# IoT Protocols Overview

## Abstract:

The advancement of IIoT 4.0 for smart factories, cities and buildings ushers in many exciting possibilities for improved automation and capabilities. IoT devices are unlocking the great potential for improved efficiency and improved user experiences. However, there are many different IoT protocols, network topologies and frequency bands, making IoT an intranet of things and not an internet of things. Therefore, in order to determine which IoT technology to use in solving your use case and future proofing your investment, an understanding of the IoT ecosystem is needed. This is the first in a series of papers describing the different protocols, topologies and frequency bands used in IoT deployments.

Clint Smith, P.E:
csmith@nextgconnect.com

The internet of things (IoT) used in industrial, military, commercial, enterprise or consumer devices is anything but a simple topic. The vastness of the types of IoT devices, their operating systems, capabilities, methods of communication, as well as initial and recurring cost in selecting the proper device that meets the use case requirements challenging.

The advancement of Industrial IoT (IIoT) 4.0 for smart factories, cities and buildings ushers in many exciting possibilities for improved automation. IoT facilitates the exchange of data between the physical world and a user or computer application. IoT devices collect and create massive amounts of data as well as exchange that data with other devices to enable actions to take place based on the data and policy rule sets defined.

IoT devices are found in many places. Some are currently deployed in industrial, transportation, health, smart cities, smart buildings, energy utilities, security and consumer products. However, the IoT industry is fragmented based on the plethora of devices and protocols being utilized. The fragmentation of the IoT industry has created an Intranet of things and not an Internet of things.

Ideally everything should utilize the internet protocol (IP), be open source and use REST commands with a common API. Unfortunately, reality is quite different and there is no single answer and sometimes your decision was made based on legacy platforms already in place.

There are numerous sources of information available regarding IoT devices from the internet and vendors all pushing a particular solution. In fact, the information is so vast and dispersed that making a detailed informed decision is beyond a challenging task.

However, if you are embarking or have embarked on an IoT path you need to be aware of the various options to pick from. Although the IoT decision process involves many steps or decision points the first thing that you need to do is determine your objective and use case. The objective determination is more of a business decision than a technical one because the business decision should be driving the technical decision. Specifically, defining what your use case or cases are that you need to solve is critical in the IoT selection process.

Choosing a particular protocol also impacts the efficiency and performance of the IoT solution and with numerous diverse protocols out there for IoT, it is hard for one to decide which ones to use. To help in the decision process this paper gives an overview of the protocols available in IoT world. This is the first in a series of papers describing the various IoT protocols that are prevalent and will focus on identifying the various protocols, frequencies and topologies that exist. The remaining papers will provide details about each of the various protocols with links to perform a deeper dive.

Figure 1 is a high-level depiction of an IoT sensor that communicates with a middleware platform to reach the application as part of the IoT ecosystem. The three different protocol classifications shown in Figure 1 the device, communication and application protocols. The true demarcation of where one protocol function begins and ends is dependent upon what your particular use case is.

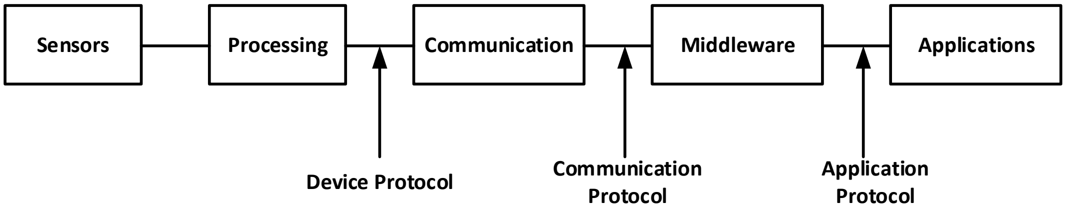


**Figure 1**: IoT Protocol locations

There are numerous data link or device protocols used for IoT. Each of the data link protocols is designed to solve a particular problem and there is currently no single data link protocol that solves everything.

All data links can be classified as either tethered or wireless. Whether the selected data link protocol is tethered or wireless, it should match the objective for the problem you are trying to solve. If you need mobility, then a data link protocol providing mobility should be looked into. The mobility protocols available for use involve both licensed and license exempt spectrum usages. Most, if not all, licensed spectrum data link protocols have monthly recurring costs and these need to be understood. Also, other data link protocols are closed systems with one hardware vendor or the protocol is not published.

It is necessary to look into the details of any device and protocol that you are considering. For instance, some data link protocols are not well suited for software updates, patches or configuration changes. Others utilize a mesh or star topology as part of the data link protocol where coverage and potential throughput need to be understood.

Then there are different frequencies for the wireless data link protocols. Some are meant for short range low data speeds using sub GHz frequencies. Others are meant for short range but higher data speeds using ISM frequencies. Also there are protocols offering long range and low data rates and others with long range and high data rates.

As you can quickly gather there are numerous issues that should be thought about and weighed regarding their technical and business merits. It's important to always remember that once you begin using a data link protocol changing to another will prove difficult and time consuming which both equate to money.

When determining which data link protocol to utilize keep in mind that there are numerous IoT devices and protocols which have not been commercially successful with limited roll outs resulting in stranded systems.

Therefore Table 1 is a list of most of the IoT Device Protocols that are in use presently. Table 1 has four categories in it. The first category is the tethered group which includes protocols associated primarily with wired connections. The second category is listed as wireless and while the remaining two are also wireless, this category fundamentally covers the device protocols using license exempt frequencies. The third category involves cellular which includes wireless broadband. The fourth category lists the primary cellular IoT technologies that are used.

If you have not heard of some of the protocols listed in table 1 you are not alone. If you do not know a particular protocol that is listed, it would be good to possibly investigate it a little more. As always, the devil is in the details and the table provided is meant to help start culling the options you are trying to figure out for your use case.

| IoT Device Protocols | | | | | | |
|---|---|---|---|---|---|---|
| **Tethered** | 802.3 Ethernet | IPv4/IPv6 | BarCode | RS-232 | RS-422 | RS-485 |
| | 4-20mA | SPI | I2C | HART | Modbus | LonTalk |
| | Fieldbus | ARCNet | ProfiNet | Foundation Fieldbus | Profibus | Interbus |
| | BACNet | LonWorks | CEBus | X10 | PLC | G.hn |
| **Wireless** | WiFi (WiFi6) | BLE | Bluetooth | ZigBee | RFID | NFC |
| | 6LoWPAN (6Lo) | 802.15.4 | Zwave | Sigfox | LoRa | LwM2M |
| | Wireless HART | DASH7 (DA7) | RuBee | ANT | EnOcean | Weightless P |
| | ISA100 | WiFi HaLow 802.ah | Ingenu RPMA | Telensa | Nwave | Neul |
| | NB-Fi | Wi SUN/ 802.15.4g | | | | |
| **Cellular** | GSM | CDMA | UMTS | LTE | WiMax | Satellite |
| **Cellular IoT** | Cat 4 | Cat 0 | LTE Cat M1 | LTE NB IoT | EC-GSM-IoT | DECT/ULE-ultra low energy |

Note: some protocols include higher OSI layers

**Table 1**: IoT Device Protocols

To complicate things some of the protocols listed in Table 1 include some higher OSI layers. Furthermore, some of the IoT device protocols are part of a closed system limiting the use to a particular protocol and or vendor even though they claim to be an open standard.

Table 2 is a list of some of the IoT communication (session) protocols. Again, as with the device protocol list some of the protocols listed in Table 2 span multiple OSI layers.

| IoT Communication Protocols | | | | | |
|---|---|---|---|---|---|
| XMPP | HTTP/REST | SNMP | SMS | HTTP/2 | SOAP |
| CoAP | MQTT | SMQTT | IEEE 1451 | AMQP | LLAP |
| Hart-ip | IBS | DNP3 | IEC61850 | CANopen | DDS |
| IEC 60870 | IEC 61968 | IEC 61968 | Multispeak | SSI | ZeroMQ |
| Websocket | IEC61334 | UPnP | IoTivity | DeviceNet | IEEE 1905.1 |
| BACNet | Modbus | LonWorks | Sinec H1 | MTConnect | Continua HDP |
| IEEE P2413 | Weave | | | | |

Note: some protocols include higher OSI layers

**Table 2**: IoT Communication Protocols

In addition to device protocols and session protocols there are application protocols shown in Table 3. Table 3 lists some of the more prevalent IoT application protocols that are present today.

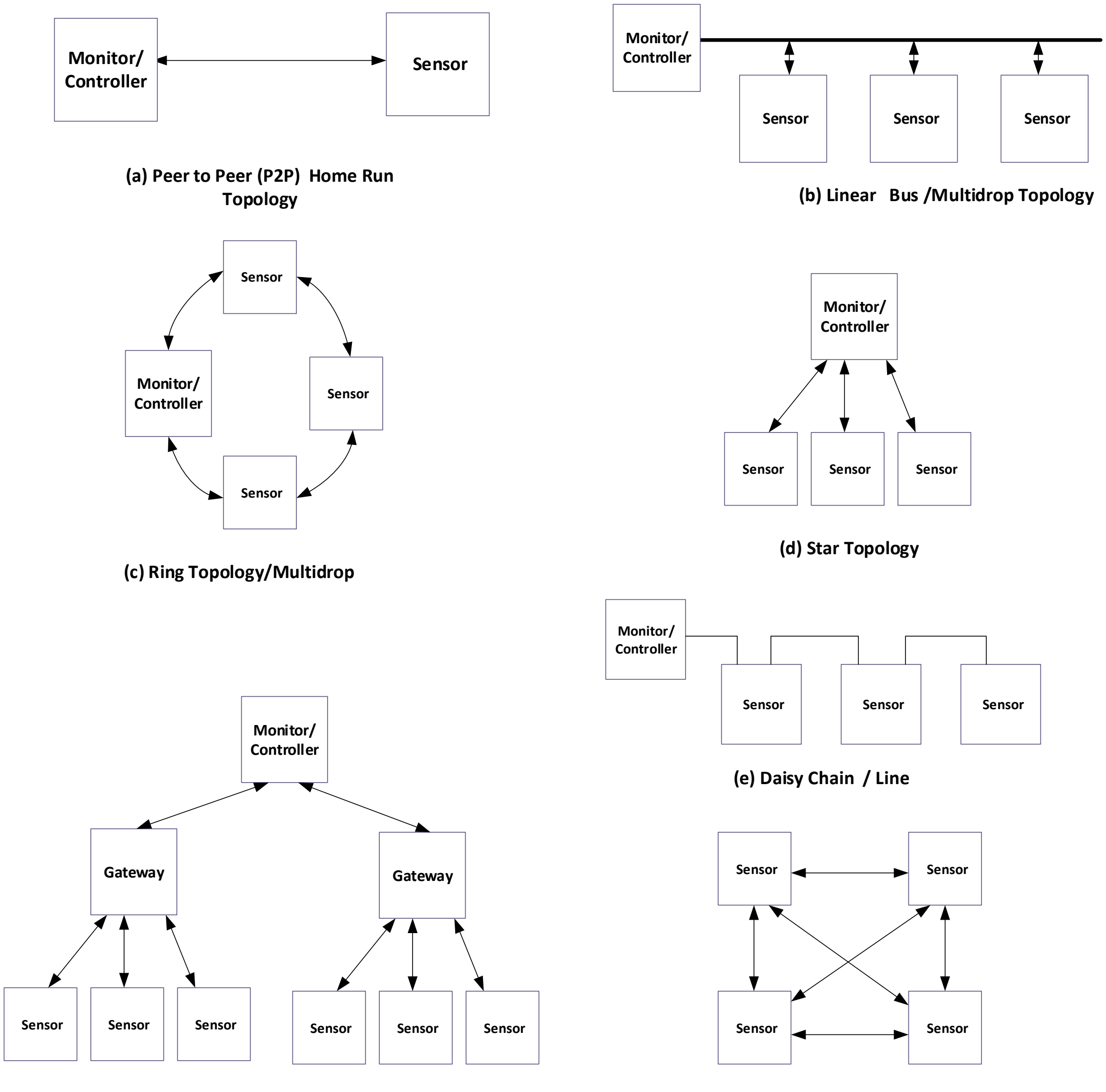
| Application Protocols | | | | |
|---|---|---|---|---|
| Juniper Mist | Haystack | AllJoyn | Thread | Tingsquare Mist |
| EEBus Spine | Dotdot 1.0 | IoTivity | ONVIF | KNX |
| HomeKit | Symphony Link | MyriaNed | Insteon | Senet |
| IoLink | Home Pod | AWS IoT | Google IoT | Azure IoT |
| Home Connect | SmartThings Hub | Amazon Echo | Google Home | Nest |

**Table 3**: IoT Application Protocols

Besides device, communication and application protocols there are numerous dashboards and OSI layer 7 applications that are available for IoT systems. These dashboard systems are how the user or device manager views their IoT world from. Therefore, when making a choice of which IoT device or devices to utilize, you need to include in the decision selection process how you will interface with the devices and system through a management layer. A key consideration about which dashboard or application you select needs to be based on what your use case is.

Each IoT device protocol and higher layers has a particular network topology it was initially designed for. When investigating an IoT solution there are numerous types of network topologies that can be used and each with its own set of unique benefits.

Figure 2 is a high-level depiction of the various network topologies. Some IoT technologies and implementations scenarios utilize a hybrid approach where there are multiple topologies used in different branches of the system.



(a) Peer to Peer (P2P) Home Run Topology

(b) Linear Bus /Multidrop Topology

(c) Ring Topology/Multidrop

(d) Star Topology

(e) Daisy Chain / Line

(f) Hierarchial (Tree) Topology

(g) Mesh Topology

**Figure 2**: Network Topologies

In addition to the network topologies shown in figure 2 there is another topology which involves clouds. The use of cloud network as part of your solution may or may not be appropriate depending on your use case. However, it is likely some part of your IoT solution will incorporate the use of a cloud solution.

As you would expect there are numerous sources for clouds available. However, keep in mind that not all cloud solutions are the same and that interoperability and real portability needs to be considered otherwise you will be locked into one service provider or solution.

Regardless a cloud environment for IoT can be looked at in three layers: cloud, fog and mist and they are shown in figure 3. In figure 3 the main layer is the cloud and it is a more traditional network model using remote servers running in a virtual environment instead of being run locally. The cloud service provides the ability to perform heavy computing, storage, and analytics. Devices can connect to the cloud directly or via an intermediary like a fog or mist environment.

A fog environment shown in figure 3 is meant to extend cloud computing closer to the edge of the network. This has many advantages for an IoT environment reducing latency, performing less intensive computing functions and minimizing the amount of data that is sent to the cloud which is not needed. Fog environments are more geographically dispersed than cloud networks. The fog environment can be thought of as an intermediate level cloud.

The next lower level cloud environment shown in figure 3 is called a mist or rather edge computing. Mist computing is meant to provide edge computing for the network. Devices making up a mist environment perform smaller functions that do not need to be elevated to the fog or cloud environments. Many mist clouds can reside within a fog environment. The mist environment is a true distributed computing environment.

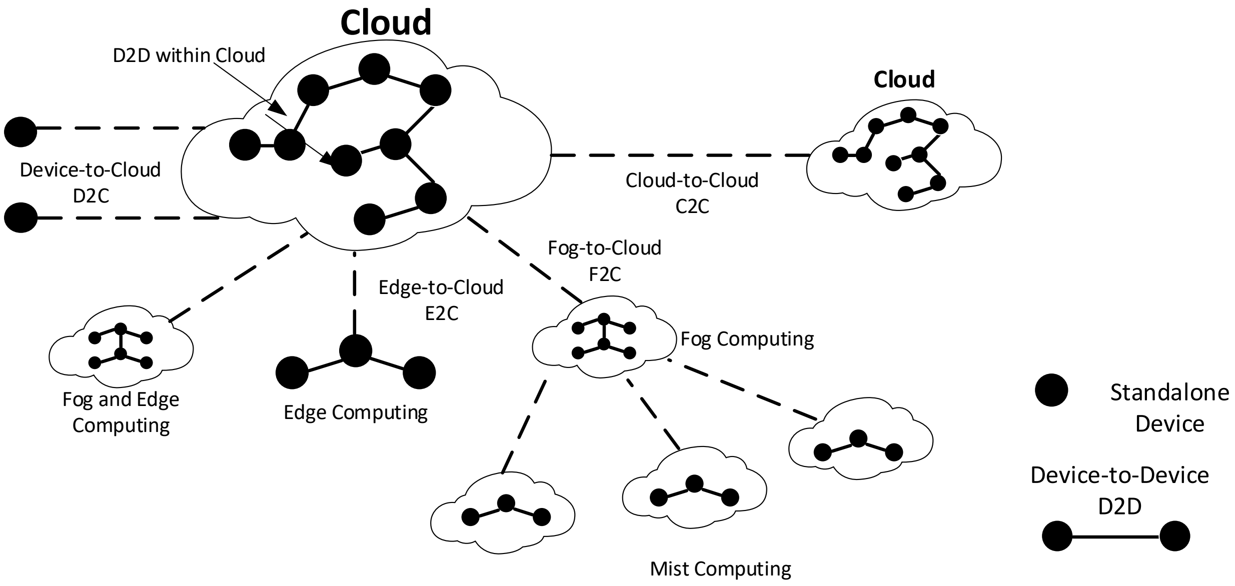


**Figure 3**: Cloud Topologies

IoT devices not only utilize a multitude of protocols and topologies they also operate in a multitude of different frequency bands. The frequency band used by the IoT device can be licensed or unlicensed and it can be either stationary, semi-mobile or mobile. The frequency band used by the IoT device has a large impact on how the use case solution is solved. For instance, devices using lower frequencies in the spectrum have more range while devices using higher frequencies can support more data rich solutions.

Figure 4 is a brief overview of the US spectrum which applies to wireless IoT devices. In reviewing figure 4 the different frequency bands which are available for IoT use are vast. In addition, all the frequency bands with the exception of the cellular spectrum are license free. IoT devices however are not solely limited to the frequencies listed in figure 4.

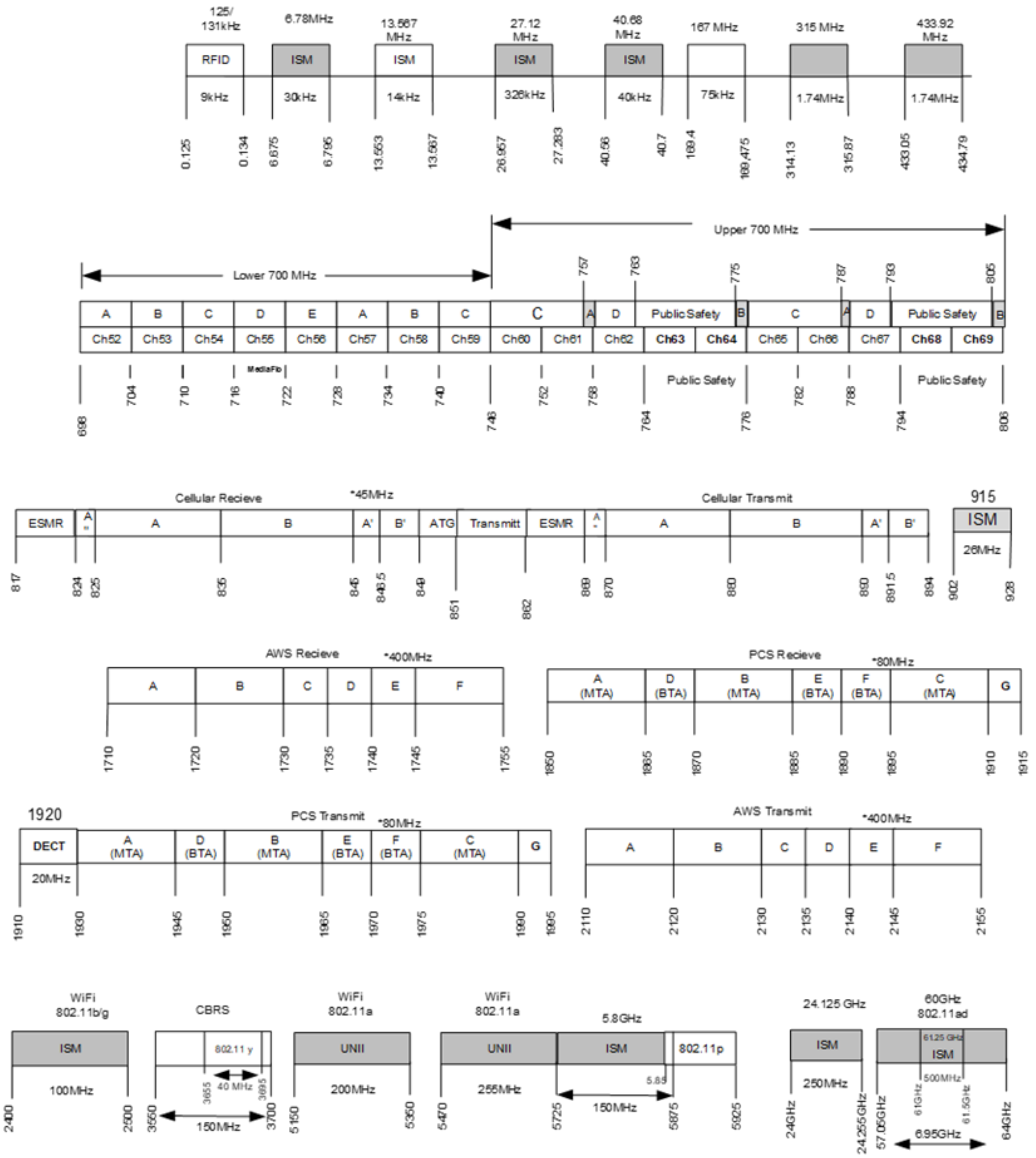


**Figure 4**: US IoT Spectrum

This article hopefully enables you to begin asking some questions you may not have thought about when putting together your IoT solution. However, when deciding on what IoT device protocol you will be utilizing it is important to understand the use case or cases you are solving.

While technology is an important component of IoT there are other issues that need to be addressed when selecting an IoT solution. The 7 Critical Musts for IoT devices you should answer as part of your IoT solution are:

1. Objective/Purpose
2. Security (cyber/physical)
3. Data Acquisition/Functions

4. Standards and Compliance Regulations
5. Business (CapEx/OpEx/Revenue)
6. Interface /User Experience
7. Technology

I trust that you found this first part of the IoT protocol articles useful.

Feel free to utilize this table in any presentation or article. I simply ask you to reference where it came from.

If you want to have a modified version of any of the tables, update, remove, and add some protocols or features/functions please contact us at info@nextgconnect.com with the ask.

Clint Smith, P.E.
Next G Connect
CTO
csmith@nextgconnect.com

**Who we are:**

NGC is a consulting team of highly skilled and experienced professionals. Our background is in wireless communications for both the commercial and public safety sectors. The team has led deployment and operations spanning decades in the wireless technology. We have designed software and hardware for both network infrastructure and edge devices from concept to POC/FOA. Our current areas of focus include 4G/5G, IoT and security.

The team has collectively been granted over 160 patents in the wireless communication space during their careers. We have also written multiple books used extensively in the industry on wireless technology and published by McGraw-Hill.

Feel free to utilize this information in any presentation or article with the simple request you reference its origin.

If you see something that should be added, changed or simply want to talk about your potential needs please contact us at info@nextgconnect.com  or call us at 1.845.987.1787.