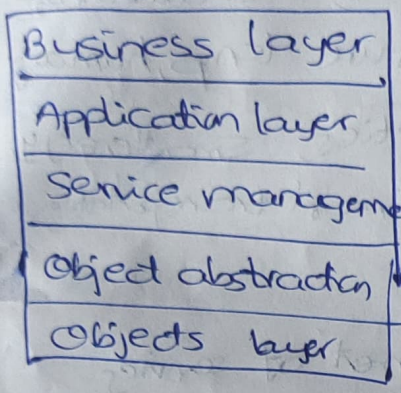
Unit 3 IOT

Layered Architecture of IOT:



1) Objects / Devices / Physical layer:

→ Physical devices collect & process info.
→ Physical devices may be sensors like light, optical, etc.
→ Plug and play mechanism is used to integrate and configure sensors in this layer.
→ Data collected is sent to object abstraction layer using secured channels.

2) Object abstraction layer:

→ It takes data from object layer & transfers to service management layer using secured channels.
→ Data transmission can happen by RFID, 3G, GSM, WiFi, Bluetooth, Zigbee.
→ Special process to handle cloud computing is present.

3) service management layer:

→ [redacted] acts as middleware.
→ It processes data received from object abstraction layer.
→ It can perform data aggregation, protocol conversion
→ It ensures that correct service is provided to requester.

4) Application Layer:

→ Provides services requested by customer.
→ Also includes data analytics, visualization tools.
→ Ex: Smart Home → measure temp, humidity
→ Provides services to smart cities, smart energy, smart buildings, smart living, smart transportation

5) Business Layer:

→ Performs overall management of services
→ Receives data from network layer & builds flowcharts, model graphs.
→ This layer also performs data analysis for decision making.
→ This layers includes business policies, rules that define how IOT system operates

---

Protocol Architecture of IOT

1) Application Layer – Application protocols – DDS, CoAP, AMQP, MQTT, MQTT-SN, XMPP, HTTP REST

2) service management – Service discovery protocols – mDNS, DNS-SD

3) Object abstraction and Object layer – Infrastructure protocols
   - Routing protocol – RPL (Routing protocol)
   - Network layer – 6LoWPAN, IPv4, IPv6
   - Link layer – IEEE 802.15.4
   - Physical/device layer – LTE-A, Z-Wave, IEEE 802.15.4, EPC global.

1) Routing protocol (RPL):

→ used in low power & lossy network → (packet are dropped more) → (LLN)

→ It is IPV6 protocol

→ LLN include WPAN's (wireless), Low power line (LPC) communication networks, Wireless sensor network.

→ Characteristics of these networks:

i) optimise, save energy

ii) Suitable for any traffic except unicast

→ It supports point to point, point to multipoint

→ Devices using RPL, must not have cycle in network.

→ RPL uses distance vector routing

DODAG: Destinated Oriented Directed Acyclic Graph

A tree where each branch leads to a single destination i.e., root. The data is sent to root only.

→ Every node knows its parent, but not it's children

→ only data transfered from child to parent.

Rank of a node = level of node

root = level 0

RPL instance: A smaller network within in a larger network

Dodag id: Each Dodag has IPV6 (128 bit) id

id is given to root only.

Dodag version: Every new tree is called new version

RPL Goal is to provide best path using DODAG.

when DODAG reaches its goal, it is called grounded

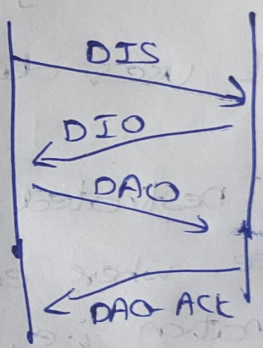
when DODAG doesn't reach goal it is called floating

Types of nodes: → keeps track of all routes in routing table

1) Storing nodes: Root is storing nodes. When packet arrives it knows how to send message & keeps track of it.

2) Non storing node: They don't know any routes only they send to parent

~~Message transmission in RPL~~ Nodes discovery in RPL



1) DIS: DODAG Information Solicitation

It is a request message from a device that it needs info about network / join the network

2) DIO: DODAG Information Object

Devices in the network send DIO messages to tell that they are part of network to new node and also shares info about network structure

3) DAO: Destination advertisement object

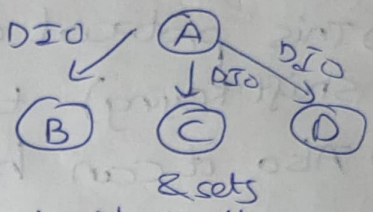
Devices use DAO to tell other devices (especially root) about the best path to reach it

4) DAO-ACK:

When a devices receives DAO, it sends DAO-ACK to confirm that it received routing info.

DODAG formation:

1) Root is a special node.
2) Assume there are 4 nodes A, B, C, D and A is the root.
3) A sends DIO to all nodes



4) Routers at each level builds the path from node to parent
5) After receiving DIO's B, C, D will know distance to A.
6) B, C, D sends DAO to A
7) A will send DAO ACK to B, C, D
8) This will continue until shortest distances are found for each node.
9) Root can store info about how to reach other devices based on DIO

Modes of operation for info exchange:

1) Non storing mode: The route which message must be sent in included in message only
2) Storing mode: Only destination is present & each device uses its own routing table to forward it.

IEEE 802.15.4:

This was created for MAC, and LR WPAN (low rate wireless private area network)

physical layer

Features:

1) Used for low data rate WPAN
2) Uses physical, MAC layer to communicate with other layers

3) Operates in ISM band.

4) Low power consumption, low data rate

5) low cost & provides CRC

→ This protocol uses QPSK (Quadratic phase shift keying) to transmit data.

→ Also it can handle upto 65k nodes.

→ Used for secured communication

→ Quality of service not guaranteed

→ This protocol works at 3 data rates

1) 250kbps at 2.4GHz

2) 40kbps at 915 MHz

3) 20kbps at 868 MHz

→ This protocol supports 2 types of nodes

1) Full Function Device (FFD): Can talk to any device

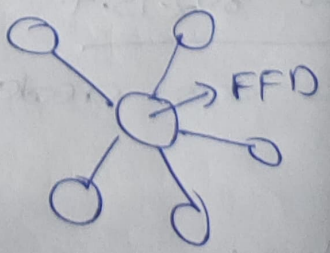
FFD can act as PAN coordinator / normal node.

Coordinate can control, maintain data.

FFD stores routing table & communicate with other device using star topology, peer to peer, cluster tree, network

a) Star topology: It contains atleast 1 FFD and few RFD (Reduced functional device)

FFD acts as coordinator and it is at center of network



Coordinator:

1) Only FFD can become not RFD

2) The node which starts a PAN becomes FFD

3) Nodes join the network by sending request to coordinator.

b) Peer to peer topology: This contains PAN coordinators and other nodes can communicate in same network or other network → using intermediate nodes.

c) cluster tree topology: special peer to peer topology contains PAN coordinator, cluster head, normal nodes

2) RFD (Reduced Functional device):
can talk to FFD, lower power req, less CPU, RAM needed

802.15.4 — FFD – PAN coordinator, router, device
RFD – Device

Frames in this protocol: Beacon, MAC, command, acknowledgment, data

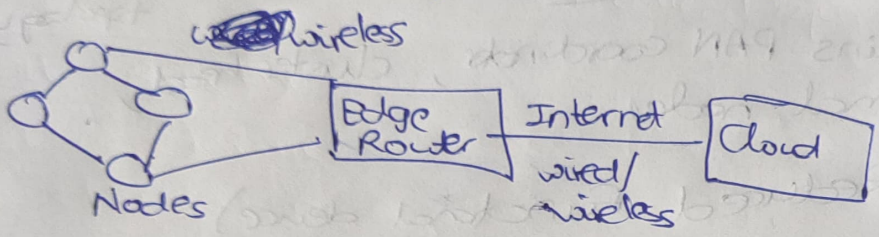
Beacon Enabled network	Non Beacon Enabled network
1) Periodic transmission of messages using slotted CSMA/CA	1) Data sent via unslotted CSMA/CA
2) Lower Power consumption due to scheduled sleep period	2) High consumption of Power
3) Low throughput & high latency due to waiting time for beacons	3) High throughput, Low latency
4) More complex network management	4) Easy to manage
5) Not scalable easily	5) Easily scalable.

6LOWPAN = IPV6 over Low Power Wireless Personal Area Network

→ Designed to support 802.15.4 in 2.4GHz band.

→ It allows communication using IPV6 protocol.

→ 6LOWPAN was designed to overcome old methods to transmit info. But this also is not that efficient for small devices.



Every node has IPV6 address. Every node sends data to edge router & it sends to cloud.

It uses AES 128 encryption.

It can communicate with zigbee, wifi devices also

Requirements: should require
1) Less memory 2) Less routing overhead
3) Device should provide sleep mode to support battery saving

Features: 1) Supports 16bit, 64 bit addressing
2) Unicast, Multicast, Broadcast are possible
3) Support Low power, lossy IOT network
4) Max nodes - 100
5) used with 802.15.4 in 2.4GHz

Advantage: 1) Low cost, 2) One-Many routing
3) Batter saved 4) IPV6

Disadvantage: 1) Less secure 2) only mesh topology

Application: 1) Home automation 2) Smart agriculture
3) Industry monitoring 4) Wireless Sensor Network

Protocol Stack:

1) Physical Layer: Converts data bits to signals
   Uses IEEE 802.15.4

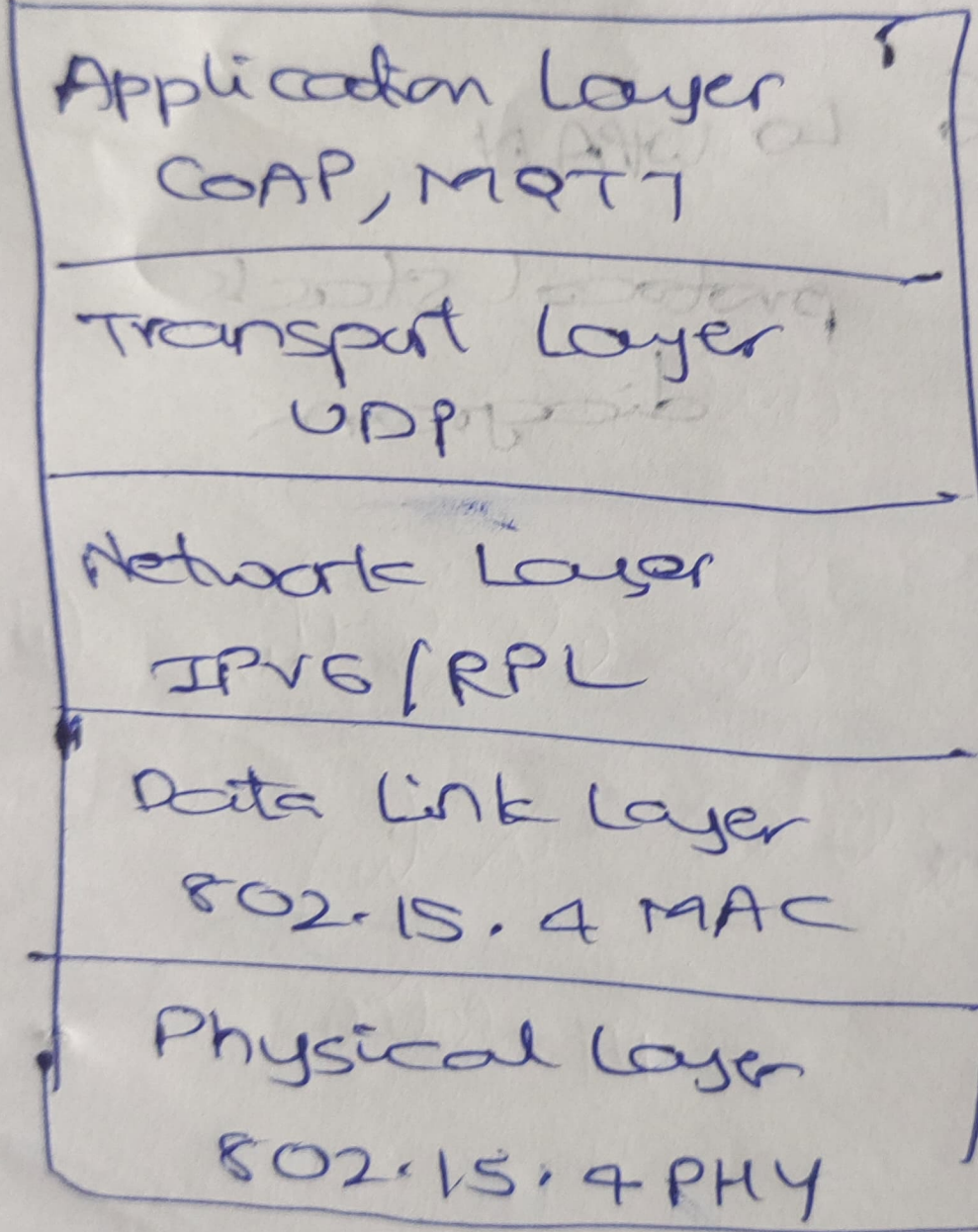
2) Data Link: Correct errors. Includes MAC for media access. 802.15.4 acts as MAC layer Contains adaptation layer which converts data from IPv6 to 802.15.4

3) Network: Handles routing of pkts from source to destination
   Uses IP address. Uses IPV6/RPL protocol

4) Transport: Uses TCP/UDP. Generally UDP preferred as it has less overhead

5) Application: Uses COAP & MQTT. HTTP is not suitable because it req TCP.

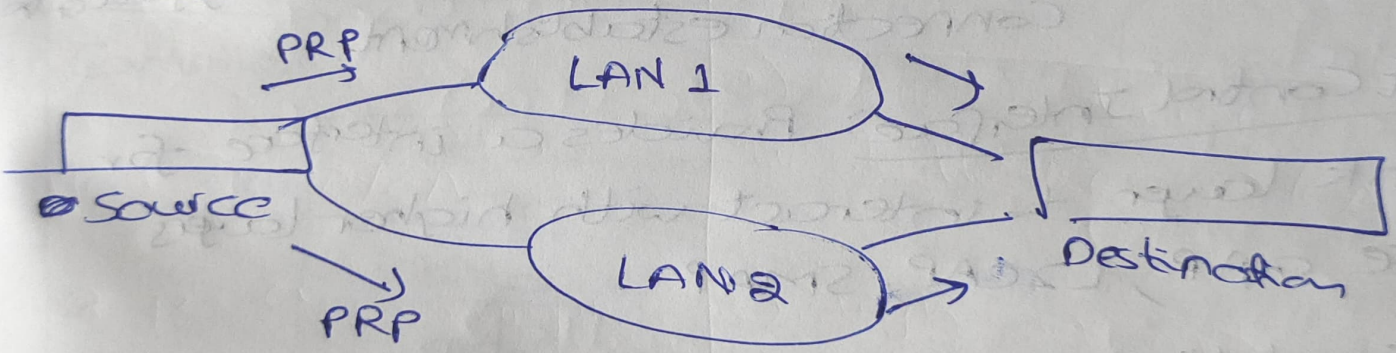
Protocol Stack



Parallel Redundancy Protocol (PRP):

It is used to increase network reliability by duplicating packets & sending them over 2 separate network. This ensures that communication remains uninterrupted even if 1 network fails.

Working:



2 LANS are setup. Both operate independently. Source sends 2 packets 1 on LAN1, other on LAN 2. The destination receives 2 packets and discards duplicate based on sequence number. If one LAN fail other can send without interruption

Fectures: 1) Guaranteed data transmission
2) Duplicate packet removal
3) Can be used with any ethernet network

Advantages: 1) Reliable 2) Easy to integrate
3) No need of special hardware to implement

Applicatia: 1) Sending signals in traffic
2) Critical care medical equipment

BLE: Blueboth Low Energy.
It is a wireless communication protocol designed to offer low power consumption. It maintains good speed and range.

Characteristics: 1) Lower Power consumption
2) Can communicate over 100m distance (more than traditional Bluetooth)
3) less Latency (15times less than traditional)

Protocol stack:

1) Physical layer: Handles data transmission & reception
2) Link layer: Performs MAC, error control, flow control, Connection establishment.

Host Control Interface: Provides a interface for Link layer to interact with higher layers like GAP, L2CAP, SMAP.

Logical Link Control Adaption Protocol (L2CAP):
Performs multiplexing: Allows multiple channels to share same connection.
Performs fragmentation & reassembly.

GAP (Generic Access Profile): Manages data discovery & link establishment.

Roles:

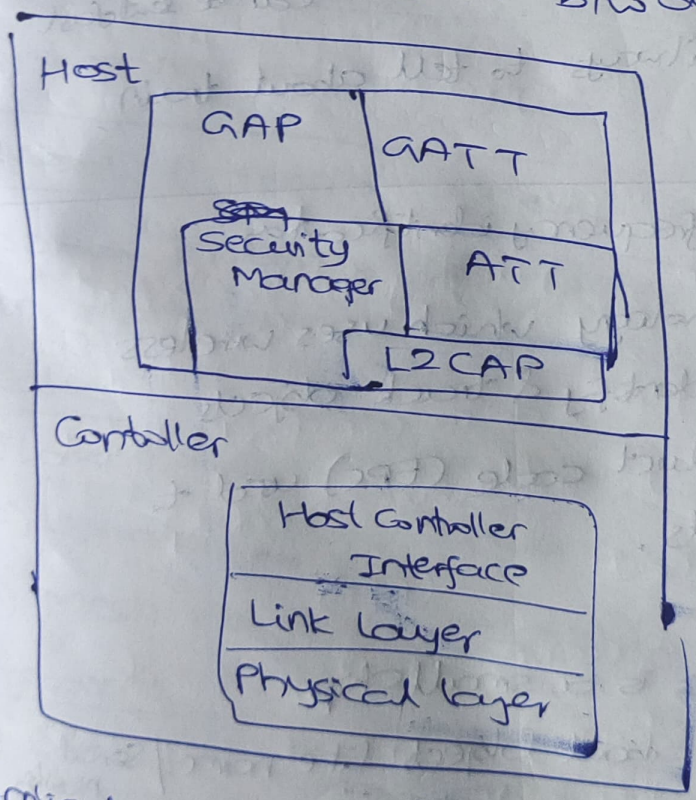
1) Broadcaster: Sends advertising pkts
2) [redacted] observer: Listens for advertising packets
3) Peripheral: Accepts connection request
4) Central: acts as master

GATT (Generic Attribute Profile): Tells how data is organized & exchanged

Roles:
1) GATT client: request data & command from server
2) GATT server: Provides data to client

Attribute protocol (ATT): used by BLE to manage data exchange b/w devices

Security Manager Protocol (SMP): ~~handles~~ ensures secure communication b/w devices.



Application: Wearable device, Beacon, Industrial automation

Long Term Evolution Advanced (LTE):

→ Also known as 4G LTE
→ Provides high data transfer rates
→ 50 times better than existing wireless network
→ LTE broadcast operates using SFN

SFN: Single Frequency Network: Allows multiple transmitters to send same signal to improve coverage area.

→ It is designed to deliver multimedia content to multiple user efficiently

Use cases: 1) Live steaming 2) Emergency alerts can be sent fast.

3) Used in railways to tell about train arrival times

RFID – Radio frequency identification

→ It is a technology which uses wireless microchips to identify & track objects
→ Electronic product code (EPC) used to identify objects.

Components:

1) RFID tag: This is a small chip
It stores info about objects like name / serial number
It has 2 main parts: Electronic chip → stores object identity
Antenna → send & receive signal

2) RFID Tag reader: Reads info stored in tag. Sends radio waves & collects data & then it sends it to a system.

working:

a) ~~RFID Reader Can~~

1) RFID reader sends radio waves, RFID tag picks them. RFID tags get charged using waves and sends data of it.
2) RFID reader receives data & sends it to a system
3) The system, known as Object Naming Services receives tag number & gets further details
4) Electronic Product Code system ~~connects~~ (EPC) helps to get data from database using tag
5) The database sends all data related to tag

Applications: 1) Warehouse 2) Trains for movement tracking
3) Shopping malls 4) Library

Z-wave: A special wireless lang that allows devices in home to communicate. It is used in smart lights, security system.

Features:

1) Lower power consumption
2) Operates in low frequency but covers entire house
3) Mesh network is created b/w devices

Components:

1) Controllers: The brain of network.
They manage communication b/w ~~devices~~ devices & keep track of who is talking to whom

2 types of controller:

1) Primary: Controls network & assigns ID to devices. only 1 primary controller

2) Secondary: Helps primary controller to manage network

2) Slave Nodes: The devices which do actual work. They can receive commands from other devices & controller.

Types:

1) Regular slave node: Just follow instructions from controller or other nodes

2) Routing slave node: Helps to find best path for message

3) Frequency listening routing slave: wakes up at defined intervals to check for messages.

Zigbee: It is a wireless communication protocol developed by ZigBee Alliance.

Features:

1) Low Power Consumption

2) Cost effective

3) Highly scalable - Support 65k nodes per network

4) If one route fails, devices can find alternate routes ensuring continuous connectivity

Types of devices used:

1) Router: (FFD) Sends & receives messages from devices. Provides redundancy, if 1 router fails to deliver then other will deliver

2) End device: (RFD) Sensors / switches. They are in sleep mode to conserve power. When data needs to transmit/receive then they wake up

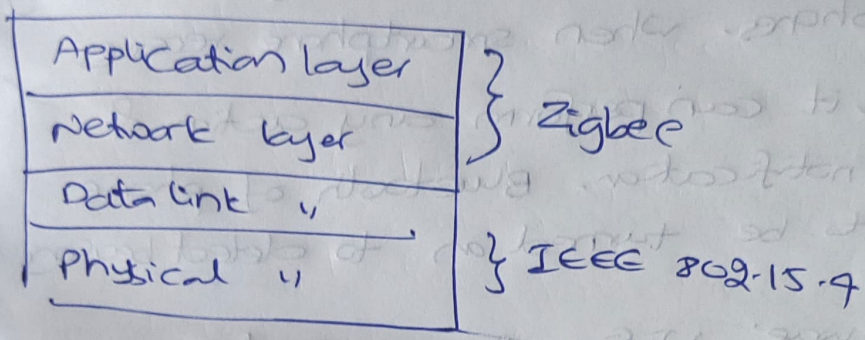
3) Coordinator: Responsible for network setup & management. When a new node wants to

join, it takes care.

4) Trust center: Manages encryption & decryption to ensure secure communication

Zigbee support star, mesh, cluster tree topology

Architecture:



Application: 1) Smart Home automation
2) Smart metering 3) Smart agriculture
4) Industrial automation

Zigbee	6 LOWPAN
1) Entire network managed by coordinatory	1) No coordinator, direct server collects data from end devices
2) Can't communicate with internet directly uses zigbee gateway	2) Can communicate
3) Has its own protocol stack	3) Uses IPV6 stack
4) Used in smart home	4) Used when small devices are present
5) Mesh, star, cluster tree topology	5) Adapts its topology according to need

Device / Service Discovery:

Every device must be uniquely identified.
We use either
1) Bluetooth beacons 2) Wifi Aware 3) Open Hybrid

1) **Bluetooth beacons:** They send signal to nearby smartphones. When smartphone receives signal, it can perform any action & shows notification. Bluetooth of phone needs to be turned on to detect beacons.

2) **Wifi Aware:** Wifi + Beacon feature.
Helps to identify & connect nearby devices.
Smartphone can tell that it is nearby to other mobiles & then connect & share.

3) **Open Hybrid:** Helps to map physical object to digital interface. When you approach near that object, your connected device will receive notification about that object. It is like virtual guide.

Criteria	Zigbee	Z-Wave	WiFi	Bluetooth	Bluetooth Low Energy
Range	Good due to inherent mesh networking	Good due to inherent mesh networking	Good if repeaters or WiFi mesh used	Not great	Not great
Power Use (in theory)	Low	Low	High	Medium	Low
Bandwidth	Poor	Poor	Excellent	Poor	Poor
RF Band	2.4 GHz	908.42 MHz	2.4 GHz/5 GHz	2.4 GHz	2.4 GHz
Needs hub?	Yes	Yes	No	No	No
# of smart devices available	Moderate	Not many (apart from sensors)	Lots	Barely any	Not many, but growing
Price of smart devices	High	High	Low	Medium	Medium