Sub:	IoT&WSN					Sub Code: 18EC741
Date:	August 2022	Duration:	90 Minutes	Max Marks:	50	Sem / Sec: A,B,C,D

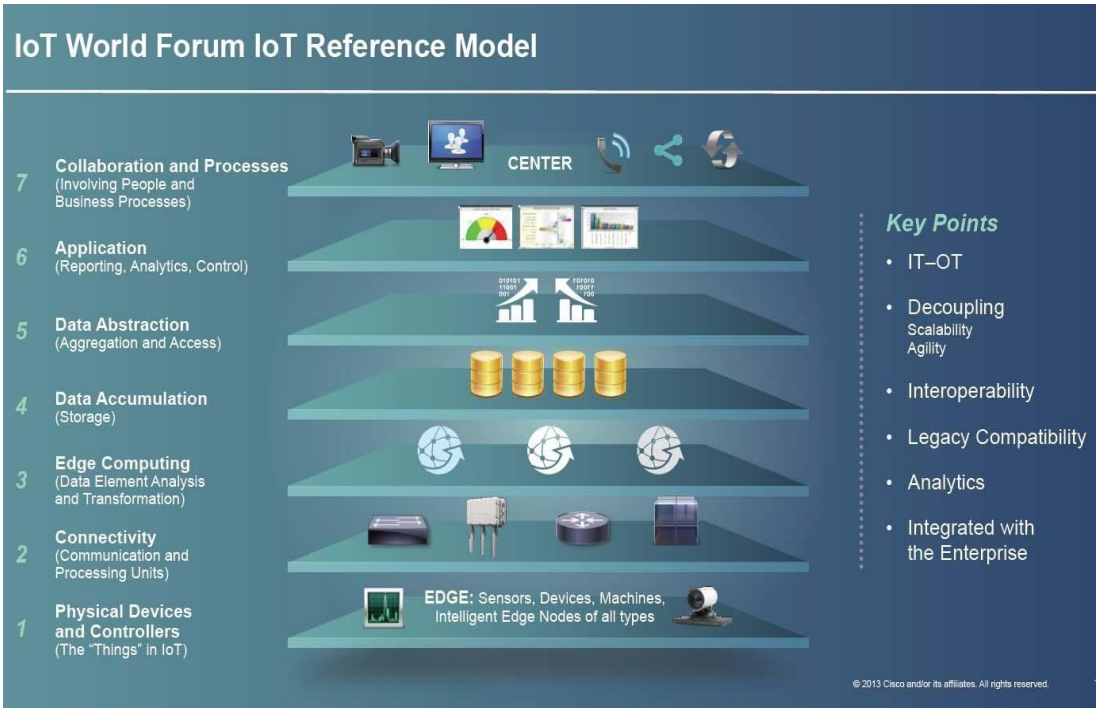
Answer any FIVE FULL Questions

1

a. What is IoT? Explain CISCO Seven leveled reference model for IoT. [8]
b. With a neat sketch, explain IETF suggested modified OSI model for IoT/M2M systems. [8]
c. Explain how data enrichment can be achieved before data dissemination to the network. [4]

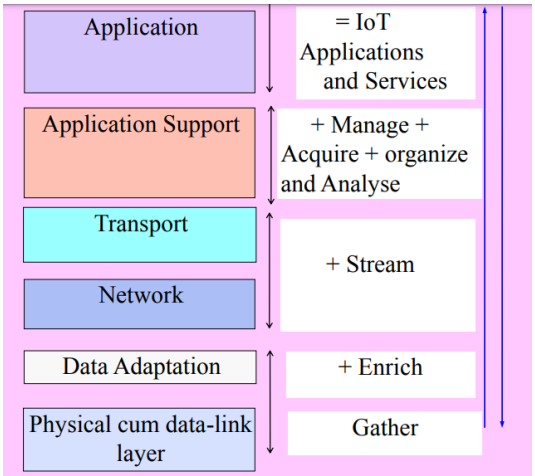
a. The Internet of Things (IoT) describes the network of physical objects—"things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.

By CISCO Seven leveled reference model for IoT



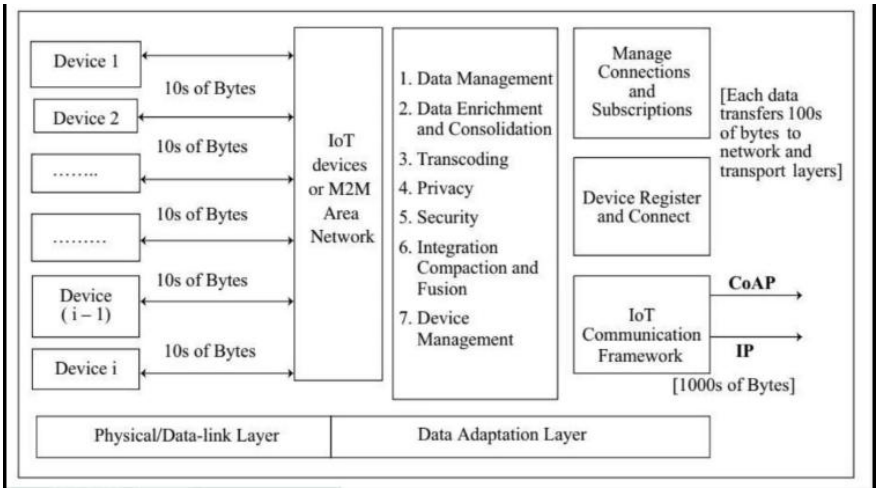
- A reference architecture of IoT
- The IOT reference model has 7 levels called "LAYERS" OR "TIERS".
- Each level is defined with some terminology.
- Each level performs some specific function.
- The model describes how the task at each layer should be handled to maintain simplicity and scalability.
- IN IOT the data flows in both directions i.e.
  From top to bottom (LAYER 7 to LAYER 1) – control pattern. From bottom to top (LAYER 1 to LAYER 7) – monitoring pattern
  But Basically follows top-down approach (means consider top layer design first and then move to the lowest).
- It defines basic architectural building blocks and their integration capability into multi-tiered systems.
- The reference model defining relation-ships among various IoT verticals, for example, transportation and healthcare
- Gives a blueprint for data abstraction
- Recommends quality 'quadruple' trust
- "Protection, Security, Privacy, and Safety"
- Defines no new architecture and no reinvent but existing architectures congruent with it

b. Modified OSI model for IoT/M2M systems



Layer 1: Smart sensing and data-link circuit with each streetlight for transferring the sensed data to the layer 2: Data Adaptation the group controller receives data of each group through Bluetooth or ZigBee, then aggregates and compacts the data for communication to Internet.
Layer 3: Network stream on the Internet to next layer •
Layer 4: Transport layer for device identity management, identity registry and data routing to next layer
Layer 5: Application support by data managing, acquiring, organizing and analyzing.
Layer 6: Application a remotely stored service program which issues the commands or programs the firmware at the service controllers
• Service controllers switch on-off, and monitor each group of streetlights in whole of the city.

c. Data enrichment can be achieved before data dissemination to the network.



Physical Layer:

- ❑ It is also called perception layer or object layer or device layer.
- ❑ The physical layer consists of the physical device called as 'Things' which can be sensors, actuators, RFID tags.

Adaptation Layer:

- □ The main function of data adaptation layer is data enrichment.
- □ Gateway is considered to work at data adaptation layer.

Gateway and network layer and transport layer
Both the layers deals with Data streaming i.e. transfer of data at a steady high-speed rate sufficient to support such applications as high- definition television (HDTV)

Transport layer:

The main functions of this layer are:

- □ Forwarding the data coming from sensors to the next upper management layer.
- □ It provides sufficient security features, bandwidth management etc.

Gateway layer:

The main functions of this layer are:

1) Routing the data coming from sensors to the next upper management layer
2) This layer is responsible for managing the traffic between networks that uses the different protocols.
3) This layer is responsible for protocol translation and other interoperability tasks
4) The IOT gateway device is employed because some of the devices can't directly communicate to the front end applications as there is no network stack present for internet connectivity, hence gateways acts as proxy.

Application support layer/middleware layer:

□ This layer is also called as service management layer or processing layer.

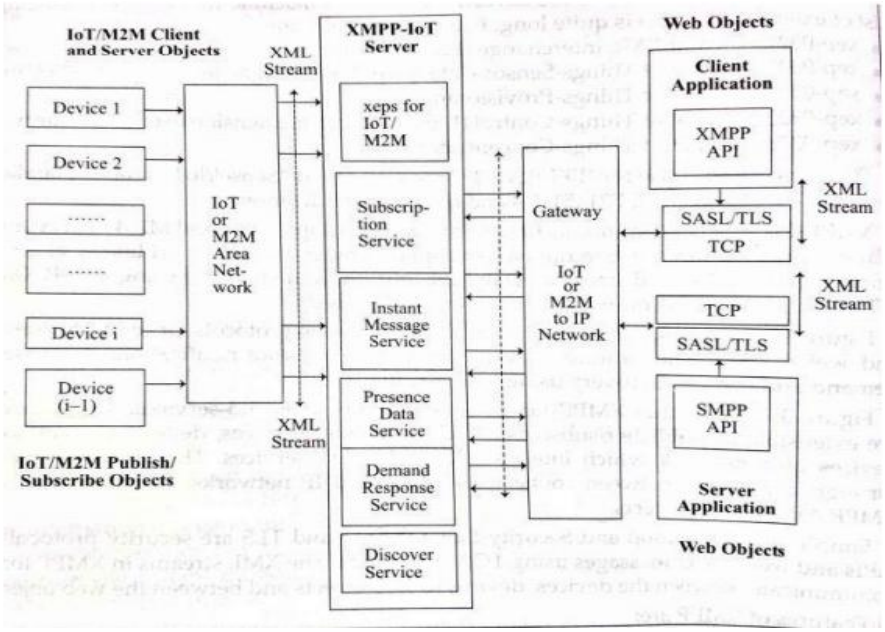
□It is called as application support as it allows the IOT application programmer to work with heterogeneous objects without consideration to specific hardware.

2

A. Define XMPP protocol with necessary diagram. [8]
B. Explain M2M communication. Explain M2M architecture. [8]
C. List the functionalities of MQTT broker [4]

A. XMPP protocol

X- Extensible: XMPP is designed to be extensible, in has been designed to grow and accommodate changes.
M-Messaging: XMPP has been designed to send instant message.
P-Presence: The presence indicator tells the server that you are online/offline/busy.
P-Protocol: XMPP is a protocol; a set of standards to talk to each other. It is widely used across web but is unadvertised.



B. M2M communications

It refers to automated applications which involve machines or devices communicating through a network without human intervention. Sensors and communication modules are embedded within M2M devices, enabling data to be transmitted from one device to another device through wired and wireless communications networks.

M2M Architecture:
Divided into three domains
1) M2M device domain
2) M2M network domain
3) M2M application domain

1)M2M device domain:
It consists of three subparts
a) Physical devices and controllers
b) Communication interface
c) Gateway (BS)

Physical devices and controllers: autonomously. Two types of devices –ones capable of directly connecting to the network and the others requires an M2M gateway in order to connect to the network

Communication interface: It is the port or processing unit that receives data from one interface and transmit it to other interface.

Gateway Gateways and routers are the endpoints of the operator's network in scenarios where sensors and M2M devices do not connect directly to the network

2) M2M Network Domain (Communication Networks)
It consists of M2M core and M2M service capabilities.
□M2Mcore covers the communications between the M2M Gateway(s) and M2M application(s), e.g. LTE, WiMAX, and WLAN.
□M2Mservice capabilities include network functions to support M2M applications. It also deals with management functions like device identity management, data storage, data collection, analysis, aggregation etc.

3) M2M application domain Two types of applications -M2M applications and client applications M2M applications: These applications are located on the servers, interacts with M2M devices. Client applications: These used to serve end-users; either receives services from M2M applications or directly from M2M devices.

C. MQTT Broker: Message Queuing Telemetry Transport

- An open source protocol for machine-to-machine (M2M)/"Internet of Things" connectivity
- (Telemetry dictionary meaning is measuring and sending values or messages to far off places by radio or other mechanism)
- Created by IBM IN 1999, as a constrained environment protocol.
- Designed to provide connectivity (mostly embedded) between applications and middle-wares (M2M/IOT objects) on one side and networks and communications (WEB Objects) on the other side.

Broker:
- The data with a topic is shared from the client/ sensor node to publisher.
- Perform store and forward operation
- Receives the topics from publishers
- Each client that wants to receive messages first subscribes to a certain topic and then

The broker delivers all messages with the matching topic to the client.

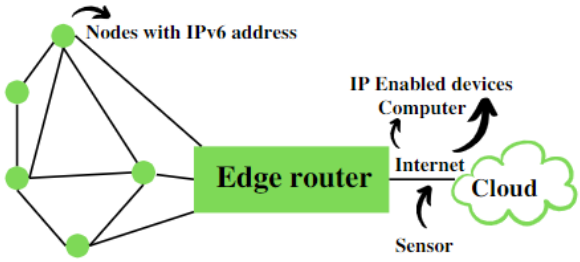
Therefore the clients don't have to know each other. They only communicate over the topic.

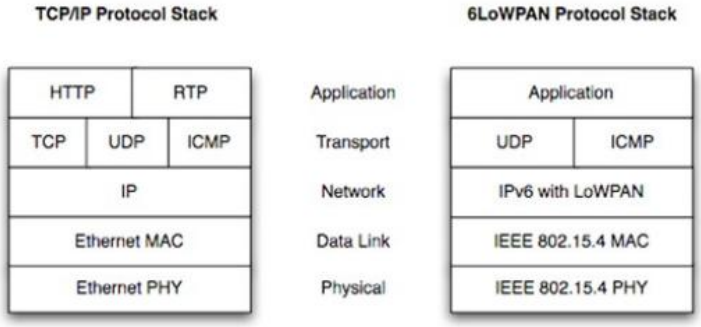
3

a. **With a neat sketch, explain 6lowPAN protocol and its features. [8]**
b. **Explain how packets route over the internet using a set of four routers between source and destination. [6]**
c. **Define cloud computing. Explain different services provided by the cloud computing.[6]**

A. 6lowPAN protocol and its features.

6LoWPAN is an IPV6 protocol, and It's extended from is IPv6 over Low Power Personal Area Network. As the name itself explains the meaning of this protocol is that this protocol works on Wireless Personal Area Network





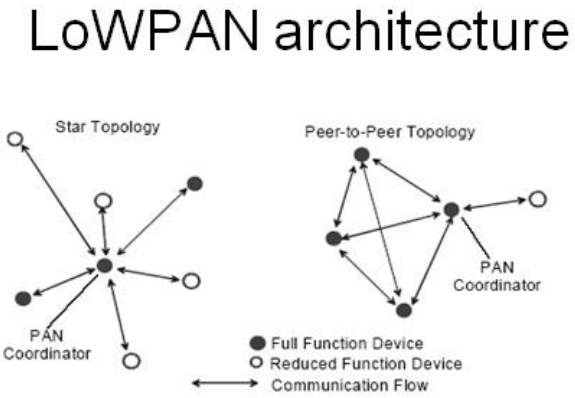


Figure 1—Star and peer-to-peer topology examples

Octets: 2	1	0/2	0/2/8	0/2	0/2/8	variable	2
Frame control	Sequence number	Destination PAN identifier	Destination address	Source PAN identifier	Source address	Frame payload	FCS
		Addressing fields					
MHR						MAC payload	MFR

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
- Small packet size
- 16-bit short or IEEE 64-bit extended media access control addresses
- Low bandwidth. (250/40/20 kbps)
- Topologies include star and mesh
- Low power, typically battery operated
- Relatively low cost
- Networks are ad hoc & devices have limited accessibility and user interfaces
- Inherently unreliable due to nature of devices in the wireless medium

B. Packets routing over the internet using a set of four routers between source and destination.

The Internet Protocol (IP) is the protocol that describes how to route messages from one computer to another computer on the network. Each message is split up into packets, and the packets hop from router to router on the way to their destination. The main steps of routing are:

Step 1: Send packet to router
Computers send the first packet to the nearest router. A router is a type of computing device used in computer networks that helps move the packets along.

Step 2: Router receives packet
When the router receives a packet, it looks at its IP header. The most important field is the destination IP address, which tells the router where the packet wants to end up.

Step 3: Router forwards packet
The router has multiple paths it could send a packet along, and its goal is to send the packet to a router that's closer to its final destination. It does using forwarding table having IP address of next device.

Step 4: Final router forwards message
If all goes well, the packet should eventually arrive at a router that knows exactly where to send it.

C. Cloud computing

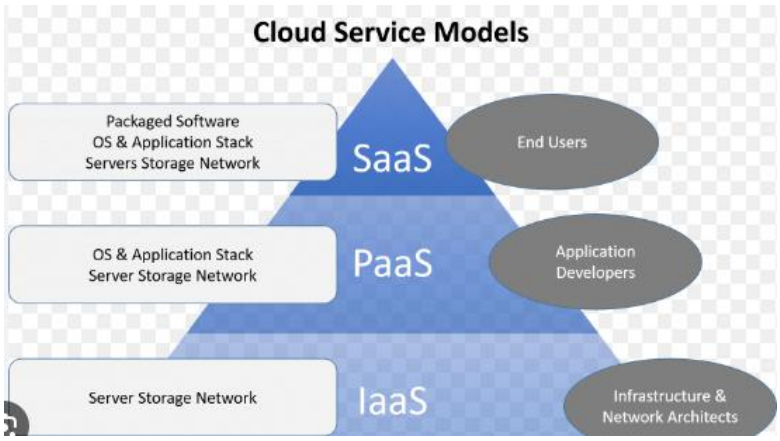
Cloud computing is a method in which resources are retrieved from the Internet through web-based tools and Applications, without using direct connection to a server.

--Cloud-based storage makes it possible to save the files to a remote database instead of keeping them on a hard drive or local storage device.

--It's called cloud computing because it does not require a user to be in a specific location to gain access to it. This type of system allows the users to store files and applications on remote servers, and then access It via the internet any time.

Service Models are the reference models on which the Cloud Computing is based. These can be categorized into three basic service models as listed below:

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)



IaaS is also known as **Hardware as a Service (HaaS)**. It is a computing infrastructure managed over the internet. The main advantage of using IaaS is that it helps users to avoid the cost and complexity of purchasing and managing the physical servers.

PaaS cloud computing platform is created for the programmer to develop, test, run, and manage the applications.

SaaS is also known as "**on-demand software**". It is software in which the applications are hosted by a cloud service provider. Users can access these applications with the help of internet connection and web browser.

4.

a. Explain IoT cloud based data collection, storage and computing using Nimbit server. [8]

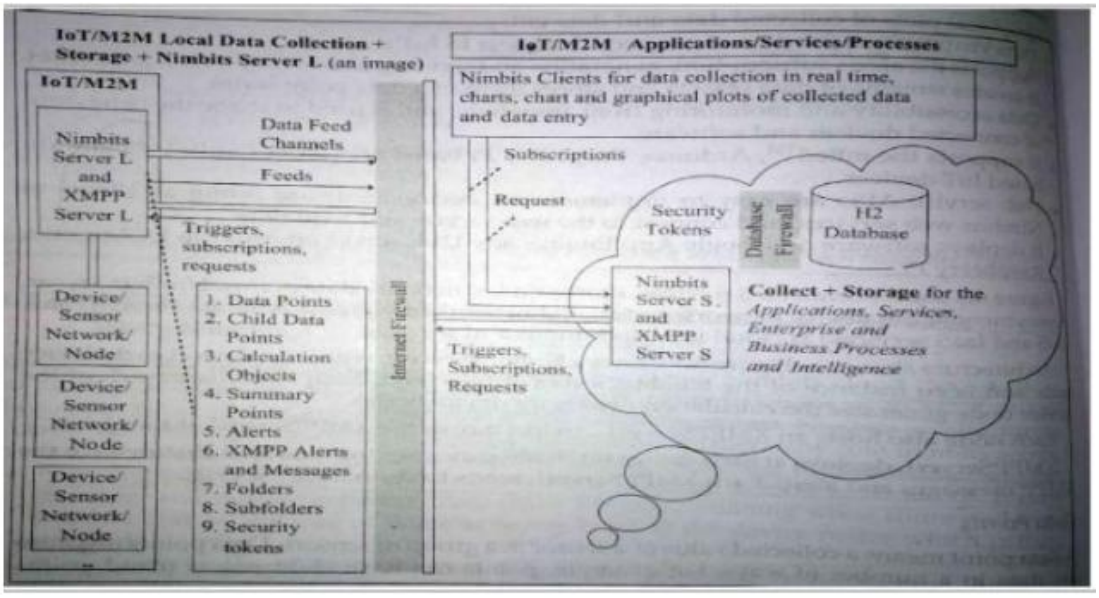
b. Explain the features of HTTP protocol. [6]

c. Explain the cloud computing deployment model. [6]

a. Nimbits enables IoT an open source distributed cloud.

Nimbits server is a web portal and API designed to:

- Provides time-stamping or geo-stamping on incoming data.
- Store and process that time and location stamped data over cloud (pushing the data over cloud and store them in a data point)
- Provide filtering to incoming data from noise, add important changes to it and then generate Trigger events and alerts based on rules and then sending them in real time over internet.
- It provides rule engine for connecting sensors, persons and software to cloud.



Working:

- The Nimbits serverL which is deployed at each device node and is an instance of the NimbitsServerS at the cloud. The server provides time-stamping or geo-stamping on incoming data then do storing, processing, filtering, adding some important changes to it and then trigger events and alerts based on rules and calculations called data feeds (A data feed contains latest updates of current information like events, alerts etc).
- The data feed is sent over data feed channels using XMPP messages and alerts to XMPPServerC.
- Data point means a collected value of a sensor in a group of sensors.
- User can apply formulas (calculations) on single data point

b. The features of HTTP protocol

1) HTTP is an web's application-layer protocol: The Hypertext Transfer Protocol is an web's application-layer protocol for transmitting various forms of data between sever and Client like plaintext, hypertext, image and sound.

2) HTTP is an client server protocol: HTTP is an client server protocol by which two machines communicates by using a reliable, connection oriented transport service such As TCP.

3) HTTP is flexible and connectionless: The HTTP client, i.e. a browser initiates an HTTP request and after a request is made, the client disconnects from the server and waits For a response. The server processes the request and re-establishes the connection with The client to send a response back.

4) HTTP is media independent: It means, any type of data can be sent by HTTP as long as Both the client and the server know how to handle the data content. It is required for the Client as well as the server to specify the content type using appropriate MIME-type.

5) HTTP is a very light protocol: It has a small format and speedy as compared to other Protocol like FTP.

6) HTTP is based on Object Oriented Programming System (OOPS): Methods are applied To the objects identified by URL. A web HTTP server listens to the port 80 only and respond to port 80 only.

c. The cloud computing deployment model

□Deployment models define access method of the cloud.
□Depending upon the access method the cloud are defined as.

- ❖ Public
- ❖ Private
- ❖ Hybrid
- ❖ Community

PUBLIC CLOUD :
The Public Cloud allows systems and services to be easily accessible to the general public. Public cloud may be less secure because of its openness, e.g., e-mail. Some of the examples of companies which provide public cloud facilities are IBM, Google, Amazon, Microsoft, etc. This cloud service is open for use.

Advantages:
• Flexible, Reliable, High Scalable, Low cost

PRIVATE CLOUD :
The Private Cloud allows systems and services to be accessible within an organization. It offers increased security

because of its private nature. For example Hewlett Packard Enterprise (HPE) -- offers the Helion Cloud Suite software, Helion Cloud System hardware

Advantages:
• Highly private and secured: As permit only authorized users to share the resources.
• Control Oriented: As it can be accessed within the organization's boundary.

COMMUNIY CLOUD :
The Community Cloud allows systems and services to be accessible by group of organizations.

Example of such a community is financial institutions/banks, joint business organizations, ventures, research organizations and tenders etc.

Advantages:
· Cost reduction, Improved security, privacy and reliability, Ease of data sharing and collaboration

HYBRID CLOUD :
The Hybrid Cloud is mixture of public and private cloud. For Example Amazon Web Services (AWS) or Microsoft Azure

Advantages:
• Flexible, Secure, Cost Effective, Rich Scalable

5

a. Explain security requirement and threat analysis. [10]

b. Write and explain traffic light control programming using Ardunio.[10]

a. **Security functional group contains five sets of functions which are required for ensuring security and privacy. Five functional components of security are defined in IOT are**:

1) Identity management
2) Authentication
3) Authorization
4) Key exchange and management
5) Trust and reputation

Identity Management:
- An object's identity should always be unique compared to the other objects from its family.
- Unique identity can be called core identity, as an object can also have several temporary identities.
- Devices must establish their identity before they can access gateways and upstream services and apps.

Secure Authentication/Authorization
- IoT devices should be authenticated with strong usernames IDs and password before being allowed to communicate with other IoT devices on the network.
- Authentication token/session should always be unique to each user along with user id, app id and device id.
- System's credentials, application, device and server should be authenticated as spoofed devices could transmit malicious data to other devices and can implement a denial- of-service attack on the IoT network
- Public key cryptography also known as asymmetric encryption keeps the data safe and secure during transmissions.
- Certification Authority (CA): This is effectively done by a issuing a digital certificate to confirm the authenticity of the device, firmware / software updates, and facilitate encrypted communications

Key exchange and management
Key exchange (also key establishment) is a method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm.

Trust and reputation
Trusted IoT Device:
The trusted IoT devices should be able to communicate with the intended hosting services only.
And the firmware / software should be frequently updated.
The Trusted IoT Master:
A trusted master must provide a secure communication with dependent sensor devices, and issue firmware/software updates to those devices and ensures that the code is authentic, unmodified and non-malicious

6) Threat Analysis
7) → Threat analysis means uncovering the security design flaws
8) After specifying stride category, data flow diagram, elements between which interactions occur during the stride and specified the processes which are activated for analysis.
9) ► Stride means taking decisive steps in a specified direction.
10) A threat analysis tool first generated the threats and then analysis the system for threats.

b. Traffic light control using Ardunio Programming:

```
testing phases.*/                                    successful running
int internalLED = 13;
/* Variables are written using a lower case first character */
int ledR0, ledY0, ledG0, ledR1, ledY1, ledG1, ledR2, ledY2, ledG2, ledR3,
ledY3, ledG3;
Assign the pins to the respectively connected LEDs */
ledR0 = 2; ledY0 = 3; ledG4 = 4; ledR1 = 5; ledY1 = 6;ledG1 = 7; ledR2 = 8;
ledY2 = 9; ledG2 = 10; ledR3 = 11; ledY3 = 12; ledG3 = 14;
/* Declare Functions for sequences of traffic lights ON-OFF as follows: */
   void north_south_Green() {
digitalWrite (ledR0, LOW); digitalWrite (ledY0, LOW); digitalWrite (ledG0,
HIGH);
digitalWrite (ledR2, LOW); digitalWrite (ledY2, LOW); digitalWrite (ledG2,
HIGH);
   };
/* Function Switch RED ON for East and West pathways*/
   void east_west_Red() {
```

```
digitalWrite (ledR1, HIGH); digitalWrite (ledY1, LOW);digitalWrite (ledG1,
LOW);
digitalWrite (ledR3, HIGH); digitalWrite (ledY3, LOW); digitalWrite (ledG3,
LOW);
   };
/*************************************************************/
void setup ( ) {
/* GPIO pins 2 to 12 and 14 are thus assigned port numbers corresponding to 12
external LEDs, R0, Y0, G0, R1, Y1, G1, R2, Y2, G2, R3, Y3, and G3.*/
/* Assign mode of each pin as output */
pinmode (ledR0, OUTPUT); // Constants are written in Upper Cases
pinmode (ledY0, OUTPUT);
.
pinmode (ledY3, OUTPUT);
pinmode (ledG3, OUTPUT);
/* Let Pin 13 be used for indicating successful running of the developed codes
during testing phases. Initialise internal Port 13 Digital IO Pin LED for
test.*/
```

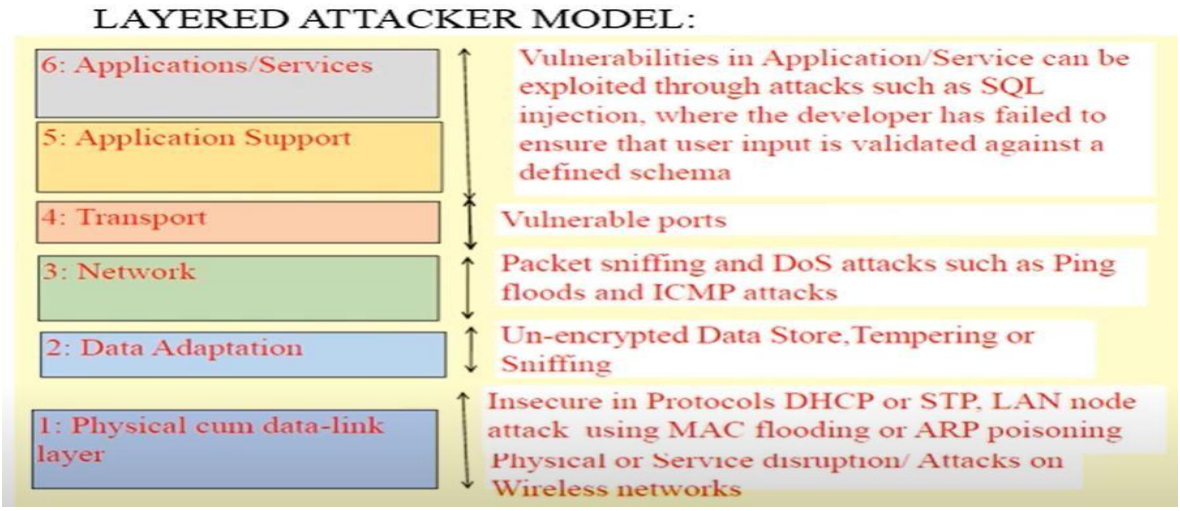
6.

a. What is IoT Security Tomography? Explain in detail the layered attack model. [10]

b. Explain five levels for software development for applications and services for IoT and M2M. [10]

a. Security tomography

It enables finding the attack vulnerable sections/subsections on observation for behaviors using finite number of objects or threats in a complex set of subsystems



b. Five levels for software development for applications and services for IoT and M2M.

There is need of developing the software at five levels:
1) Physical cum Data link layer
2) Connect to internet
3) Collect and assemble of information
4) Manage and analyze of information
5) Application and services in IOT/M2M applications and services.
Devices, Gateways, internet and web/cloud services software-development.

Hence there are five levels of software development required for applications and services in loT/M2M. That are:

1) Physical/data Link and adaptation layers software :
   Provide Gather and consolidate the data from sensors
2) loT/M2M area local network and gateway software.
   Connect to the internet; provide preprocessing of the data collected form sensors.
3) Network and transport layer software
   Collect and assemble of information and event provide management and analysis of information.
4) Application support Layer APIs/Software
   This layer supports services for client and software functions. It decides how the user will use the Data network.
   It allows the client to use the structure. For instance, it supports network-based services to the end-user.
5) Application layers APIs/Software
   The application layer manages all application process based on information obtained from middleware Layer. This application involves sending emails, activating alarm, security system, turn on or off a device, smart watch, smart agriculture, etc.

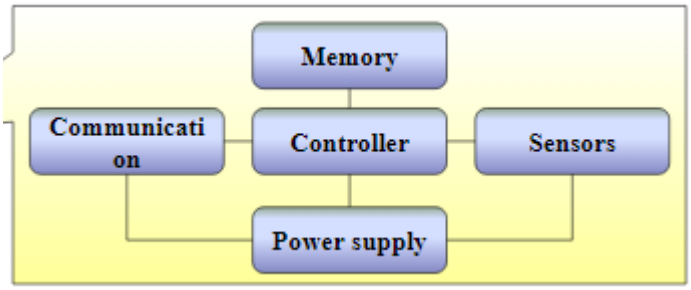
7.

a. Explain the hardware components of a sensor node. [8]

b. Explain the challenges for wireless sensor networks. [6]

c. Explain different types of mobility in WSN. [6]

a. Hardware components of a sensor node:



Mai Controller functionality:

- It is core of a wireless sensor network.
- It collects data from the sensors, processes this data, decides when and where to send it, receives data from other sensor nodes and decides on actuator's behavior.
- It is CPU of sensor node as it executes various programs ranging from time critical signal processing and communication protocols to application protocols.

Communication module:

- The communication module of a sensor node is called "Radio Transceiver".
- The essentially tasks of transceiver is to "transmit" and "receive" data between a pair of nodes.
- Depends upon the choice of transmission medium.

Sensors/Actuators:

- Measure the physical quantity and convert it into a signal which can be read by an observer by an instrument.
- Sensors can be active/passive.
- Actuators are a device or mechanism capable of performing a physical action for example motor, light bulb, LEDs etc.

Memory:

- Memory is required to store programs and intermediate data; usually, different types of memory are used in WSN for programs and data like RAM, ROM and flash memory.

Power supply module

- It should provide as much energy as possible. The power supply can be through batteries and by energy scavenging

b. Challenges for Wireless sensor networks:

Type of service:

It involves the transmission of meaningful information and/ or actions about the given task.

Quality of service:

QOS is the description or measurement of the overall performance of a service.

There are several aspects to measure quality of service such as packet loss, bit rate, throughput, bandwidth, transmission delay, availability, jitter, etc.

Fault tolerance:

Due to depletion of energy node can fail. In case of node failures network should cope up as soon as possible.

Fault tolerance is the ability of the network to sustain the problems like sensor node failures and network should function without any interruption.

Scalability:

Scalability measures the density of the sensor nodes. In some applications, tens of thousands of sensors might be deployed. At any time numbers of nodes can be increased or decreased.

Production costs:

The cost of a single node is very important to justify the overall cost of the networks.

The cost of a sensor node depends upon the application and functionalities.

Lifetime:

Lifetime of a network is a very important figure of merit in WSN.

Most of the nodes are battery operated and have limited power resources. Therefore power sources like solar cells must be available on a sensor node

Programmability:

Nodes must be programmable and their programming must be changeable during the operation when the new task becomes important.

Maintainability:

Here the nodes must adapt it according to the changing environments externally as well as internally.

Survivability in harsh environments

c. Different types of mobility in WSN

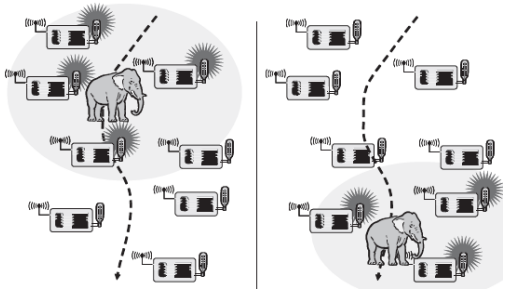
In WSN, mobility can appear in three main forms….

- Node mobility:
- Sink mobility:
- Event mobility

- Node mobility: The wireless sensor nodes themselves can be mobile e.g. in environmental control, livestock surveillance.

- Sink mobility: The information sinks can be mobile but the mobility as an information sink is not the part of sensor network e.g. a human requests some information while walking in a building.

- Event mobility: The objects to be tracked can be mobile. Hence sensor will wake up when object is near, watch their activity and then go back to sleep.



8. 8.

a. Explain optimization goals and figure of merit. [8]

b. Explain Gateway concepts in sensor networks. [8]

c. List the enabling technologies for WSN. [4]

a. Optimization goals and figure of merit.

- The main challenge for a network is how to optimize a network.
- Optimization and figures of merit depend upon certain parameters like:

  - Quality of service
  - Energy efficiency
  - Scalability
  - Robustness

Quality of service involves:
A) Low level networking device observable attributes like: Bandwidth, delay, jitter, packet loss rate
B) High level, user observable also called as subjective attributes like: Quality of voice communication or video transmission.

In WSNs, the high level attribute depends upon the application.

Quality of service: Some generic possibilities are :

- Event detection/reporting probability :
  Means the event that actually happened is detected or not or reported or not to the information sink.

  Event classification error- If events are not only to be detected but also to be classified, the error in classification must be small

- Event detection delay -It is the delay between detecting an event and reporting it to any/all interested sinks

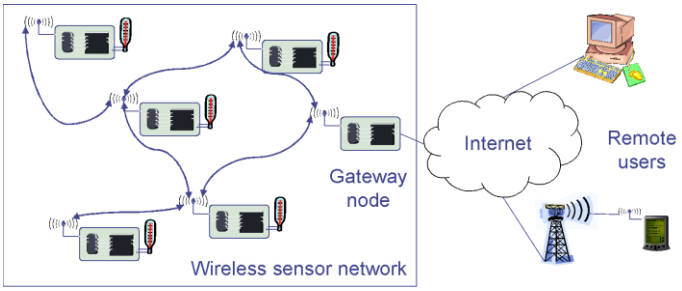
- Energy efficiency:
  The Energy efficiency of the WSN can be increased by considering various aspects.

1) Energy per correctly received bit:
   It defines the average energy consumed in transporting and receiving one bit of information, after considering all possible intermediate hops from source to destination.

2) Energy per reported event:
   It defines the average energy consumed in reporting one event. Since same event can be reported from Various sources. Hence redundant information can be reduced.

B Gateway concepts in sensor networks

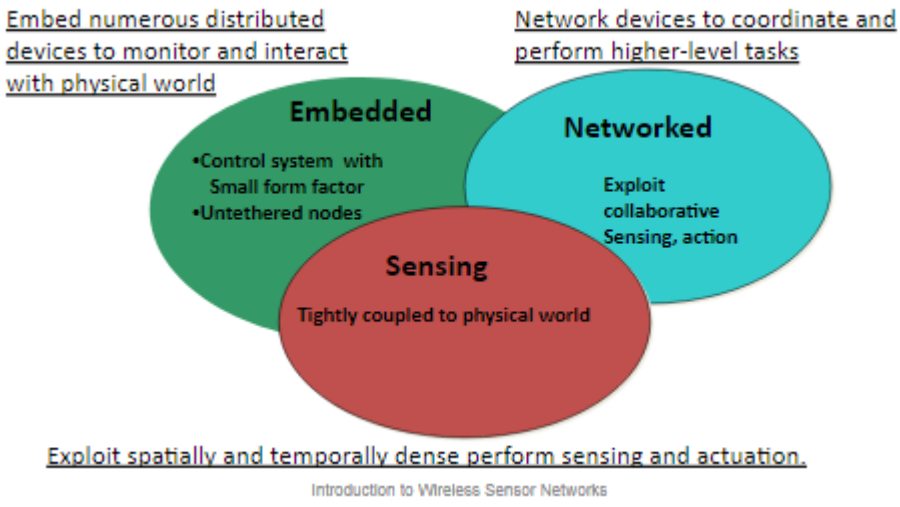
- Gateways allow the WSN to exchange the data with other devices like mobile phones.
- Gateway node bridges a gap between WSN and other communication devices
- Gateway is equipped with a radio transceiver or some standard wireless communication technique like IEEE 802.11



- But here occurs some issues like
- How to handle the several gateways.
- Choose “best” gateway (integrates routing & service discovery)

- Finding the host IP address to which it has to be forwarded.
- Gateway node is required.
- How to find the right WSN in desired location is another problem.
- Addressing of the right sensor in network.
- How to translate from IP protocols to WSN protocols, semantics?
- How to make WSN services accessible from standard web browser.

Enabling technologies for WSN.



9

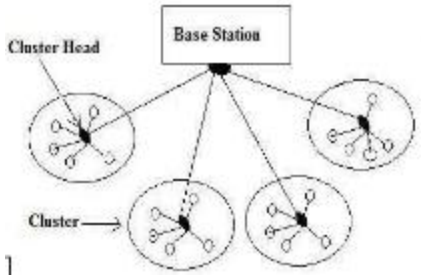
a. Explain LEACH Protocol in sensor network. [10]

B. With neat diagram, explain CSMA protocol. [10]

a **LEACH Protocol**

LEACH (Low-Energy Adaptive Clustering Hierarchy)

- It is self-organizing, adaptive clustering protocol that uses dynamic clustering method.
- Base station (sink) is fixed and away from sensors.



LEACH conserves energy through:

- Aggregation
- Adaptive Clustering
- Nodes in LEACH

All the nodes in the network are homogeneous.

- The LEACH partitions the nodes into ‘clusters ‘(round) and in each cluster elects a dedicated node called ‘Cluster head ‘to avoid excessive energy consumption.
- Cluster head assigns a TDMA schedule to all member nodes which are used to exchange the data between members and cluster head.
- Cluster head aggregates the data from member nodes and transmit it to the sink node.
- If transmission is not there for that time slots, nodes can spend time to sleeping state.

- There is no peer to peer communication.
- LEACH is dynamic because the job of cluster-head rotates.

Nodes in LEACH

- All the nodes in the network are homogeneous.
- The LEACH partitions the nodes into ‘clusters ‘(round) and in each cluster elects a dedicated node called ‘Cluster head ‘to avoid excessive energy consumption.
- Cluster head assigns a TDMA schedule to all member nodes which are used to exchange the data between members and cluster head.
- Cluster head aggregates the data from member nodes and transmit it to the sink node.
- If transmission is not there for that time slots, nodes can spend time to sleeping state.
- There is no peer to peer communication.
- LEACH is dynamic because the job of cluster-head rotates

The Set-Up Phase

- Advertisement
- Election of cluster-heads
- Membership of nodes
- Schedule creation

The Steady-State

- The cluster-head is maintained
- When data is transmitted between nodes

B CSMA Protocol

In Carrier sense multiple Accesses the node sense the channel before transmitting. If the channel is busy then the node selects other random channel, repeats the carrier sensing and after a number of unsuccessful trials it just back-off.

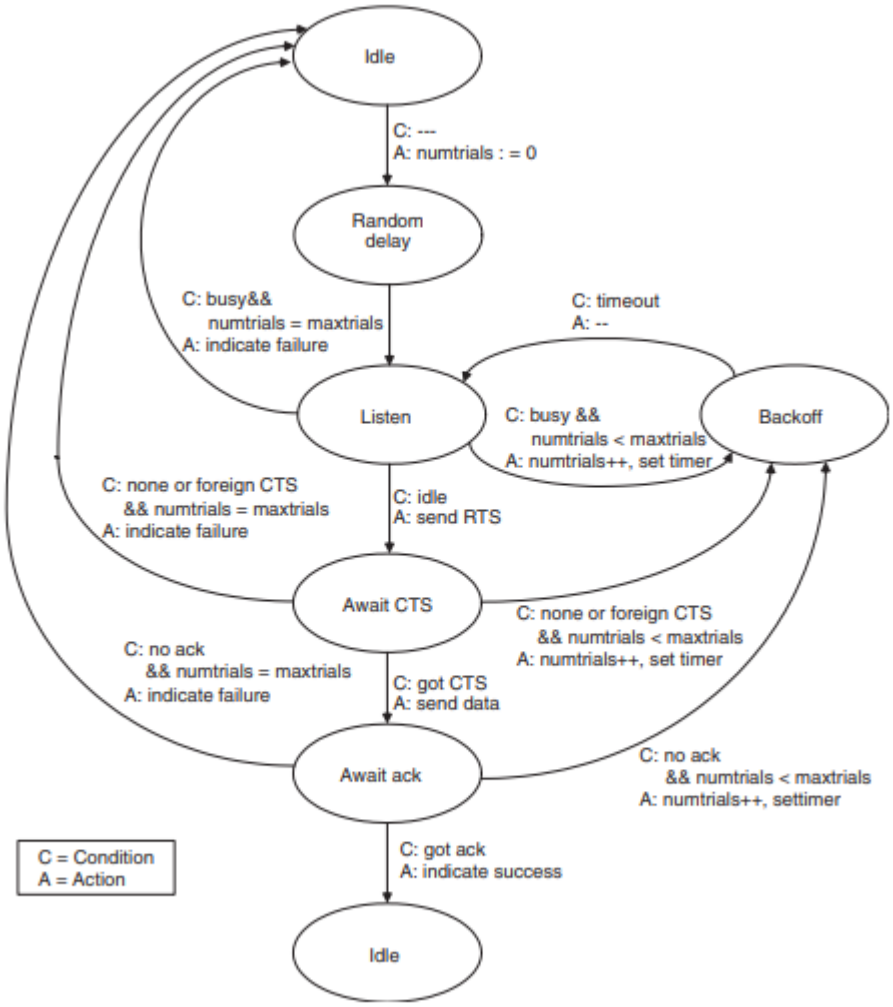


Figure 5.9 Schematic of the CSMA protocol presented in reference [888]

Step 1: ["Idle state"]

- Normally the nodes are in "idle state".

Step 2: ["Random delay"]

- When it receives the packet from upper layer for transmission to lower layer (called as downstream node), it restarts the "Random Delay".
- Counter "numtrials" is =0;
- The purpose of "Random delay" is to desynchronize the nodes if initially synchronized by the external event.

Step 3: ["Listen"]

- The nodes perform carrier listening for some time
- If the medium is found busy, it goes to "Back off" mode.
- If the medium is found free, the node transmits "RTS" packet and enters "Await CTS state".

Step 4: ["Back off"]

- Here nodes wait for a random amount of time for the channel to be free and then goes to sleep state.
- "Back off" period is used by application layer for the "phase change" i.e. to desynchronize the periodic traffic of different nodes.
- After the "Back off" period nodes listens again.

Step5: ["Await CTS state"]

- Here the node waits for CTS packet.
- If CTS packet arrives in time then node sends its data packet and waits for

- Acknowledgement and enter into "Await ask" state.

Otherwise go back to "Back off" state or drop the packet depending upon "numtrials" values.

Step6: ["Await ask state"]

It can be explicit ask or parent node piggybacks the ack on packet and then forwarded to grandparent.

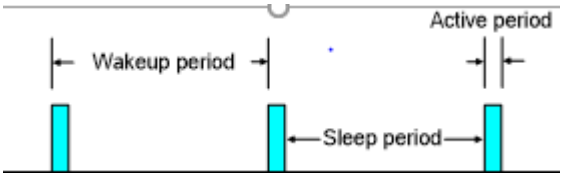
10 **a. Explain low-duty cycle and wake up concepts in WSN [8]**

b. Explain S-MAC protocol [8]

c. Briefly explain energy problems on the MAC layer. [4]

a. **Low-duty cycle and wake up concepts in WSN**.

- Wake up channel time 'T': (sleep period + active period)
- It is divided into sleep period and listen period 'Trx' (T>>> Trx) and these together are called wake up period.



Duty cycle:

- Ratio of active and wakeup period

Low duty cycle:

- As the active period is very less as compared to wakeup period.

Periodic wakeup scheme:

- The Node uses periodic wakeup scheme. Here the node spend most of time in sleeping state and wakeup periodically in 'listen period' to receive packets from other nodes.
- The sleep state is left only when node is about to transmit and receive packets.
- All the nodes must be synchronized to this wakeup period.

S-MAC protocol

Stands for Sensors Medium Access Control

- Also called as S-MAC or Scheduled MAC.
- A periodic wakeup schedule is maintained by the nodes so synchronizes sensor cluster
- It reduces energy consumption due to idle listening.
- But it introduces additional latency in packet delivery
- Specifically designed for Ad hoc wireless sensor networks
- Primary goal: Energy Efficiency

- Main features of SMAC include
- Periodic Listen and sleep
- Collision Avoidance
- Overhearing Avoidance
- Message Passing

Frame schedule:

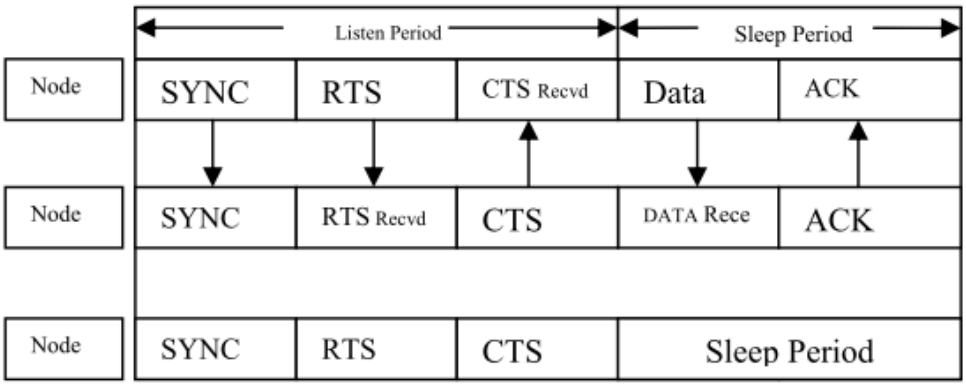
- Nodes are free to choose their listen/ sleep schedule
- Neighboring nodes are synchronized together and their listen period should start at same time.

- Schedules are exchanged (using SYNC packets)
- During sleep mode turn off radio and set a timer to awake later
- Reduce duty cycle to ~10%

Listen period: It is used to transmit and receive the packets.

- Active period is divided into SYNCH, RTS, and CTS phases.
- SYNCH for synchronization
- RTS, CTS for sending data

Sleep period : It consists of ACK and data



Energy problems on the MAC layer:

Transmissions and reception of packets are costly in WSN, Idling is also a problem.
Considering these constraint on operation of a MAC, the energy problems are classified as:

- Collisions
- Overhearing
- Idle listening
- Protocol overhead

Collision

- It happens when two nodes transmit the packet at the same time without listening to channel.
- The energy is wasted during collision as well in retransmission of packets.
- Hence use collisions can be avoided by using such techniques like fixed assignment protocols: TDMA, FDMA, CDMA, and SDMA. Demand assignment protocols: Token ring, logical ring.

  Random access protocols: ALOHA, CSMA, CSMA-CA etc.

Over Hearing

- A lot of energy is wasted in receiving a packet destined for another node called overhearing.

Idle listening

- Means a node being in idle state is ready to receive a packet but not receiving anything.

Protocol overhead

- Protocol overhead refers to the additional information that must be sent with data being routed

	through the network toward a destination ▪