UNIT - 2

Machine to Machine

M2M is a broad label that can be used to describe any technology that enables networked devices to exchange information and perform actions without the manual assistance of humans

M2M is also the foundation for the IOT

The main purpose of M2M technology is to tap into sensor data and transmit it to a network.

M2M often uses public networks and access methods - for example, cellular or Ethernet to make it more cost effective

Main components of M2M

- Sensors
- RFID
- WiFi or cellular communication link
- autonomic computing software programmed to help a network device to interpret data and make decisions

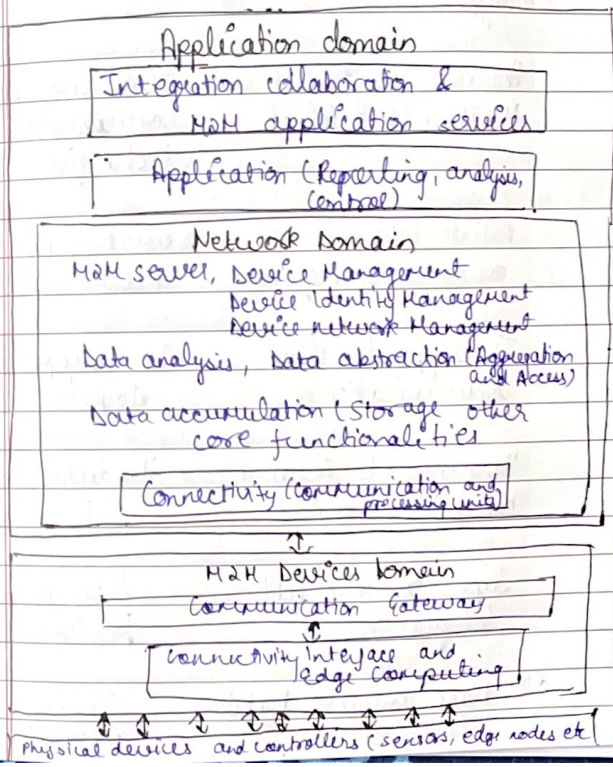
Eg telemetry

Each machine in an M2M system embeds a smart device. The device

senses the data or status of the machine and performs the computation and communication functions. A device communicates via wired or wireless systems.

M2M architecture consists of three domains

- M2M device domain
- M2M network domain
- M2M application domain



IoT	M2M
Internet of things	Machine to Machine
Devices have objects that are responsible for decision making	Some degree of intelligence is observed in this
The connection is via network and using various communication types	The connection is a point to point
Protocols used are HTTP, FTP & Telnet	Traditional protocols & communication technology techniques are used
Active Internet connection is required	Devices do not rely on an internet connection
It supports cloud communication	It supports point to point communication
Hardware & software based technology	Hardware-based technology
Supports open API integrations	There is no support for Open APIs
Eg Smart wearables, Big Data cloud etc	Sensors data, & information etc

Note M2M is a subset of IOT

primary purpose of M2M communication is to enable Machine to Machine interaction

primary purpose of IoT is to create an intelligent environment for the user.

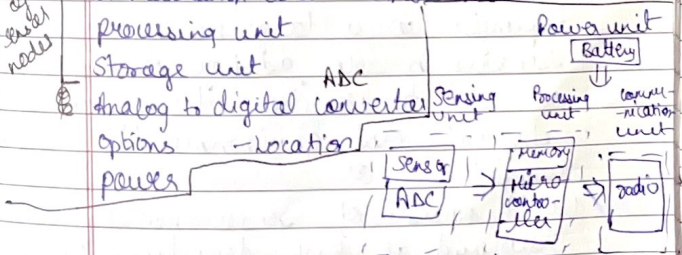
sensor node - size as small as possible

A sensor node also known as mote, is a node in a sensor network that is capable of performing some processing, gathering information and communicating with other connected nodes in a network.

A sensor node is a small and inexpensive device with limited resources of battery and computation power which are deployed in a region to monitor the environment.

components of sensor nodes

- Sensing unit
- communication unit (Trans receiver)
- processing unit
- Storage unit
- ADC analog to digital converter
- options - location
- power



Sensors (device / module / machine / subsystem)

As we know that human being collect info of the surroundings using this sense organs (sensors), namely eyes, nose, skin, etc in order to perform various tasks.

Similary systems must interact with their environment to do useful tasks. so they use sensors & actuators

without the use of sensors, there would be no automations.

Sensor is a device that measures a physical variable and converts the physical quantity into another form (electrical form) which can be read by an observer or by an instrument

Heat, temperature

WSN (wireless sensor network)

WSN is a wireless network that is deployed in a large no of wireless sensors in an ad-hoc manner that is used to monitor the system, physical and environmental conditions

Or

WSN consists of sensor nodes that are deployed in high density & often in

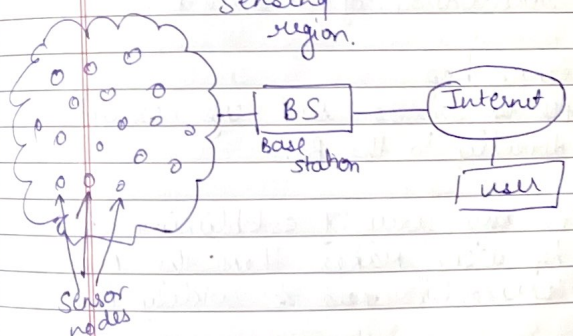
WSN is a network of many tiny disposable low power devices (nodes) that communicate through wireless channels for information sharing.

large quantities & support sensing, data processing, embedded computing & connectivity

Sensor nodes are used in WSN with the onboard processor that manages and monitor the environment in a particular area.

They are connected to the Base Station which acts as a processing unit in WSN. Base Station is connected through the Internet to share data (acts as a gateway)

WSN can be used for processing, analysis, storage & mining of the data



In WSN different radio technologies can be used for communication such as ZigBee, WiFi, Bluetooth, etc

The BS sends the commands to the sensor nodes and the sensor nodes perform the task by collaborating with each other.

After collecting the necessary data, the sensor nodes send the data back to the base station.

After receiving the data from the sensor nodes, a BS performs simple data processing and sends the updated information to the user using Internet.

There are different ways of communication in WSNs designed based on the energy conservation of the sensors.

Single hop
All the sensors send info collected directly to the BS.

One easy way of establishing single-hop WSN makes them the most commonly used & widely known type.

Multiple hop
For long distance transmission, multihop network architecture is used. Here the

energy consumption for communication will be significantly higher than data collection & computation.
Here the data of sensor node is transmitted through one or more intermediate nodes.

Sensors send the data to a aggregation node & then these nodes collect the info & finally send them to the BS.

WSN is a subset of IOT

IOT = WSN + Internet + cloud storage + Mobile/Web application

WSN are not necessarily connected to the Internet & only sensors are information gathering devices while in IOT things are always connected to Internet & things may be sensors, cameras etc that upload data to Internet.

Advantages
- avoids lot of wiring
- accomodate new devices at anytime

Disadvantages
- Lower speed
- less secure

-Mobilizer - It is needed to move sensor nodes when it is required to carry out the assigned tasks

Sensing unit - composed of sensors & ADC
The sensor collects the analog data from the physical world & an ADC converts this data to digital data. Then these digital data/signals are fed into processing unit.

Processing unit - main processing unit which is usually a microprocessor or a microcontroller, performs an intelligent data processing & manipulation.

It is generally associated with a small storage unit.

Communication unit / Transreceiver
It connects the node to the network. Communication unit consists of radio system, usually a short range radio, for data transmission & reception.

Optionals

- location finding system
It is commonly required because most of the sensor network routing techniques & sensing tasks require knowledge of location with high accuracy.

MAC protocols
MAC protocols objective is to reduce energy consumption because the sensor nodes are battery powered with limited battery power.

There are three kinds of MAC protocols used in sensor networks.

① Fixed allocation MAC protocol
Share the common medium through a pre determined assignment

It is suitable for sensor network that continuously monitor & generate deterministic data traffic.

② provide a bounded delay for each node.

However in the case of bursty traffic where the channel requirements of each node may vary overtime it may lead to inefficient usage of the channel.

② Demand - based MAC protocol
used in such cases where the channels allocated according to the demand of the node

variable rate traffic can be efficiently transmitted

require the additional overhead of a reservation process

(3) Contention based MAC protocol
Random access based contention for the channel when packets need to be transmitted

Suitable for bursty traffic

Collisions & no delay guarantees are not suitable for delay-sensitive or real time traffic.

Self organizing MAC for sensor SMACS network and Eavesdrop & register (EAR) are two protocols which handle network initialization and mobility support respectively.

SMACS
neighbor discovery and channel assignment take place simultaneously in a completely distributed manner.

A communication link between two nodes consists of a pair of time slots, at fixed frequency

This scheme requires synchronization only b/w communicating neighbors, in order to define the slots to be used for their communication

Power is conserved by turning off the transceiver during idle slots.

EAR
Enable seamless connection of nodes under mobile and stationary conditions.

This protocol make use of certain mobile nodes, besides the existing stationary sensor nodes, to offer service to maintain connections

Mobile node eavesdrop on the control signals & maintain neighbor info.

Data aggregation

Data aggregation is the process of one or more sensor nodes and detects the information result from the other sensor nodes. The aim of the data aggregation is to remove data redundancy and improves the energy lifetime in WSN. ∴ reducing the no of data packets transmitted over the network because aggregation need less power as compare to multiple packets sending having same data.

Approaches

1) Cluster based approach (Hierarchical)
whole network is separated into various cluster
Each cluster has cluster heads
The main role of the cluster head is to aggregate data received from the cluster members and transmits the results to BS.
The cluster head can share info with the sink, directly via long range transmission or multi hopping using other cluster heads.

2) Tree Based approach
This tree is defined as a minimum spanning tree in which sink node acts as a root and source node as a leaves.
Data flow from leaves node → to root node.

disadvantage- data packet lose at any level of tree which may cause failure of whole network.

3) Multipath approach.
This is used to overcome the drawback of tree based approach.
In this each and every node could send data packets over multiple paths using multiple neighbors in aggregation tree.
eg ring topology
disadvantage → overhead.

4) Hybrid approach.
Mixture of → cluster & multipath & tree based used for optimal performance of their data aggregation

Data Dissemination

It is the process in which sensor nodes is collecting the data and communicate to the base station or any other interested node. It is two steps process:

1. Interested nodes are broadcast to their neighbor nodes in the network
2. After receiving the request nodes sends requesting data.

Approaches

1) Flooding
If the destination node is not receive the data packet or specified no of hops is not reached. Then each node broadcast the gathered data until the packet is reached to their destination node.
Problem – Implosion, resource blindness & overlap

2) Gossiping
In this, the packet is sent to a single neighbor chosen from neighbor table randomly instead of broadcasting each packet to the entire neighbor.
does not face problem – implosion

3) SPIN
Sensor Protocol for Information via Negotiation

It overcomes the problems faced by flooding.
It uses three ways:
ADV, REQ and DATA.

The nodes which are interested in the event to transmit REQ message for DATA. After receiving REQ message source node sends DATA message to interested node.

In this way the data can reach in entire network.

Communication Protocols

- Bluetooth
- ZIGBEE
- WiFi
- Cellular
- NFC
- LoRaWAN

Pg No 16
– Pg No 18 Explain in detailed.

Communication Gateway

Communication gateway connects two application layers, one at sender and the other at receiver.

It enables use of two diff. protocols one at sender and other at receivers end.

The gateway facilitates the communication

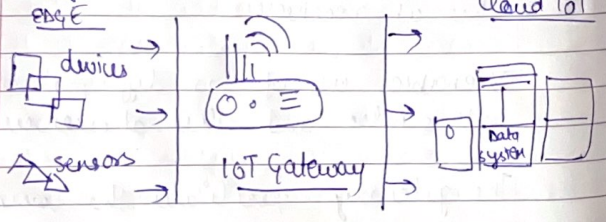
between web server using the TCP/IP protocol conversion gateway and IoT devices.

It also facilitates communication b/w the devices using CoAP client and server using HTTP

The network then connects to the web server through a gateway. The server posts and gets data using HTTP. A gateway facilitates the communication b/w IoT devices & web server.

for eg Zigbee to SOAP and IP
CoAP protocol conversion gateway for RESTful HTTP

By the help of gateways it is possible to establish device to device or device to cloud communication. A gateway can be a typical hardware device or software program.



As IoT devices work with less power consumption (Battery) → energy constrained
It won't be effective in terms of power if communicate to cloud/internet directly

∴ they communicate with gateway first and then gateway links them to cloud/Internet by converting data into a standard protocol like MQTT

functions of gateway.
- establish communication bridge
- provides security
- performs data aggregation
- pre processing & filtering data
- provide local storage
- data computing at edge level
- manage entire device

networking notes

IP address
An IP header consists of source and destination addresses called IP addresses

The internet generally uses IPv4 addresses

IoT/M2M use IPv6 addresses.

IPv4.

IP version 4 addresses consists of 32 bits. However it can be considered as four decimal numbers separated by dots
eg 198.136.56.2