MPSSDEGB
कौशल से रोजगार, समृद्धि अपार

FITT
Foundation For Innovation And Technology Transfer

SANKALP
Ministry of Skill Development & Entrepreneurship

WEEK 2-DAY 2
IoT Communication Technologies

Agenda

- Overview of Network reference Models
- IoT Wireless Edge Networks: Constrained Devices and Networks
- Non-IP IoT Wireless Edge Networks: Zigbee, Bluetooth, etc

IoT Communication Technologies

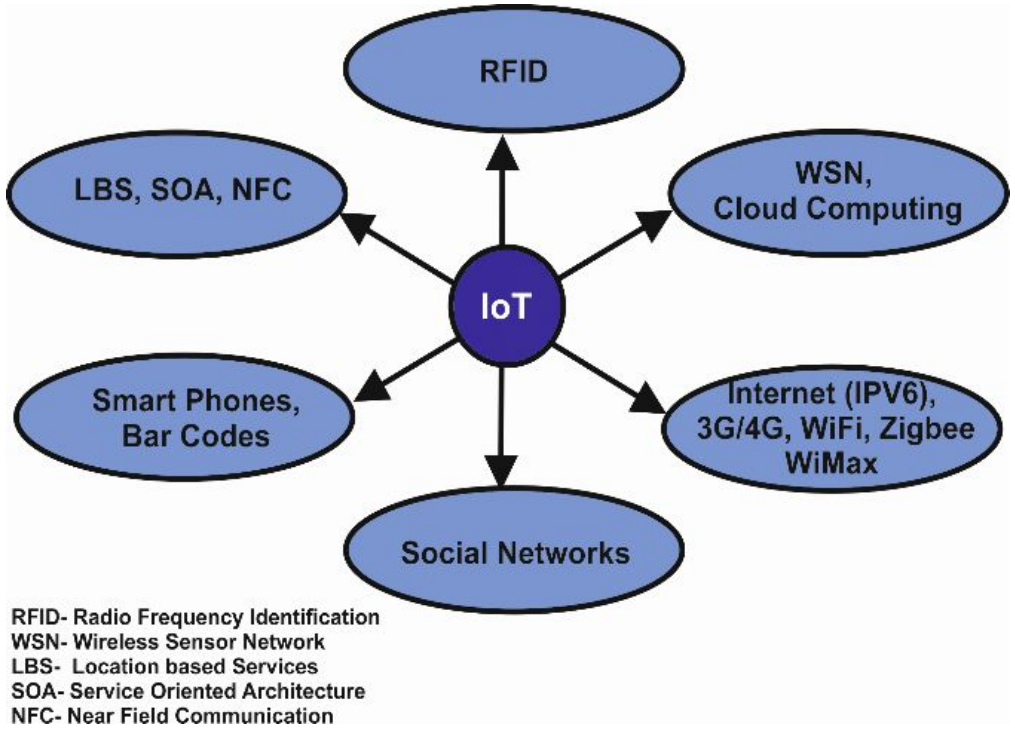
- Internet of Things (IoT) communication technologies play a crucial role in enabling devices to connect, communicate, and share data within the IoT ecosystem.
- The choice of communication technology depends on various factors such as range, power consumption, data rate, and the specific requirements of the IoT application.

IoT Communication Technologies

How will an IoT-enabled device communicate what it knows to the Internet?

- Suitable connectivity solutions range from a multitude of wired connectivity technologies such as Ethernet to wireless technologies like Wi-Fi and even 5G cellular.
- Many solutions need a combination of multiple communication technologies.
- For example, a smart car system playing video or using GPS navigation might need 4G LTE in order to communicate with the outside world and Wi-Fi and Bluetooth to communicate with devices like phones and rear seat entertainment (RSE) used by the passengers.

IoT Communication Technologies-Types



Wireless Communication Technologies

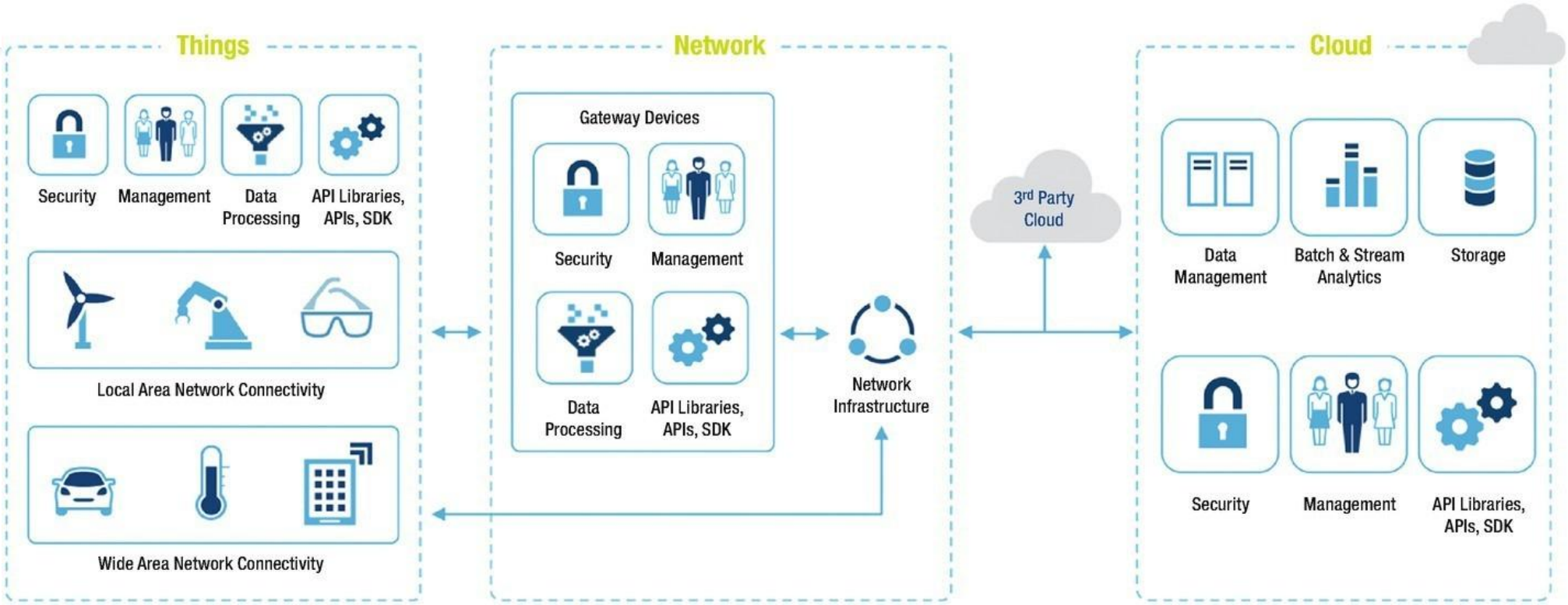
Wired Communication technologies

Source:Singh, Omveer & Iqbal, Arif. (2017). Modified Internet of Things Architecture Layer for High Power Application.

Connectivity Considerations

- Connectivity between IoT devices and outside world dictates network architecture
- Choice of communication technology dictates IoT device hardware requirement and costs
- Due to presence of numerous applications of IoT enabled devices, a single networking paradigm not sufficient to all needs of the consumer or IoT device
- Complexity of networks- interference among devices, network management, heterogeneity in networks, protocol standardization within networks

Network Configuration in IoT



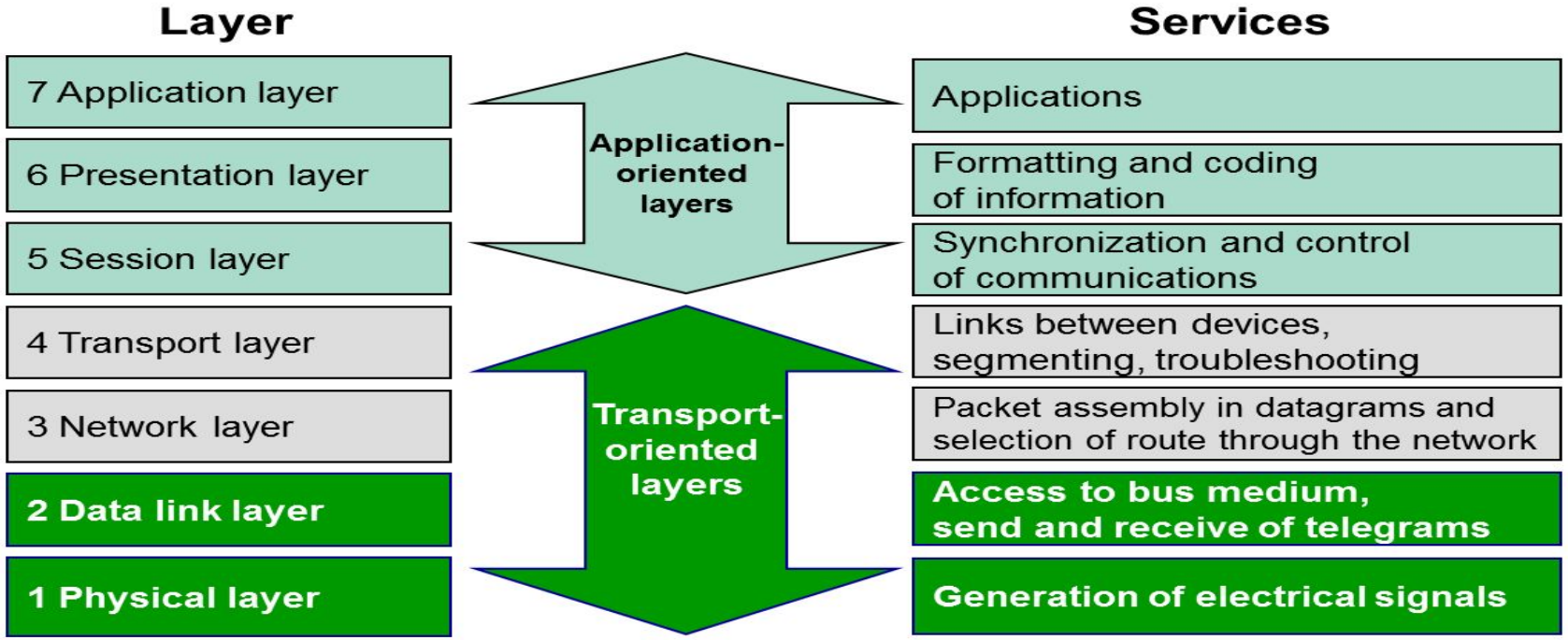
Source:Cheruvu S., Kumar A., Smith N., Wheeler D.M. (2020) Connectivity Technologies for IoT. In: Demystifying Internet of Things Security. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842- 2896-8_5

NETWORK REFERENCE MODEL

Overview of Network Reference Model

- Reference Model offers a means of standardization which is acceptable worldwide.
- In order to provide communication among heterogeneous devices, we need a standardized model i.e. a reference model, which would provide us way how these devices can communicate regardless their architecture.
- We have two reference models such as OSI model and TCP/IP reference model, however, the OSI model is a hypothetical one but the TCP/IP is absolutely practical model.

OSI Model--OSI is acronym of Open System Interface. This model is developed by the International organization of Standardization (ISO) and therefore also referred as ISO-OSI Model.

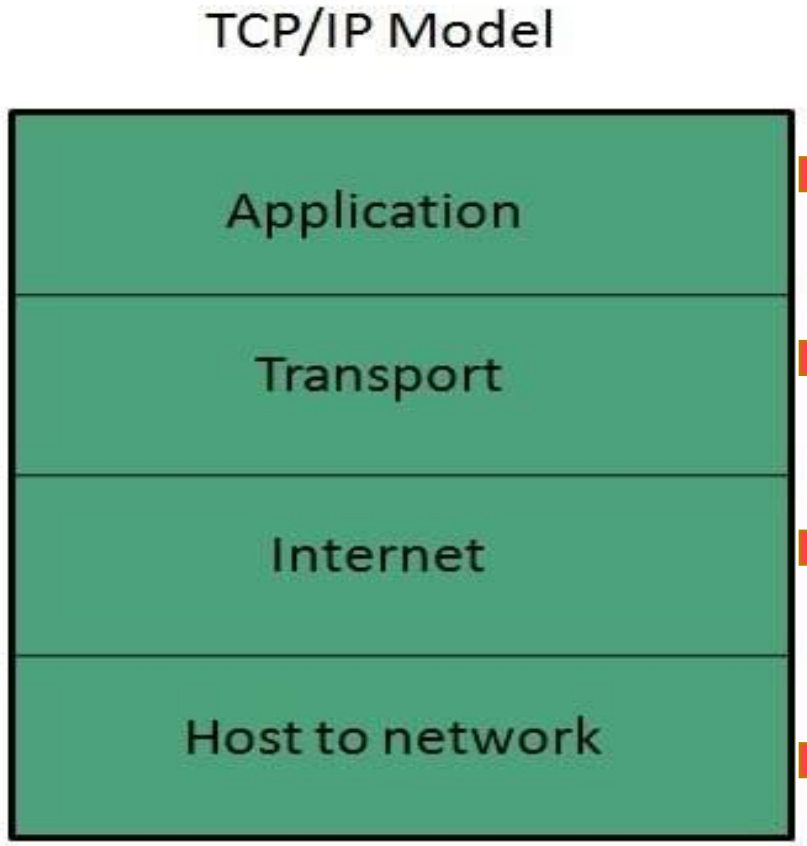


Source:https://profinetuniversity.com/industrial-automation-ethernet/network-reference-model/

TCP/IP Model

- TCP/IP model is practical model and is used in the Internet.
- TCP/IP is acronym of Transmission Control Protocol and Internet Protocol.
- The TCP/IP model combines the two layers (Physical and Data link layer) into one layer i.e. Host-to-Network layer.

TCP/IP Model



It provides different services such as manipulation of information in several ways, retransferring the files of information, distributing the results etc.

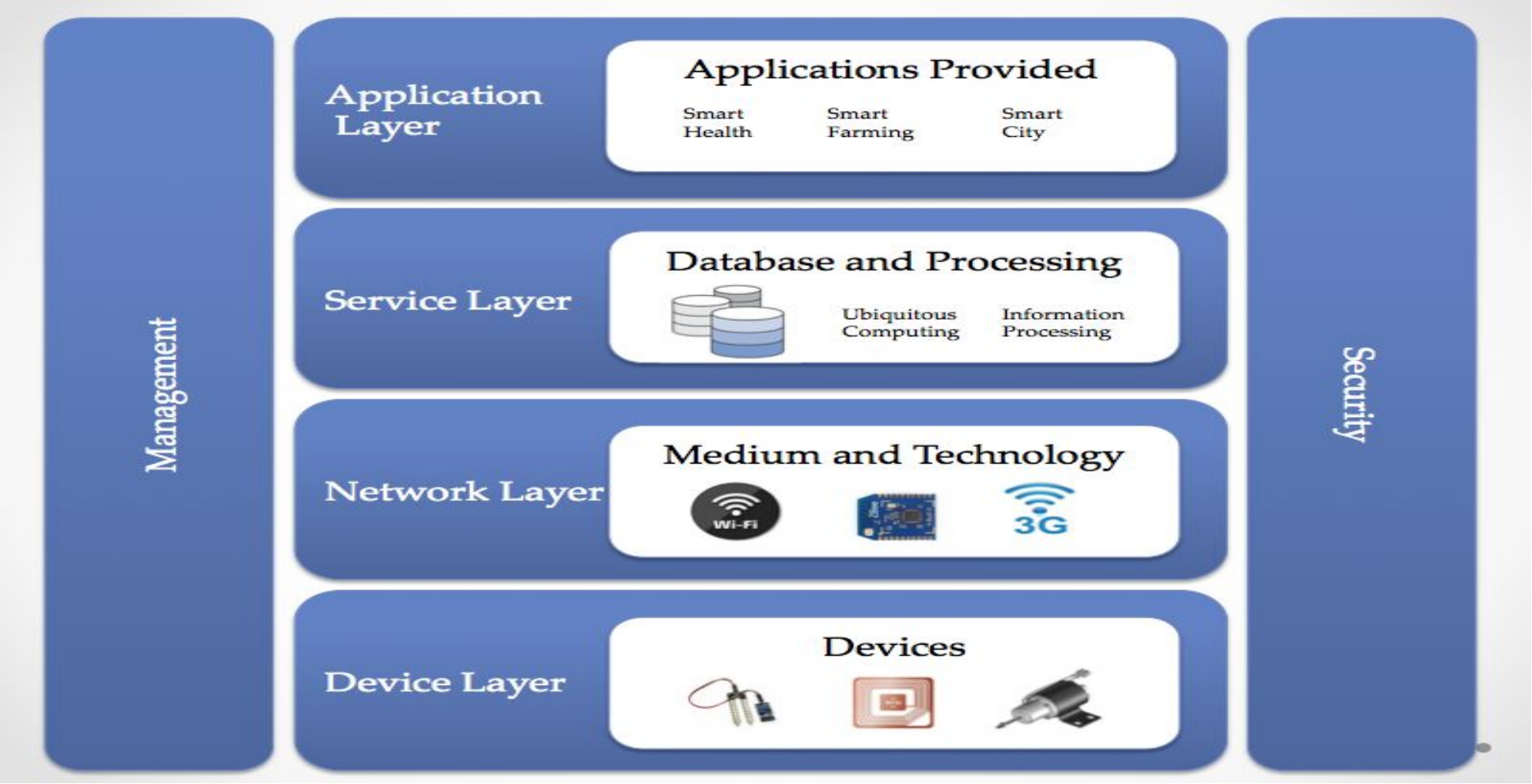
It does the same functions as that of transport layer in OSI model.

The function of this layer is to allow the host to insert packets into network and then make them travel independently to the destination. However, the order of receiving the packet can be different from the sequence they were sent.

This is the lowest layer in TCP/IP model. The host has to connect to network using some protocol, so that it can send IP packets over it. This protocol varies from host to host and network to network.

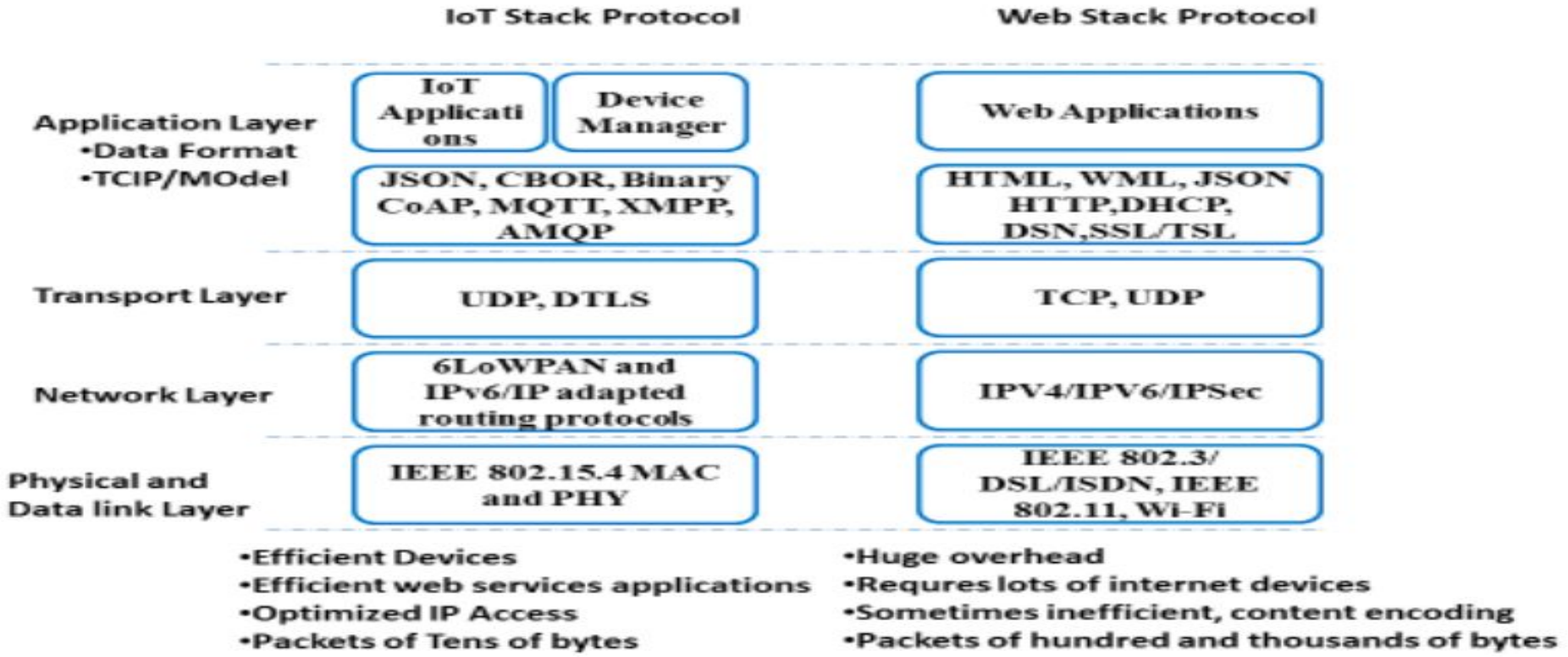
Source:-

IoT Architecture Model



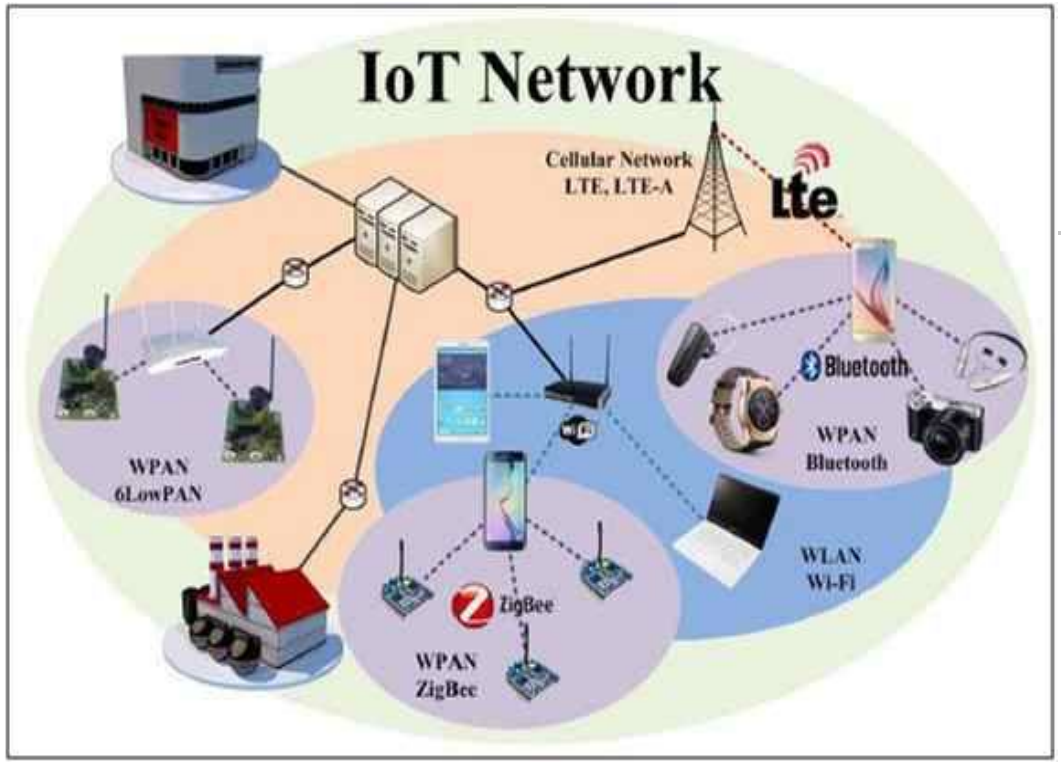
Source:https://www.mdpi.com/2624-6511/4/2/24

IoT Stack Vs Web Stack



Source:Amine, Rghioui & Sendra, Sandra & Lloret, Jaime & Oumnad, Abedlmajid. (2016). Internet of Things for Measuring Human Activities in Ambient Assisted Living and e-Health. Network Protocols and Algorithms. 8. 15. 10.5296/npa.v8i3.10146.

IoT Wireless Edge Networks



Source:
https://www.c-sharpcorner.com/UploadFile/f88748/internet-of-thingsiot-part-4-network-protocols-and-arc/

Definition:

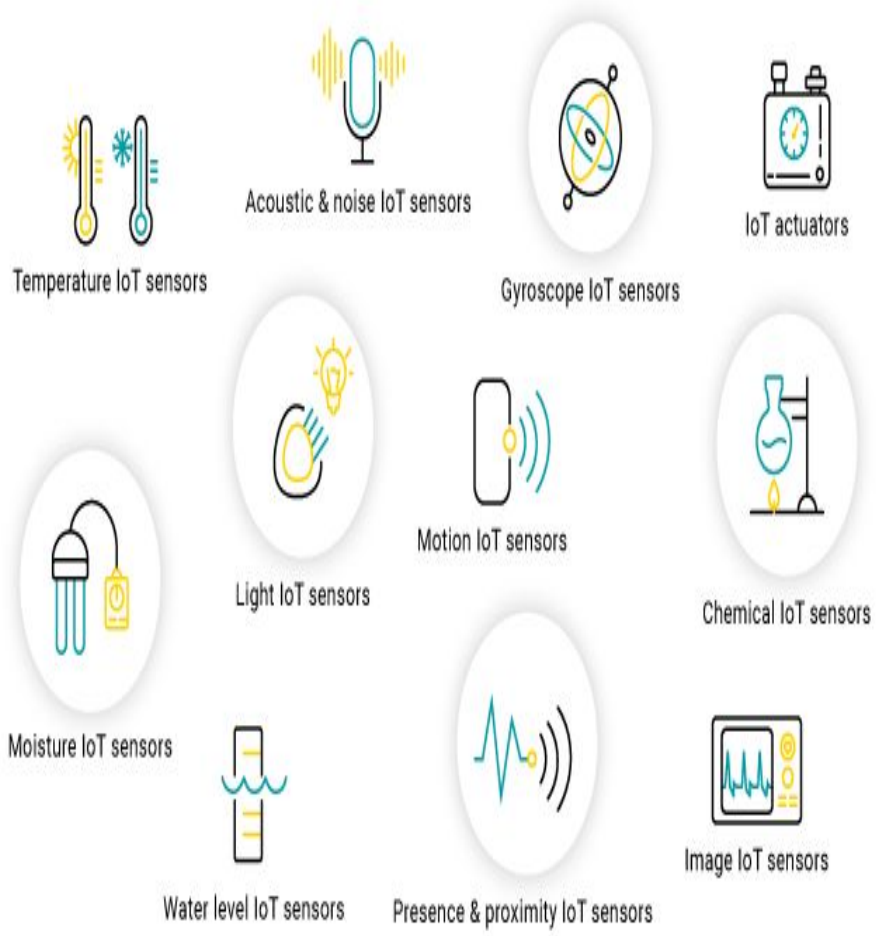
IoT Wireless Edge Networks enable decentralized communication and processing for IoT devices, utilizing wireless connectivity like LPWAN and 5G.

- Proximity to devices reduces latency, allowing real-time data analysis and efficient bandwidth usage.
- This architecture fosters scalable, responsive ecosystems, revolutionizing how IoT applications operate.

How the IoT Benefits from Edge Computing

- Edge computing benefits IoT by moving computing processes closer to the device, reducing network traffic and latency to enable real-time insights.

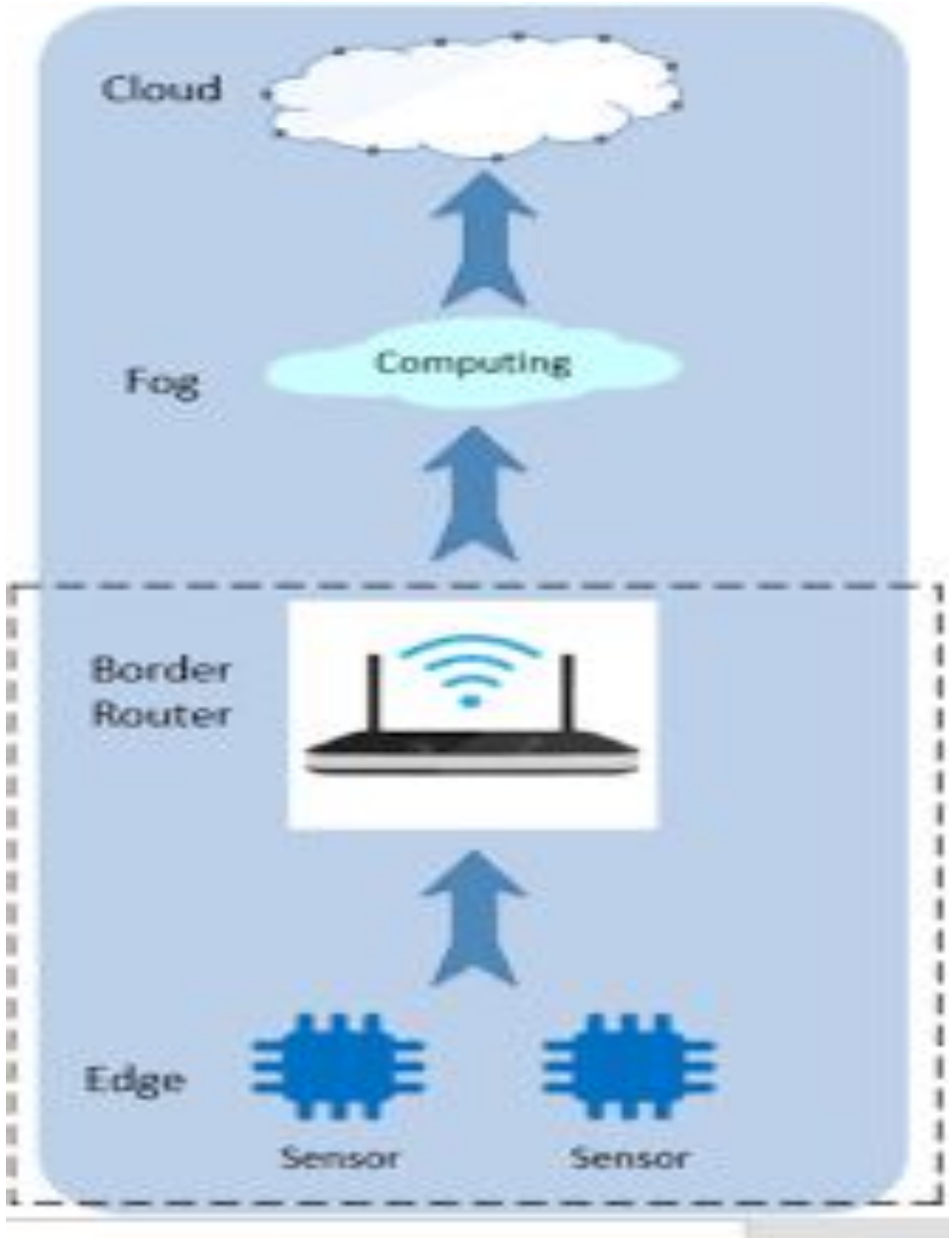
- IoT devices often send small data packets back to a central management platform for analysis.



Constrained Devices

To attempt a broad definition of the term, it can be stated that resource-constrained devices are those that by design have limited processing and storage capabilities to provide a maximal data output possible with a minimal power input while remaining cost-effective.

Source:https://www.avsystem.com/blog/iot/what-is-resource-constrained-device/



Characteristics of Constrained Devices

- Low Power Consumption
- Limited Processing Capabilities
- Restricted Memory and Storage
- Communication Constraints

Source:https://www.hcltech.com/blogs/introduction-iot-constrained-node-networks

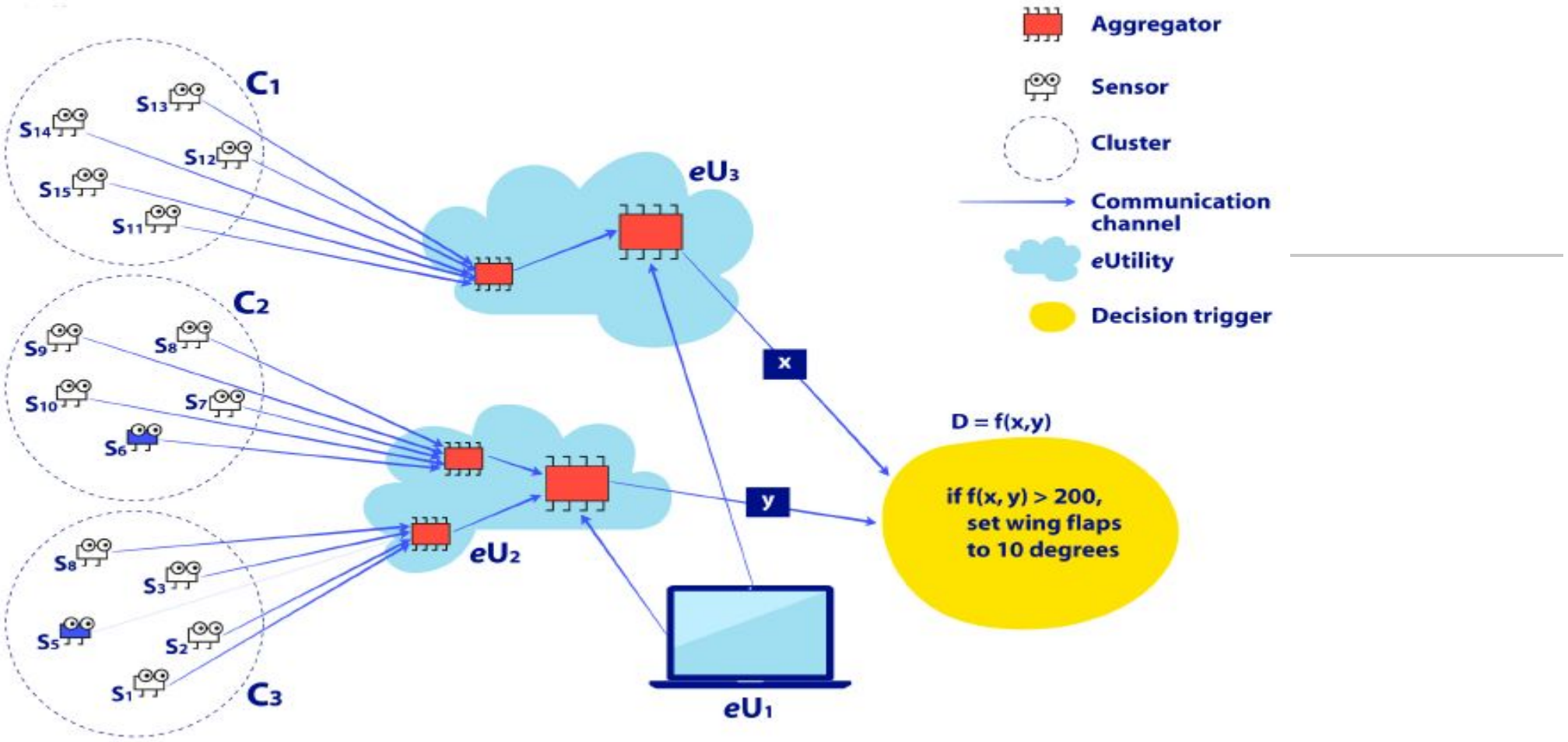
What is a Constrained Network?

A constrained network is composed of a significant portion of constrained nodes. Mostly, these constrained node networks are deployed in the edge network of an IoT system.

A constrained network exhibits below characteristics:

- Low bit-rate/throughput
- High packet loss and high variability of packet loss
- Highly asymmetric link characteristics
- Lack of advanced network services like multi-cast

Building blocks of Constrained Node Network



Source:https://www.hcltech.com/blogs/introduction-iot-constrained-node-networks

Functionality Based IoT Protocol To be Discussed

Connectivity – 6LowPAN

Identification - IPv6, URI

Communication / Transport - Wifi, Bluetooth, LPWAN

Data Protocols - MQTT, CoAP, AMQP, Web-socket

Discovery - Physical Web

Semantic – WebThing Model

1

Overview of LoWPAN

- A simple low throughput wireless network comprising typically low cost and low power devices
- Devices in the network typically work together to connect the physical environment to real world applications, e.g., wireless sensors networks
- Common topologies include – star, mesh, and combinations of star and mesh
- The Phy and MAC layers ***conform*** to IEEE 802.15.4-2003 standard

LoWPAN architecture

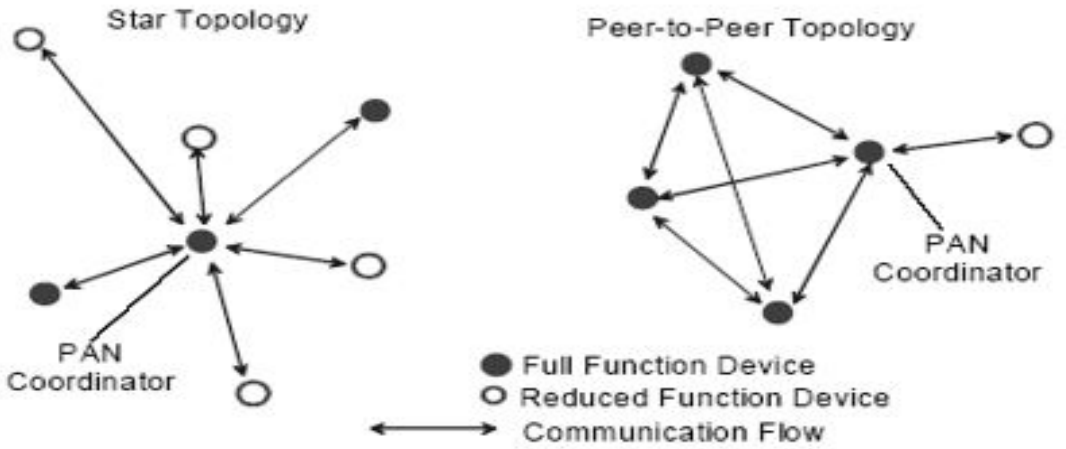


Figure 1—Star and peer-to-peer topology examples

Octets: 2	1	0/2	0/2/8	0/2	0/2/8	variable	2
Frame control	Sequence number	Destination PAN identifier	Destination address	Source PAN identifier	Source address	Frame payload	FCS
		Addressing fields					
MHR						MAC payload	MFR

Figure 34—General MAC frame format

6LoWPAN characteristics

- Small packet size
- 16-bit short or IEEE 64-bit extended media access control addresses
- Low bandwidth. (250/40/20 kbps)
- Topologies include star and mesh
- Low power, typically battery operated
- Relatively low cost
- Networks are ad hoc & devices have limited accessibility and user interfaces
- Inherently unreliable due to nature of devices in the wireless medium

Typical applications

- Equipment health monitoring
- Environment monitoring
- Security
- Home
- Building automation

Non-IP IoT Wireless Edge Networks: Zigbee, Bluetooth, etc

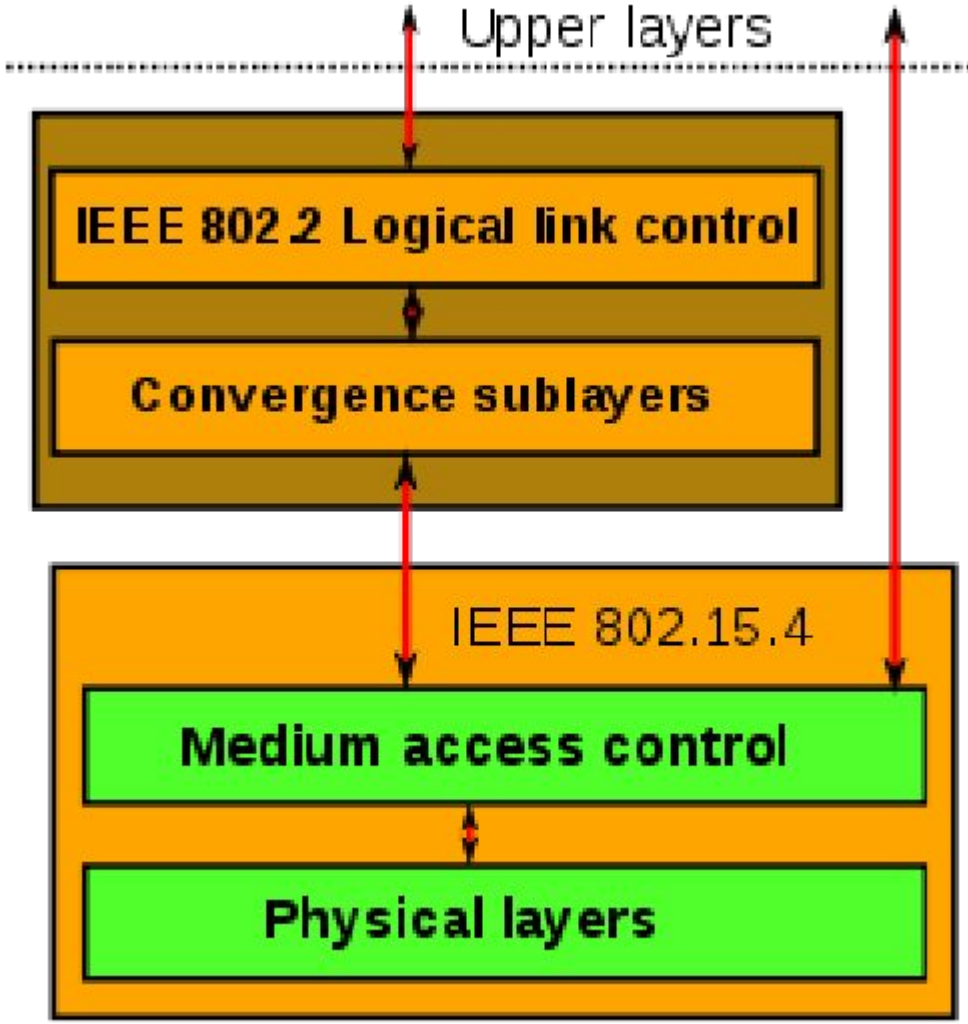
Non-IP IoT Wireless Edge Networks

Definition

Non-IP IoT Wireless Edge Networks refer to specialized communication infrastructures designed for connecting Internet of Things (IoT) devices without using the traditional Internet Protocol (IP).

Importance in IoT Connectivity:

These networks play a crucial role in facilitating efficient and optimized communication among IoT devices. Unlike traditional IP-based networks, non-IP solutions are tailored for the unique requirements of IoT applications, ensuring better performance.



IEEE 802.15.4

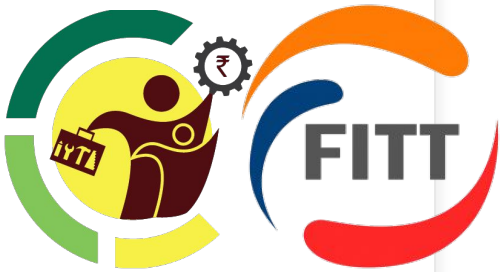
- IEEE 802.15.4 specifies Physical and Media Access Control for low rate wireless personal area network (LR-WPANs)
- It is maintained by IEEE 802.15 working group
- It is the basis for Zigbee, WirelessHART protocols which extend the standard by developing upper layers not defined in IEEE 802.15.4

Source:https://en.wikipedia.org/wiki/IEEE_802.15.4

Key Technologies

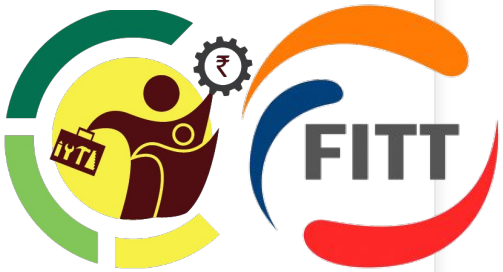
1. Zigbee
2. Bluetooth
3. Z-Wave
4. LoRa (Long Range)
5. RFID (Radio-Frequency Identification)

802.15.4 and the ZigBee™ Alliance



- **IEEE 802.15.4**
  - Composed of many of the individuals and companies that make up the ZigBee Alliance
  - Developed the basic PHY and MAC standard with the requirement that 15.4 be simple and manageable and that high-level functionality (networking, security key management, applications) be considered
- The ZigBee Alliance is
  - A consortium of end users and solution providers, primarily responsible for the development of the 802.15.4 standard
  - Developing applications and network capability utilizing the 802.15.4 packet delivery mechanism
  - Addresses application and interoperability needs of a substantial part of the market

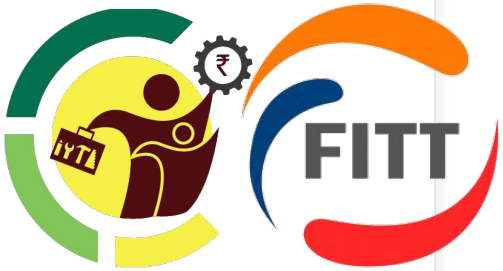
Mission Statement



- ZigBee Alliance members are defining global standards for reliable, cost-effective, low power wireless applications.

- The ZigBee Alliance is a rapidly growing, non-profit industry consortium of leading semiconductor manufacturers, technology providers, OEMs and end users worldwide.

What is the ZigBee Alliance?



- Organization defining global standards for reliable, cost-effective, low power wireless applications
- A rapidly growing, worldwide, non-profit industry consortium of
  - Leading semiconductor manufacturers
  - Technology providers
  - OEMs
  - End-users
- Sensors are one of the reasons for ZigBee!

What is ZigBee technology?

- Cost-effective, standards-based wireless networking solution
- Developed for and targets applications that need
  - Low to moderate data rates and low duty cycles
  - Low average power consumption / long battery life
  - Security and reliability
  - Flexible and dynamic network topologies
    - Star, cluster tree and mesh networks
  - Interoperable application frameworks controlled by an industry alliance to ensure interoperability/compatibility

Why do we need ZigBee technology?

- ONLY standards-based technology that
  - Addresses the unique needs of most remote monitoring and control and sensory network applications
  - Enables the broad-based deployment of wireless networks with low cost, low power solutions
  - Provides the ability to run for years on inexpensive primary batteries for a typical monitoring application

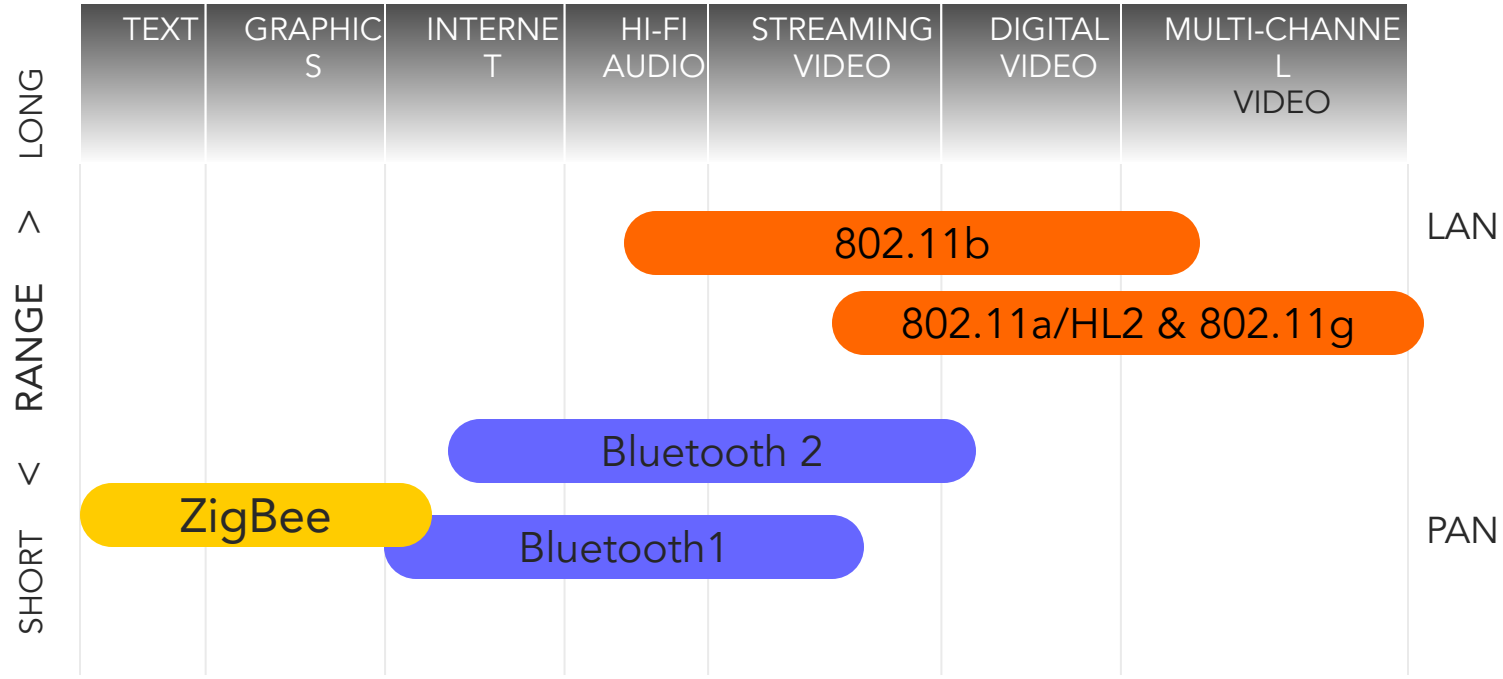
What kind of battery life can a user expect?

- ZigBee protocol was designed from the ground up to support
  - very long life battery applications
- Users can expect
  - Near-shelf life in a typical monitoring application
- Battery life is ultimately a function of
  - battery capacity and application usage
- Many industrial applications are in harsh thermal environments
  - Batteries may include alkalines or Li-primaries
  - Other forms of power generation might include solar, mechanical, piezoelectric

The ZigBee Alliance Solution

- Targeted at home and building automation and controls, consumer electronics, toys etc.
- Industry standard (IEEE 802.15.4 radios)
- Primary drivers are simplicity, long battery life, networking capabilities, reliability, and cost

The Wireless Market



Applications

Source: Singh, Karamjeet. (2012). ZigBee: A Review. IJCST. 3. 328-331.

MPSSDEGB
कौशल से रोजगार, समृद्धि अपार

FITT
Foundation For Innovation And Technology Transfer

SANKALP
Ministry of Skill Development & Entrepreneurship

Promoters

Honeywell

MITSUBISHI ELECTRIC

PHILIPS
Let's make things better.

invensys

SAMSUNG

MOTOROLA
intelligence everywhere

Participants

ABB

ADCON TELEMETRY

ANALOG DEVICES

ARDESTA
Leading the Small Tech Revolution.

ATMEL

BOSCH

Cambridge Consultants

Chipcon

CompXs

Danfoss

EATON

ember

ETS

figure 8 wireless

LEVITON

france telecom

Helicomm

inovonics WIRELESS CORPORATION

INTEGRATION ASSOCIATES

hp invent

intel

Micro Linear

NTS

OKI

OMRON

XEMICS

THE POWER OF INNOVATION

RF MICRO·DEVICES

Millennial Net
Wireless Data Links

ZMD

BlueChip communications

XANBOO

zensys

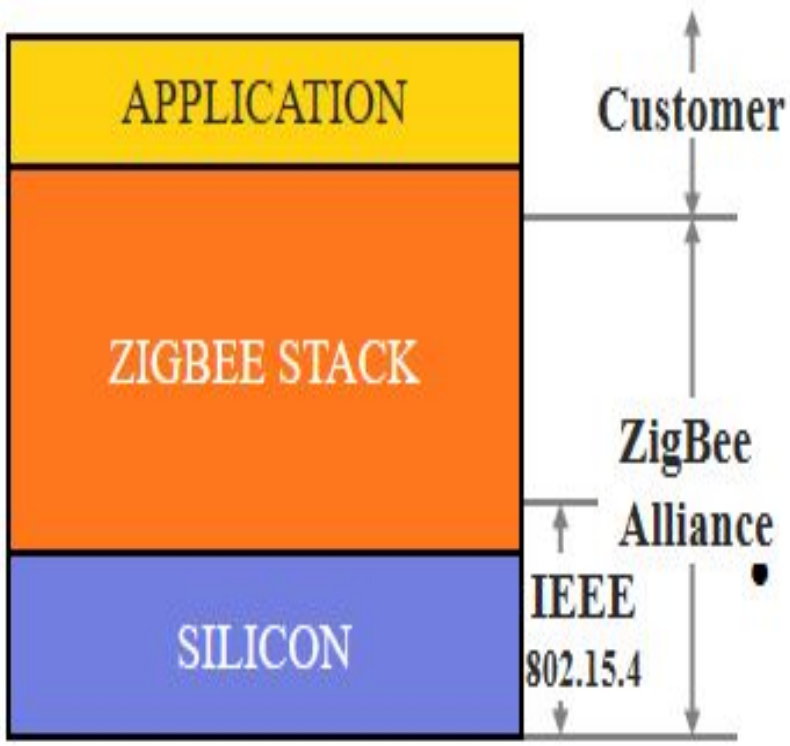
duolog

eaZix

And more each month…

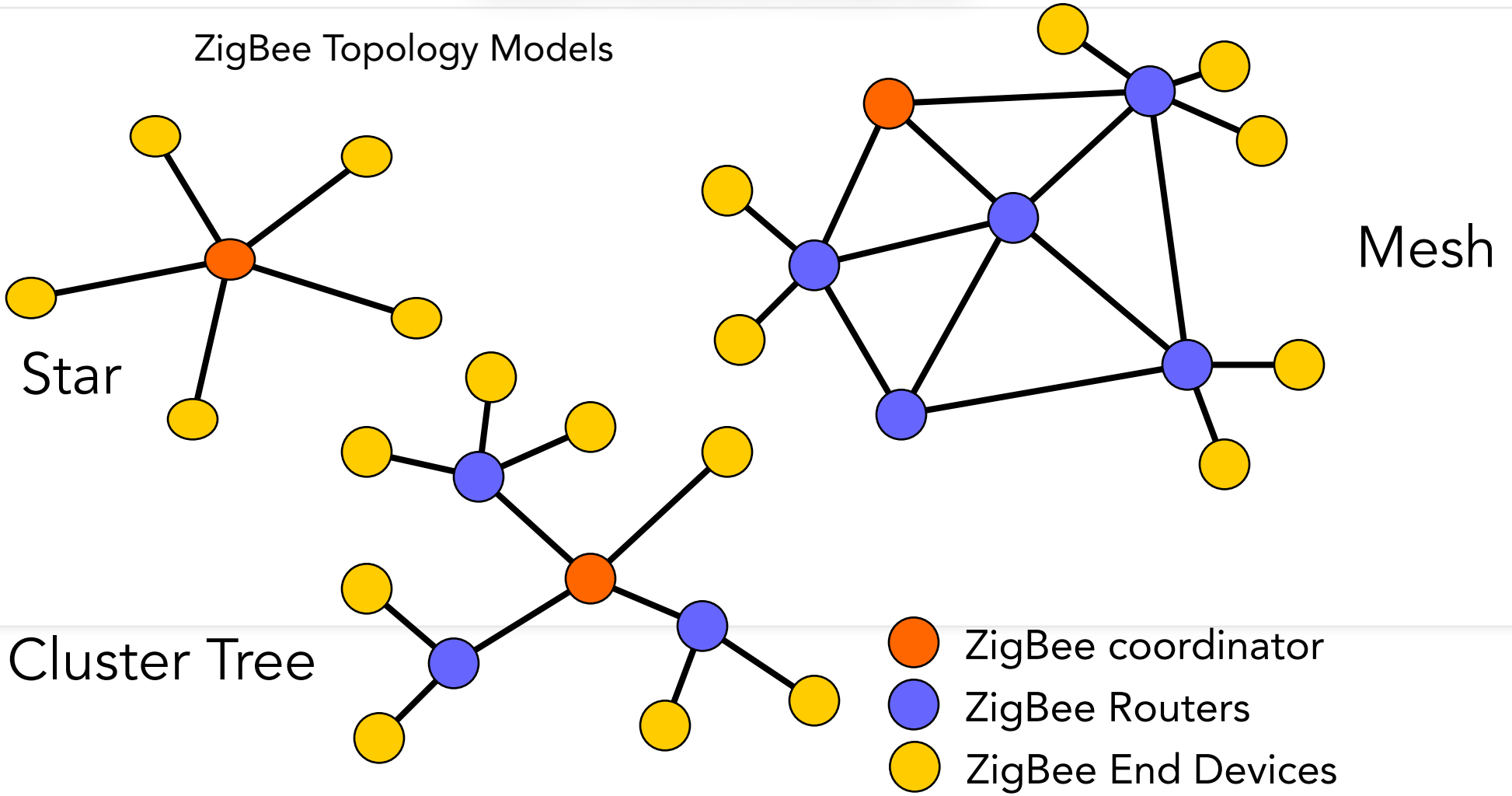
ZigBee Alliance

Development of the Standard



- **ZigBee Alliance**
  - **50+ companies**
  - **Defining upper layers of protocol stack: from network to application, including application profiles**
- **IEEE 802.15.4 Working Group**
  - **Defining lower layers : MAC and PHY**

ZigBee Topology Models

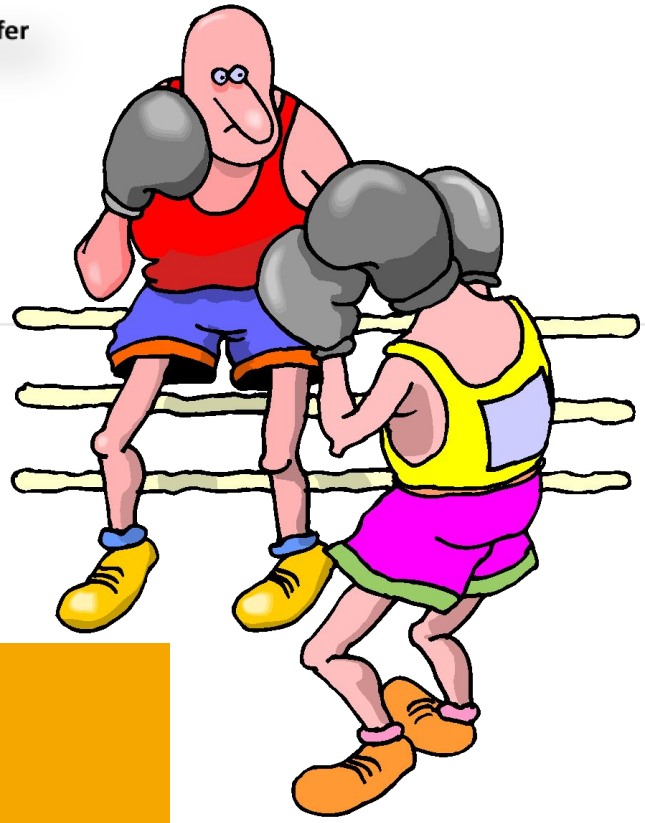


MPSSDEGB
कौशल से रोजगार, समृद्धि अपार

FITT
Foundation For Innovation And Technology Transfer

SANKALP
Ministry of Skill Development & Entrepreneurship

ZigBee and Bluetooth



Competitive or Complementary?

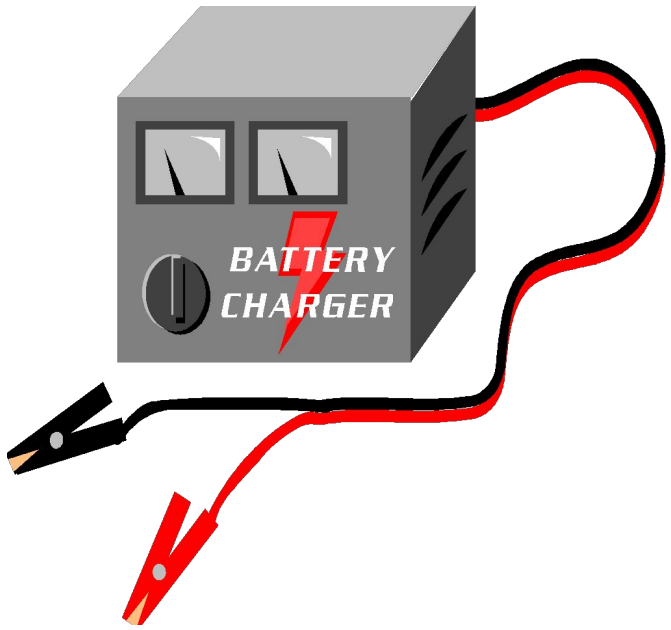
ZigBee and Bluetooth

Optimized for different applications

- ZigBee
  - Smaller packets over large network
  - Mostly Static networks with many, infrequently used devices
  - Home automation, toys remote controls
  - Energy saver!!!
- Bluetooth
  - Larger packets over small network
  - Ad-hoc networks
  - File transfer; streaming
  - Screen graphics, pictures, hands-free audio, Mobile phones, headsets, PDAs, etc.

ZigBee and Bluetooth

Address Different Needs

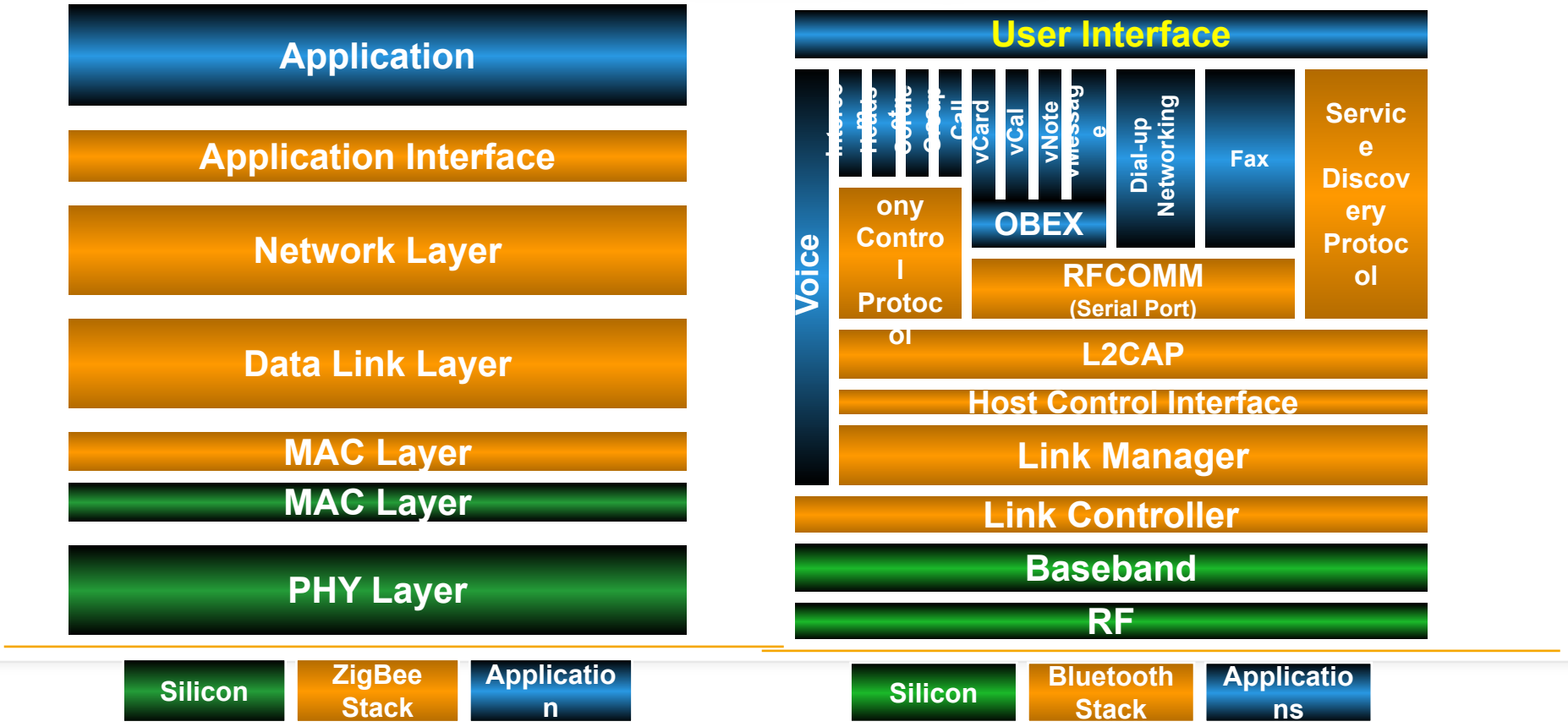


- Bluetooth is a cable replacement for items like Phones, Laptop Computers, Headsets
- Bluetooth expects regular charging
  - Target is to use <10% of host power

ZigBee and Bluetooth

Address Different Needs

- ZigBee is better for device where the battery is 'rare' replaced
  - Targets are :
    - Tiny fraction of host power
    - New opportunities where wireless not yet used



Zigbee

Bluetooth

Timing Considerations

ZigBee:

- Network join time = 30ms typically
- Sleeping slave changing to active = 15ms typically
- Active slave channel access time = 15ms typically

Bluetooth:

- Network join time = >3s
- Sleeping slave changing to active = 3s typically
- Active slave channel access time = 2ms typically

ZigBee protocol is optimized for timing critical applications

Comparison Overview

	Bluetooth	ZigBee
AIR INTERFACE	FHSS	DSSS
PROTOCOL STACK	250 kb	28 kb
BATTERY	rechargeable	non-rechargeable
DEVICES/NETWORK	8	255
LINK RATE	1 Mbps	250 kbps
RANGE	~10 meters (w/o pa)	~30 meters

Z-Wave

Z-Wave is a low-power RF communications IoT technology that primarily design for home automation for products such as lamp controllers and sensors among many other devices.

A Z-Wave uses a simpler protocol than some others, which can enable faster and simpler development, but the only maker of chips is Sigma Designs compared to multiple sources for other wireless technologies such as ZigBee and others.

Source:https://data-flair.training/blogs/iot-technology/

BLE

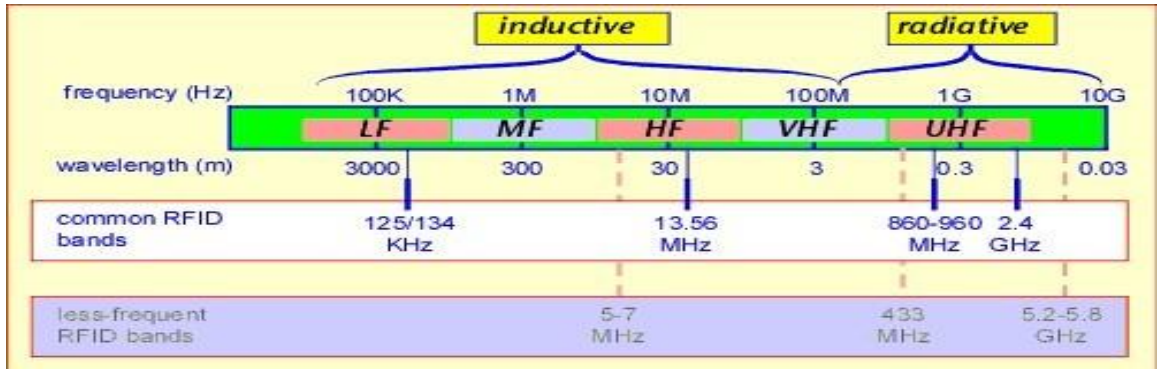
BLE is a wireless communication technology that is an extension of Bluetooth technology. BLE is commonly used for wearable devices, IoT applications, and proximity sensing. BLE operates at a frequency of 2.4 GHz and has a range of up to 100 meters.

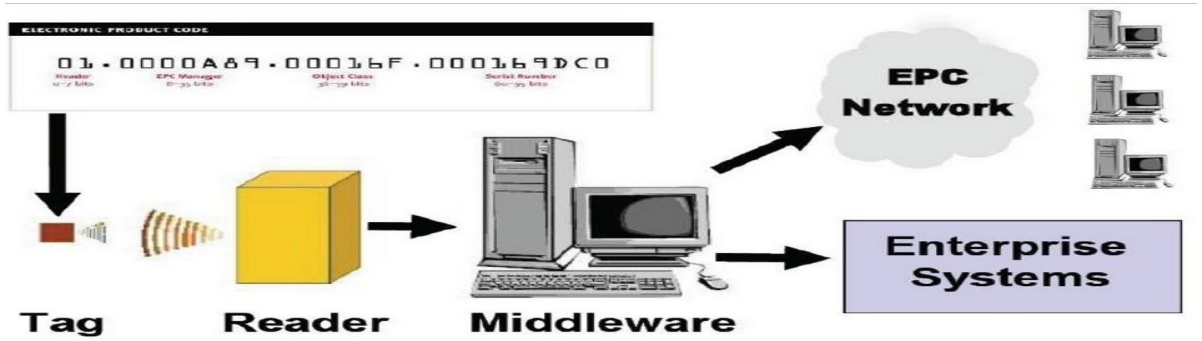
Its main advantage is its long-range communication capability. BLE can transmit data over a distance of up to 100 meters, which makes it suitable for applications that require long-range communication. Additionally, BLE has a higher data transfer rate compared to NFC and RFID technology, which means that it can be used for applications that require the transfer of large amounts of data.

However, it is also not perfect. BLE technology also has some limitations. One of the main limitations of BLE technology is its higher power consumption compared to NFC and RFID technology. This higher power consumption means that BLE devices may require frequent battery replacement, which can be expensive in the long run.

RFID: Radio Frequency Identification

- Appeared first in 1945
- Features:
  - Identify objects, record metadata or control individual target
  - More complex devices (e.g., readers, interrogators, beacons) usually connected to a host computer or network
  - Radio frequencies from 100 kHz to 10 GHz
- Operations:
  - Reading Device called Reader (connected to banckend network and communicates with tags using RF)
  - One or more tags (embedded antenna connected to chip based and attached to object)



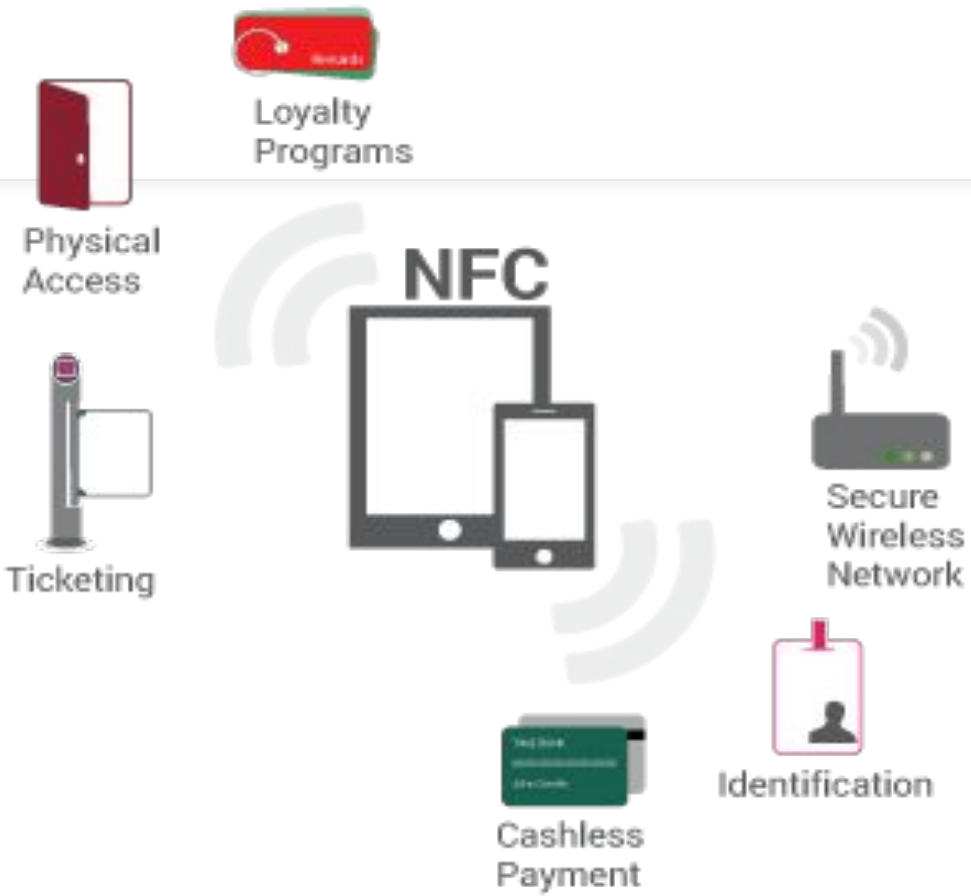


Source:https://ieeexplore.ieee.org/document/6201508

NFC

NFC is a wireless communication technology that is an extension of RFID technology. NFC allows for two-way communication between devices and is commonly used for mobile payments, ticketing, and access control. NFC uses a frequency of 13.56 MHz and operates within a range of a few centimeters.

NFC



NFC (Near Field Communication) is an IoT technology. It enables simple and safe communications between electronic devices, and specifically for smartphones, allowing consumers to perform transactions in which one does not have to be physically present.

Source:https://iotdunia.com/what-is-nfc-technology-how-does-it-works/#:~:text=Near%20Field%20Communication%20%28NFC%29%20is%20known%20as%20the,the%20data%20transfer%20facility%20easier%20than%20other%20methods.

Protocol / Feature	*Wi-Fi* IEEE 801.11.n	*ZigBee* IEEE 802.15.4	*Z-Wave* ISO/IEC 14543-3	*Bluetooth* IEEE 802.15.1	BLE IEEE 802.15.1	6LoWPAN IETF RFC-6282
Operating Frequency	120 kHz, 2.4-5 GHz	868/915 MHz, 2.4 GHz	868/915 MHz	2.402-2.482 GHz	2.402-2.482 GHz	868/921 MHz, 2.4-5 GHz
Maximum Data Rare	11-54 Mbps	20/40 kbps; 250 kbps	9.6-40 kbps	0.7-2.1 Mbps	0.27 Mbps	10-40 kbps, 250kbps
Nominal Range	10-100 m	10-1000 m	30-50 m	15-20 m	10-15 m	10-100 m
Modulation Type	BPSK, QPSK, OFDM, M-QAM	D-BPSK, O-QPSK, QPSK	FSK, GFSK, Narrowband	GFSK, CPFSK, 8-DPSK	GFSK	BPSK, O-QPSK, ASK
Network Topology	Star, Tree, P2P	Star, Mesh, Cluster Tree	Mesh	Star	Star	Star, Mesh, P2P
Network Size	32	65536	232	8	N/A	~100
Encryption	RC4 Stream & AES Block Cipher	128-bit AES	128-bit AES	AES Block Cipher	128-bit AES	128-bit AES
Coding	MC-DSSS, CCK, OFDM	DSSS(1→15) DSSS(4→32)	Manchester; NRZ	FHSS	Adaptive CCK	Header Compression, DSSS
Channel Bandwidth	20-25 MHz	0.3/0.6 MHz; 2-5 MHz	Fixed	1 MHz	8 MHz	2-5 MHz

Source:Pothuganti, Karunakar & Chitneni, Anusha. (2014). A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. 4. 655-662.

WiFi

- Wireless Alternative to Wired Technologies
- Standardized as IEEE 802.11 standard for WLANs

Standard	Frequency bands	Throughput	Range
WiFi a (802.11a)	5 GHz	54 Mbit/s	10 m
WiFi B (802.11b)	2.4 GHz	11 Mbit/s	140 m
WiFi G (802.11g)	2.4 GHz	54 Mbit/s	140 m
WiFi N (802.11n)	2.4 GHz / 5 GHz	450 Mbit/s	250 m
IEEE 802.11ah	900 MHz	8 Mbit/s	100 M

SUMMARY

- ✔ Discussed the importance of standardized models for IoT communication, including the OSI and TCP/IP reference models.
- ✔ Emphasized their role in providing a framework for seamless device communication.

- ✔ Explored the significance of IoT networks designed for constrained devices.
- ✔ Addressed challenges like limited resources and the need for optimization.

- ✔ Delved into non-IP wireless technologies such as Zigbee and Bluetooth.
- ✔ Highlighted their characteristics, applications, and importance in diverse IoT ecosystems.

Home Assignment

Imagine you are responsible for setting up a smart home system. Design a basic network plan considering the following aspects:

1.Explain whether you would choose the OSI or TCP/IP reference model for your smart home network.

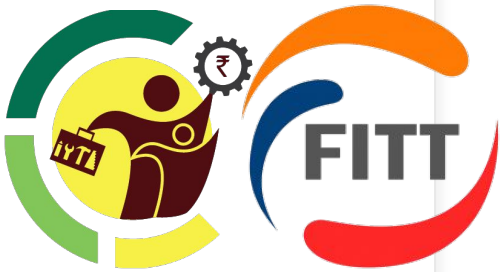
Provide a brief reason for your choice.

2.Identify two types of constrained devices you would include in your smart home (e.g., temperature sensor, smart light).Briefly discuss the challenges these devices might face in terms of communication and resource limitations.

3.Choose one wireless technology (e.g., Zigbee or Bluetooth) for connecting the constrained devices.

Explain why you chose this technology, considering its characteristics and suitability for a smart home environment.

Python Exercise



[Google Colab link]

In this part we discuss dictionaries in python.

Thank you