WHAT IS SECURITY?

Security is defined as “the quality or state of being secure—to be free from danger.”

Specialized areas of security

- ✓ **Physical security**, which encompasses strategies to protect people, physical assets, and the workplace from various threats including fire, unauthorized access, or natural disasters
- ✓ **Personal security**, which overlaps with physical security in the protection of the people within the organization
- ✓ **Operations security**, which focuses on securing the organization’s ability to carry out its operational activities without interruption or compromise
- ✓ **Communications security**, which encompasses the protection of an organization’s communications media, technology, and content, and its ability to use these tools to achieve the organization’s objectives
- ✓ **Network security**, which addresses the protection of an organization’s data networking devices, connections, and contents, and the ability to use that network to accomplish the organization’s data communication functions
- ✓ **Information security** includes the broad areas of information security management, computer and data security, and network security.

Information Security

The information security community protects the organization’s information assets from the many threats they face

Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information

Information Security components

Information Security programs are build around 3 objectives, commonly known as CIA – Confidentiality, Integrity, Availability.

- Confidentiality
- Integrity
- Availability(CIA)

CIA Triangle

The C.I.A. triangle - confidentiality, integrity, and availability - has expanded into a more comprehensive list of critical characteristics of information. At the heart of the study of information security is the concept of policy. Policy, awareness, training, education, and technology are vital concepts for the protection of information and for keeping information systems from danger.

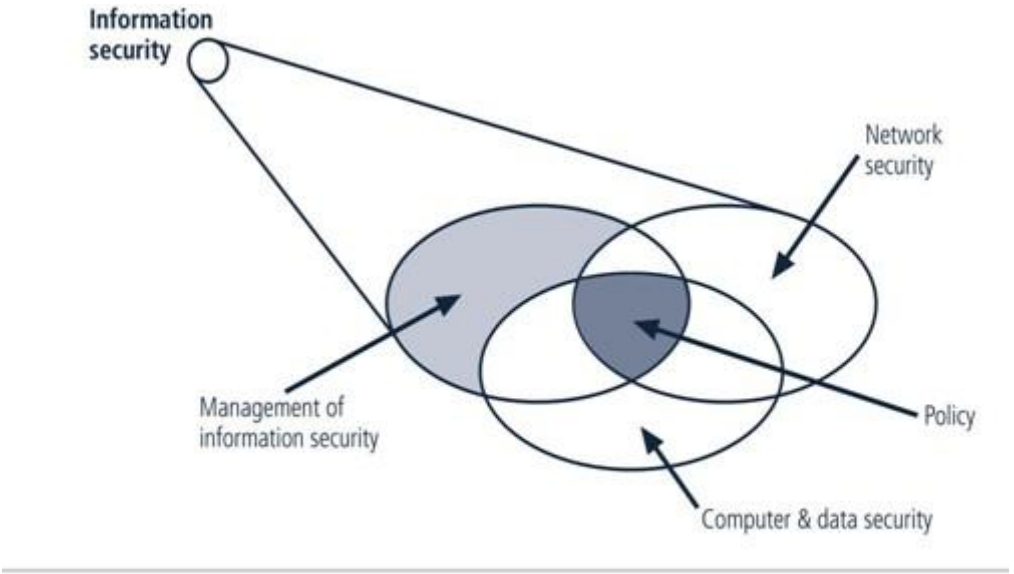


Figure 1.2.1.1 Components of Information Security

SECURING COMPONENTS

Protecting the components from potential misuse and abuse by unauthorized users.

- ✓ **Subject of an attack**

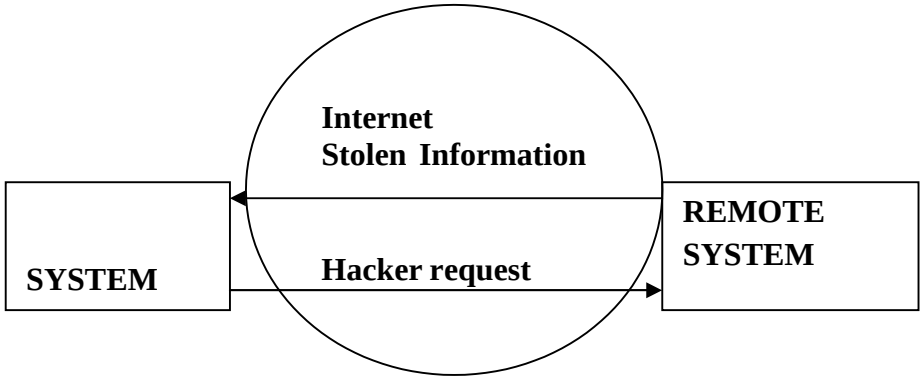
  Computer is used as an active tool to conduct the attack.

- ✓ **Object of an attack**

  Computer itself is the entity being attacked

Two types of attacks:

1. **Direct attack**
2. **Indirect attack**



Hacker using a computer as the subject of attack

Remote system that is the object of an attack

1. **Direct attack**

   When a Hacker uses his personal computer to break into a system.

2. **Indirect attack**

   When a system is compromised and used to attack other system.

THE SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

SDLC WaterfallMethodology

SDLC-is a methodology for the design and implementation of an information system in an organization.

- ✓ A methodology is a formal approach to solving a problem based on a structured sequence of procedures.
- ✓ SDLC consists of 6 phases.

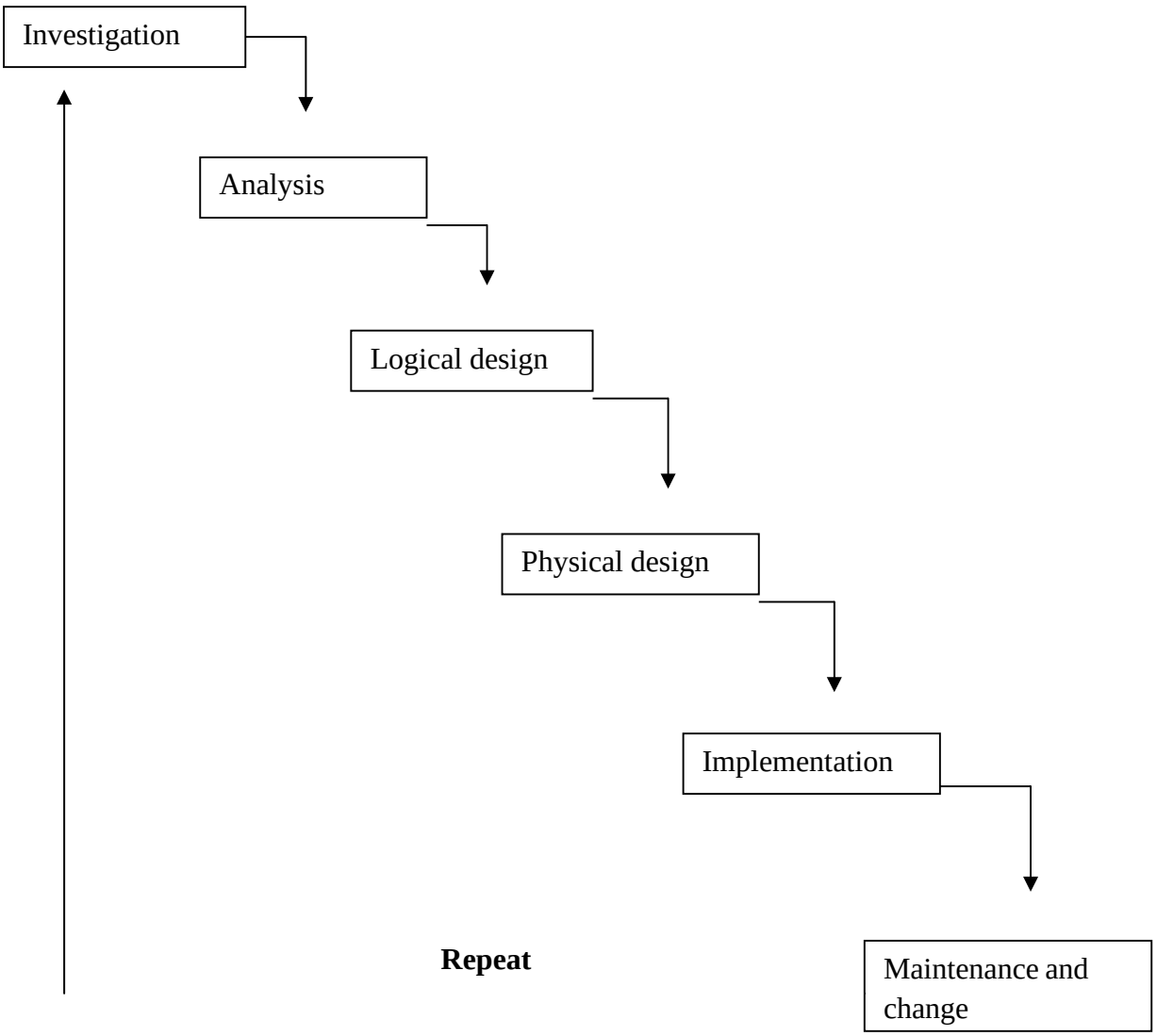


Figure 1.8.1 Systems Development Life Cycle

Investigation

- It is the most important phase and it begins with an examination of the event or planthat initiates the process.
- During this phase, the objectives, constraints, and scope of the project are specified.
- At the conclusion of this phase, a feasibility analysis is performed,

which assesses the economic, technical and behavioral feasibilities of the process and ensures that implementation is worth the organization's time and effort.

Analysis

- It begins with the information gained during the investigation phase.
- It consists of assessments (quality) of the organization, the status of current systems,and the capability to support the proposed systems.
- Analysts begin by determining what the new system is expected to do, and how it will interact with existing systems.
- This phase ends with the documentation of the findings and an update of the feasibility analysis.

Logical Design

- In this phase, the information gained from the analysis phase is used to begin creating a systems solution for a business problem.
- Based on the business need, applications are selected that are capable of providing needed services.
- Based on the applications needed, data support and structures capable of providing the needed inputs are then chosen.
- In this phase, analysts generate a number of alternative solutions, each with corresponding strengths and weaknesses, and costs and benefits.
- At the end of this phase, another feasibility analysis is performed.

Physical design

- In this phase, specific technologies are selected to support the solutions developed inthe logical design.
- The selected components are evaluated based on a make-or-buy decision.
- Final designs integrate various components and technologies.

Implementation

- In this phase, any needed software is created.
- Components are ordered, received and tested.
- Afterwards, users are trained and supporting documentation created.
- Once all the components are tested individually, they are installed and tested as asystem.
- Again a feasibility analysis is prepared, and the sponsors are then presented with thesystem for a performance review and acceptance test.

Maintenance and change

- It is the longest and most expensive phase of the process.
- It consists of the tasks necessary to support and modify the system for the remainder ofits useful life cycle.
- Periodically, the system is tested for compliance, with business needs.
- Upgrades, updates, and patches are managed.
- As the needs of the organization change, the systems that support the organization mustalso change.
- When a current system can no longer support the organization, the project is terminatedand a new project is implemented.

Advantages of Information Security

- Easy To Use
- Update Technology
- More Security
- it keeps top secret information
- User Friendly

Disadvantages of Information Security

- Technolgoy is always changing Time To Time
- Not completely secure.
- It can be extremely complex
- It can slow down productivity if a user is constantly having to enter passwords.

- Strict Regulations
- Difficult to work with for non-technical users

Application of Information Security

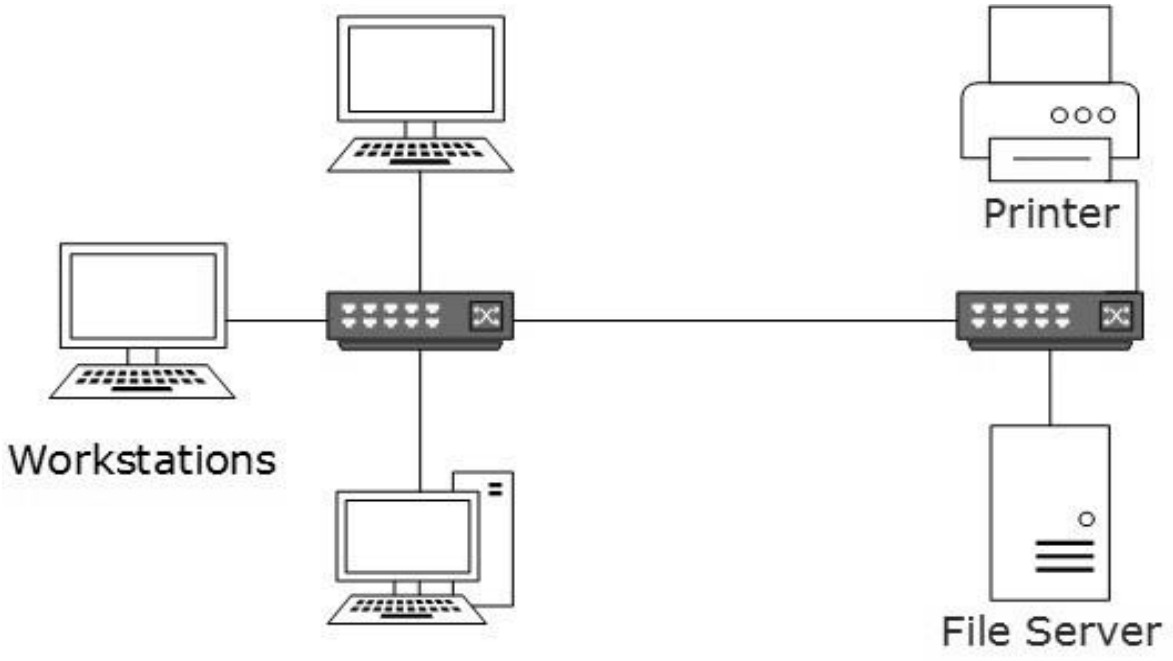
1. Cryptography
2. Mobile computing
3. Social media
4. Networks information
5. Financial information
6. Corporate information
7. Infrastructure information

UNIT 1

Types of Network based on size

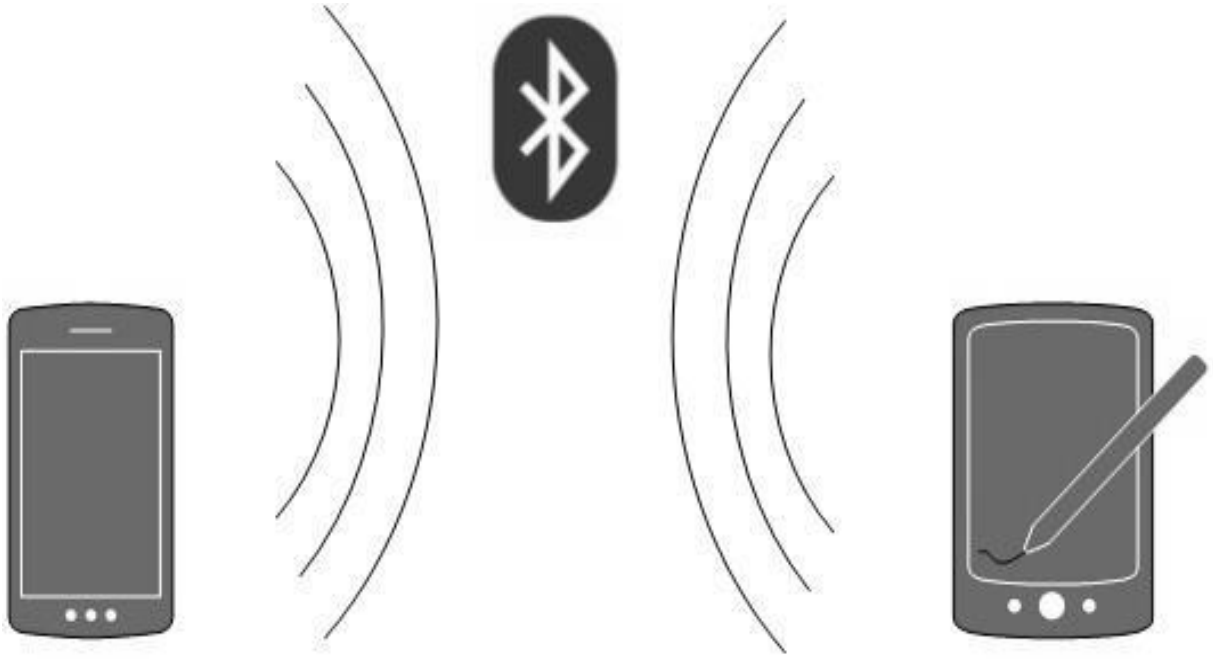
Local Area Network

A computer network spanned inside a building and operated under single administrative system is generally termed as Local Area Network (LAN). LAN covers an organization offices, schools, colleges or universities
Group of interconnected computers within a small area. (room, building, campus) Two or more pc's can from a LAN to share files, folders, printers, applications and other devices. Due to short distances, errors and noise are minimum. Data transfer rate is 10 to 100 mbps. Example: A computer lab in a school.



Personal Area Network

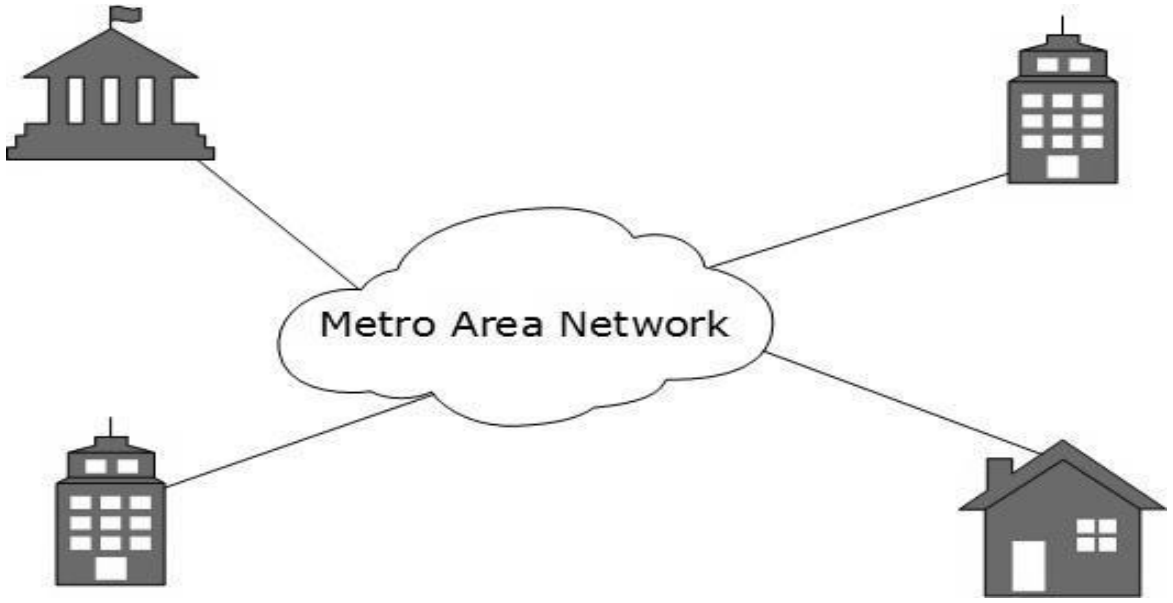
A Personal Area Network (PAN) is smallest network which is very personal to a user. PAN has connectivity range up to 10 meters. Network organized by the individual user for its personal use.



Metropolitan AreaNetwork

The Metropolitan Area Network (MAN) generally expands throughout a city such as cable TV network. For example, MAN can help an organization to connect all of its offices in a city.

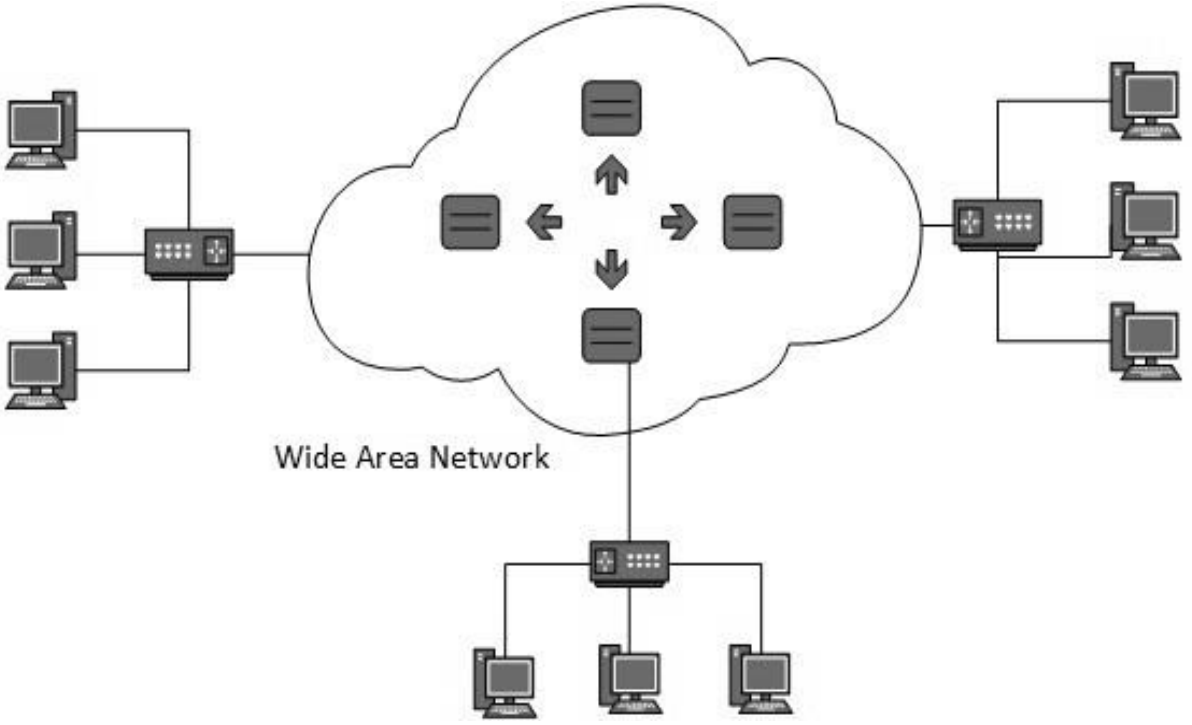
Design to extend over a large area. Connecting number of LAN's to form larger network, so that resources can be shared. Networks can be up to 5 to 50 km. Owned by organization or individual. Data transfer rate is low compare to LAN. Example: Organization with different branches located in the city



Wide AreaNetwork

Wide Area Network (WAN) covers a wide area which may span across provinces

and even a whole country. Generally, telecommunication networks are Wide Area Network.



Simplex

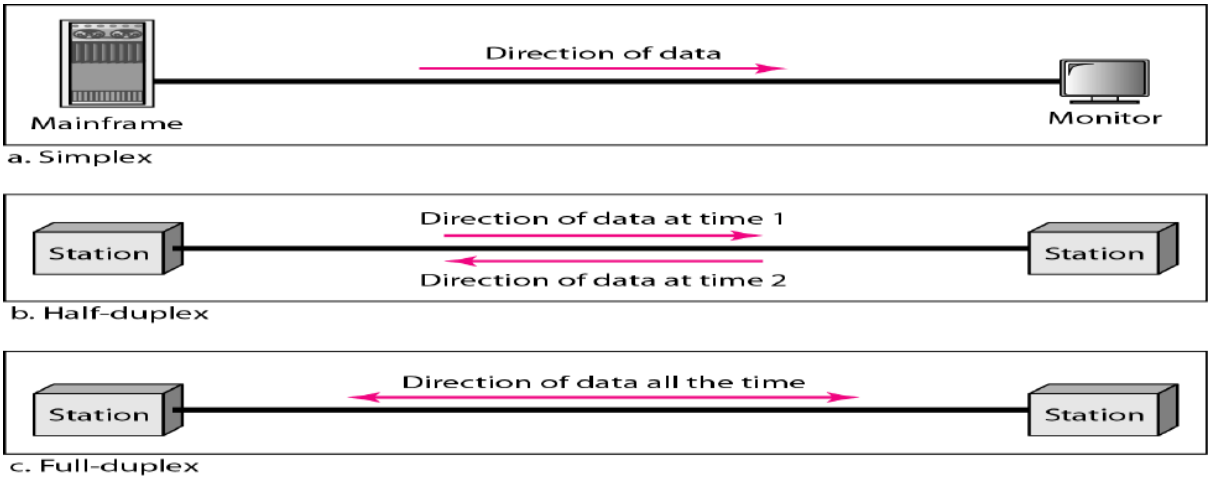
In simplex mode, the communication is unidirectional, as on a one- way street. Keyboards are examples of simplex devices.

Half-Duplex

In half-duplex mode, each station can both transmit and receive, but not at the same time. Walkie-talkies half- duplex systems.

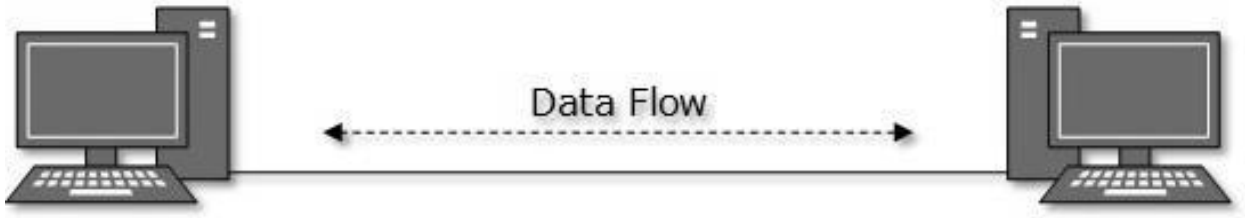
Full-Duplex

In full- duplex, both stations can transmit and receive simultaneously (Figure c). The full-duplex mode is used when communication in both directions is required all the time.



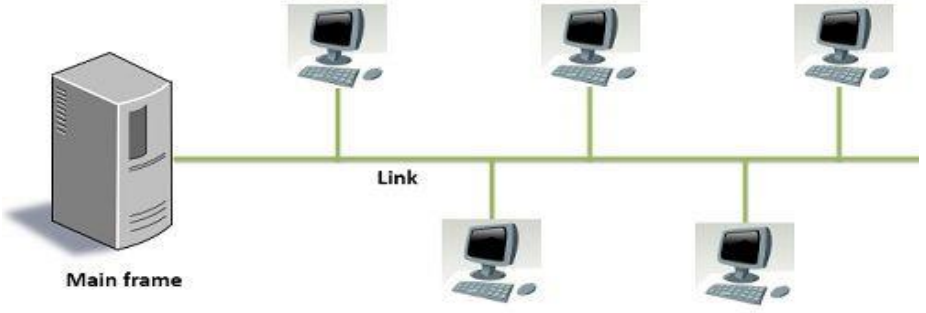
Point-to-Point

A point-to-point connection provides a dedicated link between two devices.



Multipoint

A multipoint connection is one in which more than two specific devices share a single link**. Bus Topology** is a common example of **Multipoint Topology.**



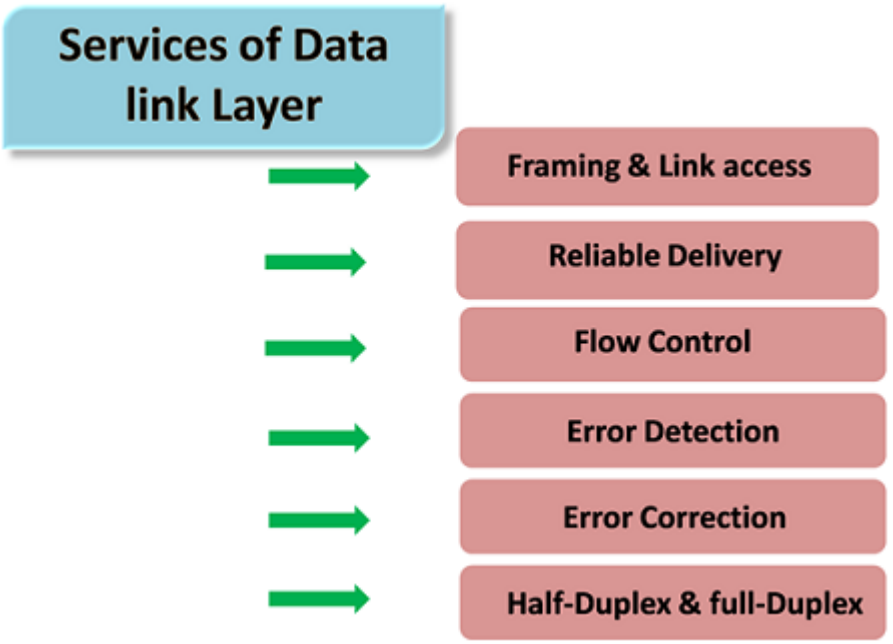
Multipoint Connection

Medium Access Control (MAC) in Wireless Network

Data Link Layer

Data link layer in the OSI (Open System Interconnections) Model, is in between the physical layer and the network layer. Error controlling is easily done Error detection bits are used by the data link layer. It also corrects the errors.

- Data link layer is a 2nd layer from the bottom. The main responsibility of the Data Link Layer is to transfer the datagram across an individual link. The Data link layer protocol defines the format of the packet exchanged across the nodes as well as the actions such as Error detection, retransmission, flow control, and random access. The Data Link Layer protocols are Ethernet, token ring, FDDI and PPP.



Framing & Link access

The stream of bits from the physical layer are divided into data frames whose size ranges from a few hundred to a few thousand bytes. Data Link Layer protocols encapsulate each network frame within a Link layer frame before the transmission across the link.

Reliable delivery

Data Link Layer provides a reliable delivery service, i.e., transmits the network layer datagram without any error. A reliable delivery service is accomplished with transmissions and acknowledgements.

Flow control

Flow control techniques, data is transmitted in such a way so that a fast sender does not drown a slow receiver.

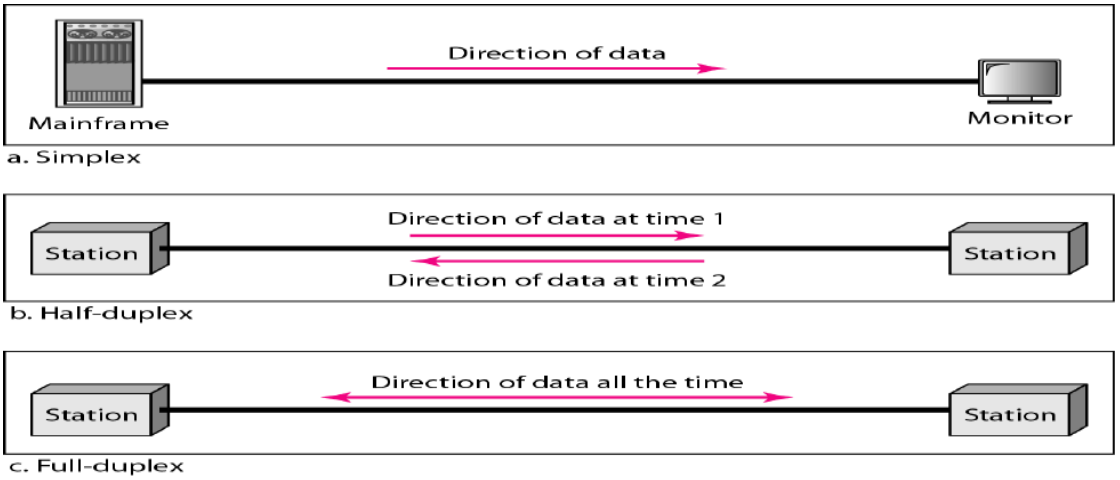
Error detection

Errors can be introduced by signal attenuation and noise. Data Link Layer protocol provides a mechanism to detect one or more errors.

Error correction

Error correction is similar to the Error detection, except that receiving node not only detect the errors but also determine where the errors have occurred in the frame.

Half-Duplex & Full-Duplex



In a Full-Duplex mode, both the nodes can transmit the data at the same time. In a Half-Duplex mode, only one node can transmit the data at the same time.

Goal of Data Link Layer

Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware.

Data link layer has two sub-layers:

Logical Link Control (LLC)

It deals with protocols, flow-control, and error control. the intermediary between the physical link and all higher layer protocols

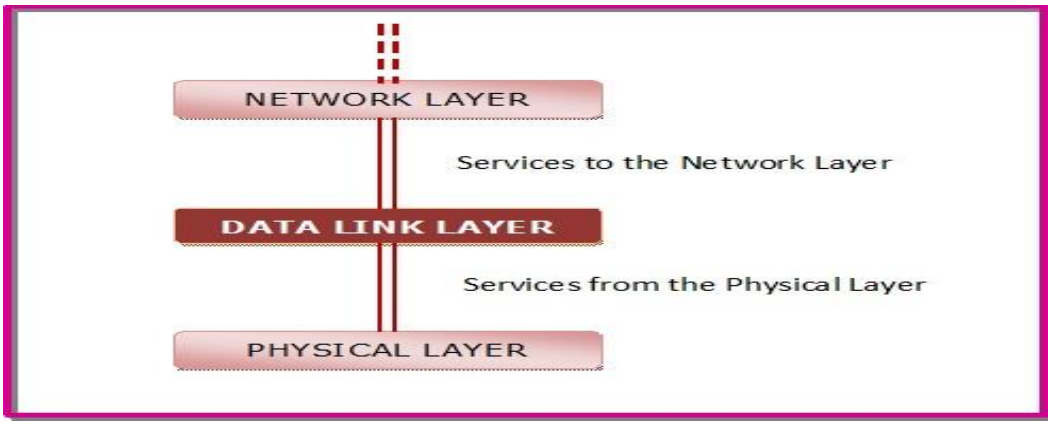
Media Access Control (MAC) or Medium Access Control

It deals with actual control of media. MAC sublayer controls access to the physical medium, serving as mediator if multiple devices are competing for the same physical link.

Design issues of DLL

- Flow Control
- Error Control
- Framing
- Providing services to the network layer
-

Services provided to the Network layer

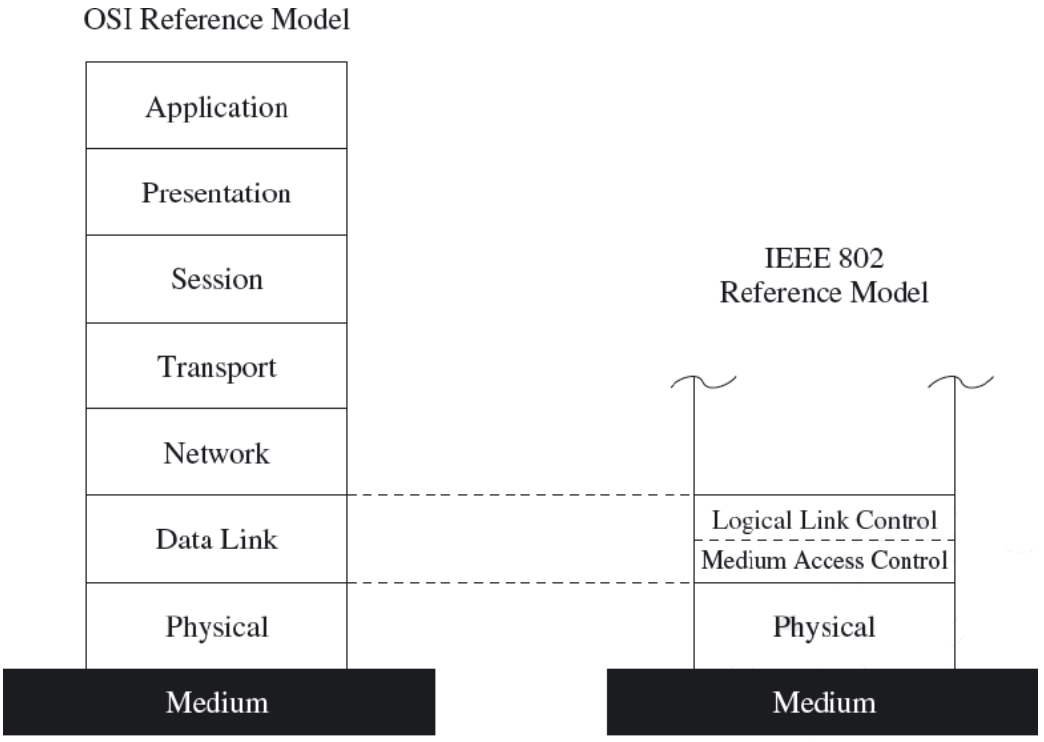


MAC layer Include

1. resolve any potential conflicts between competing nodes
2. correct communication errors occurring at the physical layer

3. perform other activities such as framing, addressing, and flow control

Second layer of the OSI reference model (data link layer) or the IEEE 802 reference model (which divides data link layer into logical link control and medium access control layer)

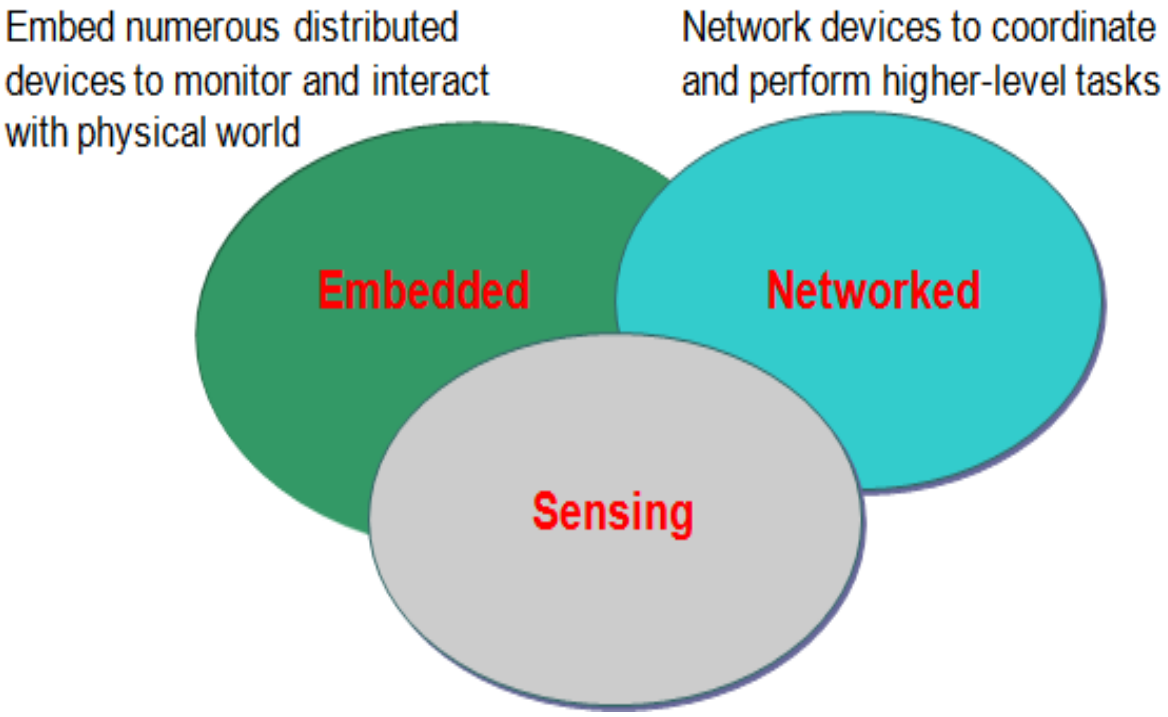


Enabling Technologies for WSN Used

1. **Zigbee**
2. **Bluetooth Technology**

Enabling Technologies for WSN

Building such wireless sensor networks has only become possible with some



fundamental advances in enabling technologies

1. Cost Reduction
2. Wireless Networking
3. Energy Saving

Zigbee

1. Zigbee technology addresses needs of industrial measurement and control (automation)
2. Zigbee Alliance is consortium of 150+ companies
3. Includes Honeywell, Motorola, Phillips, Samsung, Mitsubishi
4. IEEE 802.15.4 is "**Low-Rate Wireless PAN Standard**"
5. Zigbee Alliance promotes **IEEE 802.15.4 standard**
6. IEEE 802.15.4 defines only Physical and MAC layers
7. Not attractive for business communication networks because

of low data rate

Standard recognizes 2 types of devices

a. Full-Function Device (FFD)

- Can also function as a normal device

b. Reduced-Function Device (RFD)

- Simpler in design than FFD
- Can't function as Network Coordinator

ZigBee supports three types of topologies

1) Star Topology,

2) Tree

Bluetooth

1. Bluetooth is the most successful WPAN technology commercially available

2. Frequency range from 2402 to 2480 MHz(2.4GHz).

3. A typical Bluetooth device has a range of about 10 meters.

4. A Bluetooth PAN is also called a **piconet** and is composed ofup to 8 active devices in a master-slave relationship.

5. The first Bluetooth device in the piconet is the master, and allother devices are slaves that communicate with the master.

Bluetooth Usage

a. File transfer

b. Internet bridge

c. LAN access

d. Synchronization

e. Three-in-one phone

f. Heads

Routing in WSNs

Sending the data between Sensor Node (SA) and Base Station (BS).

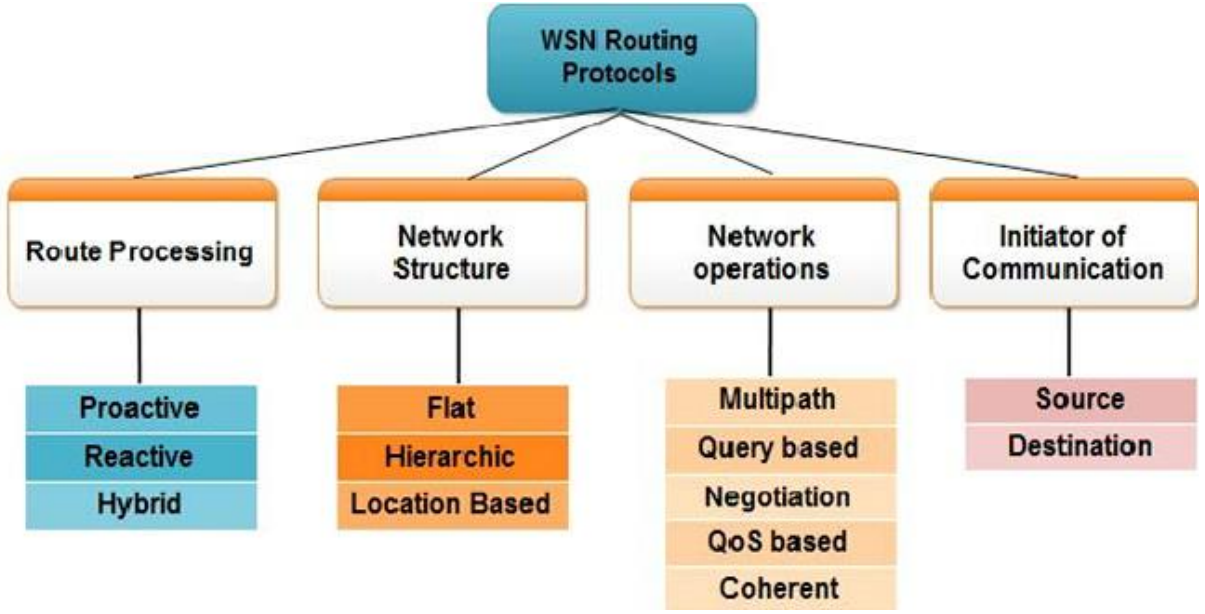
Different routing protocols that have been developed for secure sensor network and routing techniques used by the protocols to work.

Routing Challenges and Design Issues in WSN

1. limited Energy Supply
2. limited computing power
3. limited bandwidth of the wireless links connecting sensor nodes

The major requirements of a routing protocol

1. Minimum route acquisition delay
2. Quick route reconfiguration
3. Support for time-sensitive traffic
4. Security and privacy



Sensor

Sensor is a device used to gather information about a physical process and translate into electrical signals that can be processed, measured and analyzed.

A Sensor is a device that responds and detects some type of input from both the physical or environmental conditions, such as pressure, heat, light, etc.

Sensor Networks used

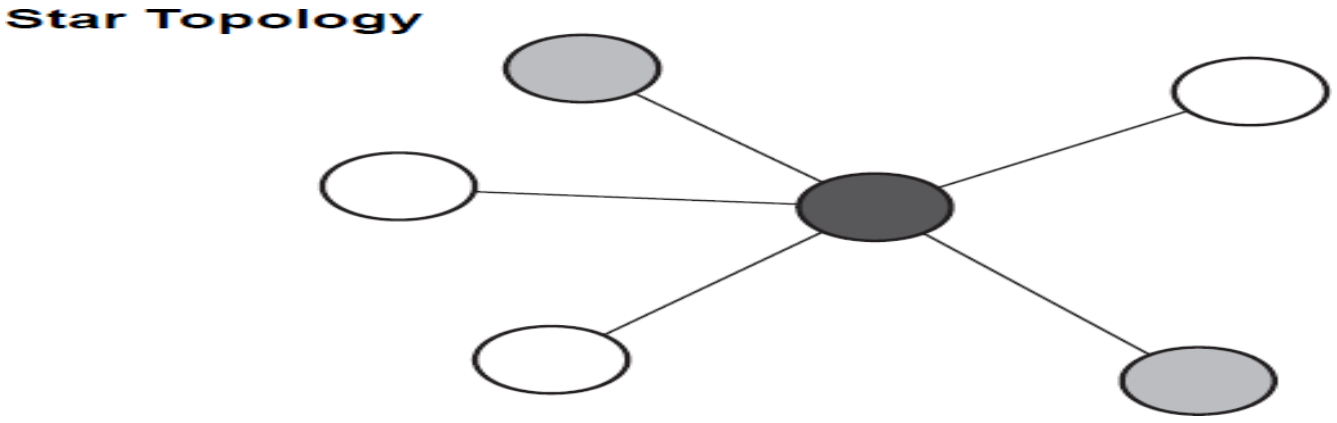
1. Remote sensing
2. Medical telemetry
3. Surveillance
4. Monitoring
5. Data collection

Sensor Network is composed of a large number of sensor nodes, which are tightly positioned either inside the phenomenon or very close to it.

Topology Management in Wireless Sensor Network

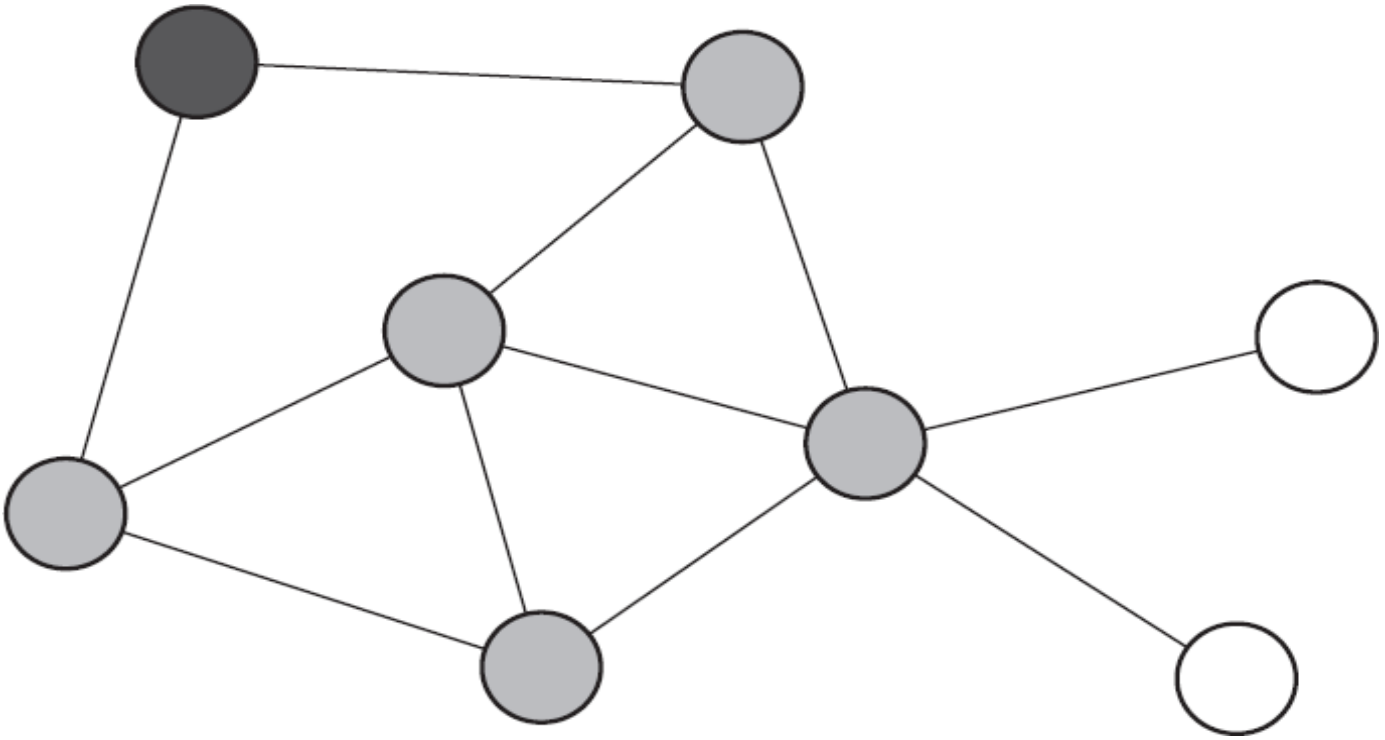
Star Topology

In the star topology, communication is established between devices and a single central controller, called the PAN coordinator



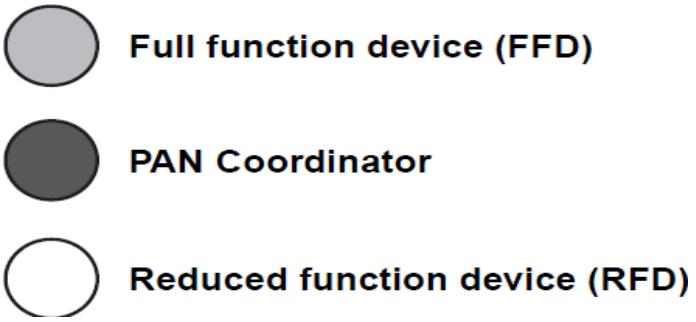
Peer-to-peer Topology

Peer-to-peer Topology peer-to-peer topology any device can communicatewith any other device as long as they are in range of one another.



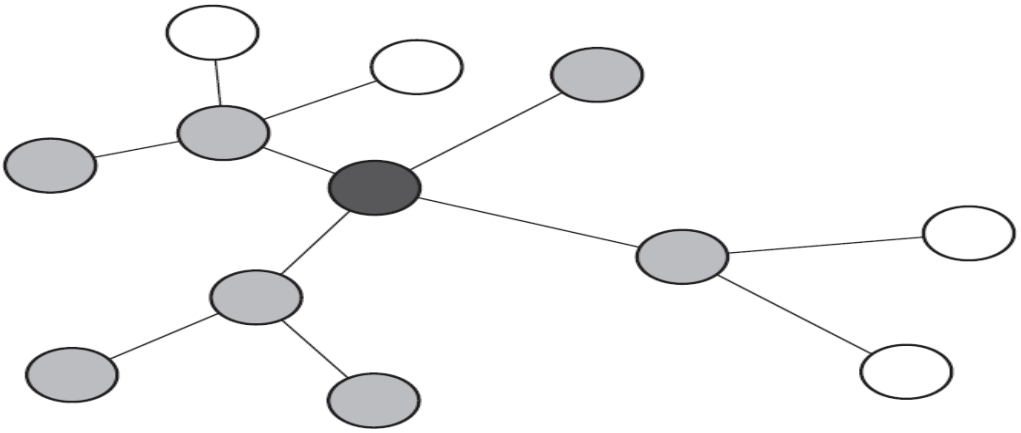
1. A peer-to-peer network can be ad hoc, self-organizing, and self-healing.

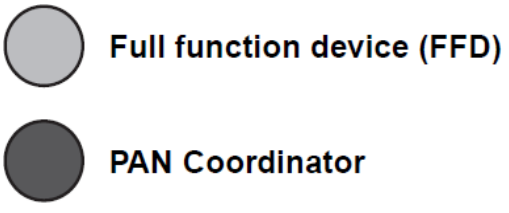
2. It can provide reliability by multipath routing



Cluster-treeTopology

The cluster-tree topology is a special case of a peer-to-peer network in which most devices are full-function devices and an RFD may connect to a cluster-tree network as a leaf node at the end of a branch





Cluster tree topology is a special case of tree topology in which a parent with its children is called a cluster. Each cluster is identified by a cluster ID.

Wireless Sensor, Coverage & Placement

wireless sensor is a device that can gather sensory information and detect changes in local environments.

wireless sensor network contains many thousands of sensor nodes

Mobile WSNs

Mobile wireless sensor network (MWSN) can simply be defined as a wireless sensor network (WSN) in which the sensor nodes are mobile.MWSNs are much more versatile than static sensor networks as they can be deployed in any scenario and cope with rapid topology changes

MWSNs generally use the many-to-one communication style, in which data is gathered from the sensors and sent to the sink.

MANETs are mobile ad hoc networks are general purpose mobile networks, in which each node is required to be able to communicate with any other node in the network. The nodes are often considered to be personal computers that are able to enter the network and leave whenever they want. This requires MANETs to provide methods of allowing any two nodes to communicate over a changing topology, with a dynamic number of nodes.

WiMAX

1. WiMAX- **World Interoperability for MicroAccess**
2. WiMAX is a family of technologies based on **IEEE 802.16 standards**
3. WiMAX networks are designed for high-speed data
4. It provides very high speed wide area Internet access in a low-cost, flexible way
5. This uses licensed worldwide spectrum -2.3 GHz, 2.5 GHz, 3.3 GHz, and 3.5 GHz frequency bands
6. WiMAX can serve as a backbone for 802.11 hotspots for connecting to the Internet.

7. Also users can connect mobile devices such as laptops and handsets directly to WiMAX base stations without using 802.11.

8. WiMAX Technology can also provide fast and cheap broadband access to markets that lack infrastructure (fiber optics or copper wire)

9. There is no uniform global licensed spectrum for WiMAX

10. The most likely bands used will be around 3.5 GHz, 2.3/2.5 GHz, or 5 GHz

11. Mobile WiMAX based on the 802.16e standard will most likely be in 2.3 GHz and 2.5 GHz frequencies

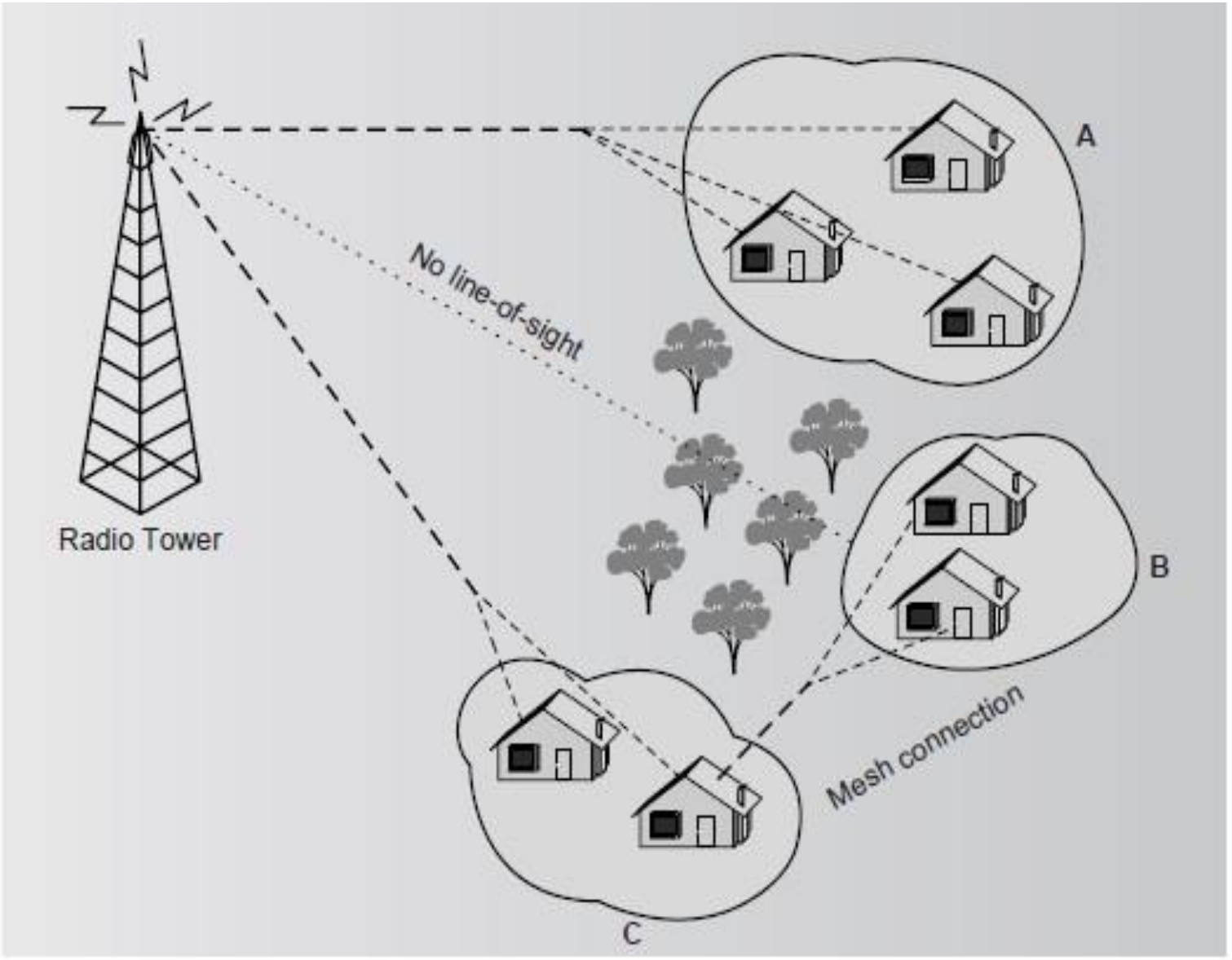
12. WiMAX can serve as a backbone for 802.11 hotspots for connecting to the Internet.

13. Also users can connect mobile devices such as laptops and handsets directly to WiMAX base stations without using 802.11.

14. WiMAX Technology can also provide fast and cheap broadband access to markets that lack infrastructure (fiber optics or copper wire)

Features WiMAX

1. **Scalability**
2. **High data rates**
3. **Quality of service (QoS)**
4. **Mobility**
5. **Security**



1. Fixed WIMAX (IEEE 802.16d — 2004)
2. Mobile WIMAX (IEEE 802.16e — 2005)

Fixed WiMAX is a point-to- multipoint technology, where the base station is fixed.
Mobile WiMAX is a multipoint-to-multipoint technology.

Standards for the Data Link Layer

ISO:	HDLC (High Level Data Link Control)
IEEE:	802.2 (LLC), 802.3 (Ethernet) 802.5 (Token Ring) 802.11(Wireless LAN)
ITU:	Q.922 (Frame Relay Standard) Q.921 (ISDN Data Link Standard) HDLC (High Level Data Link Control)
ANSI:	3T9.5 ADCCP (Advanced Data Communications Control Protocol)

WiFi

1. WiFi means **Wireless Fidelity** (Technology/Protocol)
2. WiFi provides wireless internet access in neighbourhood
3. IEEE 802.11 is "**Wireless LAN Standard**"
4. WiFi Alliance (formed in 1999) promotes IEEE 802.11 standard
5. Earlier called "Wireless Ethernet Compatibility Alliance"
6. It Certifies 802.11 products for interoperability

- IEEE 802.11-1997 (original)
- IEEE 802.11a-1999
- IEEE 802.11b-1999
- IEEE 802.11g-2002

Two modes of operation

1. **Point Coordination Function (PCF) mode**
    - managed mode

2. **Distributed Coordination Function (DCF) mode**
    - ad-hoc mode

Flooding

Flooding is simplest method packet forwarding. When a packet is received, the routers send it to all the interfaces except the one on which it was received.

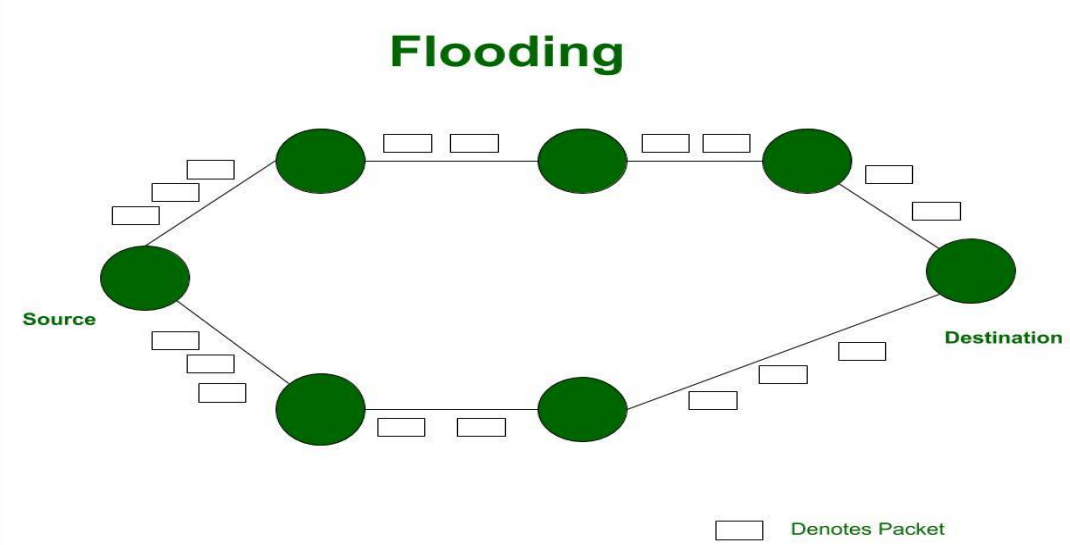
In flooding, each sensor receiving a data packet broadcasts it to all of its neighbors and this process continues until the packet arrives at the destination or the maximum number of hops for the packet is reached

Advantages of Flooding

1. Highly Robust
2. Flooding always chooses the shortest path
3. Broadcast messages to all the nodes

Drawbacks of Flooding

1. Overlap
2. Implosion
3. Resource blindness



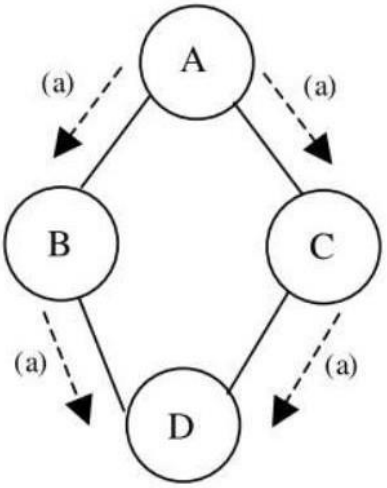


Fig. 1. The implosion problem. Node A starts by flooding its data to all of its neighbors. D gets two same copies of data eventually, which is not necessary.

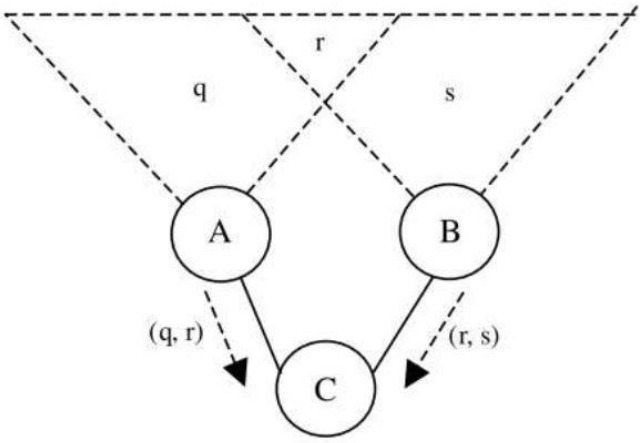


Fig. 2. The overlap problem. Two sensors cover an overlapping geographic region and C gets same copy of data form these sensors.

Gossiping

1. Gossiping is a slightly enhanced version of flooding where the receiving node sends the packet to a randomly selected neighbor, which picks another random neighbor to forward the packet to and so on.

2. Gossiping avoids the implosion problem by limiting the number of packets that each node sends to its neighbor to one copy.

3. The latency that a packet suffers on its way to the destination may be excessive, particularly in a large network.

Drawbacks

- Transmission delay

Advantage

- Avoid the implosion

Short Messaging Service

1. SMS is defined in the supplementary services of GSM

2. It can be alphanumeric messages of up to 160 characters (140 bytes).

3. It operates by making use of the existing GSM infrastructure in addition with a SMS Center(SMSC).

4. The physical layer, and the logical channels of the GSM system is used to transmit the short messages

5. SMS has both an instant delivery service if the destination MS is active or it can be stored and forwarded if the MS is inactive

Two types of services

1. Cell Broadcast - the message is transmitted to all MSs that are active in a cell.
2. PTP- Peer-to-Peer – MS sending a message to another MS

There are four layers in SMS

1. **The application layer (AL)-** can generate and display the alphanumeric message

2. **The transfer layer (TL)** - exchange SMs and receive confirmation of receipt of SMs. It can obtain a delivery report or status of the SM sent in either direction

3. **The relay layer (RL)** - relays the SMS through the LL.

4. **The link layer (LL) –** Manages the routing process

HIPERLAN

1. HIPERLAN -**High Performance Radio Local Area Network**

2. It is a European alternative for the IEEE 802.11 standards.

3. The goal of the HiperLAN was to have data rate higher than 802.11

HIPERLAN Family

1. HiperLAN/1

2. HiperLAN/2

3. HiperLAN/3- HIPERACCESS – provides up to 100 Mbps in the 40.5–43.5 GHz band

4. HiperLAN/4- HIPERMAN – designed for a WMAN in 2 GHz and 11 GHz bands (155 Mbps)

Hiperlan/1

1. Range 50 m

2. HiperLAN/1 was planned in 1991 and implemented in 1997

HiperLAN/2

1. HIPERLAN/2 has many characteristics of IEEE 802.11 WLAN

2. HiperLAN/2 functional specification was accomplished Feb 2000

3. The physical layer of HiperLAN/2 is very similar to IEEE 802.11a wireless local area networks

Wireless Personal Area Networks (WPANs)

1. wireless PAN is based on the standard IEEE 802.15
2. The three kinds of wireless technologies used forWPAN are

1. Bluetooth,

2. Infrared Data Association

3. Wi-Fi

3.The operating frequencies are around 2.4 GHz

Unit -2

Wireless Sensor Networks

Sensor is a device used to gather information about a physical process and translate into electrical signals thatcan be processed, measured and analyzed

1. Sensor networks have emerged as a promising tool for monitoring the physical world, that can sense, process and communicate.

2. WSN is a special kind of ad-hoc network that consists of large no. of wireless sensor nodes.

3. WSN is a group of low-power, low-cost, multifunctional and small size wireless sensor nodes

WSN Applications

1. Environmental monitoring
2. Health care
3. Disaster Mitigation
4. Industrial applications
5. Security and safety applications
6. Military Applications

Important Issues

1. Coverage

2. Connectivity

3. Power management

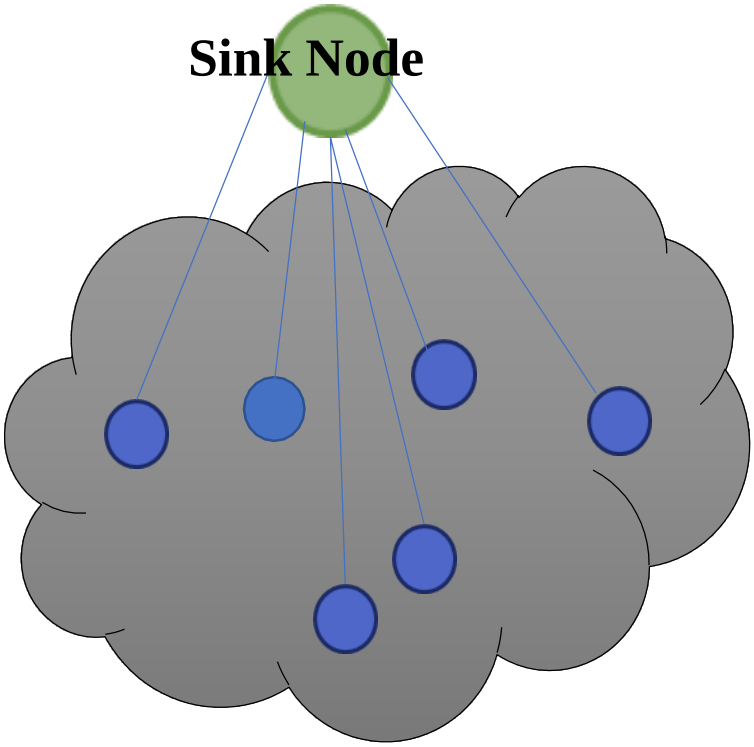
4. Self-deployment

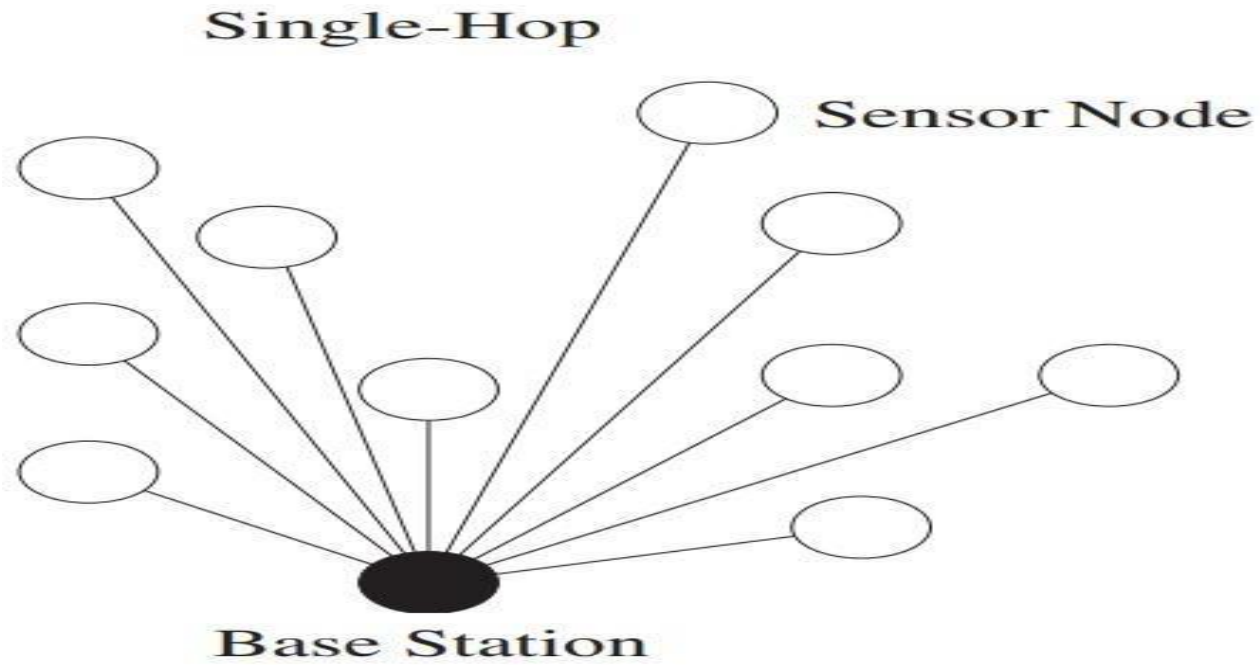
5. Security

Need of WSNs

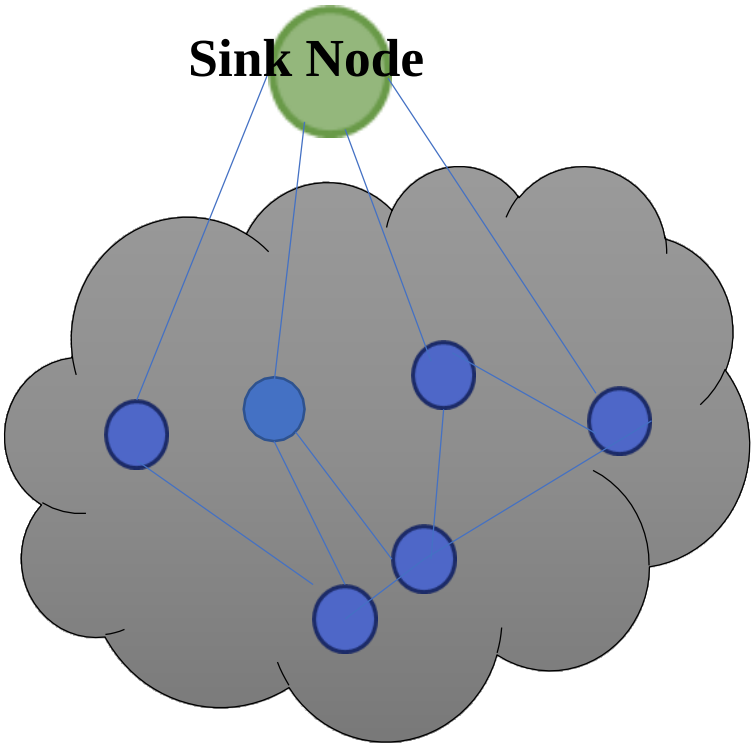
1. Sensor at inaccessible or difficult-to-access locations
2. Sensors are mobile or nomadic
3. Quick deployment
4. Ad-hoc networking

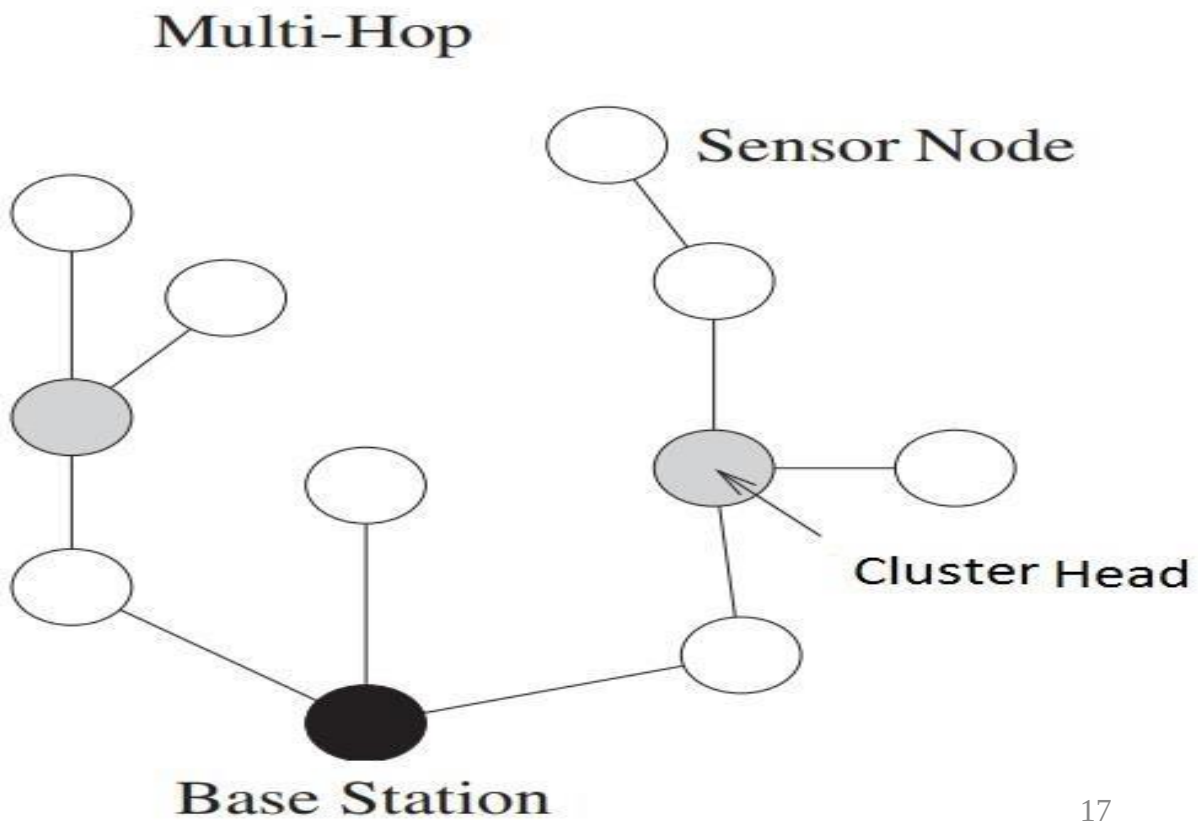
Single–hop network





Multi–hop network

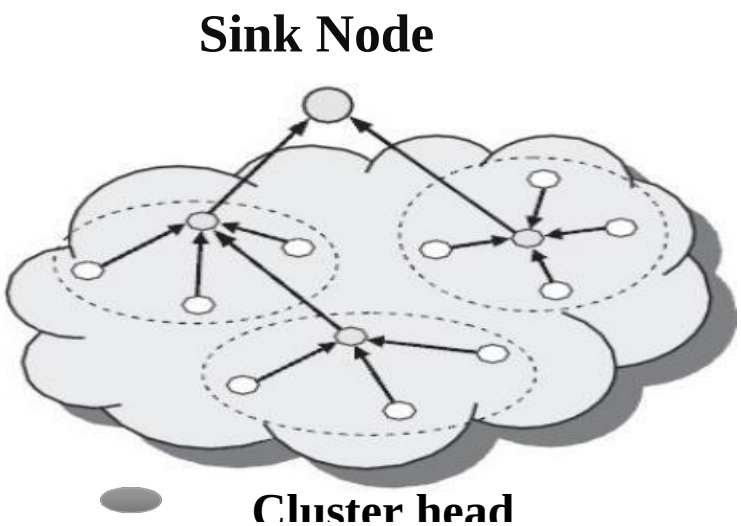


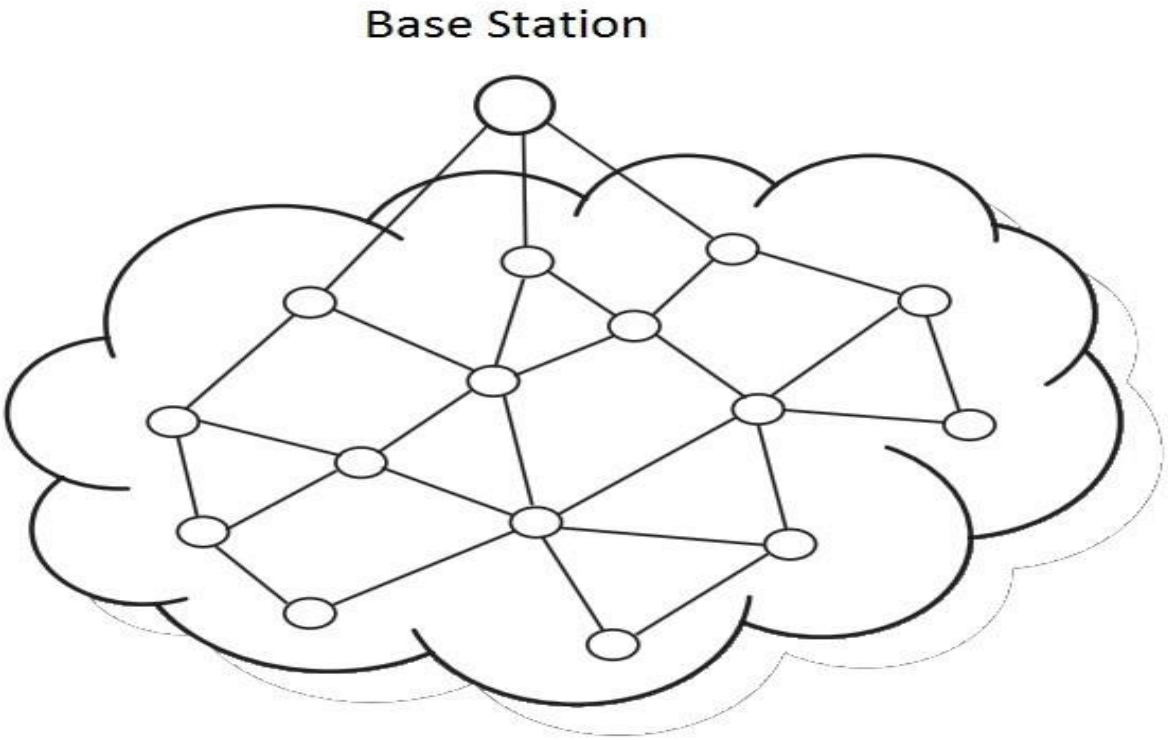


Hierarchical Architecture

1. Single-hop clustering architecture
2. Multiple-hop clustering architecture

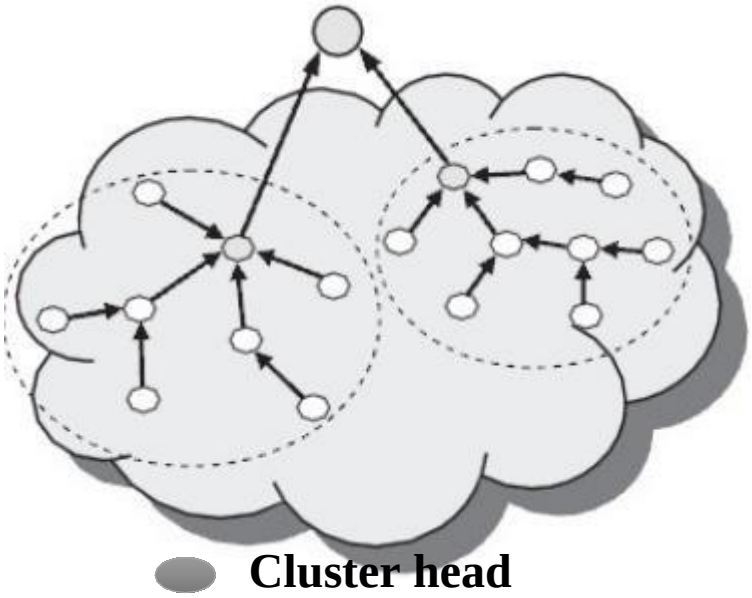
Single-hop clustering architecture

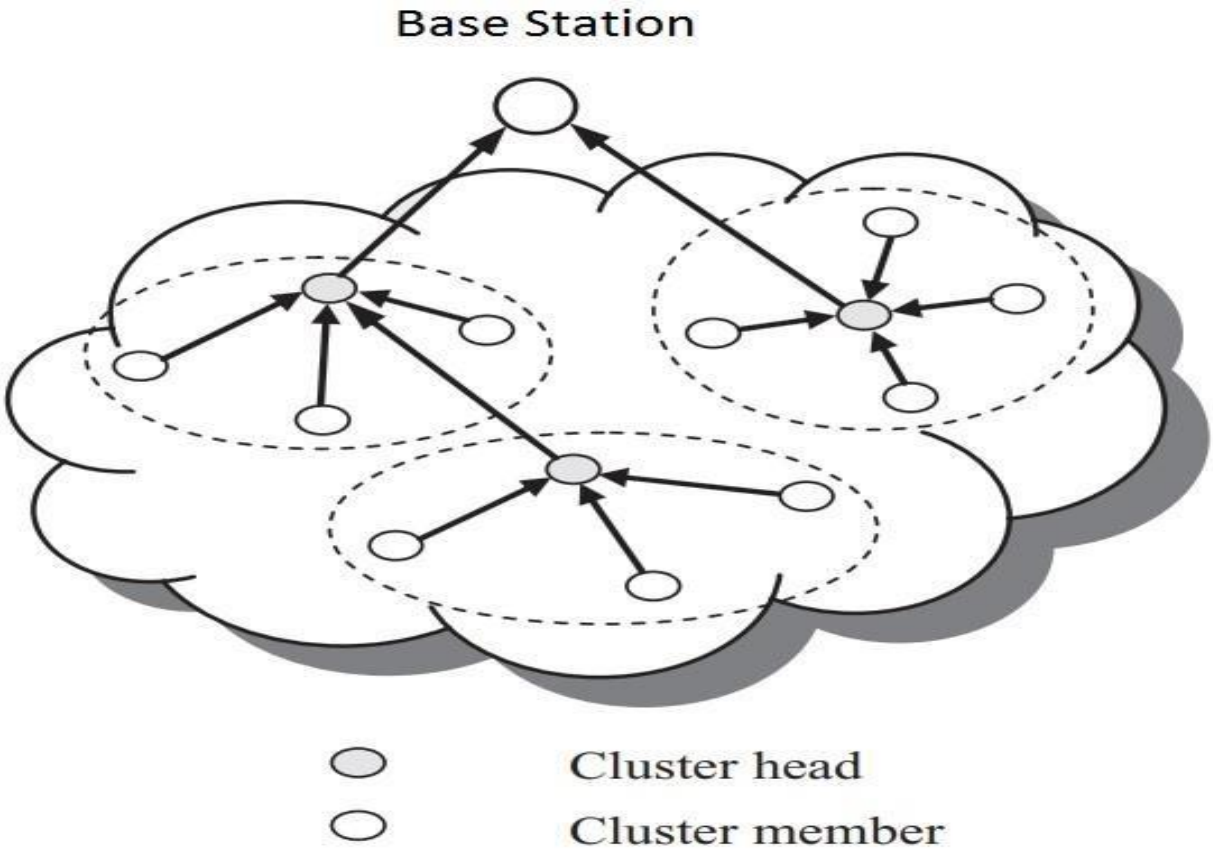




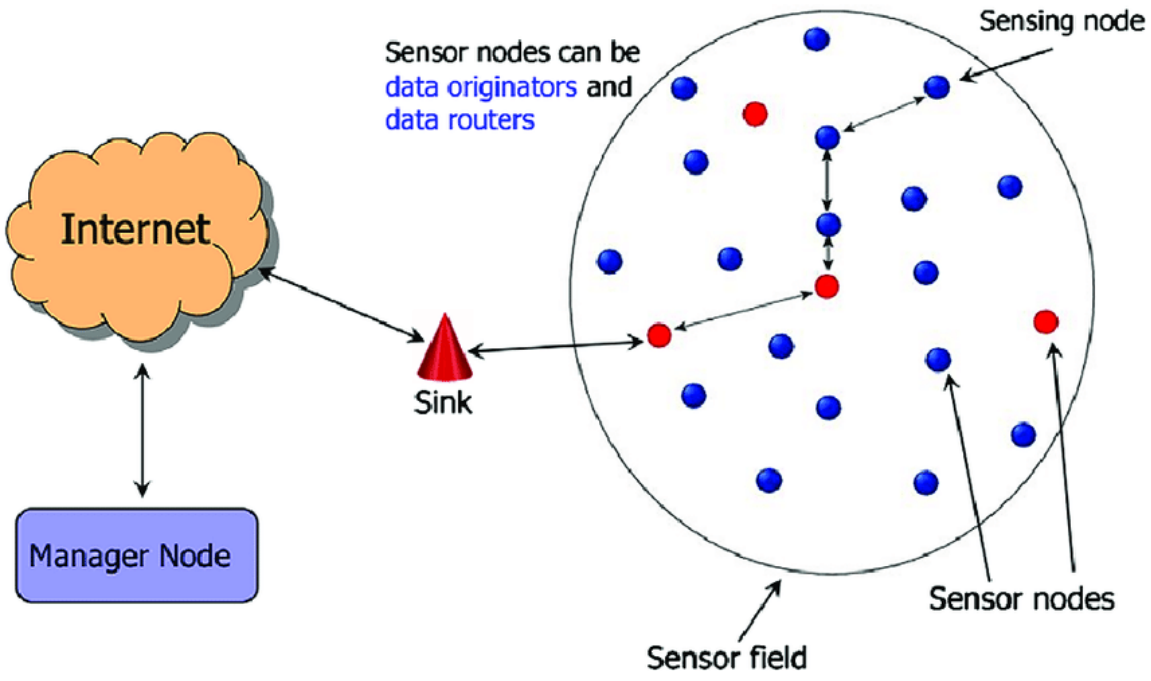
Multi-hop clustering architecture

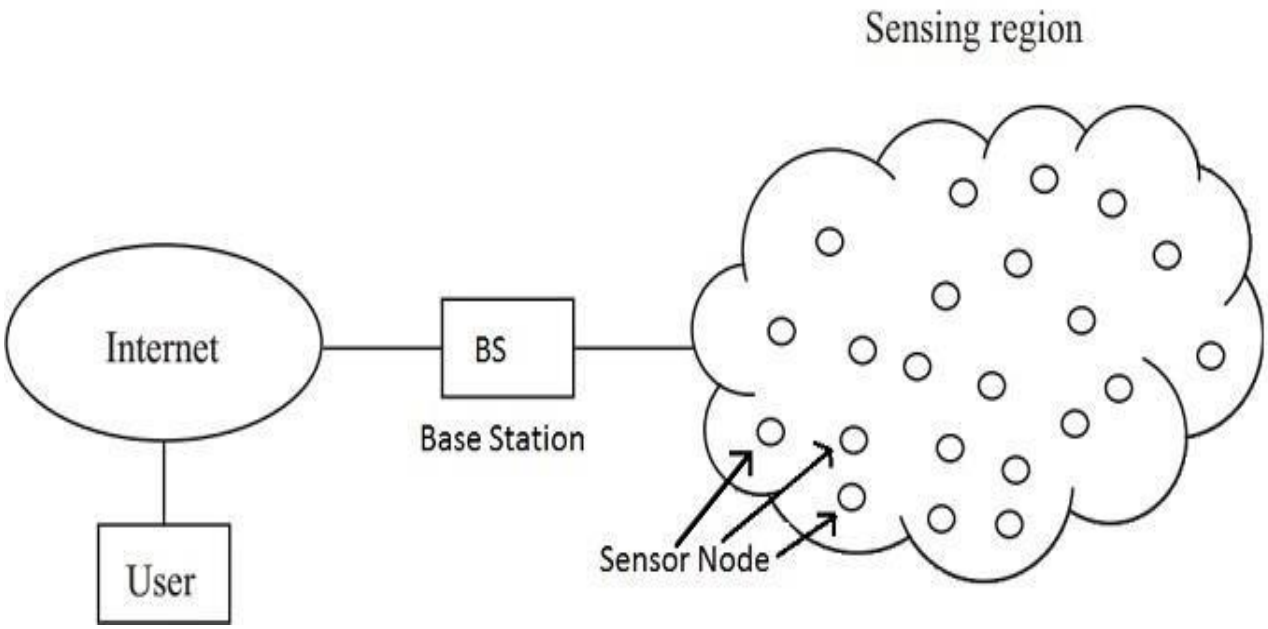
Multi-hop network architecture is usually used. Instead of one single link between the sensor node andthe base station, the data is transmitted through oneor more intermediate node**.**


Sink Node
Cluster head


Base Station
Cluster head
Cluster member

Wireless Sensor Network Architecture





Main Constraints of WSNs:

1. Limited sensing and communication range
2. Limited battery capacity
3. Limited processing

Challenges in WSN

1. Fault Performance
2. Scalability
3. Production Cost
4. Operation Environment
5. Quality of Service
6. Data Aggregation
7. Data Compression
8. Data Latency

Advantages in Wireless Sensors

1. Much cheaper to deploy than wired sensors
2. Sensor nodes can be added or removed easily
3. Node location can be changed without rewiring
4. Can be configured into different network topologies

Special Features of Wireless Sensors

1. Large number, high density deployment
2. Channels are unreliable
3. Ad-hoc transmission mode
4. Less predefined deployment
5. Vulnerable to environmental damages

Purpose of UTM

1. It Known as a Next-Generation Firewall (NGFW).
2. Provide Multiple Security Features into a single device.
3. UTM is also used by service providers for spam email detection, intrusions, filtering traffic, managing devices on the network.

UTM brands (Product) are

- Cisco
- Fortinet
- Sophos
- Netgear
- Huawei
- SonicWall

Examples (Features) of Unified threat management

- Antivirus software
- Firewalls
- Spam Email Detection
- Intrusion Detection
- Leak Prevention
- Anti-Malware
- Virtual Private Network(VPN)

Firewall

1. Network Security Device
2. Prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks.
3. A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.
4. Firewalls prevent unauthorized access to networks through software or firmware.

"System which analyzes the filters incoming or outgoing data packet based on pre defined rules".

1. **Hardware Firewall-**Example Broadband Router
2. **Software Firewall-** Called System Firewall

Types of Firewalls

1. Packet Filtering
2. Circuit-level gateways
3. Application Layer Firewalls
4. Cloud Firewall
5. Next-generation Firewalls (NGFW)