffic contract that describe the traffic type and resource requirements. A slot scheduler is responsible to assign slots in a transmission frame according to the various traffic contracts.

Flow control

A connection involves buffering at several places on the path between the sender and the receiver. Traffic type requirements concerning delay and implementation restrictions on the buffer capacity generally limit the

amount of buffer space available to a connection. Due to the dynamic character of wireless networks and user mobility, the stream of data might be hindered on the way from source to destination.

Error control

Owing to the high BER that is typical for a wireless link, many packets can be corrupted during transmission. If this rate exceeds the allowable packet loss rate of a connection, an effective and efficient error control scheme must be implemented to handle such situations. At the physical level, redundancy for detecting symbols reduce the BER for the first time.

Security and privacy

Network security refers to the protection of information and resources from loss, corruption and improper use. The MAC layer is only capable to provide some basic protection of the data on the wireless link. As it is hard to make this very secure, end-to-end security will be the most attractive and secure solution.

Mobility

In a wireless environment, the mobility of the wireless node enforces handover procedures when the node moves from one area to another. As the radius of an area decreases handover situations will be encountered frequently.

Routing

Multihop wireless networks without any infrastructure pose bigger challenges in computing proper and efficient routes for source destination pairs. This is mainly due to node mobility, that is network topology frequently changes leading to unstable and improper routes.

Power management

Wireless devices have maximum utility when they can be used anywhere anytime. However, the finite power supplies are one of the limitations to achieve this goal. As batteries provide limited power, a general constraint of wireless communication is the short continuous operation time of wireless terminals.

Pricing

This deals with pricing policies in wireless networks. The service providers should charge the prices based on the QoS requirements and the network situations.

Wireless Network Standards

Below are the wireless network standards:

Table 2.1 | Summary of wireless networking standards

Name	*Frequency band*	*Bit rate*	*Signal range*	*Modulation*	*Applications*
Bluetooth (IEEE 802.15)	2, 4 GHz	1, 2 Mbps	10 m	GMSK; device-to-device	Peer-to-peer
UWB (IEEE 802.15.3)	4, 8–10 GHz	480 Mbps	10 m	OFDM	Health monitoring
ZigBee (IEEE 802.15.4)	2, 4 GHz	250 kbps	10 m	O-QPSK	Control and automation
IEEE 802.11a	5 GHz	54 Mbps	100 m, outdoor; 30 m, indoor	OFDM, BPSK, QPSK, 16 QAM, 64 QAM	Wireless LAN
IEEE 802.11b	2, 4 GHz	11 Mbps	110 m, outdoor; 35 m, indoor	BPSK, QPSK, 64 QAM, CCK	Wireless LAN
IEEE 802.11g	2, 4 GHz	54 Mbps	110 m, outdoor; 35 m, indoor	OFDM, BPSK, QPSK, 16 QAM, 64 QAM	Military applications; example: high energy RADAR
IEEE 802.11n	2, 4/5 GHz	150 Mbps	160 m, outdoor; 70 m, indoor	MIMO	Wireless LAN
IEEE 802.16	10–66 GHz	134 Mbps	5 km	QPSK, 16 QAM, 64 QAM	Wireless MAN
IEEE 802.16a	2–11 GHz	75 Mbps	10 km	BPSK, QPSK, 16 QAM, 64 QAM	Network access for line-of-sight applications
IEEE 802.16d	2–11 GHz	75 Mbps	8 km	BPSK, QPSK, 16 QAM, 64 QAM	Last mile connectivity applications
IEEE 802.16e	2–6 GHz	30 bps; downlink/ uplink	5 km	BPSK, QPSK, 16 QAM, 64 QAM	*Mobile and wireless applications, WMAN*

Wireless body area network architecture

WBAN differs with other wireless sensor networks (WSN) with some significant points. First difference between a WBAN and WSN is mobility. In WBAN user can move with sensor nodes with same mobility pattern whereas WSN is generally used to be stationary. Energy consumption is much less in WBAN than other WSNs arrangement.

There are several wireless technologies such as Low power Wi-Fi, Bluetooth, ZigBee and IEEE 802.15.6.

WBAN Architecture

WBAN is designed with special purpose sensor which can autonomously connect with various sensors and appliances, located inside and outside of a human body.

Here we have classified the network architecture into four sections. The first section is the WBAN part which consists of several numbers of sensor nodes. These nodes are cheap and low-power nodes with inertial and physiological sensors, strategically placed on the human body. All the sensors can be used for continuous monitoring of movement, vital parameters like heart rate, ECG, Blood pressure etc. and the surrounding environment. There are vast monitoring systems are being used already based on wired connections. Any wired connection in a monitoring system can be problematic and awkward worn by a person and could restrict his mobility. So, WBAN can be a very effective solution in this area especially in a healthcare system where a patient needs to be monitored continuously and requires mobility.

The next section is the coordination node where the entire sensor nodes will directly be connected with a coordination node known as Central Control Unit (CCU). CCU takes the responsibility to collect information from the sensor nodes and to deliver to the next section. For monitoring human body activities there is no such wireless technology is fixed for targeting WBAN. Most popular

wireless technologies used for medical monitoring system are WLAN, Wi-Fi, GSM, 3G, 4G,WPAN (Bluetooth, ZigBee) etc. Except Cellular network standard all of these technologies are commonly available for short distance communication. WMTS (Wireless Medical Telemetry Service) and Ultra-Wide Band are another technology that could be used for body monitoring system as they operate in low transmission power.

The third section is the WBAN communication which will act as a gateway to transfer the information to the destination. A mobile node can be a gateway to a remote station to send Mobile Message to a cellular network using GSM/3G/4G. A router or a PC can be a remote node to communicate via email or other service using Ethernet.

The last section will be a control center consists of end node devices such as Mobile phone for message, PC for monitoring and email and server for storing the information in the database.

Network components

1. An electrocardiogram (ECG) sensor for monitoring heart activity.
2. An electromyography (EMG) sensor for monitoring muscle activity.
3. An electroencephalography (EEG) sensor for monitoring brain electrical activity.
4. A blood pressure sensor.
5. A tilt sensor for monitoring trunk position.
6. A breathing sensor for monitoring respiration.
7. Movement sensors for estimating user's activity.
8. A smart sock sensor or a sensor equipped shoe insole used to delineate phase of individual steps.

Design Issues

Interoperability

Data has to move from one device to another in a WBAN. The problem of interoperability arises due to the integration of many sensing devices each operating at a different frequency.

Temperature Control

In a WBAN there are small devices having transceivers which consume very less power, radiate heat, tolerate the heat or radiation of the human body. Rise in temperature can affect the human tissues as well as the devices. So, a WBAN should be designed by keeping in view all the heat considerations.

Changing topology

In WBAN along with the movement of the body, there is a change in topology. This causes several connections and disconnections. So, the problems arising due to change in topology should be dealt with.

Constant signalling

There is a need of constant signalling in some of the WBAN applications as they capture data which is continuous and real time. So, proper procedures should be adopted to carry out constant signalling task.

Synchronization

Synchronization represents the continuous acceptance of communication packets under energy and throughput formation. For real time data delivery Synchronization has to be improved.

Consistency

Consistency or reliability is reversely proportional to the packet loss rate. Higher the packet loss rate, lesser the communication reliability will be. In WBAN, the information packets are highly critical, so reliability is the major requirement of this network.

Network Protocols

WBAN technologies

Bluetooth

Bluetooth is an IEEE 802.15.1 standard commonly known as WPAN (Wireless Personal Area Network). Bluetooth technology was designed as a short-range wireless communication standard, anticipated to form a network with security and low power consumption. A typical Bluetooth network forms a Piconet where a Bluetooth device works as a master and another seven Bluetooth devices work as slaves which gives each device to communicate with each other simultaneously. Another type of Bluetooth network can be formed with more than one Piconet known as Scatter net. In Scatter net a node of a Piconet (can be a master or a slave) joins as a slave in another Piconet.

Bluetooth devices operate in the 2.4 GHz ISM band (Industrial, Scientific and Medical band).

ZigBee

ZigBee is an IEEE 802.15.4 standardized solutions for wireless telecommunications designed for sensors and controls, and suitable for use in harsh or isolated conditions. One of the biggest advantages of ZigBee network is its low power consumption.

Devices such as sensors are configured as end devices. They are connected to the network through the routers. Routers help to carry data across multi-hop ZigBee networks. In some cases, ZigBee network topology are formed without routers when the network is point to point and point to multipoint.

Wi-Fi

Wi-Fi is an IEEE 802.11 standard for wireless local area network (WLAN). Generally, Wi-Fi technology comes with four standards (802.11 a/b/g/n) that runs in ISM band 2.4 and 5 GHz with a modest coverage of 100 meter. Wi-Fi permits users to transfer data at broadband speed when connected to an access point (AP) or in ad hoc mode.

Wi-Fi is preferably suitable for large amount of data transfers with high-speed wireless connectivity that allows videoconferencing, voice calls and video streaming. An important advantage is that all smart phones, tablets and laptops have Wi-Fi integrated; however, the main disadvantage of this technology is high energy consumption.

IEEE 802.15.6 WBAN

IEEE 802.15.6 is the latest addition in WPAN which is known as WBAN standard that provides various medical and non-medical applications and supports communications inside and around the human body. This standard supports communication inside and outside of human body which can be used for different medical and non-medical applications such as e-Healthcare monitoring, sports, environment etc.

Mobile IP network layer

We know that the host or node within the network should not get any packet if it moves out of the network. In mobile environment the nodes are always in moving between several areas, and our goal is where ever the node is, should get the services of the network.

There are several ways to assign a topologically correct address (IP). One quick solution is DHCP. Here the problem is, nobody knows the new IP, it is impossible to find a node on network. The next solution is DNS.

Another solution for assigning topologically correct address is, creation of specific routers for mobile nodes. One more basic problem with this approach is, the routers are basically designed for fast forwarding the packets, but not for updating of routing tables.

Packet Delivery and Handover Management

Here we consider during the communication in between the correspondent node (CN) and the mobile node (MN) which are moving around different networks and the CN may be the fixed or mobile, how the services are handed over between the different networks.

Case-1: CN is a fixed node and MN in home network

Let us consider CN is a fixed node in its own network and MN is also in-home network. Now CN transmits the connection establishment message using IP protocol, through CA to the home agent of MN.

In this message source IP address is the IP address of CN and destination IP address is the IP address of MN.

Now the HA receives and then delivers it to the MN, HA also receives the response from MN and send back to CN.

Case-2: CN is a mobile node in its home network and MN is also in its home network

In this case the CN transmit the packet for connection establishment to HA of MN through CA.

Here source IP address is the IP address of CN and destination IP address is the IP address of MN.

Now the HA receives and the delivers it to the MN, the HA also receives the response from MN and send back to CN.

Case-3: CN is fixed in its home network and MN is in the foreign network

CN transmits the connection establishment message using IP protocol, through CA to the home agent (HA) of MN. In this message source IP address is the IP address of CN and destination IP address is the IP address of MN.

Now HA of MN receives the packet for MN and identifies that the MN is not available in-home network. So, HA encapsulate the receiving packet with new IP header which source address is IP address of CN and destination address is the care of address of MN in the foreign network.

Case-4: CN is mobile node at foreign network and MN is at the home network

In this case the CN sends the connection establishment message to the HA of MN through the FA where it is located. Once the connection established the data is exchanged between the HA and FA.

Tunnelling and Encapsulation

A tunnel establishes a virtual pipe for data packets between a tunnel entry and a tunnel endpoint. Packets entering a tunnel are forwarded inside the tunnel and leave the tunnel unchanged. Tunnelling, i.e., sending a packet through a tunnel is achieved by using encapsulation.

Encapsulation is the mechanism of taking a packet consisting of packet header and data and putting it into the data part of a new packet. The reverse operation, taking a packet out of the data part of another packet, is called de-capsulation. Encapsulation and de-capsulation are the operations typically performed when a packet is transferred from a higher protocol layer to a lower layer or from a lower to a higher layer respectively.

Types of Encapsulation

1. **IP-in-IP encapsulation:** required to be supported. Full IP header added to the original IP packet. The new header contains HA address as source and Care of Address as destination.
2. **Minimal encapsulation:** optional. Requires less overhead but requires changes to the original header. Destination address is changed to Care of Address and Source IP address is maintained as is.
3. **Generic Routing Encapsulation (GRE):** optional. Allows packets of a different protocol suite to be encapsulated by another protocol suite.

UNIT-III

Wireless Local Area Networks

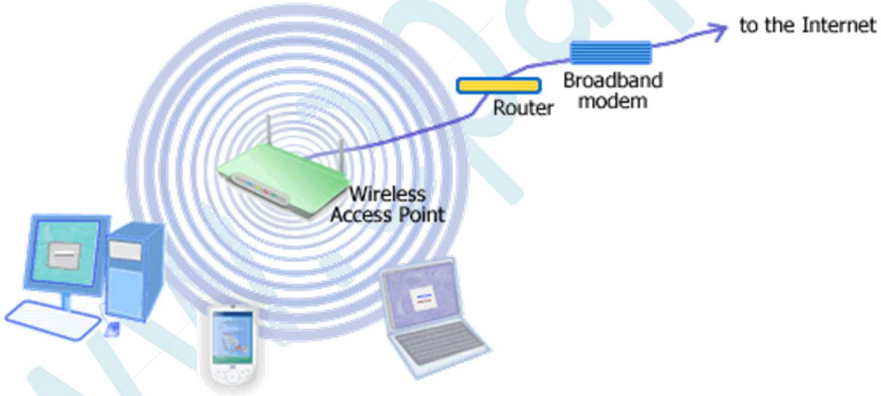
The network that cover a distance of 10-500m are called WLANs. Community. WLANs are the networks that cover offices and buildings about 50-500m distance and require communication between different database servers, wireless nodes, printers etc. WLANs are gaining significant importance in business and academic environment.

Network Components

The main components of the WLAN are adapters, access points, bridges and mobile nodes such as laptop, personal digital assistant, desktop or notebook computers.

Access Points

An access point acts as the main radio transmitter for your wireless LAN. Access points translate network traffic into radio signals and transmit that signal to wireless enabled computers. An access point can also be connected to an existing wired network via a cable in order to allow wireless enabled computers access to a wired network. You can have more than one access point on a particular network. Each access point has a limited range within which it can maintain a wireless connection with wireless enabled computers on a network. This range depends on the environment but is typically up to around 90 metres indoors. The range will be shorter if the building structure interferes with radio transmissions (e.g. presence of metal framing, large masonry structures, multiple floors and walls etc.). Performance generally suffers as distance increases beyond the limits of a range of 50-90 metres.



Wireless NIC

Your computer needs a wireless network information card, or NIC, to talk with the wireless router. A laptop comes standard with a wireless NIC, but for a desktop PC you have to get a wireless NIC as an option. It's installed internally as an expansion card, or you can use one of the various plug-in USB wireless NICs.

WLAN Adapters

WLAN adapters are add-on devices that enable you to connect to wireless networks like at the office or hotel. These adapters can be added to either desktop or laptop computers, so long as the hardware and software are compatible. While wireless adapters enable more mobility and freedom in connecting to networks, a wireless connection also provides a slower connection than a wired one.

Bridges

These are used to connect wired LANs in different buildings. The cost of deploying a fiber optic cable between buildings is high in situations where barriers exist between the buildings such as highways, bodies of water, valley etc. in such situations, a WLAN bridge can be an economical alternative. A bridge can also provide a less expensive alternative to recurring leased-line charges. WLAN bridge supports fairly high data rates and covers ranges of several miles with the use of line-of-sight directional antennas. Some Aps can also be used as a bridge between buildings of relatively close proximity.

WLAN Routers

The basic function of the router is to transfer the packets between the networks. The router chooses the next best link to send packets in order to reach closer to the final destination. Routers use internet protocol packet headers and routing tables, as well as IPs to determine the best path for each packet. A WLAN router adds a built-in AP function to a multi-port Ethernet router. This combines multiple Ethernet networks with wireless connections as well.

Design Requirements of WLAN

With the growing business on the internet the need of data sharing has increased tremendously. Users want to share data at any location and time without having to go through the tedious plugging in work.

1. **Compatibility:** WLANs should provide industry-standard interconnection with wired networks such as Ethernet or token ring. WLAN nodes should be supported by network operating systems in the same fashion as any other LAN node through the use of the appropriate drivers. Once installed, the network treats wireless nodes like any other network components.
2. **Safety:** WLANs must meet stringent government and industry regulations for safety. No adverse health effects have ever been attributed to WLANs.
3. **Battery life:** Since end user wireless products are designed to run off the main power supply, wireless products have no direct wire connectivity of their own. Therefore, the battery life must be maximum.
4. **Scalability:** The design of wireless network can be extremely simple or quite complex. Wireless networks can support large number of nodes and large physical areas by adding APs to boost or extent coverage and so the network must be scalable.
5. **Security:** Security has long been a design criterion for wireless devices. Security provisions are typically built into WLANs, making them more secure than most wired LANs. It is extremely difficult

for unintended receivers to listen WLAN traffic. In general, individual nodes must be security-enabled before they are allowed to participate in network traffic.

6. **Cost:** A WLAN implementation should look at the cost which includes both infrastructure costs, for the wireless access points and user costs, for the WLAN adapters. Infrastructure costs depend primarily on the number of Aps deployed.
7. **Licensing Issue:** For WLANs to be sold in a particular country, the manufacturer of the WLAN must ensure its certification by the appropriate agency in that country.
8. **Integrity and Reliability:** Robust design of WLAN technology is needed to achieve the integrity and reliability. Limited distance over which signals travel in WLAN results in connections that are far more robust than cellular phone connections and provide data integrity performance equal to or better than wired networking.

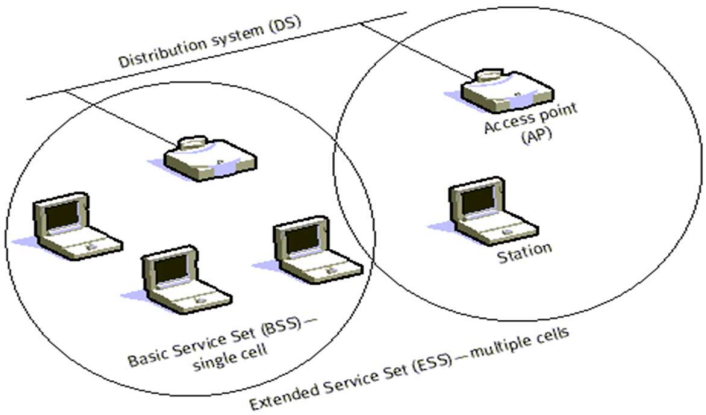
Network Architecture

Basically, there are two modes of WLANs: infrastructure-based and infrastructure-less WLAN.

Infrastructure-Based WLAN

A typical infrastructure-based WLAN defines two pieces of equipment: a wireless station, which is usually a PC equipped with a wireless network interface card and an AP, which acts as a bridge between the wireless and wired networks. An AP usually consists of a radio, a wired network interface and a bridging software conforming to the 802.1d bridging standard. The AP acts as the base station for the wireless network aggregating access for multiple WSTA's onto the wired network.

In infrastructure mode the wireless network consists of at least one AP connected to the wired network infrastructure and a set of wireless-end stations. This configuration is called a basic service set. An extended service set is a set of two or more BSS forming a single subnetwork. As most corporate WLANs require access to the wired LAN for services, they will operate in infrastructure mode.

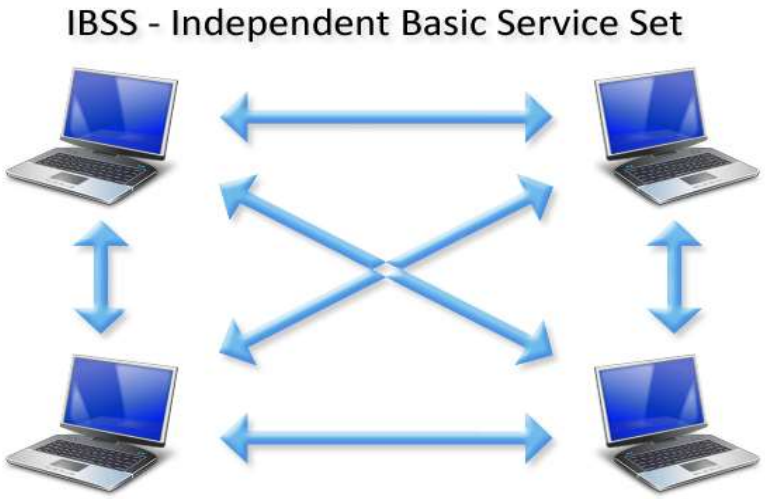


The infrastructure network provides an architecture for providing communication between wireless clients and wired network resources. Infrastructure-based wireless networks use fixed network APs with which mobile clients can communicate.

Infrastructure-Less WLAN

These are sometimes referred as ad hoc networks, as they are temporary networks established as and when

required. There are two kinds of ad hoc networks: peer-to-peer and multihop. The components are similar to those used in infrastructure-based LANs with the exception of APs.



Ad hoc mode is simply a set of WSTAs that communicate directly with one another without using an AP or any connection to a wired network. This mode is useful for quickly and easily setting up a wireless network where a wireless infrastructure does not exist or is not required for services or where access to the wired network is barred.

WLAN Standards

Convenience and cost saving are the two primary factors driving WLAN deployments. Yet there is considerable confusion in the marketplace about the various standards that exists. Each vendor defined the protocols and signalling for their own products and these proprietary products did not interoperate with one another.

IEEE 802.11

The 802.11 network architecture comprises several components and services that interact to provide station mobility transparent to the higher layers of the network stack such as wireless nodes and APs. It supports topologies such as IBSS. This standard defines the following:

1. Three different PHY layer implementations: (i) DSSS (Direct sequence spread spectrum) in the 2.4GHz band (ii) FHSS (Frequency-hopping spread spectrum) in the 2.4 GHz band and (iii) IR light.
2. Signalling techniques and modulations at PHY layer.
3. The fundamental access method of 802.11 which is carrier sense multiple access with collision avoidance.
4. Privacy and security of user data being transferred over the wireless media.
5. Address functions required for an 802.11 complaint device to operate either in a peer-to-peer fashion or integrated with an existing wired LAN.

IEEE 802.11a

The IEEE 802.11a standard is the first standard in the IEEE 802.11 series. It defines a Wi-Fi format for providing wireless connectivity in the 5 GHz ISM (Industrial, Scientific and Medical) band to give raw data speeds of up to 54Mbps.

Using the technology of the time, IEEE 802.11a was more costly and a little more difficult to implement as it operated at 5 GHz rather than 2.4 GHz and as a result it was less widely used.

The 802.11a standard uses basic 802.11 concepts as its base, and it operates within the 5GHz Industrial, Scientific and Medical (ISM) band enabling it to be used worldwide in a licence free band. The modulation is Orthogonal Frequency Division Multiplexing (OFDM) to enable it to transfer raw data at a maximum rate of 54 Mbps, although a more realistic practical level is in the region of the mid 20 Mbps region.

IEEE 802.11b

IEEE 802.11b was the first Wi-Fi standard to be widely adopted. Using 2.4 GHz the technology was much easier and cheaper to develop than the 802.11a which used the higher frequency 5 GHz band.

When transmitting data 802.11b uses the CSMA/CA technique that was defined in the original 802.11 base standard and retained for 802.11b. Using this technique, when a node wants to make a transmission it listens for a clear channel and then transmits. It then listens for an acknowledgement and if it does not receive one it backs off a random amount of time, assuming another transmission caused interference, and then listens for a clear channel and then retransmits the data.

IEEE 802.11e

It modifies current 802.11 MAC layer to support quality of services to multimedia applications. The IEEE 802.11 Task Group ‘e’ is responsible for proposing improvements to the 802.11 standard to make it better able to handle voice traffic, moving picture experts group (MPEG) video at up to 3MBPS and data stream at up to 10 MBPS.

IEEE 802.11g

It provides high-rate extension to 802.11b allowing for data rates increased to 54 MBPS from 11MBPS in the 2.4GHz industrial, scientific and medical (ISM) band. It also opens the possibility for using IEEE 802.11 networks, in more demanding applications, such as wireless multimedia video transmission and broadcast MPEG.

IEEE 802.11f

This is still under development. The scope of this is to develop recommended practices for an inter-access point protocol that provides the necessary capabilities to achieve multivendor AP interoperability across a distribution system supporting IEEE 802.11 wireless LAN links. It promises to let users move through an extended wireless LAN having multiple APs from different vendors and maintaining the connection.

IEEE 802.11h

This standard is still under development. It enhances the 802.11 MAC standard and 802.11a high speed PHY layer in the 5 GHz band. Objective is to make IEEE 802.11a products complaint with the European regulatory requirements. However, the 802.11h Task Group is working on a new version of the standard that would support transmit power control and dynamic frequency selection.

IEEE 802.11n

In 2004, IEEE announced that it had formed a new 802.11 Task Group to develop a new amendment to the 802.11 standard for local area wireless networks. The real data throughput will be at least 100mbps and should

be up to four to five times faster than 802.11a or 802.11g, and perhaps 20 times faster than 802.11b. it is projected that 802.11n will also offer a better operating distance than current networks.

IEEE 802.11p

IEEE 802.11p is a draft amendment to the IEEE 802.11 standard to add wireless access the vehicular environment. It defines enhancements to 802.11 required to support the intelligent transportation system applications. This includes data exchange between high-speed vehicles and between the vehicles and the roadside infrastructure in the licensed ITs band of 5.9 GHz.

WLAN Protocols

- **802.11a Protocol**− This protocol supports very high transmission speeds of 54Mbps. It has a high frequency of 5GHz range, due to which signals have difficulty in penetrating walls and other obstructions. It employs Orthogonal Frequency Division Multiplexing (OFDM).
- **802.11b Protocol** − This protocol operates within the frequency range of 2.4GHz and supports 11Mbps speed. It facilitates path sharing and is less vulnerable to obstructions. It uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with Ethernet protocol.
- **802.11g Protocol** − This protocol combines the features of 802.11a and 802.11b protocols. It supports both the frequency ranges 5GHz (as in 802.11a standard) and 2.4GHz (as in 802.11b standard). Owing to its dual features, 802.11g is backward compatible with 802.11b devices. 802.11g provides high speeds, varying signal range, and resilience to obstruction. However, it is more expensive for implementation.
- **802.11n Protocol** − Popularly known as Wireless N, this is an upgraded version of 802.11g. It provides very high bandwidth up to 600Mbps and provides signal coverage. It uses Multiple Input/Multiple Output (MIMO), having multiple antennas at both the transmitter end and receiver ends. In case of signal obstructions, alternative routes are used. However, the implementation is highly expensive.

IEEE 802.11p

In vehicular ad hoc networks, vehicular safety communication applications cannot tolerate long connection establishment delays before being enabled to communicate with other vehicles encountered on the road. Similarly, non-safety applications also demand efficient connection setup with roadside stations providing services because of the limited time taken for a car to drive through the coverage area. Additionally, the rapidly moving vehicles and complex roadway environment present challenges at the PHY level.

The IEEE 802.11p standard is basically proposed for the following functions:

1. It describes the functions and services required by WAVE-conformant stations to operate in a rapidly varying environment and exchange messages without having to join a BSS, as in the traditional IEEE 802.11 use case.
2. It defines the WAVE signalling technique and interface functions that are controlled by the IEEE 802.11 MAC.

The details of the WAVE PHY and MAC layers are discussed below.

Physical Layer

At PHY layer level, the main aim of IEEE 802.11p is to make minimum necessary changes to IEEE 802.11 PHY so that WAVE devices can communicate effectively among fast-moving vehicles in the roadway environment. Although MAC level amendments are fundamentally software updates that are relatively easy to make, PHY level amendments necessarily should be limited to avoid designing an entirely new wireless air-link technology. Accordingly, three changes are made as follows:

1. **MHz Channel:** IEEE 802.11p is essentially based on the OFDM (Orthogonal frequency-division multiplexing) PHY defined for IEEE 802.11a, with a 10 MHz-wide channel instead of the 20MHz one usually used by 802.11a devices. This change is a to address the accessing delay in the vehicular environment.
2. **Improved receiver performance requirement:** IEEE 802.11p introduces some improved receiver performance requirements in adjacent channel rejections. There are two categories of requirements listed in the proposed standard. Category 1 is mandatory and generally understood to be reachable with today's chip manufacturers. Category 2 is more stringent and optional.
3. **Improved transmission mask:** Four spectrum masks are defined that are meant for class A-D operations.

MAC Layer

A key amendment introduced by the IEEE 802.11p WAVE is the term "WAVE mode". A station in WAVE mode is allowed to transmit and receive data frames with the wildcard BSSID value and without the need to belong to a BSS of any kind a priori. This means two vehicles can immediately communicate with each other upon encounter without any additional overhead as long as they operate in the same channel.

1. A station in WAVE mode can send and receive data frames with the wildcard BSSID with "To DS" and "From DS" fields both set to 0, regardless of whether or not it is a member of a WBSS.
2. A WBSS is a type of BSS consisting of a set of cooperating stations in WAVE mode that communicate using a common BSSID. A WBSS is initialized when a radio in WAVE mode sends a WAVE beacon, which includes all necessary information for a receiver to join.
3. A radio joins a WBSS when it is configured to send and receive data frames with the BSSID defined for that WBSS. Conversely, it ceases to belong to WBSS when its MAC stops sending and receiving frames that use the BSSID of that WBSS.
4. A station will not be a member of more than one WBSS at one time. A station in WAVE mode will not join an infrastructure BSS or IBSS, it will not use active or passive scanning, and lastly it will not use MAC authentication or association procedures.
5. A WBSS ceases to exist when it has no members. The initiating radio is no different from any other member after the establishment of a WBSS. Therefore, a WBSS can continue if the initiating radio ceases to be a member.

WLAN Applications

Wireless networks support many applications that benefit from user mobility and higher reliability because of less error-prone cabling. Furthermore, many wireless network applications realize significant cost savings

because of increases in efficiencies and less downtime as compared to a wired network.

Internet Access

One of the most compelling reasons to install a wireless network is to enable the sharing of a single high-speed Internet connection. With this type of configuration, every member of a family or small business can easily share a single high-speed connection that a cable or DSL modem offers. This is convenient and saves money because everybody can simultaneously have access to the Internet and roam anywhere in the house or office.

Voice over Wireless

The use of wireless networks to support the transmission of voice conversations is a beneficial solution when people need to constantly stay in contact with each other. In fact, a wireless LAN designed to support voice communications can completely replace a traditional wire-based telephone system within a particular facility.

Health Care

More and more hospitals are deploying wireless networks to improve operational efficiency and convenience. In most cases, hospitals deploy wireless LANs in high patient-traffic areas including emergency rooms, critical care wards, nursing stations, as well as in doctor's offices and patient waiting areas. Hospital staff can use mobile computer devices to increase efficiency and accuracy when caring for patients.

Health-care canters must maintain accurate records to ensure quality patient care. A simple mistake can cost someone's life. As a result, doctors and nurses must carefully record test results, physical data, pharmaceutical orders, and surgical procedures. This paperwork often overwhelms health-care staff, taking 50-70 percent of their time.

Education

Many colleges and elementary schools are finding beneficial reasons to install wireless LANs, mostly to provide mobile network applications to their students. In fact, schools have begun using the existence of wireless LAN access as a competitive advantage. These schools are targeting the growing number of students with laptops and expectations of accessing the Internet and school resources from anywhere on campus, such as classrooms, libraries, quads, and dormitories.

Location-Based Services

With wireless networks, you can make the location of a particular person or item available to a central location. The ability to track the position of moving objects brings about some interesting applications. The coordinates of users can feed into a server-based application that implements a location-based service.

Real Estate

Real estate salespeople perform a great deal of their work away from the office, usually talking with customers at the property being sold or rented. Before leaving the office, salespeople normally identify a few sites to show a customer, print the Multiple Listing Service (MLS) information that describes the property, and then drive to each location with the potential buyer.

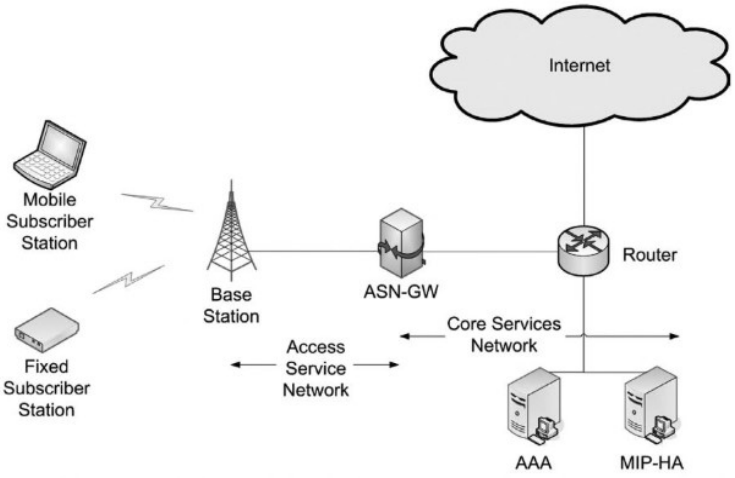
Wireless Metropolitan Area Networks

Metropolitan area network area large computer networks usually spanning a city. They typically use wireless infrastructure or optical fiber connections to link their sites. A MAN is optimized for a larger geographical area

compared to local area network (LAN), ranging from several blocks of building to the entire city. They can also depend on communication channels of moderate-to-high data rates. A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations.

WMAN Network Architecture

Below is the architecture of a WiMAX network. Each base station (BS) covers a certain area around it for network access and may typically serve a mix of mixed and mobile clients within its coverage area. Base stations in a geographic area are connected via a backhaul to access service network gateway (ASN-GW). ASN-GW is connected via traditional IP network links to a core services network (CSN). The CSN includes authentication, authorization and accounting services as well as home agent services for operation of mobile IP.



On the other hand, provides the foreign agent service of mobile IP that allows roaming mobile terminals to connect to an ASN of a different service provider than their own. Interface are defined for the following interaction within WiMAX network: mobile subscriber station to BS, BS to ASN, ASN to another ASN, ASN to CSN and CSN to another CSN. All these interfaces operate on IP-based protocols with support for both IPv4 and IPv6.

WiMAX is a separate radio system that is designed to either supplement or replace the existing broadband internet distribution systems. In practice, WiMAX competes with both 3G wireless services and ISPs that distribute internet access to fixed locations through telephone lines and cable television utilities. Home and business subscribers to a WiMAX service usually use either a wired LAN or Wi-Fi to distribute the network within their buildings.

Network Components

The main components of the WiMAX system are the BS, WiMAX receiver and the backhaul.

1. **WiMAX base station:** A WiMAX BS consists of indoor electronics and a WiMAX tower. A WiMAX BS can provide coverage area would use the MAC layer defined in the internet.

The WiMAX BSs would use the MAC layer defined in the standard. A common interface makes the networks interoperable and would allocate uplink and downlink bandwidth to subscribers according to their needs on an essentially real time basis.

2. **WiMAX receiver:** A WiMAX receiver may have a separate antenna or could be a standalone box or an interface card sitting on the laptop or computer or any other device. This is referred to as customer premise equipment.
3. **Backhaul:** A WiMAX tower station can connect directly to the internet using a high bandwidth wired connection. It can also connect to another WiMAX tower using a LOS, microwave link. Backhaul refers to the connection from the access point to the BS and from the BS to the core network.

Features of WiMAX

The WiMAX standard has been developed with many objectives in mind. The important features of WiMAX are as follows:

1. **Flexible architecture:** WiMAX supports several system architectures, including P2P, P2MP and ubiquitous coverage. The WiMAX MAC supports P2MP and ubiquitous service by scheduling a time slot for each SS.
2. **High security:** WiMAX supports Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES). By encrypting the links between the BS and the SS, WiMAX provides subscribers with privacy and security across the broadband wireless interface.
3. **Quick deployment:** Compared with the deployment of wired solutions, WiMAX requires little or no external plant construction. For example, excavation to support the trenching of cables in not required. Operators that have obtained licenses to use one of the licensed bands or plans to use one of the unlicensed bands, do not need to submit further applications to the government.
4. **Multilevel service:** The manner in which QoS is delivered is generally based on the service level agreement between the service provider and the end-user. Furthermore, one service provider can offer different SLAs to different subscribers or even to different users on the same SS.
5. **Interoperability:** WiMAX is based on international, vendor-neutral standards that make it easier for end-users to transport and use their SS at different locations or with different service providers. Interoperability protects the early investment of an operator as it can select equipment from different equipment vendors, and it will continue to drive the costs of equipment down as a result of mass adoption.
6. **Portability:** As with current cellular systems, once the WiMAX SS is powered up it identifies itself, determines the characteristics of the link with the BS, as long as the SS is registered in the system database and then negotiates its transmission characteristics accordingly.
7. **Mobility:** The IEEE 802.16e amendment has added key features in support of mobility. Improvements have been made to the OFDM and orthogonal frequency division multiple access (OFDMA) PHY layers to support devices and services in a mobile environment.
8. **Cost effective:** WiMAX is based on an open international standard. Mass adoption of the standard and the use of low-cost mass-produced chipsets will bring costs down dramatically and the resultant competitive pricing will provide considerable cost savings for service providers and end-users.

Broadband Wireless Networks

Broadband wireless networks are those which provide higher rate voice and data services to the users. Some of

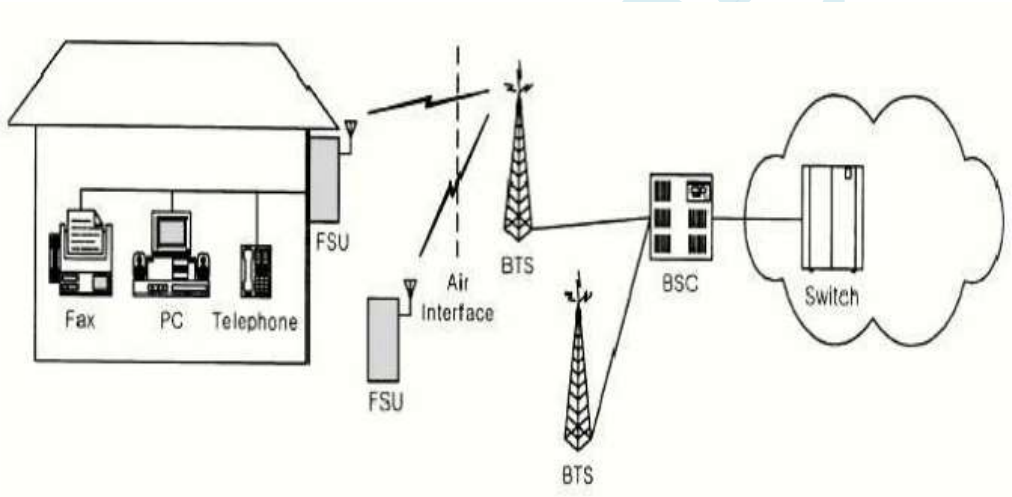
the technologies that support this wireless local loop, local multipoint distribution service, multichannel multipoint distribution service and wireless ATM.

Wireless Local Loop

As WLL systems are fixed, the requirement for interoperability of a subscriber unit with different BSs is less stringent than that of mobile services. As a result, there exist a variety of standard and commercial systems. Each standard has its own air interface specification, system architecture, network elements and terminology, the functions of the elements may differ according to systems.

The fixed subscriber unit (FSU) is an interface between subscriber's wired device and WLL network. The wired device can be computer or facsimiles (FAX) as well as telephones. Several systems use other acronyms for FSU, such as the wireless access fixed unit (WAFU).

FSU is connected with the BS via radio band that is several hundreds of MHz or around 2GHz. As well as a fixed service, high gain directional antennas can be used between the FSU and the BS, being arranged by LOS. This drastically heightens the channel efficiency and the capacity of the system.

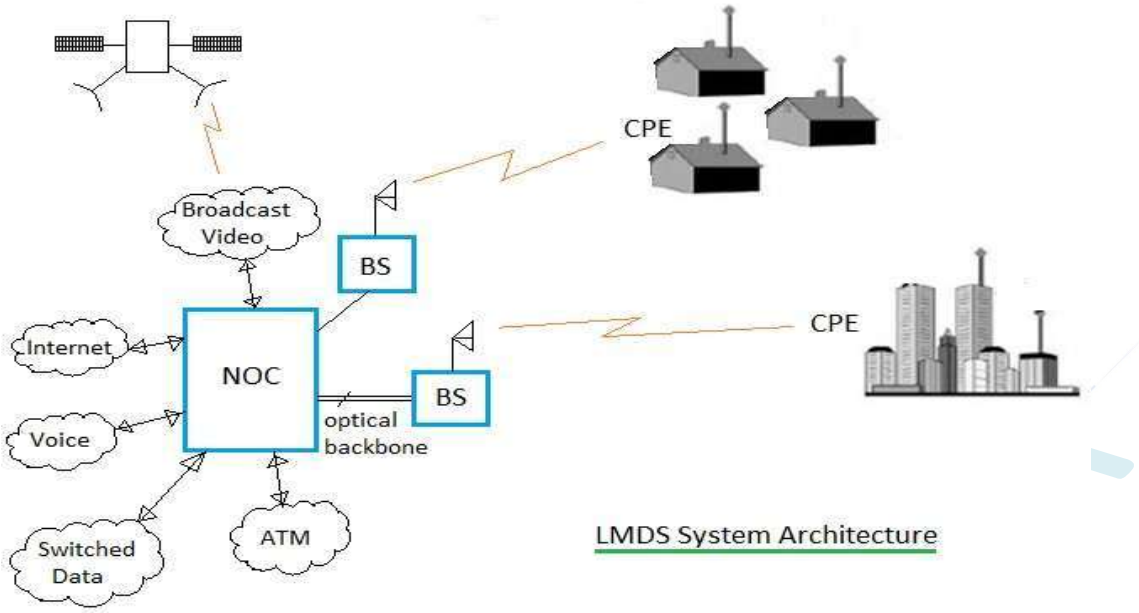


A BSC controls one or more BTSs and provides an interface to the local exchange in the control office. An important role of BSC is to transcode between the source codes used in wired network and those at the air interface. Hence, a BSC is often called the radio port control unit or the transcoding and network interface unit.

Local Multipoint Distribution Service

To compete with wireline services using digital subscriber loop, the broadband WLL system supporting multimedia services should be developed. From this point of view, the strongest candidate for B-WLL system currently is LMDS. LMDS can offer the WLL services such as video telephony, video-on-demand and high-speed internet access LMDS is a broadband wireless P2MP communication system operating above 20GHz that can be used to provide digital two-way voice, data, internet and video services.

Various network architecture is possible within and LMDS system design. The majority of system operators will be using P2MP wireless access designs, although P2P systems and TV distribution systems can be provided within the LMDS system.



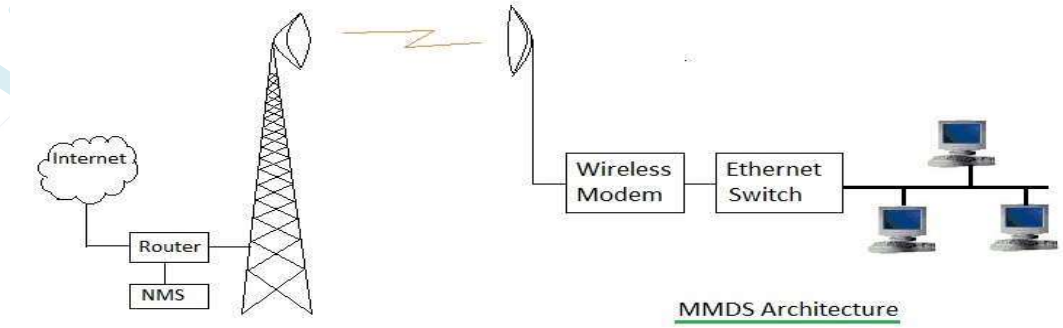
LMDS System Architecture

The NOC contains the network management system that manages large regions of the customer network. Multiple NOCs can be interconnected. The fiber-based infrastructure typically consists of synchronous optical network (SONET); optical carrier (OC)12, OC3 and DS3 links; ATM and IP switching systems.

The BS is where the conversion from fibered infrastructure to wireless infrastructure occurs. BS equipment includes the network interface for fiber termination; modulation and demodulation functions; and microwave transmission and reception equipment typically located at top of roof or a pole.

Multichannel Multipoint Distribution Service

Although wireless DSL has become the broadband technology of choice for many small businesses, home offices and even residential customers, DSL is not universally available. Cable modems are another option, but such service is generally targeted at home users who have cable television. Therefore, multichannel multipoint distribution services are better option for small businesses but not for near central offices.



MMDS Architecture

MMDS, which operates at 2.5 and 3.5GHz is not the only broadband wireless technology available. Smaller ISPs are using the 2.4GHz unlicensed bandwidth wireless LAN-based technologies successfully. There are also services operating above 10GHz frequencies referred to as millimetre wave, including local multipoint distribution service at 28 and 38GHz.

The wireless link is a dedicated, always-ON type of connection, just like DSL. Radio interface standard is derived from the specification used by cable modems, data over cable service interface specification with enhancements to the PHY and MAC layers to address the wireless medium. The MAC layer governs how multiple users share the same radio channel, whereas the PHY layer handles radio modulation.

Wireless ATM

ATM networks embody a key technology for supporting broadband multimedia services not only in the public network, but also in a local area and eventually in a home. Wireless connection to the broadband ATM network is extremely attractive, as is evidenced by the success of GSM, DECT etc.

The environment in a home wireless ATM network would consist of several appliances, for example, PC laptop, printers, machines, security systems, home appliances, digital high definition and standard definition television sets etc. the operating frequency for domestic wireless ATM networks will most likely be in the 5-6GHz band. The existing high-speed WLAN standard already has a frequency allocation within Europe.

WMAN Applications

WiMAX technology will revolutionize the way we communicate. It will provide total freedom to people who are highly mobile, allowing them to stay connected with voice, data, and video services. WiMAX network applications are grouped into two broad categories: private and public networks applications.

Private networks used exclusively by a single organization, institution or business offer dedicated communication links for the secure and reliable transfer of voice, data and video.

In public network, resource is accessed and shared by different users, including both businesses and private individuals. Public networks generally require a cost-effective means of providing ubiquitous coverage, as the location of the users is neither predictable nor fixed.

Wireless Service Provider Backhaul

Wireless service providers use WiMAX equipment to backhaul traffic from BSs in their access networks. Internet or PSTNs are connected to the WiMAX BS with the help of optical fiber link, serving as a backhaul network. Through air, WiMAX communicates with the SSs. These SSs intern communicate with the access networks. Access networks may be based on Wi-Fi, WiMAX or any proprietary wireless access technology.

Banking Networks

WiMAX technology finds an important role in banking networks. Large banks can connect branches and ATM sites to their regional office through a private WiMAX network carrying voice, data, and video traffic. These banks are normally spread over a large area and need high security and bandwidth to handle the traffic.

Education Networks

Educational institutes can use WiMAX networks to connect different colleges and administrative offices within a district. From the central administrative office, the number of associated institutes like engineering and medical colleges can be connected for number of purposes.

Public Safety

Government public safety agencies, such as police, fire and search and rescue, can use WiMAX networks to support response to medical and other emergency situations. In addition to providing two-way voice communication between the dispatch centre and on-site emergency response teams, the network relays video images and data from the site of the accident or disaster to the control center. This data can be relayed to expert teams of medical or emergency staff, who can analyse the situation in real time, as if they were on the site.

UNIT-IV

Wireless Ad Hoc networks

A wireless ad-hoc network (WANET) is a type of local area network (LAN) that is built spontaneously to enable two or more wireless devices to be connected to each other without requiring a central device, such as a router or access point. When Wi-Fi networks are in ad-hoc mode, each device in the network forwards data to the others.

Wireless ad hoc networks do not require a fixed infrastructure thus it is relatively easy to set up and deploy a wireless ad hoc network. Without the fixed infrastructure, the topology of a wireless ad hoc network is dynamic and changes frequently. It is not realistic to assume a static or a specific topology for a wireless ad hoc network. On the other hand, wireless ad hoc networks need to be self-organizing thus mobile nodes in a wireless ad hoc network can adapt to the change of topology and establish cooperation with other nodes at runtime.

Features:

Quantitative Features

1. **Network settling Time:** Time is required for a collection of mobile nodes to automatically organize themselves and to transmit the first task reliably.
2. **Network join time:** Time is required for an entering node or group of nodes to become integrated into the ad hoc network.
3. **Network adapter time:** Time is required for the ad hoc network to recognize the loss of one or more nodes and to reorganize itself to rout around the departed nodes.
4. **Memory byte requirement:** Storage space is required in bytes, including routing tables and other management tables.
5. **Network Scalability:** It is the number of nodes that the ad hoc network can scale to and reliably preserve communication. The network should be able to scale to thousands of nodes.

Qualitative Features

1. **Knowledge of nodal locations:** Does the routing algorithm require local or global knowledge of the network?
2. **Effect to topology changes:** Does the routing algorithm need complete restructuring or incremental updates?
3. **Single or Multichannel:** Does the routing algorithm utilize a separate control channel? In some applications, multichannel execution may make the network vulnerable.
4. **Real time voice services:** Can the network support simultaneous real time multicast voice while supporting routine traffic loads associated with situation awareness and other routine services?
5. **Real time video services:** Can the nodes receives or transmit video on demand, while still supporting traffic levels associated with situation awareness?

Advantages

1. They can be set up very fast.
2. They are very resilient. No single point of failure, such as a base station. Even if individual node fails the network still functions.
3. Every node can communicate with any other node, so nodes can make better use of the channel.
4. They have cheap deployment because of non-requirement of base station.

Applications

The dynamic and self-organized nature of wireless ad hoc networks makes them particularly useful in situations.

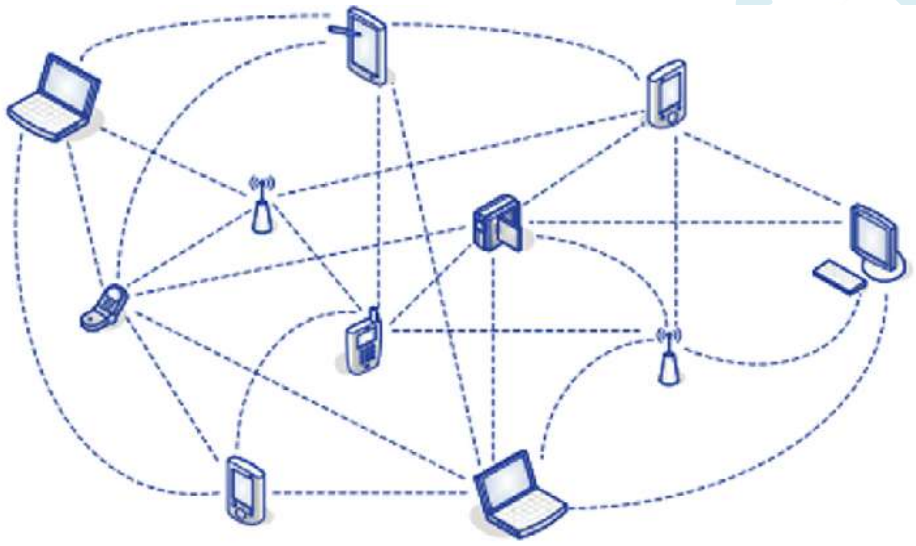
1. In military communication for search and rescue operations where the robustness and speed of deployment is critical.
2. For sensing forest fires, monitoring buildings, studying wildlife etc.
3. Wireless Local Area Network in conferences where placing wires would be a nuisance.

4. A mobile ad hoc network of satellites can be designed for emergency applications such as disaster management, rescue operations etc.
5. Campus networks: To share educational information among the students and staff.
6. To have broadband internet with mobility in fourth generation(4G) wireless networks.

Mobile Ad Hoc Networks (MANET)

A mobile ad hoc network consists of a number of mobile devices that come together to form a network as needed, without any support from any existing internet infrastructure or any other kind of fixed stations. MANET's have a wide range of applications from military networks to emergency telecommunications. MANET's are still not perfect.

Network Architecture



MANET is formed by a set of MNs, such as laptops, mobile phones and desktop machine with wireless interface capability and by communicating among themselves by means of the air as a communication media. MANETs can use either single-hop or multi-hop communication. In single-hop communication the hosts are in one coverage area, thus communication is direct from host to host. On the other hand, in multi-hop communication hosts communicate by using intermediate hosts such as in internet communications. Thus, there are many coverage areas interacting with each other.

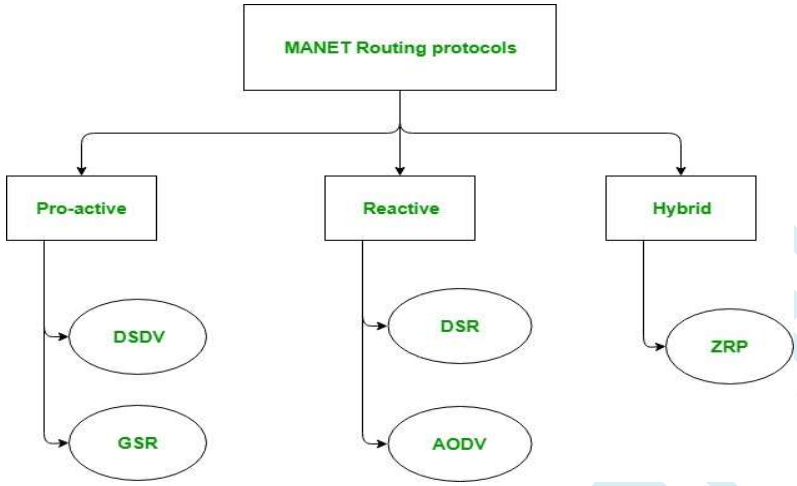
The hosts establish their own network dynamically without relying on the support of infrastructure or a central administration and cooperate to forward data in a multi-hop fashion.

Routing Protocols of MANET

In MANETs, nodes are mobile and can be connected dynamically in an arbitrary manner. All nodes of these networks behave as routers and take part in discovery and maintenance of routes to another nodes in the network.

Classification of routing protocols in MANETs can be done on routing strategy and network structure. According to the routing strategy, the routing protocols can be categorized as table-driven and source-initiated,

while depending on the network structure these are classified as flat routing, hierarchical routing and geographic position-assisted routing.



1. Pro-active routing protocols:

These are also known as table-driven routing protocols. Each mobile node maintains a separate routing table which contains the information of the routes to all the possible destination mobile nodes.

Since the topology in the mobile ad-hoc network is dynamic, these routing tables are updated periodically as and when the network topology changes. It has a limitation that is don't work well for the large networks as the entries in the routing table becomes too large since they need to maintain the route information to all possible nodes.

Destination Sequenced Distance Vector Routing Protocol (DSDV):

It is a pro-active/table driven routing protocol. In DSDV, each MN of an ad hoc network maintains a routing table which lists all available destinations, the metric and next hop to each destination and a sequence number generated by the destination node. Using such routing table stored in each MN, the packets are transmitted between the nodes of an ad hoc network. Each node of ad hoc network updates the routing table with advertisement periodically or when significant new information is available to maintain the consistency of the routing table.

Global State Routing Protocol:

In GSR, each node maintains a neighbour list, a topology table, a next hop table and a distance table. Neighbour list of a node contains the list of its neighbours. For each destination node, the topology table contains the link state information as reported by the destination node and the time stamp of the information. For each destination, the next hop table contains the next hop to which the packets for this destination must be forwarded. The distance table contains the shortest distance to each destination node.

2. Reactive routing protocols:

These are also known as on demand routing protocol. These are also known as on-demand routing protocol. In this type of routing, the route is discovered only when it is required/needed. The process of route discovery occurs by flooding the route request packets throughout the mobile network. It consists of two major phases namely, route discovery and route maintenance.

Dynamic Source Routing protocol (DSR): It is a reactive/on-demand routing protocol. In this type of routing, the route is discovered only when it is required/needed. The process of route discovery occurs by flooding the route request packets throughout the mobile network.

It consists of two phases:

Route Discovery:

- **Route Discovery:** This phase determines the most optimal path for the transmission of data packets between the source and the destination mobile nodes.
- **Route Maintenance:** This phase performs the maintenance work of the route as the topology in the mobile ad-hoc network is dynamic in nature and hence, there are many cases of link breakage resulting in the network failure between the mobile nodes.

Ad-Hoc On-Demand Vector Routing protocol (AODV):

AODV is a method of routing messages between MNs (Mobile Nodes). It allows the MNs to pass messages through their neighbours to the nodes with which they cannot directly communicate. AODV does this by discovering the routes along which messages can passed. AODV makes sure that these routes do not contain loops and tries to find the shortest route possible. AODV is also able to handle changes routes and can create new routes if there is an error.

3. Hybrid Routing Protocol:

It basically combines the advantages of both, reactive and pro-active routing protocols. These protocols are adaptive in nature and adapts according to the zone and position of the source and destination mobile nodes. One of the most popular hybrid routing protocol is Zone Routing Protocol (ZRP).

The whole network is divided into different zones and then the position of source and destination mobile node is observed. If the source and destination mobile nodes are present in the same zone, then proactive routing is used for the transmission of the data packets between them. And if the source and destination mobile nodes are present in different zones, then reactive routing is used for the transmission of the data packets between them.

Applications:

With the increase of portable devices as well as progress in wireless communication, MANET is gaining importance with the increasing number of widespread applications. MANETs can be applied anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. Typical applications of MANET are as follows:

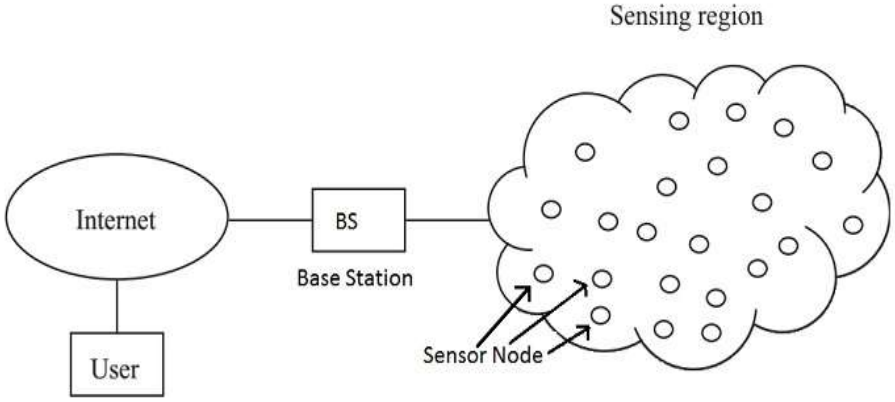
1. **Military battlefield:** Military equipment now routinely contains some sort of computer equipment. MANETs allow the military to maintain information among the soldiers, vehicles and military information headquarters. This basic technique of MANET came from this field.
2. **Commercial Sector:** MANETs can be used in emergency/rescue operations for disaster relief efforts, for example, in fire, flood or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network are needed. Information is relayed from one resque team member to another over a small handheld device.
3. **Creating personal network:** MANET can simplify the intercommunication between various mobile devices [e.g. a personal digital assistant, a laptop etc.]. Tedious wired cables are replaced with wireless connections. Such MANET extends the access to the internet or other networks by mechanism such as WLAN, general packet radio services.
4. **Local Level:** MANETs can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at a conference or classroom.
5. **Message oriented applications:** When the message is prepared, it is routed among the nodes of the network, until it arrives to the node connected to internet and so transmitted to service centre arranged for the delivery of the message.

Wireless Sensor Networks

Wireless Sensor Networks (WSNs) can be defined as a self-configured and infrastructure-less wireless networks to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location or sink where the data can be observed and analysed. A sink or base station acts like an interface between users and the network. One can retrieve required information from the network by injecting queries and gathering results from the sink. Typically, a wireless sensor network contains hundreds of thousands of sensor nodes. The sensor nodes can communicate among themselves using radio signals. A wireless sensor node is equipped with sensing and computing devices, radio transceivers and power components. The individual nodes in a wireless sensor network (WSN) are inherently resource constrained: they have limited processing speed, storage capacity, and communication bandwidth. After the sensor nodes are deployed, they are responsible for self-organizing an appropriate network infrastructure often with multi-hop communication with them. Then the onboard sensors start collecting information of interest.

Network Architecture

When a large number of sensor nodes are deployed in a large area to co-operatively monitor a physical environment, the networking of these sensor node is equally important. A sensor node in a WSN not only communicates with other sensor nodes but also with a Base Station (BS) using wireless communication.



The base station sends commands to the sensor nodes and the sensor node perform the task by collaborating with each other. After collecting the necessary data, the sensor nodes send the data back to the base station.

A base station also acts as a gateway to other networks through the internet. After receiving the data from the sensor nodes, a base station performs simple data processing and sends the updated information to the user using internet.

If each sensor node is connected to the base station, it is known as Single-hop network architecture. Although long distance transmission is possible, the energy consumption for communication will be significantly higher than data collection and computation.

Technologies

Several standards and technologies are currently either ratified or under development for wireless sensor networks. “ZigBee” is a mesh-networking standard intended for uses such as embedded sensing, medical data collection, consumer devices such as television remote controls and home automation.

Production of low cost and tiny sensor nodes for WSN is possible from recent and future progress in the fields of micro-electromechanical system and Nano-electromechanical systems.

Operating system for wireless sensor network nodes are typically less complex than general purpose operating systems both because of the special requirements of sensor network applications and of the resource constraints in sensor network hardware platforms.

Applications

A WSN consists of a number of sensors spread across a geographical area. Each sensor has wireless communication capability and some level of intelligence for signal processing and networking of the data. Some of the applications of WSN are as follows:

Military or Border Surveillance Applications: WSNs are becoming an integral part of military command, control, communication and intelligence systems. Sensors can be deployed in a battle field to monitor the presence of forces and vehicles, and track their movements, enabling close surveillance of opposing forces.

Environmental Applications: Environmental applications include tracking the movements and patterns of insects, birds or small animals.

Health Care Applications: Wireless sensor networks can be used to monitor and track elders and patients for health care purposes, which can significantly relieve the severe shortage of health care personnel and reduce the health care expenditures in the current health care systems. For example, sensors can be deployed in a patient's home to monitor the behaviours of the patient. It can alert doctors when the patient falls and requires immediate medical attention.

Environmental Conditions Monitoring: WSN applications in this area include monitoring the environmental conditions affecting crops or livestock, monitoring temperature, humidity and lighting in office buildings, and so on. These monitoring modules could even be combined with actuator modules which can control, for example, the amount of fertilizer in the soil, or the amount of cooling or heating in a building, based on distributed sensor measurements

Home Intelligence: Wireless sensor networks can be used to provide more convenient and intelligent living environments for human beings. For example, wireless sensors can be used to remotely read utility meters in a home like water, gas, electricity and then send the readings to a remote centre through wireless communication.

Industrial Process Control: In industry, WSNs can be used to monitor manufacturing process or the condition of manufacturing equipment. For example, chemical plants or oil refiners can use sensors to monitor the condition of their miles of pipelines. These sensors are used to alert in case of any failures occurred.

Agriculture: Using wireless sensor networks within the agricultural industry is increasingly common; using a wireless network frees the farmer from the maintenance of wiring in a difficult environment. Gravity feed water systems can be monitored using pressure transmitters to monitor water tank levels, pumps can be controlled using wireless I/O devices and water use can be measured and wirelessly transmitted back to a central control centre for billing. Irrigation automation enables more efficient water use and reduces waste.

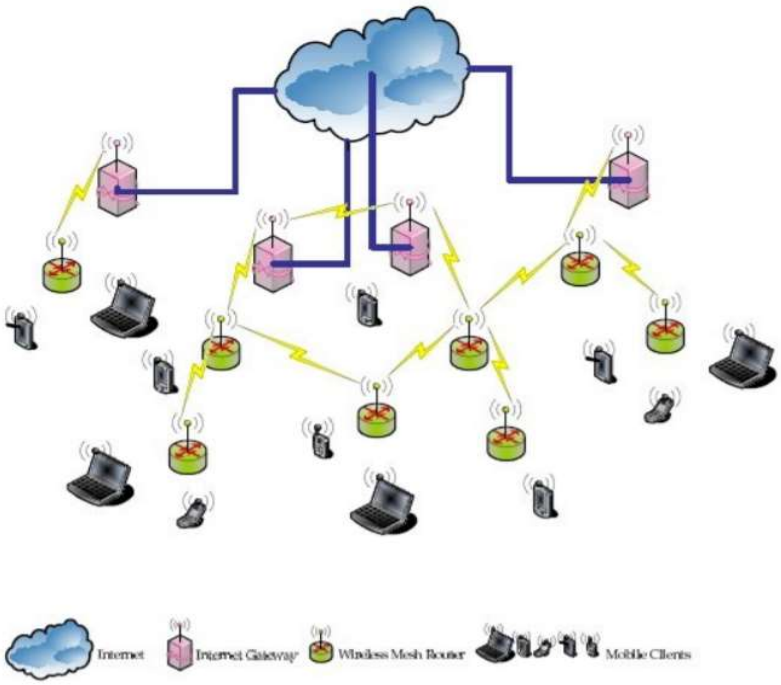
Structural Monitoring: Wireless sensors can be used to monitor the movement within buildings and infrastructure such as bridges, flyovers, embankments, tunnels etc... enabling Engineering practices to monitor assets remotely without the need for costly site visits, as well as having the advantage of daily data, whereas traditionally this data was collected weekly or monthly, using physical site visits, involving either road or rail closure in some cases.

Wireless Mesh Networks

Recently, the deployment of WMNs providing economical and scalable broadband internet connectivity among communities is becoming progressively popular. A WMN is a communication network made up of radio nodes organized in a mesh topology. The coverage area of the radio nodes working as a single network is sometimes called a "mesh cloud". Access to this mesh cloud is dependent on the radio nodes working in harmony with each other to create a radio network. A mesh network is reliable and offers redundancy. When one node can no longer operate, the rest of the nodes can still communicate with each other directly or through one or more intermediate nodes.

WMN Architecture

Wireless mesh architecture design is a first step towards providing high-bandwidth Internet access over a specific coverage area. WMNs consist of Mesh Clients (MCs) and Wireless Mesh Routers (WMRs), which relaying each other's packets in a multi-hop fashion, where mesh routers have minimal mobility and form the Backbone of WMNs. Mesh architecture breaks the long distance into a series of shorter hops to boost the signal by intermediate nodes. Intermediate nodes not only sustain signal strength, but also forward packages on behalf of other nodes based on their knowledge of the network. Such architecture allows continuous connections and reconfiguration around broken or blocked paths by making forwarding decisions from node to node until the destination is reached. Besides, it provides high-bandwidth Internet access and offers a low cost and flexible deployment.



The architecture of WMNs can be classified into three types:

1. **Infrastructure/Backbone WMNs:** In this type of wireless mesh networks (Figure 2.1) the mesh routers form an infrastructure for the clients that connect to them. Various radio technologies may be used to form the infrastructure in addition to the widely used IEEE 802.11 technology. As the mesh routers have gateway functionality the routers may be connected to the Internet. This infrastructure network enables integration of WMNs with existing wireless networks. If the same radio technology is used in both the clients and the mesh routers direct communication among them is possible. In situations where the radio technology of the client is different from that of the router, clients communicate with the base stations that have Ethernet connections to mesh routers. Typical application of infrastructure meshing is the community networking.

2. **Client WMNs:** Client meshing provides peer-to-peer networks among client devices. In this type of architecture, client nodes constitute the actual network to perform routing and configuration functionalities as well as providing end user applications to customers. Hence, a mesh router is not required for these types of networks. Client WMNs are usually formed using one type of radios on devices. Thus, a client WMN is actually the same as a conventional ad hoc network.
3. **Hybrid WMNs:** This architecture is the combination of infrastructure and client meshing. Mesh clients can access the network through mesh routers as well as directly meshing with other mesh clients. Although the infrastructure provides connectivity to other networks such as internet, Wi-Fi, WiMAX, and sensor networks, the routing capabilities of clients provide improved connectivity and coverage inside WMNs.

Applications

WMN applications are unique compared to other wireless networks such as cellular networks, ad hoc networks, wireless sensor networks.

1. **Broadband home Networking:** In mesh networking, the access points are replaced by wireless mesh routers with mesh connectivity established among them. Therefore, the communication between these nodes becomes much more flexible and more robust to network faults and link failures.
2. **Community and neighbourhood networking:** For community and neighbourhood networking, mesh networking allows many applications such as distributed file storage, distributed files access and video streaming.
3. **Enterprise Networking:** In mesh networking, access points are replaced by mesh routers and Ethernet wires can be eliminated. WMNs can grow easily as the size of enterprise expands.
4. **Transportation Systems:** Convenient passenger information services, remote monitoring of in-vehicles security video and driver communications can be supported with the help of WMNs.
5. **Health and Medical Systems:** In a hospital or medical centre monitoring and diagnosis data need to be processed and transmitted from one room to another for various purposes.
6. **Security Surveillance Systems:** As security is turning out to be very high concern, security surveillance systems become a necessity for enterprise buildings, shopping malls, grocery stores etc.

Vehicular Ad Hoc Networks (VANETs)

Recently, with the development of vehicle industry and wireless communication technology, vehicular ad hoc networks are becoming one of the most promising research fields.

VANETs provide communications among nearby vehicles and between vehicles and nearby roadside equipment but apparently differ from other networks by their own characteristics. VANETs are based on short range wireless communication between vehicles. Unlike infrastructure-based networks such as cellular networks, these networks are constructed on the fly.

The optimal goal of VANETs is to provide safer and more efficient roads in future by communicating timely information to drivers and concerned authorities. The prominent evolution of wireless communication witnessed recently has sparked the interest of the automotive industry. Many manufacturers have already developed system prototypes, allowing vehicles to communicate with their surroundings using wireless media.

Unique Characteristics of VANETs

The fundamental characteristics that differentiate VANETs from other networks are as follow:

1. **Geographically constrained Topology:** Roads limit the network topology to one dimension, the road direction. Except for crossroads or overlay bridges, roads are generally located far apart. Even in urban areas, where they are located close to each other, there exist obstacles, such as buildings and advertisement walls, which prevent wireless signals from travelling between roads.

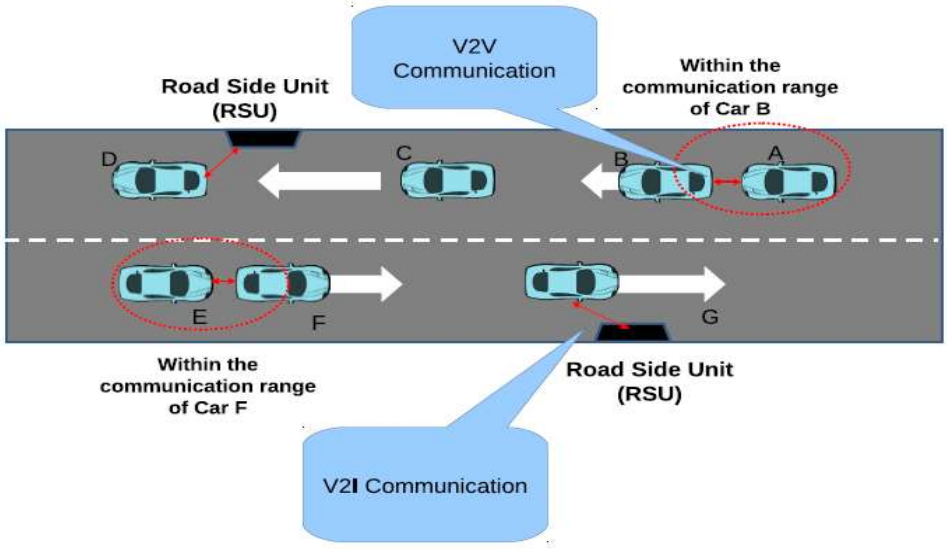
2. **Partitioning and Large-scale:** The probability of end-to-end connectivity decreases with distance, this is true for one-dimensional network topologies. In contrast, connectivity is often explicitly assumed in research for traditional ad hoc networks, sometimes even for the evaluation of routing protocols.
3. **Self-Organization:** The nodes in the network must be capable to detect each other and transmit packets with or without the need of a base station.
4. **Power consumption:** In traditional wireless networks, nodes are power-limited, and their life depends on their batteries – this is especially true for ad hoc networks. Vehicles, however can provide continuous power to their computing and communication devices.
5. **Node reliability:** Vehicles may join and leave the network at any time and much more frequently than in other wireless networks. The arrival/departure rate of vehicles depends on their speed, the environment, as well as on the driver that needs to be connected to the network.
6. **Vehicle Mobility:** As the nodes are mobile, the network topology may change rapidly and unpredictably and the connectivity among the terminals may vary with time. VANET should adapt to the traffic and propagation condition as well as the mobility patterns of the mobile network nodes.

Network Architecture

A typical VANETs architecture is shown below. Vehicle-to-vehicle and vehicle-to road-side base station/gateway communication is possible for providing safety and other information services to vehicle users. Group of vehicles together may form a cluster to disseminate information among themselves as well as to other clusters and base stations.

In a VANET, each vehicle in the system is equipped with a computing device, a short-range wireless interface and a global positioning system receiver. GPS receiver provides location, speed, current time and direction of the vehicles. Manufacturers are already enhancing cars with sensors that help drivers to park and provide GPS compasses as standard equipment on luxury cars.

Each vehicle store information about itself and other vehicles in a local database. The records in this database are periodically broadcasted. A record consists of the vehicle's identification, position in the form of latitude and longitude, current speed of the vehicle, direction and timestamps.



Applications

Some of the important applications of VANETs are as follows:

1. **Message and file delivery:** This application focuses on the delivery of messages and files in a vehicular network to the target receivers with acceptable performance.

2. **Internet Connectivity:** This application focuses on connecting the vehicles to the internet using roadside infrastructure and intervehicle communications to facilitate browsing, send/read email chatting etc.
3. **Communication-Based longitudinal control:** This application focuses on exploiting the "look-through" capability of VANETs to help avoiding accidents. For example, a vehicle can check the status of upfront vehicles status.
4. **Safety services:** Safety application include emergency braking, accidents, passing assistance, security distance warning and coordination of cars entering a lane.
5. **Traffic monitoring and management services:** In such type of services all vehicles are part of a ubiquitous sensor system. Each vehicle monitors the locally observed traffic situation such as density and average speed using an on-board sensor and the results are transferred to other vehicles via wireless data link through the network.