CoAp:

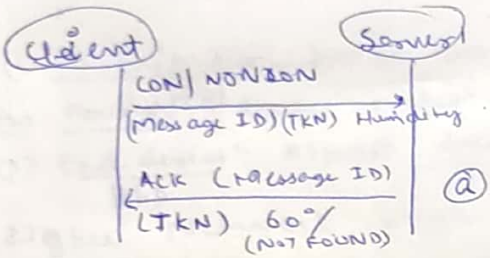
Constrained Application Protocol
- ↳ small devices, network.
- ↳ UDP (connectionless protocol)
- ↳ 4 byte header
- ↳ req / res (client, server)
- ↳ GET, POST, PUT, DELETE
- ↳ 4 msg
- ↳ one to one protocol

4 layer

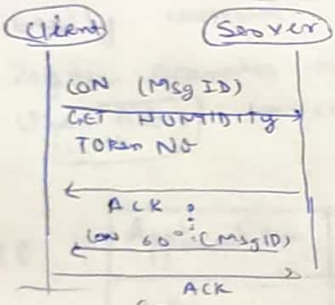
Application
Request / Response
Message
UDP

Req/Res
Msg

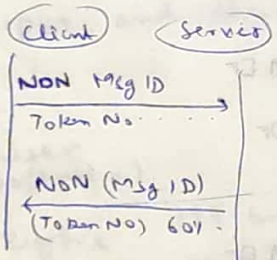
* Msg layer:
(CON) → conformable → keeps on resending until we get ack. after timeout.
(NON) → Non conformable
(ACK) → Acknolgment
(RST) → Reset



* Req / Res Layer
Piggy backed: client shall request with CON / NON.
Ack is recieved immediately with token no and message / message code (if failure) not

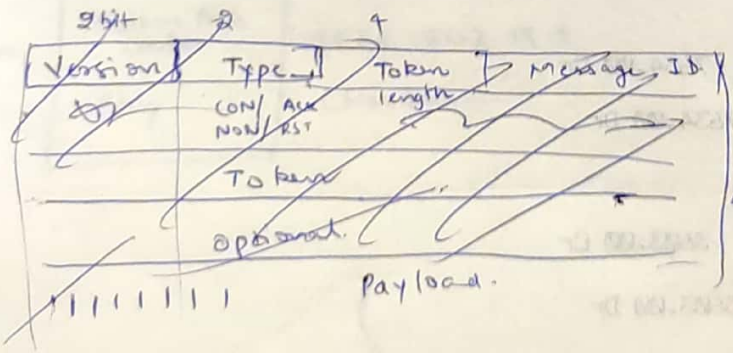


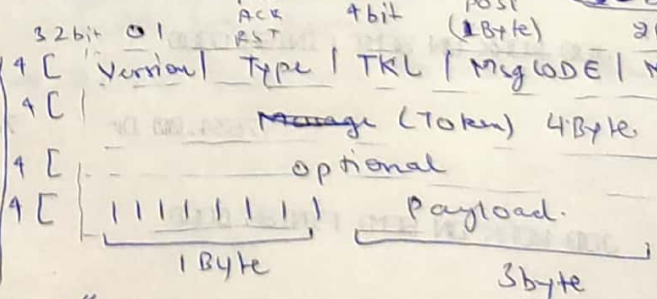
* Separate response
if server is unable to respond now, sends an ack that it will reponsd later, when it responds later, clients sends and ack.



* NON req / res
If NON req/res from client, no ack is sent back from client.

Message Format





enables asynchronous bcz (no Ack sometime)
both sync + asyc

ZigBEE

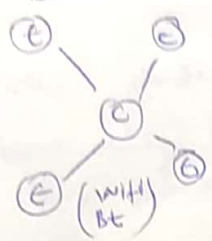
created for control and sensor (wireless)

AL
PL
SL
TL
NL — ZigBee + Additional communication Enhancement
DL (MAC) — IEEE 802.15.4
PL

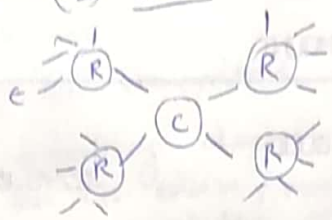
Topologies

3 nodes, Coordinator, Router, end device

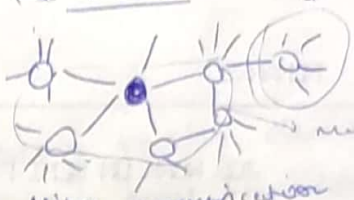
(1) Star



(2) Cluster



(3) Mesh



→ multihop communication
→ routing table

→ Mesh is connected network, hence reliable even is some nodes are down; scalable.
→ Self Healing, self configuration.

(1) Coordinator: holds most control on network, info related to transmission etc (one coordinator per network)
(2) Router (FFD) Route packets to neigh nodes connected to it.
(3) End devices: Almost dead most of time, Low power consumption.
RFD

Data Rate 250Kbps

→ Zigbee Network layer uses Adhoc On Demand Distance Vector Routing.
→ Easily connect large no of battery operated devices (wifi / Bluetooth me zyada power consumption)
→ Zigbee operates at low data rate as compared to wifi / bt.
→ Use AES 128 bit to encrypt and dec.

2 state of operation
→ Active, Sleep.

→ Coordinator selects channel and creates PAN ID, other devices joins using PAN ID
→ end devices are generally battery powered, can communicate only with its parent.
→ XCTU (software to install to use it)

App	Application	User (software)
stack	API Security N/w	Zigbee (Network & security) — 128-bit AES Mesh Top.
silicon	Medium Access control Phy	IEEE-802.15.4 (Hardware)

→ aim is making plane from data plane and centralize the netw control routing flexible. IP address much more programmable so that packet

→ Data plane is the data to be transmitted
→ control plane is basically the routing decision, every routers decided the best route for packets on its own, routers doesn't have the global vie of the network.

Since SDN is global view
→ easily to make routing decision
→ traffic monitored
→ routing decision.
→ easy manage Wireless Sensor Network (WSN)

Key principles of SDN

→ Makes networking & IP routing flexible
→ Decoupling control & data plane. (Centralized control)
→ Central view of Resource (so we have network status Availability)
→ Offload brain to centralized control.
→ Programmable network, centrally managed
→ Abstractions, easy to change bandwidth etc

SDN - WSN advantages over Traditional WSN

→ Packet Delivery ratio is large
→ Energy consumption is reduced due to central coordination.
→ Msg overhead is reduced

DDOS Attack (Network → API with not giving ack back.)

Application layer → HTTP | DNS flood overload with millions fake request using multiple bots.

DDOS is distributed DoS, hence we have to use multiple components to perform the attack like bots etc.

Attack on SDN

→ Data Plane layer
  - Denial of service (DoS)
  - Traffic diversion (divert the traffic)
  - Malinformed control message injection
  - ~~insert~~ Spoofing and Tempring

Control Lanke | Plane
  - Meet in the middle attack
  - Replay attack.
  - Eavesdropping

Active Passive attacks of Crypto

~~Attac~~ controller layer
  - spoofing and Tempring
  - Distributed Denial of Service (DDOS)

Detection!

↳ Machine learning
  ↳ DT, RF, NB, ANN.
  dependent on dataset used for training

↳ Traffic Patter Analysis
  ↳ SNORT, Entropy
    ↳ tell wrongness in the packet set.
  ↳ collect stastics like
  # of flows, Packet rate, Avg packet | flows, Avg Byte | flows
  These are compared with a predefined threshold limit and chcek if there is attack or not

ARP Poison / ARP Flood attack

(Address Routing Protocol)

ICMP → Internet Control Msg Protocol

Hacker make millions of ARC requests

→ Server is just able to reply to few as it is overloaded, moreover these requests fake hence the genuine requests are never responded.

can be prevented using Blockchain

Blockchain is distributed network hence before changing something it acknolgdes other system in network, the other system reject the request, hence the fake request are never responded. Blockchain is foundation of immutable ledgers, or records of transactions that can't be altered, deleted destroyed. They are distributed.

LORA

→ Cellular data allows to send large date over large network over high speed. (4G, 5G) but there is high power consumption (we charge our phone :))

→ In IoT, we need a low power, wide area, low Data Rate (acceptable)

LoRa (Long Range) Low power RF modules

Application layer

Media Access control (MAC)] LoRa WAN

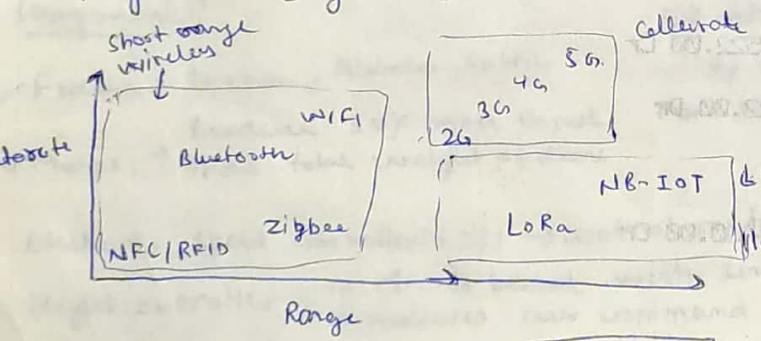
Physical layer } LoRa

LoRa uses CHIRP spread spectrum modulation technique that makes low power & high range possible. (Device)

LoRa WAN is communication protocol.

→ LoRa Nodes
↳ sensors + microcontroll + Radio commun
↳ run on battery (star topology)

→ LoRa Gateway
↳ several node connect to gateway over network, data moved to Application layer. (bidirectional)

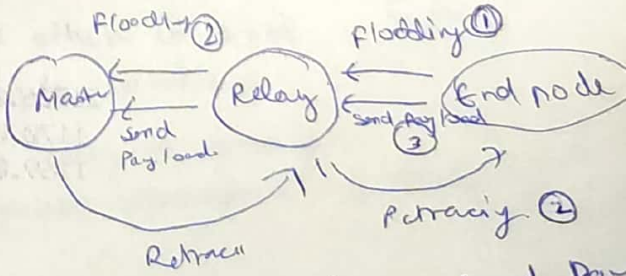


end devices → gateways ↔ Network ↔ Application

LoRa WAN

TCP/IP, MQTT

A chirp is a sinusoidal signal whose frequency increase or decrease over time. Resistant to doppler effect and can be detected even in low signal to noise (SNR) environment.



Flooding, Retracing, Send Pay

IPv6

6LOWPAN | Low power wireless Personal Area Network

→ lies above IEEE 802.15.4

→ Star + mesh topology

→ Small packet size (128bit), low power, low bandwidth (250 kbps)

→ which protocol? interoperability, scalable, secure, Plug & Play, scalable, flexible (IPv6)

→ Interoperability means that the application need not know the constraints of physical links that might carry their packets

→ It is based on CSMA/CA mode (collision avoidance)

→ Fragmentation | Reassembly of IPv6 packets.

→ 6LOWPAN on network layer.

→ There is an adaptation layer b/w Network layer and Datalink layer

(IP) ——→ (IEEE 802.15.4)

Compression + Fragmentation | Reassembly to increase payload &

UAVS (Unmanned Aerial Vehicles) | Drone

Unmanned aircraft system (UAS)

4 rotors

Uses: photography, research, military, cinema, medical, commercial, geographical

Pitch, Roll, Pitch,

Components:

✓ Frame — carbon, Alumin, fabric

KV rating tells the rpm at a voltage of the motor

Rpm = kV × Voltage

✓ Motor → Produce 50% more thrust than total weight of drone

For high performance high kV rating

Electronic speed controller (ESC) → control motor speed, recieves signal from the controller

Flight controller → circuit board with sensors which detect orientation change, → recieves user command

Communication

Propellers (blades) → generate trust and torque to keep drone flying and maneuver (thrust ∝ (spin speed))

2 propellers in clockwise and other in anti

Battery

Pitch → distance travelled in single rotation

↓

LIPO battery is used

→ Propeller with small size are easy to speed up.

→ ~~↑ pitch~~ ↑ pitch ↑ speed ↑ power consumption ↓ steady

Sensors

Barometer → Altitude
Gyroscope → orientation
Accelerometer → Linear acceleration in x, y, z direction.

Orientation

- Throttle → Vertical up and down motion
- Yaw → left and right rotation of drone
- Pitch → Forward and backward.
- Roll → controls side to side tilt.

Mode of communication

→ Radiowave, bluetooth, Wifi, Infrared, Radio controller (RC)

PID Tuning (Proportion, Integeral, Derivate) determines how responsive is drone to cont

Face recognition: (identification + Recognition)

DGCA Directorate General of Civil Aviations
some rules and regulation on drone flight.

- Application:
  SLAM → Simultaneous Localizing and Mapping

IOT Device Classification and security

Classification of Attack:

Application Layer → HTTP/ DNS Flooding, Mal. code injection, Brute Force
Transport layer → Flooding; Spoofing and Tempering.
Network layer → Traffic Diversion, Routing based Attack, Sleep Derivation Attack
Data link layer → Collision Attack, Replay Attack
Physical layer → DoS Attack, Eavedropping; MITM

ML in IOT
↳ Manual selection
KNN, NB, DT, RF
Ensemble Techniq → AdaBoost, XG Boost.
→ Automal selec
ANN, LSTM, CNN

Preprocessing of IOT devic
→ IOT Network Traffic → Capturing → Filtering/ Splitting → Flow construction (TCP/UDP) ← Feature Extraction (packet level, flow level, behaviour level) ← Traning Model

Collecting dat

Preprocessing

Attacks of IoTS

⇒ **SYN Flood Attack** type of DoS by making server unavailable by consuming all the resources by introducing false traffic.

→ Works by exploiting handshake TCP connection.

→ client send SYN packet to servers.
→ Servers respond with ACK/SNY packet
→ Client sends returns ACK, establishing TCP connect

} Three Way handshaking (TCP)

→ Seend large SYN packets with fake IP address / false IP addre
Server respond with SYN/ACK and waits to recive ack from client which never arrives. and client keeps on sending spoof SYN packets

⇒ **ARP Attack Poising**

- Address Resolution protocol enables network to reach specific device.
- Traslate IP addre ↔ MAC Address.
- ARP cache → Mapping of IP address and MAC address, if entry is not found it asks of MAC address for certain IP address and sends out ARP packet
- ARP poising → Meet in the Middle Attack, now attacker knows both IP and MAC address.

SMURF Attack → DDoS (Echos of Victim's IP address) large number of Internet control Message Protocol (ICMP) packets with Intended Vitions IP adress will be send. If machins are large in network, the victim's computer will be flooded with traffic, which will slow down his computer.

⇒ **PING of death** DoS attackers aims to disrupt target machine by sending packet larger the allowable size, causing target machine to crash.

Raspberry Pi

→ Single Board Computer (SBC)

→ 32 bit microprocessor, vidoo, audia, USB & Ethernet, HDMI, sd card, GPIO pins wifi modul, Bleuetooth

Components of Raspbery pi:

→ Ethernet cable, bluetooth, wifi

→ Audio, ~~Port~~ Video

→ CSI camera Port (add a camera roll to it, for taking pictures) (bulgary detection etc)

→ HDMI → High Defination multimedia Interface

→ Powered using micro USB with 2.5 A current.

→ DSI Display Port → connect OLED of etc

→ Micro SD (as a memory)

→ GPIO pins (connect sensor, input & etc).

→ CPU, GPU, memory chip

→ 4 USB port.

Operating system
NOOBS
Raspbian
Ubuntu Mate etc
Windows X

Total 40 GPIO Pins
3.3 V, 5 V, 8 GND Pins, UART (Universal Asynchronous Reciver) Trasmitter)
(2) (2)

Only digital logic

program can be written in python

```
mport RPi.GPIO as GPIO
PIO.setmode(GPIO.board)
PIO.setup(3, in)
PIO.setup(5, out)
PIO.input(5)
IO.output(5, Low/High)
```

Blockchain: decentralized network.

Benifits of using blockchain in IOT

→ Data Security.
→ Firewall against DDoS / Secure gateway.
→ Real Time Tracking
→ More access control
→ Stronger cloud mangment
→ Encryption for Multi-factor Authentication
→ Collaborative environment for shared economy.

* Block chain IoT use Cases

→ Supply chain managment:
- can introduce IoT integrated vehicles that can track the shipment until delivery
- Iot sensors can help company to get crucial info about shipment status like pressure, motion, temperature.
- Reliability can be improved using Blockchain
- Ones data is added to ledger, stake-holders can use smart contract to get access in real time
- companies can automate transaction.
- track entire process making manufacturing effiernt and good quality.

→ Smart Home
→ can store sensitive data like face ID, fingerprints, Voice ID. etc

→ Pharacy
manufacturing of drugs
- Application can track any legal chages in ownership of the prescription to avoid false chage.

→ Smart Parking
discover parking slots nearby, using blockchain we can get real time traffic control by amount of traffic present.

→ Smart Payment Crypto currency.

→ Agriculture → increase customer trust, weather impact and other external factors to increase quality of crops.
→ traceability of food products
→ smart contract paid in advance