Research Phase 4 – Selecting
Suitable IoT protocols

Smart-Agro

IoT Agricultural Solutions

Digital Labs - Sri Lanka Telecom PLC

Table of Contents

WHICH IOT PROTOCOL TO CHOOSE?

A guide to selecting wireless communication protocols and standards for the project

Introduction

Currently, IoT is functioning over existing communication infrastructure and standards such as Bluetooth and Wi-Fi in the Data link layer, and HTTP in the Application layer. But the advancement of the IoT concept has required specific standards to be designed especially for IoT. These protocols should ensure data transfer from end devices such as sensors to subsequent steps in the connected environment, but at the same time link a large number of low-energy, low-power devices cost effectively.

Depending on the use case, there are multiple different protocols available of specific capabilities or combination of features. Some might enable device-to-device communication while others device-to-gateway or device-to-cloud or even gateway-to-cloud communication. Choosing the right protocol is crucial for the success of an IoT project.

The need of a protocol, factors to consider when selecting a protocol, different protocol suits and stacks, and existing communication standards will be discussed briefly in the subsequent sections of this report.

.

Protocols in IoT – An Overview

The Protocols build a bridge between components of the IoT architecture. They enable exchange of data between hardware as well as software. The protocols itself defines standards needed for this data transfer.

Protocol, Protocol Suite, and Protocol Stack

A **Protocol** is a set of rules that govern how systems communicate with each other and how data is shared. A **Protocol Suite** is a collection of these protocols designed to function together. This Protocol suite is arranged in independent layers interconnected but functioning concurrently, in a stack called the **Protocol Stack**. Each level of this stack performs a particular function and communicates with the levels above and below it. Different technologies conceptualize how data is communicated over the entire stack. The most well know protocol stacks are the OSI Reference model and the TCP/IP 4-layer model.

7 Layer OSI Reference Model

7. Application Layer
- End User Layer
- HTTP, FTP, IRC, SSH, DNS

6. Presentation Layer
- Syntax layer - Data representation, compression and encryption
- SSL, SSh, IMAP, FTP, MPEG, JPEG

5. Session Layer
- Maintains connections, control ports and establishes, manages, and terminates sessions
- APIs, Sockets, WinSock

4. Transport Layer
- End-to-end connections
- TCP, UDP

3. Network Layer
- Arrange data Packets - Path determination and Logical addressing
- IP, ICMP, IPSec, IGMP

2. Data Link Layer
- Organize bits into Frames - Physical Addressing (MAC)
- Ethernet, PPP, Switches, Bridge

1. Physical Layer
- Transfer bits of data over the Physical Medium
- Coax, Fiber, Wireless, Hubs, Repeaters

4 Layer Model

4 Layer TCP/IP Model		7 Layer OSI Model
Authentication Layer	Application Layer (Data)	Application Layer
		Presentation Layer
		Session Layer
Data Flow Layer	Transport Layer (Segments)	Transport Layer
	Network Layer (Packets)	Network Layer
	Link Layer / Network Access Layer (Bits and Frames)	Data Link Layer
		Physical Layer

Other Models

In addition to this, IoT is also expressed in a multilayer model, which also includes:

1. **three-layer model:**

    - Perception
    - Network
    - Application

2. **four-layer model:**

    - Perception
    - Support
    - Network
    - Application

Expected IoT Protocols

However, in IoT as well, protocols in use generally vary by layer and they are different from the above-mentioned existing internet protocols. The new protocols are slowly replacing the existing ones.

Current protocols		Expected IoT Protocols
HTTP, FTP, SMTP, IMAP	Presentation / Application	**MQTT**, COAP, AMQP, HTTP, DDS, WebSockets
TCP, UDP	Transport	**UDP**, TCP
IPv4, IPv6	Networking	**IPv6**, IPv4
Ethernet, Wi-Fi, Cellular (GSM, LTE), Bluetooth	Data Link / Physical	Wi-fi, LoRa, LoRaWAN, Bluetooth, Zigbee, ZWave, Cellular (GSM, LTE-M, 5G), Ethernet, SigFox

IoT data protocols (Presentation / Application layers)

MQTT (Message Queuing Telemetry Transport)

MQTT is a lightweight publisher-subscriber model designed for M2M telemetry in restricted environments with constricted networks. The protocol works on top of TCP. The protocol being lightweight is advantageous in IoT with the increasing number of small, cheap, and low-power objects entering the market. MQTT architecture is relatively simple and easy to implement and also allows for simple data flow between different devices.

It is a many-to-many communication protocol for communication between multiple clients through a central broker. It decouples producer and consumer by letting clients publish and having the broker decide where to route and copy messages. Message delivery in MQTT is ensured due to the Prescence of QoS level. Therefore, reliability is guaranteed. However, the security is not built in. But this allows user to change security solutions as devices and technology evolves.
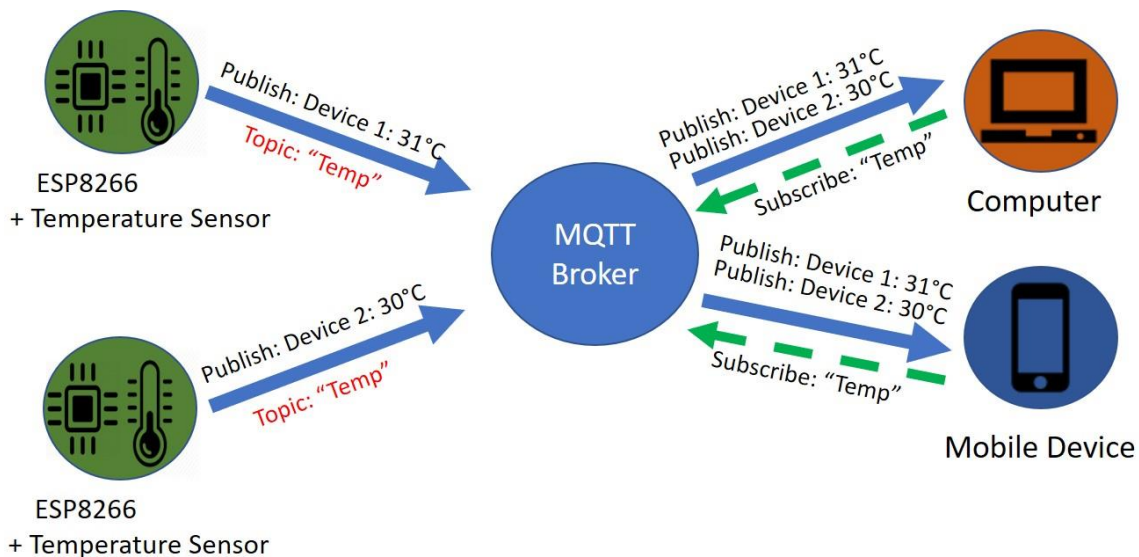
MQTT Architecture

CoAP (Constrained Application Protocol)

COAP is a RESTful application protocol running over UDP (async) as the underlying network protocol. It also uses request/response models like HTTP. The protocol is specially designed to address the limitations in HTTP when it comes to resource-constrained, low-power devices in loss prone networks such as IoT microcontrollers and WSN nodes (explained in the HTTP section). Since COAP is simpler than HTTP, it has lower latency and draw less power. It also enables secure connections and data transmission between multiple points, especially when there is a high number of end devices within the network.
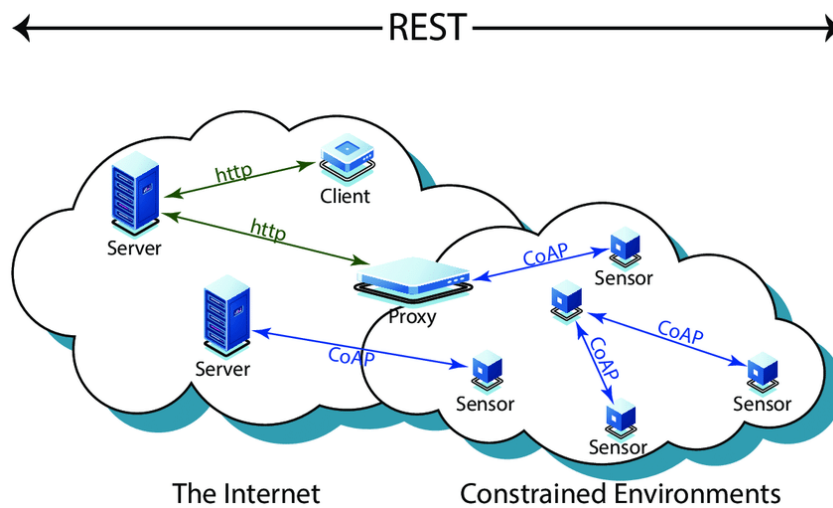
CoAP Architecture – (source: www.researchgate.net)

MQTT or CoAP?

MQTT	COAP
Publish/subscribe model with central broker, makes MQTT a many-to-many protocol	Request/Response model. Therefore a one-to-one protocol
Runs on TCP	Runs on UDP
QoS guarantees data delivery	No QoS levels
Supports persistent communications	Does not support persistent communications

- CoAP can sometimes be more resource-efficient than MQTT. Extremely low overhead makes CoAP a scalable protocol that can be used with a large number of connected devices.
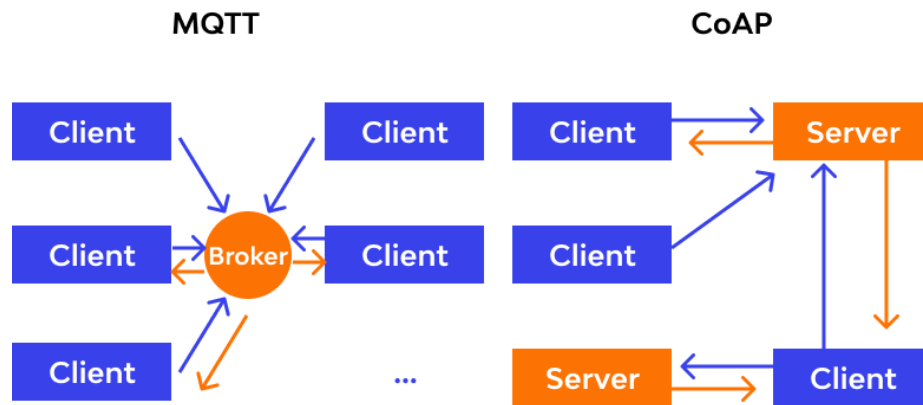
CoAP vs MQTT – (source: www.wallarm.com)

AMQP (Advanced Message Queuing Protocol)

AMQP is an open standard application layer protocol designed for interoperability between all messaging middleware. It allows client-server messages to be passed between applications.

The main functions of AMQP protocol are message orientation, message queuing, storing and routing and setting up relationships between components. The protocol is secure as well as reliable since message delivery is guaranteed

AMQP is most commonly used in server-based analytical environments such as the banking industry. However, due to its heaviness, it's not suitable for IoT sensor devices with limited memory. Therefore, it's not widely used elsewhere.

AMQP Architecture - (Source: https://www.tutorialspoint.com/)
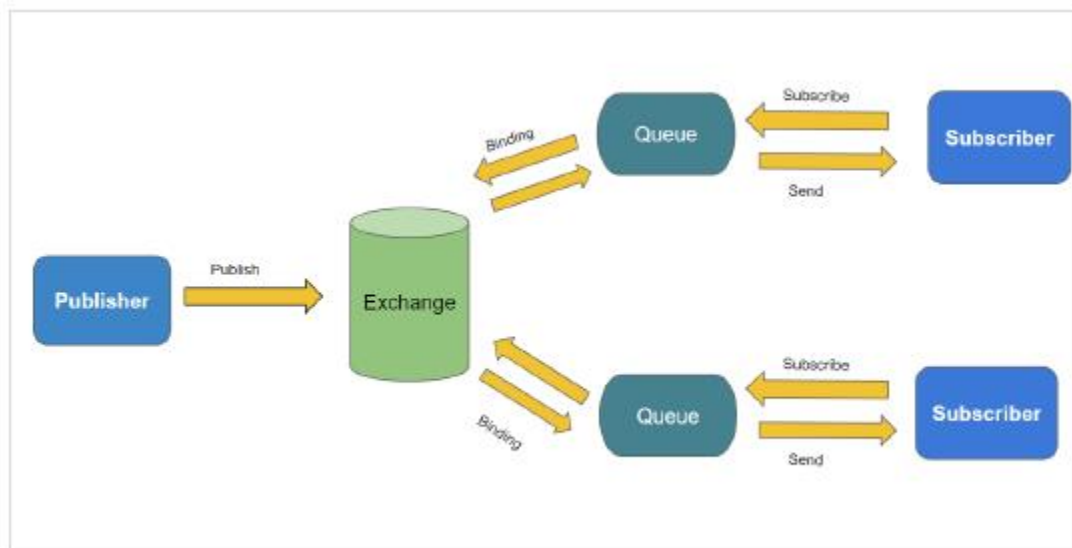
DDS (Data Distribution Service)

A middleware protocol and API standard for data-centric connectivity. It is an IoT protocol developed for M2M (Machine to Machine) Communication by OMG (Object Management Group). DDS also exchange data via a publisher-subscriber model. The protocol is best suited for embedded systems that require extremely reliable, low-latency, real-time data exchange such as aerospace and defense, medical systems, transportation systems, grid management systems etc. Unlike MQTT, the DDS protocol allows for interoperable data exchange that is independent of the hardware and the software platform. DDS also makes use of broker-less architecture unlike MQTT and CoAP protocols. DDS is considered the first open international middleware IoT standard.
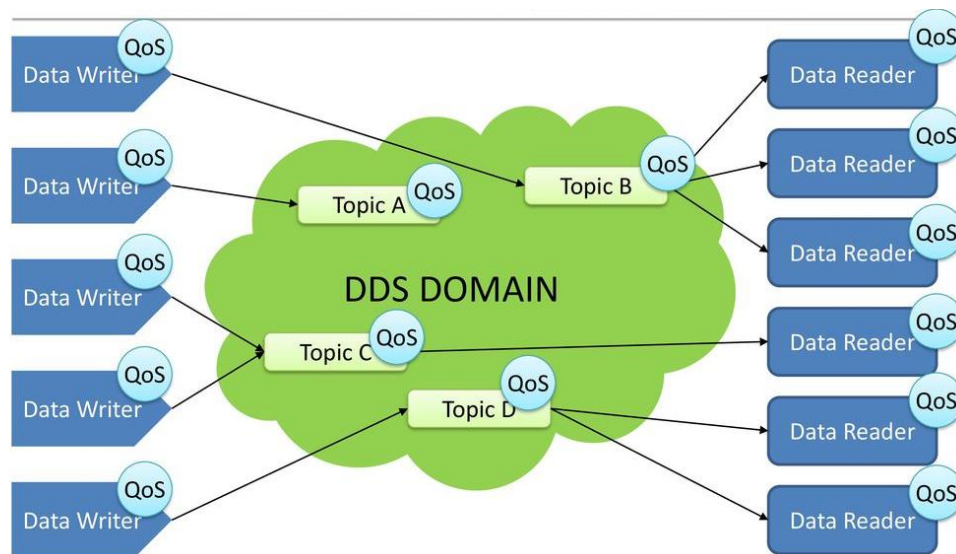
HTTP (Hypertext Transfer Protocol)

It is evident that HTTP is the protocol that powers the World Wide Web (WWW). However the protocol is a bit too heavy and power-consuming for most IoT applications.

Nevertheless, HTTP is still popular in some IoT applications that involves the use of REST APIs which are becoming the main mechanism for Web Applications and services to communicate. Manufacturing and 3-D printing also rely on the HTTP protocol due to the large amounts of data it can publish.

HTTP Architecture - (Source: https://www.tutorialspoint.com/)
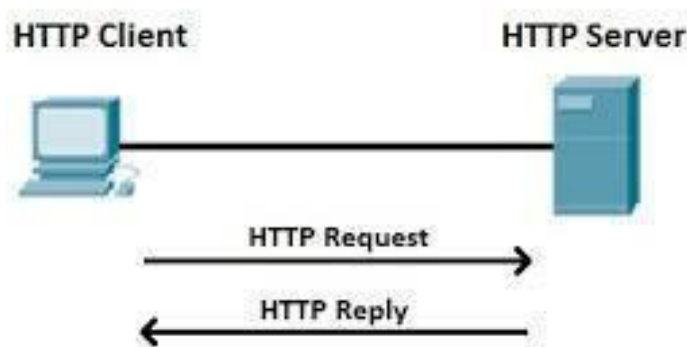
WebSocket

The WebSocket protocol is an independent TCP-based protocol. It's standard connectivity protocol helps simplify many of the complexities and difficulties involved in the management of connections and bi-direction communication on the internet. It can be applied to an IoT network where data is communicated continuously across multiple devices.

WebSockets were initially designed for the full-duplex communication channel between browsers and servers. Unlike HTTP, where updates have to be constantly requested, with websockets, updates are sent immediately when they are available. Therefore, is faster than HTTP connections.
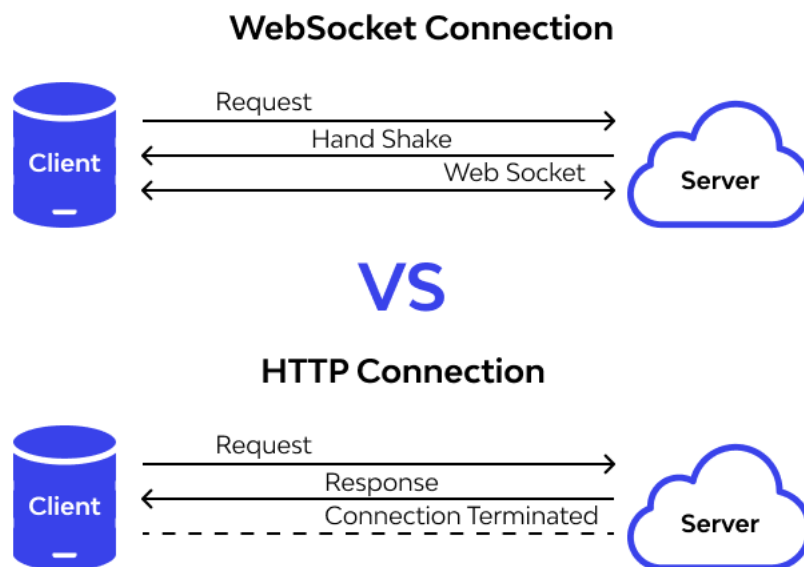
HTTP and WebSockets Comparison - (Source: www.wallarm.com)

IoT Data Protocols – A Brief Comparison

Although, a handful of protocols are available at the initial stages of IoT, history suggests that one particular standard would be more popularly used and prevail longer. Even at the early stages of WWW, there has been many protocols alongside HTTP, until it became the most widely used. Popularity suggests **MQTT** would be the prevailing standard of IoT in the days to come.
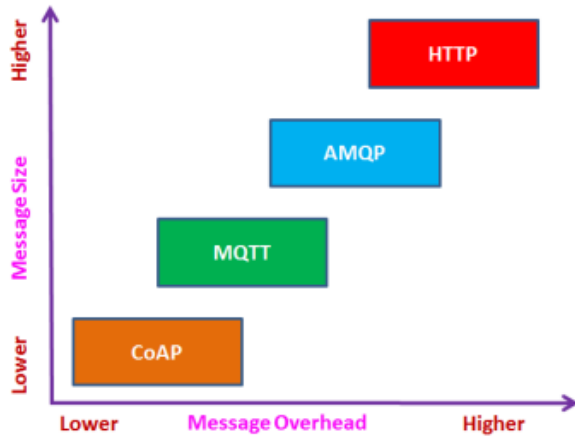
Fig. 2: Message Size vs. Message Overhead
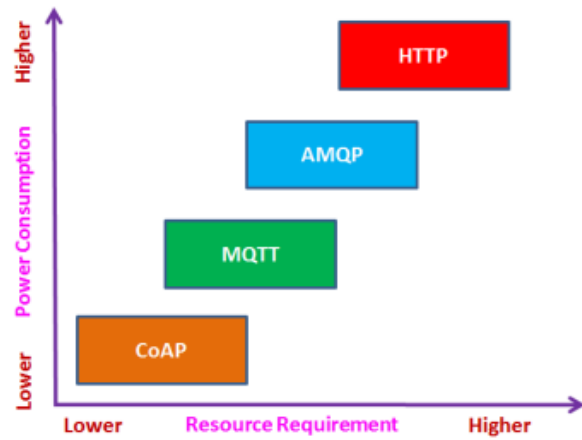
Fig. 3: Power Consumption vs. Resource Requirement
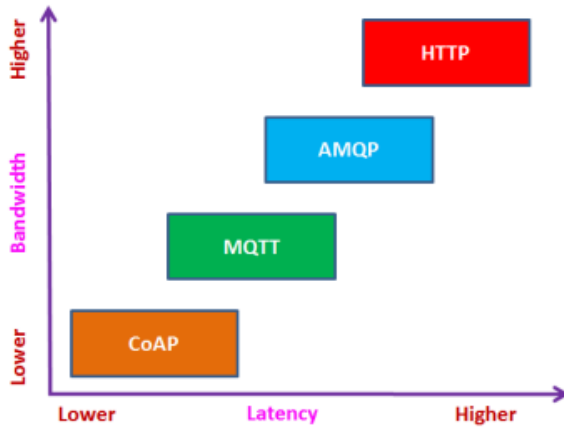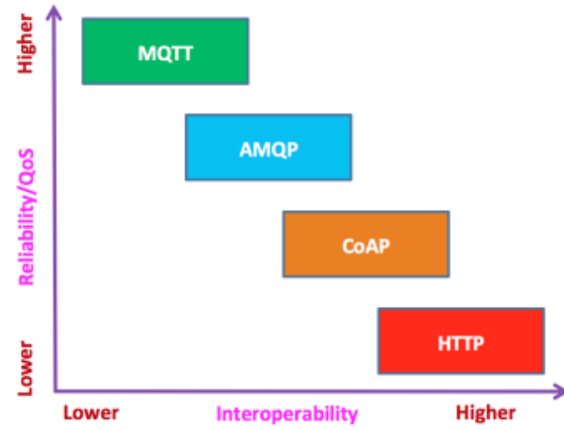

Fig. 4: Bandwidth vs. Latency
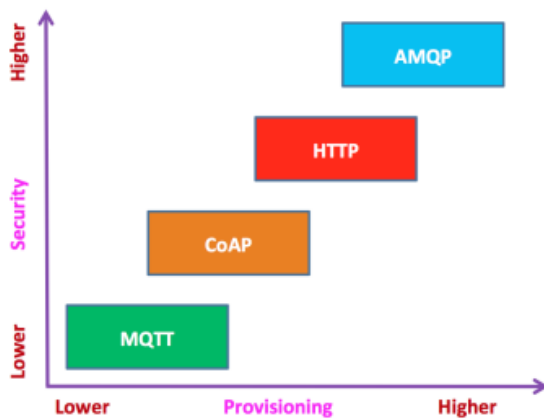

Fig. 5: Reliability/QoS vs. Interoperability

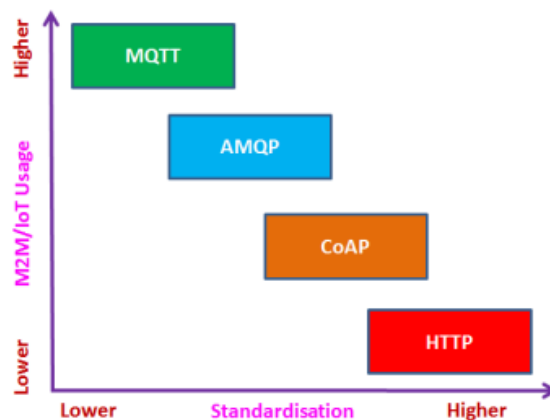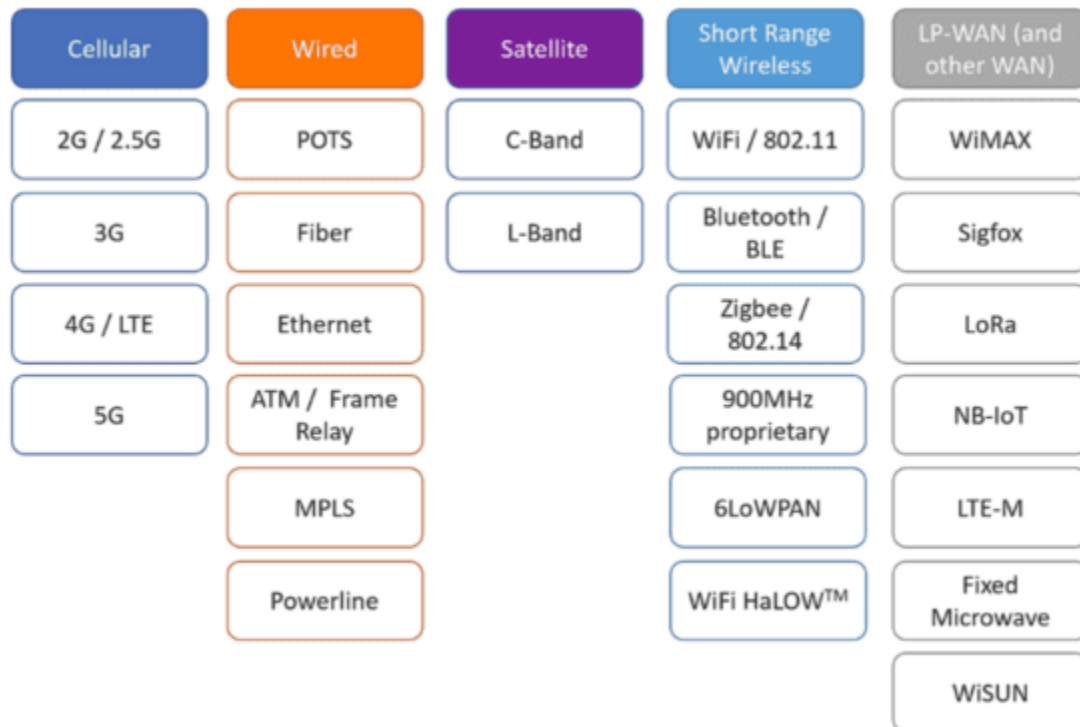Fig. 6: Security vs. Provisioning

Fig. 7: M2M/IoT Usage vs. Standardisation

(Source: "Choice of Effective Messaging Protocols for IoT Systems" by Nitin Naik)

12

Network protocols for IoT (Datalink / Physical layers)

Cellular	Wired	Satellite	Short Range Wireless	LP-WAN (and other WAN)
2G / 2.5G	POTS	C-Band	WiFi / 802.11	WiMAX
3G	Fiber	L-Band	Bluetooth / BLE	Sigfox
4G / LTE	Ethernet		Zigbee / 802.14	LoRa
5G	ATM / Frame Relay		900MHz proprietary	NB-IoT
	MPLS		6LoWPAN	LTE-M
	Powerline		WiFi HaLOW™	Fixed Microwave
				WiSUN

(Source: www.tatacommunications.com)

Wi-Fi (Wireless Fidelity)

Wi-Fi is the most popular IOT communication protocols for wireless local area network (WLAN) that utilizes the IEEE 802.11 standard through 2.4 GHz UHF and 5 GHz ISM frequencies. Both frequency ranges have several channels through which different wireless devices can work. This prevents the overflowing of the wireless networks. It provides an internet connection to nearby devices within a specific range of around 20 – 100 meters. The main impacts on the range and speed of a Wi-Fi connection are the environment and whether it provides internal or external coverage.

Wi-Fi offers fast data transfer and is capable of processing large amounts of data. However, many Wi-Fi standards, including the one commonly used in homes, is too power-consuming for some IoT use cases, particularly low-power/battery-powered devices. That limits Wi-Fi as an option for some deployments. Additionally, Wi-Fi's low range and low scalability also limit its feasibility for use in many IoT deployments.

To address this issue, there are currently different Wi-Fi standards being developed, specifically for IoT, such as Wi-Fi HaLow (802.11ah) and HEW (802.11ax) for example.
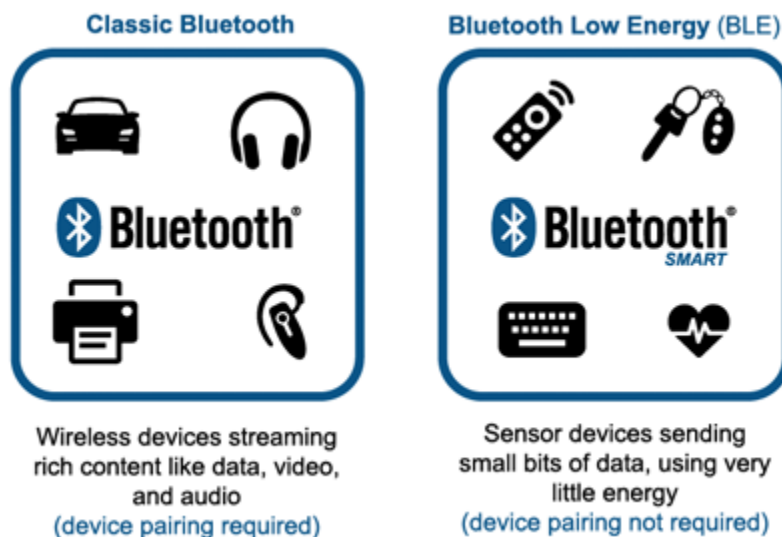
Bluetooth and BLE

Bluetooth is a low power, short-range (10-100 meters) wireless technology that uses short-wavelength, ultrahigh-frequency radio waves. The technology gained more popularity in after integration with mobile phones and wearables. Bluetooth devices automatically detect and contact each other making communication between devices very easy.

The current Bluetooth standard is at version 4.0, Bluetooth 4 has 2 flavors:

- Classic Bluetooth and
- Bluetooth Low energy

BLE (also known as **Bluetooth smart**) is optimized for IoT. It consumes less power than standard Bluetooth, which makes it particularly appealing in many use cases. This new technology can be the foundation for IoT applications that require significant flexibility, scalability, and low power consumption.

Classic Bluetooth
Wireless devices streaming rich content like data, video, and audio
(device pairing required)

Bluetooth Low Energy (BLE)
Sensor devices sending small bits of data, using very little energy
(device pairing not required)

Cellular

Cellular IoT connects physical objects to the Internet utilizing the same cellular network currently used by smartphones. It is one of the best options for deployments where communications range over longer distances. The existing 2g and 3G standards have been phased out and replaced by 4G/LTE and 5G. 5G and IoT are said to be intertwined technologies due to the low-latency, high bandwidth, high speed, massive machine type, secure and reliable communication provided by the technology.
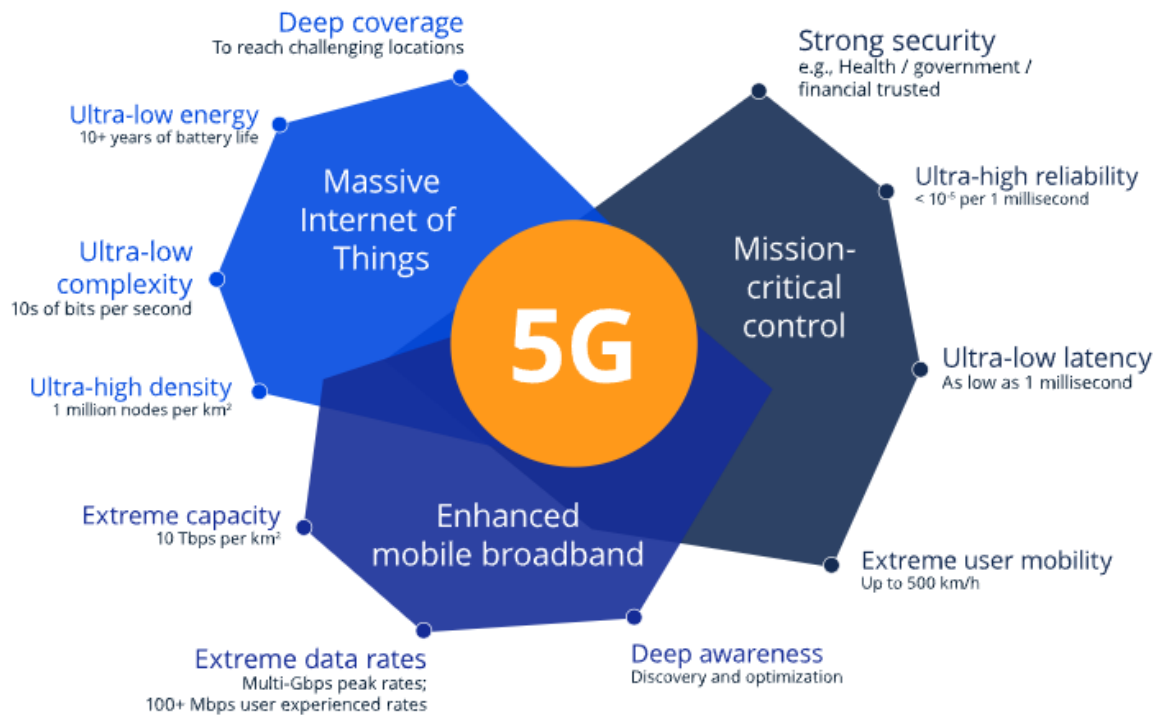
ZigBee

Zigbee, supported by the Zigbee Alliance, is a mesh network protocol designed for building and home automation applications. The protocol is similar to BLE but is more power efficient and has a longer range of communication (ZigBee can reach 200 meters, while Bluetooth maxes out at 100 meters). However, data rates are lower than BLE. It's a simple packet data exchange protocol and is often implemented in devices with small requirements, such as microcontrollers and sensors. It is easily scalable, and all the nodes are connected through the ZigBee gateway.
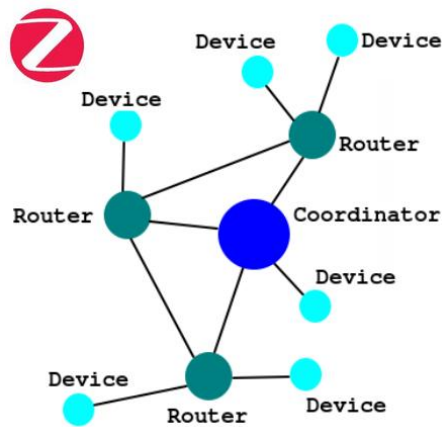
Zigbee Mesh Architecture

Z-Wave

Z-Wave is also a wireless mesh network communication protocol built on low-power radio frequency (RF) technology. It's commonly used for home automation products and security systems, as well as in applications, such as energy management technologies. Similar to Zigbee, Z-Wave is also supported by a Z-Wave Alliance. It operates on the 800-900 MHz radiofrequency, while Zigbee operates on 2.4GHz, which is also a major frequency for Wi-Fi. By operating in its own range, Z-Wave rarely suffers from any significant interference problems. However, the frequency that Z-Wave devices operate vary from country to country.

LoRa / LoRaWAN (Long Range Wide Area Network)

LoRa is an open protocol managed by the LoRa Alliance. It is a noncellular wireless technology that offers long-range communication capabilities

LoRa, short for "Long Range" is an RF modulation technique for specific wireless spectrum, while LoRaWAN is an open cloud-based media access control (MAC) IoT protocol. Its network architecture sits on top of the LoRa physical layer. LoRaWAN enables IoT devices to use LoRa for communication. It allows low-powered devices to communicate directly with internet-connected applications over a long-range wireless connection.

The LoRa Alliance describes LoRaWAN as, *"a Low Power, Wide Area (LPWA) networking protocol designed to wirelessly connect battery operated 'things' to the internet in regional, national or global networks"*
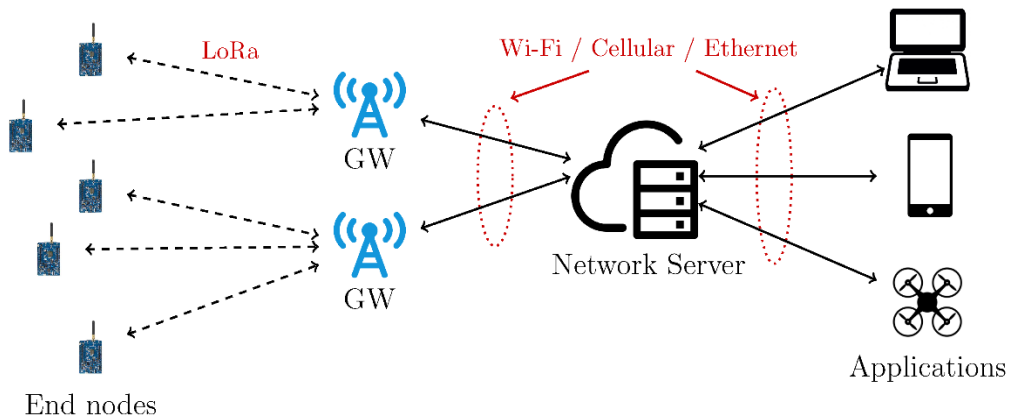
LoRaWAN Architecture

NB-IoT (Narrowband IoT)

NB-IoT is a cellular, wireless IoT protocol developed by 3GPP, using low-power wide area network (LPWAN) technology. Unlike LTE-M, NB-IoT can co-exist with both GSM and LTE mobile networks. The underlying technology is much simpler making the NB-IoT even more cost effective. NB-IoT uses DSSS modulation, which requires specific hardware.

The protocol focuses specifically on indoor coverage with improved the power consumption of user devices, system capacity and spectrum efficiency, especially in deep coverage requiring high connection density. A Battery life of more than 10 years can be supported for a wide range of use cases. The NB-IoT Connector requires a predefined MQTT-SN message content structure for processing the data and connection to Cloud of Things.

NB-IoT Architecture - (source: www.sciencedirect.com)

LTE-M

LTE Cat M is the other cellular based wireless IoT protocol built upon the already existing LTE network. Unlike NB-IoT LTE-M solely depends on 4G. It allows IoT devices to connect directly to a 4G network, without a gateway and while running on batteries. Compared to LTE, LTE-M has a much simpler architecture and isn't particularly fast. LTE-M trades in data transmission rate for better power efficiency and signal range. However, it's several times faster than NB-IoT.

Unlike LoRaWAN (which is unlicensed and free to access for both network operators and device manufacturers), both LTE-M and NB-IoT operates in a spectrum licensed for cellular networks and is optimized for spectrum efficiency over everything else.
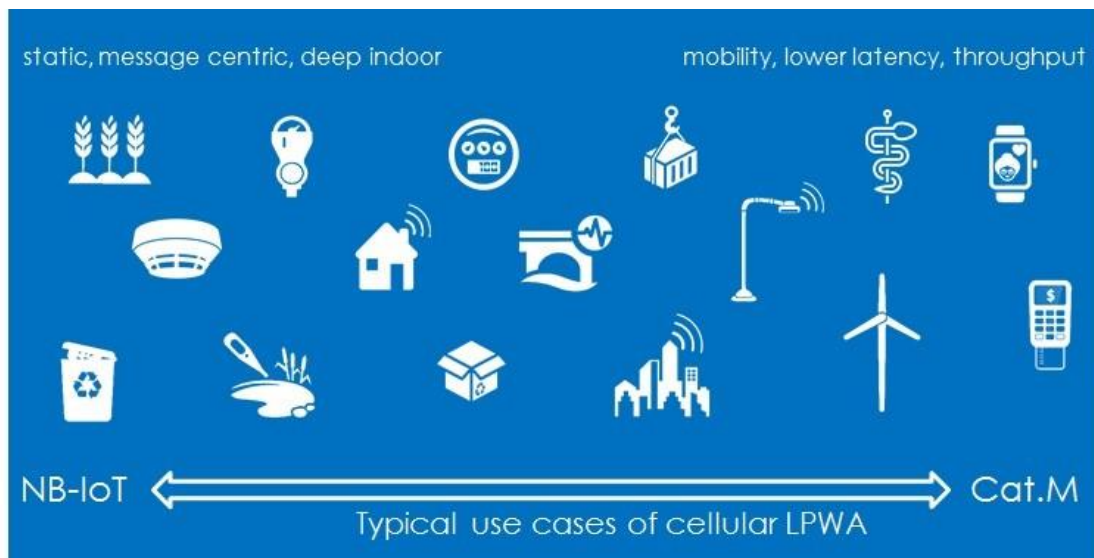
Wireless Network Protocols – A Brief Comparison

Protocol	Power Consumption	Optimized for extended battery life	Nominal Range	Average Data Rate	Spectrum
Wi-Fi (WLAN)	Medium	✗	Local (< 100m)	> 100 Mbps	2.4Ghz/5Ghz unlicensed
Low power Wi-Fi (WLAN)	Low to medium	✗	70 – 225 m	15 Mbps	2.4Ghz/5Ghz unlicensed
Bluetooth (WPAN)	Low	✓	Contact (<4cm)	100 kbps	13.56Mhz unlicensed
4G/LTE (Cellular)	Low to medium	✗	Metro (>30km)	>100 Mbps	Licensed Cellular
5G (Cellular)	Low to medium	✗	Metro (>30km)	>10 Gbps	Licensed Cellular
Zigbee (WPAN)	Medium	✓	10 – 100 m	250 kbps	2.4Ghz unlicensed
LoRaWAN (LPWAN)	Low to medium	✓	2 – 15 km	<50 kbps	900Mhz, 868Mhz, 433Mhz unlicensed
LTE-M (LPWAN - cellular)	Low	✓	1 – 11 km	1 Mbps	Licensed Cellular
NB-IoT (LPWAN - cellular)	Low	✓	1 – 15 km	200 kbps	Licensed Cellular
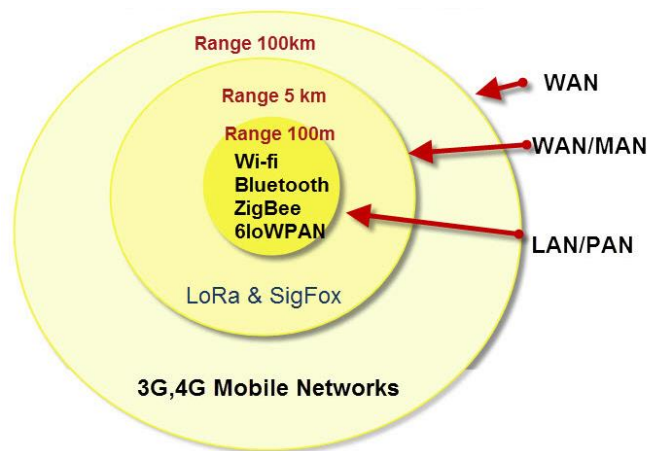
Ranges – Wireless Protocols (Source: http://www.steves-internet-guide.com/)

Characteristics to consider before selecting IOT Protocols for a project

Bottom Line, selecting the correct protocols and standards for any IoT project is crucial. Some factors to consider before selecting a suitable IoT protocol are;

- Speed – Amount of data that can be transferred/second
- Latency – amount of time a message takes to be transferred
- Power consumption
- Power requirements
- Certification and Standards
- Security and Reliability
- Range
- Unit costs
- Data throughput
- Attenuation
- IP capability
- Ease of deployment. – Example LTE-M uses the same base station equipment as LTE and requires only a software upgrade to deploy

END