Communication Technologies in IoT

Communications technology, also known as information technology, refers to all equipment and programs that are used to process and communicate information.

Bluetooth

An important short-range communications technology is of course Bluetooth, which has become very important in computing and many consumer product markets. It is expected to be key for wearable products in particular, again connecting to the IoT albeit probably via a smartphone in many cases. The new Bluetooth Low-Energy (BLE) – or Bluetooth Smart, as it is now branded – is a significant protocol for IoT applications. Importantly, while it offers similar range to Bluetooth it has been designed to offer significantly reduced power consumption.

However, Smart/BLE is not really designed for file transfer and is more suitable for small chunks of data. It has a major advantage certainly in a more personal device context over many competing technologies given its widespread integration in smartphones and many other mobile devices. According to the Bluetooth SIG, more than 90 percent of Bluetooth-enabled smartphones, including iOS, Android and Windows based models, are expected to be 'Smart Ready' by 2018.

Devices that employ Bluetooth Smart features incorporate the Bluetooth Core Specification Version 4.0 (or higher – the latest is version 4.2 announced in late 2014) with a combined basic-data-rate and low-energy core configuration for a RF transceiver, baseband and protocol stack. Importantly, version 4.2 via its Internet Protocol Support Profile will allow Bluetooth Smart sensors to access the Internet directly via 6LoWPAN connectivity (more on this below). This IP connectivity makes it possible to use existing IP infrastructure to manage Bluetooth Smart 'edge' devices. More information on Bluetooth 4.2 is available here and a wide range of Bluetooth modules are available from RS.

- Standard: Bluetooth 4.2 core specification
- Frequency: 2.4GHz (ISM)
- Range: 50-150m (Smart/BLE)
- Data Rates: 1Mbps (Smart/BLE)

Zigbee

ZigBee, like Bluetooth, has a large installed base of operation, although perhaps traditionally more in industrial settings. ZigBee PRO and ZigBee Remote Control (RF4CE), among other available ZigBee profiles, are based on the IEEE802.15.4 protocol, which is an industry-standard wireless networking technology operating at 2.4GHz targeting applications that require relatively infrequent data exchanges at low data-rates over a restricted area and within a 100m range such as in a home or building.

ZigBee/RF4CE has some significant advantages in complex systems offering low-power operation, high security, robustness and high scalability with high node counts and is well positioned to take advantage of wireless control and sensor networks in M2M and IoT applications. The latest version of ZigBee is the recently launched 3.0, which is essentially the unification of the various ZigBee wireless standards into a single standard.

- Standard: ZigBee 3.0 based on IEEE802.15.4
- Frequency: 2.4GHz
- Range: 10-100m
- Data Rates: 250kbps

Z-Wave

Z-Wave is a low-power RF communications technology that is primarily designed for home automation for products such as lamp controllers and sensors among many others. Optimized for reliable and low-latency communication of small data packets with data rates up to 100kbit/s, it operates in the sub-1GHz band and is impervious to interference from WiFi and other wireless technologies in the 2.4-GHz range such as Bluetooth or ZigBee. It supports full mesh networks without the need for a coordinator node and is very scalable, enabling control of up to 232 devices. 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.

- Standard: Z-Wave Alliance ZAD12837 / ITU-T G.9959
- Frequency: 900MHz (ISM)
- Range: 30m
- Data Rates: 9.6/40/100kbit/s

6LowPAN

A key IP (Internet Protocol)-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 and header compression mechanisms. The standard has the freedom of frequency band and physical layer and can also be used across multiple communications platforms, including Ethernet, Wi-Fi, 802.15.4 and sub-1GHz ISM. A key attribute is the IPv6 (Internet Protocol version 6) stack, which has been a very important introduction in recent years to enable the IoT. IPv6 is the successor to IPv4 and offers approximately 5 x 10^{28}addresses for every person in the world, enabling any embedded object or device in the world to have its own unique IP address and connect to the Internet. Especially designed for home or building automation, for example, IPv6 provides a basic transport mechanism to produce complex control systems and to communicate with devices in a cost-effective manner via a low-power wireless network.

Designed to send IPv6 packets over IEEE802.15.4-based networks and implementing open IP standards including TCP, UDP, HTTP, COAP, MQTT, and websockets, the standard offers end-to-end addressable nodes, allowing a router to connect the network to IP. 6LowPAN is a mesh network that is robust, scalable and self-healing. Mesh router devices can route data destined for other devices, while hosts are able to sleep for long periods of time.

- Standard: RFC6282
- Frequency: (adapted and used over a variety of other networking media including Bluetooth Smart (2.4GHz) or ZigBee or low-power RF (sub-1GHz)
- Range: N/A
- Data Rates: N/A

Thread

A very new IP-based IPv6 networking protocol aimed at the home automation environment is Thread. Based on 6LowPAN, and also like it, it is not an IoT applications protocol like Bluetooth or ZigBee. However, from an application point of view, it is primarily designed as a complement to WiFi as it recognises that while WiFi is good for many consumer devices that it has limitations for use in a home automation setup.

Launched in mid-2014 by the Thread Group, the royalty-free protocol is based on various standards including IEEE802.15.4 (as the wireless air-interface protocol), IPv6 and 6LoWPAN, and offers a resilient IP-based solution for the IoT. Designed to work on existing IEEE802.15.4 wireless silicon from chip vendors such as Freescale and Silicon Labs, Thread supports a mesh network using IEEE802.15.4 radio transceivers and is capable of handling up to 250 nodes with high levels of authentication and encryption. A relatively simple software upgrade should allow users to run thread on existing IEEE802.15.4-enabled devices.

- Standard: Thread, based on IEEE802.15.4 and 6LowPAN
- Frequency: 2.4GHz (ISM)
- Range: N/A
- Data Rates: N/A

WiFi

WiFi connectivity is often an obvious choice for many developers, especially given the pervasiveness of WiFi within the home environment within LANs. It requires little further explanation except to state the obvious that clearly there is a wide existing infrastructure as well as offering fast data transfer and the ability to handle high quantities of data.

A wireless network uses radio waves to communicate with portable devices, granting them access to other connected devices and to the Internet. Depending on the specific type of wireless network you use, Wi-Fi signals travel in two distinct frequency ranges. The 802.11b and g networks use the 2.4 GHz band, while 802.11a networks use 5 GHz and 802.11n networks broadcast on both frequencies to increase throughput.

Currently, the most common WiFi standard used in homes and many businesses is 802.11n, which offers serious throughput in the range of hundreds of megabit per second, which is fine for file transfers, but may be too power-consuming for many IoT applications. A series of RF development kits designed for building WiFi-based applications are available from RS.

- Standard: Based on 802.11n (most common usage in homes today)
- Frequencies: 2.4GHz and 5GHz bands
- Range: Approximately 50m
- Data Rates: 600 Mbps maximum, but 150-200Mbps is more typical, depending on channel frequency used and number of antennas (latest 802.11-ac standard should offer 500Mbps to 1Gbps)

Cellular

< Any IoT application that requires operation over longer distances can take advantage of GSM/3G/4G cellular communication capabilities. While cellular is clearly capable of sending high quantities of data, especially for 4G, the expense and also power consumption will be too high for many applications, but it can be ideal for sensor-based low-bandwidth-data projects that will send very low amounts of data over the Internet. A key product in this area is the SparqEE range of products, including the original tiny CELLv1.0 low-cost development board and a series of shield connecting boards for use with the Raspberry Pi and Arduino platforms.

- Standard: GSM/GPRS/EDGE (2G), UMTS/HSPA (3G), LTE (4G)
- Frequencies: 900/1800/1900/2100MHz
- Range: 35km max for GSM; 200km max for HSPA
- Data Rates (typical download): 35-170kps (GPRS), 120-384kbps (EDGE), 384Kbps-2Mbps (UMTS), 600kbps-10Mbps (HSPA), 3-10Mbps (LTE)

NFC

NFC (Near Field Communication) is a technology that enables simple and safe two-way interactions between electronic devices, and especially applicable for smartphones, allowing consumers to perform contactless payment transactions, access digital content and connect electronic devices. Essentially it extends the capability of contactless card technology and enables devices to share information at a distance that is less than 4cm.

- Standard: ISO/IEC 18000-3
- Frequency: 13.56MHz (ISM)
- Range: 10cm
- Data Rates: 100–420kbps

Sigfox

An alternative wide-range technology is Sigfox, which in terms of range comes between WiFi and cellular. It uses the ISM bands, which are free to use without the need to acquire licenses, to transmit data over a very narrow spectrum to and from connected objects. The idea for Sigfox is that for many M2M applications that run on a small battery and only require low levels of data transfer, then WiFi's range is too short while cellular is too expensive and also consumes too much power. Sigfox uses a technology called Ultra Narrow Band (UNB) and is only designed to handle low data-transfer speeds of 10 to 1,000 bits per second. It consumes only 50 microwatts compared to 5000 microwatts for cellular communication, or can deliver a typical stand-by time 20 years with a 2.5Ah battery while it is only 0.2 years for cellular.

Already deployed in tens of thousands of connected objects, the network is currently being rolled out in major cities across Europe, including ten cities in the UK for example. The network offers a robust, power-efficient and scalable network that can communicate with millions of battery-operated devices across areas of several square kilometres, making it suitable for various M2M applications that are expected to include smart meters, patient monitors, security devices, street lighting and environmental sensors. The Sigfox system uses silicon such as the EZRadioPro wireless transceivers from Silicon Labs, which deliver industry-leading wireless performance, extended range and ultra-low power consumption for wireless networking applications operating in the sub-1GHz band.

- Standard: Sigfox
- Frequency: 900MHz
- Range: 30-50km (rural environments), 3-10km (urban environments)

- Data Rates: 10-1000bps

Neul

Similar in concept to Sigfox and operating in the sub-1GHz band, Neul leverages very small slices of the TV White Space spectrum to deliver high scalability, high coverage, low power and low-cost wireless networks. Systems are based on the Iceni chip, which communicates using the white space radio to access the high-quality UHF spectrum, now available due to the analogue to digital TV transition. The communications technology is called Weightless, which is a new wide-area wireless networking technology designed for the IoT that largely competes against existing GPRS, 3G, CDMA and LTE WAN solutions. Data rates can be anything from a few bits per second up to 100kbps over the same single link; and devices can consume as little as 20 to 30mA from 2xAA batteries, meaning 10 to 15 years in the field.

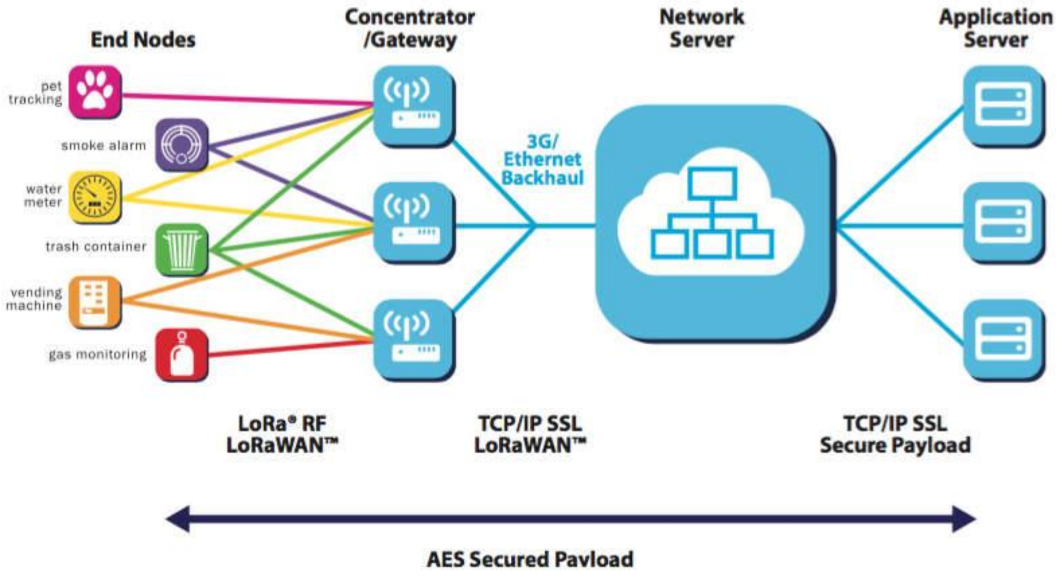
- Standard: Neul
- Frequency: 900MHz (ISM), 458MHz (UK), 470-790MHz (White Space)
- Range: 10km
- Data Rates: Few bps up to 100kbps

LoRaWAN

LoRaWAN is a media access control (MAC) protocol for wide area networks. It is designed to allow low-powered devices to communicate with Internet-connected applications over long range wireless connections. LoRaWAN can be mapped to the second and third layer of the OSI model. It is implemented on top of LoRa or FSK modulation in industrial, scientific and medical (ISM) radio bands. The LoRaWAN protocols are defined by the LoRa Alliance and formalized in the LoRaWAN Specification which can be requested on the LoRa Alliance website.

Terminology

- **End Device, Node, Mote** - an object with an embedded low-power communication device.
- **Gateway** - antennas that receive broadcasts from End Devices and send data back to End Devices.
- **Network Server** - servers that route messages from End Devices to the right Application, and back.
- **Application** - a piece of software, running on a server.
- **Uplink Message** - a message from a Device to an Application.
- **Downlink Message** - a message from an Application to a Device



Again, similar in some respects to Sigfox and Neul, LoRaWAN targets wide-area network (WAN) applications and is designed to provide low-power WANs with features specifically needed to support low-cost mobile secure bi-directional communication in IoT, M2M and smart city and industrial applications. Optimized for low-power consumption and supporting large networks with millions and millions of devices, data rates range from 0.3 kbps to 50 kbps.

- Standard: LoRaWAN
- Frequency: Various
- Range: 2-5km (urban environment), 15km (suburban environment)
- Data Rates: 0.3-50 kbps.

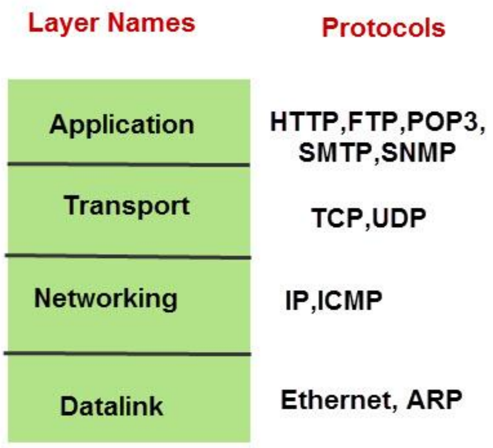
The TCP/IP Protocol

Perhaps to understand how all these communication technologies fit together, we need to start of from a familiar communication technology that we all understand, which is the TCP/IP protocol.

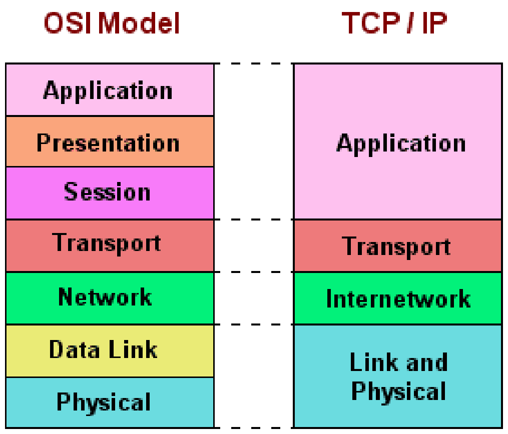
Transmission Control Protocol/Internet Protocol (TCP/IP) is the language a computer uses to access the internet. It consists of a suite of protocols designed to establish a network of networks to provide a host with access to the internet.

TCP/IP is responsible for full-fledged data connectivity and transmitting the data end to end by providing other functions, including addressing, mapping and acknowledgment. TCP/IP contains four layers, which differ slightly from the OSI model.

The technology is so common that one would rarely use the full name. In other words, in common usage the acronym is now the term itself.



TCP/IP Networking Model



Link layer: This layer is also known as the network access layer and is the equivalent of both the physical and data link layers of the OSI model. It deals with components such as cables, connectors, and network cards, like OSI Layer 1. Like Layer 2 of the OSI model, the link layer of the TCP/IP model is concerned with hardware addresses.

Internet layer: This layer aligns directly with Layer 3 of the OSI model. You may also know this layer as the network layer. It routes data from the source to the destination by defining the packet and the addressing scheme, moving data between the link and transport layers, routing packets of data to remote hosts, and performing fragmentation and reassembly of data packets. The Internet layer is where IP operates.

Transport layer: This layer is directly aligned with Layer 4 of the OSI model: It is the core of the TCP/IP architecture. It is the layer where TCP and UDP operate. This layer provides communication services directly to the application processes that are running on network hosts.

Application layer: This layer corresponds to Layers 5, 6, and 7 of the OSI model. It provides applications for file transfer, network troubleshooting, and Internet activities. It also supports network APIs, which allow programs that have been created for a particular operating system to access the network. An application layer protocol defines how application processes (clients and servers) running on different end systems pass messages to each other

- The types of messages e.g. request messages and response messages
- The syntax of the various message types i.e. the fields in the messages
- The semantics of the field i.e. the meaning of the information that the field is supposed to contain.
- Rules determining when and how a process sends messages and responds to messages.

A Closer Look At GSM

GSM or **Global System for Mobile Communications** is the most popular wireless cellular communication technique, used for public communication. The GSM standard was developed for setting protocols for second generation (2G) digital cellular networks.

It initially started as a circuit switching network, but later packet switching was implemented after integration General Packet Radio Service (GPRS) technology as well. The widely-used GSM frequency bands are 900 MHz and 1800 MHz.

In the Europe and Asia, the GSM operates in 900 to 1800 MHz frequency range, whereas in United States and other American countries, it operates in the 850 to 1900 MHz frequency range. It uses the digital air interface wherein the analog signals are converted to digital signals before transmission. The transmission speed is 270 Kbps.

GSM Architecture

The GSM architecture is divided into Radio Subsystem, Network and Switching Subsystem and the Operation Subsystem. The radio sub system consists of the Mobile Station and Base Station Subsystem.

The mobile station is generally the mobile phone which consists of a transceiver, display and a processor. Each handheld or portable mobile station consists of a unique identity stored in a module known as SIM (Subscriber Identity Chip). It is a small microchip which is inserted in the mobile phone and contains the database regarding the mobile station.

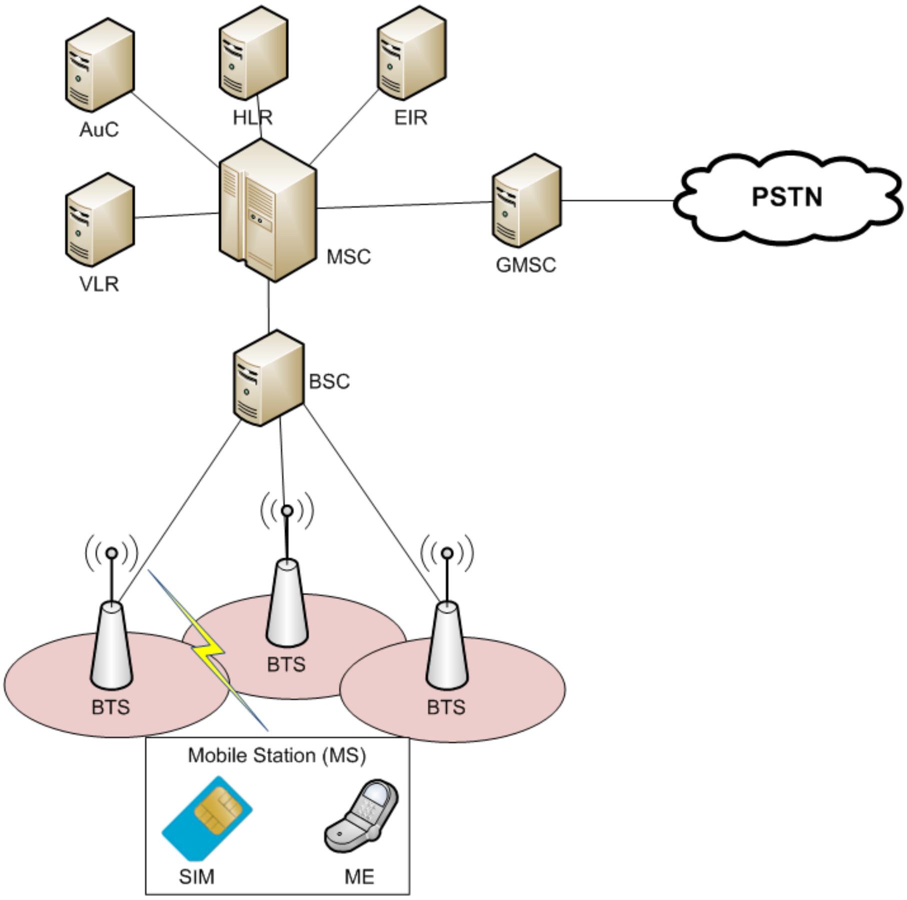


Fig – GSM Network architecture

The base station subsystem

It connects the mobile station with the network subsystem via the air interface.

It consists of the below given elements:

Base Transceiver Station: One or more Base Transceiver Station provides physical connection of a mobile station to the network in form of air interface. Depending on load, subscriber behaviour and morph structure, it can have different configurations – Standard configuration (Each BTS is assigned a different cell identity (CI) and several BTS forms a location area).

Umbrella Cell configuration (One BTS with high transmission power installed at a higher altitude, acting as an umbrella to the lower transmission power Base Transmitter Stations), Collocated configurations (several BTSs collocated at one site, but antennas cover only area of 120 or 180 degrees). It is a network of neighbouring radio cells which provide a complete coverage of the service area.

Base Station Controller: It controls operation of one more Base Transceiver Stations, basically the handover or power control. It consists of a database comprising the whole maintenance status of the BTS, quality of radio and terrestrial resources and BTS operations software).

Transcoding Rate and Adaption Unit: It is located between a Base Station Controller and a Mobile Switching Centre. It compresses or decompresses speech from the mobile station. However, it is not used for data connections.

Network Switching Subsystem: It provides the complete set of control and database functions needed to set up a call using encryption, authentication and roaming features. It basically provides network connection to the Mobile Station. It consists of the below given elements

Mobile Switching Centre: It is the main element within the overall GSM network. It is like a Public Switched Telephone Network (PSTN) exchange or Integrated Services Digital Network (ISDN) exchange. Apart from the normal functionary, it supports additional functionality like registration, authentication, call location and call routing to the subscriber.

It provides interfaces to Public Switched Telephone Network (PSTN) for connection with landline or interface to another Mobile Switching Centre (MSC) for connection to another mobile phone.

Home Location Register: It is a repository which stores data belonging to large number of subscribers. It is basically a large database which administers data of each subscriber. For security purposes, it maintains subscriber specific parameter such as parameter Ki, known only to the HLR and the SIM.

Virtual Location Register: It is similar to Home Location Register (HLR) , but differs in the fact that it stores dynamic information regarding the subscriber data. It comes to act in case of roaming where a subscriber moves from one location to another. The information is stored in the Equipment Identity Register that maintains account of all mobile stations, each identified by their International Mobile Equipment Identity (IMEI) number.

A Closer Look at MQTT

MQTT is a Client Server publish/subscribe messaging transport protocol. It is light weight, open, simple, and designed so as to be easy to implement. These characteristics make it ideal for use in many situations, including constrained environments such as for communication in Machine to Machine (M2M) and Internet of Things (IoT) contexts where a small code footprint is required and/or network bandwidth is at a premium. MQ Telemetry Transport

It was, and is, designed for small, constrained devices and makes design decisions based on those constraints. Concepts which are important in the IoT world, such as memory, bandwidth, latency, power consumption, and network reliability. Let's focus in on one of the main MQTT concepts, the publish/subscribe pattern.

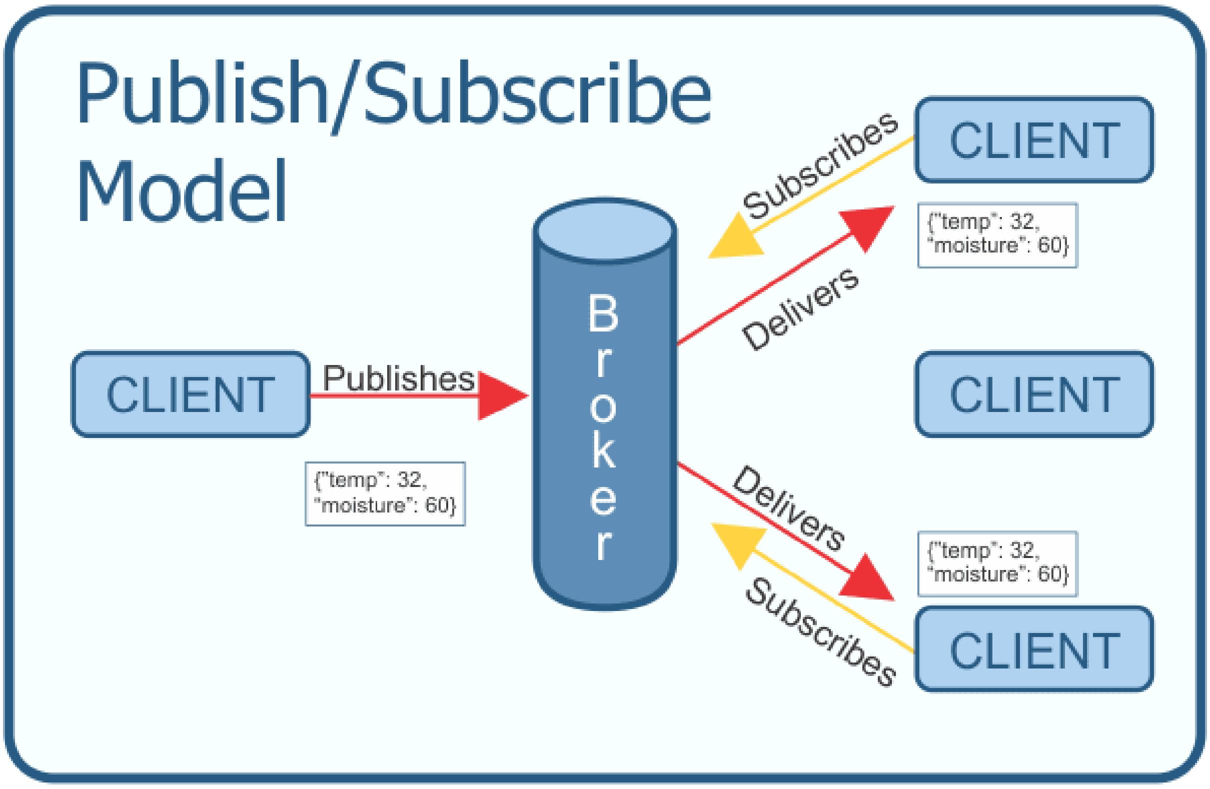
MQTT Publish/Subscribe Pattern

In a publish/subscribe pattern a client publishes information and another client can *subscribe* to the information it wants. In many cases there is a broker between the clients who facilitates and/or filters the information. This allows for a loose coupling between entities.

The decoupling can occur in a few different ways, space, time, and synchronization.

- Space - the subscriber doesn't need to know who the publisher is, for example by IP address, and vice-versa
- Time - the two clients don't have to be running at the same time
- Synchronization - Publishing and receiving doesn't halt operations

Through the filtering done on the broker not all subscribers have to get the same messages. The broker can filter on subject, content, or type of message. A client, therefore could subscribe to only messages about temperate data. Or only messages with content about centrifuge machines. Or, perhaps, we only want to receive information about specific types of errors.



Once connected to the broker the publishing client simply sends its data to the broker. Once there, the broker relays the appropriate data onto the clients who have subscribed for that data. Again, those subscriptions can be filtered. All of this data transferring is done in a light weight fashion designed for small, resource limited devices.

Message Packet

The message packet shown in the above diagram is just an example. Along with the message, or payload, a real packet would include additional information such as a packet ID, topic name, quality of service (QoS) level. Also included in the packet would be flags so the broker knows how long to retain the message and if the message is a duplicate.