**IOT Communication Technologies**

**Introduction**

IoT technology encompasses all the enabling hardware IP, tools, systems, sensors, and software that support IoT device and application development. With IoT technology, everyday objects can be made smart—from medical devices to smartphones, watches to security cameras, and cars to factory production lines. IoT technologies also include security tools to prevent internet-based attacks on networked devices and their applications.

**IOT Access Technologies:**

IoT primarily exploits standard protocols and networking technologies. However, the major enabling technologies and protocols of IoT are RFID, NFC, low-energy Bluetooth, low-energy wireless, low-energy radio protocols, LTE-A, and WiFi-Direct. These technologies support the specific networking functionality needed in an IoT system in contrast to a standard uniform network of common systems.

**OSI Model**

Open system interconnection is a framework for defining the connections and task required for network systems to communicate with one another. The main purpose to assist the vendors and communication software developers to produce inter operable network systems. It is the replacement of all the other communication models. OSI model is based on the structuring technique called layering. Layering means, communication functions are partitioned into a vertical set of layers. Each layer performs a related set of functions and enriching the services immediately

provided by the lower layer. OSI model main purpose of development is to group similar functions into one layer.

There are 7 layers

* Physical layer
* Data link layer
* Network layer
* Transport layer
* Session layer
* Presentation layer
* Application layer

**1. Physical Layer**

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together

**Functions**

* **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
* **Bit rate control**: The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
* **Physical topologies**: Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.
* **Transmission mode**: Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full-duplex

Simplex- Sender can send the data but the sender can’t receive the data. It is a unidirectional communication. keyboard and monitor

In half-duplex mode, Sender can send the data and also can receive the data one at a time. It is two-way directional communication but one at a time. walkie-talkie-type push-to-talk radio connection

In full-duplex mode, Sender can send the data and also can receive the data simultaneously. It is two-way directional communication simultaneously. wireless microphones, and surveillance cameras

**2. Data Link Layer**

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. \*\*Bits in Data Link layer is referred to as Frame.  \*\* Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.  \*\*\* Switch & Bridge are Data Link Layer devices.

Data Link Layer is divided into two sublayers:

MAC (Media Access Control) address, sometimes referred to as a hardware or physical address, is a unique, 12-character alphanumeric attribute that is used to identify individual electronic devices on a network. An example of a MAC address is: 00-B0-D0-63-C2-26.)

LLC (Logical Link Control) helps for synchronization, flow chart & Error checking

**Functions**

**Framing**: Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.

**Physical addressing**: After creating frames, the Data link layer adds physical addresses (MAC address) of the sender and/or receiver in the header of each frame.

**Error control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.

**Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving acknowledgement.

**Access control**: When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

**3. Network Layer**

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the

packet, from the number of routes available. The sender & receiver’s IP addresses are placed in the header by the network layer. \*\*Frame are considered here as Packets.

Functions:

**Routing:** The network layer protocols determine which route is suitable from source to destination.

**Logical Addressing**: In order to identify each device on internetwork uniquely, the network layer defines an addressing scheme. The sender & receiver’s IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

**4. Transport Layer**

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as Segments. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgement of the

successful data transmission and re-transmits the data if an error is found. \*\* Packets will be considered here as segments

**Functions**

**Segmenting**: break the message into smaller units. Each segment has a header.

**Service Point Addressing**: in order to deliver the smaller units to the correct destination system has a type of address called service point address.

**5. Session layer**

This layer is responsible for the establishment of connection, maintenance of sessions, authentication, and also ensures security.   
The functions of the session layer are :

**Session establishment, maintenance, and termination**: The layer allows the two processes to establish, use and terminate a connection.

**Synchronization**: This layer allows a process to add checkpoints which are considered synchronization points into the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided. The packets in the segments are synchronized/ arranged properly.

**Dialog Controller**: The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

**6. Presentation Layer**

The presentation layer is also called the Translation layer. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.   
The functions of the presentation layer are :

**Translation:** For example, ASCII to EBCDIC.

**Encryption/ Decryption**: Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.

**Compression:** Reduces the number of bits that need to be transmitted on the network.

**7. Application Layer**

At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

Example: Application – Browsers, Skype Messenger, etc

1. **Security of IEEE 802.15.4**

In a wired network, when the sender sends the data and receive the data by the receiver through signals. When the signals are transmitted over wire , it wont give rooms to others to know it. But in wireless network, in a coverage area if a sender sends a data, whoever in the coverage area they can still know the conversation. By the way the wireless network requires security concerns. The IEEE 802.11 was found to solve the security issue. Like Ethernet & Token ring network, IEEE 802.11 is designed for use in a limited geographical area. (Ex. home, office, campuses)

IEEE 802.11 is a wireless LAN technology. It is accessed through signals which is dispersed in the air/Space. It has additional feature also. Those are Power management & Security Mechanisms. IEEE 802.11 works on the principle called CSMA/CA (Carrier sense multiple access with collision avoidance). CSMS/CA cannot detect the collision because the signals are propagated through air. Whereas Ethernet based on the principle of CSMA/CD (Carrier sense multiple access with collision detection) CSMS/CD can detect the collision because the signals are propagated through wires.

IEEE 802.11 is based on two modes.

* Infrastructure mode ( desktop-printer-server)
* Adhoc Mode (no structure)

**Diagram

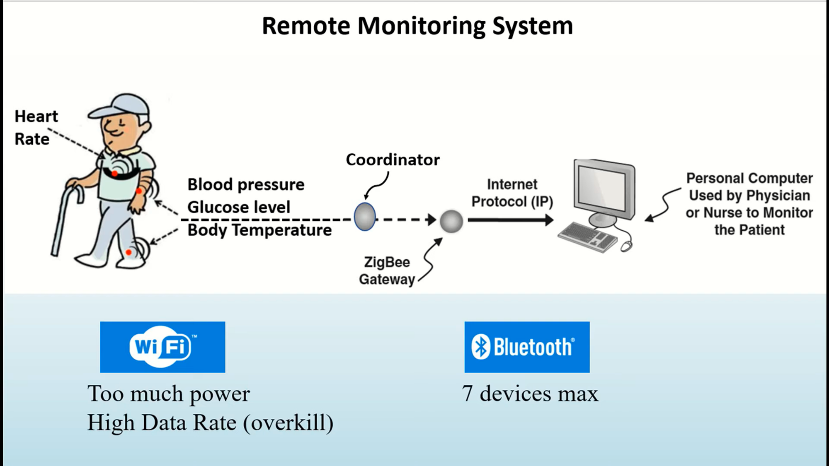
Description automatically generated**

1. **ZigBee Technology**

ZigBee is a wireless technology standard that defines a set of communication protocols for short range communications. It is specifically build for control and sensor networks. The purpose

of ZigBee is to collect the information and perform control tasks inside a building. It is a open source standard created by organization called ZigBee Alliance in 2002.

ZigBee applications – home automation, Medical Data collection, Industrial Control Systems.

Chart, radar chart

Description automatically generated

Characteristics of ZigBee Standard

* Low power consumption

Devices can typically operate for several years on a single battery.

* Low data range

It consumes only 20Kbps to 250kbps (wifi-11mbps, Bluetooth 1mbps)

* Short Range

It can operate with the range upto 75-100 meters indoor and upto 300+ meters (line of sight).

* Network joining time

It will connect in 30 msec (wifi- upto 3 secs, Bluetooth upto 10 secs)

* Support large and small networks

It can connect upto 60000 devices (wifi up to 32 devices, Bluetooth upto 7 devices)

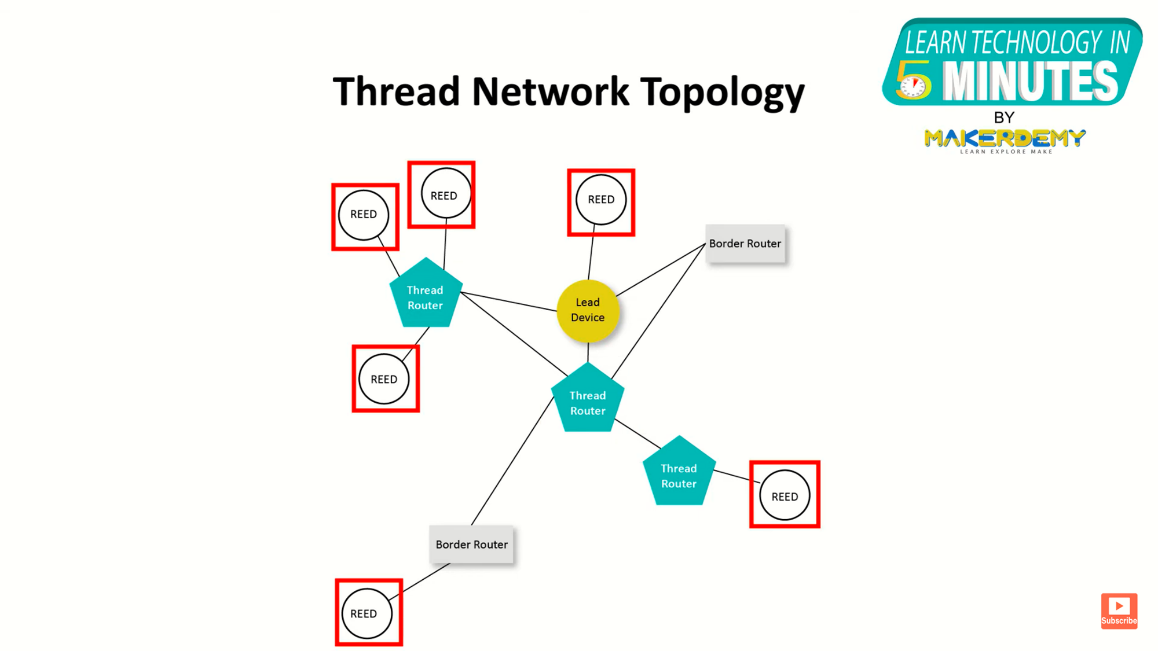
* Low cost of products and cheap implementation
* Security

It uses AES cryptographic algorithm for data encryption and data authentication.

(Advanced Encryption Standard)

1. **Thread**

Home and office automation has been built on IOT which requires reliability, security, power efficient and compatibility. To meet these requirements, the thread standard was introduced. IEEE 802.15.4 and IPv6 are wireless networks is specifically designed for low -power connected devices in the home automation space. It uses the Advanced Encryption Standard. It works on the basis of MESH Topology where you can connect up to 250 nodes. Thread was introduced in 2015 by Thread group alliance consists of google, Qualcomm, Samsung, ARM, Apple and Silicon Labs. (MESH Topology – all the devices in the network are interconnected, allows self-healing in case of failure). It has the wide variety of application in the home such as appliances, climate and access control, lighting and energy management, safety and security. Physical Layer of is based on IEEE 802.15.4, network layer access through the protocols such as IPv6, 6LowPAN.



**Thread Architecture**

1. **Borders Routers**

* More than 1 or 2 border routers
* Helps to prevent the redundancy and fail over network

1. **Lead Devices**

* Responsible for managing a registry of assigned router IDs
* Also control the request for REED (Router Eligible End Devices)
* Allows self-healing in case of failure. (MESH topology)

1. **Thread Routers**

* Manages the routing services of the mesh and never go to sleep state unless they are allowed to be downgraded to REEDs.
* Information are stored in Thread Router only.

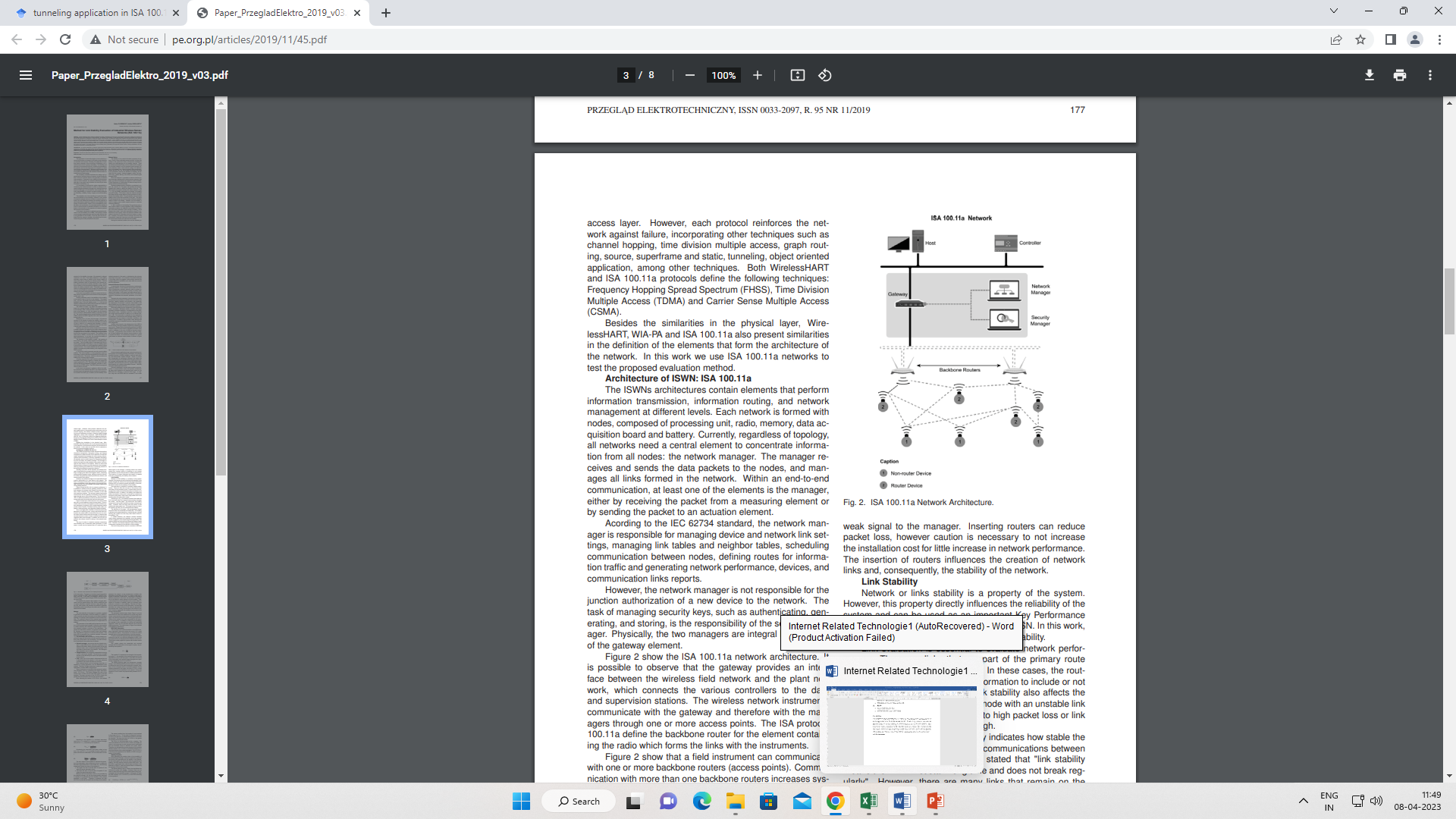
1. **REED**

* Router Eligible End Devices
* End functions can be carried by REED.

1. **ISA 100.11.A**

It is designed for large scale industries IOT. It works based on the tunnelled application layers. It used to support the VPNs. It will also connect the NRD, RD also. It is possible to observe that the gateway provides an interface between the wireless field network and the plant network, which connects the various controllers to the data and supervision stations. The wireless network instruments communicate with the gateway through one or more access points. The ISA protocol

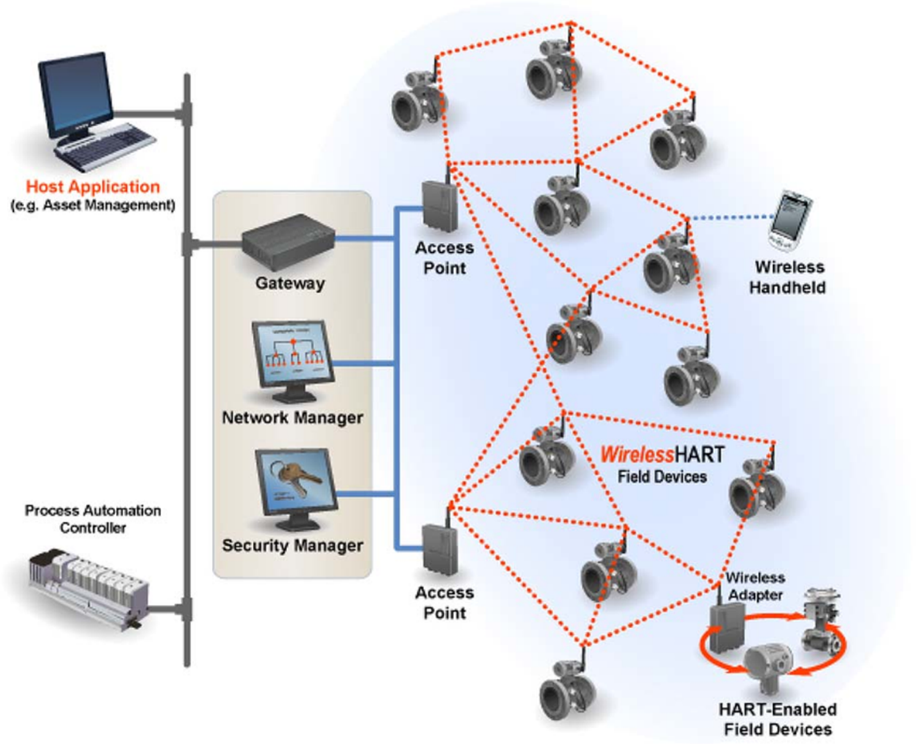
100.11a define the backbone router for the element containing the radio which forms the links with the instruments.



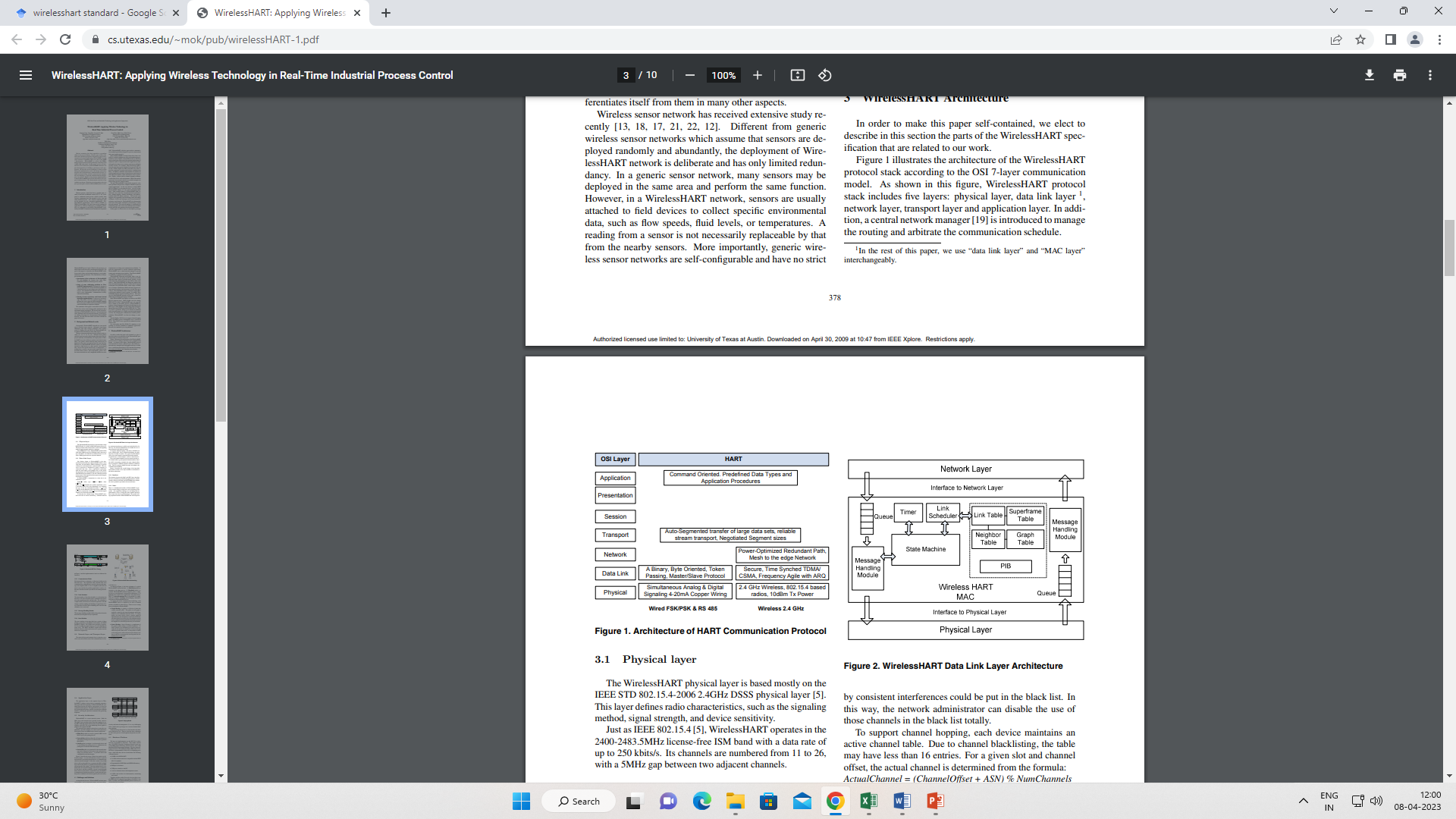
A field instrument can communicate with one or more backbone routers (access points). Communication with more than one backbone routers increases system redundancy. Multiple backbone routers provide similar benefits, including reducing data traffic congestion, reducing latency, and increasing network reliability.

1. **WirelessHART**

HART technology is a bi-directional (get and post), which means that a smart field device only speaks when spoken to by a host. The HART Protocol can be used for **communicating information to/from smart field instruments and central control or monitoring systems**. WirelessHART complements the ever so successful HART field devices by providing the possible means for communicating via wireless channels. The WirelessHART standard is designed to offer simple configuration, flexible installation and easy access of instrument data, and at the same time, ensure robust and reliable communications.



At the very bottom, it adopts IEEE 802.15.4-2006 as the physical layer. On top of that, WirelessHART defines its own time-synchronized MAC layer. Some notable features of WirelessHART MAC include network wide time synchronization, channel hopping, channel blacklisting, and industry standard AES-128 ciphers and keys. The network layer supports self-organizing and self-healing mesh networking techniques. In this way, messages can be routed around interferences and obstacles. WirelessHART also distinguishes itself from other public standards by maintaining a central network manager. The network manager is responsible for maintaining up-to-date routes and communication schedules for the network, thus guarantee the network performance.



1. **Near Field Communication**

Near Field Communication (NFC) is a specification for contactless communication between two

devices. NFC is based on the technology used for RFID and is standardised in ISO/IEC 18092. It is limited to a distance between the two devices of up to 10 cm. NFC is intended to make it easier and more convenient to make transactions, exchange digital content, and connect electronic devices with a touch. NFC has been developed jointly between NXP Semiconductors (formerly

Philips Semiconductors) and Sony Corporation. Because NFC has the ability to read and write to devices, it is believed that they will have a wider use in the future than standard smart cards.

NFC involves an initiator and a target. The initiator, as follows from the name, initiates and actively generates an RF signal and controls the exchange of data (a payment device) where the request is answered by a passive target (a Smartphone). The NFC protocol also distinguishes between two modes of communication: active and passive.

(for ref: Active is where both the initiator and target both communicate by generating their own electric fields. They do this in half duplex; deactivating their RF field until no other device is transmitting. In this mode both devices will typically have power supplies. Passive mode will be the more common application in where the initiator is the only device that generates an RF signal, the target device answers that call by modulating the existing field which the initiator device listens out for, and then processes therefore transferring data)



1. **Z-Wave**

Z-Wave was described by as a new wireless home automation technology that uses very low power. It communicates in the frequency of 900MHz and range of around 30 meters. It makes devices double as repeaters and also has network reliability that enables commercial applications.

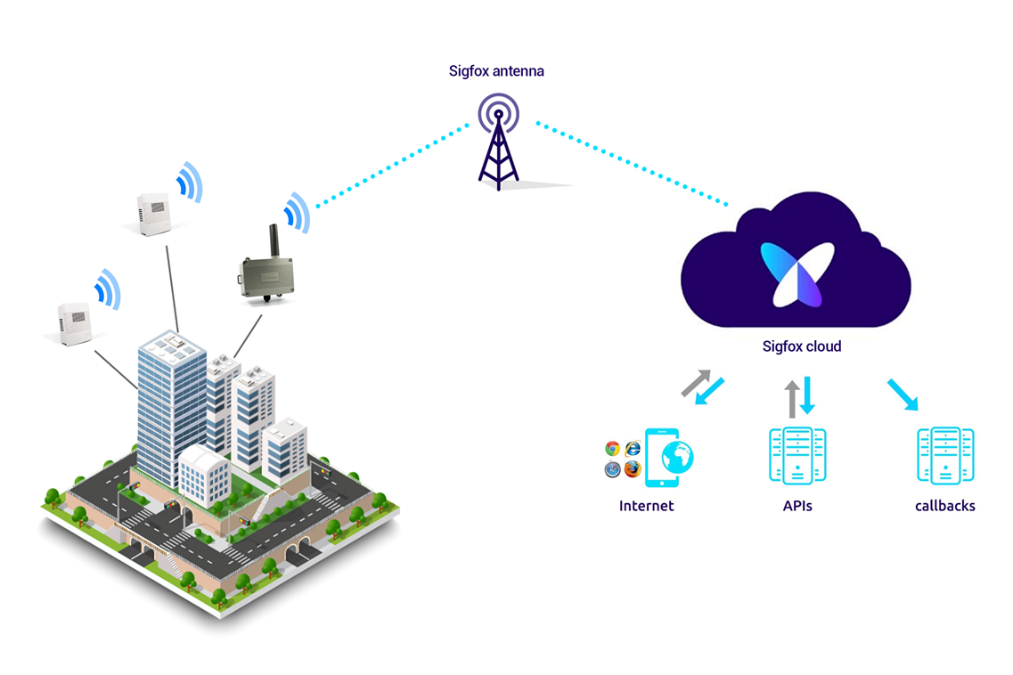
Z-Wave is mostly used for control and monitoring, and it does not allow any interference from Wi-Fi or any other 2.4GHz wireless technology.

Features:

* allows commercial devices and hundreds of nodes with high density.
* Best choice in energy saving,
* low-cost and power consumption.

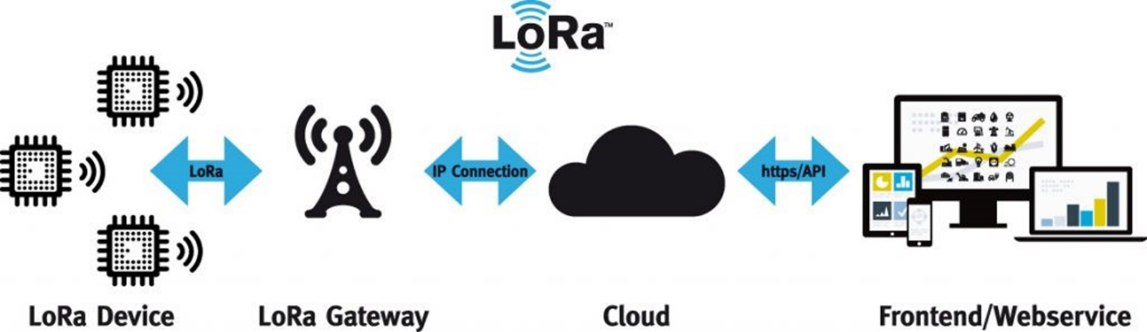
1. SIGFOX

It is a software-based communication solution. Networking and computing all are managed in cloud not on the device. Sigfox is a narrowband (or ultra-narrowband) technology. It uses a standard radio transmission method called binary phase-shift keying (BPSK),(Common examples of radio transmissions are the signals coming from over-the-air radio and television stations, cellular phones, or walkie-talkies) . It is necessary to have two elements to make a radio transmission. The first is a transmitter, which is a device that generates an alternating electrical current of a very high frequency. The transmitter is connected to the second necessary element, an **antenna**, which changes this electrical current into **electromagnetic waves.**

****

1. **LoRA -** Long range Radio

LoRa is the de facto wireless platform of Internet of Things (IoT). LoRa based communication protocol called LoRaWAN was standardized by LoRa-Alliance. Semtech's LoRa chipsets connect sensors to the Cloud and enable real-time communication of data and analytics that can be utilized to enhance efficiency and productivity.



LoRa works on the spread spectrum technology using the unlicensed sub-GHZ band. The LoRa chirp spread spectrums (CSS) modulations ensure full bidirectional communication, and the generated signal has low noise levels, enables high interference resilience, and is difficult to detect or jam.

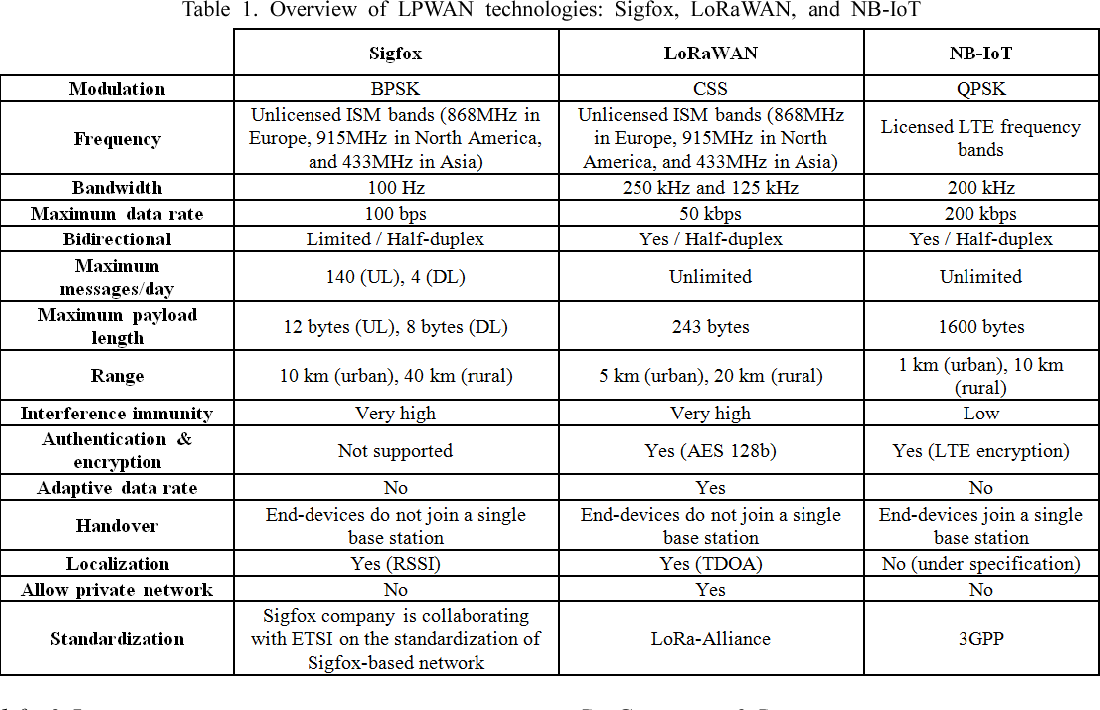
1. **Narrowband IoT**

Narrowband IoT (NB-IoT) is a wireless internet of things (IoT) protocol using low-power wide area network (LPWAN) technology. It was developed by 3GPP (3rd Generation Partnership Project) for cellular wireless communication that enables a wide range of new NB-IoT devices and services. NB-IoT can enable a broad range of new IoT devices and services. NB-IoT reduces the power consumption of connected devices, while increasing system capacity and bandwidth efficiency, particularly in locations that aren't easily covered by traditional cellular technologies

NB-IOT work based on the carrier network. A telecommunications carrier network is the collection of devices and underlying infrastructure used to transmit data from one location to another).

**Sigfox VS LoRA**

* Technology: Sigfox uses a proprietary ultra-narrowband technology, which means that it uses a very **narrow band of frequencies to transmit data**. LoRa, on the other hand, uses a **spread-spectrum technology**, which spreads data over a wider band of frequencies.
* Range: Sigfox has a longer range than LoRa, with a single base station covering up to hundreds of square kilometers. LoRa, on the other hand, has a range of up to tens of kilometers.
* Bandwidth: Sigfox has a lower bandwidth than LoRa, with a maximum data rate of 100 bits per second. LoRa, on the other hand, has a higher bandwidth, with a maximum data rate of 27 kbps.
* Cost: Sigfox devices are generally more expensive than LoRa devices, due to the proprietary technology and the cost of the Sigfox network. LoRa devices are generally less expensive, as the technology is open source and the LoRa network can be built using off-the-shelf components.
* Power consumption: Sigfox devices have lower power consumption than LoRa devices, as they transmit data less frequently. This makes Sigfox devices ideal for applications where battery life is critical.



**IOT – Infrastructure Protocols**

* **Cloud connectivity** (asset tracking, home automation, industrial automation, etc.) using technologies like WiFi or cellular networks like NB-IoT etc.
* **Long-range local networks** (smart city, smart agriculture, etc.) using technologies like LoRa, Zigbee, Sigfox, etc.
* **Short-range local networks** (tracking vital health parameters using wearables, smart door locks, etc.) using technologies like BLE, NFC, ZWave, etc.

**Infrastructure Protocols**

1. **IPv6 - Internet Protocol Version 6.**

At the Internet layer, devices are identified by IP addresses. IPv6 is typically used for IoT applications over legacy IPv4 addressing. IPv4 is limited to 32-bit addresses, which only provide around 4.3 billion addresses in total, which is less than the current number of IoT devices that are connected, while IPv6 uses 128 bits, and so provides 2 128 addresses (around 3.4 × 10 38 or 340 billion) addresses. In practice, not all IoT devices need public addresses. Of the tens of billions of devices expected to connect via the IoT over the next few years, many will be deployed in private networks that use private address ranges and only communicate out to other devices or services on external networks by using gateways.

1. **6LoWPAN- Low Power Wireless Personal Area Network**

The IPv6 Low Power Wireless Personal Area Network (6LoWPAN) standard allows IPv6 to be used over 802.15.4 wireless networks. 6LoWPAN is often used for wireless sensor networks, and the Thread protocol for home automation devices also runs over 6LoWPAN.

1. **RPL –Routing Protocol**

The Internet Layer also covers routing. RPL (pronounced “ripple”) is designed for routing packets within constrained networks such as wireless sensor networks, where not all devices are reachable at all times and there are high or unpredictable amounts of packet loss. RPL can compute the optimal path by building up a graph of the nodes in the network based on dynamic metrics and constraints like minimizing energy consumption or latency. (LOADng is also a RPL)

1. **Micro internet protocol (uIP)**

uIP is the worlds smallest full TCP/IP stack. Intended for tiny microcontroller systems where code size and RAM are severly constrained, uIP only requires 4-5 kilobytes of code space and a few hundred bytes of RAM. uIP has been ported to a wide range of systems and has found its way into many commercial products.

1. **Nano IP**

Nano IP is an open source ligthweight IP stack targeting 16 to 32bits microcontrollers.

**Discovery Protocols**

Protocol used to discover a resource. When discovering a large number of resources, network traffic associated with the discovery process might cause timeouts that result in some discoverable resources remaining undiscovered. To help prevent this problem, use one or more discovery protocols. Using a discovery protocol enables you to target specific resources and limit the number of communication protocols used during discovery. Limiting the number of communication protocols used when discovering a large number of resources helps avoid problems caused by network traffic collisions and timeouts. They are few important types of Discovery Protocols. Those are :

1. **Physical web**

Physical Web (Beacons are suitable for all kinds of application scenarios that require communication between everyday objects and their environment) If an item has been equipped with a beacon, it can send messages to smartphones that support BLE, for example informing about delays, special offers or campaign days**.** In this context, the physical web ensures, among other things, that users do not have to install new apps everywhere, but can view the news on a uniform interface.

Example 1: The intelligent bus stop: A bus stop nearby could tell waiting for people via their smartphone when the next bus will come. In this case, the physical web BLE sensor sends out a URL that leads to the website of the bus stop. In order to distinguish them from others, the URL would contain an identification code of the stop.

Example 2: Monitored household appliances: The physical web can also be used to control and monitor household appliances such as the washing machine. Each device sends out a URL that refers to an IP address and can only be reached when connected to the local network. The visibility of the URL can be limited to devices in the network if network discovery techniques such as mDNS and SSDP are used instead of BLE (Bluetooth)

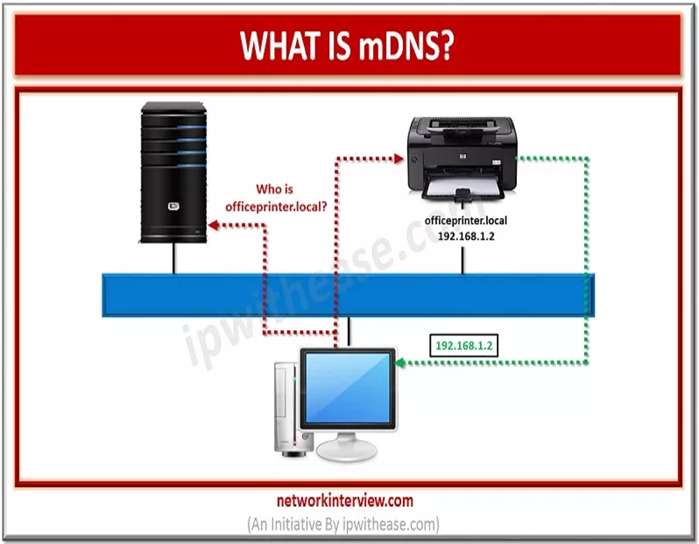


**2. Multicast DNS (multi Domain Name System)**

Multicast DNS and DNS Service Discovery are established and widely used standards in current IP-based networks to enable the discovery of devices and services at the application layer with DNS messages.

As DNS does not meet the requirements of low data rate smart object networks, Multicast DNS is designed for small networks and is intended to increase their user-friendliness. The idea is that users can connect devices in secret LANs without any issues. Because all devices exchange information with one another via their IP addresses, no server or directory has to be established.

Multicasting refers to a single source of communication with simultaneous multiple receivers. Most popular distributed multimedia applications require multicasting.



**3. Universal plug and play**

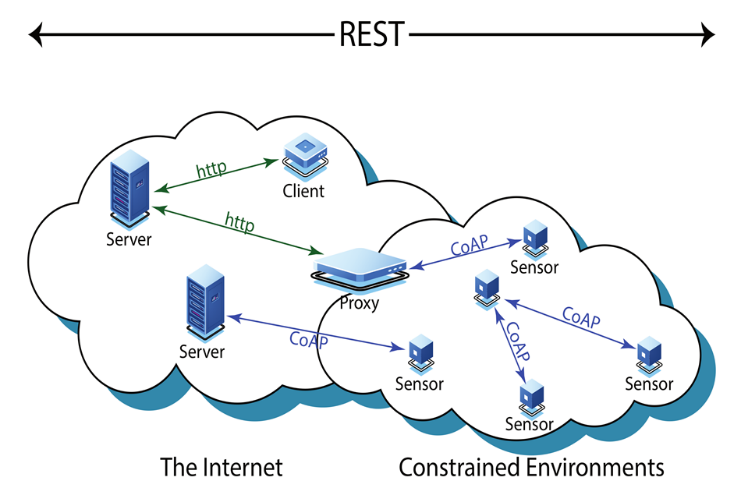
The Universal Plug and Play (UPnP) architecture enables pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices. It is a distributed, open networking architecture that leverages TCP/IP and Web technologies to enable seamless proximity networking in addition to control and data transfer among networked devices in the home, office, and everywhere in between. Universal Plug and Play (UPnP) is a protocol that allows UPnP-enabled devices on your network to automatically discover and communicate with each other.

**Application Layer Protocol**

* **CoAP ,**
* **MQTT and**
* **REST**

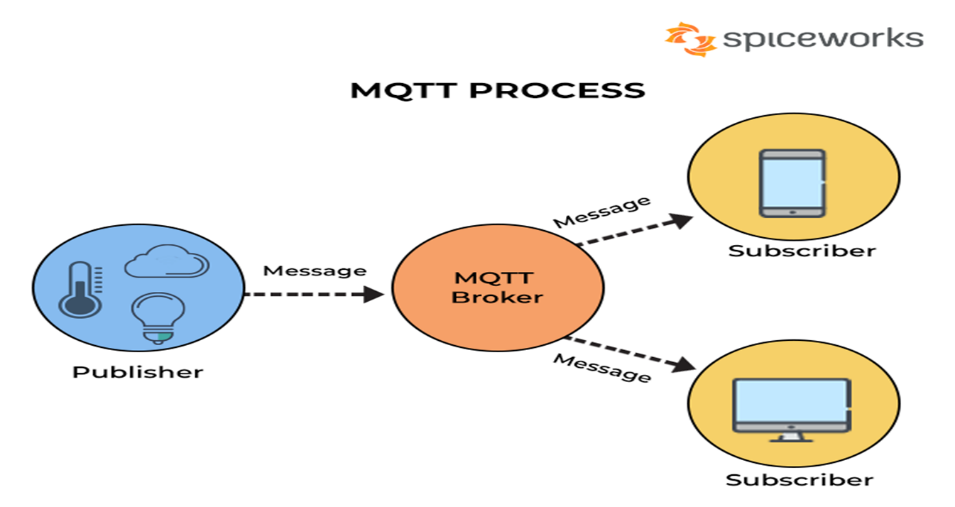
**CoAP- Constrained Application Protocol**

The Constrained Application Protocol (CoAP) is a specialized web transfer protocol for use with constrained nodes and constrained (e.g., low-power, lossy) networks. The nodes often have 8-bit microcontrollers with small amounts of ROM and RAM. The protocol is designed for machine- to-machine (M2M) applications such as smart energy and building automation.



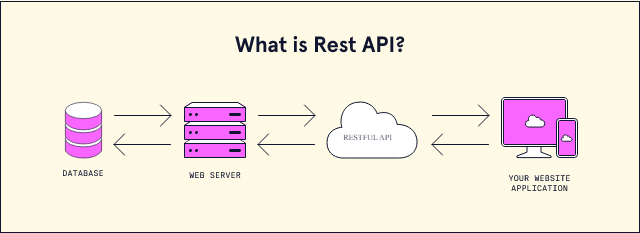
**MQTT-Message Queuing Telemetry Transport**

In IoT, device to device communications are considered through Pushing protocol. Push protocol is more suitable for IoT devices because of its light-weight and high productivity. (TCP includes a special “push” function to handle cases where data given to TCP needs to be sent immediately, Example Instant Msgs, services) There are many Push protocols available for IoT such as XMPP, MQTT, AMQP in which MQTT is most widely used. The key feature of MQTT is its light-weight and bandwidth efficiency.



**REST (Representational State Transfer)**

RESTful API is an interface that two computer systems use to exchange information securely over the internet. Most business applications have to communicate with other internal and third-party applications to perform various tasks. REST protocol, consists of independent components exposing the data they produce and consume the services they provide as independent communication endpoints referenced by URLs.



References

1. Stiller, B., Schiller, E., Schmitt, C., Ziegler, S., & James, M. (2020). An overview of network communication technologies for IoT. *Handbook of Internet-of-Things*, *12*.

2. Al-Sarawi, S., Anbar, M., Alieyan, K., & Alzubaidi, M. (2017, May). Internet of Things (IoT) communication protocols. In *2017 8th International conference on information technology (ICIT)* (pp. 685-690). IEEE.

3. Herrero, R. (2022). *Fundamentals of IoT communication technologies*. Cham: Springer.

4. Kumar, S., Dalal, S., & Dixit, V. (2014). The OSI model: Overview on the seven layers of computer networks. *International Journal of Computer Science and Information Technology Research*, *2*(3), 461-466.

5. Florencio, H., & Neto, A. D. D. (2019). Method for link stability evaluation of industrial wireless sensor networks (ISA 100.11 a). *Prz. Elektrotechniczny*, *11*, 176-183.

6. Want, R. (2011). Near field communication. *IEEE Pervasive Computing*, *10*(3), 4-7.

7. Danbatta, S. J., & Varol, A. (2019, June). Comparison of Zigbee, Z-Wave, Wi-Fi, and bluetooth wireless technologies used in home automation. In *2019 7th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-5). IEEE.

8. Al-Sarawi, S., Anbar, M., Alieyan, K., & Alzubaidi, M. (2017, May). Internet of Things (IoT) communication protocols. In *2017 8th International conference on information technology (ICIT)* (pp. 685-690). IEEE.

9. Lauridsen, M., Nguyen, H., Vejlgaard, B., Kovacs, I. Z., Mogensen, P., & Sorensen, M. (2017, June). Coverage comparison of GPRS, NB-IoT, LoRa, and SigFox in a 7800 km² area. In *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)* (pp. 1-5). IEEE.