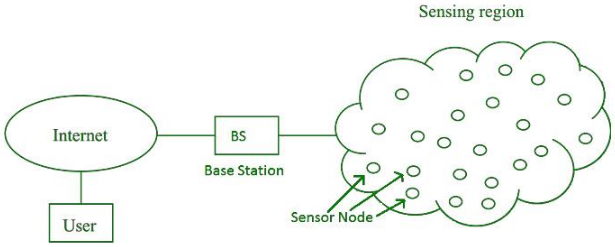
UNIT I INTRODUCTION

PART A

1. **What is a Wireless Sensor Network?**

Wireless Sensor Network (WSN) is an infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical or environmental conditions. WSN is also defined as collection of n no of tiny sensor to form a network through wireless medium.

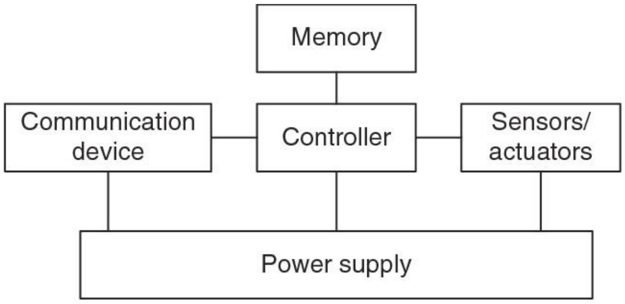


2. **Illustrate the characteristic requirements of a wireless sensor network.**

- Power consumption limitations for sensor nodes.
- Ability to cope with failures of nodes.
- Mobility of nodes.
- Heterogeneity of nodes.
- Homogeneity of nodes.
- Ability to deploy on a large scale.
- Capability to survive harsh environmental conditions.
- Helps to use easily.

3. **Name the hardware components of a Wireless sensor network.**

Wireless sensor networks, the 4 important hardware units are; a processing unit, a transceiver unit, sensing units and a power unit.



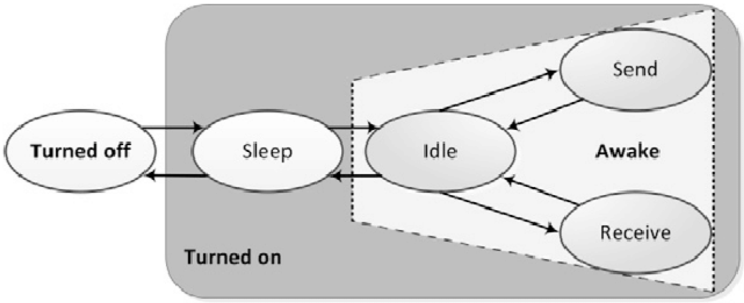
4. **What are the various operating modes of a transceiver?**

The transceiver can work in half-duplex or full-duplex mode: Half-duplex transceivers. It can either transmit or receive but not both at the same time. This is because both the transmitter and receiver are connected to the same antenna using an electronic switch.

5. **Define layered architecture**.

The layered architecture style is one of the most common architectural styles. The idea behind Layered Architecture is that modules or components with similar functionalities are organized into horizontal layers. As a result, each layer performs a specific role within the application.

6. **List various modes of a sensor node.**



7. **Comparison between Wireless Sensor Network and Ad-hoc.**

Wireless Sensor Network	Wireless ad-hoc networks
Utilize position information for routing	Uses global addressing scheme, IP-based routing.
Data moves towards sink node.	Source destination Pair changes constantly
Data is filtered or aggregated due to redundancy.	No need of aggregation
Rapid topological changes due to node mobility and failure.	Topological changes are not frequent

8. **What is a gateway?**

The gateways devices are used as protocol converter, command/data forwarder and also it can be used as Security Manager, Synchronizer in network. The Ethernet gateway has been designed to collect data from wireless sensor network and connect to the existing Ethernet network.

9. **Define clustered architecture.**

It is a computer working together as a single, integrated computing resource connected via high speed interconnects. A node – either a single or a multiprocessor network having memory, input and output functions and an operating system.

10. **Define ZigBee.**

“ZIGBEE” stands for a Zonal Intercommunication Global-standard, where Battery life is long, which is Economical to deploy, and which exhibits efficient use of resources. It is a standards-based wireless technology developed to enable low-cost, low-power wireless machine-to-machine (M2M) and internet of things (IoT) networks. It is for low-data rate, low-power applications and is an open standard.

11. **Examine how address centric network differ from with data centric network.**

Data-centric protocols differ from traditional address-centric protocols in the manner that the data is sent from source sensors to the sink. In address-centric protocols, each source sensor that has the appropriate data responds by sending its data to the sink independently of all other sensors.

12. **Summarize the Collaborative processing**.

    The Collaborative Process is an out-of-court conflict resolution process in which the participants focus their efforts on reaching a mutually acceptable resolution.

13. **Differentiate between active and passive sensors.**

    Active sensors have their own source of light or illumination. In particular, it actively sends a pulse and measures the backscatter reflected to the sensor. But passive sensors measure reflected sunlight emitted from the sun. When the sun shines, passive sensors measure this energy

14. **Outline the event detection approaches in WSN.**

    Event detection falls under three main categories:

    - Threshold Based
    - Supervised
    - Unsupervised.

15. **Interpret the term energy scavenging in Wireless Sensor Network.**

    Energy Harvesting-based WSNs (EHWSNs) are the result of endowing WSN nodes with the capability of extracting energy from the surrounding environment. Energy harvesting can exploit different sources of energy, such as solar power, wind, mechanical vibrations, temperature variations, magnetic fields, etc.

16. **Define self-organization of network**

    A self-organizing network (SON) is an automation technology designed to make the planning, configuration, management, optimization and healing of mobile radio access networks simpler and faster.

17. **Exhibit the performance metrics of wireless sensor network.**

    Wireless Sensor Network three performance metrics are: coverage, energy consumption and worst case delay.

18. **Associate the term aggregation with WSN.**

    In WSNs, data aggregation is a process of collecting and combining the useful information in a particular region of interest. The effectiveness of the communication among nodes depends on the data aggregation technique being used.

19. **Formulate the types of mobility of a sensor node in a network**

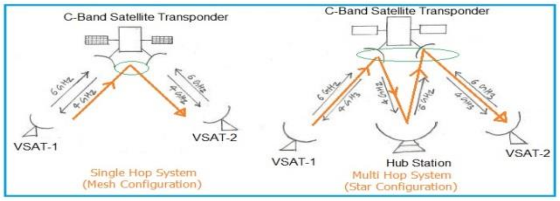
    We can distinguish three different kinds of mobility in WSNs:

    (i) Mobility of the sensor nodes;
    (ii) Mobility of the sink node and
    (iii) Mobility of a monitored event/object.

    The first kind of mobility occurs when at least part of the sensor nodes is mobile.

20. **Compare Single Hop with Multiple Hops.**

    When packet travels from source to destination using single networking device, it is known as single hop system. When packet travels from source to destination using more than one networking devices, it is known as multi hop system.



PART B & C

1. **What are the various applications of wireless sensor networks and explain any two with an example each.**

   WSNs have grown substantially over the years and have a momentous potential in diverse Applications in areas of

   - Environmental Science,
   - Medical Sciences,
   - Telecommunications,
   - Education Services,
   - Agriculture,
   - Surveillance,
   - Military Services, etc

2. **Explain characteristics of Wireless Sensor Networks**

   - Power consumption constraints for nodes using batteries or energy harvesting.
   - Ability to cope with node failures (resilience)
   - Some mobility of nodes (for highly mobile nodes see MWSNs)
   - Heterogeneity of nodes.
   - Homogeneity of nodes.
   - Scalability to large scale of deployment.

3. **Draw the sensor network architecture and describe the components in details**

   It is a 2-tier hierarchy clustering architecture. It is a distributed algorithm for organizing the sensor nodes into groups called clusters. The cluster head nodes in each of the autonomously formed clusters create the Time-division multiple access (TDMA) schedules.

   The three cross layers include the following:

   - Power Management Plane
   - Mobility Management Plane
   - Task Management Plane

   These three cross layers are mainly used for controlling the network as well as to make the sensors function as one in order to enhance the overall network efficiency. The above mentioned five layers of WSN are discussed below.

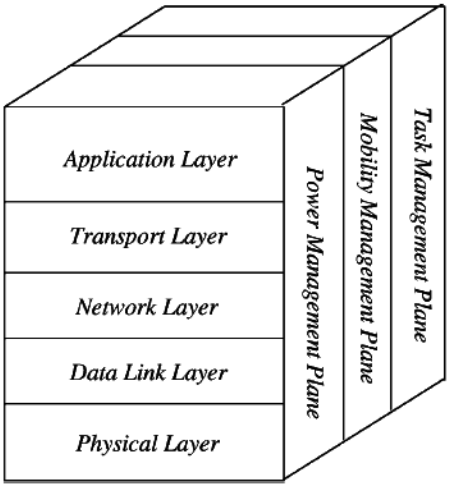
   Application Layer

   The application layer is liable for traffic management and offers software for numerous applications that convert the data in a clear form to find positive information. Sensor networks arranged in numerous applications in different fields such as agricultural, military, environment, medical, etc.

Transport Layer

The function of the transport layer is to deliver congestion avoidance and reliability where a lot of protocols intended to offer this function are either practical on the upstream. These protocols use dissimilar mechanisms for loss recognition and loss recovery. The transport layer is exactly needed when a system is planned to contact other networks.

Providing a reliable loss recovery is more energy-efficient and that is one of the main reasons why TCP is not fit for WSN. In general, Transport layers can be separated into Packet driven, Event-driven. There are some popular protocols in the transport layer namely STCP (Sensor Transmission Control Protocol), PORT (Price-Oriented Reliable Transport Protocol and PSFQ (pump slow fetch quick).



Network Layer

The main function of the network layer is routing, it has a lot of tasks based on the application, but actually, the main tasks are in the power conserving, partial memory, buffers, and sensor don’t have a universal ID and have to be self-organized.

The simple idea of the routing protocol is to explain a reliable lane and redundant lanes, according to a convincing scale called a metric, which varies from protocol to protocol. There are a lot of existing protocols for this network layer, they can be separated into; flat routing and hierarchal routing or can be separated into time-driven, query-driven & event-driven.

Data Link Layer

The data link layer is liable for multiplexing data frame detection, data streams, MAC, & error control, confirm the reliability of point–point (or) point– multipoint.

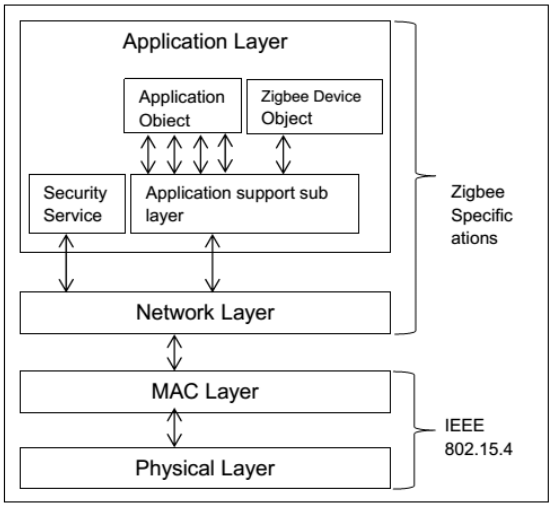
Physical Layer

The physical layer provides an edge for transferring a stream of bits above the physical medium. This layer is responsible for the selection of frequency, generation of a carrier frequency, signal detection, Modulation & data encryption. IEEE 802.15.4 is suggested as typical for low rate particular areas & wireless sensor networks with low cost, power consumption, density, the range of communication to improve the battery life. CSMA/CA is used to support star & peer to peer topology. There are several versions of IEEE 802.15.4.V.

The main benefits of using this kind of architecture in WSN is that every node involves simply in less-distance, low- power transmissions to the neighboring nodes due to which power utilization is low as compared with other kinds of sensor network architecture. This kind of network is scalable as well as includes a high fault tolerance.

4. **Briefly specify IEEE 802.15.4 MAC protocol and explain whether the MAC protocols of 802.11 & Bluetooth be used for WSN. Justify**

Whereas,802.15. 4 might outperform 802.11 in terms of power consumption and energy efficient. The high power consumption of Wi-Fi devices is also related to its high transmission power and high processing level

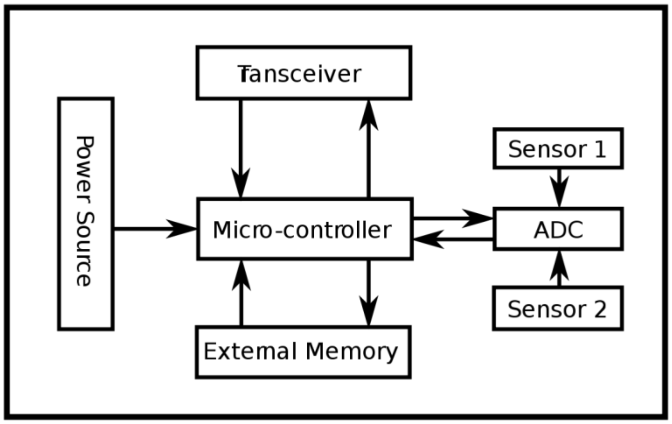


5. **Interpret the Transceiver characteristics and structure used in the sensor node.**

A transceiver is a combination transmitter/receiver in a single package. While the term typically applies to wireless communications devices, it can also be used for transmitter/receiver devices in cable or optical fiber systems. The main functionality of this electronic device is to transmit, as well as receive, different signals.

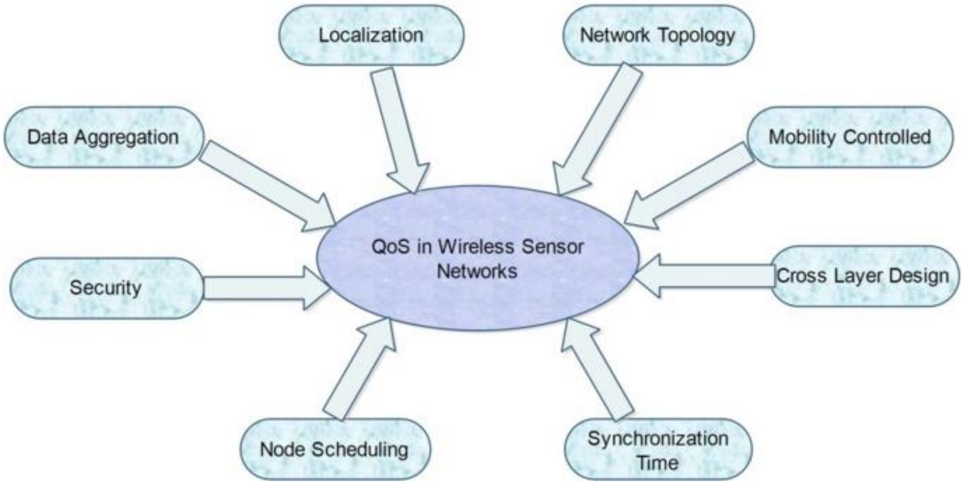
In local area networks, the transceiver is a part of the network interface card. It can both transmit signals over the network wire and detect electrical signals flowing through the wire. However, some types of networks require an external transceiver.

In wireless communication devices, like smartphones and cordless telephones, the transceiver is built into the mobile device.



6. **Examine the factors playing major role in optimizing a wireless sensor network**

Optimization Wireless Sensor Network (WSN) is necessary to reduce redundancy and energy consumption. To optimizing wireless sensor networks for secured data transmission both at cluster head and base station data aggregation is needed. Data aggregation is performed in every router while forwarding data



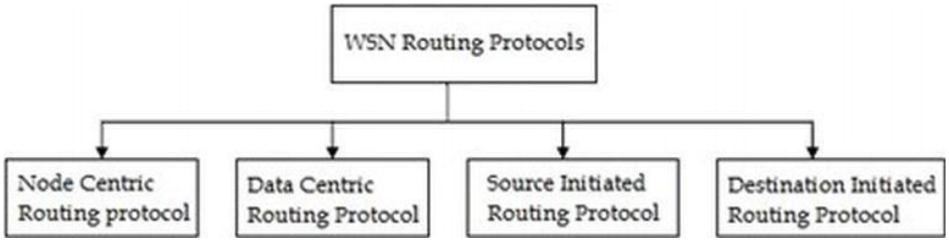
UNIT II
MAC AND ROUTING PROTOCOLS
PART-A

1. **What are the performance requirements for a MAC protocols?**
   The most important performance requirements for MAC protocols are throughput efficiency, stability, fairness, low access delay, and low transmission delay, as well as a low overhead.
2. **Discuss the concept of wake up radio.**
   Wake up Radios are the basic circuits for the on-demand communications scheme. The wake up radio handles the sending and receiving of wake up messages that switch on themain processing unit or the main radio of the required node. at least the same as the periodic listening schemes-based networks.
3. **Illustrate the difference between contention based protocols and schedule based protocols.**
   Contention-based protocols provide a contention- based bandwidth allocation for sensor nodes and are widely discussed in urban applications. Schedule-based, also known as contention-free, protocols require at least one central node time-synchronized or asynchronized networks.
4. **Determine how flooding is different from gossiping.**
   Gossiping is similar to flooding except that, a node receiving a packet, instead of broadcasting, the node sends it to only one of its randomly selected neighbor, and the neighbor in turn sends the packet to one of its randomly selected neighbor, this continues until the packet reaches its destination.
5. **Analyze the pros and cons of Scheduled based protocols.**
   The major advantage of R-CSMA against FPRP, CATA and SRMA/PA is that it doesn't reserve any bandwidth for control packets. R-CSMA doesn't allocate any control slot since control packets are transmitted only once at the reservation request step.
6. **Summarize the objective of PAMAS.**

   PAMAS: Power Aware Multi-Access (PAMAS) is one of the oldest contentions based MAC protocol designed with energy efficiency is the main object. In this protocol nodeswhich are not transmitting or receiving are in sleep mode to conserve energy.
7. **Outline the features of IEEE 802.15.4.**
   IEEE 802.15 TG4 FEATURES
   - Data rates of 250 kbps, 40 kbps, and 20 kbps.
   - Two addressing modes; 16-bit short and 64-bit IEEE addressing.
   - Support for critical latency devices, such as joysticks.
   - CSMA-CA channel access.
   - Automatic network establishment by the coordinator.
   - Fully handshake protocol for transfer reliability.
8. **Demonstrate how LEACH protocol differs from other routing protocols used in WSN.**
   LEACH is a hierarchical routing protocol used in wireless sensor networks to expandthe network lifetime. In the LEACH protocol, sensors arrange themselves in a cluster,and a single node of these nodes performs a cluster head.
9. **Explain TRAMA.**
   TRAMA is energy- aware channel access protocol for wireless sensor networks. TRAMA uses the traffic based schedules and avoids the wasting slots and switch the nodes to low power mode when there is no data to send and they are intended receivers of traffic.

10. **Define Routing Protocols.**
    The routing protocol is a process to select suitable path for the data to travel from source to destination. The process encounters several difficulties while selecting the route, which depends upon, type of network, channel characteristics and the performance metrics.

11. **Discuss about B-MAC.**
    B-MAC (Berkeley MAC) is a carrier sense media access protocol for wireless sensor networks that provides a flexible interface to obtain ultra-low power operation, effective collision avoidance, and high channel utilization.
12. **Explain the META-DATA.**
    Sensors use meta-data to succinctly and completely describe the data that they collect. If x is the meta-data descriptor for sensor data X then the size of xin bytes must be shorter than the size of X, for SPIN to be beneficial. If two pieces of actual data are distinguishable, then their corresponding meta-data should be distinguishable. Likewise, two pieces of indistinguishable data should share the same meta- data representation. SPIN does not specify a format
13. **Illustrate the types of routing protocols.**


WSN Routing Protocols
Node Centric Routing protocol
Data Centric Routing Protocol
Source Initiated Routing Protocol
Destination Initiated Routing Protocol

14. **What is meant by SPIN?**
    One of the majors being routing protocol, i.e., the task of transmitting data from source node to sink node. SPIN (Sensor Protocols for Information via Negotiation) being one of them, which efficiently disseminates information among sensor node in an energy-constrained wireless sensor network.
15. **Discuss the concept of collision, overhearing.**
    - Collisions occur when two or more sensor nodes trying to send data packets at the same time.
    - Overhearing occurs when a specific node receives a packet of data which was attended to be sent to another node.

16. **Define the methodology of directed diffusion.**
    Directed diffusion is data-centric in that all communication is for named data. All nodes in a directed-diffusion-based network are application aware. This enables diffusion to achieve energy savings by selecting empirically good paths and by caching and processing data in-network (e.g., data aggregation).
17. **What are the steps followed in direct diffusion.**
    Directed diffusion consists of several elements: interests, data messages, gradients, and reinforcements. An interest message is a query or an interrogation which specifies what a user wants. Each interest message contains a description of data interested by a user.
18. **Give the feature of PAMAS.**
    - Power Aware Multi-access with Signaling

- Overhearing avoidance mechanism
- Combines the busy tone solution and RTS/CTS handshake
- Use two channel: a data channel and a control channel

19. **What are the reasons of Hidden Terminal Problem?**

In wireless LANs (wireless local area networks), the hidden terminal problem is a transmission problem that arises when two or more stations who are out of range of each other transmit simultaneously to a common recipient.

20. **What is PEGASIS?**

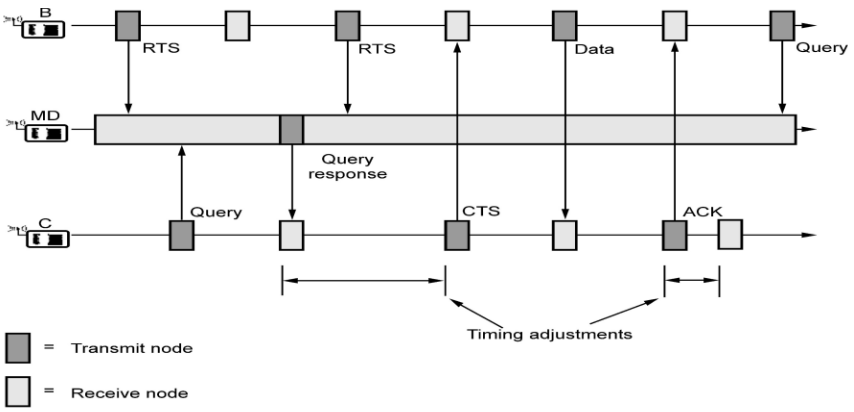
It is a hierarchical based routing algorithm used to address the overhead caused by cluster formation in LEACH by constructing chains of nodes instead of cluster.

PART B & C

1. **Depict the importance of the Mediation device protocols with relevant diagrams in wireless sensor networks.**

A protocol mediation device rewrites your alarms to a format that is compatible with your SNMP or TL1 manager. A protocol is just a format for encoding info.

1. The mediation device protocol is compatible with the peer-to-peer communication mode of the IEEE 802.15.4 low-rate WPAN standard. It allows each node in a WSN to go into sleep mode periodically and to wake up only for short times to receive packets from neighbor nodes.
2. There is no global time reference, each node has its own sleeping schedule, and does not take care of its neighbors sleep schedules.
3. Upon each periodic wakeup, a node transmits a short query beacon, indicating its node address and its willingness to accept packets from other nodes. The node stays awake for some short time following the query beacon, to open up a window for incoming packets. If no packet is received during this window, the node goes back into sleep mode.
4. When a node wants to transmit a packet to a neighbor, it has to synchronize with it. One option would be to have the sender actively waiting for query beacon, but this wastes considerable energy for synchronization purposes only.
5. The dynamic synchronization approach achieves this synchronization without requiring the transmitter to be awake permanently to detect the destinations querybeacon. To achieve this, a Mediation Device (MD) is used. The case where the mediation device is not energy constrained is discussed below and can be active all the time. Because of its full duty cycle, the mediation device can receive the query beacons from all nodes in its vicinity and learn their wakeup periods.



Suppose that node A wants to transmit a packet to node B. Node A announces this to the mediation device by sending periodically Request to Send (RTS) packets, which the MD captures. Node A sends its RTS packets instead of its query beacons and thus they have the same period. Again, there is a short answer window after the RTS packets, where A listens for answers. After the MD has received A's RTS packet, it waits for B's next query beacon. The MD answers this with a query response packet, indicating A's address and a timing offset, which lets B know when to send the answering Clear to Send (CTS) to A such that the CTS packet hits the short answer window after A's next RTS packet. Therefore, B has learned A's period. After A has received the CTS packet,it can send its data packet and wait for B's immediate acknowledgment. After the transaction has finished, A restores its periodic wakeup cycle and starts to emit query beacons again. Node B also restores its own periodic cycle and thus decouples from A's period.

3. **Determine the impact of S-MAC protocol in a network with suitable diagrams**

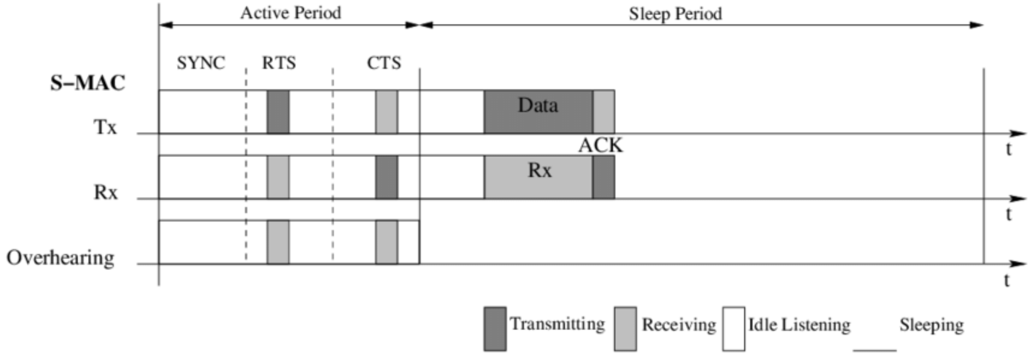
Self-organizing Medium Access Control for Sensor (SMACS) networks is a distributed protocol. This protocol forms a flat topology. SMACS invokes sensor nodes to find out its neighbors. The major functionalities of these protocols are given below:

- Network initialization
- Link layer organization
- Neighbor discovery
- Channel assignment.

Communication path can be established between two nodes by having pair of time slots for transmission and reception at a fixed frequency. Each communication link can work on different frequency. A channel is assigned to each link. The time slot can be randomly selected by the nodes during the time of link establishment. There will be no interference between nodes due to the availability of large bandwidth. Power can be saved by turning off the transceiver in idle slots. After establishing a link between nodes, the transceiver of the node can be turned on when transmission takes place. Otherwise, itwill be powered off.

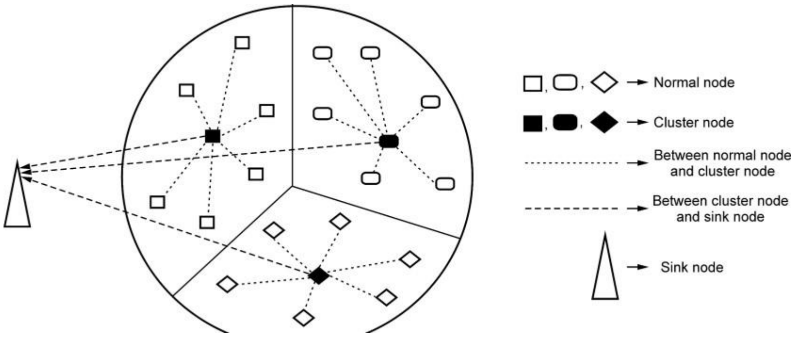
Neighbor discovery - Each node can wake up at random time. After wake up, the nodekeeps on listening to the channel to transmit the invitation message. If the node finds that none of the other nodes are transmitting invitation message, then it will start to send the invitation message on the channel at fixed frequency. The neighbor nodes which hear the invitation message will respond to the sender of the invitation message.

The node who originated the invitation message may receive multiple responses from different nodes. At a time, it accepts the response from one node from which it has received the response first and hence establishing relationship with the neighbor nodes and forms a link.



4. Explain the LEACH routing with the help of neat diagram. Give its advantages and disadvantages.

1. LEACH (Low Energy Adaptive Clustering Hierarchy) is a TDMA based protocol designed for dense sensor network. LEACH partitions the sensor nodes into clusters with a dedicated cluster head in each cluster.
2. The role of the cluster head is to create a TDMA schedule, distribute and maintain this schedule with its cluster members. The cluster head aggregates data of its members and transmits data to the sink.
3. The cluster head selection is done by each node independently based on the last timethe node served as a cluster head.


Normal node
Cluster node
Between normal node and cluster node
Between cluster node and sink node
Sink node

4. The non-cluster head choose their cluster head based on the received signal strength. Since the cluster head node is switched on all the time, so it burns its energy quickly and goes to die. This problem is solved by selecting the new cluster head in next round.

5. Summaries the method to select the protocol for SPIN and justify the reasons.

It transfers all the useful data only from each node to every node in the network assuming that all the nodes in the network are Base Station. SPIN node uses three types of messages for communication.

ADV- It is used to advertise new data.

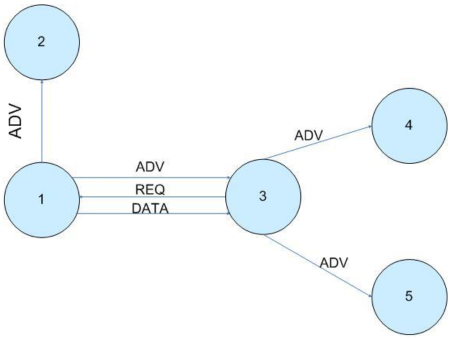
REQ- REQ is used to receive the actual data.

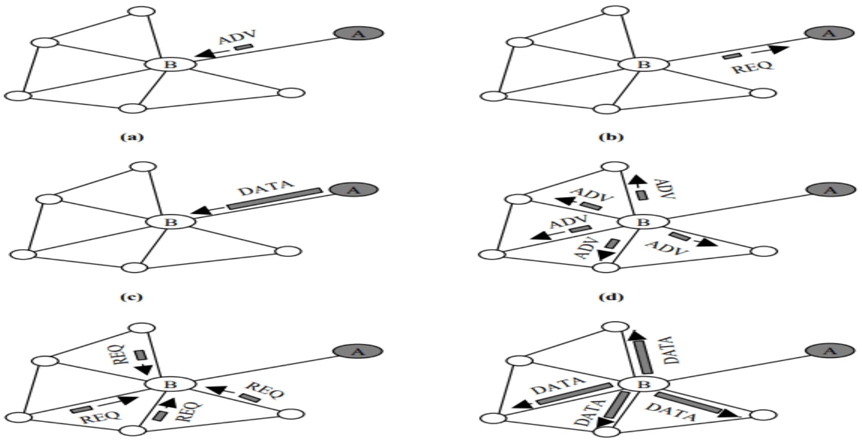
DATA- DATA is the actual message itself.

Working of SPIN protocol

Node A starts by Advertising its data to the node B. Node B responds by sending a request to the node A.

As soon as node B receives the request it sends the original data to its neighbor nodes and similarly the process goes on till all the nodes in the network receives the data. This process continues till all the nodes receive the data.





(a) (b) (c) (d)

ADVANTAGES OF SPIN

SPIN solves the problem of Implosion, Overlap and thus achieve a lot of energy efficiency.

IMPLOSION

Node A starts by flooding the data to its two neighbor's i.e B and C. These nodes store the data received from A and send a copy of it to their neighbor D. The protocol thus wastes energy and bandwidth by sending one extra copy of A to D.

OVERLAP

The sensor area of node A and node B are overlapping and the neighbor node of A and B are same therefore node C receives 2 copies of Y and energy is wasted.

COMPONENTS OF WSN

Sensing Unit: - Sensing units are made up of two units Sensor and ADC. ADC transforms Analog signal to Digital signal and transfer the information to the processing unit.

Processing Unit: - It processes the sensor nodes and store the information which is send by the sensing unit and then send it back to the transceiver.

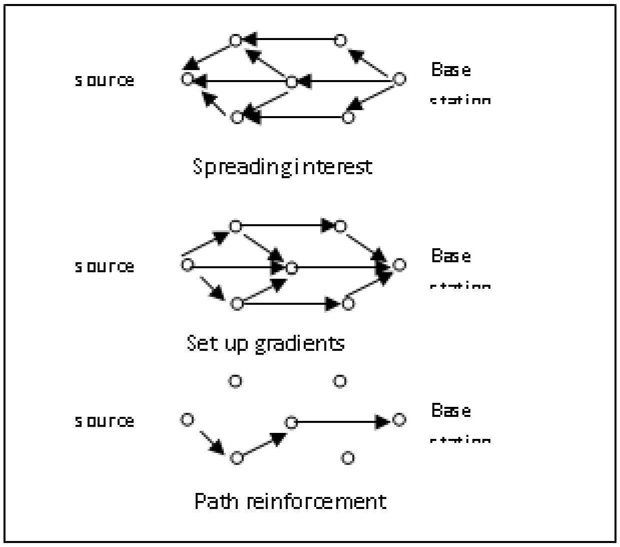
Transceiver: - Transceiver connects the node to the network.

Power Unit: - Power Units consists of solar cells which sends the power to the whole network.

Power Generator: - It gives power to the whole WSN.

6. **Explain the Directed Diffusion routing with the help of neat diagram. Give its advantages and disadvantages.**

Directed diffusion consists of several elements: interests, data messages, gradients, and reinforcements. An interest message is a query or an interrogation which specifies what a user wants. Each interest contains a description of a sensing task that is supported by a sensor network for acquiring data. Typically, data in sensor networks is the collected or processed information of a physical phenomenon. Such data can be an event, which is a short description of the sensed phenomenon. In directed diffusion, data is named using attribute-value pairs. A sensing task (or a subtask thereof) is disseminated throughout the sensor network as an interest for named data. This dissemination sets up gradients within the network designed to "draw" events (i.e., data matching the interest). Specifically, a gradient is direction state created in each node that receives an interest. The gradient direction is set toward the neighboring node from which the interest is received. Events start flowing toward the originators of interests along multiple gradient paths. The sensor network reinforces one or a small number of these paths.



Spreadinginterest

Set up gradients

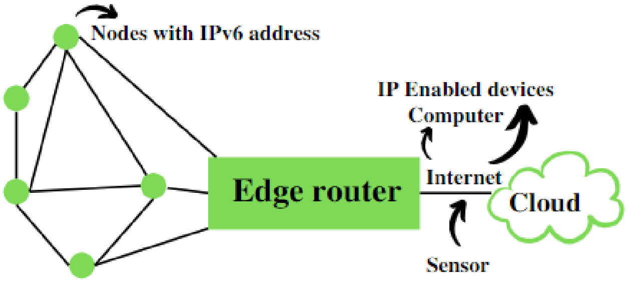
Path reinforcement

These elements of diffusion with specific reference to a particular kind of sensor network one that supports a location tracking task. As we shall see, several design choices present themselves even in the context of this specific instantiation of diffusion. We elaborate on these design choices while describing the design of our sensor network. Our initial evaluation focuses only a subset of these design choices. Different design choices result in different variants of diffusion. Moreover, even though we describe this diffusion variant for rate-based applications, diffusion also works for event-triggered applications.

UNIT III – 6LOWPAN
PART-A

1. **What is 6LOWPAN?**

   6LoWPAN stands for IPv6 over Low-power Wireless Personal Area Networks. It is a standard protocol for realizing IPv6 communication on wireless networks composed of low-power wireless modules.



2. **What are the applications of 6LOWPAN?**

   It is used in home-automation, smart agricultural techniques and industrial monitoring. It is utilized to make IPv6 packet transmission on networks with constrained power and reliability resources possible.

3. **List the features of 6LOWPAN.**
   - It is used with IEEE 802.15. 4 in the 2.4 GHz band.
   - Outdoor range: ~200 m (maximum)
   - Data rate: 200kbps (maximum)
   - Maximum number of nodes: ~100.

4. **Define Adaptation Layer.**

   The adaptation Layer helps you describe communication between the Virtual Tester and the system under test. Many different means of communication allow your systems to talk with each other. At the software application level, a communication type is identified by a set of services provided by specific functions.

5. **What is meant by link layer and its types of frames?**

   The data link layer is the protocol layer in a program that handles the moving of data into and out of a physical link in a network. The data link layer is Layer 2 in the Open Systems Interconnection (OSI) architecture model for a set of telecommunication protocols.

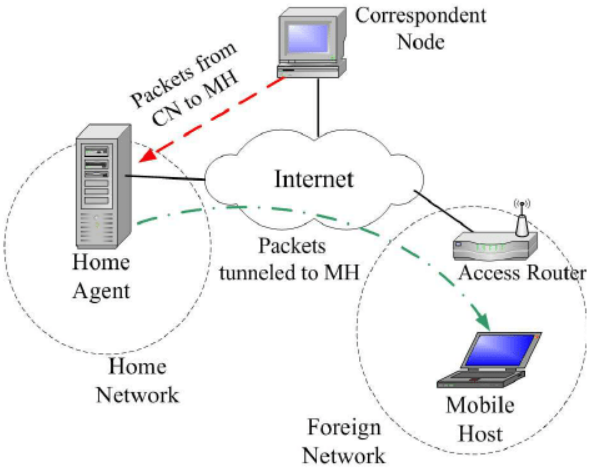
   Types of frames:

   Data frame, Acknowledgment frame, MAC layer command frames and Beacon frames.

6. **Explain Routing.**

   Routing is the process of path selection in any network. A computer network is made of many machines, called nodes, and paths or links that connect those nodes. Communication between two nodes in an interconnected network can take place through many different paths.

7. **Give the advantages of 6LOWPAN.**
    - 6LoWPAN is a mesh network that is robust, scalable, and can heal on its own.
    - It delivers low-cost and secure communication in IoT devices.
    - It uses IPv6 protocol and so it can be directly routed to cloud platforms.
    - It offers one-to-many and many-to-one routing.
8. **Define Fragmentation and Reassembly.**
    Fragmentation consists of partitioning a larger than 127 bytes input datagram into multiple fragments that are linked together through a common identifier that, in turns, is used by the decoder at reassembly.
9. **List the type of mobilities.**
    Roaming
    Handover
    Physical Movement
    Radio Channel
    Network Performance
    Sleep Schedules.
10. **What is meant by Mobile IPv6?**
    Mobile IPv6 provides mobility support for IPv6. It allows you to keep the same internet address all over the world, and allows applications using that address to maintain transport and upper-layer connections when changing locations. It allows mobility across homogenous and heterogeneous media.



11. **What is meant by Protocols?**
    It is a set of rules that need to be followed by the communicating parties in order to have successful and reliable data communication. For example - Ethernet and HTTP.
12. **Define NEMO.**
    Network Mobility is a solution for dealing with network mobility problem when the router and the nodes attached to it move their point of attachment all together.
13. **What is meant by Proactive routing?**
    Proactive routing protocols maintain information on all routes throughout the network, even if they are not required, so each node registers routes to all other nodes in the network. These

protocols exchange control information between nodes on a regular basis, which keeps updated routes for each node in the network.

14. Explain Reactive routing.

Reactive routing protocols: 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.

15. Explain Distance vector Routing?

Distance-vector routing protocols measure the distance by the number of routers a packet has to pass; one router counts as one hop. Some distance-vector protocols also take into account network latency and other factors that influence traffic on a given route.

16. Mention some disadvantage of 6LOWPAN.

Header compression may increase the processing time and complexity of low-power devices, fragmenting IPv6 packets may cause more packet loss and retransmissions, and routing IPv6 packets may require more memory and computation resources.

17. Discuss about security and interoperability with 6LOWPAN

Security: 6LoWPAN security is ensured by the AES algorithm, which is a link layer security, and the transport layer security mechanisms are included as well.

Interoperability: 6LoWPAN is able to operate with other wireless devices as well which makes it interoperable in a network.

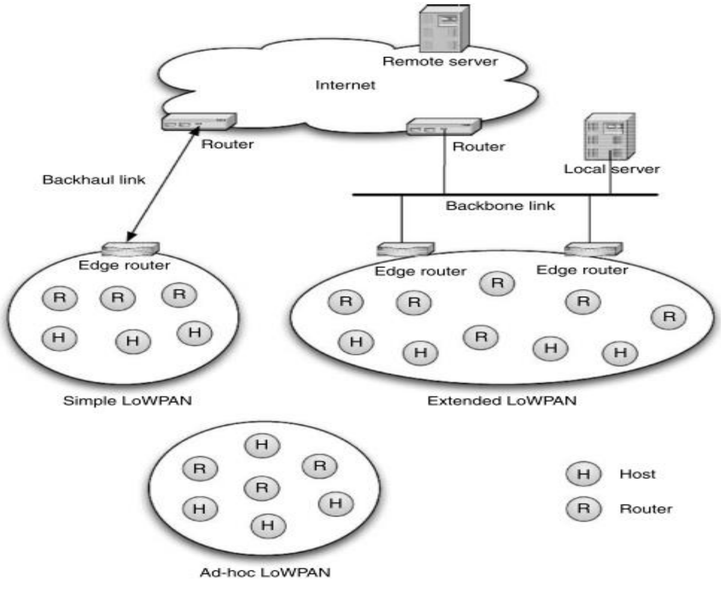
18. List the basic requirements of 6LOWPAN

6LoWPAN stands for IPv6 over Low-power Wireless Personal Area Networks. It is a standard protocol for realizing IPv6 communication on wireless networks composed of low-power wireless modules.

19. Explain Proxy home agent.

It is an entity which performs MIPv6 function on behalf of a local mobile node, interacts with the actual home agent of the node and handle route optimization and its behalf.

20. Draw the architecture of 6LOWPAN.



PART B & C

1. **Explain briefly about the architecture of 6LOWPAN.**

6LoWPAN is a protocol specification to enable IPv6 standards to be used in low-power wireless networks, specifically with IEEE 802.15.4. The IETF 6LoWPAN working group maintains it. The rationale for introducing 6LoWPAN is that the existing IPv6 is too bulky for WSN. In 6LoWPAN, the IPv6 header is compressed to only a few bytes by introducing an adaptation layer that resides between network and MAC/PHY layer while retaining the main IPv6 functionality. The transmission of 1280 bytes IPv6 Maximum Transmission Unit (MTU) over IEEE 802.15.4 is also made possible using fragmentation and reassembly provided by this adaptation layer. The detail specification of this protocol is described in IETF standard RFC4944.

The 6LoWPAN architecture is made up of low-power wireless area networks (LoWPANs), which are IPv6 subnetwork. It means a LoWPAN is the collection of 6LoWPAN nodes, which share a common IPv6 address prefix (the first 64-bits of an IPv6 address). LoWPAN nodes may play the role of host or router, along with one or more edge routers, as seen in Fig. 1.

There are three types of LoWPANs which are Simple LoWPANs, Extended LoWPANs, and Ad hoc LoWPANs [10]. A Simple LoWPAN is connected through one LoWPAN Edge Router to another IP network. An Extended LoWPAN consists of multiple edge routers along with a backbone link to interconnect them. An Ad hoc LoWPAN is not connected to the Internet and operates without an infrastructure.

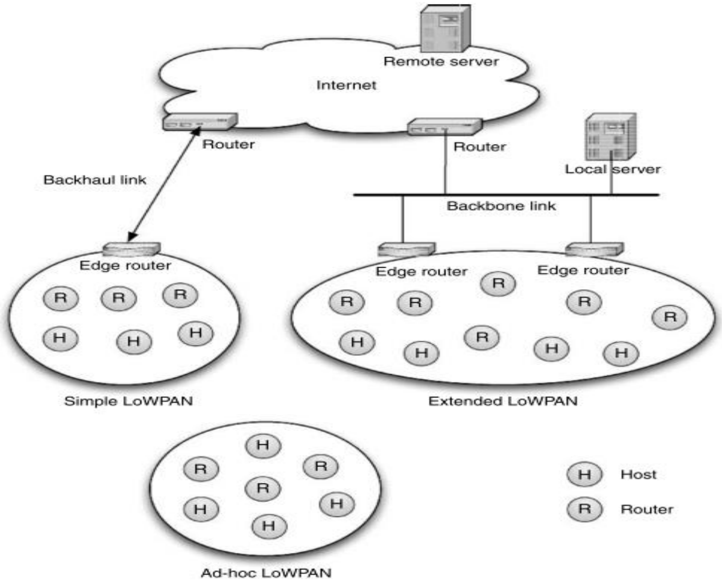
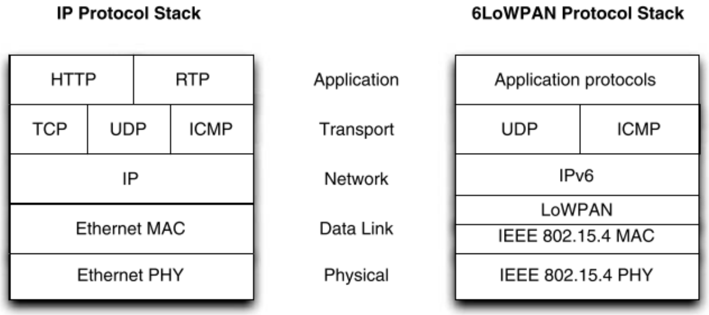


Figure 2 shows the 6LoWPAN protocol stack compared to the IP protocol stack.

It is almost identical to a normal IPv6 implementation with the following two differences: x 6LoWPAN only supports IPv6, for which a small adaptation layer (LoWPAN) has been defined to optimize IPv6 over link layers.

x Although 6LoWPAN is not bound to the IEEE 802.15.4 standard, it is designed to utilize it.



2. **Discuses about the link layer protocol and Adaptive layer.**

Link layer protocol

The link layer is the lowest layer in the Internet protocol suite, the networking architecture of the Internet. The link layer is the group of methods and communications protocols confined to the link that a host is physically connected to. The link is the physical and logical network component used to interconnect hosts or nodes in the network and a link protocol is a suite of methods and standards that operate only between adjacent network nodes of a network segment.

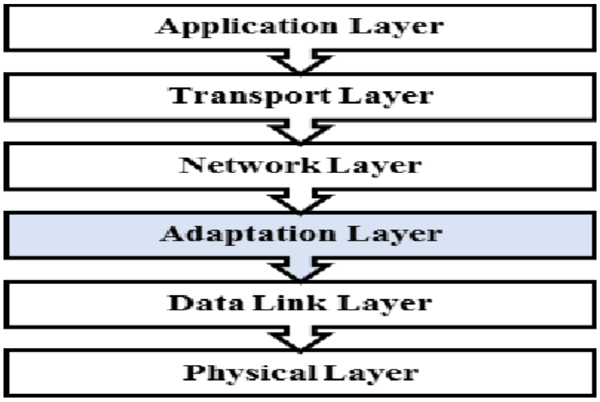
Despite the different semantics of layering between the Internet protocol suite and OSI model, the link layer is sometimes described as a combination of the OSI's data link layer (layer 2) and physical layer (layer 1).

The link layer in the TCP/IP model is a descriptive realm of networking protocols that operate only on the local network segment (link) that a host is connected to. Such protocol packets are not routed to other networks. The link layer includes the protocols that define communication between local (on-link) network nodes which fulfill the purpose of maintaining link states between the local nodes, such as the local network topology, and that usually use protocols that are based on the framing of packets specific to the link types.

Adaptive layer:

The usage of IPv6 in transmission of packets over LoWPAN (IEEE standard 802.15.4) is not a natural fit. Hence an adaptation layer is proposed by IETF to make IPv6 and 802.15.4 compatible with each other [5]. This layer is placed between network layer and data link layer in 6LoWPAN protocol stack as shown in Fig.1. There are three main functions of this layer. First main function is header compression and decompression. This layer compresses the IPv6 and UDP header. Various techniques have been suggested to perform this function. Second function of adaptation layer is fragmentation and reassembly of packets. Third major task of this layer is Routing. Usually, routing is considered as the main task of network layer but it can also be handled by adaptation layer. When routing decision takes place at adaptation layer it is called mesh under routing and when routing is done at network layer it is route over routing. [7] [8]. The border nodes of the WSN should be able to route IPv6 packets into the WSN nodes from outside and route inside packets to outside IP network. Besides these three major functions, there are other functions of the adaptation layer on networking related things like neighbour discovery and multicast support.

Functions Of Adaptation Layer 6LoWPAN is a communication protocol for wireless connectivity in sensor based applications with restrictive resources. It enhances the scalability and mobility of sensor networks. The challenge of 6LoWPAN is that the IPv6 network and IEEE 802.15.4 network are totally different. Placing an adaptation layer between the IP layer and the Data link layer is the solution to transport IPv6 packets over IEEE 802.15.4 links.



3. **Draw a neat diagram and explain Routing.**

- A Router is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router.
- A Router works at the network layer in the OSI model and internet layer in TCP/IP model
- A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.
- The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.
- The routing protocols use the metric to determine the best path for the packet delivery. The metric is the standard of measurement such as hop count, bandwidth, delay, current load on the path, etc. used by the routing algorithm to determine the optimal path to the destination.
- The routing algorithm initializes and maintains the routing table for the process of path determination.

Routing Metrics and Costs

Routing metrics and costs are used for determining the best route to the destination. The factors used by the protocols to determine the shortest path, these factors are known as a metric.Metrics are the network variables used to determine the best route to the destination. For some protocols use the static metrics means that their value cannot be changed and for some other routing protocols use the dynamic metrics means that their value can be assigned by the system administrator.

Hop count: Hop count is defined as a metric that specifies the number of passes through internetworking devices such as a router, a packet must travel in a route to move from source to the destination. If the routing protocol considers the hop as a primary metric value, then the path with the least hop count will be considered as the best path to move from source to the destination.

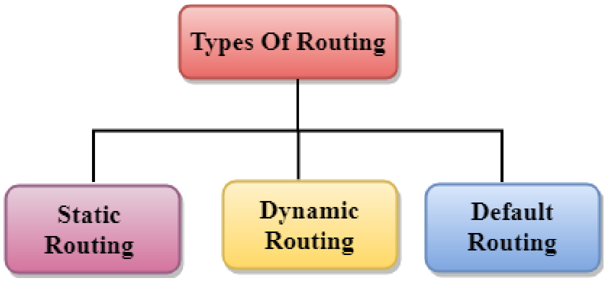
Delay: It is a time taken by the router to process, queue and transmit a datagram to an interface. The protocols use this metric to determine the delay values for all the links along the path end-to-end. The path having the lowest delay value will be considered as the best path.

Bandwidth: The capacity of the link is known as a bandwidth of the link. The bandwidth is measured in terms of bits per second. The link that has a higher transfer rate like gigabit is preferred over the link that has the lower capacity like 56 kb. The protocol will determine the bandwidth capacity for all the links along the path, and the overall higher bandwidth will be considered as the best route.

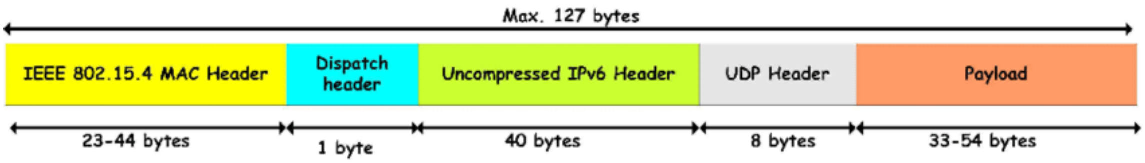
Load: Load refers to the degree to which the network resource such as a router or network link is busy. A Load can be calculated in a variety of ways such as CPU utilization, packets processed per second. If the traffic increases, then the load value will also be increased. The load value changes with respect to the change in the traffic.

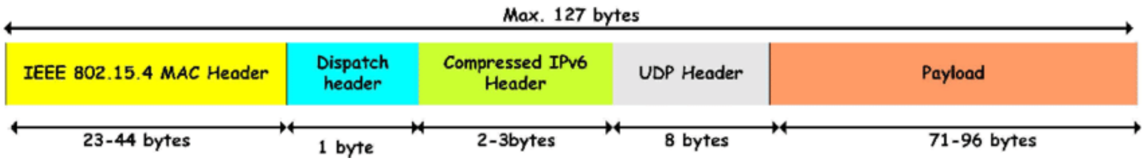
Reliability: Reliability is a metric factor may be composed of a fixed value. It depends on the network links, and its value is measured dynamically. Some networks go down more often than others. After network failure, some network links repaired more easily than other network links. Any reliability factor can be considered for the assignment of reliability ratings, which are generally numeric values assigned by the system administrator.

Types of Routing:



4. **Explain briefly about the header Compression.**
Header compression of a TCP data segment whose window field has not changed from with respect its antecedent, the two bytes of the lowest bytes of the sequence number that have been changed. The size of this header is seven bytes.
6LoWPAN compresses the IPv6 header by removing the not needed fields, by removing fields that have always the same content and by compressing the IPv6 ad- dresses by inferring them from link layer addresses.



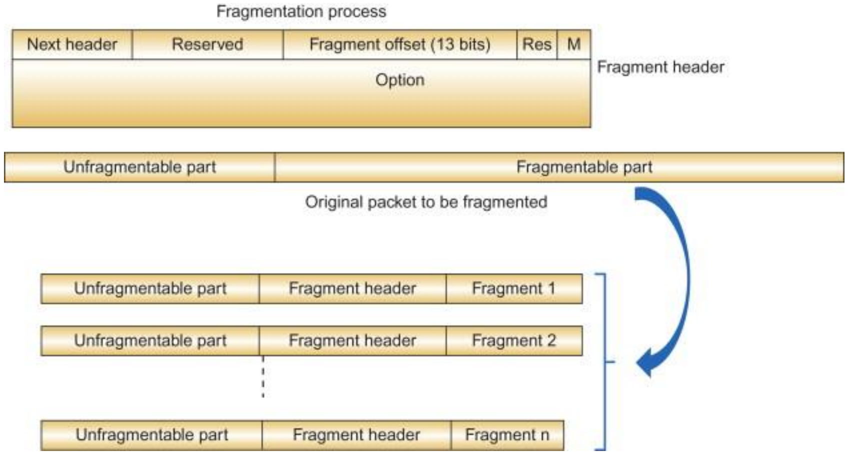


With the mechanisms provided by the adaptation layer, there are four basic header types defined in 6LoWPAN: Dispatch Header, Mesh Header, Fragmentation Header and the HC1 Header. HC1 was first header compression technique for 6LoWPAN suggested in RFC 4944 for compressing IPv6 header. HC1 is acronym for Header Compression 1. In place of 40 bytes of IPv6 header, 2 bytes are used which indicates the way IPv6 header is compressed and from where its values.

Dispatch header indicates which header will be coming next. Bit numbers 0-1 in dispatch header indicates IPv6 header will be followed after it. Bit numbers 6-7 of first byte has value 10 are indicative of the presence of compressed IPv6 (HC1) header. Source address (SA) and destination address (DA) fields in HC1 header are fetched from link layer address. Field T represents traffic class and flow label which is 0 in HC1. Field next header (NH) indicates which header will be followed by compressed IPv6 header. NH field can have 4 values i.e. 00, 01, 10 and 11 representing uncompressed header, UDP, TCP and ICMP respectively. HC2 field indicates the way next header arrives. If HC2 is 0, then next header is uncompressed, otherwise compressed. Hop limit is uncompressible field in this technique hence it has to be carried inline. HC1 technique works well when addresses are link local but doesn't support compression when global unicast & multicast are there [12]. Hence, global multicast address is carried inline (128 bits of address without compression). Hop limit is uncompressible field in this technique [10]. As HC1 technique doesn't support compression of global addresses hence HC1g, extension of HC1 was suggested [5]. HC1g is acronym for header compression of global address. It can compress global unicast address. In this technique, 6LoWPAN network is assigned a single global address prefix of 64 bits in length. When source or destination address matches this assigned default value, it can be compressed by eliding the prefix

5. **Define about Fragmentation and Reassembly. With neat diagram.**

Maximum transmission unit (MTU) of IPv6 packets is of 1280 bytes whereas in 802.15.4 the permissible packet size is only 127 bytes. In 6LoWPAN, IPv6 packets are to be transmitted over 802.15.4 which is not possible without fragmenting them to support MTU of it. Hence to encapsulate the IPv6 large sized packets onto 802.15.4, they need to be fragmented, transmitted and reassembled after reaching the destination. At sender node when an IPv6 packet size exceeds the available link layer payload size, the 6LoWPAN fragmentation mechanism takes place. It will treats the IPv6 packet as a single data field and iteratively break this data into fragments. The size of the fragments will be according to the maximum frame size at the data link layer. Each fragment will then include a fragment header before it is transmitted. The task of fragmentation and reassembly of packets is performed by adaptation layer. From network layer of source node, packets will come to adaptation layer which will first check its size. If packet size is greater, then it will fragment it and forward to MAC layer. Fragment header is send with each fragment when it is transmitted. The fields of fragment header are Datagram Size, Offset and Tag.



The first two bit of byte 1 are ‘11’ that means this header is a fragment header. D_size indicates the size of datagram before fragmentation. The size of un-fragmented datagram is send with every fragment so that sufficient buffer is allocated on receiver side as datagram may reach out of order. D_Tag is a unique number which is attached with each fragment belonging to same datagram. D_offset indicates the placing of the fragment in an un-fragmented datagram. It is useful for arranging the fragments in order during reassembly of datagram. Bit number 3 of byte 1 represents offset (O) whose value could be 0 or 1. The offset value of first fragment will be 0 and for rest of the fragments it will be 1. The fragment header of first fragment is of 4 bytes as there is no need to send the offset value in it. For rest of the fragments, the fragment header is of 5 bytes. Bit numbers 4 and 5 are reserved bits (R) for future use.

Reassembly process takes place at adaptation layer of receiver node. Each fragment carries information about how much buffer need to be reserved at receiver node so that during reassembly of complete packet there is no memory crunch. The datagram offset field indicates the position of the current payload within the original IPv6 packet. Fragment reassembly time is usually 60 sec. If all fragments belonging to same packet does not arrive and misses then reassembly buffer is drained. In this case all fragments need to be transmitted again by the sender. When fragments reach the adaptation layer of receiver then they are reassembled to form a complete packet and then passed to the upper layer. If datagram is small and a single frame is sufficient enough to carry the payload than there is no need to perform fragmentation. In that case no fragment header is attached with the packet.

6. Describe Mobility and its types.

6LoWPAN is comprised of a fixed gateway that connects with the internet segregated into three kinds such as mobile FFDs, anchor FFDs and backbone FFDs. While RFDs are mobile in nature excluding the routing and forwarding function that is primarily utilized in sensing the data. There are three different classes of mobility in WSNs: sink mobility, node mobility and user mobility

Sink mobility: Sink mobility is another energy-efficient technique for WSNs where the sink moves on a sink movement trajectory either by the robots or vehicles. Sink halts after every fixed time interval and gathers the data of the sensor nodes in the vicinity.

Node mobility can be defined as hiding from the application. or user changes in the connection point to the Internet of. the terminal. Node mobility can be broken down into two. forms of mobility: wide area mobility and local mobility.

UNIT -IV
APPLICATION
PART A

1. **What is proxying?**

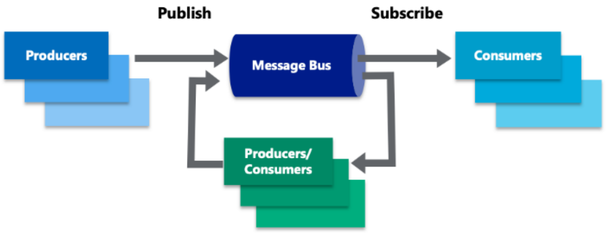
   It works by accessing the internet on behalf of the user while hiding their identity and computer information. An anonymous proxy is best suited for users who want to have full anonymity while accessing the internet.

2. **What are the commonly addressed issues in the application of 6LOWPAN?**

   - Link layer
   - Networking
   - Host issues
   - Compression
   - Security

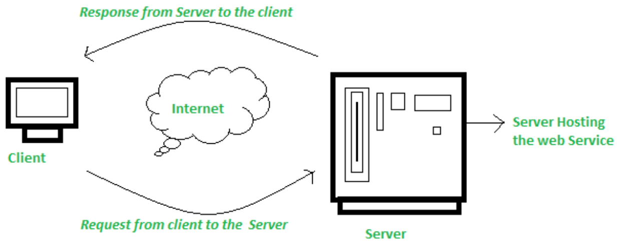
3. **What is publish/subscribe?**

   Publish/Subscribe is an interaction pattern that characterizes the exchange of messages between publishing and subscribing clients. Subscribers express interest in receiving messages and publishers simply publish messages without specifying the recipients for a message.



4. **Define web service.**

   A web service is a software system that supports interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically, web Service Definition Language, or WSDL). web services fulfill a specific task or a set of tasks.


Response from Server to the client
Internet
Client
Server Hosting
the web Service
Request from client to the Server
Server

5. **What is a method?**
A Service based web service interface is typically designed with a single URL that implements several Remote Procedure-Calls (RPCs) called method.

6. **Name two commonly used web service protocols in 6LOWPAN.**
   - MQTT-S
   - ZigBee Cap

7. **Does SIP do keep alive?**
SIP itself doesn't have a keep alive mechanism during call.

8. **What is SIP? Where does it lie on OSI layer?**
SIP is a session-based protocol in the OSI model, or application-layer protocol in the TCP/IP model, that enables the creation, management, and tear-down of SIP traffic for VoIP, as well as other messaging and media applications. It lies in application layer.

9. **What are the different between MQTT and MQTT-S?**
MQTT is a widely used network protocol in IoT for sending messages between devices and a server. To keep the connection secure, MQTTS is normally used. Unfortunately, the added security from MQTT to MQTTS requires more traffic and drains device batteries quicker.

10. **What are the layers of BACnet?**
The four layers from the OSI model within the BACnet architecture are:
    - Application.
    - Network.
    - Data Link.
    - Physical.

11. **What are the two modes in which the application protocol in Gateway approach function?**
Gateway can function in two modes
Transparent mode, where the connection to the broker is maintained for each or in.
Aggression mode, where the gateway aggregates messages from all clients into a single broker connection

12. **Explain the disadvantages of SNMP.**
    - The network's bandwidth is reduced as a result of this protocol.
    - Some of the most serious security problems include access control, authentication, and data privacy.
    - SNMP works with data that is neither detailed nor well structured.

13. **Differentiate RTP and RTCP.**

RTP	RTCP
This protocol enables the transport of real-time applications with features like security, content identification, loss detection, timing reconstruction, etc	This protocols transports media connection statistics and information such as the number of packets delivered, delay fluctuation, packet misplacement, packet delay, etc.

This protocol only provides a method for transferring real-time traffic over a network.	This protocol provides the appropriate delivery quality of the data transmitted via the RTP protocol.

14. If Zigbee uses horizontal or vertical approach. Justify.

Zigbee makes use of a vertical profile approach over the ZAL and ZCL, with profile for different industry application such as the Zigbee Home Automation Profile (ZigbeeHA) or the Zigbee Smart Energy Profile (ZigbeeSE).

15. What are the applications of BACnet protocol?

BACnet was designed to allow communication of building automation and control systems for applications such as heating, ventilating, and air-conditioning control (HVAC), lighting control, access control, and fire detection systems and their associated equipment.

16. Define networking.

Cellular, satellite, Wi-Fi and Ethernet can also be used. Connectivity options have tradeoffs in terms of power consumption, range and bandwidth, all of which must be considered when choosing connected devices and protocols for an IoT application.

17. What are the types of protocol Paradigms

- End-to-End paradigms
- Streaming
- Session
- Publish/Subscribe
- Web service

18. Write the disadvantages of Gateway approach.

- Complexity: The configuration and management of a gateway can be complex.
- Cost: A hardware gateway can be expensive.

19. What are elements used to made MQTT-S Architecture?

- MQTT brokers
- MQTT-S gateway
- MQTT-S forwarders
- MQTT-S clients.

20. Define Konnex (KNX).

KNX stands for "Konnex" or "connectivity" (connection) and is a field bus for building automation. KNX emerged from the merger of the European organizations EIBA, EHSA and BCI, which aimed at a common standard for the fieldbuses existing at that time.

PART B &C

1. **Explain the operation of MQTTS protocol with relevant diagram.**

MQTT is a standards-based messaging protocol, or set of rules, used for machine-to-machine communication. Smart sensors, wearables, and other Internet of Things (IoT) devices typically have to transmit and receive data over a resource-constrained network with limited bandwidth. These IoT devices use MQTT for data transmission, as it is easy to implement and can communicate IoT data efficiently. MQTT supports messaging between devices to the cloud and the cloud to the device.

The MQTT protocol has become a standard for IoT data transmission because it delivers the following benefits:

Lightweight and efficient

MQTT implementation on the IoT device requires minimal resources, so it can even be used on small microcontrollers. For example, a minimal MQTT control message can be as little as two data bytes. MQTT message headers are also small so that you can optimize network bandwidth.

Scalable

MQTT implementation requires a minimal amount of code that consumes very little power in operations. The protocol also has built-in features to support communication with a large number of IoT devices. Hence, you can implement the MQTT protocol to connect with millions of these devices.

Reliable

Many IoT devices connect over unreliable cellular networks with low bandwidth and high latency. MQTT has built-in features that reduce the time the IoT device takes to reconnect with the cloud. It also defines three different quality-of-service levels to ensure reliability for IoT use cases— at most once (0), at least once (1), and exactly once (2).

Secure

MQTT makes it easy for developers to encrypt messages and authenticate devices and users using modern authentication protocols, such as OAuth, TLS1.3, Customer Managed Certificates, and more.

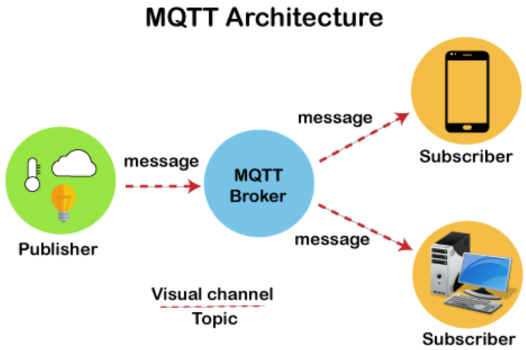
Well-supported

Several languages like Python have extensive support for MQTT protocol implementation. Hence, developers can quickly implement it with minimal coding in any type of application.

Characteristics of MQTT

- It is a machine-to-machine protocol, i.e., it provides communication between the devices.
- It is designed as a simple and lightweight messaging protocol that uses a publish/subscribe system to exchange the information between the client and the server.

- It does not require that both the client and the server establish a connection at the same time.
- It provides faster data transmission, like how WhatsApp/messenger provides a faster delivery. It's a real-time messaging protocol.
- It allows the clients to subscribe to the narrow selection of topics so that they can receive the information they are looking for.



2. **Define industry-based protocols. Explain any two protocols in detail.**

Industrial Protocols are communications protocols that ensure connectivity between machines, devices, and systems as part of an industrial network. Communication protocols enable industrial communication so managers can have greater visibility and control of their operations. With connected PLCs, machine controls, HMIs, sensors, and systems, manufacturers can overcome data siloes and drive industrial automation.

Historically, industrial communication was based on serial connections, resulting in many protocols that continue to be used today, such as Modbus and Profibus. The industry as a whole has begun to move to industrial ethernet communication protocols. The reason for this is that Ethernet is faster, more reliable, and has greater flexibility compared to serial communication. This has resulted in industrial protocols such as EtherNet/IP and Profinet.

There are now many, many communications protocols available, depending on various factors including equipment and devices in use, networks, and the goal of the control system.

there are many industrial protocols available. Here is a list that includes many of the existing protocols, but it is by no means comprehensive:

ANSI C12.18
ANSI C12.21
ANSI C12.22
AS-i
BSAP
CC-Link Industrial Networks
CIP (Common Industrial Protocol)
Controller Area Network or CAN bus
ControlNet

Data Distribution Service (DDS).

Data Distribution Service (DDS).

The Data Distribution Service (DDS) for real-time systems is an Object Management Group (OMG) machine-to-machine (sometimes called middleware or connectivity framework) standard that aims to enable dependable, high-performance, interoperable, real-time, scalable data exchanges using a publish–subscribe pattern. DDS addresses the real-time data exchange needs of applications within aerospace, defense, air-traffic control, autonomous vehicles, medical devices, robotics, power generation, simulation and testing, smart grid management, transportation systems, and other applications.

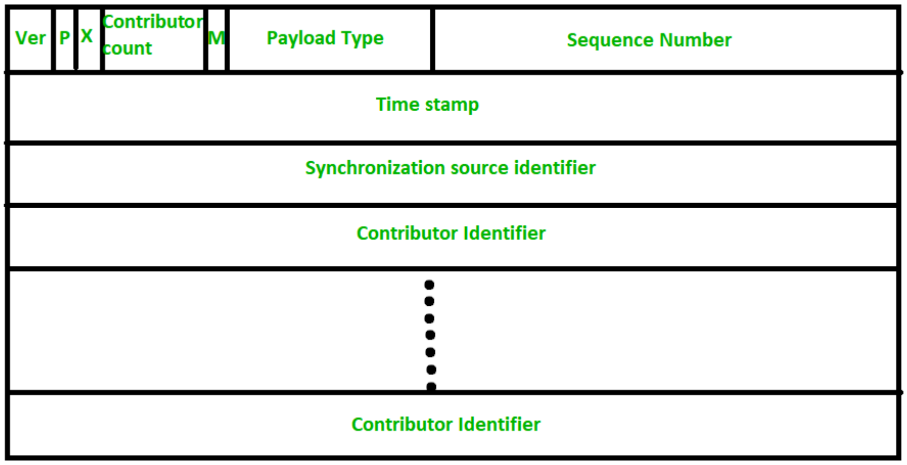
CIP (Common Industrial Protocol):

Common Industrial Protocol (CIP) CIP provides a wide range of standard objects and services for access to data and for control of network devices via so-called "implicit" and "explicit" messages. The CIP data packets are encapsulated before they will be sent with standard TCP or UDP telegrams on the Ethernet.

3. **Briefly describe the function of RTP header structure.**

A protocol is designed to handle real-time traffic (like audio and video) of the Internet, is known as Real Time Transport Protocol (RTP). RTP must be used with UDP. It does not have any delivery mechanism like multicasting or port numbers. RTP supports different formats of files like MPEG and MJPEG. It is very sensitive to packet delays and less sensitive to packet loss.

RTP Header Format : The diagram of header format of RTP packet is shown below:



header format of RTP is very simple and it covers all real-time applications. The explanation of each field of header format is given below:Version : This 2-bit field defines version number. The current version is 2.

1. P – The length of this field is 1-bit. If value is 1, then it denotes presence of padding at end of packet and if value is 0, then there is no padding.

2. X – The length of this field is also 1-bit. If value of this field is set to 1, then its indicates an extra extension header between data and basic header and if value is 0 then, there is no extra extension.
3. Contributor count – This 4-bit field indicates number of contributors. Here maximum possible number of contributors is 15 as a 4-bit field can allows number from 0 to 15.
4. M – The length of this field is 1-bit and it is used as end marker by application to indicate end of its data.
5. Payload types – This field is of length 7-bit to indicate type of payload. We list applications of some common types of payload.
6. Sequence Number – The length of this field is 16 bits. It is used to give serial numbers to RTP packets. It helps in sequencing. The sequence number for first packet is given a random number and then every next packet's sequence number is incremented by 1. This field mainly helps in checking lost packets and order mismatch.
7. Time Stamp – The length of this field is 32-bit. It is used to find relationship between times of different RTP packets. The timestamp for first packet is given randomly and then time stamp for next packets given by sum of previous timestamp and time taken to produce first byte of current packet. The value of 1 clock tick is varying from application to application.
8. Synchronization Source Identifier – This is a 32-bit field used to identify and define the source. The value for this source identifier is a random number that is chosen by source itself. This mainly helps in solving conflict arises when two sources started with the same sequencing number.
9. Contributor Identifier – This is also a 32-bit field used for source identification where there is more than one source present in session. The mixer source use Synchronization source identifier and other remaining sources (maximum 15) use Contributor identifier.

4. Explain the SNMP components with neat diagram.

SNMP is an application layer protocol that uses UDP port number 161/162.SNMP is used to monitor the network, detect network faults, and sometimes even used to configure remote devices.

SNMP components

There are 3 components of SNMP:

SNMP Manager

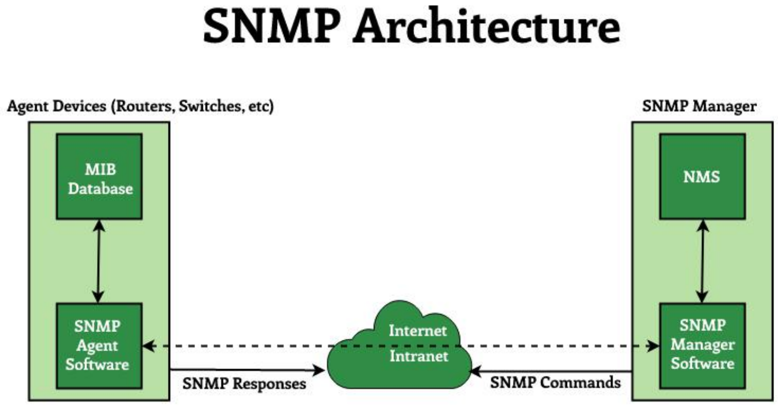
It is a centralized system used to monitor network. It is also known as Network Management Station (NMS)

SNMP agent

It is a software management software module installed on a managed device. Managed devices can be network devices like PC, routers, switches, servers, etc.

Management Information Base

MIB consists of information on resources that are to be managed. This information is organized hierarchically. It consists of objects instances which are essentially variables.



SNMP messages

Different variables are:

Get Request –

SNMP manager sends this message to request data from the SNMP agent. It is simply used to retrieve data from SNMP agents. In response to this, the SNMP agent responds with the requested value through a response message.

GetNextRequest –

This message can be sent to discover what data is available on an SNMP agent. The SNMP manager can request data continuously until no more data is left. In this way, the SNMP manager can take knowledge of all the available data on SNMP agents.

GetBulkRequest –

This message is used to retrieve large data at once by the SNMP manager from the SNMP agent. It is introduced in SNMPv2c.

SetRequest –

It is used by the SNMP manager to set the value of an object instance on the SNMP agent.

Response –

It is a message sent from the agent upon a request from the manager. When sent in response to Get messages, it will contain the data requested. When sent in response to the Set message, it will contain the newly set value as confirmation that the value has been set.

Trap –

These are the message sent by the agent without being requested by the manager. It is sent when a fault has occurred.

InformRequest –

It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to send trap message continuously until it receives an Inform message. It is the same as a trap but adds an acknowledgement that the trap doesn't provide.

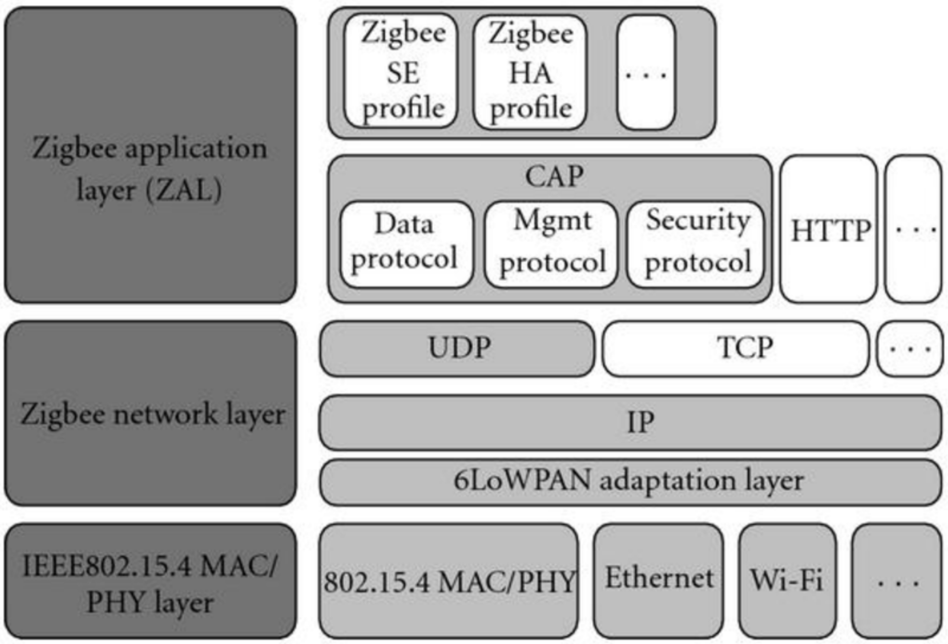
SNMP security levels –

It defines the type of security algorithm performed on SNMP packets. These are used in only SNMPv3. There are 3 security levels namely:

NoAuthNoPriv –

This (no authentication, no privacy) security level uses a community string for authentication and no encryption for privacy.

5. **Explain the protocol stack of CAP protocol.**



6. **Describe the design issues in the applications of 6LOWPAN**
   - It is less secure than zigbee.
   - It has less immunity to interference than wifi or bluetooth devices.
   - It supports short range without mesh topology.
     - Link layer
     - Networking
     - Host issues
     - Compression
     - Security

UNIT-5 TOOLS
PART A

1. **List the challenges of sensor network programming.**
   Challenges in such WSN include high bandwidth demand, high energy consumption, quality of service (QoS) provisioning, data processing and compressing techniques, and cross-layer design. physical environment.
2. **Write the three categories of sensor node hardware.**
   As wireless sensor nodes are typically very small electronic devices, they can only be equipped with a limited power source of less than 0.5-2 ampere-hour and 1.2-3.7 volts. Sensors are classified into three categories: passive, omnidirectional sensors; passive, narrow-beam sensors; and active sensors.
3. **What are the characteristics of Berkeley mote family?**
   The first three motes have an 8-bit Atmel ATmega processor, 128 KB instruction memory (FLASH) and 4 KB RAM. The CPU is clocked at 4 MHz on the Mica2dot and at 7.37 MHz on the Mica2 and MicaZ. The Telos has an 8 MHz, 16-bit TI MSP430 processor, 48 KB FLASH and 10 KB RAM.
4. **Point out the two-CPU design of MICA motes.**
   The MICA motes have a two-CPU design. The main microcontroller (MCU), an Atmel ATmega103L, takes care of regular processing. A separate and much less capable coprocessor is only active when the MCU is being reprogrammed. The ATmega103L MCU has integrated 512 KB flash memory and 4 KB of data memory.
5. **Outline the transmission characteristics of MICA motes.**
   It operates in an ON/OFF key mode at speeds up to 50 Kbps. Control signals configure the radio to operate in either transmit, receive, or power-off mode. The radio contains no buffering, so each bit must be serviced by the processor in time.
6. **Name the features of Node-Level Software Platforms**
   A typical operating system abstracts the hardware platform by providing a set of services for applications, including file management, memory allocation, task scheduling, peripheral device drivers, and networking.
7. **Create the two representative examples of node-level programming.**
   Depending on how the time is advanced in the simulation, there are two types of execution models: cycle-driven simulation and discrete-event simulation.
8. **How does TinyOS support Berkeley mote?**
   TinyOS programs are built of software components, some of which present hardware abstractions. Components are connected to each other using interfaces. TinyOS provides interfaces and components for common abstractions such as packet communication, routing, sensing, actuation and storage.
9. **Develop the application example of TinyOS.**
   TinyOS is an embedded, component-based operating system and platform for low-power wireless devices, such as those used in wireless sensor networks (WSNs), smartdust, ubiquitous computing, personal area networks, building automation, and smart meters.
10. **Express the need for nesC.language for sensor network programming**
    nesC (pronounced "NES-see") is a component-based, event-driven programming language used to build applications for the TinyOS platform. TinyOS is an operating environment designed to run on embedded devices used in distributed wireless sensor networks.
11. **Interpret about the component interfaces of nesC.**

There are two types of components in nesC: modules and config- urations. Modules provide application code, implementing one or more interfaces. Configurations are used to wire other components together, connecting interfaces used by components to interfaces provided by others.

12. Relate the TinyGALS with TinyOS

The TinyGALS code generation toolset was designed to be compatible with software components written for TinyOS (version 0.6.1). TinyOS is a component-based runtime environment for the Motes

13. Identify the components of node-level simulator.

Components of Node-Level Simulator

Visualization and Statistics. Sensor node model. Communication model. Physical Environment model.

14. Define TOSSIM.

TOSSIM is abbreviated from TinyOS sensor network and it's mainly designed for the discrete event simulator. If we need to compile TinyOS application, TOSSIM framework is best for that kind of compilation in personal computers.

15. **Define COOJA network simulator interface**.

COOJA is a network simulator which permits the emulation of real hardware platforms. COOJA is the application of Contiki OS concentrating on network behavior. COOJA is capable of simulating wireless sensor network without any particular mote.

16. What are the two types of nesC?

nesC, code can be classified into two types: Asynchronous code (AC): Code that is reachable from at least one interrupt handler. Synchronous code (SC): Code that is only reachable from tasks. units by specifying data dependencies among them.

17. What are the types of components in TinyOS?

TinyOS provides interfaces and components for common abstractions such as packet communication, routing, sensing, actuation and storage. TinyOS is fully non-blocking: it has one call stack. Thus, all input/output (I/O) operations that last longer than a few hundred microseconds are asynchronous and have a callback.

18. Explain the difference between provides and uses interfaces in nesC.

The provided interface are intended to represent the functionality that the components provides to its user, the used interface represent the functionality the components needs to perform its job.

19. Distinguish between cycle driven and discrete event simulation.

Cycle based simulators work only with synchronous designs. Event based Simulator: Simulation based on events in logic means that whenever there is change in a input event, the output is evaluated. This makes the simulation very slow compared to Cycle based simulators. Verilog-XL is an event-based simulator.

20. Name the two representative examples of node-level programming tools.

Sensor Node Hardware – Berkeley Motes, Programming Challenges, Node-level software platforms – TinyOS, nesC, CONTIKIOS, Node-level Simulators – NS2 and its extension to sensor networks, COOJA, TOSSIM, Programming beyond individual nodes – State centric programming.

PART-B&C

1. **Define sensor node hardware and explain in detail about three categories of sensor node hardware with examples.**

WSNs are generally composed of a large number of nodes which operate in a specific configuration. Typically, the sensor nodes are autonomous and spatially distributed and cooperate to monitor and to gather environmental conditions. Data processing can be done either in a centralized/decentralized mode or by sending data to a sink which sends them to other networks (e.g., through a gateway). Project, design, prototyping, and utilization of a WSN include a wide range of application-specific constraints.

Though the WSNs are application dependent, it is possible to classify them in relation to common features namely,

1) Self-organization capabilities.
2) Short-range communication and/or star/multihop routing.
3) Centralized or decentralized cooperation of sensor nodes.
4) Capability to modify topology in runtime.
5) Constrains in energy consumption, transmission range, memory, computing power, and security.

- Components of WSN
- Hardware components o sensor node and its work.
- Characteristics of the Sensor Node for WSN Performance Evaluation
- WSN Sensor Node Types based on their Working in the Network

2. **Write a note on Berkeley motes.**

1. The Berkeley motes are a family of embedded sensor nodes sharing roughly the same architecture as that of MICA.
2. Motes are tiny, self-contained, battery powered computers with radio links, which enable them to communicate and exchange data with one another, and to selforganize into ad hoc networks
3. Berkeley mote consists of

i. Micro-controller with internal flash program memory
ii. Data SRAM
iii. Data EEPROM
iv. A set of actuator and sensor devices, including LEDs
v. A low-power transceiver
vi. An analog photo-sensor
vii. A digital temperature sensor
viii. A serial port
ix. A small coprocessor unit

4. Hardware Platform
5. Software platform

3. **What are WSN simulators? Explain with example**

Introduction to Simulators and Various Simulators - COOJA, TOSSIM

1. In order to realize a real scenario or a test bench which provides realistic results, the physical architecture and the hardware development require a lot of resources, and the WSN programming and debug become extremely complex. In this context, wireless sensor network simulation becomes a very important and essential tool which provides good results in a cost effective way.

2. The WSN simulators can be divided into different categories in relation to their features and applications. These categories are namely,

i) Code level simulators.
ii) Topology control simulators.
iii) Environment and wireless medium simulators.

3. Due to the ability to increase the real WSN prototyping, the Cross Levels Simulators, like COOJA, have become an important class of simulators. This kind of simulators operates at three abstraction levels: the network level, the operating system level, and the machine code instruction set level.

4. Although these simulators are open source, flexible, and extensible at all levels, the test interface, the external connection at a physical level and the direct interaction with the process control via the WSN are very poor.

5. In recent years, to solve these problems, a few numbers of co-simulators have been developed which integrate WSN simulators and MATLAB/Simulink tools.

6. The Simulink tool provides a wide range of library and simulation model blocks but does not provide an adequate physical connection with the hardware devices used in a Cyber-Physical System (CPS), and it is not possible to simulate complex systems like WBAN or IEEE1451 standard architecture.

7. The main simulators for WSNs are discussed below:

(1) Avrora. Avrora is an emulator and a code level simulator. It is used to emulate the sensor hardware or to process the program code as it would be on a real hardware device. Avrora is a command-line framework compatible with MEMSIC Mica2 and MicaZ sensor platforms.

(2) TOSSIM. It is an emulator for WSNs running TinyOS. The simulation environment permits creating a common topology which runs exactly the same TinyOS applications.

(3) COOJA. COOJA Simulator, by Swedish Institute of Computer Science, is an open-source simulator for the Contiki sensor node operating system. The simulator operates at three abstraction levels, the code level, the topology control level, and the environment and wireless medium level.

(4) Atarraya. Atarraya is a simulator for topology construction and topology maintenance in WSNs.

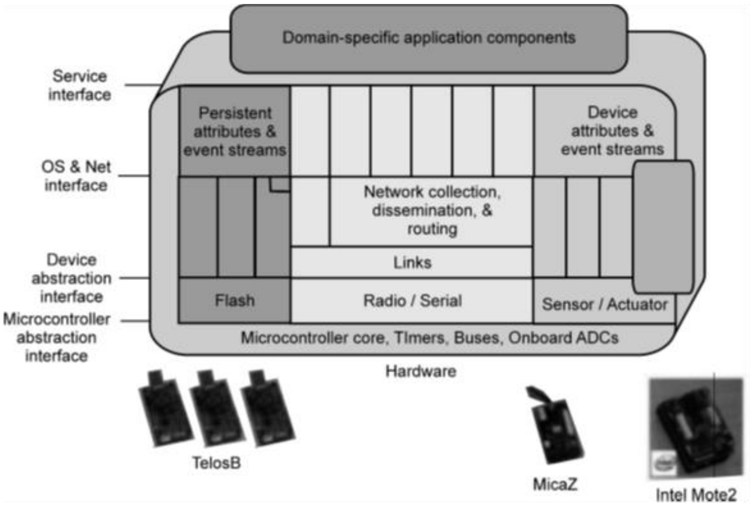
4. Discuss TinyOs for WSN.

Specially designed for sensor network, TinyOS is an open source, flexible, component based and application-specific operating system. TinyOS supports concurrent programs with very low memory requirements. The OS has a footprint that fits in 400 bytes. The TinyOS component library includes network protocols, distributed services, sensor drivers, and data acquisition utility.

TinyOS Architecture

TinyOS falls under the monolithic architecture class which is depicted

TinyOS uses the component model and, according to the requirements of an application, different components are glued together with the scheduler to compose a static image that runs on the mote. A component is an independent computational entity that exposes one or more interfaces. Components have three computational abstractions: commands, events, and tasks. Mechanisms for inter-component communication are commands and events. Tasks are used to express intra-component concurrency. A command is a request to perform some service, while the event signals the completion of the service. TinyOS provides a single shared stack and there is no separation between kernel space and user space.


Domain-specific application components
Service interface
OS & Net interface
Device abstraction interface
Microcontroller abstraction interface
Persistent attributes & event streams
Device attributes & event streams
Network collection, dissemination, & routing
Links
Flash
Radio / Serial
Sensor / Actuator
Microcontroller core, Timers, Buses, Onboard ADCs
Hardware
TelosB
MicaZ
Intel Mote2

- TinyOS Programming Model
- TinyOS Scheduling
- TinyOS Memory Management and Protection
- TinyOS Communication Protocol Support
- TinyOS Resource Sharing
- TinyOs Support for Real-Time Applications

5. What are various challenges faced in sensor network programming

1. Traditional programming technologies rely on operating systems to provide abstraction for processing, I/O, networking, and user interaction hardware. When applying such a model to programming networked embedded systems, such as sensor networks, the application programmers need to explicitly deal with message passing, event synchronization, interrupt handling, and sensor reading.

2. Therefore, an application is typically implemented as a Finite State Machine (FSM) that covers all extreme cases such as unreliable communication channels, long delays, irregular arrival of messages, simultaneous events etc.

3. For resource-constrained embedded systems with real-time requirements, several mechanisms are used in embedded operating systems to reduce code size, improve response time, and reduce energy consumption. Microkernel technologies modularize the operating system so that only the necessary parts are deployed with the application. Real-time scheduling allocates resources to more urgent tasks so that they can be finished early.

4. Event-driven execution allows the system to fall into low-power sleep mode when no interesting events need to be processed. At the extreme, embedded operating systems tend to expose more hardware controls to the programmers, who now have to directly face device drivers and scheduling algorithms, and optimize code at the assembly level. Although these techniques may work well for small, standalone embedded systems, they do not scale up for the programming of sensor networks for two reasons.

5. Sensor networks are large-scale distributed systems, where global properties are derivable from program execution in a massive number of distributed nodes. Distributed algorithms themselves are hard to implement, especially when infrastructure support is limited due to the ad hoc formation of the system and constrained power, memory, and bandwidth resources.

6. As sensor nodes deeply embed into the physical world, a sensor network should be able to respond to multiple concurrent stimuli at the speed of changes of the physical phenomena of interest. There no single universal design methodology for all applications.
7. Depending on the specific tasks of a sensor network and the way the sensor nodes are organized, certain methodologies and platforms may be better choices than others. For example, if the network is used for monitoring a small set of phenomena and the sensor nodes are organized in a simple star topology, then a client-server software model would be sufficient. If the network is used for monitoring a large area from a single access point(i.e., the base station), and if user queries can be decoupled into aggregations of sensor readings from a subset of nodes, then a tree structure that is rooted at the base station is a better choice.
8. However, if the phenomena to be monitored are moving targets, as in the target tracking, then neither the simple client-server model nor the tree organization is optimal. More sophisticated design and methodologies and platforms are required for efficient execution of overall network operations.
6. Explain about the following (a) COOJA (b) TOSSIM.

COOJA:

COOJA is a flexible Java-based simulator designed for simulating networks of sensors running the Contiki operating system. COOJA simulates networks of sensor nodes where each node can be of a different type; differing not only in on-board software, but also in the simulated hardware. COOJA is flexible in that many parts of the simulator can be easily replaced or extended with additional functionality. Example parts that can be extended include the simulated radio medium, simulated node hardware, and plug-ins for simulated input/output.

A simulated node in COOJA has three basic properties: its data memory, the node type, and its hardware peripherals. The node type may be shared between several nodes and determines properties common to all these nodes. For example, nodes of the same type run the same program code on the same simulated hardware peripherals. And nodes of the same type are initialized with the same data memory. During execution, however, nodes' data memories will eventually differ due to e.g. different external inputs. COOJA currently is able to execute Contiki programs in two different ways. Either by running the program code as compiled native code directly on the host CPU, or by running compiled program code in an instruction-level TI MSP430 emulator.

COOJA is also able to simulate nonContiki nodes, such as nodes implemented in Java or even nodes running another operating system. All different approaches have advantages as well as disadvantages. Javabased nodes enable much faster simulations but do not run deployable code. Hence, they are useful for the development of e.g. distributed algorithms. Emulating nodes provides more fine-grained execution details compared to Javabased nodes or nodes running native code. Finally, native code simulations are more efficient than node emulations and still simulate deployable code. Since the need of abstraction in a heterogeneous simulated network may differ between the different simulated nodes, there are advantages in combining several different abstraction level in one simulation. For example, in a large simulated network a few nodes may be simulated at the hardware level while the rest are implemented at the pure Java level. Using this approach combines the advantages of the different levels. The simulation is faster than when emulating all nodes, but at the same time enables a user to receive fine-grained execution details from the few emulated nodes. COOJA executes native code by making Java Native Interface (JNI) calls from the Java environment to a compiled Contiki system. The Contiki system consists of the entire Contiki core, pre-selected user processes, and a set of special simulation glue drivers. This makes it possible to deploy and simulate the same code without any modifications, minimizing the delay between simulation and deployment. The Java simulator has full control over the memory of simulated nodes.

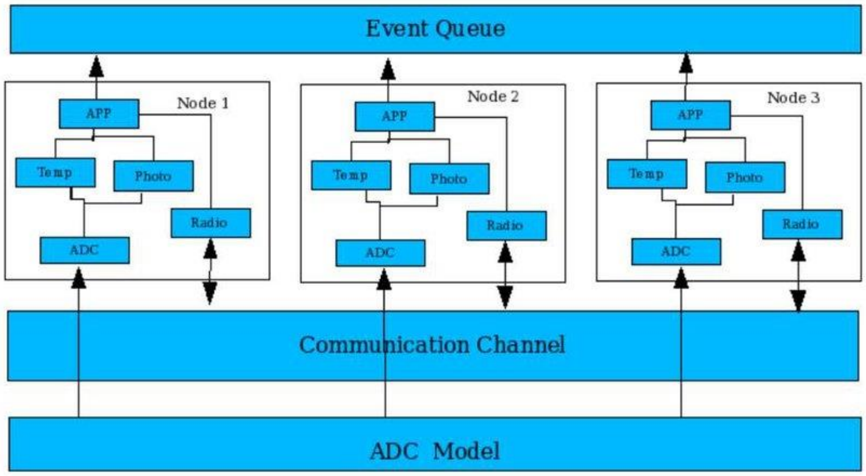
Hence the simulator may at all times view or change Contiki process variables, enabling very dynamic interaction possibilities from the simulator. Another interesting consequence of using JNI is the ability to debug Contiki code using any regular debugger, such as gdb, by at teaching it to the entire Java simulator and breaking when the JNI call is performed.

TOSSIM

TOSSIM is abbreviated from TinyOS sensor network and it’s mainly designed for the discrete event simulator. If we need to compile TinyOS application, TOSSIM framework is best for that kind of compilation in personal computers. It gives permission to the user for the repeatable and controlled environment for debugging, analyzing, and testing the application.

It is represented as a TinyOS wireless sensor network to simulate the discrete event in the distributed system. From the concept of network simulator version 2, TOSSIM is built based on NS2 Simulator. Due to this, the attraction and behavior of the network are based on the granularity of bits and do not base on the packet level. Here, the sensor networks are called motes.

This is the basic concept of TOSSIM in WSN. The overall concept of TOSSIM is to simulate the TinyOS application for discrete events. Then the following topics will go through what is TinyOS event-driven, the reason for using TinyOS, aspects, and suitable sensors for TinyOS. Let we will separately see each topic.


Event Queue
Node 1
APP
Temp
Photo
Radio
ADC
Node 2
APP
Temp
Photo
Radio
ADC
Node 3
APP
Temp
Photo
Radio
ADC
Communication Channel
ADC Model