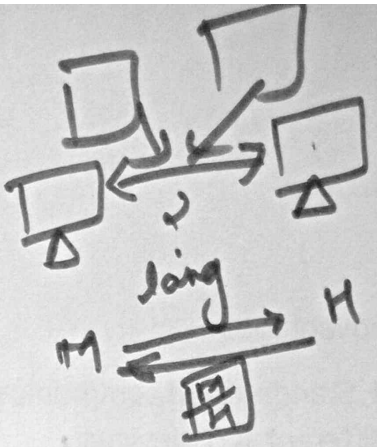


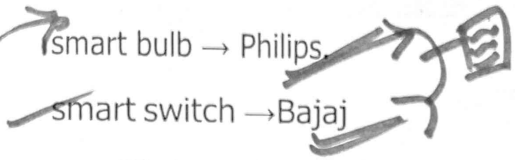
M2M Protocol

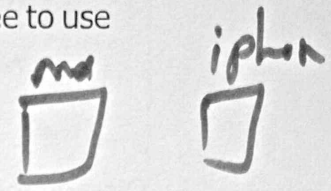
1. M2M protocols define how IoT devices exchange data efficiently and securely.

2. These protocols ensure standardized communication so that devices from different manufacturers can work together.

3. M2M protocols acts like a common language that all devices agree to use

4. smart bulb → Philips.
   smart switch →Bajaj





they can still share data and work smoothly

Characteristics:

1. Interoperable:- Work across devices and applications.

2. Scalable: can connect a small number or millions of devices

3. Secure: use encryption to protect data.

Functionalities:

1. Data Transmission: Transfer sensor data → to server or another device

2. Device communication management:- Handles how devices connect, send and receive information.

3. Error Detection and Handling:- Ensure data integrity even if network Is weak.

Advantages

1. Standardized communication: Ensures smooth data exchange between different IOT devices.

2. Scalable: work for both small and large IOT networks.

3. Flexible: m2m protocol can operate over a variety of communication network:

   - wired : Ethernet
   - wireless: WI-FI,Bluetooth , Zigbee

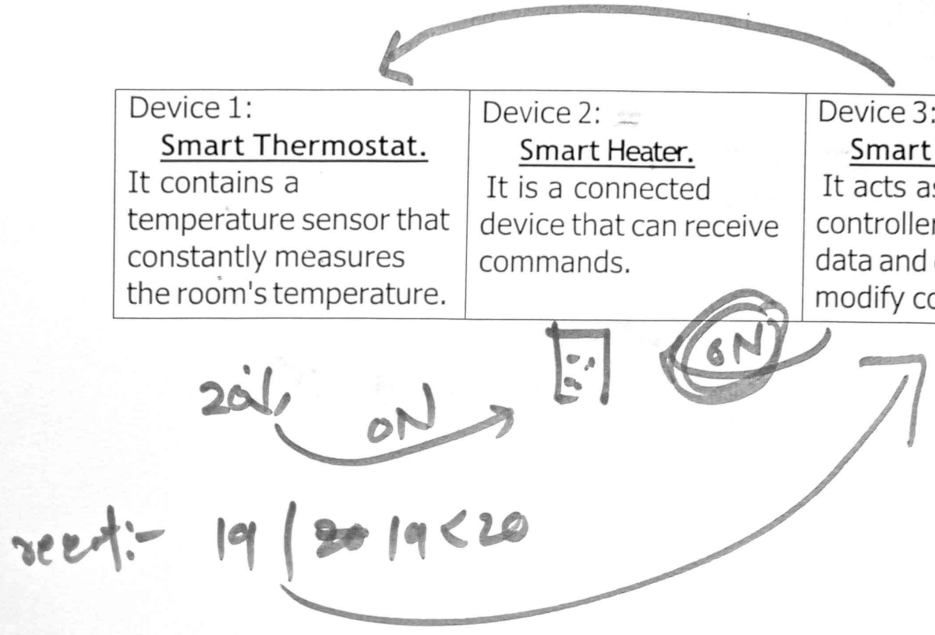
Dis-advantages :

1. Compatibility issues: older devices may not support the new protocol version.

2. Security risk: Old devices are easily attacked so there is a major security risk in the whole IOT system.

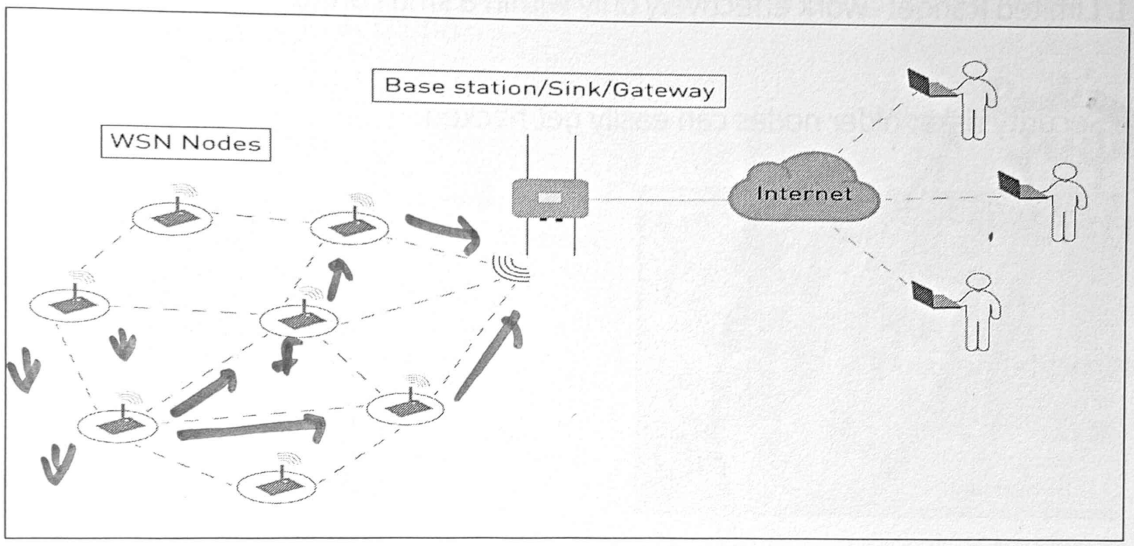
Example: M2M protocols includes MQTT,CoAP,HTTP

Device 1: **Smart Thermostat.** It contains a temperature sensor that constantly measures the room's temperature.	Device 2: **Smart Heater.** It is a connected device that can receive commands.	Device 3: **Smart Home Hub.** It acts as a central controller that logs data and can trigger or modify commands.



WSN PROTOCOL

1. It is used for communication between multiple sensor nodes in an Iot environment.
2. collects, processes and transmit sensor data to a gateway
3. operates on low power and low bandwidth.



Characteristics:

1. Low power consumption: Work efficiently on small batteries for a long time.
2. Scalability: can easily expand network size AND able to add more devices.
3. self- Healing: If one node fails, data can be rerouted through others.

Functionalities:

1. Data sensing: sensors capture enviromental data
2. Routing: uses efficient routing protocols to send data to the gateway.
3. Monitoring: Enables real time monitoring

Advantages

1. Energy efficient: optimized for long term operation on limited power.
2. Flexible and scalable: can easily expand network size.

Dis-Advantages

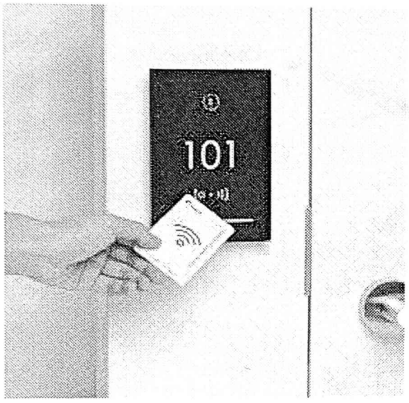
1. Limited Range: work effectively only within a small area.
2. Security risks: older nodes can easily get hacked.

Example

Smart home

RFID

1. Uses radio signals to identify and track tag attached to objects
2. components: RFID tags,
   RFID readers,
   and antenna



Radio frequency

Characteristics:

1. wireless communication: operates via radio signals..
2. unique Identification :- Each tag has a unique electronic product code.
3. Range Flexibility : works at short
   OR
   long range
   depending upon types (passive or active)

Functionalities:

1. Identification:- Detects and Identifies tagged items automatically using radio frequency.
2. Authentication: verifies object Identity
3. Data Transmission: Transfers tag data to the reader without physical contact.

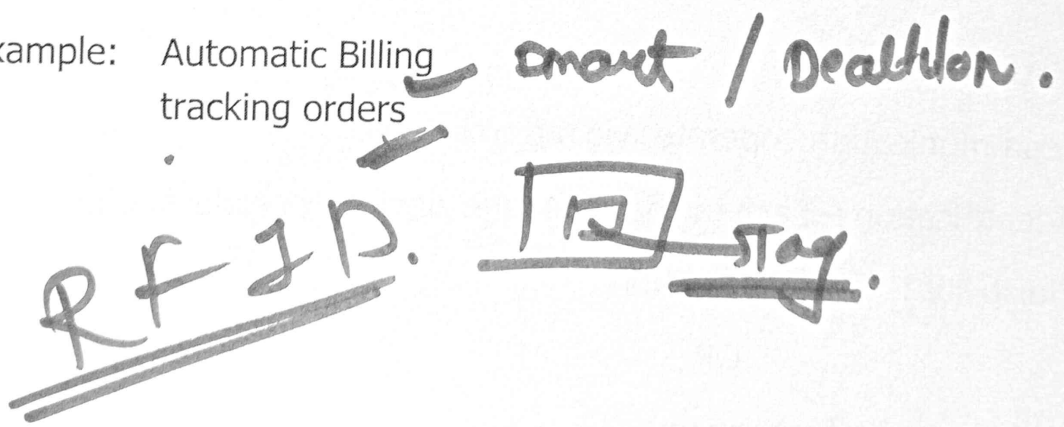
Advantages

1. Fast : saves times compared to manual entry
2. Supports bulk reading :- can read multiple tags at once.

Limitations:

1. High cost - tags and readers can be expensive for large-scale use.
2. Privacy issues: tags can be scanned without permission.

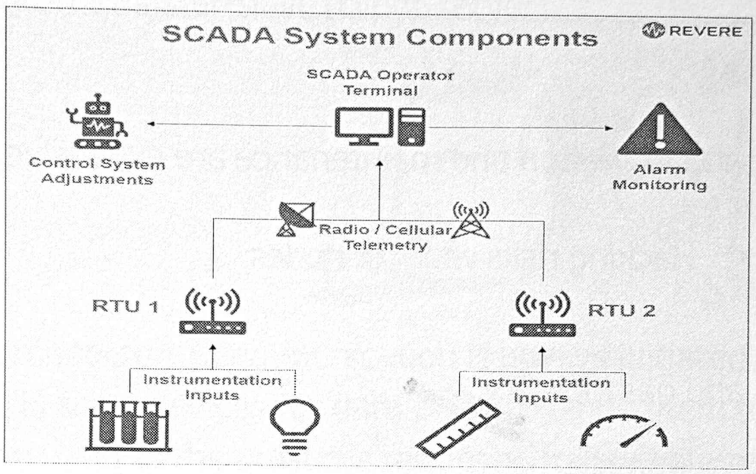
Example: Automatic Billing
tracking orders



SCADA

1. SCADA is a control and monitoring system used to supervise industrial processes like power plants , oil refineries and water treatment.

3. It allows real-time data collection and control from sensors, controllers.



Characteristics:

1. Interoperability: supports multiple communication protocols.
2. Scalability: Can handle large industrial networks. 3.Reliability: Designed for continuous 24/7 operation.

Functionalities:

1. Data collection: Collect data from sensors to send it to the gateway.
2. Alarm Handling: Triggers alarm when needed.
3. Monitoring and control: Allows real, time monitoring and remotely controlling devices

Advantages

1.Remote monitoring:

1. Real time data access: Enables quick decision making and real time data is accessed continuously.

Dis- Advantages

1. High setup cost: Installation and maintenance are expensive.

2. security Risks: Hacking risks with old nodes

Example: oil and gas industry:

Manage

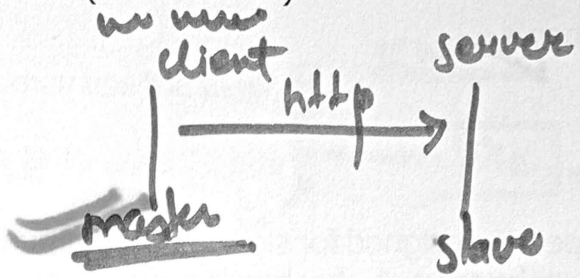
pipelines

Pressure and

flow remotely

Modbus Protocol

1. Modbus is a communication protocol developed by Modicon in 1979.
2. It is used for data exchange between devices like sensors, controllers, and industrial instruments.
3. It works mainly on a master-slave (client-server)



Characteristics:

1. Master-slave architecture: Communication is always initiated by a master device, which polls slave devices for data or commands them to perform actions. Slaves respond to the master's requests, following a request-response model.
2. Real-time data exchange: Modbus facilitates the real-time monitoring and control of equipment, which is crucial for operational efficiency in many industrial applications.

Functionalities:

1. Monitor and control industrial equipment remotely.
2. Exchange real-time data like temperature, pressure, or motor speed.

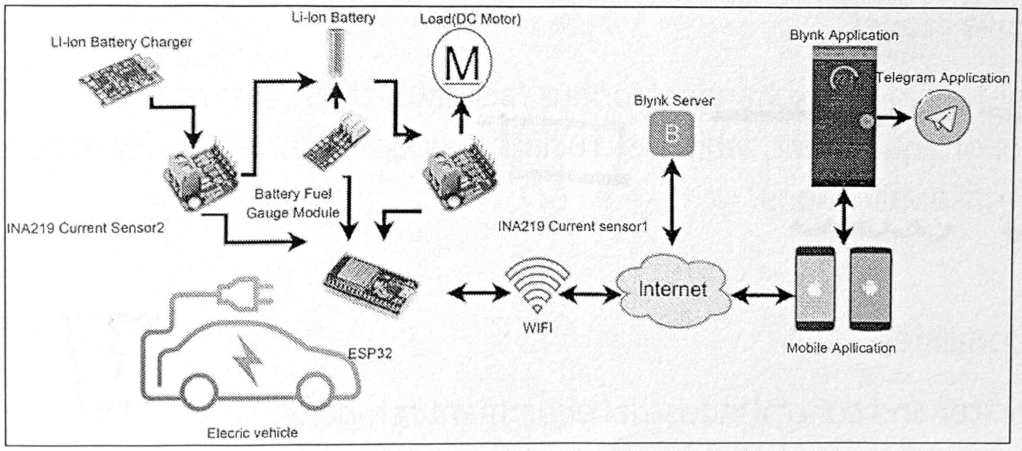
Advantages:

1. Simple and easy to implement - lightweight and widely supported.
2. Open and free protocol no licensing fees.
3. Reliable communication - works well even in noisy industrial environments.

Limitations:

1. Low speed - designed for slow serial communication.
2. Limited data capacity can only handle small amounts of data per message.

Example:



- Used in EVs for internal communication.
- Monitors battery systems (BMS).
- Supports EV charging station communication.

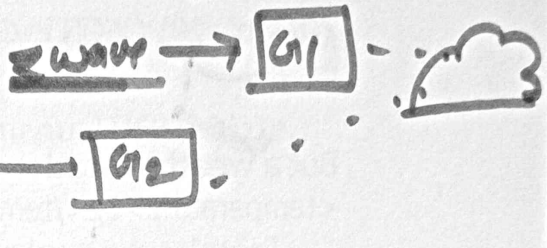
Issues with standardization of protocols

.1. Lack of Universal Standards

- There is **no single global standard** for IoT communication.
- Different organizations (IEEE, oneM2M, etc.) create their own standards.

Ex:

A **Samsung smart door sensor** may use the **Z-Wave** protocol, while a **Philips smart bulb** uses **Zigbee**.



Since both follow **different communication standards**, they cannot connect or talk to each other directly.

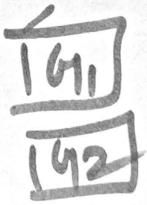
Because there is **no common IoT standard**, the user needs a separate gateway to make these devices work together.

.2. Fragmentation of Protocols

Many protocols exist for similar purposes (MQTT, CoAP, AMQP for messaging).Leads to inconsistent device behavior and compatibility issues.

Ex.

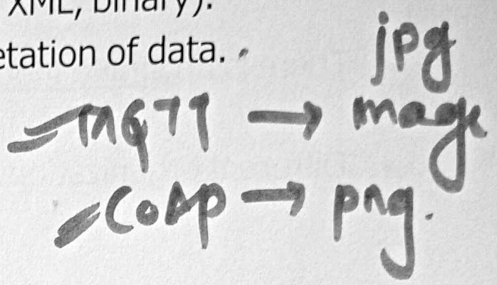
- A **smart bulb** may use **MQTT** to receive ON/OFF commands.
- A **smart thermostat** may use **CoAP** to send temperature readings.



Because each device uses a **different protocol**, they **cannot communicate directly** with each other or work smoothly under one controller.

.3. Data Format and Semantic Differences

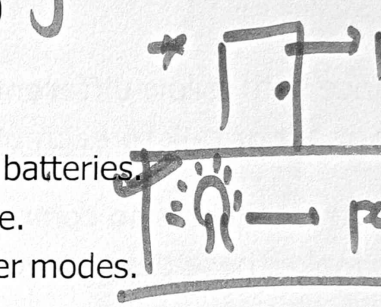
- Devices may send data in different formats (JSON, XML, binary).
- No common semantic model results in misinterpretation of data.



Ex.

A **temperature sensor** sends data as:
{"temp": 28} (JSON in Celsius)

But a **weather station** sends temperature as:
<temperature>82</temperature> (XML in Fahrenheit)



4. Power and Resource Constraints

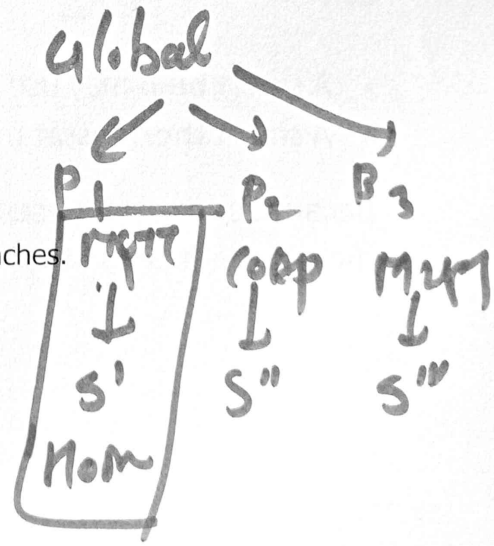
- Many IoT devices use low-power processors and batteries.
- Protocols must be optimized for low energy usage.
- But not all protocols have standardized low-power modes.

Ex.

Zigbee and 6LoWPAN are optimized, but Wi-Fi consumes more power.

.5. Security Standard Gaps

- No uniform security framework across IoT protocols.
- Some protocols lack built-in encryption or authentication.
- This makes IoT devices vulnerable to hacking and data breaches.



Ex.

Early versions of MQTT had no default encryption.

.6. Security Standard Gaps

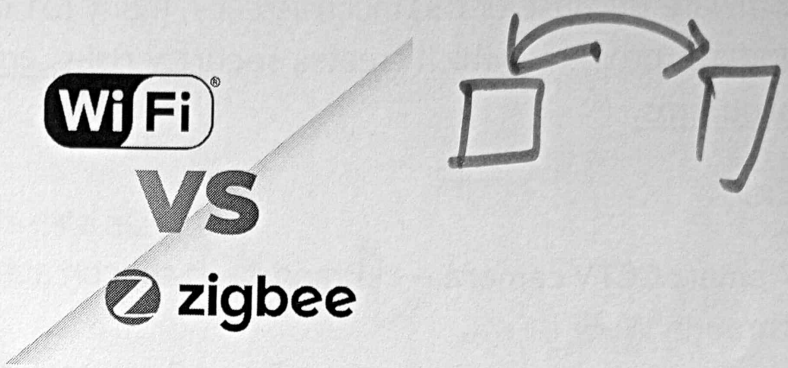
In IoT, different companies use **different methods** for updating device firmware.Because of this inconsistency, many IoT devices do not receive updates properly, which creates **security risks,** errors and **maintenance problems.**

Ex.

A **smart CCTV camera** ---> Brand A --->support automatic OTA updates through Wi-Fi,
but a **smart door lock** ---->from Brand B ---> require a **manual USB update.**

This difference in update methods leads to **uneven security** across the IoT system.

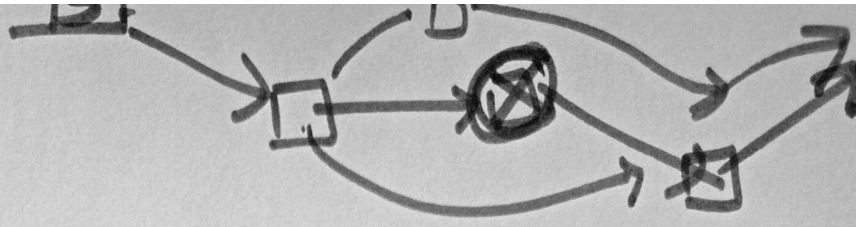
ZIGBEE IS POPULAR THEN WIFI OR BLUETOOTH



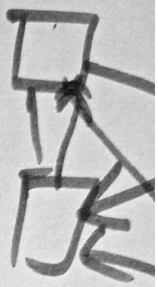
1. Very Low Power Consumption (Best for Battery Devices)

- ZigBee devices consume **far less power** than Wi-Fi and even Bluetooth.
- Can run on a small battery for **months or years.**
- Suitable for sensors, smart locks, smart bulbs, etc.

Reason: Wi-Fi consumes high power; Bluetooth consumes moderate power but still more than ZigBee.



2. Supports Large Networks (Up to 65,000 Devices)



- ZigBee supports **mesh networking**, allowing thousands of devices to connect.
- Nodes act as routers, increasing range and reliability.

Reason:

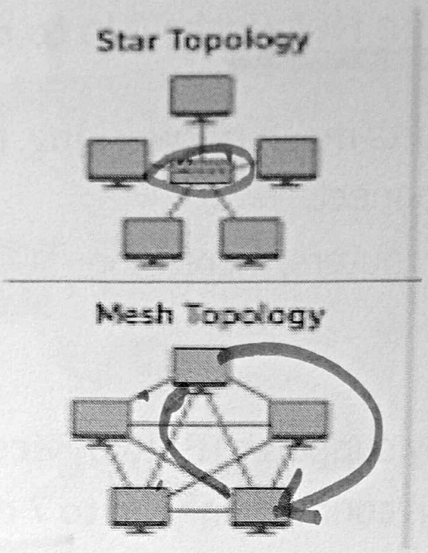
- Wi-Fi typically supports **10-20 devices.** 30-40
- Bluetooth can connect **only up to 7 devices** in one network.

3. Better Range Using Mesh Technology

- ZigBee uses mesh networking, meaning devices relay data for one another.
- Mesh networks are **self-healing**, so if one device fails, data automatically finds another path.

Reason:

- Wi-Fi has good range but consumes high power.
- Bluetooth has very short range (10–30 meters).



4. Highly Reliable 24/7

- ZigBee mesh ensures continuous communication even if some nodes go offline.
- This improves reliability.

Reason:

- Wi-Fi networks may crash when overloaded.
- Bluetooth is easily interrupted by obstacles.

5. Low Cost and Simple Hardware

- ZigBee modules are cheaper than Wi-Fi modules.
- Best choice for mass IoT deployment (hundreds/thousands of devices).

Reason:

- Wi-Fi hardware is more expensive and power-heavy.
- Bluetooth modules are cheap but not suitable for large networks.

6. Designed Specifically for IoT Applications

- ZigBee was created for **automation**:
  smart home,
  industrial IoT,
  healthcare,
  agriculture.
- Built for **low data rate**, low power, and secure communication.

Reason:

- Wi-Fi was designed for high-speed internet.

Bluetooth was designed for personal short-range communication

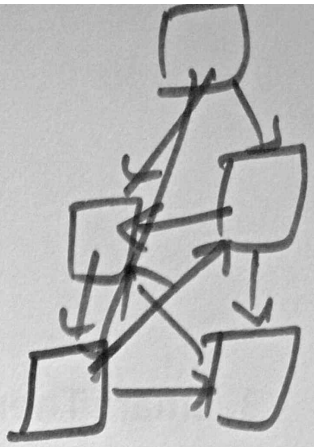
.

7. Better Security for Small IoT Devices

- ZigBee supports **AES-128 encryption** with low power usage.
- Good for smart home security systems.

Reason:

- Wi-Fi encryption is strong but requires more processing power.



ZigBee Technology in Smart Home System

1. Smart Lighting

ZigBee bulbs and smart switches communicate with each other through a mesh technology.
Users can remotely control brightness and on/off.

Extra Points:

- Lights can automatically turn ON when someone enters the room (using motion sensors).
- Energy saving is higher because lights run at low power and follow automation rules.

2. Smart Door/Window Sensors

ZigBee magnetic sensors detect if a door or window is opened or closed.
Sensors can trigger lights to turn on automatically when a door opens.

Instant alerts are sent to the homeowner's smartphone or central hub.

3. Smart Thermostats

ZigBee thermostats measure temperature and communicate with AC/Heater systems.

They help maintain comfortable and energy-efficient climate conditions.

adjust temperature automatically based ---> on time of day

22
20 Heater ON

4. Smart Security System

ZigBee supports various security devices like motion sensors, sirens, smoke detectors, and alarms.

If smoke is detected ------> alarms trigger automatically.

and send alerts to smartphones.

All devices continue to work even if Wi-Fi fails.

High power fire alarm

zigbee

5. Smart Irrigation s Garden Control

Used in home gardens and indoor plants for automated watering.

- Soil moisture sensors send ZigBee data to the hub.
- Irrigation turns ON only when soil is dry.
- Saves water and keeps plants healthy.

6.Smart Home Automation Scenes

ZigBee allows integration of multiple devices to run together in scenes.

Examples:

- **"Good Morning Scene"** → Lights ON, curtains open, thermostat adjusts temperature.
- **"Good Night Scene"** → All lights OFF, doors lock, security system ON.
- Improves energy management with automation.

Advantages of ZigBee in Smart Home Systems

1. Low Power Consumption
2. Supports Large Number of Devices
3. Mesh Networking Improves Coverage
4. Reliable and Secure Communication
5. Low Cost Hardware

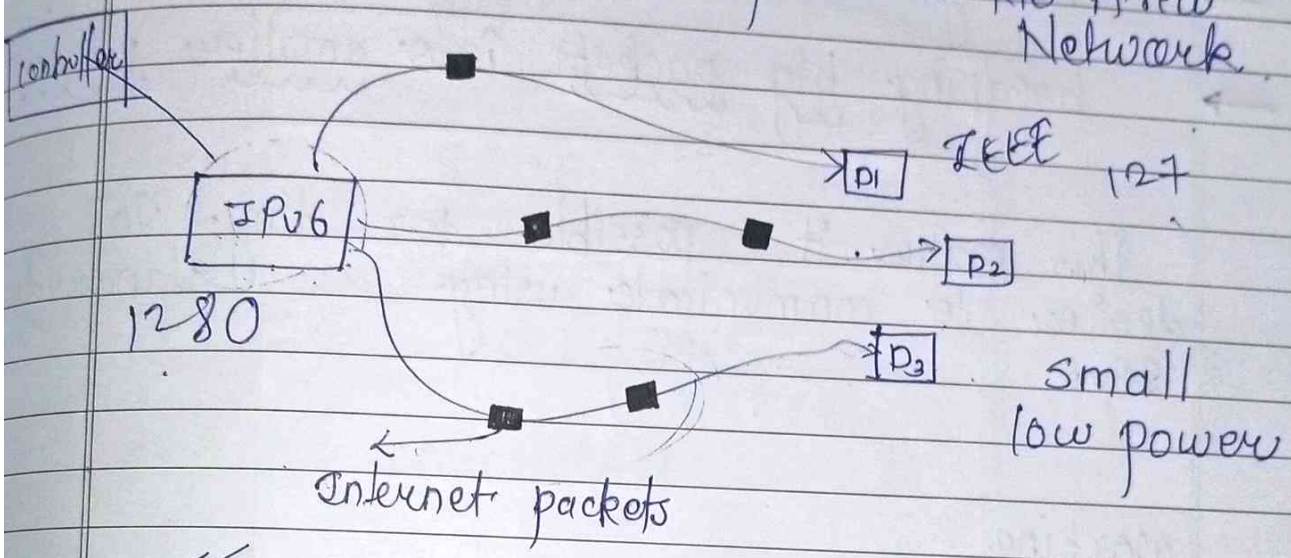
Disadvantages of ZigBee in Smart Home Systems

1. **Low Data Rate**
   20–250 kbps
2. **Requires a ZigBee Hub/Gateway:**
   Devices cannot directly connect to smartphones without a hub.
3. **Shorter Range Per Device:**
   Single ZigBee node has smaller range than Wi-Fi.
4. Slight delay due to multi-hop communication.
5. **Compatibility Issues Across Brands:**
   Devices from different manufacturers may not always work together.

IP BASED PROTOCOL

2. 6LoWPAN

IPv6 low Power Wireless Personal Area Network.



6LoWPAN, is a network protocol that helps send IPV6 internet packets over small & LP devices.

main problem,

IPv6 packets are large (1280 bytes)

IEEE 802.15.4 supports (127 bytes)

So IPv6 cannot directly fit into these frames.

1280 bytes → 127

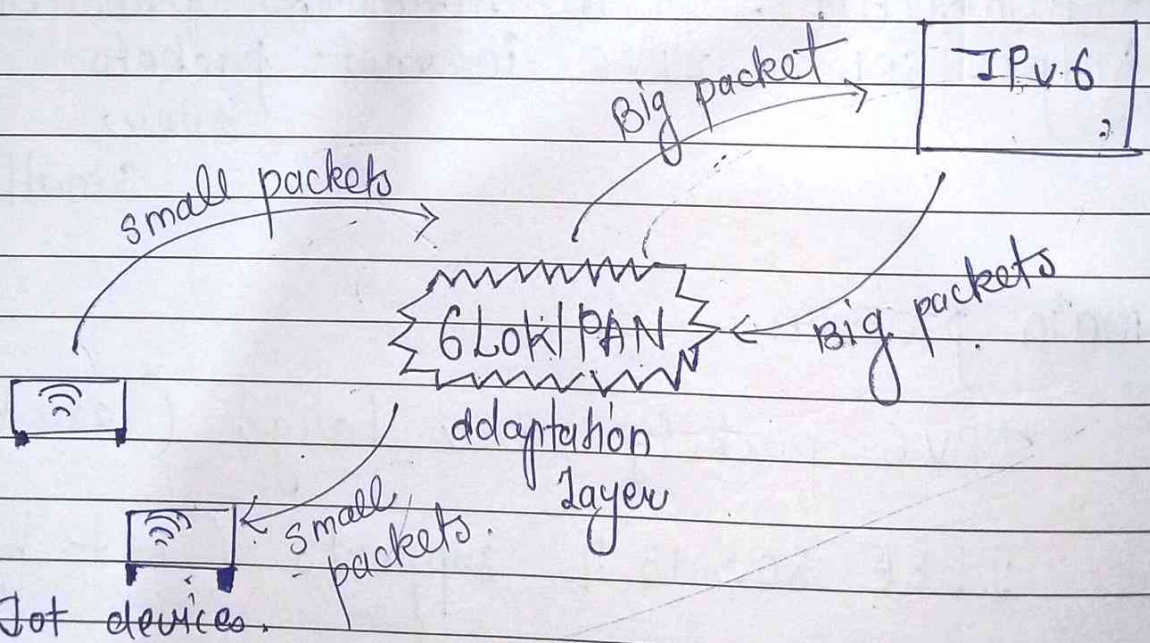
6LoWPAN solves :

→ making IPv6 header smaller ↓

→ breaking big packets into smaller pieces.

This makes it possible for tiny IoT devices to communicate using standard IPv6

working



step 1:
IoT devices uses IEEE 802.15.4.

- This provides low-power wireless comm^n but send small packets

step 2: IPV6

- It uses big packets.

step 3: 6LoWPAN

- It acts as a adaptation layer between IPV6 and IEEE 802.15.4.

step 4: compress + fragments.

Makes IPV6 header smaller

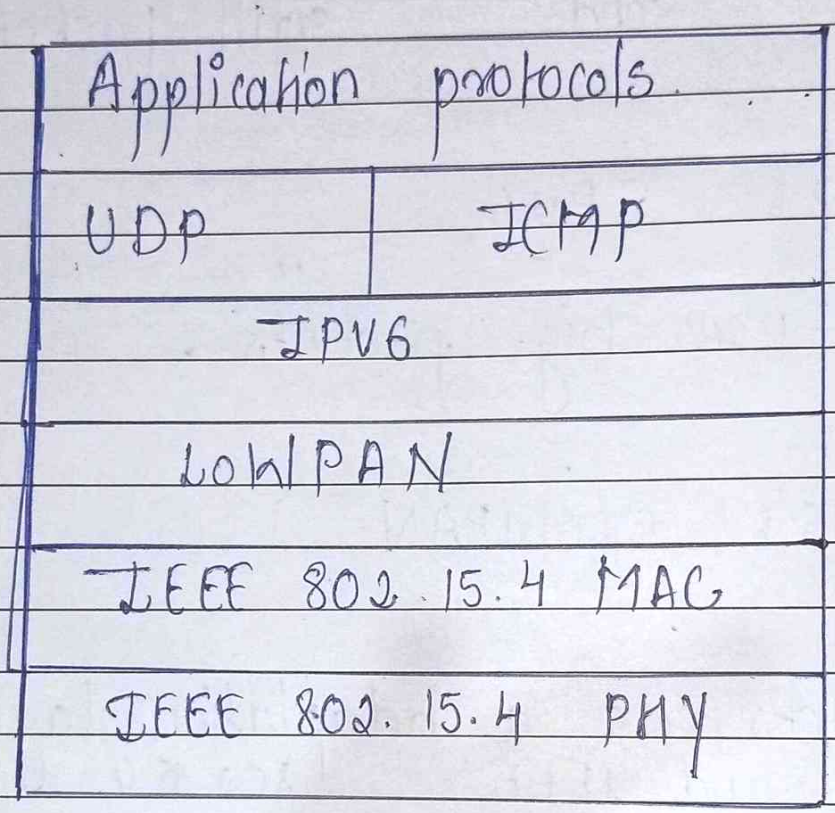
40 bytes → 2,3 bytes

Splits big IPV6 packets into smaller pieces.

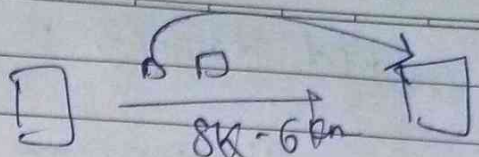
step 5: Rebuild.

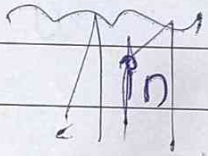
- When IEEE 802.15.4 sends small pices. 6LoWPAN combines all pices again.

6LoWPAN protocol stack

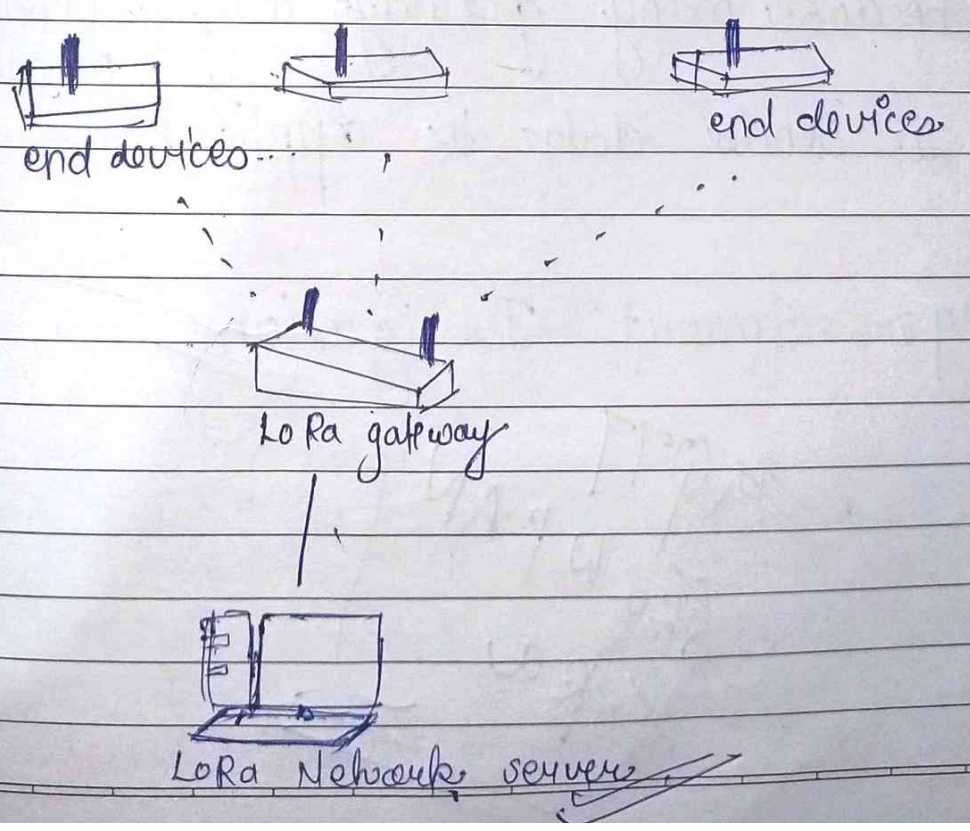


3. # LoRa



1. LoRa = Long Range.
2. It is a wireless technology used for IoT devices.
3. ✓ sends small data,
   ✓ over very long distances.
   ✓ uses very low power ↓
4. Range, 5 km  in cities.
   15 km in open rural areas

LoRa Network.



end devices :

small sensors : temperature sensor,
water meter,
GPS tracker.

They send data using LoRa.

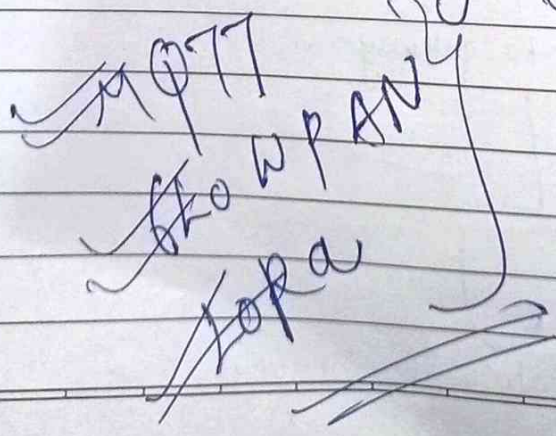
Gateways :

send → Recieve LoRa signals from sensors.

→ Network server.

1. Removes duplicate messages.
(because many gateways may recieve same message)
2. Sends data to application.

eg :- Smart Irrigation



LoRa in Smart Irrigation System

A smart irrigation system is one of the best application of LoRa :

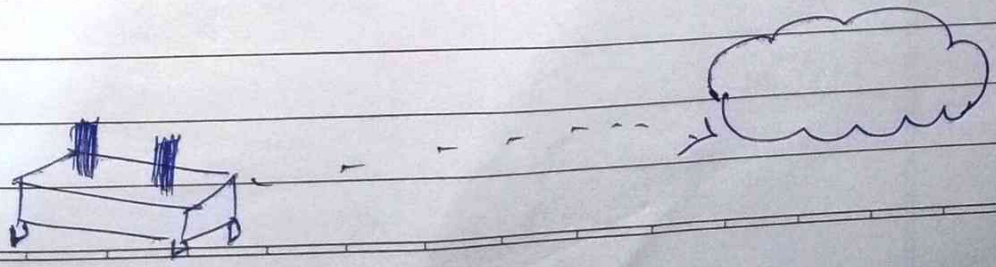
- Large farm area
- Less power availability
- Low data requirement

1. Soil Moisture sensor

Each fild section has LoRa node connected to soil moisture sensor

2. LoRa Gateway

- Recieves long range LoRa signals from many sensor.
- gateway
- ~~to~~ Now LoRa sends data to cloud.



3. Cloud platform :

- stores data
- sends control command back to gateway

4. Irrigation controller

- A LoRa connected controller can automatically switch :

Pump ON / OFF