Unit IV
IoT Protocols

(Prof. P. R. Patil)

≫ Protocol Standardization for IoT Efforts

- IoT Standardization is needed for data representation & protocols.
- Following areas that need to be concentrated in achieving IoT standardization.

① To create an architectural foundation for IoT that will be interoperable with future internet
② Using existing technologies instead of creating new ones.
③ Proving usability of applications with help of use cases.
④ Creating interdisciplinary goin which targets more deployment aspects that will generate strong stakeholders.
⑤ Uniting heterogenous IoT technologies into a single IoT entity.

Standardization of IOT:-
① Work Package (WP) framework
② Internet Protocol for Smart object (IPSO)

① Work Package (WP) framework
- WP framework defines overall gross view of an IoT systems with respect all stakeholders.
- Service providers, developers, investors & users can gain insightful knowledge from work package framework.

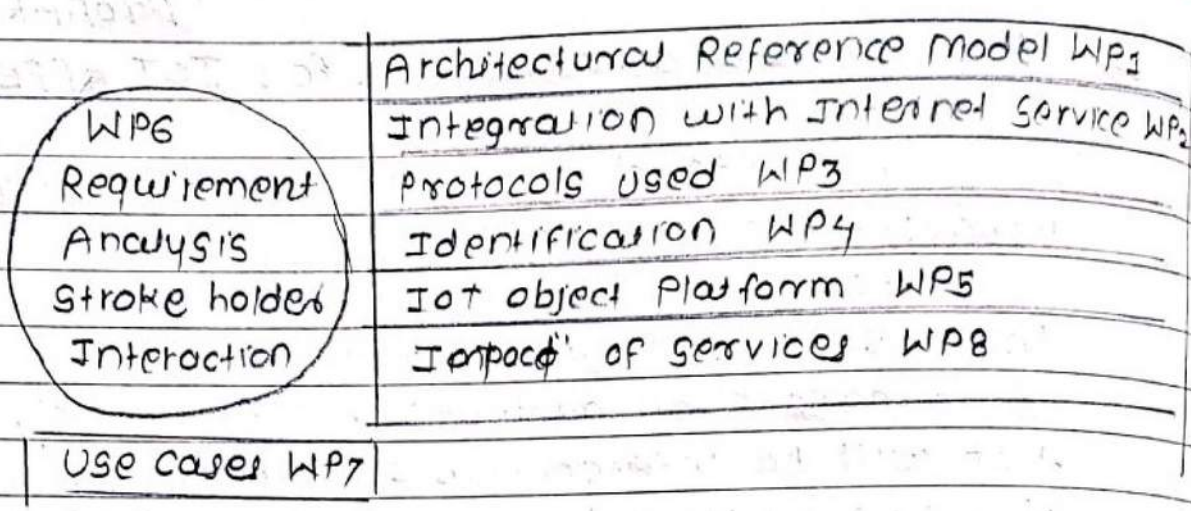

Fig. General Work Package Framework

- As shown in fig. WP framework gives implementation standards for developers using architectural reference model.
- Which smart objects will deployed in the field, How they will be communicating i.e. protocols used & service identification & How this service will be integrating with future developments of IoT. All things are described in Architectural Reference Model.
- Architectural Reference Model is generated by gathering requirements from stakeholders and they are validated by stakeholders time to time.
- WP also defines ① use cases of the appln which gives clear idea of available functionalities ② circulation of these services worldwide & its impact over the business.
- Maintenance strategy & coordination of appln after deployment.

(2) Internet Protocol for Smart objects (IPSO)

- IPSO defines an All IP approach for IoT Standardization.
- IP defines high wide range of protocols that can be used to create highly scalable comm^n technology.
- IP provides an open, lightweight, stable, pervasive & managable way to comm^n betn appln & services.
- IPSO defines a smart object as
  1. An RFID Tag (Intelligent device)
  2. Sensor - A device that measures physical change in analog or digital format.
  3. An Actuator - A device that is able to alter or control physical devices in field
  4. Embedded device - to serve specific functionality.

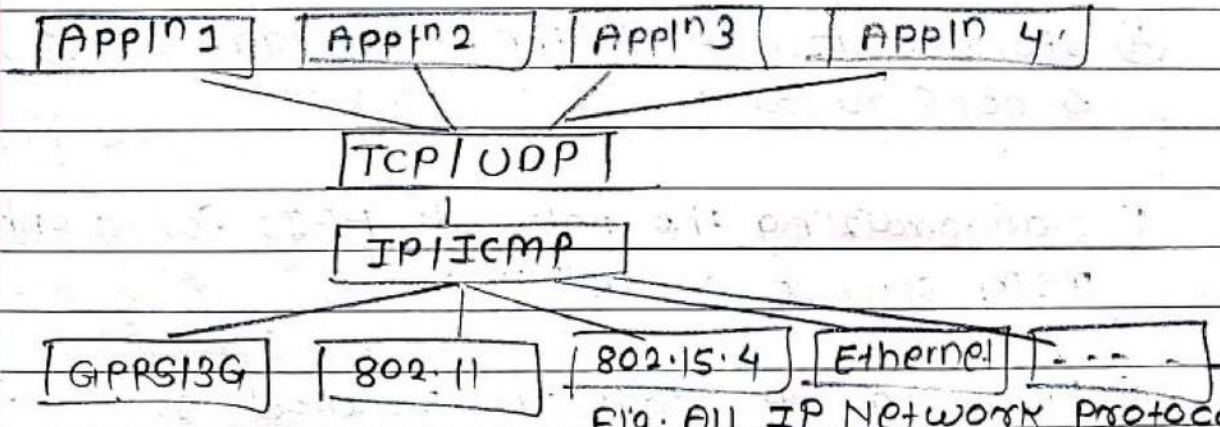

Fig. All IP Network protocols

- IPSO uses IP based network protocols to comm^n betn lower level devices & top layer appl^n.

DOMS Page No 4
Date / /

≫ M2M & WSN Protocols

- M2M protocol & WSN protocol standardization is important for growth of M2M & IOT industry.

» M2M Protocol Standardization Activities

① Data transport protocol standards
- Focusing on the standardization of JSON, M2MXML.

② M2M device protocol standards
- Extension of OMA DM such that it can be collaborated & supported M2M protocol management objects.

③ Standardization of the device management for M2M.

④ Standardization of the device gateways system & configuration.

⑤ Standardizing the network APIs for to enhance M2M service capabilities.

⑥ Resolving IP addressing related issued for devices supporting IPV6.

⑦ Standardization related to remote provisioning & discovery.

(2) WSN protocol Standardization activities

- There are many standard bodies in area of wireless sensor network. The concentration of IEEE is on physical layer & MAC Layer.
- IEEE 1452 is a standard for set of smart transducer interfaces which allows to develop network independent common & open interface for connecting sensors & actuator.
- The primary objective of this standard is to provide a standard & common interface for connecting diff transducers (sensors & actuators)

Activities include :-

1. 1451.0-2007 - Standardization of interface fun, comm protocols
2. 1451.1-1999 - Network capable appln processor information model.
3. 1451.2-1997 - Transducer to microprocessor comm protocols
4. 1451.3-2003 - Digital comm.
5. 1451.7.2010 - Transducers to RFID system comm.

≫ SCADA & RFID Protocols

- SCADA & RFID are enabling technology

(1) SCADA standardization activities

- More advanced commercial cloud appln SCADA is popular in IOT appln.
- Std C37.1 is the IEEE standard for the automation system & SCADA (Supervisory control & data acquisition)

- IEEE Std C37.1 SCADA architecture is suited & applicable to recent automation based industrial upgradations.
- for power system it can be observed that processing is now distributed: functions & operations which had to be performed by control centred is now performed by systems called IEDs (Intelligent electronic devices). They can be IoT devices too.
- SCADA is standardized in sense that how diffn vertical standards (specific industry technology standards) interact with each other.

(2) RFID Standardization Activities

- RFID data formats & protocols are well defined by EPCGlobal.
- Electronic product code Information Service (EPCIC), object Name service (ONS) are some standardizations in RFID.
- Physical markup Language (PML) is XML like language which defines its own tags to represent data related to individual Electronic product code.
- Appln level events & ALE) standard created by EPCGlobal specifies an interface to write a business logic to specify behavior & functionalities of software.
- One such standardizations is being used in contactless payment system which uses RFID archi.
- Contactless smart card payment system uses ISO/ISE 14443 Standardizations & ISO/ISE 15693 which allows commn.

Issues with IoT Standardization

- IoT standardization provides a solid way to develop IoT based systems but it also limits the innovation & productivity in some cases.

» Challenges & issues in standardization of IoT

- Many standards for internet are not adequate for supporting IoT efficiently since IoT didn't exist when protocols were designed & implemented.
- There are no global validated standardization frameworks at the IoT stack level.
- Diff^{n} organizations, forums, alliances & groups are working on their own with limited scope & focusing areas only they are comfortable with.
- Example EPCGlobal works only works with RFID while 3GPP for cellular networks only.
- ICT standardization is highly decentralized activity. Now challenge is how these activities of heterogenous standards can be coordinated
- It is a challenge to develop a platform where various forums can collaborate to develop the standardization for IoT.
- It is essential to allow all interested stake holders to participate in the IoT standardization process towards & understand their requirements.

≫ Unified Data Standards

for comm^n & data exchange.

- The Internet was originally Internet of multimedia & documents. So WWW & Internet use HTML & HTTP to represent data over Internet.
- most protocols use XML based file representation which makes data exchange easier for heterogenous techniques.
- Resource Description Framework (RDF) is work of W3C (Word wide web consortium) for metadata model.
- RDF can be used for modeling of information that is deployed as web source, various syntax formats. used for WOT appln.
- SOAP & REST frameworks used to provide data exchange protocols for IOT appln.
- Electronic Data Interchange (EDI) is a technology that describes format of electronic documents that can be shared over Internet.
- EDI defines techniques FTP, email, HTTPet
- Combination of two famous techniques EDI & XML gives new technique called ebXML.
- ebXML used for e-commerce coln for interaction betn two parties.

Additional formats accepted by WOT are

1. CBRN - Chemical, Biological, Radiological & Nuclear data
2. EXDL - Emergency data exchange language of OASIS.
3. M2M XML - Machine to machine XML.

>> Protocols - IEEE 802.15.4

- Institute of Electrical & Electronics Engineers (IEEE) group defined 802 standard protocol for physical & data link layer technologies. It explores, physical layer & media Access control protocols are specified in IEEE 802.15.4 standards & Logical Link Control Layer is defined in IEEE 802.2 standards.

- IEEE 802.15.4 standard published in 2003.

- IEEE 802.15.4 defines physical layer & MAC layer comm^n methods used to access wired & wireless network.

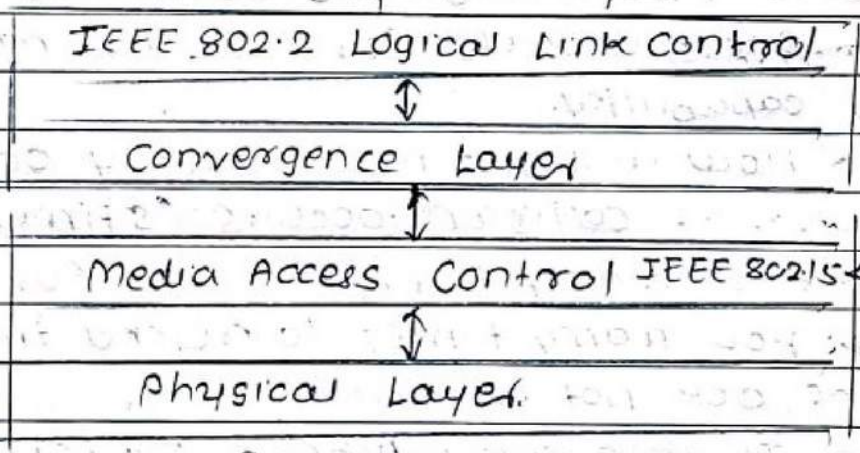

fig. IEEE 802.15.4 Stack

- Data frames are sent via physical layer & MAC layer to LLC for formatting.

- The LLC IEEE 802.2 standard converts this data frames into defined frame formats which are understable to upper layer.

>> IEEE 802.15.4 : Physical Layer

- Federal comm^n commission (FCC) manages the distribution of frequency band in USA.

- FCC avocated frequencies for Industrial Scientific, medical appln & for transmission power below 1 Watt doesn't require license.

>> IEE 802.15.4 : Media Access Control Layer

- 802.15.4 describes MAC in two parts one MAC layer responsible for data transfer also known as MAC common part sub layer (MCPS) and second part responsible for MAC layer management also known as MAC Layer management Entity (MLME)

- MLME configuration & state parameters for MAC Layer.

- It contains following details

> which addressing to use 64 bit IEEE address called as Extended Unique Identifier (EUI-64) or 16 bit short address for node having less computational capability.

> How many times to retry accessing the network if collision occurs. (5 times max)

> How many times to wait for acknowledgement

> How many times to resend the packet in case of ack not received ?

- It this way MAC layer handles frame validation, time slots for packets & manages delivery of packets.

802.15 frame Format

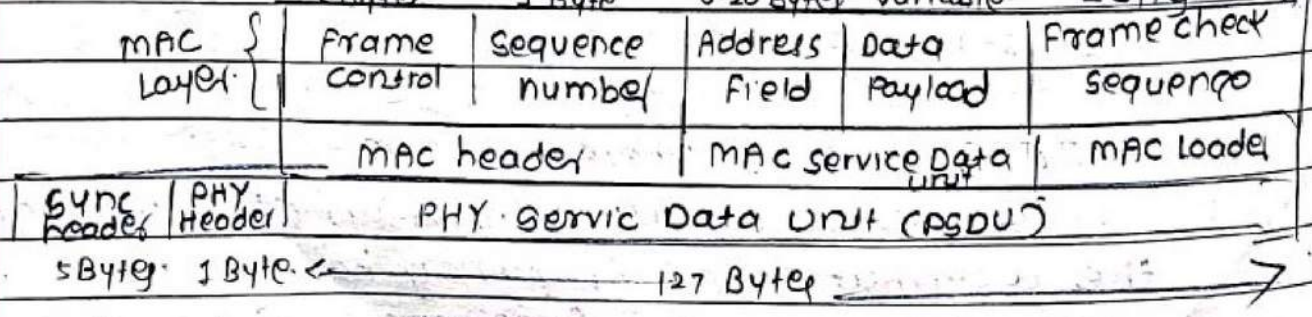

Fig. IEEE 802.15.4 frame format

- MAC layer frame resides above PHY layer frame.
- Data upload part containg the data to be transferred in network layer.
- sequence number & frame check sequence (FSC) manages ack.

» Limitations of IEEE 802.15.4
- It has maximum packet size of 127 byte. so appln needs to take care of packets that might exceed limit.
- Limited bandwidth is also an issue.
- PHY layer waits for ack so packets can't send continuously.

» Uses of IEEE 802.15.4
- It is suited for IoT appln working with multiple sensor nodes.
- Network maintenance is low cost & reliable.

» ~~BACNet (Protocol)~~

- BACNet (Building Automation & control Networks)
- BACNet targets industrial automation & control mechanisms.
- BACNet is object oriented protocol which views its implementation in form of objects.
- BACNet protocol defined by three characteristics object, services & properties.

ModBus :-

- ModBus is a serial comm^n protocol developed by Modicon Inc in 1979.
- ModBus is an appln layer protocol which provides client server comm^n to the devices connected via buses & network.
- ModBus works on top of serial comm^n standards like RS232, RS442, RS485.
- ModBus works with master slave model. One master device initiates the transaction by generating query and sent it to an individual slave address or broadcasted in the network.
- Modbus has two mechanism modes that defines framing & bit encoding for message to be transmitted on the network.
  - American standard code for Information Interchange (ASCII) Transmission mode.
  - Remote Terminal Unit (RTU) Transmission Mode.
- All the nodes in the ModBus Network have to use the same transmission mode & Serial parameters to function.

ASCII Transmission Mode

- Coding System
  - One Hexadecimal character is contained in each ASCII character of message.
  - ASCII character 0-9, A-F

START	ADDRESS	FUTCTION	DATA	LRC CHECK	END
1 CHAR	2 CHARS	2 CHARS	n CHARS	2 CHARS	2 CHARS FILE

Fig. ModBus ASCII Message Frame

- Each ASCII character is sent separately as
  - 1 start bit
  - 7 bit for even / odd parity, no bit for no parity.
  - 1 bit for even / odd parity, no bit for no parity
  - 1 stop bit if parity is used.

- Longitudo Redundancy Check (LRC) is used for error checking.
- Advantage of ASCII mode is interval of one second between two characters without causing error.
- Message starts with a represented by ASCII 3A hex & CRLF defines carriage return line feed ASCII 0A & 0D to specify end of frame.

≫ RTU transmission Mode

- Cyclic Redundancy check is used for error checking.
- Each msg is transmitted in continuous stream, time delay causes error.
- RTU doesn't have specific characters to represent start & end of frame in ASCII

START	ADDRESS	FUNCTION	DATA	CRC CHECK	END
T1-T2-T3-T4	8 BITS	8 BITS	nX8 BITS	16 BITS	T1-T2-T3-T4

Fig. ModBus RTU Message Frame

>> ModBus Address

- ModBus address begins with 8 bit addr of target that ranges from decimal value 1-247.
- 0 is for broadcast address.
- Each query has address of specific slave defined in frame format for both addr.

>> ModBus function

- Function defines the action to be taken by message.
- ModBus fun^n field containg 2 characters in ASCII mode & 8 bits in RTU mode

example.

① ModBus function 0x02 : Read Input Status.
② ModBus function 0x11 : Report Slave ID.

>> ModBus Data Field

- Data field defines the appln level information to be used by ModBus fun^n.
- When data size is variable byte count needs to be specified at start of data field.

>> KNX

- KNX Standardization (Konnex Association) was formed by the merger of three European companies working for Smart Automation of homes & buildings.

≫ Zigbee Architecture, Network Layer, APS Layer

Zigbee

≫ Zigbee Architecture

- Zigbee resides on top of the PHY and MAC Layer defined in 802.15.4 PHY & MAC Layer provides functionality of OSI physical & link layers.

≫ Application Support (APS) sublayer

- APS handles 64 bit IEEE to 16 bit zigbee address mapping.
- APS routes the network layer message to a suitable appln object. Each application object is identified by endpoint ID.
- APS maintains a local binding table that holds record of remote nodes & endpoints registered to receive message from local endpoint.
- APS also handles acknowledgements, retry sending messages if not received & data appln.

Octets: 2					
Frame control	Destination address	Source address	Radius	Sequence number	Frame payload
		Routing Fields			
	NWK header				NWK payload

Fig. Zigbee NWK Frame format

>> Zigbee Device Object (ZDO)

- ZDO is a special appln running on Endpoint 0 & manages the state of Zigbee Node
- ZDO initializes the APS, NWK & security service provider.
- ZDO provides interfacing betn appln objects, zigbee Device Profile & APS.
- ZDO provid manages security policies & security configuration of a device provided by security Service Provider.
- ZDO gathers configuration information from endpoint appln & provides device & service discovery.

>> Zigbee Cluster Library

- ZCL was added in zigbee architecture & defines a library of interface specifications like commands & attributes used for appln profiles
- ZCL also provides functionalities for network interface group information & management.
- ZCL acts a common mechanism for appln development even with ongoing development of zigbee.

>> Zigbee Application Framework

- This provides API for zigbee appln development and each zigbee appln is apparted in endpoint starting from 1.

=> Types of Zigbee Node

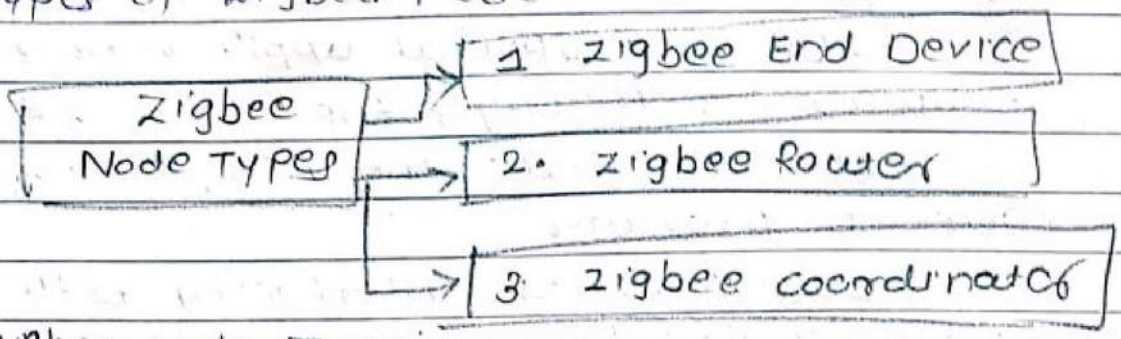

fig. zigbee node Types

① Zigbee End Device (ZED)

- ZED works with 802.15.4 & provides fully reduced functioning device (RFD)
- These nodes are battery operated & are not always listening or sensing.
- ZED has connect to a network layer via zigbee Router which acts as its parent.

② Zigbee Router (ZR)

- ZR works with 802.15.4 & provides fully functioning device (FFD).
- ZR are permanently listening & able to route packets once it's joins the existing zigbee network.

③ Zigbee controller (ZC)

- ZC works with 802.15.4 & provides fu functioning device.
- ZC can create network & can also acts as 802.15.4 based personal area Network (PAN) coordinator
- ZC can form a network & can also connect to the existing network & are able to route packets in such cases ZC becomes ZR.
- ZED also acts as ZR.

⇒ Zigbee Network Layer (NWK)

- NWK provides multihop routing of data packets in mesh network which is not available in 802.15.4.
- zigbee use short address allocation to nodes ranging from 0x0000 to 0xFFF7.
- zigbee coordinator node use short address 0x000.
- zigbee supports two address allocation mode:
- Stock profile 0x01 in which address is allocated based on the position of the node in mesh / tree topology. Each potential parent node is associated with sub block of network address.
- Stock profile 0x02 use random address allocation mechanism & any address conflicts are detected & resolves by zigbee.

⇒ Zigbee Network Layer Frame Format

Field	field size in octets (& bits)
frame control	2
Destination addr	2 or 8
source addr	2 or 8
Radius	1
Sequence number	1
Payload	Variable

- Frame control bits are used to define various parameters like:
  - communication type - unicast / multicast
  - security enabled / disabled
  - Route discovery enabled / disabled.
  - Source IEEE address is specified or not.
  - Destination IEEE address is specified or not

- Address field can be 2 or 8 octets to handle 16 bit zigbee address or 64 bit IEEE address.
- Radius defines maximum number of hops allowed for packet.
- Sequence number is packet counter
- payload carries APS & NWK layer commands if any.

>> Zigbee APS Layer

>> zigbee APS layer

Field	Field size in octets (8 bits)
Frame control	1
Destination point	1
Cluster Identifier	1
Appln profile Identifier	2
Source endpoint	1
Counter	1
payload	variable upto 80 bytes

- APS manages & provides support for local appln & also provides mechanisms for developing & interconnecting zigbee appln.

* IP Based Protocols :-

- Internet Protocol (IP) provide delivery of packets from one host in the Internet to any other host in the Internet, even if the hosts are on different networks.
- It provides unreliable & connectionless datagram delivery service.
- Internet packets are called "datagrams" and may be to 64 KB in length.

Key advantages of Internet protocol :-

① Versatile :-
Layered IP architecture as well equipped to cope with any of physical & data link layers.

② Ubiquitous :-
All recent OS releases have an integrated dual stack that gets enhanced over time.

③ Scalable
IP has massively deployed and tested for robust scalability.

(4) IP is manageable & highly secure.
(5) It is stable & resilient.

* MQTT

- message queue Telemetry Transport is open connectivity for mobile, M2M & IoT.

- MQTT is designed for high latency, low bandwidth or unreliable networks.

- MQTT is lightweight broker based publish subscribe messaging protocol is that designed to be open, simple, eightweight & easy to implement.

* MQTT Characteristics

(1) Lightweight message queueing & transport protocol.
(2) Asynchrous communication model with message (events)
(3) Low overhead for low to network bandwidth application.
(4) Publish / subscribe model:
(5) Decoupling of data producer through topics.
(6) Runs on connection oriented transport.

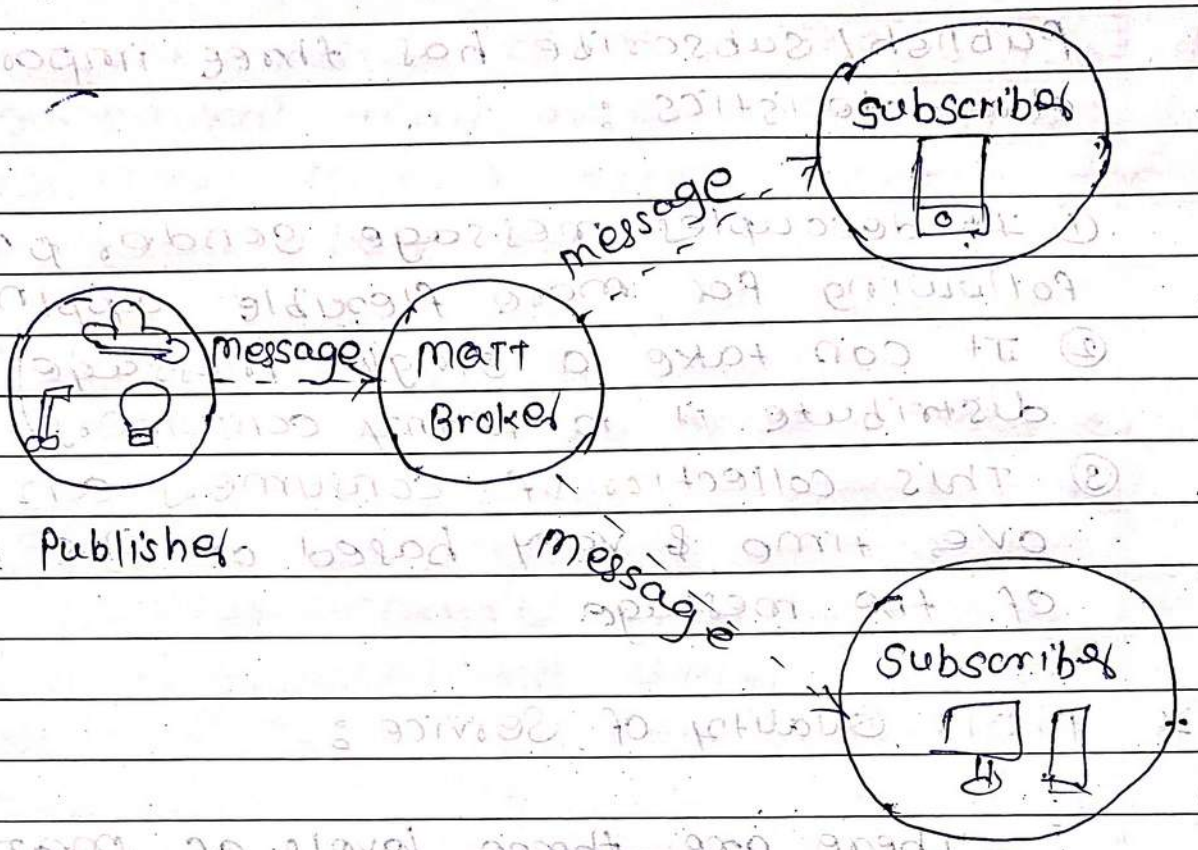

Fig. MQTT Publish/ Subscribe framework.

- Producer publishes a message (publication) on a topic (subject).
- consumer subscribes (make subscription) for a message on a topic (subject)
- message server called broker matches publications to subscription
- If none of them match the message is discarded after modifying the topic If one or more matches the message is delivered to matching consumer after modifying topic.

Page No.
Date

Publish / subscribe has three important characteristics :-

① It decouples message sender & receivers following for more flexible appln.
② It can take a single message & distribute it to many consumers.
③ This collection of consumers can change over time & vary based on the nature of the message.

* MQTT Quality of Service :-

There are three levels of MQTT QoS.

① QoS : AT most once

- Guarantees that a particular message is only ever received by the subscribe a maximum of one time.
- The sender & receiver will attempt to deliver the message.

② QoS : AT Least once

- Guarantees that message will reach its intended recipient one or more times the sender will continue to send the message until it receives an ack from receipient, confirming it has received the message.

- The result of this QoS is that the receipient may receive the message multiple times & also increase the n/w overhead than QoS 0.

③ QoS2 : Exactly once

: The most costly of the QoS will ensure that message is received by a receipient exactly one time.

This ensures that receiver never gets any duplicate copies of the message & will eventually get it.

* Difference between CoAP & MQTT

	CoAP	MQTT
①	CoAP uses UDP Protocol	MQTT uses TCP Protocol.
②	It uses Request/ Response messaging	It uses publish/ subscribe messaging
③	Comm^n model is one to one.	Comm^n model is many to many.
④	Advantages : - Lightweight & fast - Low overhead - support for multi - casting.	Advantages - simple management - Scalability - Robust comm^n.
⑤	Weakness : Not as reliable as TCP based MQTT	weakness : Higher overhead no multicasting support.

Page No.
Date

* 6LOWPAN :-

- In order to enable IPV6 over IEEE 802.15.4 networks the adaptation layer called 6LOWPAN was developed.
- Subsequently 6Lo made use of 6LOWPAN as a basis to support IPV6 over Bluetooth LE, ITU-T G.9959, DECT ULE, NFC.
- A key IP based technology is 6LOWPAN (IPV6 Low-power wireless personal Area Network). Rather than being an IOT application protocols technology like bluetooth or zigbee, 6LOWPAN is a network protocol that defines encapsulation & header compression mechanisms.
- 6LOWPAN provides a means of carrying packet data in the form of IPV6 over IEEE 802.15.4 & other networks.
- It provides end to end connectivity & direct connectivity.
- In order to send packet data IPV6 over 6LOWPAN it is necessary to have method of converting packet data into a format that can be handled by the IEEE 802.15.4 lower layer system.

Page No.:
Date :

IP Protocol Stack | | | | GLOWPAN Protocol stack

HTTP	RTP		Appln	Appln Protocol	
TCP	UDP	ICMP	Transport	UDP	ICMP
IP			Network	IPV6	
Ethernet MAC			Data Link	6LOWPAN	
Ethernet PHY			Physical	IEEE 802.15.4 MAC	
				IEEE 802.15.4 PHY	

fig. 6LOWPAN protocol stack compared to the IP Protocol stack.

- It is almost identical to a normal IPV6 implementation with two differences. 6LOWPAN only supports IPV6 for which a small adaption layer (6LOWPAN) has been defined to optimize IPV6 over link layers. 6LOWPAN is not bound to the IEEE 802.15.4 standard it is designed to utilize it.

* 6LOWLAN Header Stack

802.15.4 Header	IPV6 Header compression	IPV6 payload

802.15.4 Header	Fragment Header	IPV6 Header compression	IPV6 payload

802.15.4 Header	Mesh Addr Header	Fragment Header	IPV6 Header compression	IPV6 Payload

fig. 6LOWLAN Header Stack

Page No.:
Date :

* LoRa

- LoRa is a long Range, low data rate, low power wireless platform technology for building IoT network.
- LoRa is a patented digital wireless data comm^n IoT technology developed by Cycleo of Grenoble, France.
- LoRa transmits over license-free megahertz radio frequency bands like 169 MHz, 433 MHz (Europe) & 915 (MHz) (North America).
- LoRa enables very long range transmission (more than upto 10 miles in rural areas) with low power consumption.
- LoRa developed the LoRaWAN protocol for use by mobile n/w operators who want to use unlicensed spectrum to communicate with IoT devices in their network.
- LoRaWAN defines with the comm^n protocol & system architecture for the network while the LoRa physical layer enables the long-range comm^n link.
- LoRaWAN communication protocol ensure reliable comm^n & secure comm^n.

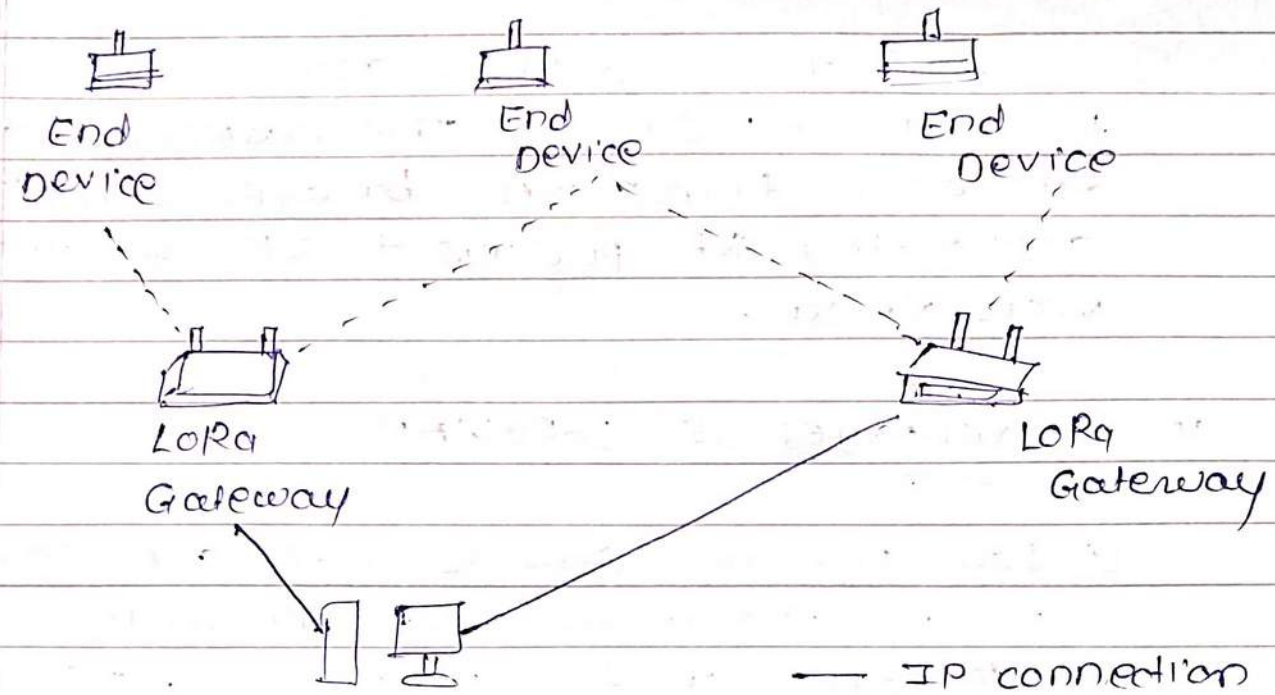

fig. LoRa Network

- LoRa network uses a star topology in which an end node can send message to multiple gateways that comm with the network server. Since an end node does not belong to a specific gateway more than one gateway can receive a message sent by an end device.

- LoRa radio access technology is used in communication between an end device & the gateways. The gateways & network server are connected via standard IP connections.

- LoRa sensors transmit data the LoRa gateways connect to the internet via standard IP protocol & transmit data received from the LoRa embedded sensors

- Gateway devices are always connected to a power source. The gateway comm acts as a transparent bridge, simply converting RF packets to IP packets & vice versa.

* Advantages of LoRaWAN

1. Low powered sensors that can cover a wide area measured in miles.
2. Operates in the industrial, scientific, & medical radio bands.
3. Low powered means long battery life devices. Sensor battery can last for two to five years (class A & class B)
4. Single LoRa gateway device is designed to take care of thousands of end devices or nodes.
5. perfect for monitoring field deployed assets
6. It is widely used for m2M/IoT appln.
7. LoRaWAN governed by an alliance,
8. fully bidirectional comm.

* Disadvantages of LoRaWan

1. Not for large data payloads
2. Has no support for audio or video.
3. Limited line of sight comm.
4. Not for continuous monitoring.